(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 802 420**

(21) Número de solicitud: 201930642

(51) Int. CI.:

H04L 9/06 (2006.01)
G06F 16/00 (2009.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

10.07.2019

(43) Fecha de publicación de la solicitud:

19.01.2021

(71) Solicitantes:

UNIVERSITAT DE LES ILLES BALEARS (100.0%)
Cra. de Valldemossa, km 7.5
07122 Palma de Mallorca, (Illes Balears) ES

(72) Inventor/es:

PAYERAS CAPELLÀ, Maria Magdalena;
MUT PUIGSERVER, Macià;
HUGUET ROTGER, Llorenç y
CABOT NADAL, Miquel Àngel

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

(54) Título: **Método para notificaciones y entregas certificadas basadas en tecnología blockchain**

(57) Resumen:

Método para notificaciones y entregas certificadas basadas en tecnología blockchain.

El método es una aplicación descentralizada basada en una cadena de bloques para seguimiento de notificaciones y entregas, certificadas y confidenciales, de mensajes o archivos de datos a como mínimo un destinatario, generándose pruebas de no repudio de envío y recepción, y del resultado de la notificación: participantes, marca temporal del instante de notificación y estado final. El método controla el flujo de intercambio de datos y pruebas mediante funciones de contrato inteligente invocadas por remitente y destinatario/s, sin intervención de terceras partes de confianza para tramitar el proceso o resolver conflictos entre partes. El contenido de la notificación no se guarda en la cadena de bloques, pero puede confirmarse, a partir de los datos almacenados por el contrato inteligente, que los datos aportados por cualquiera de los participantes se corresponden a los datos del intercambio, incluido el mensaje. Alternativamente, también se permite la entrega de mensajes públicos y accesibles a través del contrato inteligente.

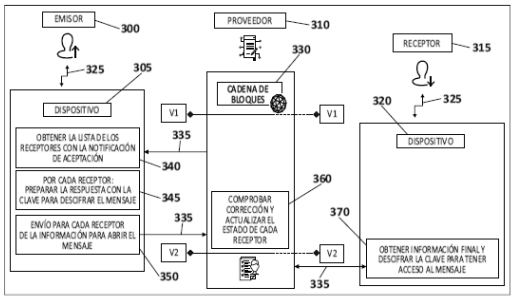

FIG. 3

ES 2 802 420 A1

DESCRIPCIÓN

Método para notificaciones y entregas certificadas basadas en tecnología blockchain

OBJETO DE LA INVENCIÓN

La presente invención se aplica en la industria de las telecomunicaciones y las tecnologías de la información. Más particularmente, la presente invención se refiere a un método para notificaciones y entregas de datos digitales, certificadas (confidenciales o públicas), que usa tecnología de Cadena de Bloques (en inglés, “Blockchain”).

ANTECEDENTES DE LA INVENCIÓN

La entrega certificada o registrada de datos efectuada de forma electrónica (en inglés, “Registered eDelivery”) requiere la utilización de protocolos que proporcionen pruebas o evidencias de la ejecución de la entrega. Estos servicios, también conocidos como servicios de notificaciones certificadas, o incluso de correo electrónico certificado cuando el medio usado para el envío es el correo electrónico, permiten a un remitente probar que ha enviado unos datos digitales (en adelante, el mensaje), pudiéndose tratar de mensajes de notificación u otro tipo de datos, como un archivo, a un receptor o conjunto de receptores. Por lo tanto, estos servicios proporcionan evidencia de que un receptor tiene acceso a la información desde una fecha / hora específica.

En general, los servicios de confianza deben ser seguros, proteger la privacidad de los usuarios y, al mismo tiempo, deben tener en cuenta las regulaciones existentes. Los datos enviados y recibidos utilizando el servicio de entrega certificada deben presentar las propiedades de integridad de los datos, la identificación del remitente de los datos y también de su receptor. Un servicio de entrega certificada cualificado debe ofrecer las siguientes funcionalidades: integridad de los datos, autenticación de origen y autenticación del momento de la entrega. La confidencialidad no se considera una funcionalidad básica, pero generalmente se proporciona como parte de una solución más completa.

Las características básicas de un sistema de entrega certificada son:

1) Efectividad. Si las partes se comportan correctamente, recibirán los elementos esperados.

2) Equidad. Después de completar una ejecución, cada parte ha recibido el elemento esperado o ninguna de las partes ha recibido ninguna información útil sobre el elemento esperado.

3) No repudio. Si una parte A entrega un elemento a una parte B, A no puede negar el origen del elemento y B no puede negar la recepción del mismo.

4) Independencia de terceras partes de confianza. Se considera deseable no requerir una tercera parte de confianza que garantice el estado final del intercambio que representa la entrega.

5) Transferibilidad de la evidencia. Las pruebas generadas por el sistema pueden transferirse a entidades externas o ser consultadas por estas entidades para probar el resultado del intercambio.

6) Confidencialidad. Solo el remitente y el destinatario de los datos conocen el contenido del mensaje certificado.

7) Eficiencia. Un protocolo eficiente utiliza el número mínimo de pasos que permiten el intercambio efectivo o el coste mínimo.

Algunos ejemplos de uso de los servicios de entrega certificada son:

- correo electrónico certificado, una forma mejorada de correo electrónico transmitida por medios electrónicos que proporciona evidencia relacionada con el manejo de un mensaje, incluida la prueba de envío y entrega;
- entrega de notificaciones electrónicas oficiales y soporte de presentaciones oficiales en servicios de administración electrónica;
- acceso e intercambio de datos confidenciales y certificaciones notariales.

En el servicio de entrega certificada, los elementos a intercambiar son los datos que forman el mensaje a entregar junto con las pruebas de no repudio de origen y recepción. Los datos que pueden enviarse en un servicio de entrega electrónica desde un remitente a un receptor pueden ser de cualquier tipo (incluidos los ficheros digitales) y los medios de transmisión pueden ser de cualquier tipo. De esta manera, las notificaciones certificadas y el correo electrónico certificado se incluyen en los servicios de entrega certificada.

Una extensión de los sistemas de entrega certificada a un remitente son los sistemas que permiten la entrega simultánea a diversos receptores. Un protocolo de entrega certificada multidestinatario permite entregas más eficientes y funcionales que un protocolo que permite

únicamente el envío a un destinatario. En tal escenario, diferentes partes están involucradas en un intercambio de mensajes.

Como arriba se ha indicado, los servicios de entrega certificada, junto con otros servicios electrónicos, como la firma electrónica de contratos o la compra electrónica (pago a cambio de un recibo o producto digital), requieren un intercambio equitativo de elementos entre dos o más usuarios. Para poder realizar estos intercambios existen propuestas de protocolos que siguen el patrón genérico denominado intercambio equitativo de valores. Un intercambio equitativo siempre proporciona un tratamiento igual para todos los usuarios y, al final de cada ejecución, o bien cualquiera de las partes tiene el elemento que desea obtener de la otra parte, o bien el intercambio no se ha realizado con éxito para nadie (ninguna parte ha recibido el elemento esperado).

Para resolver el problema de los intercambios equitativos, las soluciones tradicionales incluyen terceras partes de confianza (TTP, por sus siglas en inglés: “Trusted Third Party”) que gestionan los intercambios en mayor o menor medida y son responsables de resolver cualquier conflicto que surja como resultado de intercambios interrumpidos o intentos de fraude.

Además de eso, estas soluciones normalmente usan mecanismos de no repudio para generar evidencia que demuestre el comportamiento de los actores del protocolo, de modo que, en caso de disputa, un árbitro externo puede evaluarlos y tomar una decisión inequívoca.

Sin embargo, en la práctica, la implementación y aceptación de este tipo de entidades basadas en TTPs es un obstáculo para extender el uso de protocolos en la red. Por un lado, es difícil tener TTPs que sean realmente de confianza para cualquier usuario en la red y que tengan un marco de acción definido (por ejemplo, los documentos electrónicos generados por la TTP tienen que ser aceptados para resolver disputas en un tribunal, de acuerdo a las leyes de diferentes países). Además, las TTPs también pueden causar problemas a nivel técnico (por ejemplo, pueden causar cuellos de botella desde el punto de vista de las comunicaciones), falta de eficiencia en los protocolos y aumentar el coste de la ejecución del protocolo (por ejemplo, cobrar altas tarifas por la prestación de servicios). Además, son un punto muy sensible en la red, ya que desempeñan un papel importante en la seguridad de los protocolos electrónicos y su confiabilidad es un problema que necesita atención, ya que la seguridad del intercambio se puede romper si la TTP tiene alguna vulnerabilidad.

El rol de la TTP puede ser muy diferente entre las soluciones existentes para entregas certificadas, pudiendo desempeñar un papel importante porque la TTP participa en cada intercambio de elementos, o llevar a cabo un papel más relajado en el que la TTP solo está activa cuando surge una disputa entre las partes (protocolos optimistas).

Debido a la incompatibilidad entre algunas de las propiedades de los servicios de entrega certificada y la dificultad de lograr simultáneamente un determinado conjunto de ellas en un mismo procedimiento, es posible encontrar protocolos que resuelven el intercambio de manera eficiente con una TTP optimista, aunque solo logren una equidad débil, mientras que otros sistemas están enfocados en el logro de características específicas como la transferencia de pruebas, la verificabilidad de la TTP, evitar el rechazo selectivo basado en la identidad del remitente, la flexibilidad para permitir la entrega simultánea a múltiples receptores o la reducción del volumen de información de estado que la tercera parte debe mantener.

A continuación, se mencionan algunas soluciones del estado de la técnica previo, que presentan sistemas y/o métodos de entrega certificada donde se garantiza alguna de las propiedades citadas, pero no todas a la vez, como por ejemplo:

- US2009094452A1 divulga un protocolo optimista para el intercambio de correo electrónico o email certificado en el que una TTP interviene únicamente en caso de disputas. El mensaje se cifra con una clave que comparten el remitente y una TTP, pero también se plantea la posibilidad de que la clave de cifrado del mensaje se cifre con la clave pública de la TTP. La TTP solo interviene en caso de disputa (certificado del remitente o recibo del destinatario no válidos o interrupción del protocolo). En caso contrario las pruebas de no repudio se generan sin su participación. Por consiguiente, esta solución requiere la participación de una TTP, aunque su participación se limite a la resolución de disputas. No utiliza ningún contrato inteligente (en inglés “smart contracts”), ni prevé que los mensajes sean públicos.
- EP0955745A2 describe un método de intercambio equitativo en redes de comunicaciones de firmas digitales entre una primera parte y una segunda parte, incluido el uso de una o más firmas confiables, de modo que cada parte recibe una firma digital válida de la otra parte, o ninguna de las partes recibe una firma digital válida. Este método comprende una pluralidad de transferencias de mensajes

entre las dos partes, y usa una tercera parte confiable (TTP) que puede actuar como un confirmador, verificando independientemente la validez de una firma confirmable que se origina en la primera parte o la segunda parte.

