(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 006 025**

(51) Int. Cl.:

H04L 9/32 (2006.01)
H04L 9/08 (2006.01)
H04L 9/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.12.2019 PCT/US2019/065524**

(87) Fecha y número de publicación internacional: **18.06.2020 WO20123538**

(96) Fecha de presentación y número de la solicitud europea: **10.12.2019 E 19856488 (2)**

(97) Fecha y número de publicación de la concesión europea: **13.11.2024 EP 3895372**

(54) Título: **Uso de protocolos de cadena de bloques virtuales para implementar un intercambio electrónico justo**

(30) Prioridad:

10.12.2018 US 201862777410 P
12.12.2018 US 201862778482 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.03.2025

(73) Titular/es:

ALGORAND LABS S.R.L. (100.00%)
Via Di San Nicola Da Tolentino 67
00187 Rome, IT

(72) Inventor/es:

MICALI, SILVIO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Uso de protocolos de cadena de bloques virtuales para implementar un intercambio electrónico justo

REFERENCIA CRUZADA A LAS SOLICITUDES RELACIONADAS

Esta solicitud reivindica el beneficio de la solicitud provisional estadounidense 62/777,410, presentada el 10 de diciembre de 2018 y de la solicitud provisional estadounidense 62/778,482, presentada el 12 de diciembre de 2018.

CAMPO TÉCNICO

Esta descripción se refiere en general al uso de protocolos de cadena de bloques virtuales para implementar un intercambio electrónico justo (FEE).

ANTECEDENTES

Un registro público es una secuencia de datos a prueba de manipulaciones que puede leerse y aumentarse. Los registros públicos compartidos pueden revolucionar la forma en que funciona una sociedad moderna. Las transacciones tradicionales, tales como los pagos, las transferencias de activos y la titularidad, pueden garantizarse en el orden en que se producen. Se pueden habilitar nuevas transacciones, tales como las criptomonedas y los contratos inteligentes. Puede reducirse la corrupción, eliminarse los intermediarios y puede introducirse un nuevo paradigma de confianza. La publicación «Digital Contract Using Block Chaining and Elliptic Curve Based Digital Signature» de KALAMSYAH SONY ADAN ET AL, publicada en 2018

6TH INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATION

TECHNOLOGY (ICOICT), IEEE, págs. 435-440, propone un método de implementación de un testigo que usa cadenas de bloques. Dado que los acuerdos convencionales usan solamente firmas digitales, el remitente de los documentos del contrato puede autenticarse, pero sigue existiendo el problema porque ambas partes no pueden realizar una autenticación mutua y esto no puede resolver una disputa legal. Por lo tanto, se requería un testigo para superar los problemas cuando se producía una disputa legal. Para implementar el testigo, se propone un encadenamiento de bloques. Se han propuesto varios trabajos para realizar la autenticación y uno de ellos es el uso de RSA propuesto por Raji et al. Dado que el RSA necesita una gran complejidad, en esta investigación se proponen entonces la ECC y el ECDSA. Se propone la ECC y el ECDSA puesto que tienen menos complejidad que el RSA. Según el resultado del experimento, se demuestra que la disputa legal puede resolverse y que el nivel de seguridad del método propuesto es superior al de RSA. Mientras tanto, la complejidad del ECDSA es menor que la de la firma digital basada en RSA. El documento WO 2018/200215 A1 propone un método de combinación de múltiples interacciones en una única entrada de registro. Puede crearse un paquete de datos que represente un conjunto de interacciones y cada entidad asociada a una interacción puede revisar el paquete de datos. Cada entidad puede indicar un acuerdo con las interacciones firmando digitalmente el paquete de datos. Una vez firmado por cada entidad implicada, el paquete de datos puede ser almacenado en un registro tal como una cadena de bloques.

Sin embargo, los registros públicos tradicionales no alcanzan su potencial. Los registros públicos tradicionales pueden depositar toda la confianza en una única entidad, que puede denegar arbitrariamente la publicación de los pagos realizados con las claves dadas y es vulnerable a un ciberataque. De hecho, una vez que la autoridad central única se ve comprometida, también lo está todo el sistema. Algunos sistemas tradicionales son caros de ejecutar, desperdician recursos de cálculo y otros recursos valiosos, concentran el poder en manos de nuevas entidades (mineros), presentan una ambigüedad considerable (bifurcaciones) y tienen una latencia prolongada y un rendimiento reducido. Otras implementaciones tradicionales están autorizadas o asumen la capacidad de penalizar a los usuarios maliciosos, o ambas cosas, y/o confían en que algún subconjunto de usuarios sea inmune a los ciberataques durante un tiempo suficientemente largo.

