(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 990 144**

(51) Int. Cl.:

H04L 9/32 (2006.01)
G06Q 20/38 (2012.01)
G06Q 30/06 (2013.01)
G06Q 30/02 (2013.01)
G06Q 20/32 (2012.01)
G06Q 20/40 (2012.01)
G06Q 20/42 (2012.01)
G06F 16/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.09.2016 PCT/US2016/054920**

(87) Fecha y número de publicación internacional: **20.04.2017 WO17066002**

(96) Fecha de presentación y número de la solicitud europea: **30.09.2016 E 16855952 (4)**

(97) Fecha y número de publicación de la concesión europea: **14.08.2024 EP 3362970**

(54) Título: **Plataforma de identidades y transacciones basada en cadena de bloques**

(30) Prioridad:

17.10.2015 US 201562495574 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.11.2024

(73) Titular/es:

BANQU, INC. (100.0%)
4100 Heatherton Place
Minnetonka, MN 55345, US

(72) Inventor/es:

GADNIS, ASHISH;
KEISER, JEFFREY A.;
LINTON, MICHAEL y
NATALENKO, STANISLAV

(74) Agente/Representante:

MILTENYI, Peter

DESCRIPCIÓN

Plataforma de identidades y transacciones basada en cadena de bloques

Referencia cruzada a solicitud relacionada

Esta solicitud reivindica el beneficio de la Solicitud Provisional de Estados Unidos n.° 62/495.574, presentada el 17 de octubre de 2015, y titulada "UNIVERSAL IDENTITY AND PERSONAL DATA STORAGE, UPDATE AND RETRIEVAL IN THE BLOCKCHAIN. THIS INCLUDES PERSONAL DEMOGRAPHIC INFORMATION, CREDIT HISTORY AND TRANSACTIONS, CONTACTS AND RELATED RELATIONSHIPS, PROPERTY AND ASSET RIGHTS, GENERAL PREFERENCES AND GEO-LOCATION. ALL STORED IN THE BLOCKCHAIN."

Antecedentes

En la economía moderna actual, los individuos típicamente establecen cuentas con diferentes instituciones y entidades y usan estas cuentas para interactuar con otros para obtener bienes y servicios y establecer historiales. Las cuentas típicamente se mantienen en ordenadores de servidor bajo el control de la institución o entidad. Sin embargo, tales cuentas suelen ser vulnerables a riesgos de seguridad como la piratería y el robo de identidad y, con frecuencia, están desactualizadas o son inconsistentes. Tales cuentas también son tradicionalmente menos accesibles para los individuos que viven en países en desarrollo o zonas de refugiados.

Gideon Greenspan, *et al: MultiChain Private Blockchain - White Paper"* - 24 de julio de 2015, URL: http://web.archive.org/web/20150724003212if_/http://www.multichain.com/download/MultiChain-White-Paper.pdf describe una plataforma llamada "multichain" para la creación y desarrollo de cadenas de bloques privadas. Multichain restringe el acceso a la cadena de bloques a una lista de usuarios permitidos ampliando la toma de contacto que ocurre cuando se conectan dos nodos de cadena de bloques. En multichain, todos los privilegios se conceden y revocan mediante transacciones de red que contienen metadatos especiales.

Sumario

El objeto de la presente invención es facilitar una cadena de bloques con seguridad mejorada.

Este objeto se resuelve mediante la materia objeto de la reivindicación independiente.

Las realizaciones preferidas de la presente invención se definen por las reivindicaciones dependientes.

Los ejemplos descritos en el presente documento se refieren a plataformas de identidades y transacciones basadas en cadena de bloques. En un enfoque ilustrativo, la información de identidad (por ejemplo, una foto) de una persona se puede cifrar y almacenar en una cadena de bloques como parte de la inscripción de la persona como usuario en una plataforma de identidades y transacciones basada en cadena de bloques. Se pueden formar relaciones de confianza entre el usuario y otros usuarios, y los registros de las relaciones de confianza se pueden almacenar en la cadena de bloques. Se pueden autorizar transacciones entre el usuario y otros usuarios con los que el usuario haya formado una relación de confianza. Los registros de las transacciones también se pueden almacenar en la cadena de bloques. La autorización puede implicar, por ejemplo, un proceso de verificación de múltiples etapas que accede a la información almacenada en la cadena de bloques. Las transacciones y la información de identidad, junto con otra información, pueden contribuir a la identidad económica de la persona. Almacenar una identidad económica (y la información subyacente que forma la identidad económica de la persona) en la cadena de bloques da como resultado una plataforma segura accesible para las personas independientemente de sus circunstancias económicas o geográficas.

Se proporciona este sumario para introducir una selección de conceptos de una forma simplificada que se describen adicionalmente a continuación en la descripción detallada. Este sumario no se pretende para identificar características clave o características esenciales de la materia objeto reivindicada, ni se pretende que se use para limitar el alcance de la materia objeto reivindicada.

Los anteriores y otros objetos, características y ventajas de la invención serán más evidentes a partir de la siguiente descripción detallada, que procede con referencia a las figuras adjuntas.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques de un entorno ilustrativo en el que se puede implementar una plataforma de identidades y transacciones basada en cadena de bloques.

La Figura 2 ilustra un ejemplo de identidad económica.

La Figura 3 es un diagrama que ilustra un método ilustrativo para autorizar transacciones en una plataforma de

identidades y transacciones basada en cadena de bloques.

La Figura 4 es un diagrama que ilustra un método ilustrativo para inscribir a una persona como usuario en una plataforma de identidades y transacciones basada en cadena de bloques.

La Figura 5 es un diagrama que ilustra un método ilustrativo de autorización de transacciones en una plataforma de identidades y transacciones basada en cadena de bloques usando un proceso de verificación de múltiples etapas.

La Figura 6 ilustra interacciones en una autorización de transacción ilustrativa.

La Figura 7 ilustra interacciones en una autorización de transacción ilustrativa en la que se envía un segundo código a un dispositivo móvil del usuario.

Las Figuras 8-23 ilustran interfaces de usuario ilustrativas para interactuar con una plataforma de identidades y transacciones basada en cadena de bloques.

La Figura 24 es un diagrama de un sistema informático ilustrativo en el que se pueden implementar algunas realizaciones descritas.

La Figura 25 es un dispositivo móvil ilustrativo que se puede usar en conjunto con las tecnologías descritas en el presente documento.

La Figura 26 es un entorno soportado por la nube que se puede usar en conjunto con las tecnologías descritas en el presente documento.

La Figura 27 es un diagrama de personas ilustrativo basado en una identidad económica basada en cadena de bloques asegurada.

Descripción detallada

Usando los sistemas, métodos y medios legibles por ordenador descritos en el presente documento, se puede implementar una plataforma de identidades y transacciones basada en cadena de bloques. Las personas pueden inscribirse como usuarios en la plataforma usando información de identidad, tal como una imagen o fotografía (por ejemplo, de la cara de la persona). Una vez que se ha establecido un perfil de usuario, el usuario puede formar relaciones de confianza con otros usuarios de la plataforma y realizar transacciones. Las transacciones pueden incluir, por ejemplo, transferencias de fondos, autorización de tratamiento médico, autorización de asistencia alimentaria y otras transacciones. La información de identidad, las relaciones de confianza, las transacciones y otra información se almacenan en bloques en una cadena de bloques. A diferencia de los enfoques convencionales en los que una información del usuario se almacena y mantiene en ordenadores de servidor centralizados gestionados por muchas entidades diferentes y almacenados detrás de cortafuegos específicos de entidad, cada uno de los cuales puede ser vulnerable a amenazas de seguridad, los ejemplos de plataformas de identidades y transacciones basadas en cadena de bloques que se describen en el presente documento proporcionan almacenamiento seguro de una información del individuo a través de una red distribuida de ordenadores.

Las plataformas de identidades y transacciones basadas en cadena de bloques ilustrativas también permiten a una persona integrar diversos tipos de información para crear una identidad económica que puede usarse para acceder a bienes y servicios. La identidad económica puede incluir, por ejemplo, el historial de ingresos, empleo, pagos a acreedores u otras partes de una persona, etc. La identidad económica se puede usar para establecer las calificaciones y los antecedentes que le permiten a la persona participar en una economía basada en crédito (o de otro modo sofisticada). Por ejemplo, es posible que los individuos en países en desarrollo o áreas de refugiados no tengan acceso a instituciones y entidades necesarias para construir un historial (por ejemplo, una calificación crediticia) que les permita acceder a créditos que puedan usarse para iniciar un negocio, comprar equipo agrícola necesario, realizar mejoras de capital, etc. Una identidad económica establecida a través de una plataforma de identidades y transacciones basada en cadena de bloques puede proporcionar evidencia de la solvencia, identidad, estado legal, etc. de una persona que le permita obtener crédito. Debido a la naturaleza distribuida de una cadena de bloques, una identidad económica de este tipo es portátil y accesible independientemente de la situación económica o geopolítica en la ubicación actual del usuario. Además de proporcionar a quienes viven en el mundo desarrollado una plataforma segura e integrada, los ejemplos descritos en el presente documento tienen el potencial de reducir drásticamente la pobreza en los países en desarrollo y ayudar a millones de refugiados a establecerse en la economía mundial proporcionándoles acceso al crédito. A continuación, se describen ejemplos con referencia a las Figuras 1-27.

La Figura 1 ilustra un entorno 100 ilustrativo en el que se puede implementar una plataforma de identidades y transacciones basada en cadena de bloques. Como se usa en el presente documento en este documento, "cadena de bloques" se refiere a una plataforma y red de almacenamiento distribuido en la que "bloques" individuales están conectados en una cadena. Cada bloque está vinculado al bloque anterior en la cadena de bloques, por ejemplo, incluyendo una función de troceo del bloque anterior como "prueba de trabajo". Se pueden usar diversas funciones de

troceo, incluyendo funciones de las familias del Algoritmo de Función de Troceo Seguro (Secure Hash Algorithm, SHA) 1 o 2, tal como SHA-256, para realizar una función de troceo unidireccional. Para una función de troceo unidireccional, generalmente se considera imposible o poco práctico generar la entrada (el "mensaje") a la función de troceo basándose en la salida (el "resumen de mensaje" o "resumen") de la función de troceo.

En una cadena de bloques, los bloques individuales pueden almacenar una diversidad de datos que pueden o no estar relacionados (por ejemplo, pueden estar asociados o no con un mismo usuario). En el entorno 100, los dispositivos informáticos móviles 102 y 104 están en comunicación con el dispositivo o dispositivos informáticos 106 a través de una red 108. La red 108 puede ser Internet, una red de área local (LAN), una red de área local inalámbrica (WLAN), una red de área extensa (WAN) u otro tipo de red, alámbrica o inalámbrica. El dispositivo o dispositivos informáticos 106 pueden ser, por ejemplo, uno o más ordenadores de servidor. El dispositivo o dispositivos informáticos 106 incluyen procesador o procesadores 110, almacenamiento local 112 y memoria 114. El entorno 100 también puede incluir uno o más dispositivos informáticos adicionales, tales como ordenadores de sobremesa, (no mostrados) en comunicación con el dispositivo o dispositivos informáticos 106 a través de la red 108.

El dispositivo o dispositivos informáticos 106 también incluyen un motor de inscripción 116 y un motor de transacciones 118. El motor de inscripción 116 está configurado para inscribir, mediante el procesador o procesadores 110, a una persona como usuario en la plataforma de identidades y transacciones económica basada en cadena de bloques basándose en la información de identidad de la persona. Como ejemplo, una persona puede usar el dispositivo informático móvil 102 (u otro dispositivo informático, tal como un ordenador de sobremesa) para introducir un nombre, un número de identificación asignado por el gobierno, etc. y/o tomar una imagen (por ejemplo, una "autofoto") de sí misma y, usando una aplicación web o usando software del lado del cliente instalado en el dispositivo informático móvil 102, cargar la imagen y/u otra información en el dispositivo o dispositivos informáticos 106 como información de identidad. Se ilustran interfaces de usuario de software ilustrativas en las Figuras 8-23. El motor de inscripción 116 está configurado para crear un identificador único para la persona basándose en la información de identidad cargada. La información de identidad se puede cifrar, ya sea mediante el dispositivo o dispositivos informáticos 106 o a través de un servicio de cifrado 120. Los servicios de cifrado se analizan con más detalle a continuación. La información de identidad cifrada puede almacenarse a continuación en una cadena de bloques 122. La cadena de bloques 122 se implementa en un grupo de dispositivos informáticos distribuidos 124 que son accesibles a través de la red 108. A continuación, se analizan en detalle ejemplos de inscripción adicionales con respecto, por ejemplo, a la Figura 4.

El motor de transacciones 118 está configurado para autorizar, mediante el procesador o procesadores 110, transacciones entre usuarios que están en una relación de confianza. Las relaciones de confianza pueden establecerse, por ejemplo, mediante solicitud o invitación de un usuario y aceptación por otro usuario. Las transacciones pueden autorizarse, al menos en parte, a través de la interacción con un dispositivo informático de agente de verificación 126. El dispositivo informático de agente de verificación 126 se comunica con el dispositivo o dispositivos informáticos 106 a través de la red 108. Como ejemplo, un primer usuario puede iniciar una transferencia de fondos a un segundo usuario a través de una aplicación web o a través de software del lado del cliente. El motor de transacciones 118 se puede configurar para realizar una verificación de la transferencia de fondos usando, por ejemplo, un enfoque de verificación de múltiples etapas que accede a la información almacenada en la cadena de bloques 122. Los ejemplos de verificación de transacciones se analizan en detalle a continuación con respecto, por ejemplo, a las Figuras 5, 6 y 7.

La información de identidad, información de transacción y otra información para un usuario que se almacena en la cadena de bloques 122 puede formar una identidad económica del usuario. La Figura 2 ilustra un ejemplo de identidad económica 200. La identidad económica 200 incluye información de identidad 202, cuentas vinculadas 204, historial de empleo 206, información de servicios públicos 208, historial de educación 210, registro de ayuda 212, posesión de propiedades 214, historial médico 216 e historial de transacciones 218. Aunque se muestra que la identidad económica 200 incluye cada una de las categorías de información particulares anteriores, las identidades económicas ilustrativas también pueden incluir únicamente algunas de estas categorías de información y/o incluir categorías de información adicionales. La información de identidad 202 puede incluir, por ejemplo, una imagen de un usuario, un nombre, identificador o identificadores gubernamentales y/o información de huellas digitales o patrón ocular del usuario (u otra información biométrica del usuario). Las cuentas vinculadas 204 pueden incluir, por ejemplo, cuentas bancarias, de inversión o de crédito asociadas con el usuario. El historial de empleo 206 puede incluir nombres y/o direcciones de empleadores, títulos de trabajo, fechas de empleo, salarios y/u otra información de empleo.

La información de servicios públicos 208 puede incluir cuentas de servicios públicos para el usuario, registros de pagos anteriores y/u otra información. El historial de educación 210 puede incluir títulos obtenidos, niveles educativos completados, cursos completados, certificaciones obtenidas, puntuaciones de exámenes, etc. El registro de ayuda 212 puede incluir asistencia alimentaria (por ejemplo, paquetes de alimentos distribuidos por las Naciones Unidas u otra entidad de ayuda) o préstamos recibidos, préstamos reembolsados, etc. La posesión de propiedades 214 puede incluir información de escritura de propiedad, información de ubicación de propiedad, información de transacciones de propiedad, etc. El historial médico 216 puede incluir registros médicos, información de seguro médico, información de ayuda médica (por ejemplo, vacunas recibidas), etc. El historial de transacciones 218 puede incluir transferencias de fondos recibidas o proporcionadas, autorizaciones de ayuda o asistencia médica (incluso si también se incluyen en el registro de ayuda 212 o en el historial médico 216) u otra información de transacciones. La información incluida en la

información de identidad 202, cuentas vinculadas 204, historial de empleo 206, información de servicios públicos 208, historial de educación 210, registro de ayuda 212, posesión de propiedades 214, historial médico 216 e historial de transacciones 218 se puede presentar como información agregada o como elementos individuales.

La identidad económica 200 también puede incluir una puntuación de "confianza" similar a una puntuación crediticia que indica un nivel de solvencia o responsabilidad que pueden usar las empresas o instituciones que son usuarios de la plataforma de identidades y transacciones basada en cadena de bloques. La puntuación de confianza se puede determinar basándose en un esquema de ponderación (por ejemplo, cuantificación del historial de empleo ponderada al 50 %, cuantificación del historial de transacciones ponderada al 30 %, cuantificación del historial de educación ponderada al 20 %, etc.). En algunos ejemplos, empresas o instituciones particulares pueden seleccionar criterios de interés y/o ponderaciones deseadas particulares para diferentes criterios, y se determina una puntuación de confianza personalizada basándose en esos criterios. Se pueden usar diversos enfoques para cuantificar una categoría particular (por ejemplo, rango percentil de criterios, escala de 1-10, etc.).

La identidad económica 200 se almacena en la cadena de bloques 220. Los bloques 222, 224, 226 y 228 de la cadena de bloques 220 se muestran en la Figura 2, pero cualquier número de bloques puede formar la cadena de bloques 220. Como se indica por las flechas entre los bloques 222, 224, 226 y 228, los bloques respectivos están vinculados al bloque anterior en la cadena de bloques. Este enlace puede tener la forma de, por ejemplo, una función de troceo (*hash*) del bloque anterior.

La Figura 3 ilustra un método 300 para autorizar transacciones en una plataforma de identidades y transacciones basada en cadena de bloques. En el bloque de proceso 302, la información de identidad de una persona se cifra y la información de identidad cifrada se almacena en una cadena de bloques como parte de la inscripción del usuario en la plataforma de identidades y transacciones económica basada en cadena de bloques. La información de identidad puede incluir, por ejemplo, una imagen de la persona. La información de identidad puede incluir, como alternativa, o, adicionalmente, al menos uno de un nombre, identificador o identificadores gubernamental, información de huella digital o de patrón ocular.

En el bloque de proceso 304, los registros de las relaciones de confianza entre el usuario y otros usuarios se almacenan en la cadena de bloques. Para los usuarios de la plataforma de identidades y transacciones basada en cadena de bloques, se puede formar una relación de confianza, por ejemplo, realizando una búsqueda o consulta de usuarios registrados y enviando a un usuario identificado a través de la búsqueda o consulta un mensaje que indica que se desea una relación de confianza. Si el otro usuario acepta la solicitud, a continuación, se establece una relación de confianza. Sin embargo, en algunas situaciones, es posible que un usuario desee transferir fondos o realizar otra transacción con una persona que no sea usuario de la plataforma de identidades y transacciones basada en cadena de bloques. En tales situaciones, un usuario puede enviar una invitación para conectarse a la dirección de correo electrónico, cuenta de mensajería u otro punto de contacto de la persona, y el mensaje incluye un enlace o instrucciones para crear una cuenta con la plataforma e indica que el usuario desearía establecer una relación de confianza.

Las transacciones entre el usuario y uno o más de los otros usuarios con quienes el usuario ha formado una relación de confianza se autorizan en el bloque de proceso 306. Las transacciones se almacenan en la cadena de bloques. Los registros de las transacciones se almacenan en la cadena de bloques en el bloque de proceso 308. Al menos algunas de las transacciones y la información de identidad contribuyen a la identidad económica de la persona. La identidad económica también puede incluir al menos uno de información de historial de empleo, información de historial de educación, información de propiedad de tierras o información de historial médico del usuario. La información adicional que puede ser parte de la identidad económica se ilustra, por ejemplo, en la Figura 2.

En el bloque de proceso 306, la información de identidad de un usuario puede usarse en la autorización. Por ejemplo, cuando la información de identidad incluye una imagen de la persona, esta imagen puede usarse para autorizar las transacciones. El bloque de proceso 306 puede incluir un enfoque de verificación de múltiples etapas como se analiza, por ejemplo, con respecto a las Figuras 5 y 6. En algunos ejemplos, el método 300 comprende además proporcionar la identidad económica del usuario a una parte solicitante, donde la parte solicitante es un usuario en la plataforma de identidades y transacciones económica basada en cadena de bloques. Por ejemplo, un usuario puede desear establecer una línea de crédito, comprar equipo o realizar otra transacción, y antes de iniciar o autorizar la transacción, la parte solicitante puede solicitar la identidad económica del usuario (por ejemplo, a través de una aplicación de software del lado del cliente) para evaluar al usuario como potencial deudor, comprador, empleado, etc.

En algunos ejemplos, las empresas e instituciones que establecen cuentas con la plataforma de identidades y transacciones económica basada en cadena de bloques pueden acceder (por ejemplo, a través de una aplicación web o software del lado del cliente) a una interfaz de usuario que permite a la empresa o institución ver las identidades económicas de otros usuarios que dan permiso. En algunos ejemplos, los usuarios pueden controlar qué categorías de información se incluyen en su identidad económica y/o pueden autorizar el acceso de lectura de únicamente ciertas categorías en respuesta a una solicitud. Por ejemplo, si un usuario está interesado en obtener un préstamo de una entidad y la entidad solicita la identidad económica del usuario, el usuario puede optar por no compartir información de historial médico u otra información que pueda no ser relevante para la entidad.

La Figura 4 ilustra un método 400 para inscribir a una persona como usuario en una plataforma de identidades y transacciones basada en cadena de bloques. En el bloque de proceso 402, se recibe información de identidad de una persona. La información de identidad puede incluir una imagen de la persona (por ejemplo, una autofoto) y/o un nombre, identificador o identificadores gubernamentales, huellas digitales o información de patrón ocular. En el bloque de proceso 404, la información de identidad se cifra. Se pueden usar varias técnicas de cifrado. En el bloque de proceso 406, la información de identidad cifrada se almacena en un bloque de una cadena de bloques. En algunos ejemplos, se puede usar una única clave de cifrado y se puede almacenar como, por ejemplo, una variable de entorno en un dispositivo de almacenamiento informático asociado con la plataforma de identidades y transacciones basada en cadena de bloques.

En algunos ejemplos, se puede usar un servicio de cifrado, tal como el servicio de cifrado 120 de la Figura 1. El servicio de cifrado puede crear y gestionar claves de cifrado. En un ejemplo de este tipo, el software que implementa aspectos de la plataforma de identidades y transacciones basada en cadena de bloques puede realizar una llamada al servicio de cifrado para cifrar la información de identidad recibida en el bloque de proceso 402. El servicio crea las claves, retiene una clave privada y proporciona tanto una clave pública como la información de identidad cifrada al software que realizó la llamada al servicio. El servicio de cifrado puede ser un servicio web.

En el bloque de proceso 408, se establece un identificador único asociado con la persona basándose en la información de identidad cifrada. En algunos ejemplos, el bloque de proceso 408 incluye designar la información de identidad cifrada como el identificador único. También se pueden usar otros identificadores únicos. En algunos ejemplos, se pueden tomar diversas acciones para validar o autenticar la identidad de un usuario antes de establecer el identificador único. Por ejemplo, se pueden usar diversas fuentes de información de terceros para verificar la identidad del usuario.

El método 400 también puede comprender además asociar, con el identificador único, al menos una información médica, de empleo, de educación, de propiedad o económica (por ejemplo, cuentas vinculadas, historial de transacciones, etc.) correspondiente a la persona y almacenar la información médica, de empleo, de educación, de propiedad o económica en la cadena de bloques. Parte o toda la información asociada se puede usar para formar la identidad económica de la persona, como se analizó, por ejemplo, anteriormente con respecto a la Figura 2. La información de transacciones que representa una o más transacciones entre la persona y una o más partes adicionales, así como las relaciones de confianza entre la persona y las partes adicionales, también se puede almacenar en la cadena de bloques en asociación con el identificador único u otra información que indica al usuario (tal como la clave pública, incluso si la clave pública no se usa como el identificador único).

La Figura 5 ilustra un método 500 para verificar una transacción en una plataforma de identidades y transacciones basada en cadena de bloques. En el bloque de proceso 502, se identifica un receptor de una transacción. Un receptor es, por ejemplo, la persona o usuario que recibirá una transferencia de fondos, recibirá asistencia médica, recibirá asistencia alimentaria, etc. En algunos ejemplos, un receptor puede ser cualquier persona y, en algunos ejemplos, el receptor se limita a un usuario de la plataforma de identidades y transacciones basada en cadena de bloques. En algunos ejemplos en los que el receptor no es un usuario de la plataforma, se le puede enviar a la persona un enlace o instrucciones para inscribirse como usuario en la plataforma después de que se inicia la transacción, y la transacción no continúa hasta que la persona se inscribe y establece una relación de confianza con el emisor. En tales ejemplos, el receptor es un receptor potencial hasta que la persona se inscribe y establece la relación de confianza.