Por otra parte, existen algunas propuestas de protocolos para intercambios equitativos, distintos a las entregas certificadas, que utilizan tecnología de cadena de bloques (blockchain, en inglés). Estas propuestas se centran en las operaciones de compra justa entre un producto (o un recibo) a cambio de criptomonedas (generalmente bitcoin), pero no existe ninguna propuesta de notificaciones multidestinatario confidenciales y entregas certificadas basada en blockchain.

A continuación, se mencionan algunas propuestas del estado de la técnica previo que utilizan tecnología blockchain, para intercambios equitativos que no son notificaciones ni entregas certificadas:

- US2018130050A1 presenta un método para administrar datos transaccionales en bloques con firma criptográfica en un sistema basado en cadena, que implica verificar si la transacción se realiza según los privilegios asociados con las billeteras de partes que intentan realizar la transacción, utilizando tecnología blockchain. El objetivo del sistema es gestionar transacciones en bloques firmados criptográficamente, por lo que no se trata propiamente de un sistema de intercambio de información.
- CN108566395A presenta un método para transmitir archivos desde el transmisor al receptor basado en la cadena de bloques, que implica realizar el proceso de identificación de identidad de la cadena de bloques mediante el uso de un certificado digital, y la transmisión de un sobre digital al receptor basado en la cadena, proporcionan un sistema de transmisión de archivos basado en blockchain. Utiliza cifrado para la transmisión y certificados digitales para la identificación de las partes. Sin embargo, el sistema no genera pruebas de no repudio.
- US2019036778A1 presenta un método para utilizar los contratos inteligentes de blockchain para gestionar los requisitos de uso dinámico de datos. Un contrato inteligente (en inglés, “smart contract”) es un programa informático que vive en un sistema no controlado por ninguna de las partes (o sus agentes), y que facilita, asegura, hace cumplir y ejecuta acuerdos registrados entre dos o más partes (por ejemplo personas u organizaciones). Cuando se dispara una condición pre-programada, no sujeta a ningún tipo de valoración humana, el contrato inteligente ejecuta la cláusula contractual correspondiente. En el caso de la gestión de los

requisitos de uso dinámico de datos, implica modificar el estado operativo de la red en función de las políticas y los umbrales de datos que se superan, y almacenar el estado operativo modificado en blockchain. El método descrito en US2019036778A1 utiliza contratos inteligentes para ese propósito, que es un objetivo técnico totalmente diferente al que aquí se propone.

El problema técnico objetivo que se presenta es pues proveer un método para el seguimiento de entrega de mensajes (confidenciales y públicos) a uno o diversos destinatarios, controlando el flujo de intercambio de datos y notificaciones a través de las funciones de los contratos inteligentes de una cadena de bloques que pueden ser invocadas por los destinatarios (o destinatario único) y remitente.

DESCRIPCIÓN DE LA INVENCIÓ

La presente invención sirve para solucionar el problema mencionado anteriormente, presentando un método para notificaciones y entrega de mensajes certificadas, en el que se generan pruebas no repudiables tanto de envío como de recepción de los mensajes y notificaciones, además de confirmación del estado de la finalización o cancelación de la entrega/notificación, donde no se usa ninguna tercera parte confiable (TTP) sino que utiliza una cadena de bloques (blockchain). El método que se propone constituye un protocolo o aplicación distribuida que controla el flujo de intercambio de datos y pruebas a través de las funciones de un contrato inteligente de blockchain que son invocadas por los participantes/usuarios del método: remitente y destinatario/s. Además, el método permite la firma de contratos entre dos o más usuarios firmantes, donde el contrato a firmar se refiere a cualquier contrato, en su concepto genérico, no se refiere a un contrato inteligente.

Los usuarios pueden actuar como:

- Usuario emisor: Usuario que genera la notificación o los datos a entregar a través del método, actuando como remitente.
- Usuario(s) receptor(es): Usuario(s) que recibirán la entrega certificada, actuando como destinatario(s).
- Usuarios firmantes de contratos.

Las notificaciones y entregas de mensajes se efectúan desde un emisor a uno o diversos receptores.

Los posibles datos a intercambiar en el método entre el usuario emisor y el, al menos uno, usuario receptor son:

- Mensaje, entendiéndose por mensaje tanto el texto perteneciente a una notificación como un archivo o registro de datos digitales de cualquier tipo. Los mensajes pueden ser confidenciales o públicos.
- Prueba de no repudio de emisión, que impide que el emisor pueda negar la emisión del mensaje específico.
- Prueba(s) de no repudio de recepción. Una por cada receptor del mensaje específico, que impiden que el(los) receptor(es) puedan negar la recepción del mensaje.

A partir de los datos intercambiados, el método proporciona pruebas del resultado de la notificación: entidades participantes, marca temporal del instante de la notificación y estado final.

El intercambio de elementos se realiza sobre una cadena de bloques o blockchain. El método controla el flujo de intercambio de datos y pruebas a través de la ejecución de las funciones de un contrato inteligente. Un contrato inteligente principal puede ser utilizado para diferentes notificaciones o entregas y se genera un contrato inteligente específico para cada una de las notificaciones/entregas. El contrato principal permite la consulta de las notificaciones finalizadas por cada usuario. El método además proporciona mecanismos para que se pueda finalizar el servicio de notificación o entrega de mensajes entre el emisor y un subconjunto de los destinatarios, cancelándose para el resto de los destinatarios. El método además permite definir el valor de unos períodos de aceptación y finalización de cada notificación/entrega.

Un aspecto de la invención se refiere a un método para notificaciones y entregas certificadas de datos digitales (mensajes) que usa una red de cadena de bloques (blockchain), donde un proveedor proporciona un servicio de notificación o entrega certificada a través de al menos un contrato inteligente desplegado sobre la blockchain entre un usuario emisor y uno o más usuarios receptores. Los usuarios interaccionan con el servicio de notificación o entrega certificada mediante dispositivos de acceso o terminales de usuario emisor o receptor. Los usuarios y el proveedor interactúan con la blockchain a través de una interfaz de comunicación. El método comprende los siguientes pasos:

- el proveedor despliega un contrato inteligente principal;
- los usuarios envían información para darse de alta en el servicio:

- el usuario emisor prepara una notificación o entrega de un mensaje, privado o público;
- para cada notificación o entrega preparada, el usuario emisor accede al contrato inteligente principal para crear un contrato inteligente específico de la notificación o entrega que gestiona la notificación o entrega certificada del mensaje a intercambiar y que comprende un conjunto de receptores y al menos un primer vencimiento (V1) que define un umbral de tiempo límite superior dado al conjunto de receptores para aceptar la notificación o entrega;
- para cada notificación o entrega preparada, cada usuario receptor detecta la notificación o entrega y accede al contrato inteligente específico;
- cada usuario receptor prepara una respuesta de aceptación que representa un reconocimiento de la notificación o entrega detectada;
- cada usuario receptor que envía la respuesta de aceptación antes del primer vencimiento (V1) es añadido por el proveedor a un subconjunto de receptores;
    - el usuario emisor accede a ese subconjunto de receptores y, para cada usuario receptor del subconjunto, calcula una respuesta que comprende información para habilitar a cada usuario receptor del subconjunto a leer el mensaje, y la envía al proveedor;
- el proveedor comprueba la corrección de las respuestas enviadas por el usuario emisor y establece un estado final del intercambio: estado de finalización, si la comprobación determina que las respuestas enviadas son correctas, y estado de cancelación, en caso contrario;
    - en caso de estado de finalización, cada usuario receptor que ha aceptado la notificación o entrega obtiene la respuesta calculada por el usuario emisor para que pueda leer el mensaje;
    - en caso de estado de cancelación, cada usuario receptor que ha aceptado la notificación o entrega obtiene unas evidencias de cancelación de la notificación o entrega.

En una posible realización, el servicio de notificación o entrega de mensajes se realiza mediante las siguientes etapas:

1) Despliegue del contrato inteligente principal.

2) Registro en el sistema de las direcciones públicas usadas en la cadena de bloques (blockchain) por los usuarios.

Por cada entrega o notificación, en el caso de mensajes confidenciales:

3) Generación de unas claves de notificación y cifrado, por parte del emisor, de los datos a entregar.

4) Acceso al contrato inteligente principal por parte del usuario emisor. Despliegue automático del contrato inteligente específico de la entrega/notificación que gestiona el intercambio y ejecución, sobre el contrato inteligente desplegado en este paso, y por parte del emisor, de la función de envío del mensaje cifrado utilizando un elemento o parámetro de cifrado. Esta función tiene como parámetros el mensaje cifrado, el receptor o conjunto de receptores y los valores de unos vencimientos (o límites superiores de tiempo) que determinan los períodos de aceptación y finalización: un primer vencimiento especifica el período válido para que los receptores acepten la entrega/notificación antes de que el remitente la finalice, y un segundo vencimiento determina el plazo para que el emisor finalice la entrega y el momento a partir del cual los receptores pueden leer el mensaje u obtener evidencias de cancelación de la entrega/notificación no finalizada por parte del remitente. En el caso de que las notificaciones/entregas sean para un único usuario destinatario puede utilizarse una simplificación del método donde se elimina uno de los vencimientos.

5) Acceso del usuario o de los usuarios receptores al contrato inteligente específico desplegado en la etapa 4.

6) Por cada uno de los receptores de la entrega/notificación, creación de los elementos necesarios para que el emisor genere la respuesta que permite que el contrato inteligente específico verifique la posibilidad de acceso a los datos por parte del receptor, pudiéndose tratar de claves de entrega/notificación, reto y cifrado de su clave privada de entrega/notificación.