COMPENDIO

Las realizaciones en esta invención se refieren a métodos, sistemas y aparatos para implementar protocolos de cadena de bloques virtuales, como se define en las reivindicaciones independientes. Un primer dispositivo informático genera una clave pública y una clave privada correspondiente. La clave pública está destinada a transmitir un mensaje de un remitente a un destinatario. El primer dispositivo informático está asociado al remitente. El primer dispositivo informático encripta el mensaje usando la clave pública y una clave criptográfica del destinatario para generar una primera carga útil de datos. La clave criptográfica del destinatario indica una identidad del destinatario. El primer dispositivo informático firma un paquete de datos usando una clave criptográfica del remitente para generar una segunda carga útil de datos. La clave criptográfica del remitente indica una identidad del remitente. El paquete de datos incluye la identidad del remitente, la identidad del destinatario, la clave pública y una función de creación de códigos de comprobación de la primera carga útil de datos.

El primer dispositivo informático transmite la primera carga útil de datos y la segunda carga útil de datos a un segundo dispositivo informático asociado al destinatario. El primer dispositivo informático recibe una versión firmada de la segunda carga útil de datos del segundo dispositivo informático. La versión firmada de la segunda carga útil de datos

se firma mediante el uso de la clave criptográfica del destinatario. El primer dispositivo informático determina que la versión firmada de la segunda carga útil de datos se ha publicado en una cadena de bloques. En respuesta a la determinación de que la versión firmada de la segunda carga útil de datos se ha publicado en la cadena de bloques, el primer dispositivo informático publica la clave privada en la cadena de bloques para que el destinatario desencripte el mensaje criptográfico.

Los beneficios y ventajas de las realizaciones descritas en esta invención incluyen un esfuerzo de cálculo reducido en comparación con otras técnicas. La cadena de bloques permanece en segundo plano y se usa muy raramente, si es que se usa, en la ejecución del protocolo de cadena de bloques virtuales. Cuando se implementa un intercambio electrónico justo (FEE) usando el protocolo de cadena de bloques virtuales, el protocolo proporciona transacciones equitativas desde el punto de vista comercial realizadas por partes honestas sin el uso de la cadena de bloques. Una parte se considera «honesta» si la parte no intenta obtener un beneficio de una transacción a expensas de la otra parte. Por otro lado, si una primera parte recibe el beneficio de una transacción y una segunda parte no, la segunda parte puede invocar la cadena de bloques para restablecer la equidad comercial de la transacción.

El protocolo de cadena de bloques virtuales proporciona un intercambio equitativo desde el punto de vista comercial de una manera más eficiente y económica en comparación con otras técnicas. La cadena de bloques interviene muy raramente en el protocolo de cadena de bloques virtuales. Cuando ambas partes son honestas, la transacción se lleva a cabo fuera de la cadena. La cadena de bloques se usa únicamente cuando se produce una transacción comercialmente inequitativa, para restablecer la equidad comercial de la transacción. De hecho, se desaconseja la falta de cumplimiento puesto que las ventajas que se obtienen al incumplir se reducen en comparación con otras técnicas. Los costos de transacción se reducen en comparación con otras técnicas puesto que las partes realizan transacciones bilateralmente sin pasar por la cadena de bloques, evitando el pago de tarifas de transacción por publicar información en bloques y evitando la espera a que se genere un nuevo bloque.

Los criptoactivos y otras transacciones, tales como correo electrónico certificado o contratos firmados electrónicamente, pueden producirse en menos tiempo usando protocolos de cadena de bloques virtuales en comparación con otras técnicas y las transacciones se finalizan antes. Otros beneficios y ventajas incluyen la privacidad y la confidencialidad de las transacciones. Los protocolos de cadena de bloques virtuales pueden cumplir con un régimen regulatorio al que están sujetos para garantizar transacciones equitativas desde el punto de vista comercial. Los protocolos de cadena de bloques virtuales pueden reducir la necesidad de contratos inteligentes más complejos y costosos desde el punto de vista computacional.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La FIG. 1 ilustra un protocolo de cadena de bloques virtuales ejemplar.

La FIG. 2 ilustra un método para protocolos de cadena de bloques virtuales.

La FIG. 3 ilustra una máquina ejemplar.

DESCRIPCIÓN DETALLADA

A veces se recurre a un tercero de confianza para garantizar una transacción, por ejemplo, la transmisión de un correo electrónico certificado, la firma y la entrega de un contrato firmado electrónicamente o una transacción de criptoactivos. Sin embargo, una transacción donde participe un tercero de confianza puede resultar ineficaz o costosa ya que dicho tercero de confianza puede ralentizar la transacción y exigir una remuneración por sus servicios. Puede usarse una cadena de bloques en lugar de un tercero de confianza en ciertos entornos a un costo reducido. Sin embargo, una cadena de bloques también puede generar costos en términos de tiempo de procesamiento y restricciones monetarias. Las realizaciones descritas en esta invención proporcionan protocolos de cadena de bloques virtuales para implementar un intercambio electrónico justo (FEE). Un FEE representa un conjunto de transacciones que incluye el correo electrónico certificado, la firma electrónica de contratos y otras implementaciones.