Los datos de autenticación de primera etapa se generan en el bloque de proceso 504. Los datos de autenticación de primera etapa pueden ser, por ejemplo, un código que incluye números y/o letras. Los datos de autenticación de primera etapa se pueden proporcionar al receptor y pueden servir como indicación para el receptor de que está disponible para reclamarse un beneficio. Por ejemplo, el receptor puede recibir un mensaje de texto, un mensaje de correo electrónico o una alerta de aplicación que incluye: una declaración de que un beneficio está disponible para reclamarse; un código (por ejemplo, un código numérico de 9 dígitos, alfanumérico o de letras); e instrucciones para completar el proceso de verificación para poder reclamar el beneficio. En algunos ejemplos, los datos de autenticación de primera etapa únicamente son válidos durante un período de tiempo determinado (una hora, un día, una semana, etc.). En algunos ejemplos, los datos de autenticación de primera etapa son válidos el tiempo suficiente para permitir que el receptor reclame el beneficio de acuerdo con la planificación del receptor (por ejemplo, hasta que se complete un turno de trabajo, un viaje u otro evento).

En el bloque de proceso 506, se recibe una indicación de que los datos de autenticación de primera etapa se han proporcionado a un agente de verificación. Un agente de verificación es un usuario de la plataforma de identidades y transacciones basada en cadena de bloques que desempeña una función de tercero. El agente de verificación puede comunicarse con la plataforma a través, por ejemplo, del dispositivo informático de agente de verificación 126 de la Figura 1. Por ejemplo, en un contexto de refugiados, el agente de verificación puede ser un miembro de las Naciones Unidas u otra entidad que sea un proveedor de asistencia, y cuando un refugiado recibe (por ejemplo, a través de un mensaje de texto en el teléfono móvil del refugiado) un mensaje y un código que indica que hay un paquete de asistencia alimentaria disponible, el refugiado lleva el código al agente de verificación, que puede estar ubicado en un quiosco, edificio u otra instalación. A continuación, el agente de verificación introduce el código a través de una interfaz de usuario de aplicación de software. El "agente de verificación", como se usa en el presente documento, también

puede referirse a un dispositivo informático de agente de verificación. En algunos ejemplos, la persona puede introducir un código en un terminal automatizado.

En el bloque de proceso 508, se verifican los datos de autenticación de primera etapa. Por ejemplo, el código proporcionado en el mensaje inicial se puede comparar con el código introducido por el agente (o, en algunos ejemplos, introducido por la persona). La verificación de los datos de autenticación de primera etapa proporciona cierta confirmación de que la persona que proporcionó el código al agente es el receptor real.

En el bloque de proceso 510, la información de identidad del receptor se recupera de uno o más bloques en una cadena de bloques después de verificar los datos de autenticación de primera etapa y se transmite (por ejemplo, al agente de verificación). La información de identidad se puede usar para confirmar aún más que la persona es el receptor real. Continuando con el ejemplo de refugiados anterior, después de que el agente de verificación haya introducido el código proporcionado por la persona y se haya verificado que el código (por ejemplo, mediante un ordenador de servidor remoto) coincide con el código proporcionado en el mensaje original, se puede proporcionar una imagen del receptor al agente. La imagen puede ser la imagen usada para crear el perfil del receptor (y la imagen que se cifra y almacena en la cadena de bloques). Si la imagen parece ser la misma persona que la persona en presencia del agente que proporcionó el código, a continuación, el agente confirma una coincidencia de identidad.

En algunos ejemplos, se usa software de reconocimiento facial para determinar si existe una coincidencia entre la persona y la imagen. En algunos ejemplos, se puede realizar la comparación de huellas digitales o patrones oculares en lugar de comparar la apariencia de la persona con una imagen. En ejemplos en los que se usa un terminal automatizado, se pueden presentar instrucciones para que la persona coloque su dedo, ojo o cara en un escáner o delante de una cámara, y la comparación de la información de identidad se puede realizar mediante software.

En algunos ejemplos, en lugar de confirmar afirmativamente una coincidencia de identidad, el agente puede rechazar completar cualquier acción adicional (por ejemplo, introducir un segundo código) si la persona en presencia del agente no parece coincidir con la imagen (u otra información biométrica).

La información de identidad, tal como una imagen, se almacena de forma cifrada en la cadena de bloques. En los ejemplos en los que se usa un servicio de cifrado, el software asociado con la plataforma puede realizar una llamada al servicio de cifrado y solicitar un testigo temporal para descifrar la imagen. El testigo (*token*) puede ser válido durante un tiempo limitado y, al devolverlo al servicio de cifrado, la imagen descifrada (o huella digital, patrón ocular, etc.) se proporciona al software (o al dispositivo informático de agente de verificación). A continuación, el software proporciona o pone a disposición de otro modo la imagen descifrada para el agente de verificación.

Los datos de autenticación de segunda etapa (por ejemplo, un segundo código tal como un código de 6 dígitos) se generan y transmiten en el bloque de proceso 512. En algunos ejemplos, los datos de autenticación de segunda etapa se transmiten sustancialmente al mismo tiempo que se transmite la información de identidad. En algunos ejemplos, los datos de autenticación de segunda etapa se transmiten después de que se confirma una coincidencia entre la información biométrica y la persona en presencia del agente de verificación. La cuenta de la plataforma de identidades y transacciones basada en cadena de bloques del receptor puede incluir un número de teléfono asociado u otra información que identifica un dispositivo móvil, tal como un teléfono inteligente, un teléfono con características o una tableta. En algunos ejemplos, los datos de autenticación de segunda etapa se envían al dispositivo móvil asociado con el receptor, y si la persona en presencia del agente de verificación está en posesión del dispositivo móvil asociado, a continuación, la persona puede proporcionar el segundo código al agente de verificación. En algunos ejemplos, los datos de autenticación de segunda etapa se envían de manera similar a los datos de autenticación de primera etapa (por ejemplo, mediante mensaje de correo electrónico, alerta de aplicación o mensaje de texto).

En el bloque de proceso 514, se recibe una indicación de que los datos de autenticación de segunda etapa se han proporcionado al agente de verificación. Los datos de autenticación de segunda etapa y el código proporcionado al agente de verificación se pueden comparar a continuación para verificar que el código proporcionado al agente de verificación sea correcto. Después de verificar los datos de autenticación de segunda etapa, se determina en el bloque de proceso 516 que la persona en presencia del agente de verificación es el receptor real y se autoriza la transacción. En el ejemplo de los refugiados, la autorización puede incluir el paquete de alimentos que se le entrega al refugiado. En ejemplos de transferencia de fondos, la autorización puede incluir entregar dinero físicamente a la persona o iniciar/completar una transferencia entre cuentas. En algunos ejemplos, la plataforma de identidades y transacciones basada en cadena de bloques puede retener fondos como intermediario y desembolsarlos en una cuenta vinculada cuando se autoriza la transacción. En otros ejemplos, la plataforma en realidad no tiene acceso o control sobre los fondos.

La verificación de múltiples etapas proporciona varias capas de seguridad y requiere que una persona que intenta reclamar un beneficio deba tener los datos de autenticación de primera etapa (por ejemplo, el primer código) asociados con el beneficio, así como los datos de autenticación de segunda etapa (por ejemplo, el segundo código) enviados después de la verificación del primer código. Además, en algunos ejemplos, el agente confirma explícitamente que la persona tiene una apariencia física u otra característica correspondiente al receptor real o confirma implícitamente una coincidencia de identidad introduciendo el segundo código. Se puede implementar mayor seguridad requiriendo que

la persona en presencia del agente esté en posesión física del dispositivo móvil del receptor previsto. En algunos ejemplos, se pueden omitir una o más de estas capas de seguridad. En un ejemplo particular, se usan menos capas de seguridad para transacciones de menor valor (por ejemplo, transferencias de fondos de menos de 100 $) y se proporcionan capas adicionales de seguridad para transacciones de mayor valor. Capas de seguridad adicionales más allá de las analizadas con respecto a la Figura 5 también son posibles.

En algunos ejemplos, se omite el bloque de proceso 510 (y no se transmite una imagen o datos biométricos del receptor previsto), y después de que se verifican los datos de autenticación de primera etapa, se generan los datos de autenticación de segunda etapa y se transmiten a la cuenta y/o dispositivo móvil del receptor.

El método 500 también puede incluir almacenar un registro de la transacción (por ejemplo, incluyendo componentes de transacción particulares, datos de ubicación, detalles técnicos del dispositivo/red, etc.) en la cadena de bloques en asociación con el receptor y/o emisor. En algunos ejemplos, únicamente se almacenan las transacciones autorizadas y completadas. La información almacenada puede incluir el receptor, el emisor y las características de la transacción (por ejemplo, transferencia de fondos, asistencia de ayuda, etc.). Los datos de autenticación de primera y segunda etapa se pueden asociar tanto con el receptor como con la transacción.

La Figura 6 es un diagrama de interacción 600 que ilustra un proceso de verificación de transacción tal como el descrito con respecto a la Figura 5. La Figura 6 se analiza con referencia a un ejemplo específico en el que la transacción es una transferencia de fondos, los datos de autenticación de primera etapa son un primer código, la información de identidad es una imagen y los datos de autenticación de segunda etapa son un segundo código. Un conjunto similar de interacciones se aplica a otras situaciones, tal como la autorización de asistencia alimentaria o médica.

Un emisor inicia una transferencia de fondos a un receptor que tiene una cuenta con la plataforma de identidades y transacciones basada en cadena de bloques. El receptor tiene una relación de confianza con el emisor. En la interacción 602, los detalles de la transacción iniciada, incluido el receptor, el tipo de transacción (transferencia de fondos) y la cantidad a transferir, se envían por el emisor a un ordenador de servidor o servidores que implementa aspectos de la plataforma de identidades y transacciones basada en cadena de bloques, tal como el ordenador u ordenadores de servidor 106 de la Figura 1. En la interacción 604, los datos de autenticación de primera etapa (un primer código) se envían a la cuenta del receptor. El primer código se puede enviar, por ejemplo, como mensaje de texto o correo electrónico. El primer código también se puede enviar como una alerta de cuenta que aparece en una interfaz web (o en un software del lado del cliente que se ejecuta en un dispositivo informático o dispositivo móvil). El mensaje también puede proporcionar instrucciones al receptor para completar la transacción y reclamar los fondos.

A continuación, el receptor proporciona el primer código a un agente de verificación en la interacción 606. En algunos ejemplos, el código se puede mostrar a una persona que da servicio como un agente, quien a continuación introduce el código en un dispositivo informático de agente de verificación. En otros ejemplos, el receptor puede introducir el código en un terminal o quiosco automatizado. En otros ejemplos más, el dispositivo informático de agente de verificación puede ser remoto y el receptor reenvía el mensaje al agente de verificación o introduce el código a través de una interfaz web.

El agente de verificación introduce y envía el código proporcionado por el receptor de vuelta al servidor o servidores en la interacción 608. El servidor o servidores verifican que el código coincide con el primer código enviado en la interacción 604. En algunos ejemplos, si no hay coincidencia, la transacción se cancela. En otros ejemplos, se permite un número limitado de intentos de entrada de código antes de cancelar la transacción.

Después de determinar que el primer código coincide, se usa información de identidad (por ejemplo, una imagen del receptor previsto) para confirmar que la persona que proporcionó el primer código es el receptor previsto. En la interacción 610, el servidor o servidores envían el identificador único del receptor (por ejemplo, la clave pública correspondiente a la imagen cifrada del receptor u otra información de identidad) a la cadena de bloques para recuperar la imagen cifrada del receptor. En la transacción 612, la imagen cifrada se proporciona al servidor o servidores. En los ejemplos en los que el cifrado se gestiona por el servidor o servidores, a continuación, la imagen se descifra. En ejemplos en los que se utiliza un servicio de cifrado, tal como la Figura 6, el servidor o servidores interactúan con el servicio de cifrado para descifrar la imagen. En la Figura 6, esto se hace a través del uso de un testigo de descifrado. Los servidores envían una solicitud de testigo al servicio de cifrado en la interacción 614, y se proporciona un testigo de descifrado de vuelta al servidor o servidores en la interacción 616. El testigo de descifrado permite que el servidor o servidores descifren la imagen y proporcionen la imagen descifrada al agente de verificación en la interacción 618. En algunos ejemplos, la imagen descifrada se puede enviar directamente desde el servicio de cifrado al agente de verificación. En ciertos casos, cuando se usan otras formas de datos biométricos (tales como huellas digitales, patrones de iris o reconocimiento facial), las etapas de descifrado pueden incluir hacer coincidir una huella digital, un iris o una cara presentados físicamente con datos biométricos almacenados (por ejemplo, datos biométricos cifrados y almacenados en la cadena de bloques).

En ejemplos en los que el agente de verificación es una persona que interactúa con un dispositivo informático de agente de verificación, la imagen descifrada del receptor previsto se puede presentar en el dispositivo informático de agente de verificación, y el agente puede juzgar si la persona en presencia del agente parece ser la misma que la

persona que se muestra en la imagen. En ejemplos en los que el agente de verificación es un terminal automatizado, la persona puede presentar su cara para permitir que la terminal cree una imagen y, a continuación, comparar esa imagen con la imagen descifrada del receptor previsto usando reconocimiento facial u otro software de reconocimiento de imágenes. En ejemplos en los que el agente de verificación es remoto (ya sea una persona remota o un dispositivo informático remoto), se puede dar instrucción a la persona que se tome una autofoto y la envíe a un agente de verificación/cargue la autofoto. La persona remota o el software que se ejecuta en el dispositivo informático remoto pueden comparar a continuación la autofoto y la imagen descifrada. En la interacción 620, el dispositivo informático de agente de verificación proporciona una confirmación de coincidencia de identidad al servidor o servidores de verificación indicando que la persona parece ser el receptor previsto.

En este punto, se han utilizado tanto el primer código como una imagen del receptor previsto para verificar que la persona que intenta reclamar los fondos es el receptor previsto. Es posible que una persona que no sea el receptor previsto pudiera haber interceptado el primer código (por ejemplo, accediendo al mensaje inicial mientras usa el teléfono del receptor previsto) y, además, es posible que la persona que intercepte el primer código se parezca al receptor previsto suficientemente como para convencer a un agente de verificación (o software de reconocimiento facial). Aunque tales situaciones probablemente sean raras, también se puede usar una capa adicional de seguridad - enviar un segundo código al receptor.

En la interacción 622, el servidor o servidores envía(n) datos de autenticación de segunda etapa (por ejemplo, un segundo código), que puede tener un límite de tiempo, a la cuenta del receptor (por ejemplo, mediante mensaje de texto, mensaje de correo electrónico o alerta de aplicación). A continuación, el receptor proporciona el segundo código de vuelta al agente de verificación en la interacción 624. El agente de verificación envía el segundo código proporcionado al servidor o servidores en la interacción 626, y si el código coincide con el segundo código enviado a la cuenta del receptor en la interacción 622, a continuación, la transacción está autorizada. En los ejemplos en los que el segundo código tiene un límite de tiempo, la transacción únicamente está autorizada si se ejecuta dentro de restricciones de tiempo predeterminadas. A continuación, se puede completar o autorizar la transferencia de fondos. En ejemplos en los que el beneficio es un elemento o servicio físico, tal como un paquete de alimentos o ayuda médica (por ejemplo, una vacuna, medicamento, suplemento, procedimiento, etc.), a continuación, el servidor o servidores comunican al agente de verificación que la liberación del elemento/servicio está autorizada. En un contexto de refugiados, por ejemplo, se puede manejar o dispensar automáticamente un paquete de alimentos al receptor. La transacción completada a continuación se almacena en la cadena de bloques en asociación con el receptor y/o el emisor.

En algunos ejemplos, la interacción 620, en la que se proporciona la confirmación de coincidencia de identidad al servidor o servidores, no se realiza afirmativamente, pero se confirma implícitamente una coincidencia cuando el agente de verificación introduce el segundo código en la interacción 626. En tales ejemplos, después de que el agente de verificación haya proporcionado el primer código al servidor o servidores en la interacción 608, y el primer código haya sido verificado por el servidor o servidores (y después de las interacciones de recuperación/descifrado 610, 612, 614, y 616, si se realizan), el segundo código se envía a la cuenta del receptor en la interacción 622 sustancialmente al mismo tiempo que la imagen descifrada se envía al agente de verificación en la interacción 618. Cuando la persona en presencia del agente de verificación proporciona el segundo código al agente en la interacción 624, el agente puede rechazar introducir el segundo código (o cancelar la transacción) si la persona en presencia del agente no parece coincidir con la imagen descifrada. Un ejemplo de este tipo se ilustra en la Figura 7.

En diversos ejemplos, el agente de verificación puede implementarse en el servidor o servidores o eliminarse. Por ejemplo: el primer código proporcionado en la interacción 604 se puede proporcionar directamente de vuelta al servidor o servidores; la imagen descifrada puede conservarse en el servidor o servidores y no enviarse al agente de verificación y, en su lugar, una persona puede proporcionar una autofoto que se compara con la imagen descifrada en el servidor o servidores; y el segundo código recibido en el dispositivo móvil del receptor se puede proporcionar directamente de vuelta al servidor o servidores (por ejemplo, introduciendo/cargando el código a través de una interfaz en el dispositivo móvil).

La Figura 7 es un diagrama de interacción 700 que ilustra un proceso de verificación de transacción tal como el descrito con respecto a las Figuras 5 y 6. En la Figura 7, la transacción es una transferencia de fondos, los datos de autenticación de primera etapa son un código de 9 dígitos, la información de identidad es una imagen y los datos de autenticación de segunda etapa son un código de 6 dígitos. Como con la Figura 6, puede aplicarse un conjunto similar de interacciones a otras situaciones, tales como la autorización de asistencia alimentaria o médica.

Un emisor inicia una transferencia de fondos a un receptor que tiene una cuenta con la plataforma de identidades y transacciones basada en cadena de bloques. El receptor tiene una relación de confianza con el emisor. En la interacción 702, los detalles de la transacción iniciada, incluido el receptor, el tipo de transacción (transferencia de fondos) y la cantidad a transferir, se envían por el emisor a un ordenador de servidor o servidores que implementa aspectos de la plataforma de identidades y transacciones basada en cadena de bloques, tal como el ordenador u ordenadores de servidor 106 de la Figura 1. En la interacción 704, los datos de autenticación de primera etapa (un código de 9 dígitos) se envían a la cuenta del receptor. El código de 9 dígitos se puede enviar, por ejemplo, como mensaje de texto o correo electrónico. El código también se puede enviar como una alerta de cuenta que aparece en

una interfaz web (o software del lado del cliente que se ejecuta en un dispositivo informático o dispositivo móvil). El mensaje también puede proporcionar instrucciones al receptor para completar la transacción y reclamar los fondos.

A continuación, el receptor proporciona el código de 9 dígitos a un agente de verificación en la interacción 706. En algunos ejemplos, el código se puede mostrar a una persona que da servicio como un agente, quien a continuación introduce el código en un dispositivo informático de agente de verificación. En otros ejemplos, el receptor puede introducir el código en un terminal o quiosco automatizado. En otros ejemplos más, el dispositivo informático de agente de verificación puede ser remoto y el receptor reenvía el mensaje al agente de verificación o introduce el código a través de una interfaz web.

El agente de verificación introduce y envía el código de 9 dígitos proporcionado por el receptor de vuelta al servidor o servidores en la interacción 708. El servidor o servidores verifican que el código coincide con el código enviado en la interacción 704. En algunos ejemplos, si el código no coincide, la transacción se cancela. En otros ejemplos, se permite un número limitado de intentos de entrada de código antes de cancelar la transacción.

Después de determinar que el código de 9 dígitos coincide, se usa información de identidad (por ejemplo, una imagen del receptor previsto) para confirmar que la persona que proporcionó el código de 9 dígitos es el receptor previsto. En la interacción 710, el servidor o servidores envían el identificador único del receptor (por ejemplo, la clave pública correspondiente a la imagen cifrada del receptor u otra información de identidad) a la cadena de bloques para recuperar la imagen cifrada del receptor. En la transacción 712, la imagen cifrada se proporciona al servidor o servidores. En los ejemplos en los que el cifrado se gestiona por el servidor o servidores, a continuación, la imagen se descifra. En ejemplos en los que se utiliza un servicio de cifrado, tal como las Figuras 6 y 7, el servidor o servidores interactúan con el servicio de cifrado para descifrar la imagen. En la Figura 7, esto se hace a través del uso de un testigo de descifrado. Los servidores envían una solicitud de testigo al servicio de cifrado en la interacción 714, y se proporciona un testigo de descifrado de vuelta al servidor o servidores en la interacción 716. El testigo de descifrado permite que el servidor o servidores descifren la imagen y proporcionen la imagen descifrada al agente de verificación en la interacción 718.

En la interacción 720, el servidor o servidores envían datos de autenticación de segunda etapa (por ejemplo, un código de 6 dígitos), que puede tener un límite de tiempo, al dispositivo móvil del receptor (o, en algunos ejemplos, a la cuenta del usuario). La interacción 720 puede ocurrir sustancialmente al mismo tiempo que la imagen descifrada se transmite al agente de verificación en la interacción 718. A continuación, el receptor proporciona el código de 6 dígitos de vuelta al agente de verificación en la interacción 722. Si la imagen descifrada proporcionada al agente en la interacción 718 no parece coincidir con la persona en presencia del agente, el agente de verificación puede rechazar introducir el código de 6 dígitos o cancelar la transacción. Esto sirve como una capa adicional de seguridad para garantizar que la persona que intenta reclamar un beneficio sea el receptor previsto. Si la imagen descifrada coincide con la persona en presencia del agente, a continuación, el agente de verificación envía el código de 6 dígitos proporcionado de vuelta al servidor o servidores en la interacción 724, y si el código coincide con el código de 6 dígitos enviado al dispositivo móvil del receptor en la interacción 720, a continuación, se autoriza la transacción.

En los ejemplos en los que el código de 6 dígitos tiene un límite de tiempo, la transacción únicamente está autorizada si se ejecuta dentro de restricciones de tiempo predeterminadas. A continuación, se puede completar o autorizar la transferencia de fondos. En ejemplos en los que el beneficio es un elemento o servicio físico, tal como un paquete de alimentos o ayuda médica (por ejemplo, una vacuna, medicamento, suplemento, procedimiento, etc.), a continuación, el servidor o servidores comunican al agente de verificación que la liberación del elemento/servicio está autorizada. En un contexto de refugiados, por ejemplo, se puede manejar o dispensar automáticamente un paquete de alimentos al receptor. La transacción completada a continuación se almacena en la cadena de bloques en asociación con el receptor y/o el emisor.

La Figura 8 ilustra una interfaz de usuario 800 que proporciona un número de opciones diferentes para iniciar sesión en una plataforma de identidades y transacciones basada en cadena de bloques, que incluye la opción 802 para iniciar sesión usando una cuenta de Facebook, la opción 804 para iniciar sesión usando una cuenta de Twitter, la opción 806 para inicie sesión usando una cuenta de Google y la opción 808 para iniciar sesión usando un número de teléfono o dirección de correo electrónico. La interfaz de usuario 800, así como las interfaces de usuario analizadas con referencia a las Figuras 9-23, se pueden presentar en una aplicación web o software del lado del cliente que se ejecuta en un dispositivo informático cliente.

En la Figura 9, la interfaz de usuario 900 muestra una interfaz de usuario de inicio de sesión de correo electrónico. La Figura 10 ilustra una interfaz de usuario 1000 en la que el usuario ha iniciado sesión. La interfaz de usuario 1000 incluye una pestaña "Transferencias" 1002, una pestaña "Conexiones" 1004 y una pestaña de usuario 1006 (se muestra el usuario "Ashish Gadnis"). La pestaña transferencias 1002 puede mostrar todas o las transferencias recientes hacia o desde el usuario que inició sesión realizadas a través de la plataforma de identidades y transacciones basada en cadena de bloques. La pestaña conexiones 1004, la pestaña activa en la interfaz de usuario 1000, muestra conexiones con las que el usuario ha establecido una relación de confianza.

La Figura 11 muestra una interfaz de usuario 1100 en la que está activa una pestaña de usuario 1102, que puede ser

similar a la pestaña de usuario 1006. La interfaz de usuario 1100 muestra información de perfil para el usuario, que incluye el perfil de plataforma del usuario 1104, que puede incluir información de inicio de sesión/contraseña, fecha de nacimiento, número de teléfono móvil con capacidad de texto, dirección de correo electrónico, dirección física u otra información. La información de perfil también puede incluir información del pasaporte 1106, información de permiso de conducción 1108, información de la seguridad social de Estados Unidos 1110 e información de identidad fuera de los Estados Unidos 1112. La información de perfil también puede incluir información adicional tal como de visa u otra información de estado. Parte o toda la información del perfil también puede ser parte de la identidad económica del usuario.

La Figura 12 ilustra una interfaz de usuario 1200 a través de la que un usuario puede invitar a otra persona a formar una relación de confianza o a establecer una cuenta como usuario de la plataforma y formar una relación de confianza. La interfaz de usuario 1200 se presenta mientras está activa una pestaña de conexiones 1202. La información de invitación 1204 puede incluir el nombre, dirección de correo electrónico, número de teléfono móvil con capacidad de texto, país, dirección y/u otra información del invitado. Una vez que se introduce la información de invitación 1204, se puede enviar un mensaje al invitado y se le puede solicitar que establezca una cuenta y/o establezca una relación de confianza con el usuario.