7) Por cada uno de los receptores que quiere seguir adelante con la entrega/notificación, aceptación (en el periodo establecido) de la entrega/notificación y envío de los elementos generados en la etapa 6, incluyendo un posible reto y la clave cifrada.

8) Determinación, por parte del contrato inteligente específico, del conjunto de los receptores con los que se va a finalizar el intercambio.

9) Para cada receptor del conjunto anterior, obtención, por parte del emisor, de la clave privada de entrega/notificación del receptor.

10) Para cada receptor del conjunto anterior, preparación y envío, por parte del emisor, en el periodo establecido, de la respuesta que permite que el contrato inteligente específico verifique la posibilidad de acceso a los datos por parte del receptor, pudiendo utilizar la clave de entrega/notificación del receptor, el reto y el elemento de cifrado del mensaje.

11) Acceso del usuario emisor al contrato inteligente desplegado en la etapa 4 introduciendo los datos necesarios para la finalización del intercambio, incluyendo datos para que el contrato inteligente valide la respuesta al reto mediante, por ejemplo, una prueba de conocimiento nulo.

12) Verificación por parte del contrato inteligente específico de los datos aportados por el emisor mediante, por ejemplo, una prueba de conocimiento nulo, de modo que permita asegurar que el receptor tiene acceso al elemento de cifrado y por tanto al mensaje. El contrato inteligente específico no puede acceder al mensaje, por lo que éste puede permanecer como mensaje confidencial. Determinación del estado final del intercambio: los receptores que hayan aceptado el intercambio pasan al estado finalizado, mientras que el resto pasan al estado rechazado. El estado final del intercambio puede ser: de finalización, habiéndose generado pruebas de no repudio de origen y recepción; o bien, de cancelación, estado en el que no existen pruebas de no repudio válidas.

13) En caso de finalización del intercambio, cada receptor del conjunto de receptores que han aceptado la entrega/notificación descifra el mensaje a partir de los datos aportados por el contrato inteligente específico.

14) En caso de no finalización correcta por parte del emisor, los receptores pueden obtener una prueba de cancelación de la entrega/notificación que invalida cualquier prueba de no repudio de recepción. Esta prueba está disponible después del segundo vencimiento.

Las pruebas de no repudio generadas por el método garantizan la autenticidad de las partes, al verificarse la identidad de los usuarios que ejecutan las funciones del contrato inteligente. La ejecución de las funciones requiere, por tanto, el conocimiento de las claves secretas de las direcciones de la cadena de bloques (blockchain). Una prueba de no repudio de origen puede generarse en la etapa 7 o en la etapa 11:

- En la etapa 7, la prueba de no repudio se genera cuando el(los) usuario(s) receptor(es) aceptan la recepción de la notificación/entrega; entonces el contrato inteligente autentica al usuario que accede a la función de aceptación garantizando el no repudio en recepción. Estas pruebas de no repudio de recepción se invalidan en la etapa 14 si el emisor no finaliza el intercambio en el periodo establecido (segundo vencimiento).
- En la etapa 11, la prueba de no repudio se genera cuando en usuario emisor ejecuta la función de finalización y proporciona los datos con los que el receptor obtiene el elemento para el descifrado del mensaje; entonces el contrato inteligente

autentica al usuario que accede a la función de finalización y los datos aportados, garantizando el no repudio en origen.

El método además puede generar pruebas del resultado de la notificación que son transferidas y consultadas para la difusión del resultado del intercambio. Las pruebas de no repudio y las pruebas del resultado de la notificación garantizan la equidad del intercambio de datos.

El método satisface la propiedad de integridad de los datos, ya que el contrato inteligente comprueba que el mensaje o conjunto de datos que el(los) receptor(es) puede(n) descifrar se corresponde con el mensaje cifrado en la etapa 3 (y enviado en la etapa 4). Este método evita que el emisor pueda cambiar el mensaje en función de las aceptaciones recibidas en la etapa 7.

Otra posible realización es el caso de una notificación o entrega de mensaje pública, donde no hay cifrado y el remitente puede publicar el mensaje en la cadena de bloques. El método para mensajes públicos presenta una solución para la entrega equitativa multidestinataria con un remitente y múltiples receptores. El remitente de la entrega y el conjunto de receptores intercambian el mensaje y las pruebas de no repudio siguiendo los pasos de un protocolo de intercambio como sigue:

1) Un remitente envía un mensaje al conjunto de receptores creando un contrato a través de la invocación de la función de constructor de la factoría desplegada por el proveedor, incluyendo como parámetros el “hash” del mensaje a entregar, las direcciones de los receptores y unos plazos de vencimiento V1 y V2. El “hash” o resumen criptográfico del mensaje es una serie única de datos que se crea cuando la colección de información que se desea proteger se ejecuta a través de una función hash o función resumen. El vencimiento V1 determina el límite temporal de aceptación de una entrega para los receptores antes de que el remitente la finalice, y el vencimiento V2 determina el plazo para que el emisor finalice la entrega y el receptor pueda obtener el mensaje y la prueba de no repudio de origen o la evidencia de cancelación de la notificación. Opcionalmente se puede incluir en esta etapa un depósito o pago por el servicio.

2) Cada receptor del conjunto de receptores puede decidir individualmente si acepta la entrega o no. En caso de aceptación debe ejecutar la función correspondiente del contrato inteligente antes de V1, expresando su voluntad. Si un receptor no acepta antes de V1, se asume un rechazo.

3) Después del vencimiento del primer plazo V1, o bien, después de que todos los receptores del conjunto han aceptado la recepción (el acto que se produzca en primer lugar), el remitente puede publicar el mensaje enviándolo al contrato inteligente y finalizar la entrega al subconjunto de receptores que ha aceptado la notificación del mensaje. El contrato inteligente verifica si el hash del mensaje recibido es igual al hash almacenado en la cadena de bloques, y luego marca todos los receptores que han aceptado utilizando el estado finalizado como prueba de no repudio, mientras que todos los receptores que no han aceptado pasan al estado rechazado. Como consecuencia, el contrato inteligente publica la prueba de no repudio para los receptores que aceptaron la notificación.

4) Finalmente, después del segundo plazo de espera V2, los receptores que han aceptado la entrega pueden acceder al mensaje a través de la interfaz de comunicación (por ejemplo, WEB3 o similar). Si el emisor no ha finalizado con éxito la emisión, los receptores tienen acceso a las evidencias de cancelación correspondientes.

Por otra parte, este método de notificaciones y entrega de mensajes puede además ser utilizado para la operación de firma de contratos inteligentes por parte de dos o más firmantes. En una posible realización de la operación de firma, se realiza un intercambio equitativo de firmas sobre el contrato. Los usuarios dejan de dividirse en emisor y receptores y todos los usuarios son firmantes del contrato. Uno de los usuarios firmantes del contrato actúa como proponedor del contrato a firmar. Existen dos diferencias fundamentales entre el uso del método para notificación o entrega y su uso para firma de contratos. La primera diferencia es que los usuarios (firmantes) conocen siempre el contenido del mensaje (en este caso, el texto del contrato a firmar) antes de su aceptación. La segunda diferencia es que no se considera finalizado un intercambio de firma de contratos hasta que toda la pluralidad de firmantes acepta el contrato.

Las ventajas de la presente invención frente al estado de la técnica anterior son fundamentalmente:

- La invención proporciona una aplicación descentralizada o distribuida basada en tecnología blockchain que elimina la necesidad de la participación de terceras partes de confianza (TTP) al tiempo que satisface los requisitos de la normativa creada por la Unión Europea para las entregas certificadas (eDeliveries, en inglés

"Registered Electronic Deliveries"). La aplicación distribuida y el contrato inteligente de blockchain gestionan íntegramente el flujo de intercambio de datos y pruebas, por lo que no se requiere la intervención de TTP externa para tramitar el proceso ni para resolver conflictos entre las partes.

- La invención garantiza la confidencialidad de las notificaciones y entrega de mensajes, siendo el usuario receptor el único que puede conocer el contenido del mensaje. En las notificaciones confidenciales, el contenido de la notificación no se guarda en claro en la cadena de bloques (blockchain). Sin embargo, puede confirmarse, a partir de los datos almacenados por el contrato inteligente de la blockchain, que los datos aportados por cualquiera de los usuarios se corresponden a los datos del intercambio, incluido el contenido de la notificación. De forma opcional, las partes pueden acordar que la notificación sea pública, registrando en la blockchain el contenido de la notificación. En el caso de notificaciones públicas, el contenido del mensaje puede consultarse como un dato más a través de funciones de consulta al contrato inteligente.

BREVE DESCRIPCIÓN DE LAS FIGURAS

A continuación, se pasa a describir de manera muy breve una serie de dibujos que ayudan a comprender mejor la invención y que se relacionan expresamente con una realización de dicha invención que se presenta como un ejemplo no limitativo de ésta.

FIGURA 1.- Muestra un esquema general de un método para notificaciones y entrega de mensajes certificadas basado en blockchain y de las entidades participantes en el método, según una realización preferente de la invención.

FIGURA 2.- Muestra las funciones y procedimientos que se realizan antes de una fecha y hora de vencimiento determinadas en el método, según una posible realización de la invención.

FIGURA 3.- Muestra las funciones y procedimientos que se realizan después de una fecha y hora de vencimiento determinadas en el método, según una posible realización de la invención.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

En las Figuras 1, 2, y 3 se ha representado un solo usuario receptor pero se ilustran los elementos y procesos que también aplican en el caso de múltiples usuarios receptores que puede tener cualquier envío de una notificación que utiliza el método aquí descrito.

En una realización preferente de la invención se propone un método o protocolo de seguimiento de entrega de mensajes certificada basado en una aplicación descentralizada y contratos inteligentes de una blockchain. La entrega de mensajes puede ser a uno o diversos usuarios receptores o destinatarios. El protocolo genera pruebas de no repudio tanto de envío como de recepción además de información relativa al proceso de finalización del seguimiento. Puede tratarse de mensajes de notificación o de entregas de datos de cualquier naturaleza. El protocolo controla el flujo del intercambio de datos y pruebas a través de las funciones de un contrato inteligente que son invocadas por los participantes en el sistema: remitente y destinatario/s.