Un protocolo de cadena de bloques virtuales es aquel que se puede usar para completar de forma segura una transacción entre dos partes en presencia de una cadena de bloques, de modo que la cadena de bloques no se use cuando ambas partes sean honestas y ninguna de las partes incurra en un gasto adicional. Si una primera parte no es honesta, el protocolo de cadena de bloques virtuales usa mínimamente la cadena de bloques, de modo que la segunda parte no esté en desventaja. Por consiguiente, un protocolo de cadena de bloques virtuales es aquel donde la cadena de bloques funciona en segundo plano y no se invoca a menos que una de las partes actúe de manera inequitativa desde el punto de vista comercial.

La FIG. 1 ilustra un protocolo de cadena de bloques virtuales ejemplar. La ilustración de la FIG. 1 incluye un remitente 112, un dispositivo informático 104, un destinatario 116, un dispositivo informático 108 y una cadena de bloques 120. El remitente 112 es una entidad que desea transmitir un mensaje M al destinatario 116 para realizar una transacción, tal como la transmisión de un correo electrónico certificado o una transacción de criptoactivos. Por ejemplo, el remitente 112 puede representar una cuenta de criptoactivos, una empresa, una universidad o una sola persona, etc. El dispositivo informático 104 está acoplado de manera comunicativa al remitente 112 y puede ser un teléfono inteligente, una tableta, un ordenador portátil u otro dispositivo informático implementado usando los componentes ilustrados y

descritos con más detalle con referencia a la FIG. 3. El destinatario 116 es una entidad a la que está destinado el mensaje M. Por ejemplo, el remitente 116 puede representar una cuenta de criptoactivos, una empresa, una universidad o una sola persona, etc. El dispositivo informático 108 está acoplado de manera comunicativa al remitente 116 y puede ser un teléfono inteligente, una tableta, un ordenador portátil u otro dispositivo informático implementado usando los componentes ilustrados y descritos con más detalle con referencia a la FIG. 3.

Los dispositivos informáticos 104, 108 usan un protocolo de cadena de bloques virtuales para transmitir el mensaje M del remitente 112 al destinatario 116. El protocolo de cadena de bloques virtuales permite transacciones bilaterales, tales como las que se usan para implementar un FEE. Cuando el remitente 112 y el destinatario 116 son partes honestas, la cadena de bloques 120 no se usa de hecho para realizar la transacción. Una parte se considera «honesta» si la parte no intenta obtener un beneficio de una transacción a expensas de la otra parte. Por ejemplo, considérese un escenario donde el remitente 112 tiene un título de automóvil y el destinatario tiene una dirección electrónica de una cuenta de criptoactivos. Ninguna de las partes conoce inicialmente el activo de la otra, pero reconocerá que puede acceder al activo. Si el remitente 112 es «honesto», no intentará obtener la dirección electrónica de la cuenta de criptoactivos mientras no transmita el título de automóvil al destinatario.

El remitente 112 y el destinatario 116 pueden usar cada uno la cadena de bloques 120 una vez, para registrar información sobre sí mismos y luego pueden interactuar honestamente con otras partes honestas sin involucrar a la cadena de bloques 120. La información registrada puede incluir, por ejemplo, una clave criptográfica pública A del remitente 112 y una clave criptográfica pública B del destinatario 116. Las claves criptográficas públicas A, B también se denominan a veces claves públicas o claves de encriptado públicas. Una clave criptográfica puede ser una clave pública o una clave privada (secreta) que se usa para firmar digitalmente, encriptar o desencriptar datos, tales como un mensaje. Cuando una de las dos partes no es honesta, el protocolo de cadena de bloques virtuales resuelve el problema al permitir la publicación de información en la cadena de bloques 120, de modo que la parte honesta no esté en desventaja.

En algunas realizaciones, el protocolo de cadena de bloques virtuales permite que los bloques (por ejemplo, los bloques 124, 128) de la cadena de bloques 120 incorporen información de tiempo con un nivel de precisión particular. En otras realizaciones, como alternativa, el protocolo de cadena de bloques virtuales mide el tiempo en conjuntos de bloque. Por ejemplo, publicar la información Y en la cadena de bloques 120 dentro de un período de tiempo determinado desde la aparición del bloque 124 da como resultado la publicación de Y en uno de los 25 bloques siguientes al bloque 124, por ejemplo, el bloque 128.