La Figura 13 ilustra una interfaz de usuario 1300 que muestra un número de transacciones anteriores 1302 mostradas bajo el encabezado "Mis transferencias". Las transacciones anteriores 1302 incluyen transferencias de fondos tanto hacia como desde el usuario. En algunos ejemplos, el usuario puede filtrar los tipos de transacciones mostradas (por ejemplo, mostrar únicamente transferencias de fondos, mostrar autorización de asistencia médica y alimentaria, etc.). La Figura 14 muestra una interfaz de usuario 1400 en la que se muestra una vista de transacción detallada. La transacción 1402 incluye un mensaje "Salud", así como los primeros datos de autenticación "Código de clave secreta: B33-99C-861", e instrucciones para proporcionar el código al agente local para recibir la transferencia. La transacción 1404 incluye de manera similar un mensaje, código e instrucciones.

La Figura 15 ilustra una interfaz de usuario 1500 en la que ha iniciado sesión un administrador de plataforma, como se indica en la pestaña de "Administrador de BanQu" 1502. El administrador puede ver información adicional y realizar acciones adicionales. Por ejemplo, la pestaña "Agente" 1504 permite al administrador actuar como agente, y la pestaña "Cadena de bloques" 1506 permite al administrador acceder a una vista de cadena de bloques de una transacción, como se ilustra en la Figura 20.

En la interfaz de usuario 1600 de la Figura 16, la pestaña de agente 1602 está activa y se presenta una interfaz de búsqueda de transferencias 1604. Las transferencias se pueden buscar mediante un código de clave (por ejemplo, un código de 9 dígitos) y/o información adicional tal como el nombre de receptor, la dirección de correo electrónico o el número de teléfono. La interfaz de usuario 1600 puede ser, por ejemplo, la interfaz a través de la que un agente introduce primeros datos de autenticación (tal como un código de 9 dígitos). En la interfaz de usuario 1700 de la Figura 17, se ha introducido un código de clave y se presenta una interfaz de transferencia encontrada 1702 que incluye información de identidad 1704 para el receptor (una imagen) junto con la "Etiqueta electrónica de foto (PhotoETag)" 1706, que es una clave privada, habilitada para un uso único, que verifica la foto y la identidad del receptor. En algunos ejemplos, la interfaz de búsqueda de transferencias 1604 es lo que un agente de verificación puede usar durante un proceso de verificación de transacciones como se analiza, por ejemplo, con respecto a las Figuras 5, 6 y 7.

La Figura 18 ilustra una interfaz de usuario 1800 similar a la interfaz de usuario 1700 de la Figura 17, pero está presente información adicional (que indica una etapa posterior en la verificación), que incluye los datos de autenticación de segunda etapa 1802, mostrados como un código de 6 dígitos, que se envió a una cuenta o dispositivo móvil del receptor y se presentó e introdujo por un agente de verificación. En algunos ejemplos, la interfaz de usuario 1700 de la Figura 17 y la interfaz de usuario 1800 de la Figura 18 son lo que ve un agente después de que se determina que los datos de autenticación de primera etapa coinciden (Figura 17) y después de que el agente haya introducido los datos de autenticación de segunda etapa (Figura 18). La imagen (información de identidad 1704) mostrada en la interfaz de usuario de transferencia encontrada 1702 puede ser la información de identidad descifrada proporcionada al agente. Por ejemplo, a un agente de verificación que ha introducido un código de 9 dígitos se le presenta la imagen del receptor previsto y puede (en algunos ejemplos) confirmar que una persona en presencia del agente parece coincidir con la imagen. La confirmación puede ser una etapa explícita o la confirmación puede ser implícita si el agente introduce un segundo código (u otros datos de autenticación de segunda etapa que se generaron después de la verificación de los datos de autenticación de primera etapa) proporcionados por la persona en presencia del agente.

En algunos ejemplos, después de que se muestra la interfaz de usuario de transferencia encontrada 1702, el agente confirma que la imagen mostrada se parece a una persona en presencia del agente, y, a continuación, se generan los datos de autenticación de segunda etapa 1802 y se envían al dispositivo móvil del receptor y se muestran en la interfaz de usuario 1800. En algunos ejemplos, no se realiza la confirmación de la identidad de la persona o está implícita en que el agente de verificación introduce un segundo código. En algunos ejemplos, los datos de autenticación de segunda etapa 1802 se muestran en la interfaz de usuario 1800 en el momento en que los datos de autenticación de segunda etapa 1802 se envían al dispositivo móvil del receptor, y el agente puede verificar si la persona en presencia del agente ha proporcionado o no el código correcto. En otros ejemplos, al agente no se le proporciona el código, y el agente simplemente introduce lo que la persona en presencia del agente proporciona, y la plataforma determina la

verificación del código.

Una vez que el receptor recibe los datos de autenticación de segunda etapa 1802 y proporciona este código al agente, el agente puede autorizar la transacción si hay una coincidencia o introducir el código proporcionado, y si se determina una coincidencia, se notifica al agente que la transacción está autorizada y/o se ha completado, como se muestra en la interfaz de usuario de transferencia completa 1902 de la interfaz de usuario 1900 de la Figura 19.

En la interfaz de usuario 2000 de la Figura 20, la pestaña cadena de bloques 2002 está activa. La interfaz de usuario 2000 incluye una vista de panel de control que incluye un número de bloque actual 2004 en la cadena de bloques donde se almacena la transacción completa. La vista de panel de control también incluye información de sesión de explorador 2006 que indica cuántos exploradores están accediendo actualmente directamente a la cadena de bloques en el punto actual e información de pares de cadena de bloques 2008 que indica a cuántos nodos de cadena de bloques se está accediendo para mostrar las transacciones de cadena de bloques de plataforma. La vista pendiente 2010 ilustra los datos almacenados en el bloque actual, que incluyen la transacción.

La Figura 21 muestra una interfaz de usuario 2100 en la que una vista pendiente 2102 incluye un desglose transacción por transacción de lo que está almacenado en el bloque actual. Los datos cifrados y de función de troceo se almacenan en la cadena de bloques. Cada transacción, y la diferente información que la describe, se convierte en parte de los bloques inmutables que se almacenan en la cadena de bloques autorizada (por ejemplo, una cadena de bloques de Ethereum). La información almacenada representa, incluyendo los datos de autenticación de primera etapa ("testigo"), la cantidad transferida ("cantidad"), así como la información de emisor, receptor y agente.

La Figura 22 ilustra una interfaz de usuario 2200 de un programa de correo electrónico en el que se envía un mensaje 2202 al receptor que indica que se han proporcionado datos de autenticación de primera etapa y que incluye un "Código de confirmación de retirada" (datos de autenticación de segunda etapa) que ha de proporcionarse al agente de verificación para completar la transacción. En algunos ejemplos, los datos de autenticación de segunda etapa se envían a un dispositivo móvil asociado con el receptor, y, en otros ejemplos, tal como el que se muestra en la Figura 22, los datos de autenticación de segunda etapa se envían por correo electrónico o alerta de mensaje enviados a través de una aplicación de software asociada con la plataforma.

La Figura 23 ilustra una interfaz de usuario 2300 que ilustra una confirmación de correo electrónico de transferencia completa 2302 proporcionada al emisor después de completar con éxito una transferencia.

La información asociada a un usuario se puede almacenar en diferentes bloques, ya estén predefinidos por la aplicación o creados ad-hoc por el usuario, en la cadena de bloques. Para recuperar esta información, por ejemplo, cuando un usuario inicia sesión en una aplicación web y se presenta el perfil del usuario, se puede crear una "proyección" buscando en la cadena de bloques información asociada con el usuario y recuperando esa información. Por ejemplo, se puede realizar una búsqueda basándose en el identificador único del usuario.

Se pueden crear proyecciones para toda la información asociada con una cuenta del usuario y/o para diferentes "personas". Un usuario puede establecer diferentes personas dentro de la cuenta del usuario, cada una de las cuales puede incluir diferentes tipos y cantidades de información. Por ejemplo, un usuario puede crear una persona de "salud" que incluye información de identidad e información de salud (registros de vacunas, registros médicos, etc.), pero no información de empleo, información de educación, etc. que no esté relacionada con la salud del usuario. De manera similar, un usuario puede crear una persona de educación que incluye información de identidad y educación, pero no información de salud, de propiedad, etc. que no esté relacionada con la educación del usuario.

El usuario también puede establecer diferentes inicios de sesión/enfoques de inicio de sesión para acceder a las diferentes personas. En algunos ejemplos, se encuentran disponibles inicios de sesión con distintos niveles de seguridad, y se pueden usar enfoques de inicio de sesión más seguros (por ejemplo, autenticación de múltiples factores, huellas digitales, etc.) para la información que el usuario considera más sensible o confidencial, y se pueden usar enfoques de inicio de sesión menos seguros (por ejemplo, pin, contraseña, frase de paso, etc.) para información que el usuario considera menos sensible o confidencial. En algunos ejemplos, se usa el mismo inicio de sesión para algunas o todas las personas. Los inicios de sesión se pueden usar, por ejemplo, cuando un usuario desea compartir una persona particular con otro usuario o entidad.

Se ilustran personas ilustrativas en la Figura 27. Una identidad económica basada en cadena de bloques asegurada 2702 (que puede ser similar a la identidad económica 200 de la Figura 2, por ejemplo) se almacena en uno o más bloques en una cadena de bloques. Diferentes personas incluyen o acceden a diferentes aspectos de la identidad económica 2702. Por ejemplo, una persona de salud 2704, accesible mediante un inicio de sesión con huella digital 2706, puede incluir unos registros médicos o el historial de vacunación del usuario y permite a un usuario visitar una clínica médica o una estación de ayuda médica que tiene una cuenta en la plataforma de identidades y transacciones basada en cadena de bloques, introducir información de contacto y/o un nombre de usuario, y proporcionar una huella digital para permitir que la clínica médica tenga acceso a los registros de salud del usuario y otra información incluida en la persona de salud 2704. Una clínica médica también puede tener una persona predefinida establecida que puede acceder a la información del usuario (con el permiso del usuario).

La persona de educación 2708 puede incluir informes de calificaciones, expedientes académicos u otra información y puede ser accesible, por ejemplo, a través de la frase de paso 2710. La persona de servicios públicos 2712 puede incluir diversos registros de servicios públicos, incluyendo direcciones de servicios, pagos, historial de uso, etc., y se puede acceder mediante el código PIN 2714. También se puede crear una persona general o predeterminada. El enfoque de persona permite a un usuario controlar qué información está liberando el usuario a diversas instituciones y otros usuarios y mantener otros datos como privados. Aunque se muestran en la Figura 27 los métodos de acceso particulares (huella digital 2706, frase de paso 2710, y código PIN 2714) como asociados con personas particulares, pueden seleccionarse o asignarse diversos métodos de acceso diferentes a cualquier persona.

Las capacidades de almacenamiento seguro de la cadena de bloques se han analizado en el presente documento, pero la cadena de bloques también puede ejecutar código, que puede implementarse como "contratos inteligentes", que son programas que se almacenan en la cadena de bloques y se ejecutan en la cadena de bloques.

Sistemas informáticos ilustrativos

La Figura 24 representa un ejemplo generalizado de un sistema informático 2400 adecuado en el que se pueden implementar las innovaciones descritas. El sistema informático 2400 no pretende sugerir ninguna limitación en cuanto al alcance de uso o funcionalidad, ya que las innovaciones pueden implementarse en diversos sistemas informáticos de propósito general o especial.

Con referencia a la Figura 24, el sistema informático 2400 incluye una o más unidades de procesamiento 2410, 2415 y memoria 2420, 2425. En la Figura 24, esta configuración básica 2430 se incluye dentro de una línea discontinua. Las unidades de procesamiento 2410, 2415 ejecutan instrucciones ejecutables por ordenador. Una unidad de procesamiento puede ser una unidad central de procesamiento (CPU) de propósito general, un procesador en un circuito integrado de específico de la aplicación (ASIC) o cualquier otro tipo de procesador. En un sistema multiprocesamiento, múltiples unidades de procesamiento ejecutan instrucciones ejecutables por ordenador para aumentar la potencia de procesamiento. Por ejemplo, la Figura 24 muestra una unidad central de procesamiento 2410, así como una unidad de procesamiento de gráficos o unidad de coprocesamiento 2415. La memoria tangible 2420, 2425 puede ser memoria volátil (por ejemplo, registros, caché, RAM), memoria no volátil (por ejemplo, ROM, EEPROM, memoria flash, etc.), o alguna combinación de las dos, accesible por la unidad o unidades de procesamiento. La memoria 2420, 2425 almacena software 2480 que implementa una o más innovaciones descritas en el presente documento, en forma de instrucciones ejecutables por ordenador adecuadas para su ejecución por la unidad o unidades de procesamiento. Por ejemplo, la memoria 2420 puede almacenar software 2480 que implementa el motor de inscripción 116 y el motor de transacciones 118 de la Figura 1.

Un sistema informático puede tener características adicionales. Por ejemplo, el sistema informático 2400 incluye almacenamiento 2440, uno o más dispositivos de entrada 2450, uno o más dispositivos de salida 2460 y una o más conexiones de comunicación 2470. Un mecanismo de interconexión (no mostrado) tal como un bus, controlador o red interconecta los componentes del sistema informático 2400. Típicamente, el software de sistema operativo (no mostrado) proporciona un entorno operativo para otro software que se ejecuta en el sistema informático 2400 y coordina las actividades de los componentes del sistema informático 2400.

El almacenamiento tangible 2440 puede ser extraíble o no extraíble e incluye discos magnéticos, cintas o casetes magnéticos, CD-ROM, DVD o cualquier otro medio que pueda usarse para almacenar información y al que se pueda acceder dentro del sistema informático 2400. El almacenamiento 2440 almacena instrucciones para el software 2480 que implementa una o más innovaciones descritas en el presente documento.

El dispositivo o dispositivos de entrada 2450 pueden ser un dispositivo de entrada táctil tal como un teclado, ratón, lápiz o bola de mando, un dispositivo de entrada de voz, un dispositivo de escaneo u otro dispositivo que proporciona entrada al sistema informático 2400. Para la codificación de vídeo, el dispositivo o dispositivos de entrada 2450 pueden ser una cámara, tarjeta de vídeo, tarjeta sintonizadora de TV o dispositivo similar que acepte entrada de vídeo en forma analógica o digital, o un CD-ROM o CD-RW que lea muestras de vídeo en el sistema informático 2400. El dispositivo o dispositivos de salida 2460 pueden ser una pantalla, una impresora, un altavoz, una grabadora de CD u otro dispositivo que proporcione salida desde el sistema informático 2400.

La conexión o conexiones de comunicación 2470 permiten la comunicación a través de un medio de comunicación con otra entidad informática. El medio de comunicación transporta información tal como instrucciones ejecutables por ordenador, entrada o salida de audio o video u otros datos en una señal de datos modulada. Una señal de datos modulada es una señal que tiene una o más de sus características establecidas o modificadas de tal manera que codifican información en la señal. A modo de ejemplo, y sin limitación, los medios de comunicación pueden usar una portadora eléctrica, óptica, de RF u otra.

Las innovaciones se pueden describir en el contexto general de instrucciones ejecutables por ordenador, tales como aquellas incluidas en módulos de programa, que se ejecutan en un sistema informático en un procesador real o virtual objetivo. En general, los módulos de programa incluyen rutinas, programas, bibliotecas, objetos, clases, componentes,

estructuras de datos, etc., que realizan tareas particulares o implementan tipos de datos abstractos particulares. La funcionalidad de los módulos de programa se puede combinar o dividir entre módulos de programa según se desee en diversas realizaciones. Las instrucciones ejecutables por ordenador para módulos de programa pueden ejecutarse dentro de un sistema informático local o distribuido.

Los términos "sistema" y "dispositivo" se usan indistintamente en el presente documento. A menos que el contexto indique claramente lo contrario, ninguno de los términos implica limitación alguna sobre un tipo de sistema informático o dispositivo informático. En general, un sistema informático o dispositivo informático puede ser local o distribuido y puede incluir cualquier combinación de hardware de propósito especial y/o hardware de propósito general con software que implemente la funcionalidad descrita en el presente documento.

Por motivos de presentación, la descripción detallada usa términos como "determinar" y "usar" para describir las operaciones informáticas en un sistema informático. Estos términos son abstracciones de alto nivel para operaciones realizadas por un ordenador y no deben confundirse con actos realizados por un ser humano. Las operaciones informáticas reales correspondientes a estos términos varían dependiendo de la implementación.

Dispositivos móviles ilustrativos

La Figura 25 es un diagrama de sistema que representa un dispositivo móvil 2500 ilustrativo que incluye una diversidad de componentes de hardware y software opcionales, mostrados en general en 2502. Cualquier componente 2502 en el dispositivo móvil puede comunicarse con cualquier otro componente, aunque no se muestran todas las conexiones, para facilitar la ilustración. El dispositivo móvil puede ser cualquiera de una diversidad de dispositivos informáticos (por ejemplo, teléfono celular, teléfono inteligente, ordenador de mano, asistente digital personal (PDA), etc.) y puede permitir comunicaciones bidireccionales inalámbricas con una o más redes de comunicaciones móviles 2504, tales como una red celular, satelital u otra.

El dispositivo móvil 2500 ilustrado puede incluir un controlador o procesador 2510 (por ejemplo, procesador de señal, microprocesador, ASIC u otra circuitería lógica de control y procesamiento) para realizar tareas tales como codificación de señales, procesamiento de datos, procesamiento de entrada/salida, control de potencia, y/u otras funciones. Un sistema operativo 2512 puede controlar la asignación y el uso de los componentes 2502 y el soporte para uno o más programas de aplicación 2514. Los programas de aplicación pueden incluir aplicaciones informáticas móviles comunes (por ejemplo, aplicaciones de correo electrónico, calendarios, gestores de contactos, exploradores web, aplicaciones de mensajería) o cualquier otra aplicación informática. La funcionalidad 2513 para acceder a una tienda de aplicaciones también se puede usar para adquirir y actualizar programas de aplicación 2514.

El dispositivo móvil 200 ilustrado puede incluir memoria 2520. La memoria 2520 puede incluir memoria no extraíble 2522 y/o memoria extraíble 2524. La memoria no extraíble 2522 puede incluir RAM, ROM, memoria flash, un disco duro u otras tecnologías de almacenamiento de memoria bien conocidas. La memoria extraíble 2524 puede incluir una memoria flash o una tarjeta de módulo de identidad de abonado (SIM), que es bien conocida en los sistemas de comunicación de GSM, u otras tecnologías de almacenamiento de memoria bien conocidas, tales como "tarjetas inteligentes". La memoria 2520 se puede usar para almacenar datos y/o código para ejecutar el sistema operativo 2512 y las aplicaciones 2514. Los datos de ejemplo pueden incluir páginas web, texto, imágenes, archivos de sonido, datos de video u otros conjuntos de datos para ser enviados y/o recibidos desde uno o más servidores de red u otros dispositivos a través de una o más redes alámbricas o inalámbricas. La memoria 2520 se puede usar para almacenar un identificador de abonado, tal como una identidad de abonado móvil internacional (IMSI), y un identificador de equipo, tal como un identificador de equipo móvil internacional (IMEI). Tales identificadores pueden transmitirse a un servidor de red para identificar usuarios y equipo. La memoria 2520 puede almacenar instrucciones o código que implementa el motor de inscripción 116 y el motor de transacciones 118 de la Figura 1.

El dispositivo móvil 2500 puede soportar uno o más dispositivos de entrada 2530, tales como una pantalla táctil 2532, micrófono 2534, cámara 2536, teclado físico 2538 y/o bola de mando 2540 y una o más dispositivos de salida 2550, tales como un altavoz 2552 y una pantalla 2554. Otros posibles dispositivos de salida (no mostrados) pueden incluir dispositivos de salida piezoeléctricos u otros hápticos. Algunos dispositivos pueden tener más de una función de entrada/salida. Por ejemplo, la pantalla táctil 2532 y la pantalla 2554 se pueden combinar en un único dispositivo de entrada/salida.

Los dispositivos de entrada 2530 pueden incluir una Interfaz de Usuario Natural (Natural User Interface, NUI). Una NUI es cualquier tecnología de interfaz que permite a un usuario interactuar con un dispositivo de manera "natural", sin restricciones artificiales impuestas por dispositivos de entrada tales como ratones, teclados, controles remotos y similares. Ejemplos de métodos de NUI incluyen aquellos que se basan en el reconocimiento de voz, el reconocimiento táctil y de lápiz óptico, el reconocimiento de gestos tanto en la pantalla como adyacentes a ella, los gestos aéreos, el rastreo de la cabeza y los ojos, la voz y el habla, la visión, el tacto, los gestos y la inteligencia artificial. Otros ejemplos de NUI incluyen detección de gestos de movimiento usando acelerómetros/giroscopios, reconocimiento facial, pantallas 3D, seguimiento de cabeza, ojos y mirada, realidad aumentada inmersiva y sistemas de realidad virtual, todos los cuales proporcionan una interfaz más natural, así como tecnologías para detectar la actividad cerebral mediante electrodos de detección de campos eléctricos (EEG y métodos relacionados). Por lo tanto, en un ejemplo

específico, el sistema operativo 2512 o las aplicaciones 2514 pueden comprender software de reconocimiento de voz como parte de una interfaz de usuario de voz que permite a un usuario operar el dispositivo 2500 mediante comandos de voz. Además, el dispositivo 2500 puede comprender dispositivos de entrada y software que permitan la interacción de usuario a través de gestos espaciales del usuario, tales como detectar e interpretar gestos para proporcionar entrada a una aplicación de juego.

Un módem inalámbrico 2560 se puede acoplar a una antena (no mostrada) y puede soportar comunicaciones bidireccionales entre el procesador 2510 y dispositivos externos, como es bien entendido en la técnica. El módem 2560 se muestra genéricamente y puede incluir un módem celular para comunicarse con la red de comunicación móvil 2504 y/u otros módems basados en radio (por ejemplo, Bluetooth 2564 o Wi-Fi 2562). El módem inalámbrico 2560 se configura típicamente para comunicación con una o más redes celulares, tales como una red de GSM para comunicaciones de voz y datos dentro de una única red celular, entre redes celulares o entre el dispositivo móvil y una red telefónica pública conmutada (PSTN).

El dispositivo móvil puede incluir además al menos un puerto de entrada/salida 2580, una fuente de alimentación 2582, un receptor de sistema de navegación por satélite 2584, tal como un receptor de Sistema de Posicionamiento Global (GPS), un acelerómetro 2586 y/o un conector físico 2590. que puede ser un puerto USB, un puerto IEEE 1394 (FireWire) y/o un puerto RS-232. Los componentes ilustrados 2502 no son obligatorios o no se incluyen todos, ya que se puede eliminar cualquier componente y se pueden añadir otros componentes.

Entornos soportados en la nube ilustrativos

La Figura 26 ilustra un ejemplo generalizado de un entorno soportado en la nube 2600 adecuado en el que se pueden implementar las realizaciones, técnicas y tecnologías descritas. En el entorno ilustrativo 2600, una nube 2610 proporciona diversos tipos de servicios (por ejemplo, servicios informáticos). Por ejemplo, la nube 2610 puede comprender una colección de dispositivos informáticos, que pueden estar ubicados centralmente o distribuidos, que proporcionan servicios basados en la nube a diversos tipos de usuarios y dispositivos conectados a través de una red tal como Internet. El entorno de implementación 2600 se puede usar de diferentes maneras para lograr tareas informáticas. Por ejemplo, algunas tareas (por ejemplo, procesar la entrada de usuario y presentar una interfaz de usuario) se pueden realizar en dispositivos informáticos locales (por ejemplo, los dispositivos conectados 2630, 2640, 2650) mientras que otras tareas (por ejemplo, el almacenamiento de datos a usar en el procesamiento posterior) se puede realizar en la nube 2610.

En el entorno 2600 ilustrativo, la nube 2610 proporciona servicios para dispositivos conectados 2630, 2640, 2650 con una diversidad de capacidades de pantalla. El dispositivo conectado 2630 representa un dispositivo con una pantalla de ordenador 2635 (por ejemplo, una pantalla de tamaño mediano). Por ejemplo, el dispositivo conectado 2630 podría ser un ordenador personal tal como un ordenador de sobremesa, un ordenador portátil, un portátil, un portable o similar. El dispositivo conectado 2640 representa un dispositivo con una pantalla de dispositivo móvil 2645 (por ejemplo, una pantalla de tamaño pequeño). Por ejemplo, el dispositivo conectado 2640 podría ser un teléfono móvil, un teléfono inteligente, un asistente digital personal, una tableta y similares. El dispositivo conectado 2650 representa un dispositivo con una pantalla grande 2655. Por ejemplo, el dispositivo conectado 2650 podría ser una pantalla de televisión (por ejemplo, una televisión inteligente) u otro dispositivo conectado a una televisión (por ejemplo, un decodificador de salón o consola de juegos) o similar. Uno o más de los dispositivos conectados 2630, 2640, 2650 pueden incluir capacidades de pantalla táctil. Las pantallas táctiles pueden aceptar entrada de diferentes maneras. Por ejemplo, las pantallas táctiles capacitivas detectan entrada táctil cuando un objeto (por ejemplo, la punta de un dedo o un lápiz óptico) distorsiona o interrumpe una corriente eléctrica que recorre la superficie. Como otro ejemplo, las pantallas táctiles pueden usar sensores ópticos para detectar entrada táctil cuando se interrumpen los haces de los sensores ópticos. El contacto físico con la superficie de la pantalla no es necesario para que algunas pantallas táctiles detecten la entrada. Los dispositivos sin capacidades de pantalla también se pueden usar en el entorno 2600 ilustrativo. Por ejemplo, la nube 2610 puede proporcionar servicios para uno o más ordenadores (por ejemplo, ordenadores de servidor) sin pantallas.