La aplicación descentralizada y los contratos inteligentes gestionan íntegramente el proceso de entrega de mensajes certificada, por lo que no se requiere la intervención de ninguna tercera parte de confianza externa para tramitarlo ni para resolver conflictos entre las partes. La aplicación descentralizada proporciona pruebas del resultado de la notificación, aportando información de las entidades participantes, marca temporal del instante de la notificación y del estado final del proceso.

Las posibles realizaciones del método contemplan la entrega de dos tipos de mensajes, confidenciales o públicos, siendo la entrega pública una variante, menos compleja, del protocolo confidencial.

En el caso de las notificaciones confidenciales, el contenido de la notificación no se guarda en la blockchain en claro. Sin embargo, a partir de los datos almacenados en el contrato inteligente, puede confirmarse si los datos aportados por cualquiera de las entidades participantes se corresponden a los datos del intercambio, incluido el contenido confidencial de la notificación.

En el caso de notificaciones públicas, el contenido del mensaje puede consultarse como un dato más a través de funciones de consulta del contrato inteligente.

El protocolo de intercambio de datos (confidenciales o públicos) comprende los siguientes pasos:

1º En el caso de intercambio de datos confidenciales, el remitente A cifra el mensaje a enviar, utilizando un elemento secreto de cifrado y su clave privada, obtenidos de un par de claves de notificación creado específicamente para la entrega de datos. Para ello, el remitente A crea un contrato inteligente invocando la función de constructor de la factoría desplegada por el proveedor, incluyendo como parámetros: el mensaje cifrado, la clave pública de notificación del remitente, las direcciones de los receptores y unos plazos de vencimiento (V1, V2). El primer vencimiento (V1) o vencimiento de aceptación especifica el período válido para que los receptores acepten la entrega antes de que el remitente la finalice. El segundo vencimiento (V2) o vencimiento de finalización determina el plazo para que el remitente finalice la entrega y el momento a partir del cual los receptores pueden leer el mensaje u obtener evidencias de cancelación de la entrega no finalizada por parte del remitente. Opcionalmente se puede incluir en esta etapa un depósito o pago por el servicio de entrega. En el caso de un intercambio de datos público, no hay cifrado, el remitente A simplemente envía el “hash” del mensaje para publicarlo en la blockchain. Para publicar en la blockchain ese resumen criptográfico del mensaje (público) o el mensaje (confidencial) cifrado, el remitente A utiliza como parámetros la dirección del receptor y el vencimiento de finalización que determina el plazo para que se complete la entrega.

2º Cada receptor Bi del conjunto de receptores B puede decidir individualmente si acepta la entrega o no. En caso de aceptación debe ejecutar la función correspondiente del contrato inteligente antes del primer vencimiento (V1). En el caso de intercambio de datos confidenciales, cada receptor que quiere aceptar la entrega genera su propio par de claves de notificación y los elementos necesarios para que el remitente A le pueda hacer entrega de forma confidencial de la clave para descifrar el mensaje. El contrato inteligente generado por el remitente A comprueba si el receptor Bi es capaz de descifrar el mensaje confidencial; es decir, si el remitente A envía la clave que se ha comprometido a enviar en el inicio del envío de esta notificación. En una de las soluciones posibles, el receptor Bi crea una variable que se utiliza como reto en el paso siguiente del protocolo de intercambio y a continuación envía su clave pública de notificación, el reto, y su clave privada de notificación cifrada, utilizando la clave pública de notificación del remitente. El reto se almacena de igual forma que el resto de parámetros en el contrato inteligente. Si algún receptor del conjunto de receptores B no acepta la entrega antes de primer vencimiento (V1), se asume un rechazo.

3º Después del primer vencimiento (V1) o después de la aceptación por parte de todos los receptores del conjunto de receptores B (el acto que se produzca en primer lugar), el remitente A puede finalizar la entrega permitiendo el acceso al mensaje a los receptores que han aceptado la entrega. En el caso de intercambio de datos confidenciales, el remitente A genera los elementos necesarios para que el contrato inteligente asegure al destinatario su acceso al mensaje. En una posible realización, el remitente A puede generar, para cada receptor, una respuesta al reto en forma de prueba de conocimiento nulo, utilizando el elemento secreto usado en el cifrado del mensaje, el reto y la clave privada de notificación del receptor. Con esta respuesta el contrato inteligente puede verificar, mediante los datos almacenados, que el receptor es capaz de obtener el elemento secreto para poder descifrar el mensaje. No obstante, el contrato inteligente no conoce dicho elemento y por tanto el mensaje permanece confidencial. El contrato inteligente marca todos los receptores que han aceptado, que constituyen un subconjunto B' del conjunto B de receptores, utilizando el estado finalizado como prueba de no repudio. Por otra parte, el contrato inteligente marca todos los receptores que no han aceptado, i.e., los receptores del conjunto B que no pertenecen al subconjunto B', con el estado rechazado. Como consecuencia, el contrato inteligente publica la prueba de no repudio para los receptores miembros del subconjunto B′. El proceso de finalización por parte del remitente A tiene que finalizar antes del segundo vencimiento (V2). En el caso de intercambio público de datos, el remitente A envía el mensaje y el contrato inteligente comprueba que se trata del mensaje utilizado para la creación del "hash" enviado anteriormente (en el paso 1º).

4º Finalmente, después del plazo de espera delimitado por el segundo vencimiento (V2), los receptores del subconjunto B′ que han aceptado la entrega pueden acceder al mensaje a través de una interfaz WEB3 o similar. En caso de que el remitente A no finalice con éxito la entrega antes del segundo vencimiento (V2), los receptores del subconjunto B′ tienen acceso a las evidencias de cancelación correspondientes.

Después del protocolo de intercambio, el método de seguimiento de la entrega procede con los siguientes pasos:

- El contrato inteligente comprueba que los receptores del subconjunto B′ disponen del elemento para descifrar el mensaje, que no está almacenado en la cadena de bloques si es confidencial. Para ello, el contrato inteligente almacena una variable booleana

"*finalizado"* para cada receptor Bi, de forma que para los receptores que han finalizado el intercambio, la variable *Finalizado (Bi ∈ B') = verdadero*, mientras que para el resto *Finalizado (Bi∉ B') = falso*. Si el intercambio de datos es público, se dispone directamente del mensaje, puesto que está almacenado en la cadena de bloques, pero solo los miembros de B′ pueden probar que han sido notificados por A. El contrato inteligente igualmente almacena la variable booleana *finalizado* para cada receptor, de forma que para los receptores que han finalizado el intercambio *Finalizado(Bi ∈ B') = verdadero*, mientras que *Finalizado (Bi∉ B') = falso.*

- Después del segundo vencimiento (V2), para el caso confidencial, el mensaje puede ser descifrado por todos los receptores Bi ∈ B′. Si después del segundo vencimiento (V2) el remitente A no ha publicado la prueba de conocimiento nulo de forma correcta, los receptores Bi ∈ B′ pueden obtener las evidencias de cancelación de la entrega. En el caso público, si después del segundo vencimiento (V2) el remitente A no ha publicado el mensaje, los receptores Bi pueden tener a partir de los datos almacenados en la blockchain la evidencia de cancelación de su notificación. Si, por el contrario, el remitente A ha dejado su mensaje en la blockchain antes del segundo vencimiento (V2), los receptores tienen acceso al mismo y obtienen la prueba de no repudio de origen.

El protocolo también presenta una variante para la entrega a un único destinatario. Si bien puede usarse el protocolo (tanto público como confidencial) descrito anteriormente con un único receptor, esta variante presenta una mayor eficiencia.

El protocolo de intercambio de datos para el caso de un solo remitente y un solo receptor es el siguiente:

- El remitente creador del mensaje usa el contrato inteligente para publicar en la blockchain el "hash" del mensaje o el mensaje cifrado, dependiendo de si se pretende una notificación pública o confidencial.
- El receptor, si acepta la recepción, ejecuta la función de aceptación.
- Finalmente, el remitente publica el mensaje, en el caso de notificaciones públicas, o los elementos de descifrado, en el caso de entregas confidenciales. Como consecuencia, el contrato inteligente publica la prueba de no repudio.
- Si no se ejecutan los tres pasos, el contrato inteligente no se destruye automáticamente y, después del vencimiento de finalización (V2), ambas partes pueden acceder a una función del contrato inteligente para solicitar la cancelación de los elementos transferidos.
    - Cancelación de recepción, solicitada por el receptor, si el remitente no

publica el mensaje cuando el receptor ha aceptado la notificación.

- Cancelación de emisión, solicitada por el remitente, si el receptor no ha aceptado la notificación.

En ambos casos, el contrato inteligente verifica la identidad del usuario (receptor o remitente) que solicita la cancelación y el plazo de vencimiento. El contrato inteligente genera una transacción para señalar que la notificación ha sido cancelada. Puede observarse que la principal diferencia en el protocolo para un único destinatario se halla pues en la gestión de los vencimientos.

En una posible realización, a partir del método de intercambio descrito anteriormente para el caso multidestinatario y público pueden realizarse intercambios para la firma de contratos públicos multiparte del siguiente modo:

1) El usuario firmante proponedor crea el contrato inteligente del modo descrito anteriormente incluyendo como parámetros: el mensaje (que ahora consiste en el texto del contrato a firmar y no su “hash”), las direcciones de los firmantes y los plazos de vencimiento V1 y V2.

2) Cada firmante puede decidir individualmente si acepta/firma o no el contrato ejecutando la función correspondiente del contrato inteligente antes del primer plazo V1. Si algún receptor no acepta antes del primer plazo V1, se cancela la firma del contrato para todos los firmantes.

3) Después de que todos hayan aceptado/firmado el contrato, el usuario firmante proponedor puede finalizar el proceso de firma, prescindiendo de la comprobación del “hash”.

Después del protocolo de intercambio, el texto del contrato y las direcciones de los firmantes son públicas y quedan almacenadas en la cadena de bloques. Si después del segundo plazo, el firmante proponedor no ha procedido a la finalización/firma del contrato, los demás firmantes pueden tener la evidencia de cancelación del contrato.

En otra posible realización, el método puede ser utilizado para la firma de contratos multiparte confidenciales:

1) Un firmante proponedor que propone la firma del contrato cifra el texto del contrato

y crea el contrato inteligente como se ha descrito anteriormente.

2) Cada usuario firmante implicado en la firma que no es el proponedor genera su propio par de claves de notificación y un reto, y procede al envío de los elementos para que el firmante proponedor pueda responder al reto como se ha descrito anteriormente.