El dispositivo informático 104 genera una clave pública P y una clave privada S correspondiente. La clave pública P está destinada a transmitir el mensaje M del remitente 112 al destinatario 116. El remitente 112 tiene su propio identificador único A, por ejemplo, una clave de encriptado pública, una clave de firma pública o una clave criptográfica pública. El remitente 112 también tiene su propia clave secreta o clave de desencriptado privada correspondiente. La clave criptográfica pública A del remitente 112 puede publicarse en la cadena de bloques 120 cuando el remitente 112 se inscribe en un determinado sistema, por ejemplo, un sistema de correo electrónico certificado. De manera similar, el destinatario 116 tiene un identificador único B, por ejemplo, una clave criptográfica pública. El remitente 112 puede firmar el mensaje M para generar un mensaje firmado indicado por $SIG_A(M)$. El remitente 112 puede encriptar el mensaje M para generar un mensaje encriptado indicado por $E_A(M)$.

El dispositivo informático 104 encripta el mensaje M usando la clave pública P y una clave criptográfica B del destinatario 116 para generar una primera carga útil de datos $Z = E_{PB}(A, B, M)$. La clave criptográfica B del destinatario 116 indica una identidad del destinatario 116. De hecho, cualquier usuario, por ejemplo, el destinatario 116, puede encriptar el mensaje M usando la clave criptográfica pública A del remitente 112, pero solamente el remitente 112 puede desencriptar $E_A(M)$ siempre que el remitente 112 tenga su clave de desencriptado privada correspondiente. Los métodos de firma digital y encriptado descritos en esta invención no son maleables y son seguros con respecto a CCA-2. La seguridad de CCA-2 se refiere a un estándar de indistinguibilidad de texto cifrado para la seguridad criptográfica. Es probable que los métodos de firma digital y encriptado descritos en esta invención sean descifrables sin revelar las claves de encriptado privadas. Por otra parte, los métodos de firma digital y encriptado descritos en esta invención son seguros frente a los ataques de mensajes elegidos adaptativos.

El encriptado descrito por las realizaciones descritas en esta invención se implementa en más de una fase. Por ejemplo, en una primera fase, el dispositivo informático 104 puede encriptar el mensaje M usando solamente la clave pública P para generar una carga útil de datos $E_P(A, B, M)$. En una segunda fase, el dispositivo informático 104 puede encriptar el mensaje M usando la clave pública P, así como una clave de un solo uso o temporal O para generar una carga útil de datos $E_{PO}(A, B, M)$. La clave temporal O se denomina a veces clave efímera. En algunas realizaciones, el encriptado del mensaje M usando la clave pública P incluye el encriptado de M en un criptosistema de clave privada usando una clave privada K y el encriptado de la K privada usando P.

En algunas realizaciones, los métodos de firma digital y encriptado descritos en esta invención implementan un encriptado conjunto. Por ejemplo, P indica una clave de encriptado pública y S indica una clave de desencriptado privada correspondiente. Continuando con el ejemplo, X indica otra clave de encriptado pública y Sx indica una clave secreta correspondiente de X. El dispositivo informático 104 puede calcular, a partir de P y X, una clave de encriptado pública «conjunta» PX, cuya clave secreta (privada) conjunta correspondiente incluye S y Sx. El encriptado del

mensaje M usando la clave de encriptado pública conjunta PX se indica por Z, donde Z = E_{PX}(M). Un mensaje encriptado de este tipo puede desencriptarse cuando un dispositivo informático puede acceder tanto a S como a Sx. Cuando Z = E_{PX}(M), PX indica una clave de encriptado pública y Sx indica una clave de desencriptado secreta correspondiente, el dispositivo informático 108 puede desencriptar conjuntamente (P, X, S, Sx, Z) para obtener el mensaje M. Los datos E_{PX}(M) permanecen seguros siempre que solamente el destinatario 116 tenga acceso a las claves secretas S y Sx. Cuando Z = E_{PX}(M) pero otra clave S' no es la clave de desencriptado secreta correspondiente a P, entonces los datos M' obtenidos mediante el desencriptado conjunto (P, X, S', Sx, Z) serán muy diferentes de los de M y pueden probarse sin revelar Sx.