Los servicios pueden proporcionarse por la nube 2610 a través de proveedores de servicios 2620, o a través de otros proveedores de servicios en línea (no representados). Por ejemplo, los servicios en la nube se pueden personalizar según el tamaño de la pantalla, la capacidad de visualización y/o la capacidad de la pantalla táctil de un dispositivo conectado particular (por ejemplo, los dispositivos conectados 2630, 2640, 2650).

En el entorno 2600 ilustrativo, la nube 2610 proporciona las tecnologías y soluciones descritas en el presente documento a los diversos dispositivos conectados 2630, 2640, 2650 usando, al menos en parte, los proveedores de servicios 2620. Por ejemplo, los proveedores de servicios 2620 pueden proporcionar una solución centralizada para diversos servicios basados en la nube. Los proveedores de servicios 2620 pueden gestionar suscripciones de servicios para usuarios y/o dispositivos (por ejemplo, para los dispositivos conectados 2630, 2640, 2650 y/o sus respectivos usuarios). Parte o toda la funcionalidad del motor de inscripción 2660 y el motor de transacciones 2662, que pueden ser similares al motor de inscripción 116 y al motor de transacciones 118 de la Figura 1, se puede implementar en la nube 2610.

Implementaciones ilustrativas

Aunque las operaciones de algunos de los métodos divulgados se describen en un orden secuencial particular para una presentación conveniente, debe entenderse que esta manera de descripción abarca la reorganización, a menos que se requiera un orden particular mediante el lenguaje específico expuesto a continuación. Por ejemplo, las operaciones descritas secuencialmente, en algunos casos, pueden reorganizarse o realizarse al mismo tiempo. Además, por motivos de simplicidad, es posible que las figuras adjuntas no muestren las diversas formas en que se pueden usar los métodos divulgados en conjunto con otros métodos.

Cualquiera de los métodos divulgados puede implementarse como instrucciones ejecutables por ordenador o un producto de programa informático almacenado en uno o más medios de almacenamiento legibles por ordenador y ejecutado en un dispositivo informático (por ejemplo, cualquier dispositivo informático disponible, incluyendo teléfonos inteligentes u otros dispositivos móviles que incluyen hardware informático). Los medios de almacenamiento legibles por ordenador son cualquier medio tangible disponible al que se pueda acceder dentro de un entorno informático (por ejemplo, uno o más discos de medios ópticos tales como DVD o CD, componentes de memoria volátil (tales como DRAM o SRAM) o componentes de memoria no volátil (tales como memoria flash o discos duros)). A modo de ejemplo y con referencia a la Figura 24, los medios de almacenamiento legibles por ordenador incluyen la memoria 2420 y 2425, y el almacenamiento 2440. A modo de ejemplo y con referencia a la Figura 25, los medios de almacenamiento legibles por ordenador incluyen la memoria y almacenamiento 2520, 2522 y 2524. La expresión medios de almacenamiento legibles por ordenador no incluye señales ni ondas portadoras. Además, la expresión medios de almacenamiento legibles por ordenador no incluye conexiones de comunicación (por ejemplo, 2470, 2560, 2562 y 2564).

Cualquiera de las instrucciones ejecutables por ordenador para implementar las técnicas divulgadas, así como cualquier dato creado y usado durante la implementación de las realizaciones divulgadas, se puede almacenar en uno o más medios de almacenamiento legibles por ordenador. Las instrucciones ejecutables por ordenador pueden ser parte de, por ejemplo, una aplicación de software especializada o una aplicación de software a la que se accede o se descarga a través de un explorador web u otra aplicación de software (tal como una aplicación informática remota). Tal software se puede ejecutar, por ejemplo, en un único ordenador local (por ejemplo, cualquier ordenador disponible comercialmente adecuado) o en un entorno de red (por ejemplo, a través de Internet, una red de área amplia, una red de área local, una red de cliente-servidor (tal como una red de informática en la nube), u otra red similar) usando uno o más ordenadores de red.

Para mayor claridad, únicamente se describen ciertos aspectos seleccionados de las implementaciones basadas en software. Se omiten otros detalles que son bien conocidos en la técnica. Por ejemplo, debe entenderse que la tecnología divulgada no se limita a ningún lenguaje o programa informático específico. Por ejemplo, la tecnología divulgada puede implementarse mediante software escrito en C++, Java, Perl, JavaScript, Adobe Flash o cualquier otro lenguaje de programación adecuado. Análogamente, la tecnología divulgada no se limita a ningún ordenador o tipo de hardware particular. Ciertos detalles de ordenadores y hardware adecuados son bien conocidos y no es necesario exponerlos en detalle en esta divulgación.

Además, cualquiera de las realizaciones basadas en software (que comprenden, por ejemplo, instrucciones ejecutables por ordenador para hacer que un ordenador realice cualquiera de los métodos divulgados) se puede cargar, descargar o acceder de forma remota a través de un medio de comunicación adecuado. Tales medios de comunicación adecuados incluyen, por ejemplo, Internet, la red informática mundial, una intranet, aplicaciones de software, cable (que incluye cable de fibra óptica), comunicaciones magnéticas, comunicaciones electromagnéticas (incluyendo comunicaciones de RF, microondas e infrarrojos), comunicaciones electrónicas, u otros medios de comunicación de este tipo.

Los métodos, aparatos y sistemas divulgados no deben interpretarse como limitativos de ninguna manera. En su lugar, la presente divulgación está dirigida a todas las características y aspectos novedosos y no evidentes de las diversas realizaciones divulgadas, en solitario y en diversas combinaciones y subcombinaciones entre sí. Los métodos, aparatos y sistemas divulgados no se limitan a ningún aspecto o característica específica o combinación de los mismos, ni las realizaciones divulgadas requieren que estén presentes una o más ventajas específicas o que se resuelvan problemas.

Las tecnologías de cualquier ejemplo se pueden combinar con las tecnologías descritas en uno cualquiera o más de los otros ejemplos. En vista de las muchas realizaciones posibles a las que pueden aplicarse los principios de la tecnología divulgada, debe reconocerse que las realizaciones ilustradas son ejemplos de la tecnología divulgada y no deben tomarse como una limitación del alcance de la tecnología divulgada.

REIVINDICACIONES

1. Un método implementado por ordenador que comprende:

cifrar (302) información de identidad para una persona y almacenar la información de identidad cifrada en una cadena de bloques como parte de la inscripción de la persona como primer usuario en una plataforma de identidades y transacciones económica basada en cadena de bloques;

almacenar (304), en la cadena de bloques, registros de relaciones de confianza entre el primer usuario y otros usuarios;

autorizar (306) transacciones entre el primer usuario y uno o más de los otros usuarios con quienes el primer usuario ha formado una relación de confianza, en donde la autorización comprende autenticar al primer usuario con la información de identidad almacenada en la cadena de bloques; y

almacenar (308) registros de las transacciones en la cadena de bloques, en donde al menos algunas de las transacciones y la información de identidad contribuyen a una identidad económica del primer usuario.

2. El método de la reivindicación 1, que comprende además proporcionar la identidad económica del primer usuario a una parte solicitante, en donde la parte solicitante es otro usuario en la plataforma de identidades y transacciones económica basada en cadena de bloques.

3. El método de la reivindicación 1, en donde la identidad económica comprende además al menos una de información de historial de empleo, información de historial de educación, información de posesión de propiedades o información de historial médico para el primer usuario, y en donde la al menos una de información de historial de empleo, información de historial de educación, información de posesión de propiedades o información de historial médico se almacena en la cadena de bloques.

4. El método de la reivindicación 1, en donde la información de identidad comprende una imagen de la persona, en donde la relación de confianza entre el primer usuario y el uno o más de los otros usuarios se ha establecido mediante la aceptación, por el uno o más de los otros usuarios, de una solicitud o invitación para conectarse desde el primer usuario, y en donde la cadena de bloques es una cadena de bloques autorizada, habiendo sido inscritos el primer usuario y los otros usuarios en la plataforma basada en cadena de bloques mediante un motor de inscripción de la plataforma basada en cadena de bloques.

5. El método de la reivindicación 4, en donde:

la imagen de la persona se usa al autorizar las transacciones; o

la información de identidad comprende además al menos una de información de un nombre, un identificador gubernamental, una huella digital o un patrón ocular.

6. El método de la reivindicación 1, en donde las transacciones comprenden al menos una de una transferencia de fondos, una autorización de tratamiento médico o una autorización de asistencia alimentaria.

7. El método de la reivindicación 1, en donde la información de identidad cifrada se almacena en un bloque de la cadena de bloques, comprendiendo además el método, como parte de la inscripción de la persona en la plataforma de identificación y transacciones económicas basada en la cadena de bloques:

establecer, basándose en la información de identidad cifrada, un identificador único asociado con la persona.

8. El método de la reivindicación 7, en donde la información de identidad comprende una imagen de la persona, y en donde la información de identidad comprende además al menos una de información de un nombre, un identificador gubernamental, una huella digital o un patrón ocular.

9. El método de la reivindicación 8, en donde establecer el identificador único comprende designar la información de identidad cifrada como el identificador único.

10. El método de la reivindicación 8, que comprende además asociar, con el identificador único, al menos una de información médica, de empleo, educativa, de posesión de propiedades o económica correspondiente a la persona y almacenar la información médica, de empleo, educativa, de posesión de propiedades o económica en la cadena de bloques, en donde al menos una de información económica o de empleo se almacena en la cadena de bloques en asociación con el identificador único y representa la identidad económica de la persona.

11. El método de la reivindicación 1, en donde la autorización (306) de las transacciones incluye:

identificar (502) un receptor para una transacción dada de las transacciones;

generar (504) datos de autenticación de primera etapa;

recibir (506) una indicación de que los datos de autenticación de primera etapa se han proporcionado a un agente de verificación;

verificar (508) los datos de autenticación de primera etapa;

después de verificar los datos de autenticación de primera etapa, recuperar (510) información de identidad para el receptor de uno o más bloques en la cadena de bloques, en donde la información de identidad recuperada incluye una imagen cifrada digitalmente del receptor;

descifrar la imagen cifrada del receptor;

transmitir la imagen descifrada del receptor;

tras recibir una confirmación de que la imagen descifrada del receptor coincide con una segunda persona, estando la segunda persona en presencia del agente de verificación, generar y transmitir (512) datos de autenticación de segunda etapa;

recibir (514) una indicación de que los datos de autenticación de segunda etapa se han proporcionado al agente de verificación; y

después de verificar los datos de autenticación de segunda etapa, determinar (516) que la segunda persona es el receptor y autorizar la transacción.

12. El método de la reivindicación 11, en donde la información de identidad recuperada para el receptor está cifrada, y en donde descifrar la imagen cifrada del receptor incluye solicitar y recibir un testigo de descifrado.

13. El método de la reivindicación 11, en donde:

el almacenamiento (308) de registros de las transacciones en la cadena de bloques incluye almacenar un registro de la transacción dada en la cadena de bloques en asociación con el receptor; o

la autorización (306) de transacciones incluye, además, antes de generar los datos de autenticación de primera etapa: establecer un registro de una relación de confianza entre el receptor y el primer usuario, como emisor; y el almacenamiento (304) de los registros de relaciones de confianza incluye almacenar el registro de la relación de confianza entre el receptor y el emisor en la cadena de bloques; o

los datos de autenticación de primera y segunda etapa son códigos que comprenden al menos uno de números o letras.

14. Un dispositivo informático que comprende uno o más procesadores y uno o más medios de almacenamiento legibles por ordenador que tienen almacenados en los mismos instrucciones ejecutables por ordenador para hacer que el uno o más procesadores, cuando estén programados de este modo, realicen el método de una cualquiera de las reivindicaciones 1-13.

15. Una o más memorias o dispositivos de almacenamiento legibles por ordenador que tienen almacenados en los mismos instrucciones ejecutables por ordenador para hacer que un sistema informático, cuando se programa de este modo, realice el método de una cualquiera de las reivindicaciones 1-13.

FIG. 1

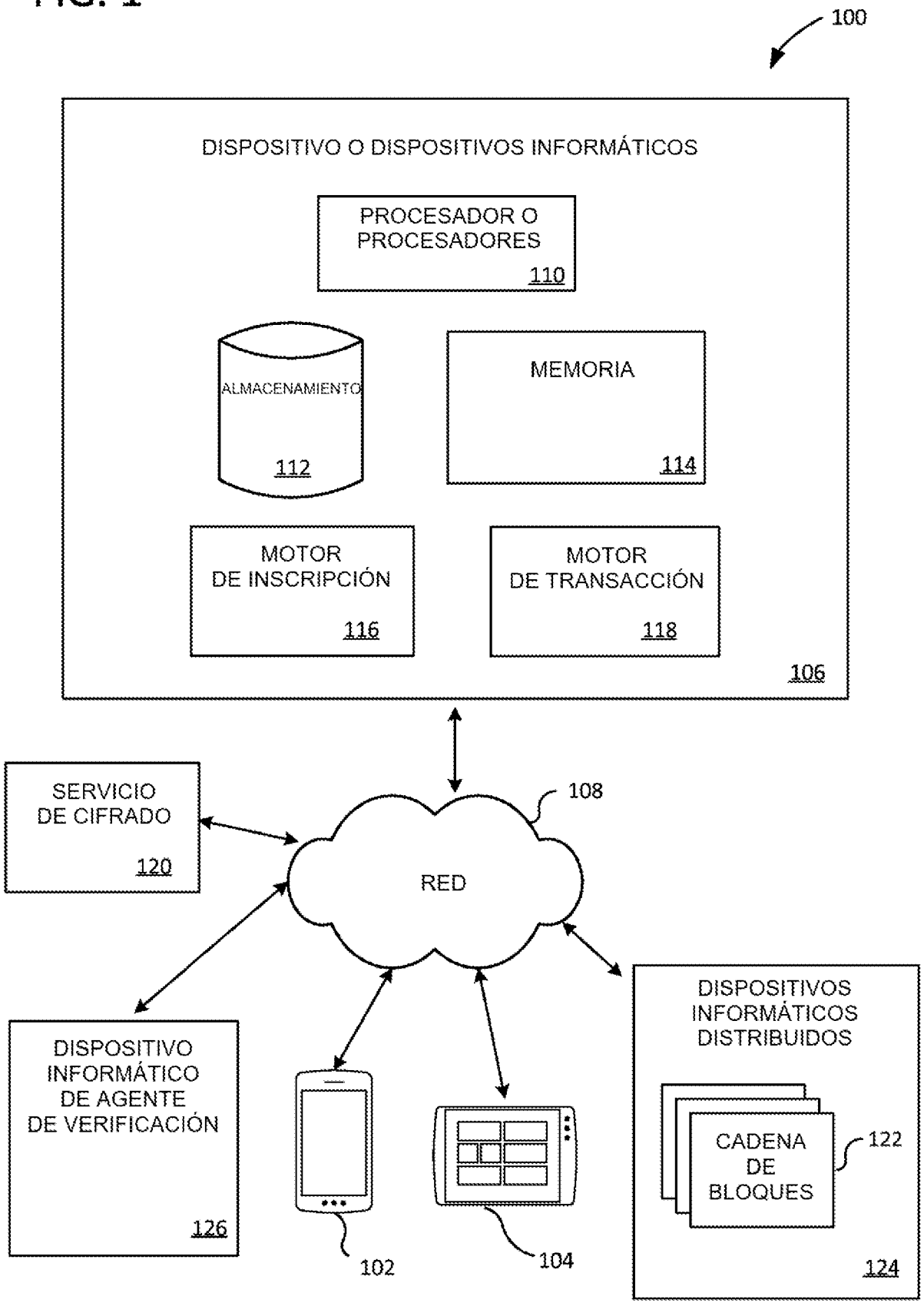

100
DISPOSITIVO O DISPOSITIVOS INFORMÁTICOS
PROCESADOR O PROCESADORES
110
ALMACENAMIENTO
112
MEMORIA
114
MOTOR DE INSCRIPCIÓN
116
MOTOR DE TRANSACCIÓN
118
106
SERVICIO DE CIFRADO
120
108
RED
DISPOSITIVO INFORMÁTICO DE AGENTE DE VERIFICACIÓN
126
102
104
DISPOSITIVOS INFORMÁTICOS DISTRIBUIDOS
CADENA DE BLOQUES
122
124

FIG. 2

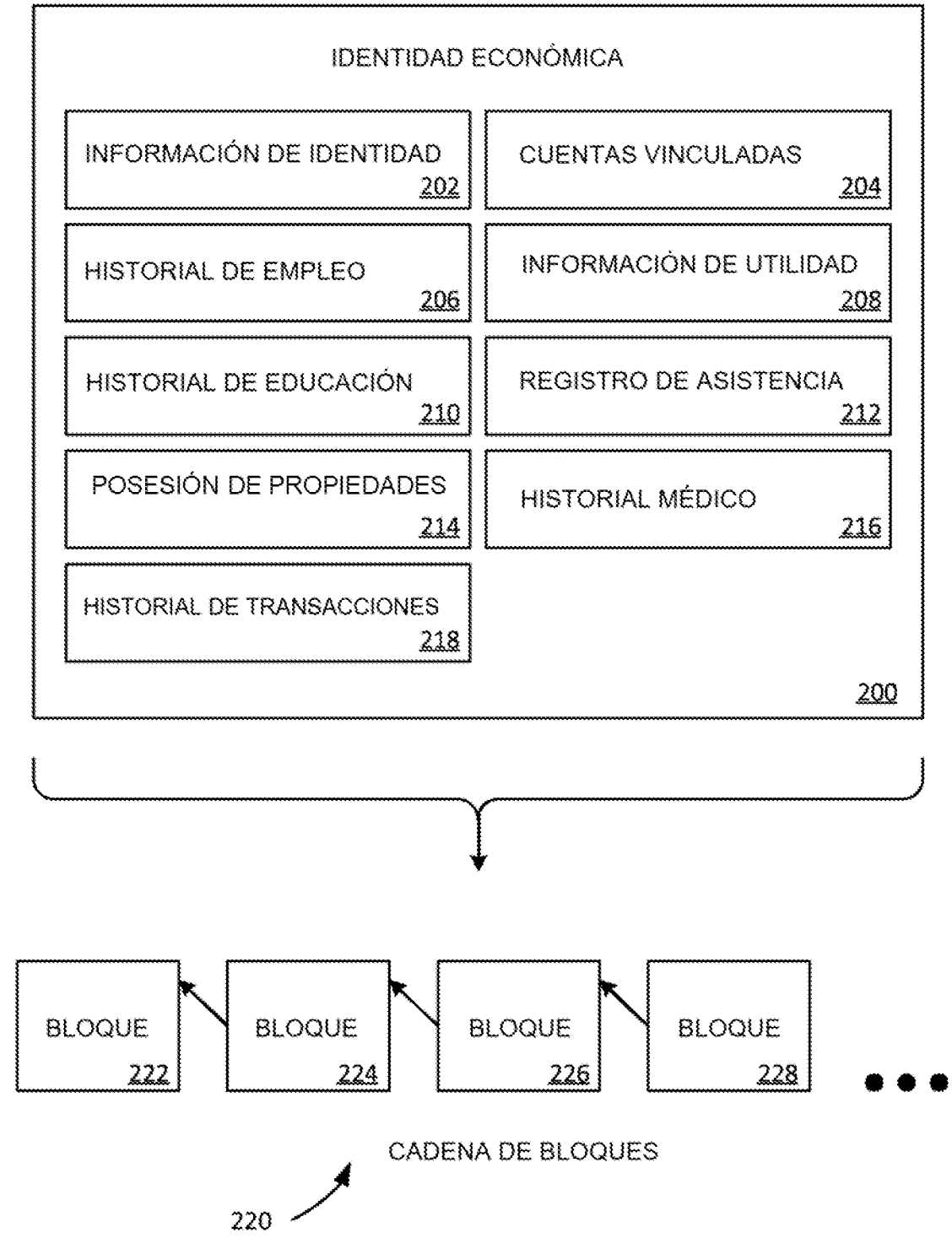

IDENTIDAD ECONÓMICA
INFORMACIÓN DE IDENTIDAD
202
CUENTAS VINCULADAS
204
HISTORIAL DE EMPLEO
206
INFORMACIÓN DE UTILIDAD
208
HISTORIAL DE EDUCACIÓN
210
REGISTRO DE ASISTENCIA
212
POSESIÓN DE PROPIEDADES
214
HISTORIAL MÉDICO
216
HISTORIAL DE TRANSACCIONES
218
200
BLOQUE
222
BLOQUE
224
BLOQUE
226
BLOQUE
228
CADENA DE BLOQUES
220

FIG. 3

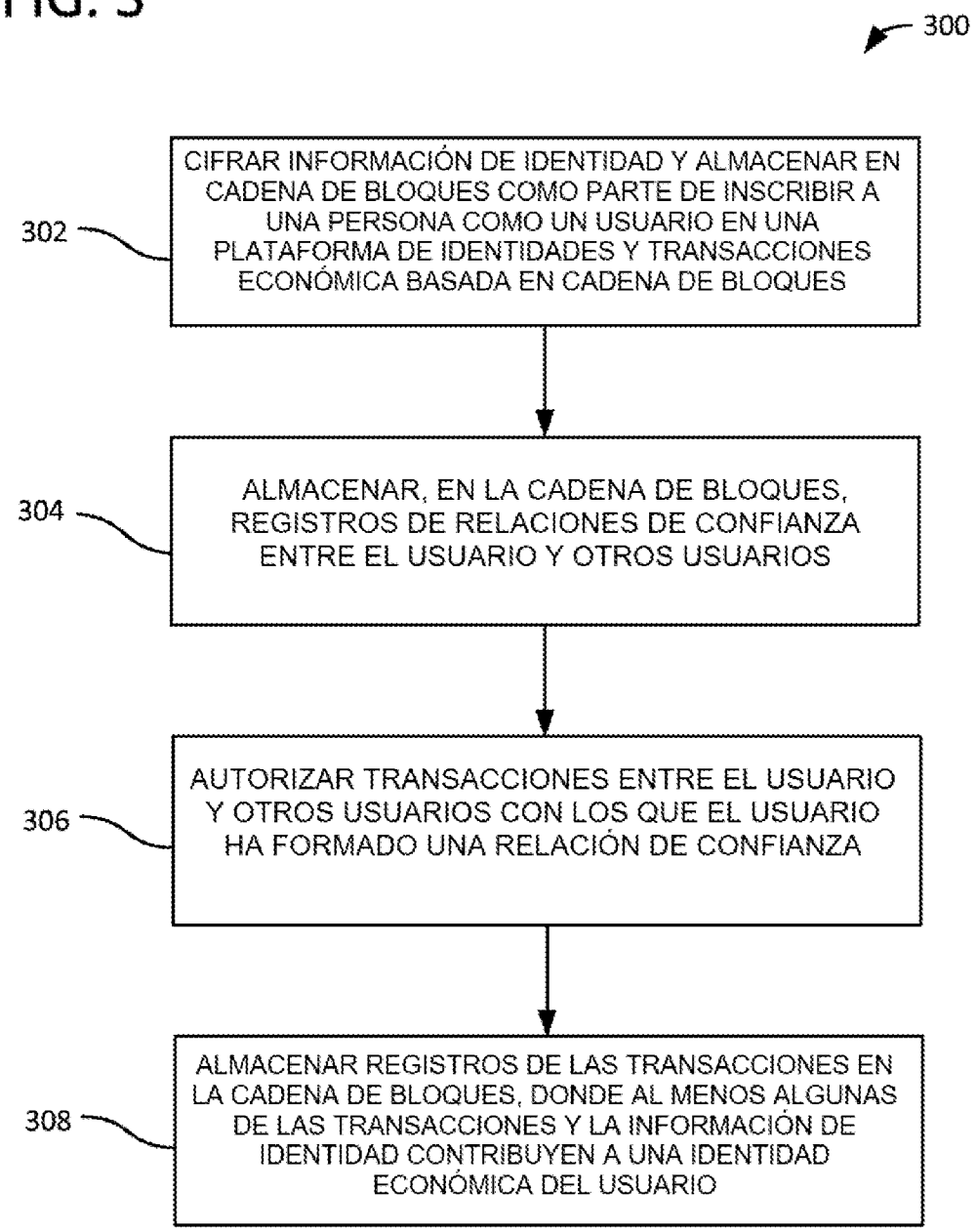

300
302
CIFRAR INFORMACIÓN DE IDENTIDAD Y ALMACENAR EN CADENA DE BLOQUES COMO PARTE DE INSCRIBIR A UNA PERSONA COMO UN USUARIO EN UNA PLATAFORMA DE IDENTIDADES Y TRANSACCIONES ECONÓMICA BASADA EN CADENA DE BLOQUES
304
ALMACENAR, EN LA CADENA DE BLOQUES, REGISTROS DE RELACIONES DE CONFIANZA ENTRE EL USUARIO Y OTROS USUARIOS
306
AUTORIZAR TRANSACCIONES ENTRE EL USUARIO Y OTROS USUARIOS CON LOS QUE EL USUARIO HA FORMADO UNA RELACIÓN DE CONFIANZA
308
ALMACENAR REGISTROS DE LAS TRANSACCIONES EN LA CADENA DE BLOQUES, DONDE AL MENOS ALGUNAS DE LAS TRANSACCIONES Y LA INFORMACIÓN DE IDENTIDAD CONTRIBUYEN A UNA IDENTIDAD ECONÓMICA DEL USUARIO