3) El firmante proponedor responde al reto y el contrato inteligente valida la respuesta asegurando que todos los firmantes tienen acceso al texto del contrato.

4) Cada firmante, que no es el proponedor, puede decidir individualmente si acepta/firma o no el contrato recibido. Si alguno de esos firmantes no acepta antes del primer plazo (V1), se cancela el intercambio para todos los firmantes.

5) Después del primer plazo (V1), el usuario firmante proponedor puede finalizar la firma del contrato. El proceso de finalización por parte del emisor tiene que realizarse antes del segundo plazo (V2).

Después del protocolo de intercambio el texto del contrato firmado es confidencial y no está almacenado en la cadena de bloques, pero el contrato inteligente puede probar que los firmantes han podido descifrar el texto del contrato antes de aceptarlo. En caso de que después del segundo plazo, el usuario proponedor no haya finalizado la firma del contrato, los firmantes pueden obtener las evidencias de cancelación del proceso de firma.

En otra posible realización, el método puede ser utilizado para la firma de contratos entre dos usuarios, definiéndose a partir del protocolo de intercambio de datos para el caso de un solo remitente y un solo receptor. La única diferencia con el protocolo de intercambio público se halla en el hecho de que el usuario firmante proponedor incluye el texto en claro del contrato en el primer paso en lugar de incluir un “hash” del mensaje y por tanto se elimina la comprobación del tercer paso. En la versión confidencial, debe ejecutarse la fase de creación/respuesta al reto antes de la aceptación por parte del otro firmante.

La Figura 1 muestra un esquema general del protocolo de intercambio de datos descrito anteriormente con las entidades participantes y pasos básicos que conlleva. Un usuario emisor (100) interacciona (125) a través de un dispositivo de usuario emisor (105) con la

aplicación distribuida de notificaciones y entregas descrita. El usuario receptor (115), que puede ser uno o más de uno, similarmente dispone de un dispositivo de usuario receptor (120) con el que interacciona (125) para las notificaciones y entregas. Un proveedor de contratos inteligentes (110) del servicio de notificaciones y entregas dispone de una interfaz de comunicación (135), por ejemplo, una interfaz web3 o similar, con una blockchain o cadena de bloques (130). El proveedor de contratos inteligentes (110) es la parte que activa el despliegue (140) de una factoría para contratos inteligentes y que puede invocar la función de añadir usuario (155) a la lista de receptores que aceptan la notificación. La función de creación (145) de una nueva notificación y la función de respuesta (160) a cada receptor con entrega aceptada son invocadas por el usuario emisor (105). La función de reconocimiento (150) de entrega y la función de obtención de respuesta para tener acceso al mensaje (165) son invocadas por el usuario receptor (115).

Esta Figura 1, como el resto de Figuras 2-3, también son aplicables a la realización del método para el intercambio de firma electrónica de contratos, de acuerdo con lo descrito anteriormente, cuando en vez de distinguir entre usuario emisor y receptores, se distingue un usuario firmante proponedor y uno o más usuarios firmantes.

En resumen, el esquema de la Figura 1 representa lo siguientes pasos principales:

- Despliegue (140) de la factoría o contrato inteligente principal.
- Invocación del servicio de notificaciones y entregas para la creación (145) de una nueva notificación o entrega con una lista de receptores.
- Reconocimiento (150) de la notificación o entrega por parte de los receptores.
- Creación de la lista de receptores que aceptan la entrega o notificación (155).
- Respuesta (160) para cada receptor que ha aceptado la entrega o notificación y que permite el acceso a los datos.
- Obtención de los elementos de respuesta que permiten el acceso al mensaje (165).

La Figura 2 muestra las funciones y procedimientos que se realizan antes del primer vencimiento (V1) determinado en el protocolo de intercambio de datos para que los receptores acepten la entrega. Un usuario emisor (200), a través de un dispositivo del usuario emisor (205) con una relación de interacción (225) dispositivo-usuario con la aplicación o app de notificaciones, procede a iniciar la acción de envío de la información necesaria para darse de alta (245) como usuario en el sistema. La misma acción para darse de alta (245) como usuario realiza el usuario receptor (215) a través de su dispositivo del usuario receptor (220). La

información necesaria para dar de alta a emisor y receptor como usuarios llega a la factoría (240) de generación de contratos inteligentes provista por el proveedor del servicio de notificaciones (210) sobre la blockchain o cadena de bloques (230), que cuenta con una interfaz de comunicación (235) con dicha blockchain. Invocando la función de creación en la blockchain de una nueva notificación (255) el emisor (200) crea una nueva notificación eDELIVERY de entrega y la lista de usuarios receptores, para la que se despliega un contrato inteligente específico para el intercambio (260) del emisor (200) con cada usuario receptor (215) de la lista. El usuario emisor (205) se encarga de preparar (250) la nueva entrega mediante un procedimiento de cifrado del mensaje, establecimiento de vencimientos de la entrega y parámetros criptográficos y asimismo invocando la función de creación de una nueva notificación (255) de entrega, eDELIVERY, con la lista de receptores. En la parte del usuario receptor (215) se realiza un procedimiento de detección de nueva entrega (265) y se prepara la respuesta de aceptación de notificación (270) por parte del usuario receptor (215), que procede al envío de reconocimiento y aceptación de la nueva notificación (275), en respuesta a lo que el proveedor (210) invoca la función de añadir a la lista de receptores (280) cada usuario receptor (215) que acepta la notificación.

La Figura 3 muestra las funciones y procedimientos que se realizan en el protocolo de intercambio de datos después del primer vencimiento (V1) y antes del segundo vencimiento (V2) que determina el plazo para que el remitente finalice la entrega. En el protocolo el usuario emisor (300) actúa con un dispositivo del usuario emisor (305) y el usuario receptor (315) con un dispositivo del usuario receptor (320), ambos teniendo una relación de interacción (325) dispositivo-usuario con la app de notificaciones. El proveedor (310) del servicio de notificaciones que usa contratos inteligentes de blockchain o cadena de bloques (330) se comunica con las partes emisoras y receptoras mediante la interfaz de comunicación (335) que tiene con la blockchain. El usuario emisor (300) realiza, antes del primer vencimiento (V1) y, por ende, antes del segundo vencimiento (V2), la acción de listado (340) con todos los usuarios que han aceptado la notificación en curso. Por cada receptor, el usuario emisor (300) realiza un procedimiento de cálculo de la respuesta (345) a cada receptor para que pueda obtener el mensaje a entregar y, tras ello, procede al envío de la respuesta (350) calculada para cada usuario con notificación aceptada. El proveedor (310) se encarga de invocar la función de comprobación (360) de la corrección de las respuestas calculadas por el emisor (300), de acuerdo con los compromisos de emisión de claves y posterior actualización de los datos para cada usuario en la blockchain. La función de obtención (370) por parte del dispositivo receptor (320) de la respuesta generada por el emisor (300) con la que el usuario

receptor (315) puede tener acceso al mensaje se realiza ya después del segundo vencimiento (V2), i.e., una vez que el remitente da por finalizada la entrega.

En una implementación preferida, pero que no limita la invención, el proveedor (110, 210, 310) proporciona el servicio de notificación o entrega certificada a través de un contrato inteligente desplegado sobre una red blockchain o de cadena de bloques (130, 230, 330), por ejemplo, pudiéndose tratar de una red Ethereum u otra red que ofrece las prestaciones de ejecución de contratos inteligentes como las descritas anteriormente. Dicho proveedor (110, 210, 310) utiliza una interfaz de comunicación (135, 235, 335) con la cadena de bloques, que puede ser la interfaz web3 o similar. El “smart contract” o contrato inteligente desplegado (140) puede crear nuevos contratos inteligentes específicos para la gestión de cada uno de los envíos después de la invocación por parte de los remitentes.

El usuario emisor (100, 200, 300) interacciona (125, 225, 325) con la aplicación distribuida de notificaciones y entregas certificadas mediante un dispositivo de acceso del usuario emisor (105, 205, 305), que puede tratarse de un ordenador, teléfono inteligente, tableta, etc. Dicha aplicación puede ser una aplicación para un dispositivo de escritorio o para un dispositivo portátil con diferentes sistemas operativos (Windows, OSX, Android, iOS,…) y una aplicación programada en lenguajes de programación diversos, como por ejemplo Java, C#, Javascript, etc., y con una unidad de almacenamiento, como por ejemplo una base de datos, etc.

El usuario o usuarios receptores (115, 215, 315) interacciona (125, 225, 325) con la anteriormente mencionada aplicación mediante un dispositivo de acceso de usuario receptor (120, 220, 320) que igualmente puede tratarse de un ordenador, teléfono inteligente, tableta, etc. Dicha aplicación puede ser una aplicación para un dispositivo de escritorio o para un dispositivo portátil con diferentes sistemas operativos (Windows, OSX, Android, iOS,…) y una aplicación programada en lenguajes de programación diversos como Java, C#, Javascript, etc., y con una unidad de almacenamiento como por ejemplo una base de datos, etc.

Todos los actores interactúan con la red blockchain utilizando la interfaz de comunicación (135, 235, 335), por ejemplo, web3, implementada en su parte de aplicación distribuida de notificaciones y entregas certificadas.

La ejecución de la aplicación se puede desglosar en cuatro etapas diferentes, que son las siguientes y se explican más en detalle a continuación:

- Acciones iniciales.
- Acciones previas al primer vencimiento (V1).
- Acciones realizadas entre el primer vencimiento (V1) y el segundo vencimiento (V2).
- Acciones posteriores al segundo vencimiento (V2).

1) Acciones Iniciales:

Las acciones iniciales son aquellas que son independientes de una entrega o notificación concreta. Estas acciones se llevan a cabo una vez y sus resultados son aplicables a un conjunto de entregas o notificaciones.

Estas acciones iniciales pueden organizarse en las siguientes fases:

- Despliegue (240) del contrato inteligente principal o factoría para contratos inteligentes del servicio de notificaciones y entregas certificadas, representado en la Figura 2.
- Este contrato inteligente permite la creación de los contratos específicos que gestionan cada notificación o entrega.
- Determinación de los valores de los parámetros públicos usados en las funciones matemáticas y criptográficas utilizadas en el servicio.
- Acción, por parte de cada usuario, de envío de información necesaria para darse de alta (245) en el servicio/sistema, registrando en el sistema las direcciones públicas usadas por los usuarios en la red de cadena de bloques.