Después de que el dispositivo informático 104 haya recibido el mensaje M del remitente 112, el dispositivo informático 104 genera el correspondiente par de encriptado público y secreto (privado) (P, S) y calcula los datos Z = E_{PB}(A, B, M), que indican un encriptado conjunto que usa P y la clave criptográfica pública B del destinatario 116. Z indica una primera carga útil de datos e identifica al remitente 112 por A y al destinatario 116 por B. En algunas realizaciones, la primera carga útil de datos Z incluye, por tanto, la clave criptográfica B del destinatario y la clave criptográfica A del remitente. La primera carga útil de datos Z no contiene S. La primera carga útil de datos Z excluye así la clave de desencriptado privada S que necesita el destinatario 116 para desencriptar la primera carga útil de datos E_{PB}(A, B, M) y acceder al mensaje M.

El dispositivo informático 104 firma un paquete de datos (A, B, P, t, H(Z)) usando la clave criptográfica A del remitente 112 para generar una segunda carga útil de datos Y. La clave criptográfica A del remitente 112 indica una identidad del remitente 112. Por tanto, el paquete de datos incluye la identidad del remitente 112, la identidad del destinatario 116, la clave pública P y una función de creación de códigos de comprobación H(Z) de la primera carga útil de datos Z. En algunas realizaciones, t indica un tiempo límite para que el remitente 112 o el destinatario 116 realicen una función de seguimiento. Por ejemplo, t puede indicar un tiempo límite para que el dispositivo informático 104 reciba una confirmación de recepción de la segunda carga útil de datos Y del segundo dispositivo informático 108. En otras realizaciones, t especifica un momento futuro después del cual el destinatario 116 no podrá restablecer la «equidad» de la transacción.

Un intercambio o transacción se considera «justo» si es equitativo desde el punto de vista comercial, de modo que una entidad maliciosa no se beneficia a expensas de una entidad no maliciosa. Continuando con el ejemplo anterior, donde el remitente 112 tiene un título de automóvil y el destinatario tiene una dirección electrónica de una cuenta de criptoactivos. Ninguna de las partes conoce inicialmente el activo de la otra, pero reconocerá que puede acceder al activo. En un protocolo de intercambio, se desea (pero no se garantiza) que las partes intercambien electrónicamente sus activos, es decir, que el remitente obtenga la dirección electrónica de la cuenta de criptoactivos y el destinatario 116 obtenga el título de automóvil. El protocolo de intercambio se denomina «justo» si (sin forzar un intercambio en contra de la voluntad de las partes) el protocolo establece que el destinatario 116 obtenga el título de automóvil si y solamente si el remitente 112 obtiene la dirección electrónica de la cuenta de criptoactivos. El protocolo debe tener solamente dos posibles resultados equitativos desde el punto de vista comercial: (1) el remitente 112 obtiene la dirección electrónica de la cuenta de criptoactivos y el destinatario 116 obtiene el título del automóvil o (2) ninguna de las partes obtiene el activo de la otra.

Continuando con el ejemplo ilustrado en la FIG. 1, en algunas realizaciones, t puede omitirse o establecerse en un valor grande, tal como infinito. El dispositivo informático 104 genera la segunda carga útil de datos Y = SIG_A(A, B, P, t, H(Z)) usando la clave criptográfica A del remitente 112. En algunas realizaciones, H es una función de creación de códigos de comprobación resistente a colisiones. Por lo tanto, existe únicamente una probabilidad muy baja de que se encuentren dos secuencias diferentes C y D, de modo que H(C) = H(D)). La función de creación de códigos de comprobación H(Z) se usa para codificar Z, de modo que un primer tamaño de la primera carga útil de datos Y sea superior a un segundo tamaño de la segunda carga útil de datos Z.

El dispositivo informático 104 transmite datos 132 (la primera carga útil de datos Z y la segunda carga útil de datos Y) al dispositivo informático 108 asociado al destinatario 116. Al recibir los datos Y del dispositivo informático 104, en algunas realizaciones, el dispositivo informático 108 determina si el momento actual es suficientemente anterior al tiempo límite t, de modo que el dispositivo informático 108 pueda restablecer la equidad de la transacción si es necesario. El dispositivo informático 108 firma digitalmente los datos Y para generar los datos 136 (SIG_B(Y)). Los datos 136 se usan como recepción para indicar al dispositivo informático 104 que el dispositivo informático 108 recibió los datos 132. Por ejemplo, el dispositivo informático 104 recibe la versión firmada SIG_B(Y) de la segunda carga útil de datos Y del dispositivo informático 108. La versión firmada SIG_B(Y) de la segunda carga útil de datos Y se firma mediante el uso de la clave criptográfica B del destinatario 116. En algunas realizaciones, el paquete de datos (A, B, P, t, H(Z)) indica un tiempo límite (usando el valor de t) para que el dispositivo informático 104 reciba la versión firmada de la segunda carga útil de datos Y del dispositivo informático 108. Por ejemplo, si se infringe t, la transacción se anulará o cancelará.