FIG. 4

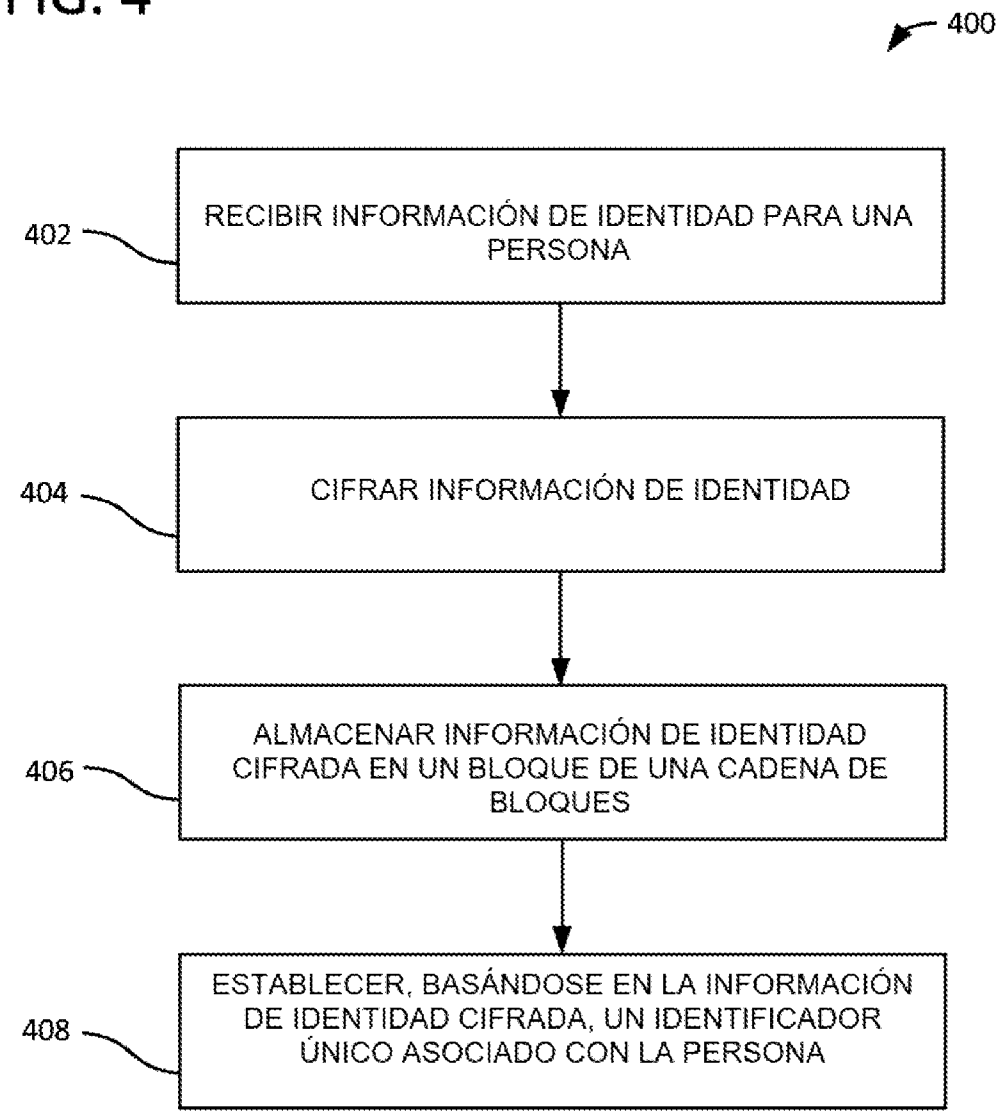

400
402
RECIBIR INFORMACIÓN DE IDENTIDAD PARA UNA PERSONA
404
CIFRAR INFORMACIÓN DE IDENTIDAD
406
ALMACENAR INFORMACIÓN DE IDENTIDAD CIFRADA EN UN BLOQUE DE UNA CADENA DE BLOQUES
408
ESTABLECER, BASÁNDOSE EN LA INFORMACIÓN DE IDENTIDAD CIFRADA, UN IDENTIFICADOR ÚNICO ASOCIADO CON LA PERSONA

FIG. 5

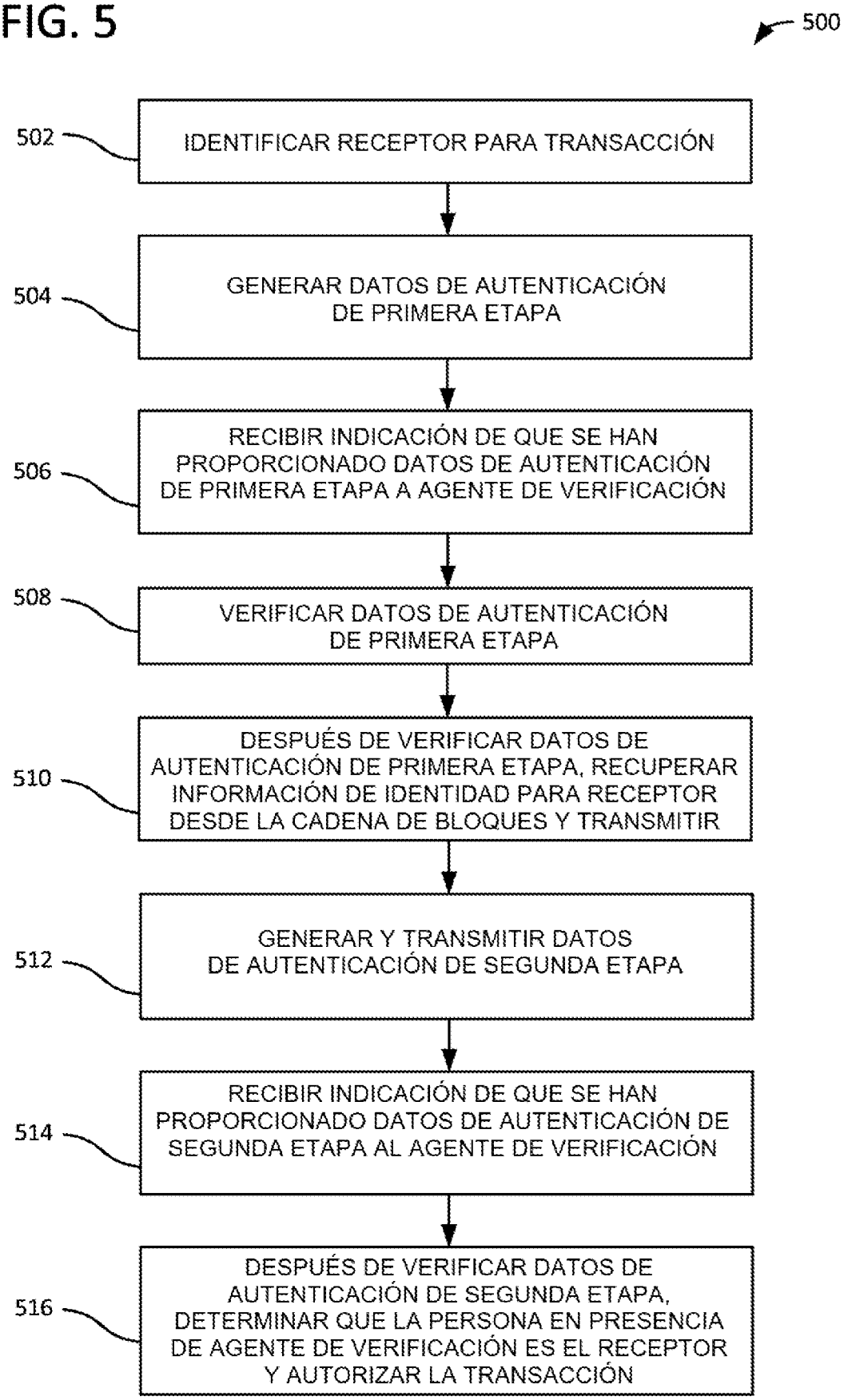

500
502
IDENTIFICAR RECEPTOR PARA TRANSACCIÓN
504
GENERAR DATOS DE AUTENTICACIÓN DE PRIMERA ETAPA
506
RECIBIR INDICACIÓN DE QUE SE HAN PROPORCIONADO DATOS DE AUTENTICACIÓN DE PRIMERA ETAPA A AGENTE DE VERIFICACIÓN
508
VERIFICAR DATOS DE AUTENTICACIÓN DE PRIMERA ETAPA
510
DESPUÉS DE VERIFICAR DATOS DE AUTENTICACIÓN DE PRIMERA ETAPA, RECUPERAR INFORMACIÓN DE IDENTIDAD PARA RECEPTOR DESDE LA CADENA DE BLOQUES Y TRANSMITIR
512
GENERAR Y TRANSMITIR DATOS DE AUTENTICACIÓN DE SEGUNDA ETAPA
514
RECIBIR INDICACIÓN DE QUE SE HAN PROPORCIONADO DATOS DE AUTENTICACIÓN DE SEGUNDA ETAPA AL AGENTE DE VERIFICACIÓN
516
DESPUÉS DE VERIFICAR DATOS DE AUTENTICACIÓN DE SEGUNDA ETAPA, DETERMINAR QUE LA PERSONA EN PRESENCIA DE AGENTE DE VERIFICACIÓN ES EL RECEPTOR Y AUTORIZAR LA TRANSACCIÓN

FIG. 6

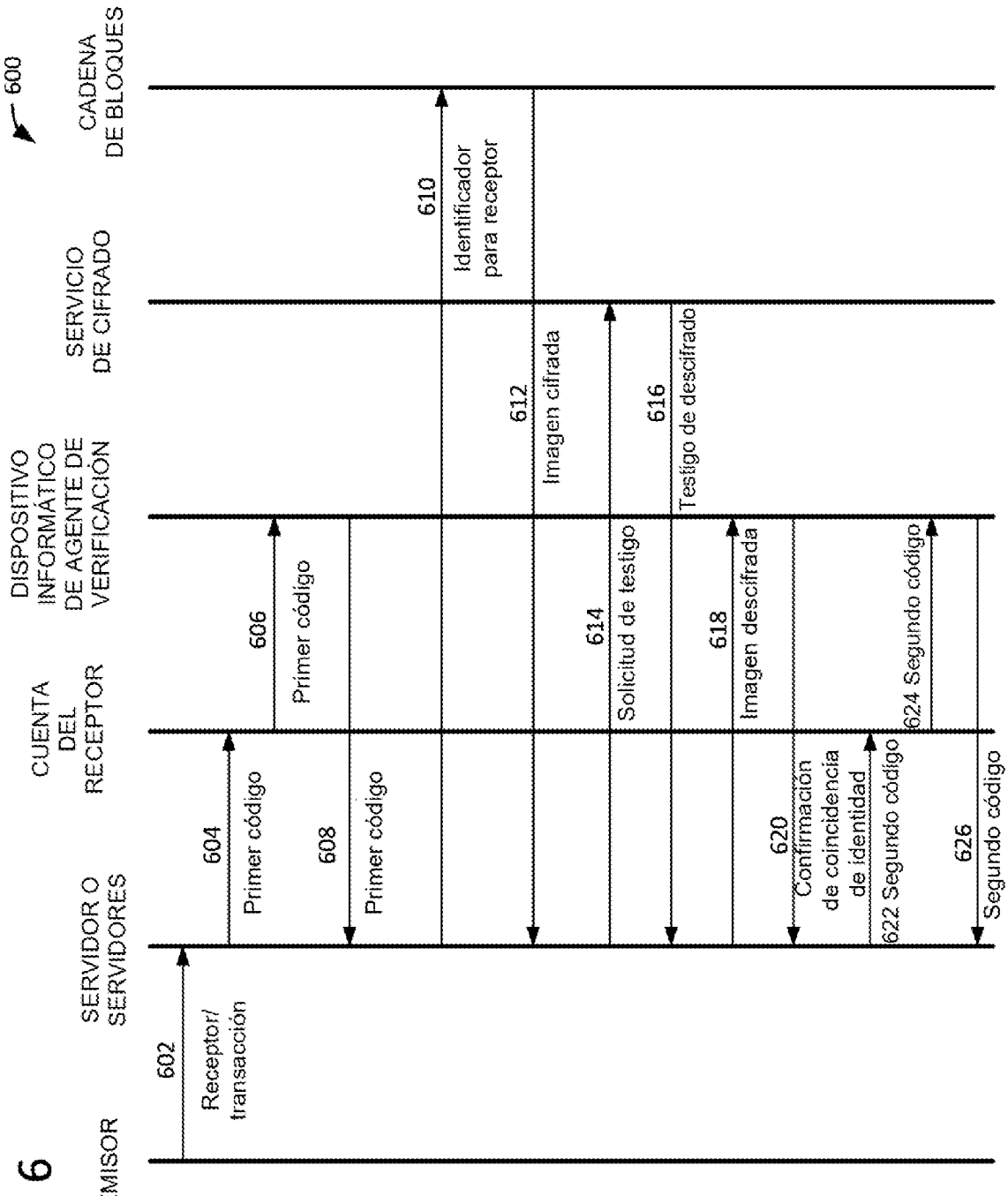

600
EMISOR
SERVIDOR O SERVIDORES
CUENTA DEL RECEPTOR
DISPOSITIVO INFORMÁTICO DE AGENTE DE VERIFICACIÓN
SERVICIO DE CIFRADO
CADENA DE BLOQUES
602
Receptor/ transacción
604
Primer código
606
Primer código
608
Primer código
610
Identificador para receptor
612
Imagen cifrada
614
Solicitud de testigo
616
Testigo de descifrado
618
Imagen descifrada
620
Confirmación de coincidencia de identidad
622 Segundo código
624 Segundo código
626
Segundo código

FIG. 7

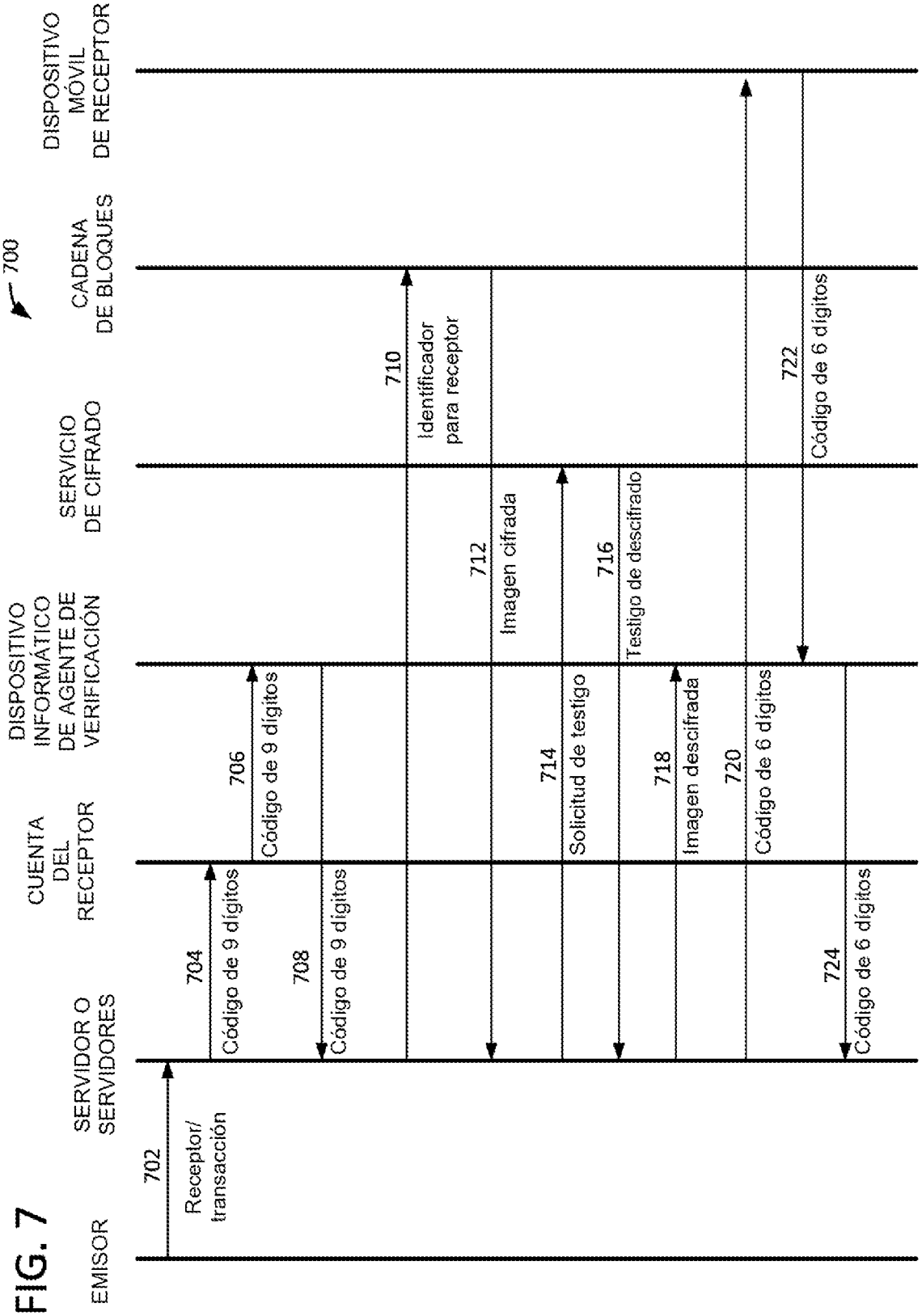

700
EMISOR
SERVIDOR O SERVIDORES
CUENTA DEL RECEPTOR
DISPOSITIVO INFORMÁTICO DE AGENTE DE VERIFICACIÓN
SERVICIO DE CIFRADO
CADENA DE BLOQUES
DISPOSITIVO MÓVIL DE RECEPTOR
702
Receptor/ transacción
704
Código de 9 dígitos
706
Código de 9 dígitos
708
Código de 9 dígitos
710
Identificador para receptor
712
Imagen cifrada
714
Solicitud de testigo
716
Testigo de descifrado
718
Imagen descifrada
720
Código de 6 dígitos
722
Código de 6 dígitos
724
Código de 6 dígitos