2) Acciones previas al primer vencimiento (V1), representadas en la Figura 2:

Las acciones de esta etapa se realizan por cada entrega o notificación. De acuerdo con el protocolo las acciones de esta segunda etapa pueden organizarse en las siguientes fases:

- Preparación (250) de una nueva notificación o entrega, con la generación de claves de notificación, determinación de vencimientos y cifrado, por parte del emisor, del mensaje o datos a entregar. La preparación de la entrega (250) se realiza de la siguiente manera:
    1. En caso necesario, el mensaje se fragmenta en partes de longitud menor y fija.
    2. El usuario emisor (100, 200, 300) genera una clave privada de notificación y calcula la clave pública. En una implementación preferida, pero que no limita la invención, este par de claves se generará utilizando el criptosistema de ElGamal.
    3. El emisor (100, 200, 300) genera aleatoriamente el elemento a utilizar para el

cifrado de ElGamal. Este elemento se mantendrá en secreto. En la implementación preferida, puede utilizarse el elemento directamente en un cifrado del ElGamal o puede generarse una cadena de elementos de cifrado pseudoaleatorios a partir de su hash.

4. Cifrado del mensaje utilizando la clave privada de notificación de emisor y el elemento secreto generado en el paso anterior.

- Invocación de la función de creación (255) del nuevo contrato inteligente que gestiona la entrega al receptor o lista de receptores (115, 215, 315). Acceso al contrato inteligente principal del sistema por parte del usuario emisor (100, 200, 300). Despliegue automático del contrato inteligente que gestiona el intercambio (260) y ejecución, sobre el contrato inteligente desplegado en este paso, y por parte del emisor (100, 200, 300), de la función de envío del mensaje cifrado utilizando un elemento o parámetro de cifrado. Esta función tiene como parámetros: el mensaje cifrado, el receptor o conjunto de receptores, la clave pública de notificación del emisor y los valores de los vencimientos (V1, V2) que determinan los períodos de aceptación y finalización.
- Procedimiento de detección (265) de nueva entrega/notificación y acceso del usuario o de los usuarios receptores (115, 215, 315) al contrato inteligente desplegado en el paso anterior.
- Por cada uno de los receptores (115, 215, 315) de la entrega/notificación, preparación de la respuesta de aceptación (270) que representa el reconocimiento de la nueva entrega. En una implementación preferida, que no limita la invención, y que utiliza una prueba de conocimiento nulo, se procede a la creación de las claves de notificación, un reto y el cifrado de su clave privada de notificación, como sigue:
    1. Generación del par de claves de notificación del receptor, utilizando, por ejemplo ElGamal.
    2. Generación del reto que se utiliza en la prueba de conocimiento nulo.
    3. Cifrado de la clave privada de notificación del receptor con la clave pública de notificación del emisor.
- Por cada uno de los receptores (115, 215, 315) que quiere seguir adelante con la notificación, aceptación (275) de la nueva entrega en el periodo establecido por el primer vencimiento (V1), y envío del reto y de la clave cifrada generados en la fase anterior.
- Determinación, por parte del contrato inteligente, del conjunto de los receptores con los que se va a finalizar el intercambio, mediante una función de adición (280) de un

usuario receptor a la lista de receptores que aceptan la notificación. El contrato inteligente registra el estado de los receptores que, antes del vencimiento, han aceptado la notificación. Para cada receptor del conjunto, el contrato inteligente registra el valor del reto, la clave pública de notificación y la clave cifrada.

3) Acciones realizadas entre el primer vencimiento (V1) y el segundo vencimiento (V2):

Después del primer vencimiento (V1), para cada receptor del conjunto que ha aceptado la entrega o notificación, se continuará con las fases ilustradas en la Figura 3:

- Obtención, por parte del emisor (100, 200, 300), del listado de receptores (340) que ha aceptado la notificación en curso.
- Para cada receptor del conjunto anterior, obtención de la clave privada de notificación del receptor, descifrando el elemento registrado en el contrato inteligente.
- Procedimiento de cálculo de la respuesta a cada receptor para que pueda obtener el mensaje. En una implementación preferida, que no limita la invención, para cada receptor del conjunto anterior, preparación (345), por parte del emisor (100, 200, 300), de la respuesta al reto, consistente en una prueba de conocimiento nulo. El emisor (100, 200, 300) prepara y envía, en el periodo establecido, la respuesta al reto utilizando la clave de notificación del receptor, el reto y el elemento secreto de cifrado del mensaje, generado en el paso de preparación de la nueva notificación/entrega (250).
- Envío de las respuestas (350) con la información para que cada receptor pueda descifrar el mensaje, a cada usuario con notificación/entrega aceptada.
- Acceso del usuario emisor (100, 200, 300) al contrato inteligente específico desplegado en el paso de intercambio (260), introduciendo los datos necesarios para la finalización del intercambio, incluyendo datos para que el contrato inteligente valide la respuesta al reto mediante una prueba de conocimiento nulo. En una implementación preferida, pero que no limita la invención puede utilizarse una prueba de conocimiento nulo basada en ElGamal mediante el uso de sumas y exponenciaciones modulares.
- Función de comprobación (360) de la corrección de las respuestas del emisor de acuerdo con los compromisos de emisión de claves y posterior actualización de los datos para cada usuario de la blockchain. Para ello, en la implementación preferida, se realiza una verificación por parte del contrato inteligente de los datos aportados por el emisor mediante una prueba de conocimiento nulo, de modo que le permita asegurar

que el receptor tiene acceso al elemento de cifrado y por tanto al mensaje. El contrato inteligente no puede acceder al mensaje por lo que éste permanece como confidencial. Determinación del estado final del intercambio: los receptores que hayan aceptado el intercambio pasan al estado finalizado mientras que el resto pasa al estado rechazado. Si la verificación de los datos aportados por el emisor es negativa, el smart contract actualiza el estado del envío a cancelado.

4) Acciones posteriores al segundo vencimiento (V2).

Después del segundo vencimiento (V2), solamente es necesario realizar el acceso de los receptores al mensaje, representado en la Figura 3.

- Ejecución de la función de obtención (370), por parte de cada receptor, de la respuesta del emisor para poder tener acceso al mensaje. En caso de finalización del intercambio, cada receptor del conjunto de receptores que han aceptado la notificación descifra el mensaje a partir de los datos aportados por el contrato inteligente. Si la finalización no ha sido correcta por parte del emisor (100, 200, 300), los receptores obtienen una evidencia de cancelación del envío.

REIVINDICACIONES

1. Un método para notificaciones y entregas certificadas de mensajes, donde un proveedor (110, 210, 310) proporciona un servicio de notificación o entrega certificada a través de al menos un contrato inteligente desplegado sobre una red de cadena de bloques (130, 230, 330) entre un usuario emisor (100, 200, 300) y al menos un usuario receptor (115, 215, 315) que interaccionan (125, 225, 325) con el servicio de notificación o entrega certificada mediante un dispositivo de acceso de usuario emisor (105, 205, 305) y un dispositivo de acceso de usuario receptor (120, 220, 320) respectivamente, y donde el usuario emisor (100, 200, 300), el, al menos un, usuario receptor (115, 215, 315) y el proveedor (110, 210, 310) interactúan con la red de cadena de bloques (130, 230, 330) utilizando una interfaz de comunicación (135, 235, 335);

   el método **caracterizado por que** comprende:

   - desplegar (140), por el proveedor (110, 210, 310) un contrato inteligente principal;
   - enviar información por el usuario emisor (100, 200, 300) y por cada usuario receptor (115, 215, 315) para darse de alta (245) como usuario en el servicio:
   - preparar (250), por el usuario emisor (100, 200, 300), una notificación o entrega de un mensaje;
   - para cada notificación o entrega preparada, acceder por el usuario emisor (100, 200, 300) al contrato inteligente principal para crear (255) un contrato inteligente específico de la notificación o entrega que gestiona la notificación o entrega certificada del mensaje a intercambiar (260) entre el usuario emisor (100, 200, 300) y cada usuario receptor (115, 215, 315), donde el contrato inteligente específico comprende un conjunto de receptores que contiene cada usuario receptor (115, 215, 315) y al menos un primer vencimiento (V1) que define un umbral de tiempo límite superior dado al conjunto de receptores para aceptar la notificación o entrega por cada usuario receptor (115, 215, 315) del conjunto;
   - para cada notificación o entrega preparada, detectar (265) por cada usuario receptor (115, 215, 315) la notificación o entrega y acceder por cada usuario receptor (115, 215, 315) al contrato inteligente específico de la notificación o entrega detectada;

- por cada usuario receptor (115, 215, 315) del conjunto, preparar una respuesta de aceptación (270) que representa un reconocimiento de la notificación o entrega detectada;
- añadir (280) por el proveedor (210) a un subconjunto de receptores cada usuario receptor (115, 215, 315) del conjunto que envía la respuesta de aceptación (275) preparada antes del primer vencimiento (V1);
- acceder (340) al subconjunto de receptores por el usuario emisor (100, 200, 300) y, para cada usuario receptor (115, 215, 315) del subconjunto,
  - calcular por el usuario emisor (100, 200, 300) una respuesta (345), la respuesta comprendiendo información para habilitar a cada usuario receptor (115, 215, 315) del subconjunto a leer el mensaje, y
  - enviar la respuesta (350) calculada por el usuario emisor (100, 200, 300) al proveedor (310);
- comprobar (360) por el proveedor (310) la corrección de las respuestas enviadas por usuario emisor (100, 200, 300), y establecer un estado final del intercambio que se selecciona entre estado de finalización, si la comprobación (360) determina que las respuestas enviadas son correctas, y estado de cancelación, en caso contrario;
  - en caso de que el estado final del intercambio establecido por el proveedor (310) es estado de finalización, cada usuario receptor (115, 215, 315) del subconjunto que ha aceptado la notificación o entrega obtiene (370) la respuesta (350) calculada por el usuario emisor (100, 200, 300) para leer el mensaje;
  - en caso de que el estado final del intercambio establecido por el proveedor (310) es estado de cancelación, cada usuario receptor (115, 215, 315) del subconjunto que ha aceptado la notificación o entrega obtiene (370) unas evidencias de cancelación de la notificación o entrega.