Cuando el remitente 112 recibe la recepción debidamente firmada (la versión firmada SIG_B(Y) de la segunda carga útil de datos Y) del destinatario 116, se supone que el remitente 112 debe enviar los datos 140 (clave privada S) al destinatario 116. En algunas realizaciones, t indica un tiempo límite donde el dispositivo informático 104 debe transmitir la clave privada S al dispositivo informático 108 después de que el dispositivo informático 104 haya recibido los datos 136. Si el dispositivo informático 108 determina que ha recibido la clave privada S en un momento suficientemente

anterior al tiempo límite t, el protocolo de cadena de bloques virtuales se completa de forma satisfactoria.

En algunas realizaciones, el dispositivo informático 108 determina si el dispositivo informático 108 no recibe la clave privada S (datos 140) del dispositivo informático 104. En otras realizaciones, el dispositivo informático 108 determina que el dispositivo informático 104 no transmitió la clave privada S al dispositivo informático 108 antes del tiempo límite t. Por tanto, se puede infringir el FEE. En un ejemplo, el remitente 112 es un vendedor de automóviles, el destinatario 116 es un comprador de automóviles y C indica una oferta para vender un automóvil por parte del remitente 112. El remitente 112 transmite los datos $SIG_A(C)$ al destinatario 116, pero el destinatario 116 nunca responde. En este caso, el remitente 112 puede vender su automóvil a otro comprador, después de lo cual el destinatario 116 reclama el automóvil. De este modo, una parte puede reconocer que ha obtenido la información deseada y luego obligar a que el intercambio quede incompleto.

Para implementar un FEE, en respuesta a la determinación de la falta de recepción de la clave privada S, el dispositivo informático 108 plantea un desafío a la cadena de bloques 120. El desafío incluye la versión firmada $SIG_B(Y)$ de la segunda carga útil de datos Y. La publicación de la versión firmada $SIG_B(Y)$ en la cadena de bloques 120 indica, al dispositivo informático 104, que el dispositivo informático 108 no ha recibido la clave privada S del dispositivo informático 104. La FIG. 1 ilustra que el dispositivo informático 108 publica el desafío en el bloque 124. En algunas realizaciones, t indica un tiempo límite para que el dispositivo informático 108 publique la versión firmada de la segunda carga útil de datos Y en la cadena de bloques 120. El paquete de datos (A, B, P, t, H(Z)) indica así un tiempo límite t=T1 donde el dispositivo informático 108 debe publicar el desafío en la cadena de bloques 120. Si se incumple T1, el contrato se anula o cancela y el remitente 112 no tiene que cumplirlo. Si los datos $SIG_B(Y)$ aparecen en la cadena de bloques 120 dentro del tiempo t (T1), el dispositivo informático 104 publica la clave privada S en la cadena de bloques 120 dentro de una cantidad de tiempo determinado, siempre que el remitente 112 desee realizar la transacción de forma honesta y completa la transacción de manera justa. El valor de t (T1) permite al remitente 112 establecer el límite superior del tiempo durante el cual la transacción permanece «abierta». Antes de enviar al dispositivo informático 104 la recepción SIGB (Y), el destinatario 116 puede evaluar subjetivamente si el destinatario tiene tiempo de reaccionar (mediante el tiempo T1) en caso de que el dispositivo informático 104 no transmita S al destinatario 116.

En algunas realizaciones, el dispositivo informático 104 determina que la versión firmada $SIG_B(Y)$ de la segunda carga útil de datos Y se ha publicado en la cadena de bloques 120. En respuesta a la determinación de que la versión firmada $SIG_B(Y)$ de la segunda carga útil de datos Y se ha publicado en la cadena de bloques 120, el dispositivo informático 104 publica la clave privada S en la cadena de bloques 120 para que el destinatario 116 desencripte el mensaje M. Por ejemplo, la clave privada S puede publicarse en el bloque 128. En algunas realizaciones, el dispositivo informático 104 publica la clave privada S en la cadena de bloques 120 en respuesta a la determinación de que la versión firmada $SIG_B(Y)$ de la segunda carga útil de datos Y se publica en la cadena de bloques 120 antes del tiempo límite T1. En algunas realizaciones, t indica un tiempo límite T2 para que el dispositivo informático 104 publique la clave privada S en la cadena de bloques 120 después de que el dispositivo informático 108 publique la versión firmada de la segunda carga útil de datos Y en la cadena de bloques 120. El dispositivo informático 104 debe, por lo tanto, publicar S al bloque 128 antes del tiempo T2.