FIG. 8

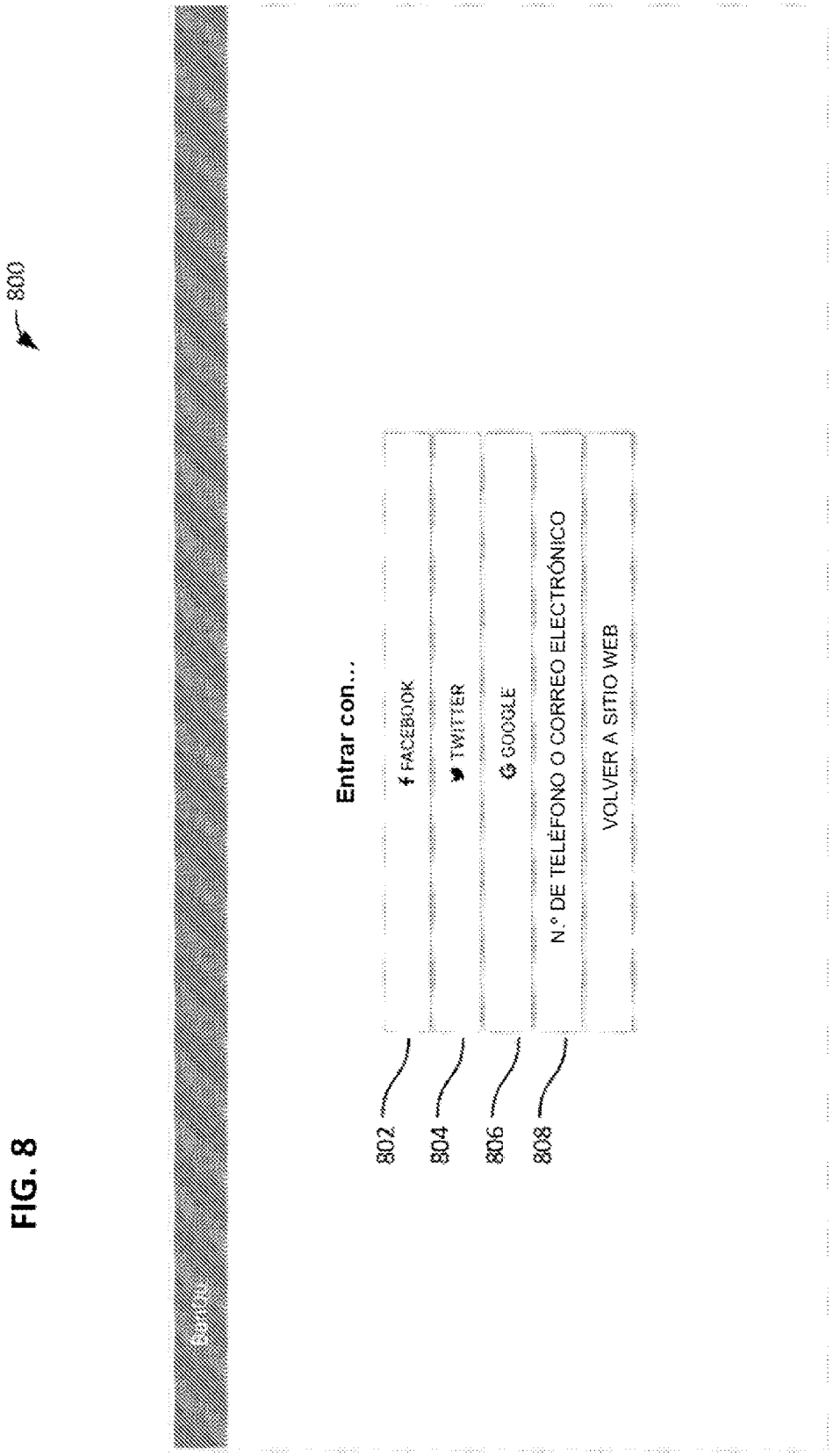

800
Entrar con...
FACEBOOK
TWITTER
GOOGLE
N.º DE TELÉFONO O CORREO ELECTRÓNICO
VOLVER A SITIO WEB
802
804
806
808

FIG. 9

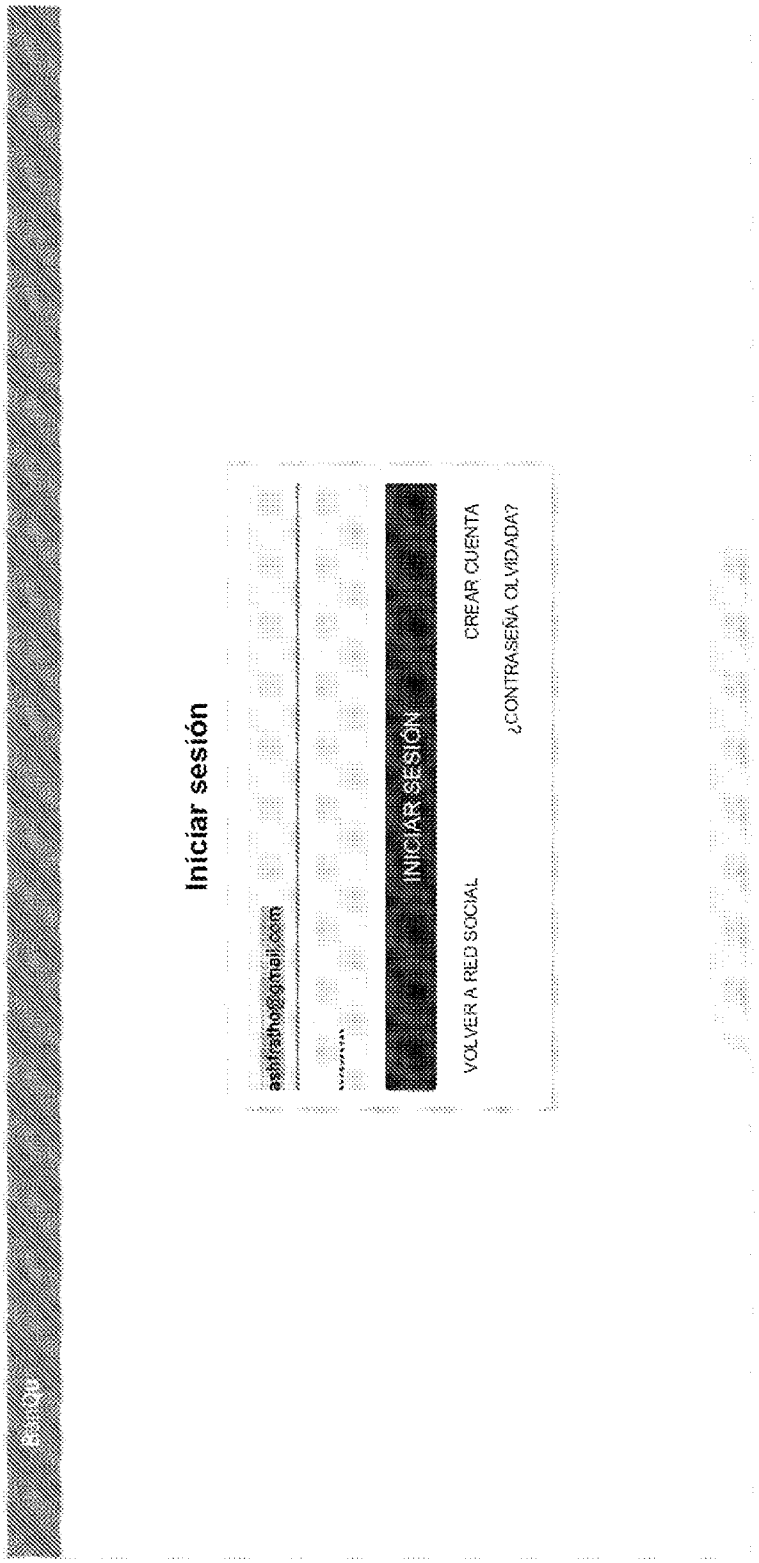

900
Iniciar sesión
INICIAR SESIÓN
CREAR CUENTA
VOLVER A RED SOCIAL
¿CONTRASEÑA OLVIDADA?

FIG. 10

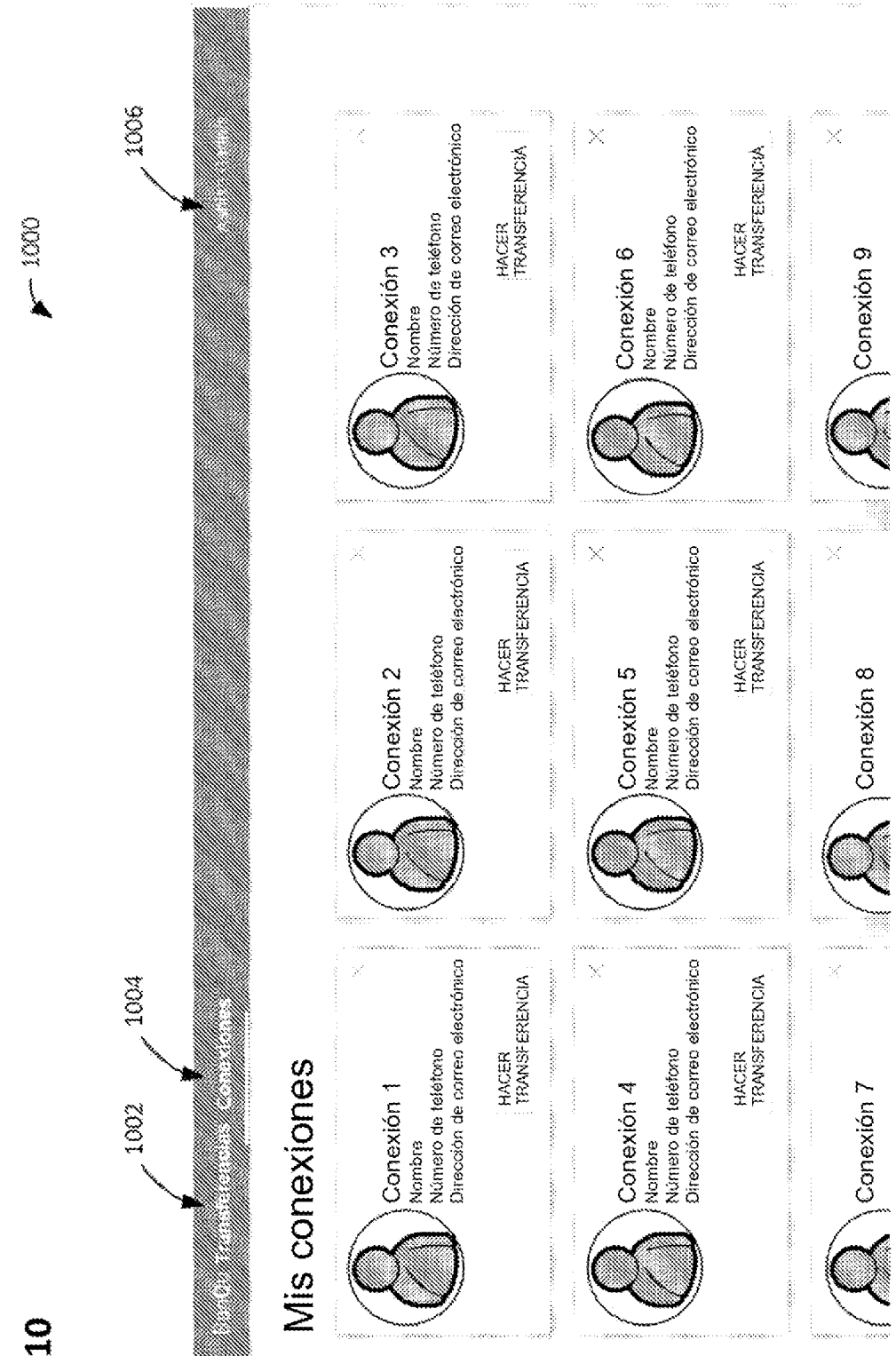

1000
1002
1004
1006
Mis conexiones
Conexión 1
Nombre
Número de teléfono
Dirección de correo electrónico
HACER TRANSFERENCIA
Conexión 2
Nombre
Número de teléfono
Dirección de correo electrónico
HACER TRANSFERENCIA
Conexión 3
Nombre
Número de teléfono
Dirección de correo electrónico
HACER TRANSFERENCIA
Conexión 4
Nombre
Número de teléfono
Dirección de correo electrónico
HACER TRANSFERENCIA
Conexión 5
Nombre
Número de teléfono
Dirección de correo electrónico
HACER TRANSFERENCIA
Conexión 6
Nombre
Número de teléfono
Dirección de correo electrónico
HACER TRANSFERENCIA
Conexión 7
Conexión 8
Conexión 9

FIG. 11

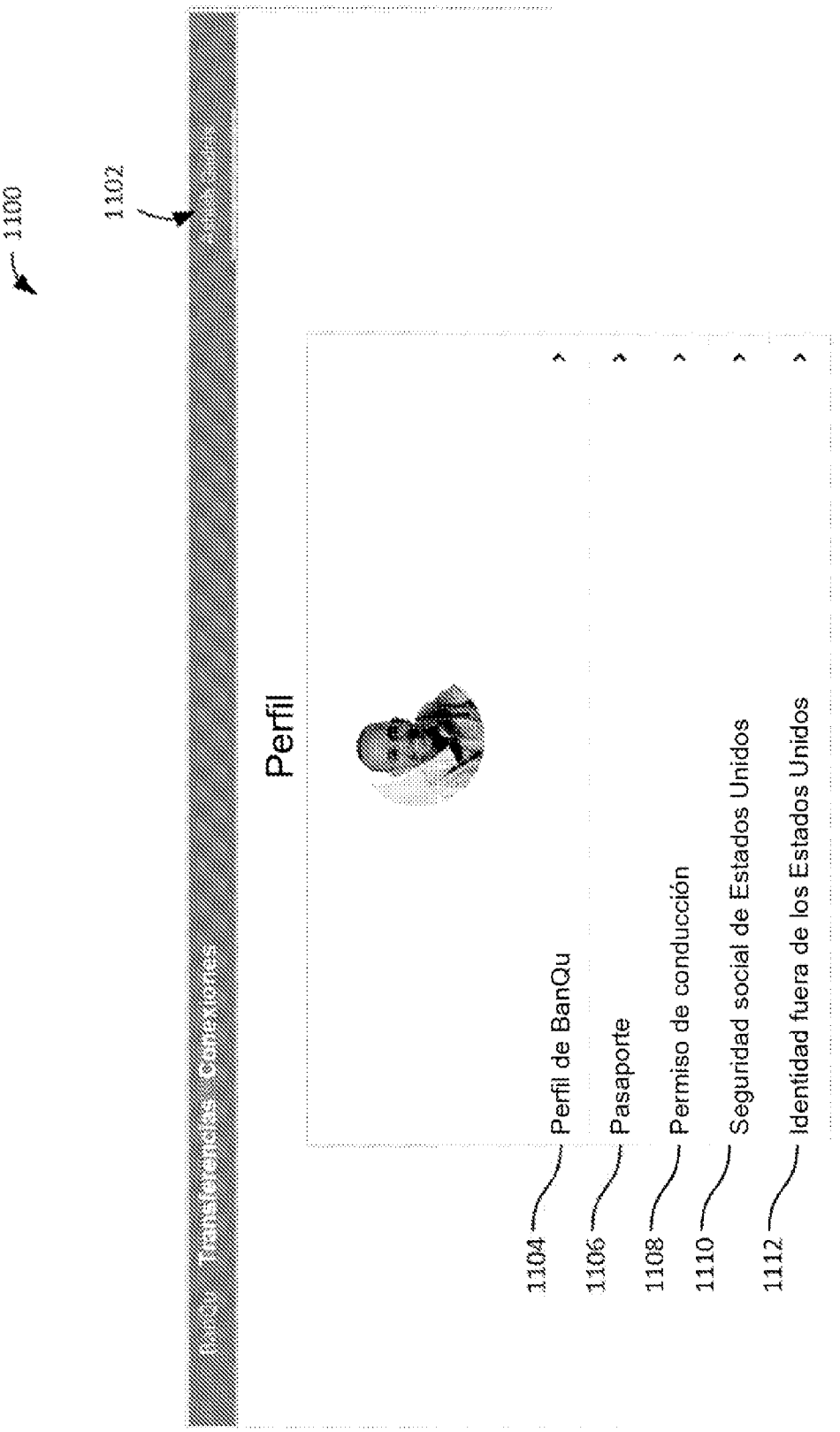

1100
1102
Perfil
Perfil de BanQu
Pasaporte
Permiso de conducción
Seguridad social de Estados Unidos
Identidad fuera de los Estados Unidos
1104
1106
1108
1110
1112

FIG. 12

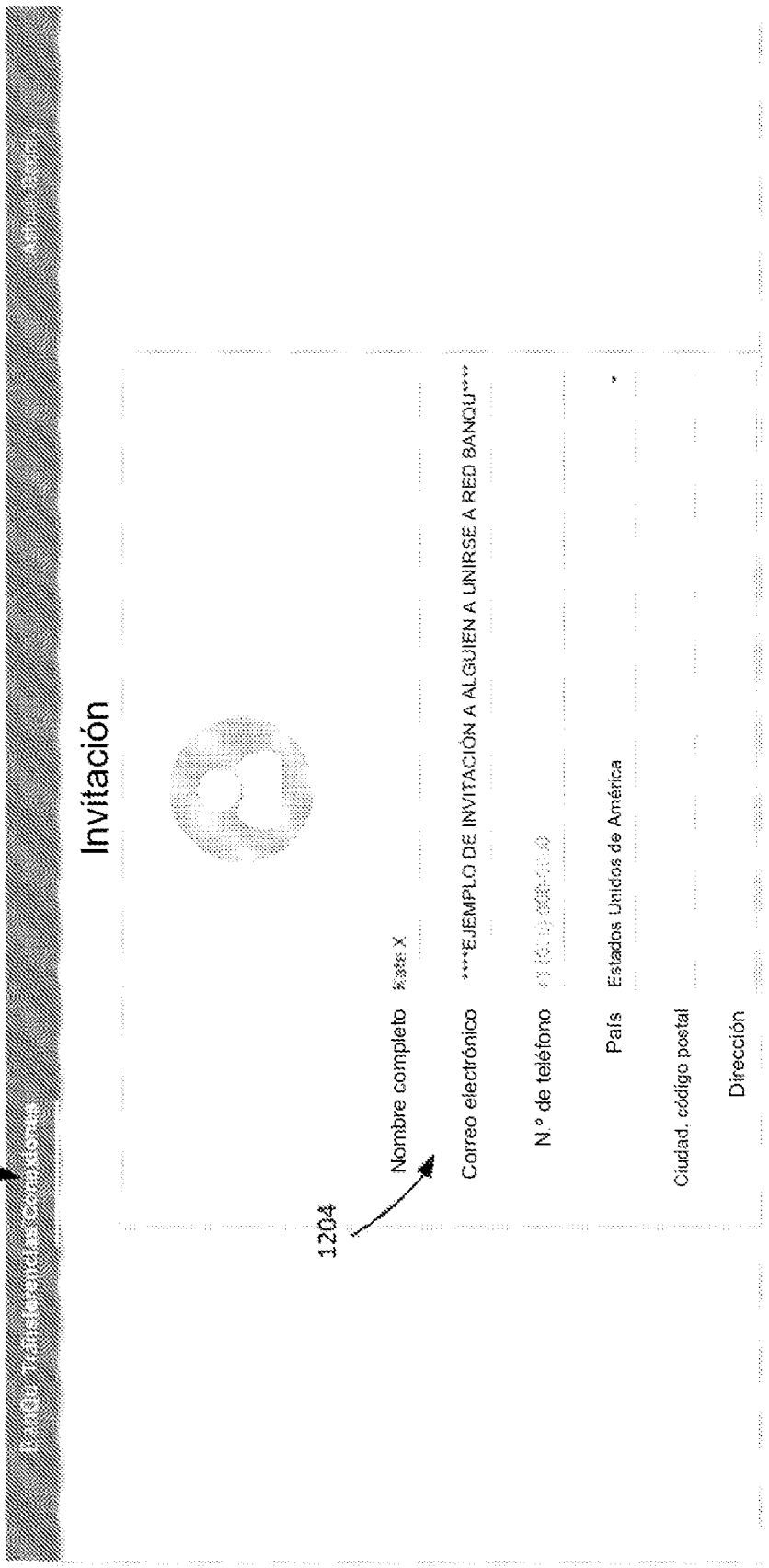

1200
1202
1204
Invitación
Nombre completo
Correo electrónico
EJEMPLO DE INVITACIÓN A ALGUIEN A UNIRSE A RED BANQU
N.º de teléfono
País
Estados Unidos de América
Ciudad, código postal
Dirección

FIG. 13

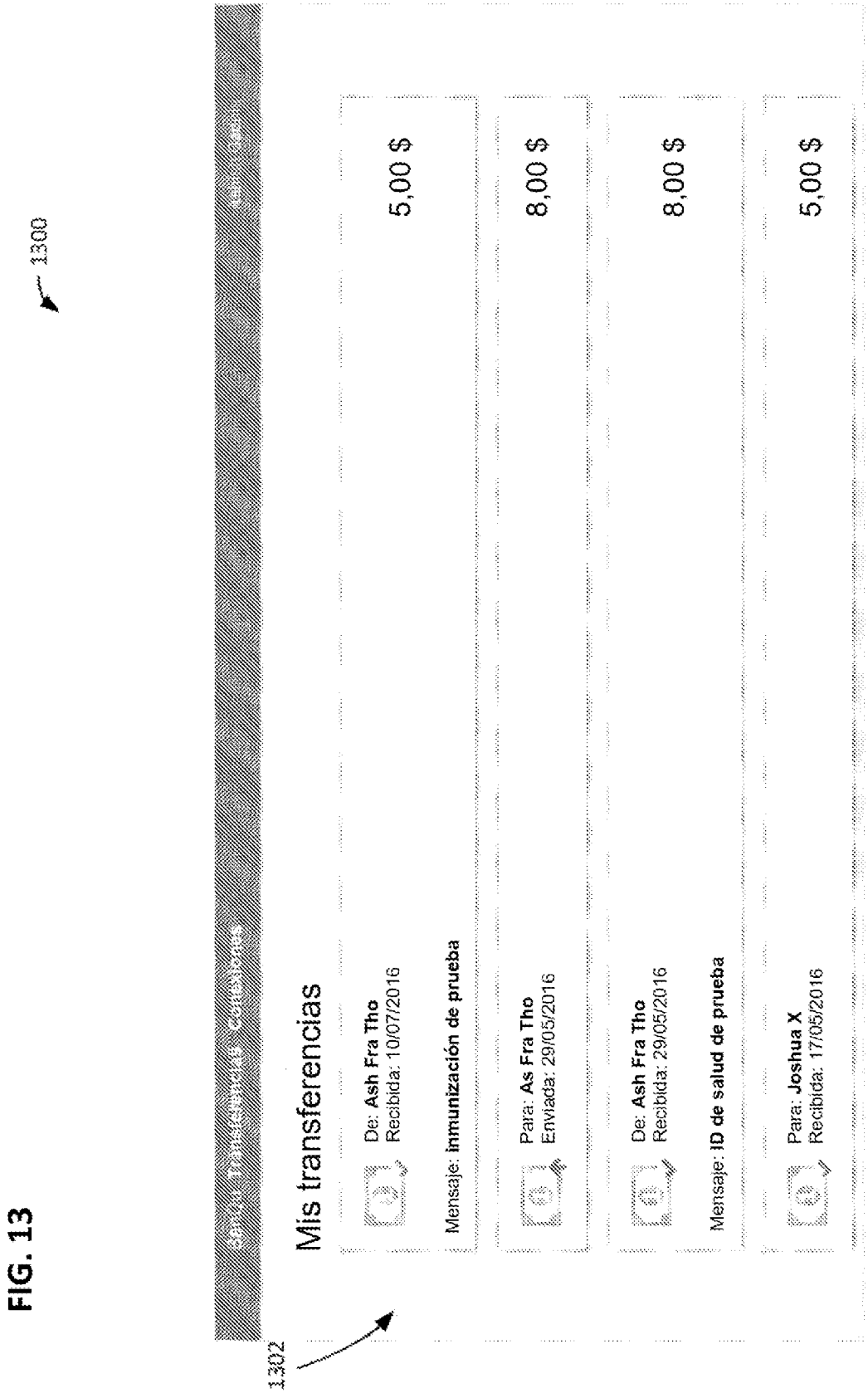

1300
1302
Mis transferencias
De: Ash Fra Tho
Recibida: 10/07/2016
5,00 $
Mensaje: inmunización de prueba
Para: As Fra Tho
Enviada: 29/05/2016
8,00 $
De: Ash Fra Tho
Recibida: 29/05/2016
8,00 $
Mensaje: ID de salud de prueba
Para: Joshua X
Recibida: 17/05/2016
5,00 $

FIG. 14

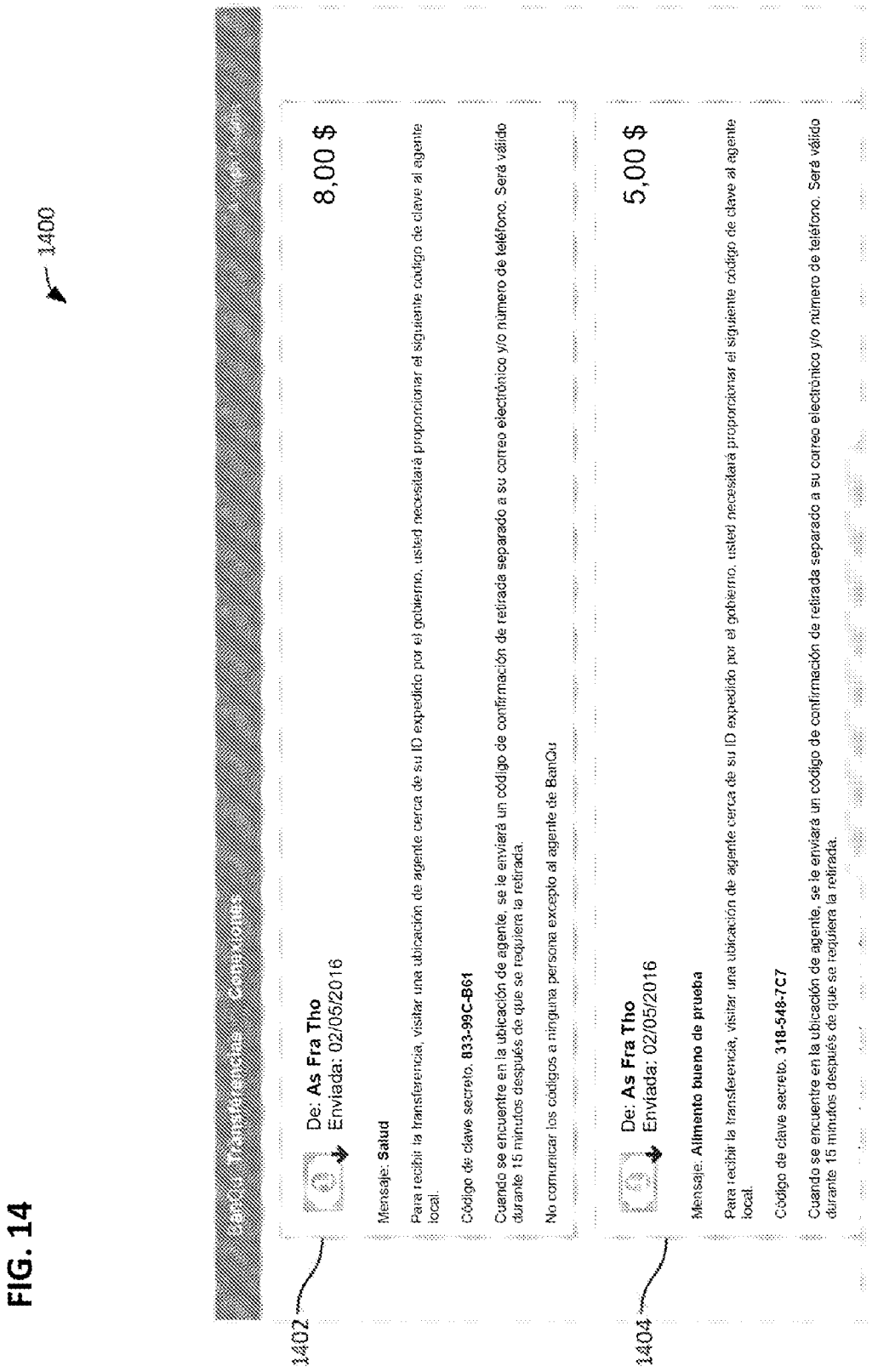

1400
Cerca Transferencia
1402
De: As Fra Tho
Enviada: 02/05/2016
8,00 $
Mensaje: Salud
Para recibir la transferencia, visitar una ubicación de agente cerca de su ID expedido por el gobierno, usted necesitará proporcionar el siguiente código de clave al agente local.
Código de clave secreto. 833-99C-B61
Cuando se encuentre en la ubicación de agente, se le enviará un código de confirmación de retirada separado a su correo electrónico y/o número de teléfono. Será válido durante 15 minutos después de que se requiera la retirada.
No comunicar los códigos a ninguna persona excepto al agente de BanQu
1404
De: As Fra Tho
Enviada: 02/05/2016
5,00 $
Mensaje: Alimento bueno de prueba
Para recibir la transferencia, visitar una ubicación de agente cerca de su ID expedido por el gobierno, usted necesitará proporcionar el siguiente código de clave al agente local.
Código de clave secreto. 318-548-7C7
Cuando se encuentre en la ubicación de agente, se le enviará un código de confirmación de retirada separado a su correo electrónico y/o número de teléfono. Será válido durante 15 minutos después de que se requiera la retirada.