2. El método de acuerdo con la reivindicación 1, **caracterizado por que** la cadena de bloques tiene almacenado el mensaje que es público, el usuario emisor (100, 200, 300) y el contrato inteligente específico publica el mensaje o un resumen criptográfico del mensaje.
3. El método de acuerdo con la reivindicación 1, **caracterizado por que** preparar (250) la notificación o entrega comprende generar, por el usuario emisor (100, 200, 300), información para cifrar el mensaje, que es confidencial.
4. El método de acuerdo con la reivindicación 3, **caracterizado por que** la información

para cifrar el mensaje se genera mediante un cifrado de ElGamal.

5. El método de acuerdo con cualquiera de las reivindicaciones 3-4, **caracterizado por que** preparar (250) la notificación o entrega comprende generar, por el usuario emisor (100, 200, 300), una clave privada de notificación de emisor y una clave pública de emisor, y un elemento secreto, donde la clave privada de notificación de emisor y el elemento secreto se utilizan para cifrar el mensaje.

6. El método de acuerdo con cualquiera de las reivindicaciones 3-5, **caracterizado por que** el contrato inteligente específico además comprende el mensaje cifrado.

7. El método de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** preparar (250) la notificación o entrega además comprende fragmentar el mensaje.

8. El método de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** comprobar (360) la corrección de las respuestas enviadas por el usuario emisor (100, 200, 300) comprende verificar por el proveedor (310) el contrato inteligente específico accedido por el usuario emisor (100, 200, 300) mediante una prueba de conocimiento nulo.

9. El método de acuerdo con la reivindicación 8, **caracterizado por que** la información la prueba de conocimiento nulo está basada en un cifrado de ElGamal.

10. El método de acuerdo con cualquiera de las reivindicaciones 8-9 **caracterizado por que** preparar una respuesta de aceptación (270) por cada usuario receptor (115, 215, 315) comprende generar una clave privada de notificación de receptor y una clave pública de receptor y un reto por dicho usuario receptor (115, 215, 315) para realizar la prueba de conocimiento nulo, y cifrar la clave privada de notificación de receptor con una clave pública de notificación del emisor generada por el usuario emisor (100, 200, 300) al preparar (250) la notificación o entrega.

11. El método de acuerdo con la reivindicación 10, **caracterizado por que** además comprende enviar, por cada uno de los usuarios receptores (115, 215, 315) del subconjunto que ha aceptado la notificación o entrega, el reto y la clave cifrada del receptor.

12. El método de acuerdo con la reivindicación 11, **caracterizado por que,** en caso de que el estado final del intercambio establecido por el proveedor (310) es estado de finalización, obtener (370) por cada uno de los usuarios receptores (115, 215, 315) del subconjunto la respuesta comprende recibir unos parámetros que son el reto, la clave cifrada del receptor y un elemento secreto generado por el usuario emisor (100, 200, 300) al preparar (250) la notificación o entrega, parámetros que se usan para leer el

mensaje.

13. El método de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** el contrato inteligente específico además comprende un segundo vencimiento (V2) que define un umbral de tiempo límite superior dado al usuario emisor (100, 200, 300) para finalizar la notificación o entrega y a partir del que se habilita al subconjunto de receptores que han aceptado la notificación o entrega a leer el mensaje, en caso de que el estado final del intercambio establecido por el proveedor (310) es estado de finalización, o a obtener las evidencias de cancelación de la notificación o entrega, en caso de que el estado final del intercambio establecido por el proveedor (310) es estado de cancelación.

14. El método de acuerdo con la reivindicación 13, **caracterizado por que** obtener (370) por cada uno de los usuarios receptores (115, 215, 315) del subconjunto la respuesta enviada por el emisor (100, 200, 300) se realiza ya después del segundo vencimiento (V2).

15. El método de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** enviar información para dar de alta (245) comprende registrar unas direcciones públicas usadas por el usuario emisor (100, 200, 300) y cada usuario receptor (115, 215, 315) en la red de cadena de bloques (130, 230, 330).

16. El método de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** la red de cadena de bloques (130, 230, 330) es una red Ethereum.

17. El método de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** la interfaz de comunicación (135, 235, 335) es una interfaz web3.

18. El método de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** el dispositivo de acceso de usuario emisor (105, 205, 305) y el dispositivo de acceso de usuario receptor (120, 220, 320) se seleccionan entre un ordenador, un teléfono inteligente y una tableta.

19. El método de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** el mensaje es un texto de un contrato a firmar y el contrato inteligente principal es creado por un usuario firmante proponedor, y donde

uno o más usuarios firmantes diferentes del usuario firmante proponedor seleccionan, mediante una función de aceptación provista en el contrato inteligente principal, entre aceptar o no aceptar firmar el contrato antes del primer vencimiento (V1); y

el usuario firmante proponedor finaliza la firma del contrato, después del primer vencimiento (V1) y antes del segundo vencimiento (V2), si y sólo si todos los

usuarios firmantes diferentes del usuario firmante proponedor aceptan firmar el contrato antes del primer vencimiento (V1) y, si no, cancela la firma del contrato para todos los usuarios firmantes.

5

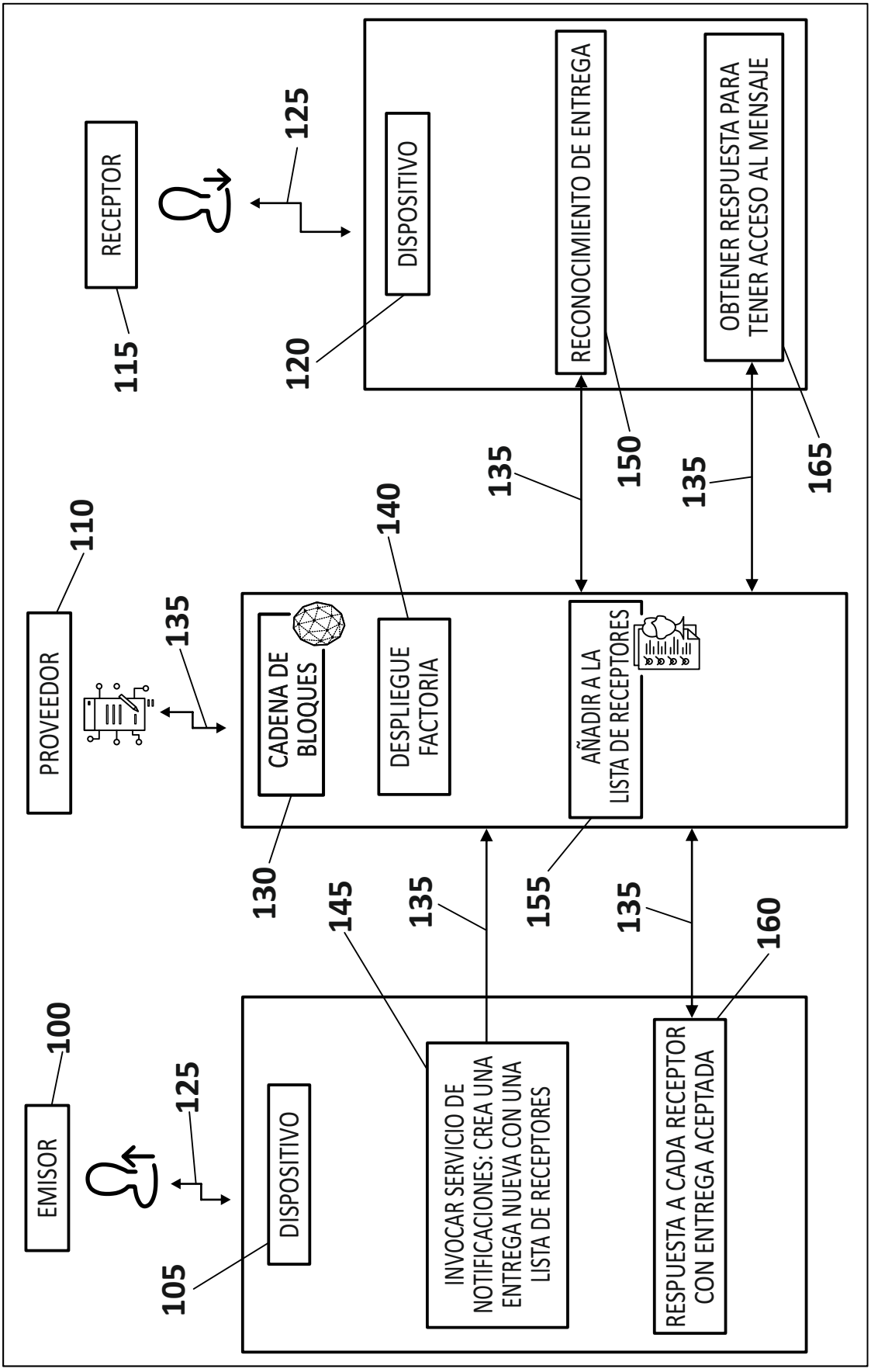
EMISOR
100
DISPOSITIVO
105
125
INVOCAR SERVICIO DE NOTIFICACIONES: CREA UNA ENTREGA NUEVA CON UNA LISTA DE RECEPTORES
RESPUESTA A CADA RECEPTOR CON ENTREGA ACEPTADA
PROVEEDOR
110
135
CADENA DE BLOQUES
130
DESPLIEGUE FACTORIA
140
AÑADIR A LA LISTA DE RECEPTORES
145
135
155
135
160
RECEPTOR
115
125
DISPOSITIVO
120
RECONOCIMIENTO DE ENTREGA
150
OBTENER RESPUESTA PARA TENER ACCESO AL MENSAJE
135
165