Continuando con el ejemplo, el dispositivo informático 108 determina que el dispositivo informático 104 publica la clave privada S en la cadena de bloques 120. El dispositivo informático 108 desencripta la primera carga útil de datos Z usando la clave privada S para obtener el mensaje M. Por otro lado, si el dispositivo informático 104 no publica S en la cadena de bloques 120 dentro del tiempo límite T2 posterior a la publicación de los datos $SIG_B(Y)$, esto significa que el remitente 112 acepta que el destinatario 116 no ha recibido el mensaje M comprometido por la función H(Z).

Si el remitente 112 actúa con honestidad, entonces, dados los datos SIG (Y), el remitente 112 puede, al liberar M y S, probar el contenido del mensaje para el que el $SIG_B(Y)$ sea una recepción. Cualquier entidad puede verificar que S es la clave de desencriptado correspondiente a P y que el encriptado conjunto de (A, B, M) en relación con P y la clave criptográfica B del destinatario 116 es, de hecho, Z. Por tanto, cualquier entidad puede verificar que, dada S, el destinatario 116 puede recuperar M. Si el destinatario 116 nunca recibió S, el dispositivo informático 108 publicará de manera oportuna Y en la cadena de bloques 120, de modo que el remitente 112 publique públicamente S o acepte públicamente que el destinatario 116 está «libre de responsabilidad» en relación con la recepción del mensaje M. Por ejemplo, si el dispositivo informático 104 no publica de manera oportuna la clave privada S después de que Y se haya publicado de manera oportuna en la cadena de bloques 120, entonces se puede hacer que el remitente 112 reembolse al destinatario 116 (al menos parte de) los costes de transacción para publicar Y en la cadena de bloques 120.

En algunas realizaciones, en lugar de usar el encriptado único $E_{PX}(A, B, M)$, el remitente 112 puede usar dos (o más) encriptados para transmitir M, en relación con diferentes claves públicas. En algunas realizaciones, el remitente 112 puede registrar múltiples claves de encriptado públicas en la cadena de bloques 120. En otras realizaciones, el destinatario 116 puede no tener ninguna clave de encriptado pública registrada, pero puede generar la(s) necesaria(s) cuando el remitente 112 alerta al destinatario 116 de que el remitente 112 transmitirá un mensaje certificado, por ejemplo, M. Por ejemplo, el destinatario 116 puede poseer solamente una clave o claves de firma públicas y usarlas para autenticar cualquier clave de encriptado pública que el destinatario 116 necesite para el protocolo de cadena de bloques virtuales.

Cuando se recibe el valor $Z = E_{PX}(A, B, M)$ del dispositivo informático 104, el destinatario no puede desencriptar con facilidad M de Z (puesto que S aún no está disponible). Por tanto, si el destinatario 116 detiene el procesamiento, el remitente 112 no recibirá la recepción $SIG_B(Y)$ y el destinatario 116 tampoco recibirá el mensaje M. Si el dispositivo informático 108 transmite la recepción $SIG_B(Y)$ al dispositivo informático 104, entonces el remitente 112 recibe una recepción válida del destinatario 116 para el mensaje M. Por tanto, para que el intercambio del mensaje M y la recepción $SIG_B(Y)$ sea justo, el destinatario 116 debería poder obtener fácilmente M. El FEE se implementa cuando el remitente 112 transmite la clave privada S. Si el remitente 112 no transmite la clave privada S, entonces el dispositivo informático 108 debe publicar de manera oportuna la recepción $SIG_B(Y)$ en la cadena de bloques 120, solicitando esencialmente al dispositivo informático 104 que publique S de manera oportuna en la cadena de bloques 120.

En algunas realizaciones, el protocolo de cadena de bloques virtuales descrito en esta invención se usa para implementar un sistema de cheques y transferencias electrónicos (fuera de la cadena de bloques 120). Por ejemplo, el destinatario 116 puede acceder al dinero desde un cheque electrónico si y sólo si el remitente 112 recibe una recepción de que el destinatario 116 recibió el cheque. En algunas realizaciones, el protocolo de cadena de bloques virtuales descrito en esta invención puede usarse para implementar un sistema donde un agente tiene la obligación de informar a otro agente (por ejemplo, con respecto a un tiempo límite para ejercer una opción). El sistema funciona de manera que demuestra que el agente cumplió con sus obligaciones (por ejemplo, informar a una junta directiva para que notifique a los empleados los plazos de sus opciones).