FIG. 15

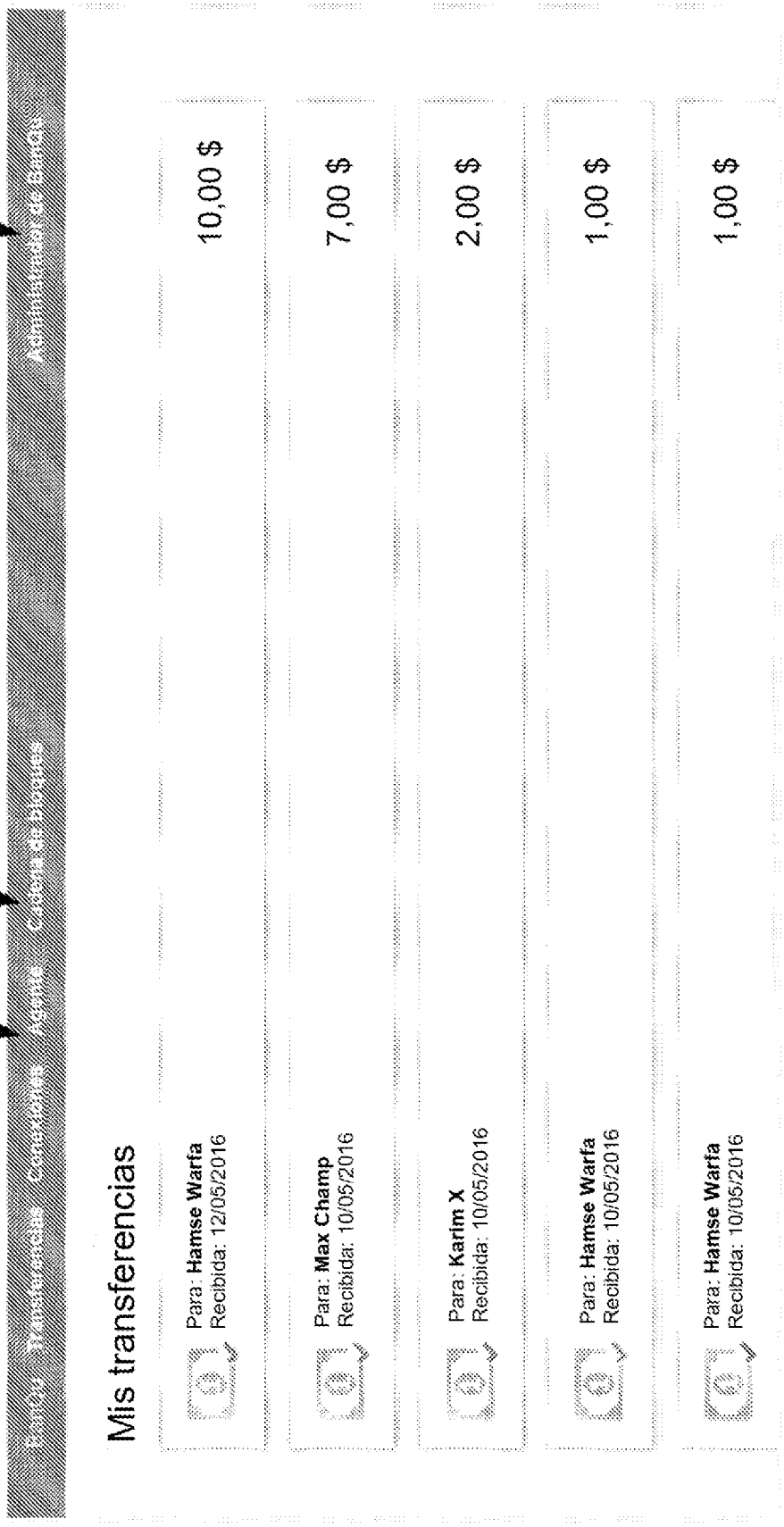

1500
1502
1504
1506
Administrador de cuentas
Cuentas de clientes
Agente
Contabilidad
Transacciones
Panel
Mis transferencias
Para: Hamse Warfa
Recibida: 12/05/2016
10,00 $
Para: Max Champ
Recibida: 10/05/2016
7,00 $
Para: Karim X
Recibida: 10/05/2016
2,00 $
Para: Hamse Warfa
Recibida: 10/05/2016
1,00 $
Para: Hamse Warfa
Recibida: 10/05/2016
1,00 $

FIG. 16

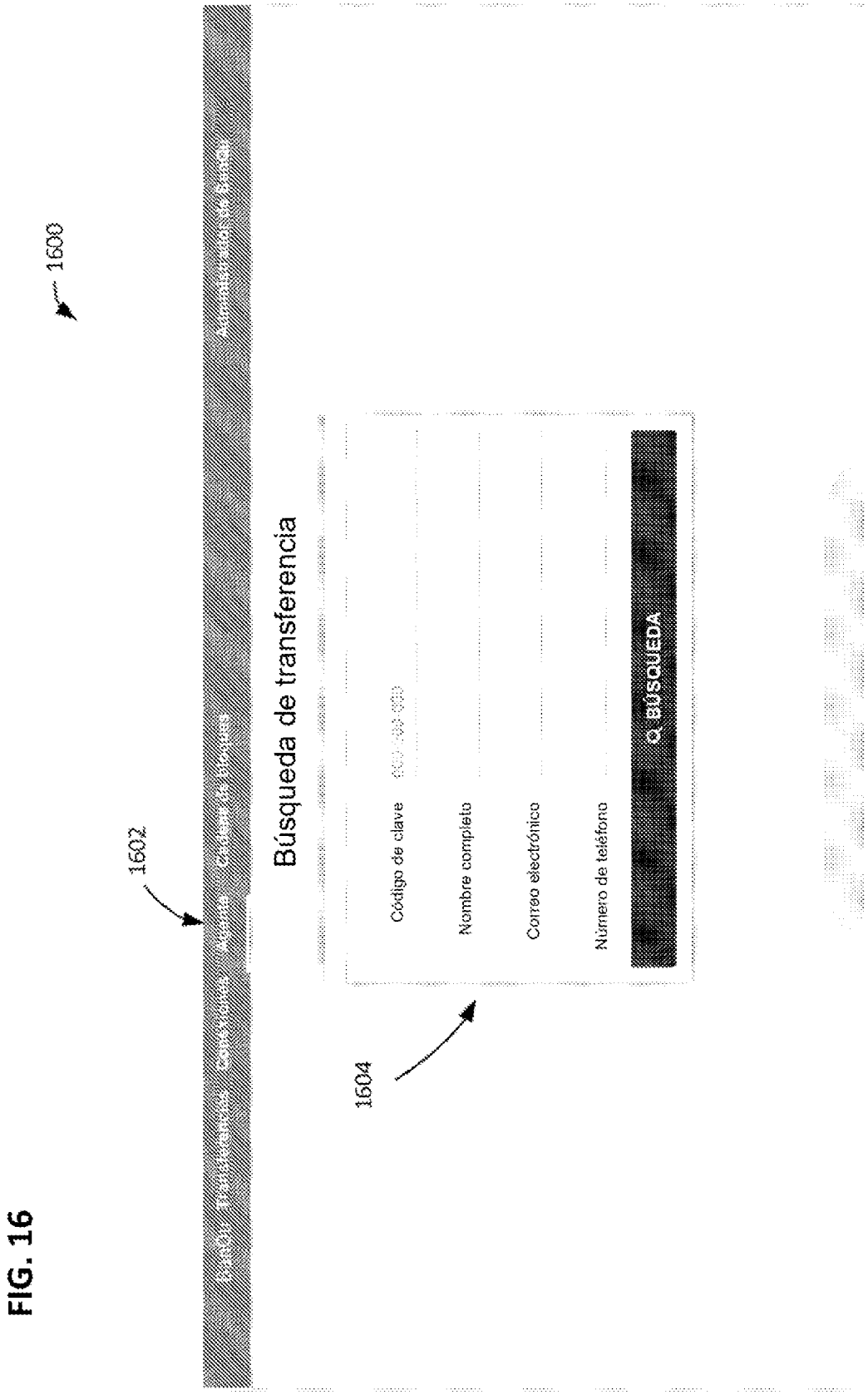

1600
1602
1604
Búsqueda de transferencia
Código de clave
Nombre completo
Correo electrónico
Número de teléfono
BÚSQUEDA

FIG. 17

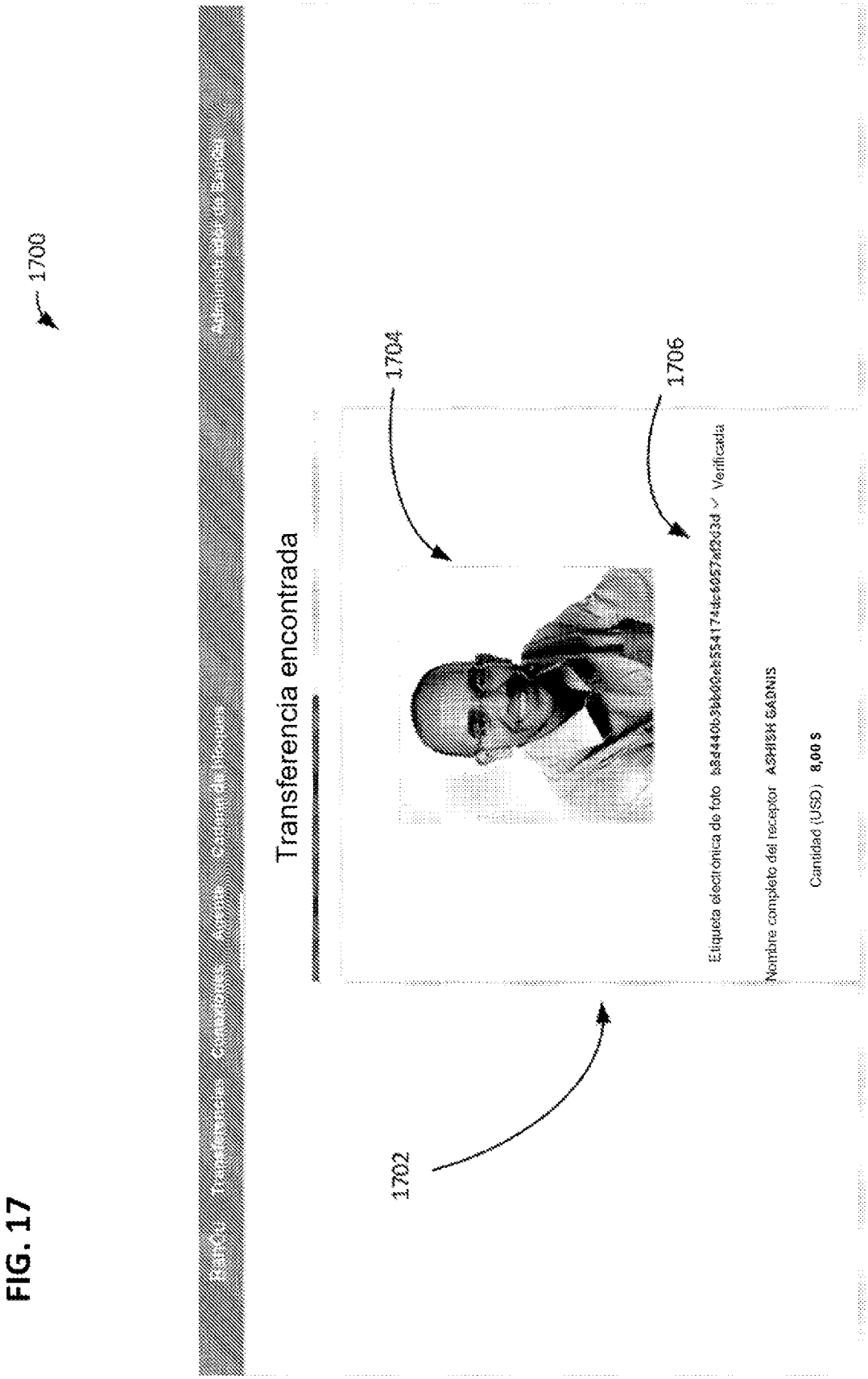

1700
Transferencias
Cuentas
Ayuda
Cerrar sesión
Administrador del Banco
Transferencia encontrada
1702
1704
1706
Etiqueta electrónica de foto
Verificada
Nombre completo del receptor
ASHISH SADNIS
Cantidad (USD)
8,00 $

FIG. 18

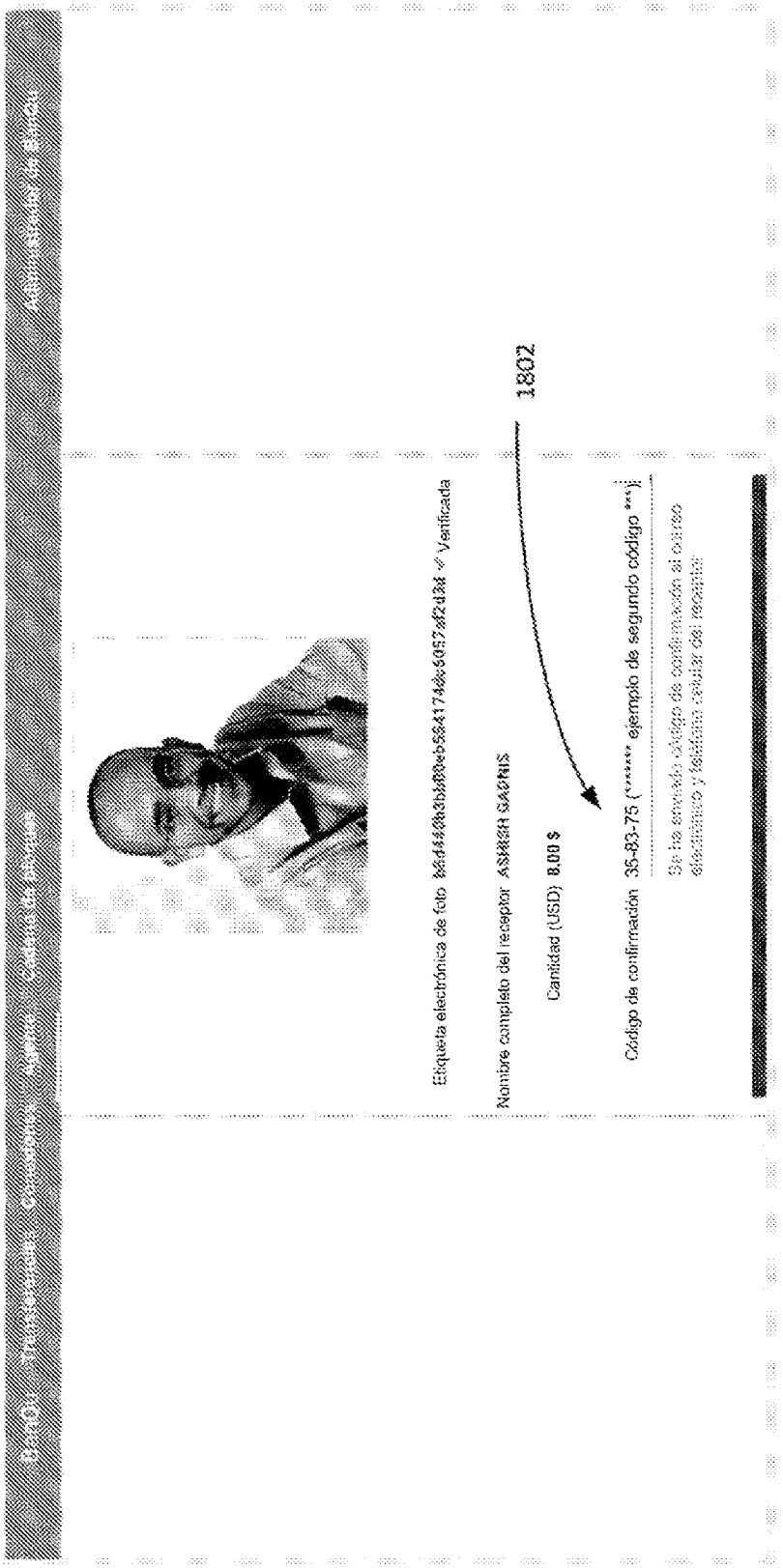

1800
1802
Etiqueta electrónica de foto
Verificada
Nombre completo del receptor
Cantidad (USD) 8.00 $
Código de confirmación 35-83-75 (****** ejemplo de segundo código ***)

FIG. 19

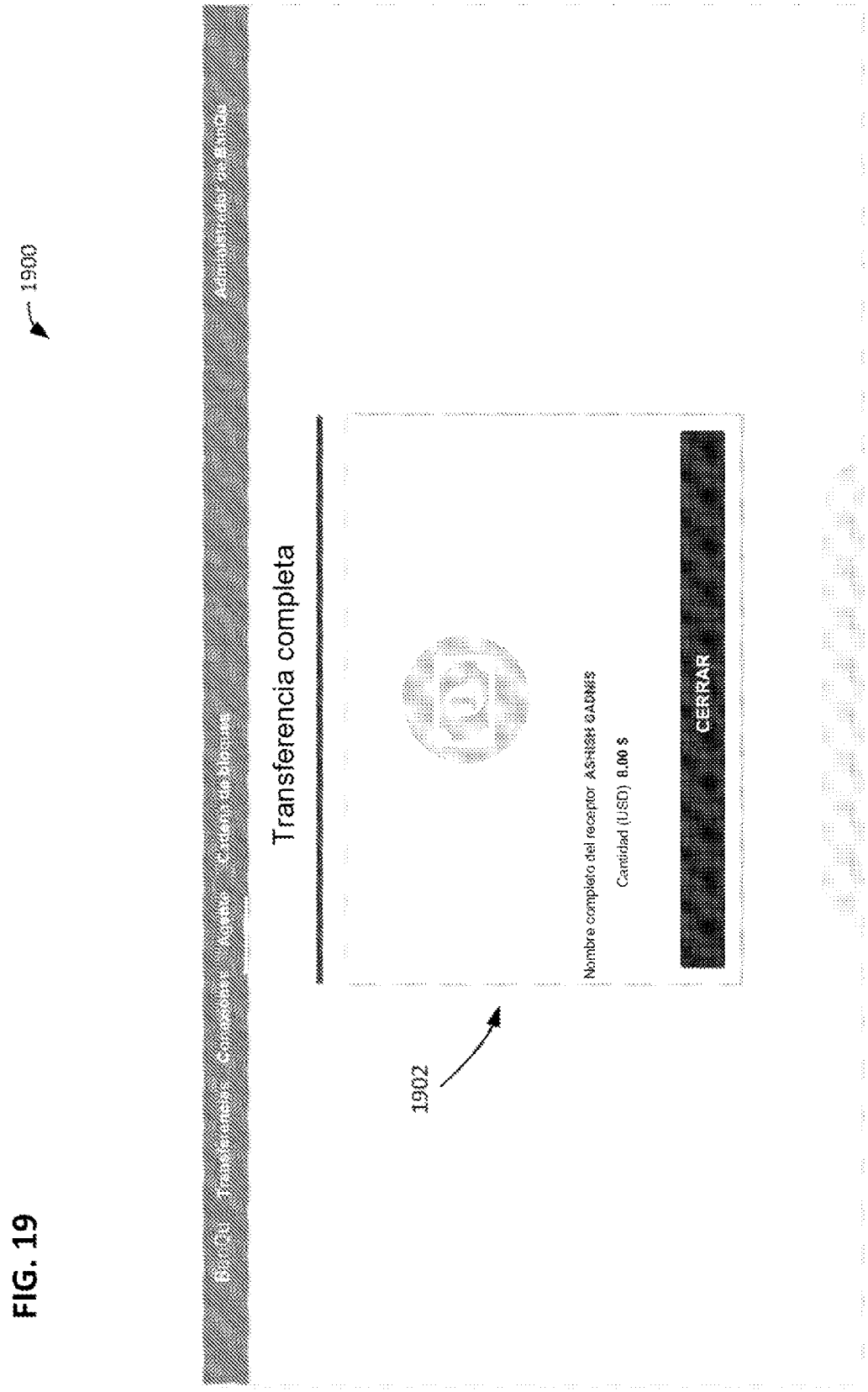

1900
Transferencia completa
1902
Nombre completo del receptor
Cantidad (USD) 8.00 $
CERRAR

FIG. 20

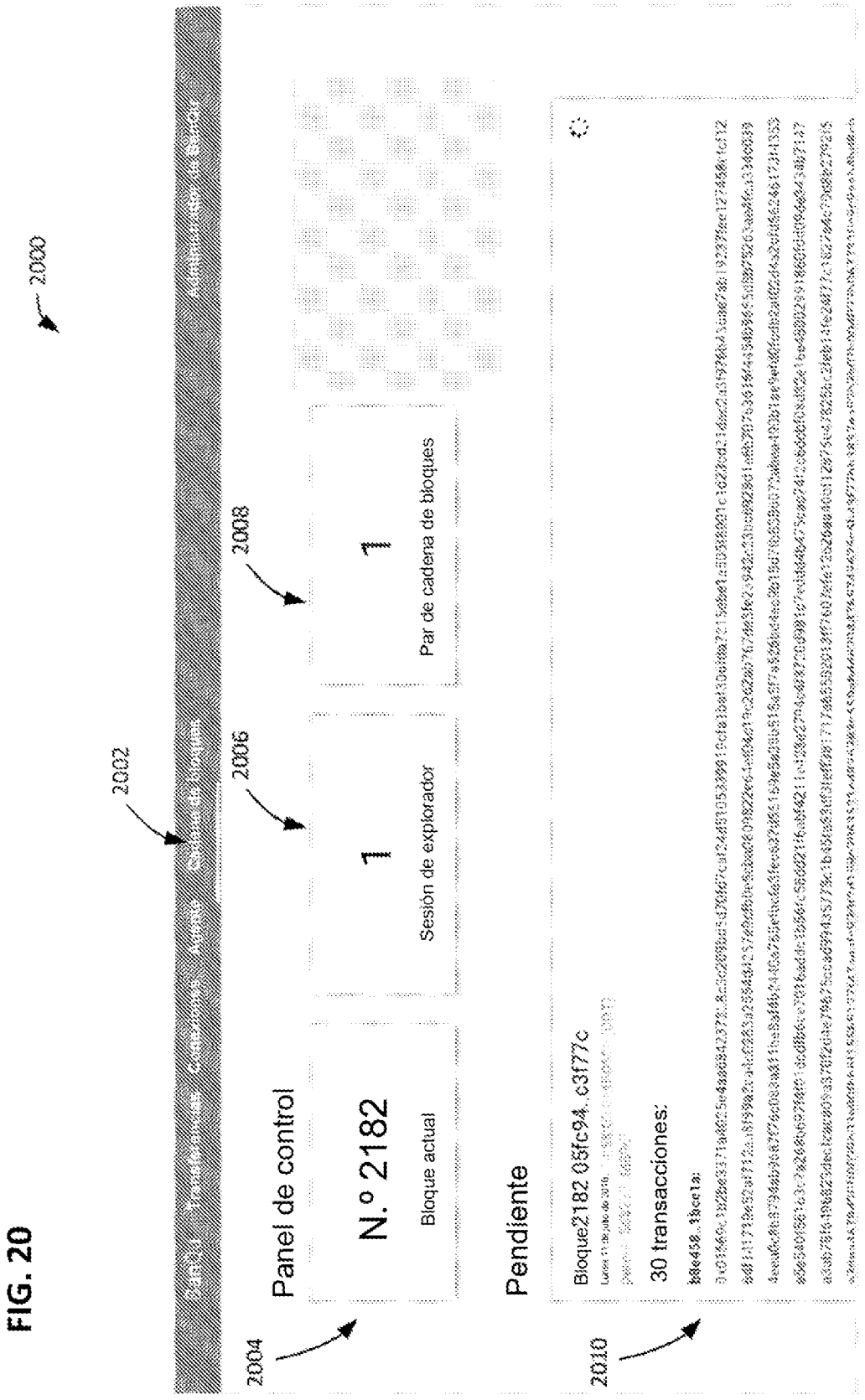

2000
2002
2004
2006
2008
2010
Panel de control
N.º 2182
Bloque actual
1
Sesión de explorador
1
Par de cadena de bloques
Pendiente
Bloque2182 05fc94..c3177c
30 transacciones:

FIG. 21

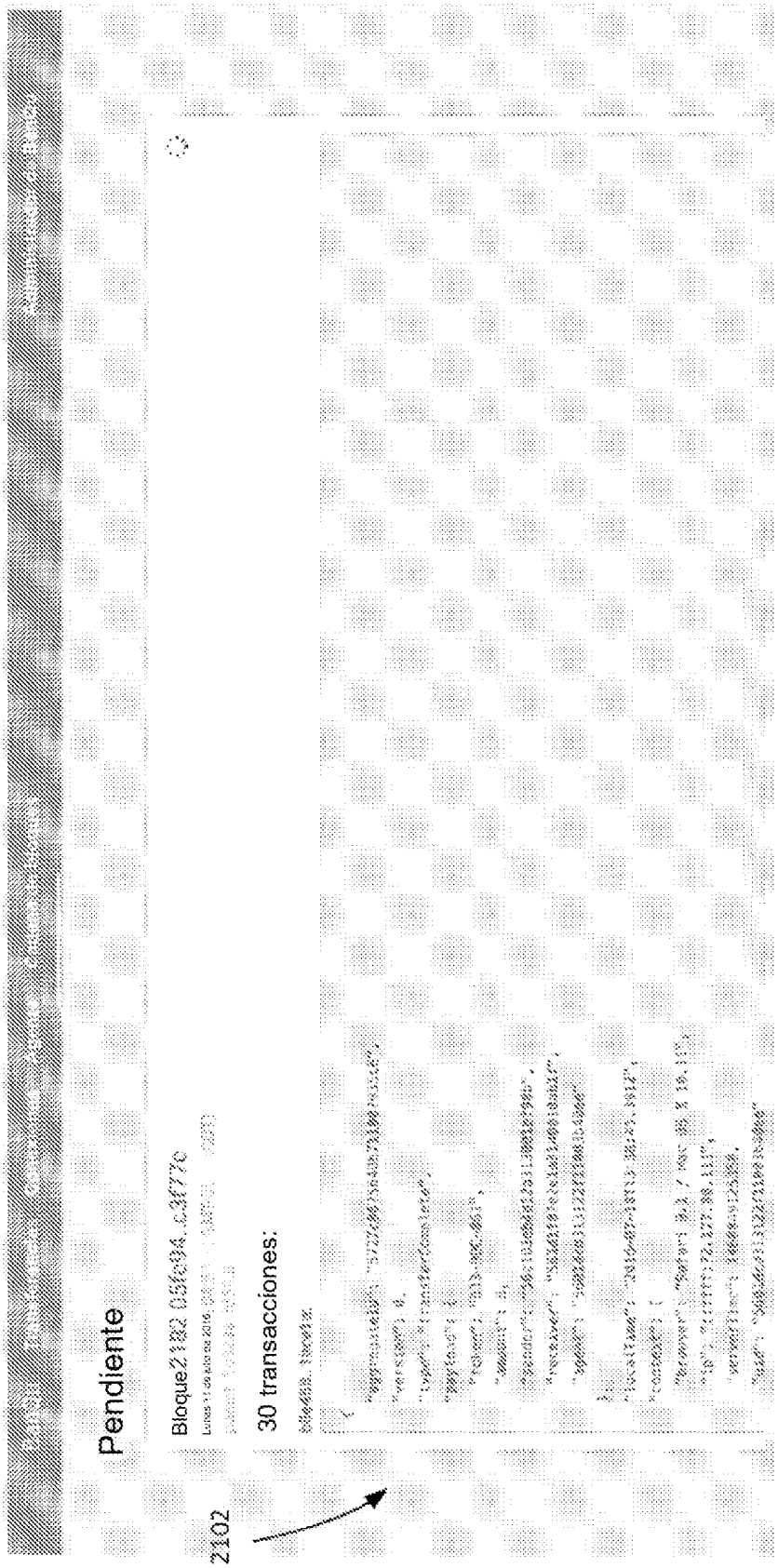

2100
Pendiente
Bloque2182 05fc94..c3f77c
30 transacciones:
2102

FIG. 22

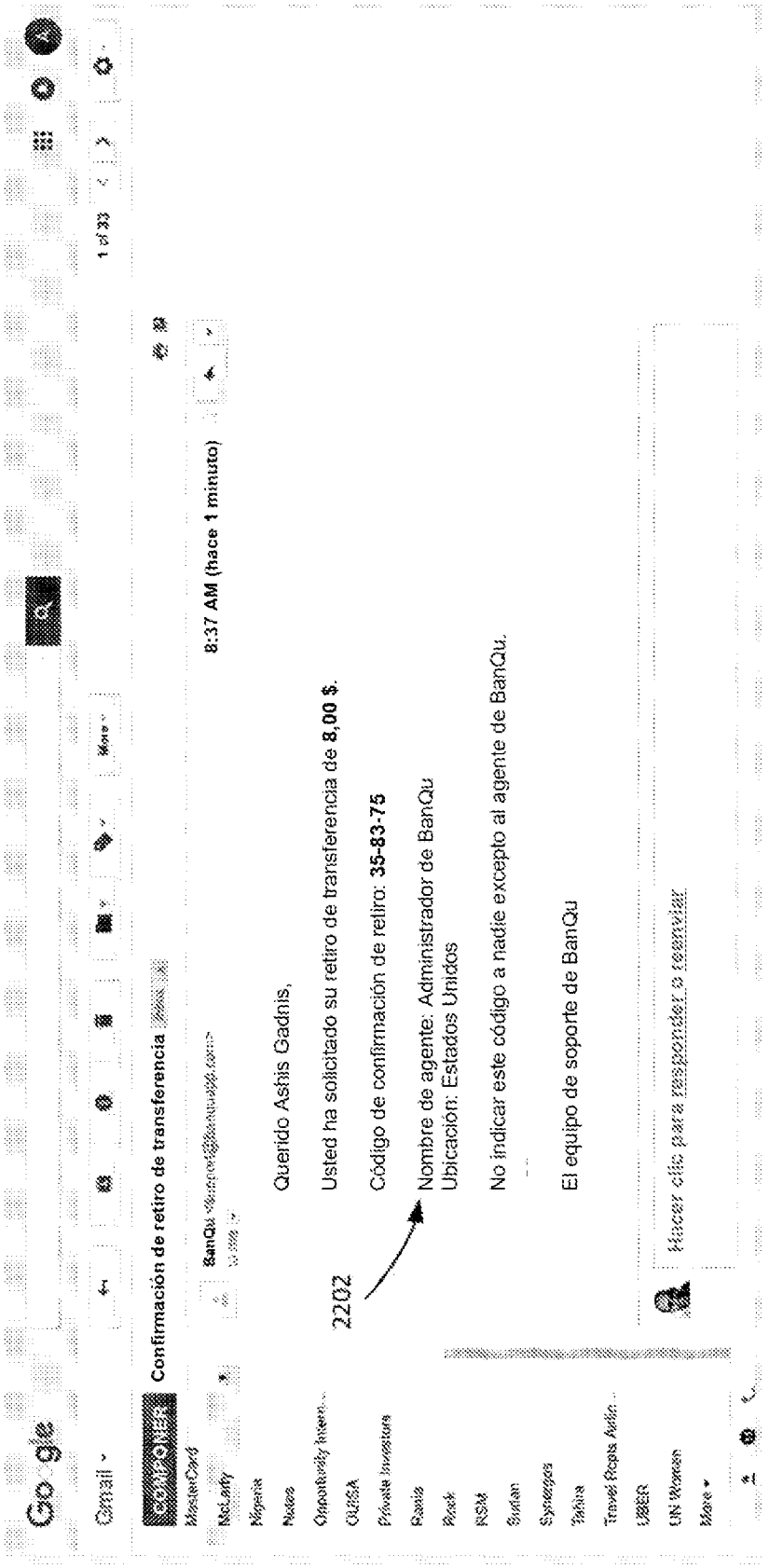

2200
Google
Gmail
Confirmación de retiro de transferencia
8:37 AM (hace 1 minuto)
Querido Ashis Gadnis,
Usted ha solicitado su retiro de transferencia de 8,00 $.
Código de confirmación de retiro: 35-83-75
2202
Nombre de agente: Administrador de BanQu
Ubicación: Estados Unidos
No indicar este código a nadie excepto al agente de BanQu.
El equipo de soporte de BanQu
Hacer clic para responder o reenviar

FIG. 23

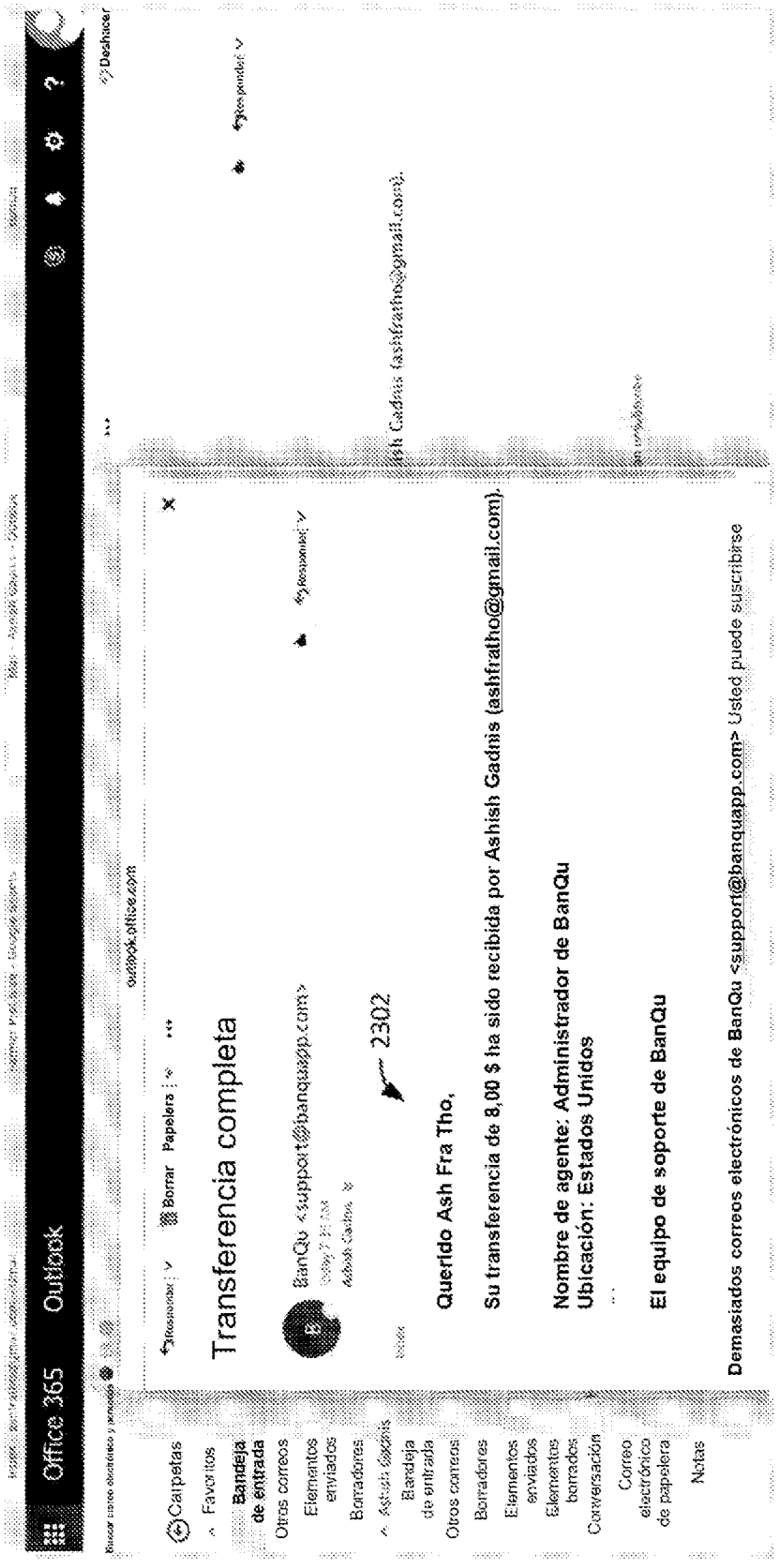

2300
Office 365
Outlook
Deshacer
Carpetas
Favoritos
Bandeja de entrada
Otros correos
Elementos enviados
Borradores
Ashish Gadnis
Bandeja de entrada
Otros correos
Borradores
Elementos enviados
Elementos borrados
Conversación
Correo electrónico de papelera
Notas
Borrar
Papelera
Responder
Transferencia completa
BanQu <support@banquapp.com>
2302
Querido Ash Fra Tho,
Su transferencia de 8,00 $ ha sido recibida por Ashish Gadnis (ashfratho@gmail.com).
Nombre de agente: Administrador de BanQu
Ubicación: Estados Unidos
El equipo de soporte de BanQu
Demasiados correos electrónicos de BanQu <support@banquapp.com> Usted puede suscribirse

FIG. 24

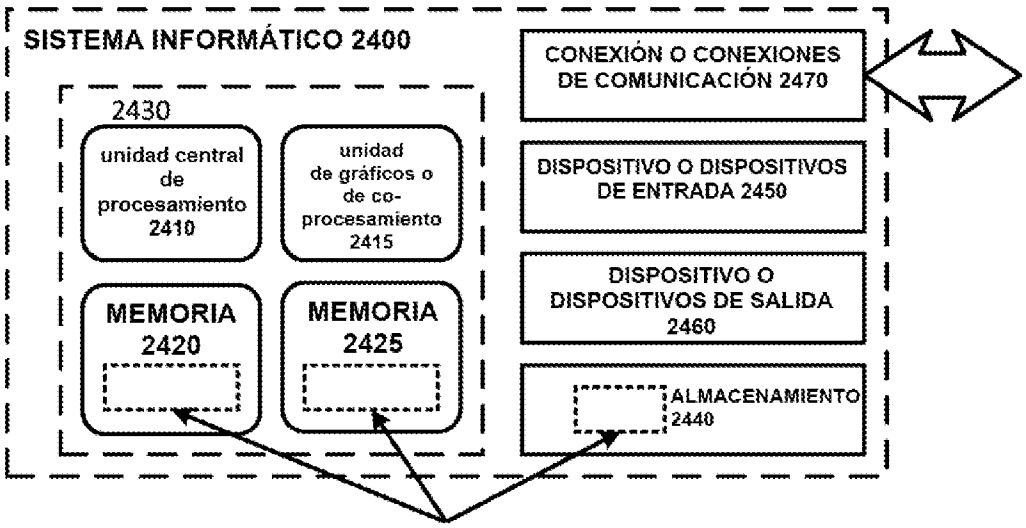

SISTEMA INFORMÁTICO 2400
2430
unidad central de procesamiento 2410
unidad de gráficos o de co-procesamiento 2415
MEMORIA 2420
MEMORIA 2425
CONEXIÓN O CONEXIONES DE COMUNICACIÓN 2470
DISPOSITIVO O DISPOSITIVOS DE ENTRADA 2450
DISPOSITIVO O DISPOSITIVOS DE SALIDA 2460
ALMACENAMIENTO 2440
SOFTWARE 2480 QUE IMPLEMENTA TECNOLOGÍAS DESCRITAS

FIG. 25

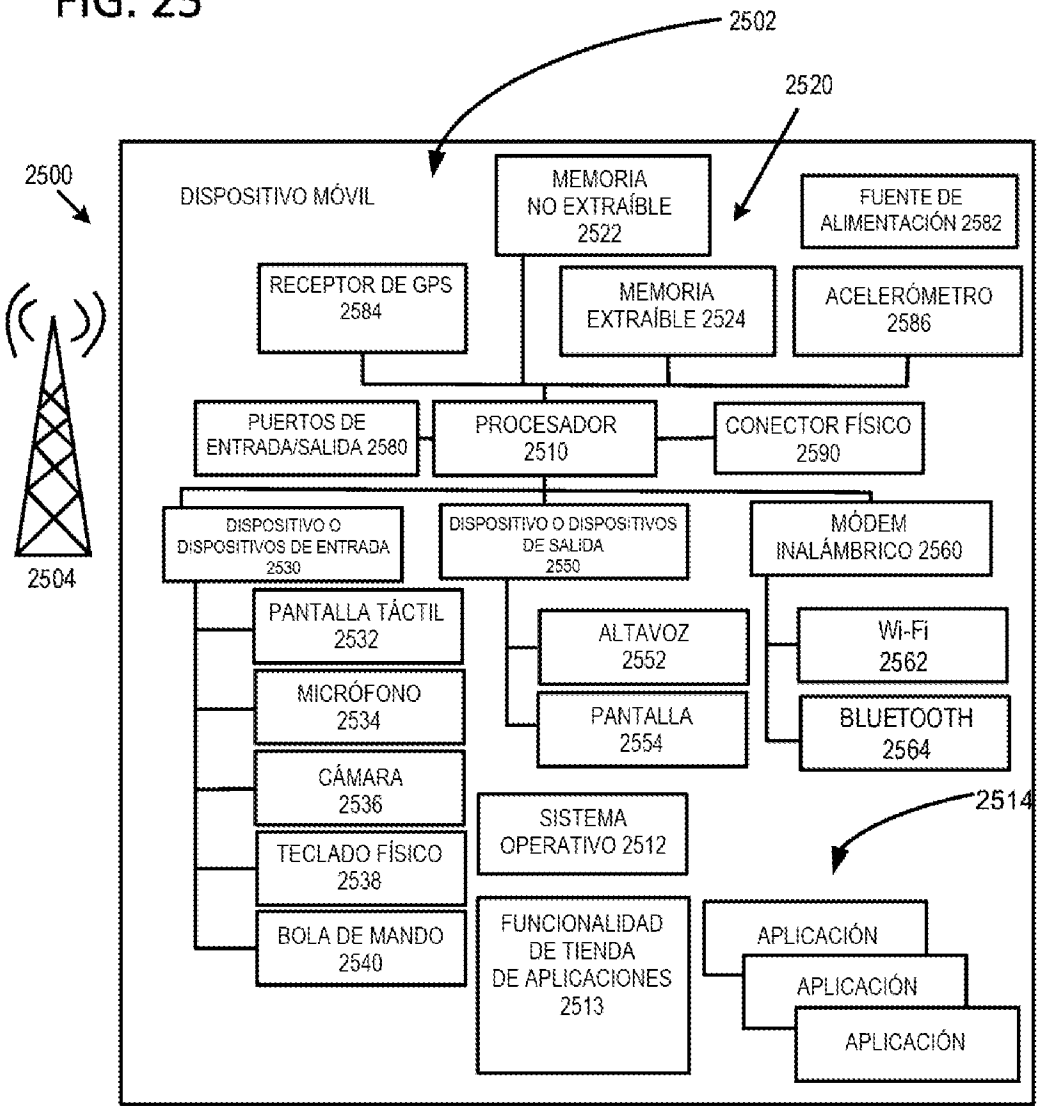

2502
2520
2500
DISPOSITIVO MÓVIL
MEMORIA NO EXTRAÍBLE 2522
FUENTE DE ALIMENTACIÓN 2582
RECEPTOR DE GPS 2584
MEMORIA EXTRAÍBLE 2524
ACELERÓMETRO 2586
PUERTOS DE ENTRADA/SALIDA 2580
PROCESADOR 2510
CONECTOR FÍSICO 2590
DISPOSITIVO O DISPOSITIVOS DE ENTRADA 2530
DISPOSITIVO O DISPOSITIVOS DE SALIDA 2550
MÓDEM INALÁMBRICO 2560
PANTALLA TÁCTIL 2532
ALTAVOZ 2552
Wi-Fi 2562
MICRÓFONO 2534
PANTALLA 2554
BLUETOOTH 2564
CÁMARA 2536
SISTEMA OPERATIVO 2512
2514
TECLADO FÍSICO 2538
BOLA DE MANDO 2540
FUNCIONALIDAD DE TIENDA DE APLICACIONES 2513
APLICACIÓN
APLICACIÓN
APLICACIÓN
2504

FIG. 26

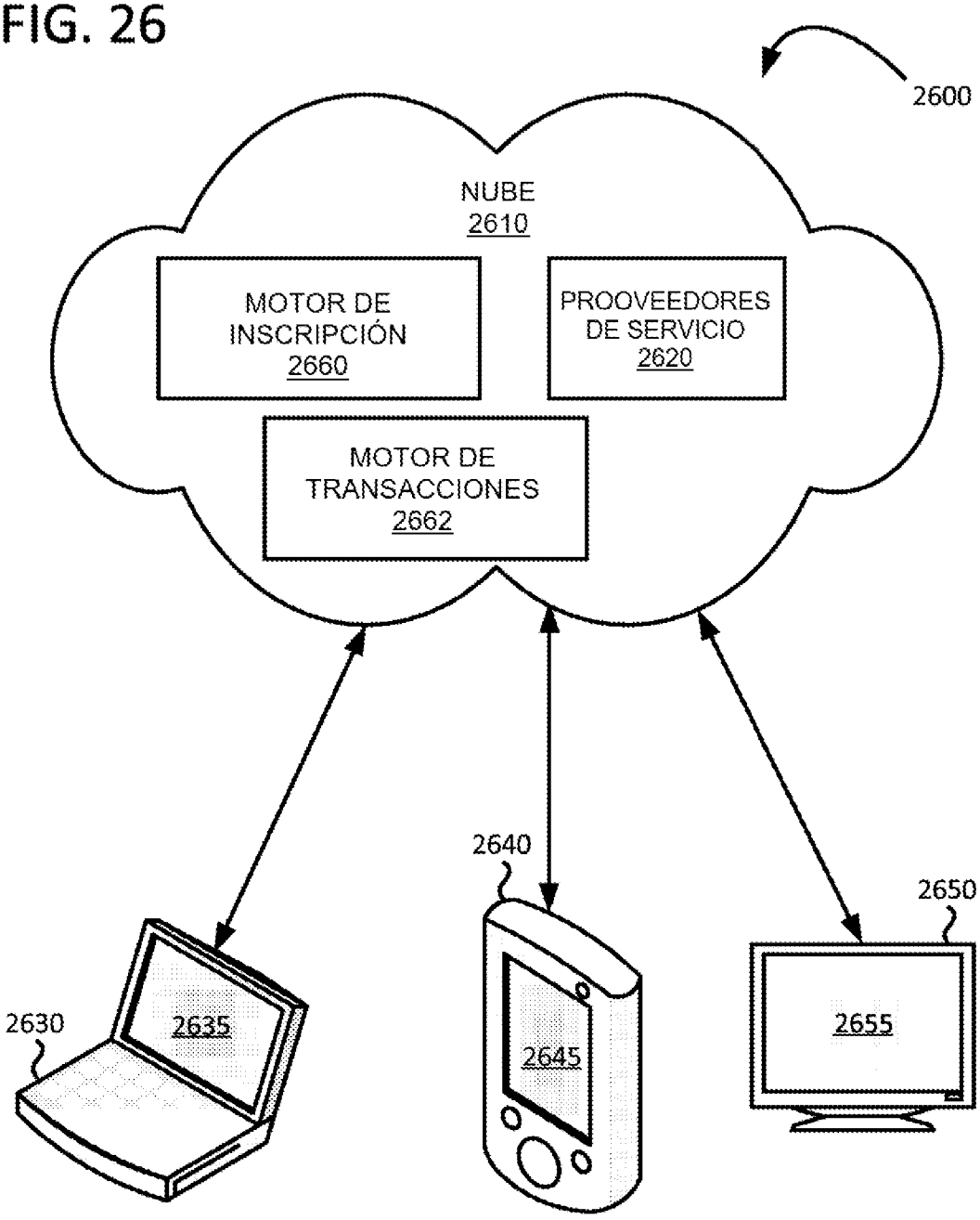
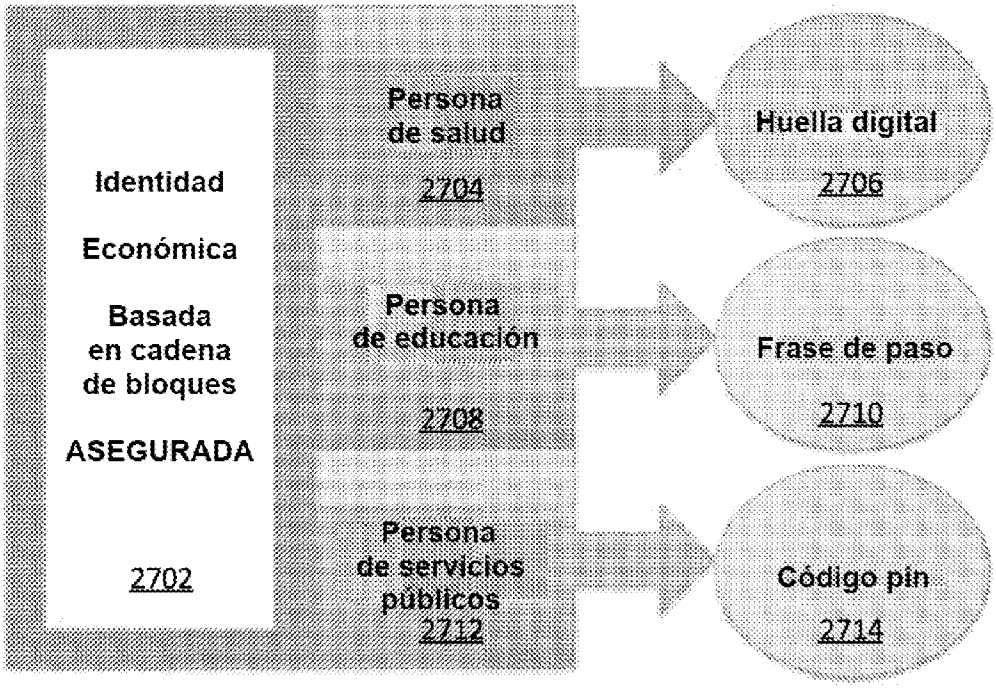

2600
NUBE
2610
MOTOR DE INSCRIPCIÓN
2660
PROOVEEDORES DE SERVICIO
2620
MOTOR DE TRANSACCIONES
2662
2630
2635
2640
2645
2650
2655

FIG. 27


Identidad
Económica
Basada en cadena de bloques
ASEGURADA
2702
Persona de salud
2704
Persona de educación
2708
Persona de servicios públicos
2712
Huella digital
2706
Frase de paso
2710
Código pin
2714