FIG. 1

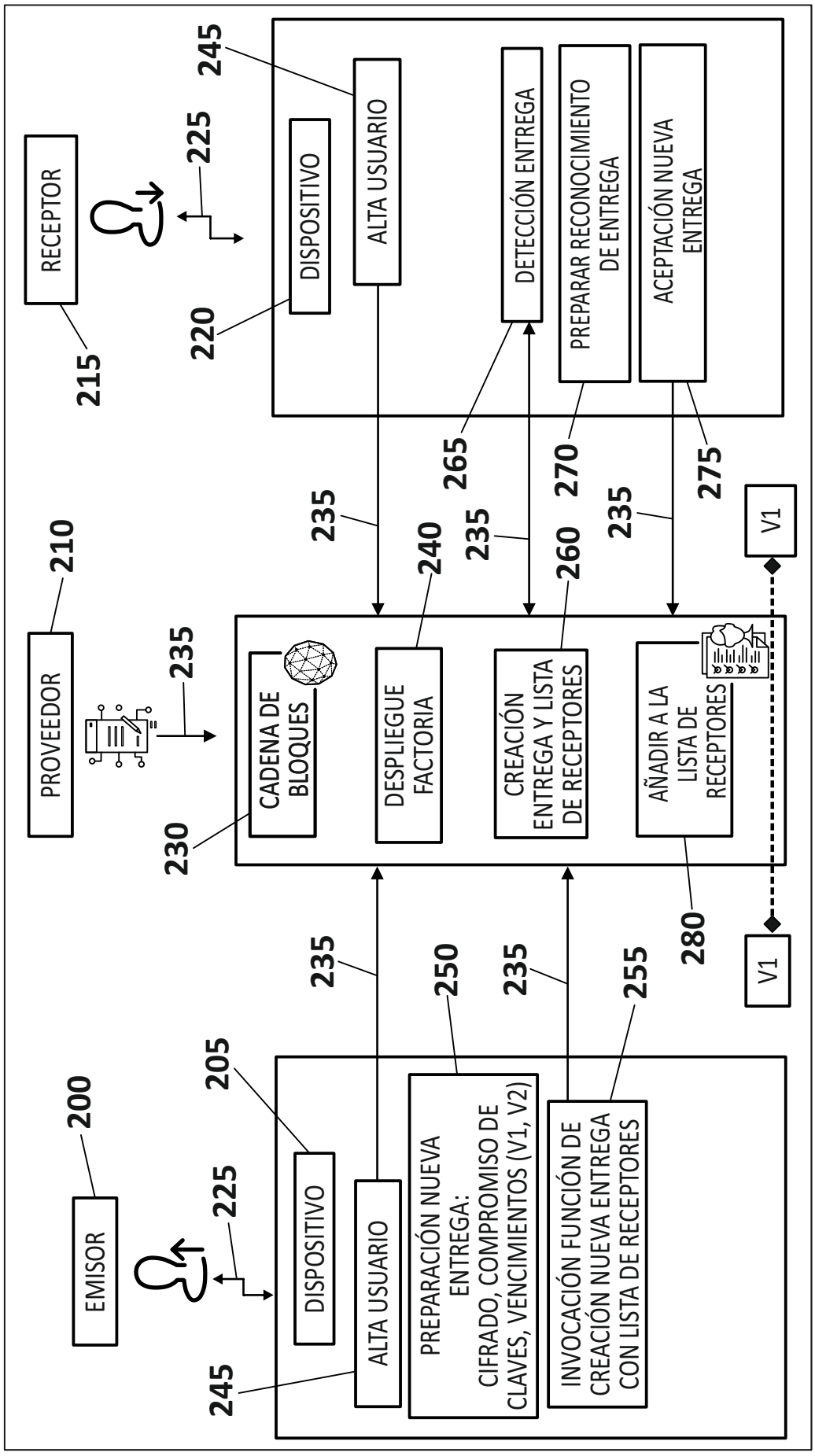
RECEPTOR
215
225
220
DISPOSITIVO
ALTA USUARIO
245
DETECCIÓN ENTREGA
PREPARAR RECONOCIMIENTO DE ENTREGA
ACEPTACIÓN NUEVA ENTREGA
265
270
275
235
240
260
PROVEEDOR
210
CADENA DE BLOQUES
DESPLIEGUE FACTORIA
CREACIÓN ENTREGA Y LISTA DE RECEPTORES
AÑADIR A LA LISTA DE RECEPTORES
230
V1
280
EMISOR
200
205
DISPOSITIVO
ALTA USUARIO
PREPARACIÓN NUEVA ENTREGA: CIFRADO, COMPROMISO DE CLAVES, VENCIMIENTOS (V1, V2)
INVOCACIÓN FUNCIÓN DE CREACIÓN NUEVA ENTREGA CON LISTA DE RECEPTORES
250
255

FIG. 2

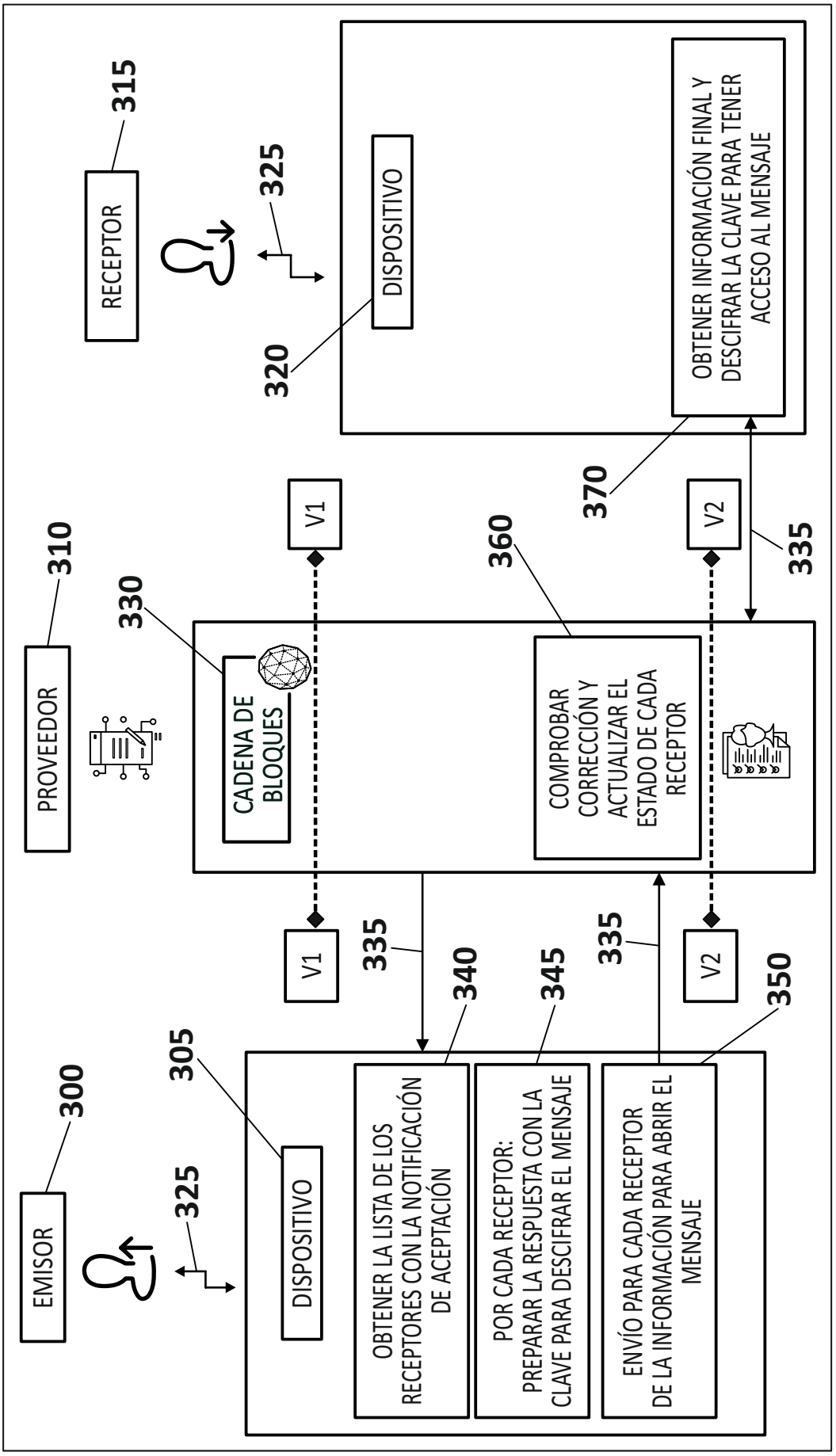
EMISOR
300
DISPOSITIVO
305
325
OBTENER LA LISTA DE LOS RECEPTORES CON LA NOTIFICACIÓN DE ACEPTACIÓN
340
POR CADA RECEPTOR: PREPARAR LA RESPUESTA CON LA CLAVE PARA DESCIFRAR EL MENSAJE
345
ENVÍO PARA CADA RECEPTOR DE LA INFORMACIÓN PARA ABRIR EL MENSAJE
350
335
V1
V2
PROVEEDOR
310
330
CADENA DE BLOQUES
360
COMPROBAR CORRECCIÓN Y ACTUALIZAR EL ESTADO DE CADA RECEPTOR
370
RECEPTOR
315
320
DISPOSITIVO
325
OBTENER INFORMACIÓN FINAL Y DESCIFRAR LA CLAVE PARA TENER ACCESO AL MENSAJE

FIG. 3

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201930642

(22) Fecha de presentación de la solicitud: 10.07.2019

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L9/06*** (2006.01)
G06F16/00 (2019.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
A	PAYERAS-CAPELLA MAGDALENA et al. Smart Contract for Multiparty Fair Certified Notifications. 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW), 20181127 IEEE. , 27/11/2018, Páginas 459 - 465, <DOI: 10.1109/CANDARW.2018.00089>. Todo el documento.	1-19
A	XU YANG et al. A Blockchain-Based Nonrepudiation Network Computing Service Scheme for Industrial IoT. IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, 20190601 IEEE SERVICE CENTER, NEW YORK, NY, US. , 01/06/2019, Vol. 15, Páginas 3632 - 3641, ISSN 1551-3203, <DOI: 10.1109/TII.2019.2897133>. Todo el documento.	1-19
A	US 2009094452 A1 (SHAO JUN et al.) 09/04/2009, Todo el documento.	1-19
A	HASAN HAYA R et al. Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts. IEEE Access IEEE, USA. , 30/11/0002, Vol. 6, Páginas 65439 - 65448, <DOI: 10.1109/ACCESS.2018.2876971>. Todo el documento	1-19

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

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
24.09.2019	M. Muñoz Sanchez	1/2

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

H04L, G06F

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

INVENES, EPODOC, WPI, NPL, XPIEE, XPI3E