En algunas realizaciones, el protocolo de cadena de bloques virtuales descrito en esta invención se usa para implementar un modelo basado en suscripción. En un modelo basado en suscripción, una entidad debe pagar un precio recurrente a intervalos regulares para acceder a un producto o servicio. Para obtener la capacidad de usar la cadena de bloques, cuando sea necesario, para restablecer la equidad de una transacción, se puede exigir al remitente 112 y al destinatario 116 que paguen una cuota de suscripción mensual o anual, por ejemplo, publicando una transacción en la cadena de bloques 120, especificando una secuencia particular (que indica el tipo de servicio solicitado) y pagando una cuota. El tipo de servicio puede ser correo electrónico certificado, contratos firmados electrónicamente, etc. La cuota puede (a) pagarse a una entidad (por ejemplo, una empresa, una fundación, etc.) que es responsable del mantenimiento de la cadena de bloques 120, (b) incorporarse a una agrupación de cargos por transacción que se distribuirán a los usuarios que contribuyen al mantenimiento de la cadena de bloques 120, (c) pagarse a una entidad o usuario E en particular o (d) una combinación de los mismos. Si, por ejemplo, el destinatario 116 no ha pagado dicha cuota de suscripción, entonces no está habilitado para usar la cadena de bloques 120 para restablecer la equidad.

Las ventajas y beneficios del modelo basado en suscripción del protocolo de cadena de bloques virtuales incluyen la posibilidad de que los usuarios realicen múltiples intercambios honestos y justos sin costo adicional. La empresa o fundación que mantiene la cadena de bloques 120 se beneficia de las cuotas de suscripción para prestar un servicio que no involucre más a la empresa o fundación en cada transacción. Si las cuotas de suscripción se incorporan a una agrupación de transacciones, los beneficiarios de la agrupación se benefician aún más cuando un usuario engañado (por ejemplo, el destinatario 116) utiliza la cadena de bloques 120 para publicar los datos $SIG_B(Y)$ que restablecen la equidad de la transacción. En el protocolo de cadena de bloques virtuales, un usuario acepta pagar una cuota de suscripción *a priori*. Se paga una cuota de transacción *a posteriori* solamente para las transacciones donde se producen fraudes. En las técnicas tradicionales basadas en la cadena de bloques, el usuario debe aceptar pagar un cargo por transacción *a priori* por cada transacción, incluso cuando todas las partes son honestas, puesto que pueden producirse fraudes. Además, un suscriptor F en un modelo basado en suscripción del protocolo de cadena de bloques virtuales puede representar un conjunto de usuarios en lugar de un solo usuario. Por ejemplo, F puede representar a un bufete de abogados y la cuota de suscripción pagada por F puede ser proporcional al número de usuarios que usan un servicio de FEE implementado mediante el modelo basado en suscripción del protocolo de cadena de bloques virtuales. En algunas realizaciones, F puede actuar en nombre de todos los usuarios. Por ejemplo, en un sistema CEM, F puede representar un servidor informático que proporciona recepciones para los mensajes dirigidos a algunos de sus usuarios y, a continuación, distribuye los mensajes internamente según sea necesario. El servidor informático puede implementarse usando los componentes ilustrados y descritos con más detalle con referencia a la FIG. 3.

La FIG. 2 ilustra un método para protocolos de cadena de bloques virtuales. En algunas realizaciones, el método de la FIG. 2 es realizado por el dispositivo informático 104 ilustrado y descrito con más detalle con referencia a la FIG. 1. Otras entidades realizan algunas o todas las etapas del método en otras realizaciones. Del mismo modo, las realizaciones pueden incluir etapas diferentes y/o adicionales o realizar las etapas en diferentes órdenes.

El dispositivo informático 104 genera 204 una clave pública P y una clave privada S correspondiente. La clave pública P y la clave privada S se ilustran y describen con más detalle con referencia a la FIG. 1. La clave pública P está destinada a transmitir un mensaje M de un remitente 112 a un destinatario 116. El mensaje M, el remitente 112 y el destinatario 116 se ilustran y describen con más detalle con referencia a la FIG. 1. El dispositivo informático 104 está asociado al remitente 112.

El dispositivo informático 104 encripta 208 el mensaje M usando la clave pública P y una clave criptográfica B del destinatario 116 para generar una primera carga útil de datos Z. La clave criptográfica B del destinatario 116 indica una identidad del destinatario 116. La primera carga útil de datos Z se expresa como $E_{PB}(A, B, M)$. De hecho, cualquier usuario, por ejemplo, el destinatario 116, puede encriptar el mensaje M usando la clave criptográfica pública A del

remitente 112, pero solo el remitente 112 puede desencriptar $E_A(M)$ siempre que el remitente 112 tenga su clave de desencriptado privada correspondiente.

El dispositivo informático 104 firma 212 un paquete de datos (A, B, P, t, H(Z)) usando la clave criptográfica A del remitente 112 para generar una segunda carga útil de datos Y. La clave criptográfica A del remitente 112 indica una identidad del remitente 112. El paquete de datos incluye la identidad del remitente 112, la identidad del destinatario 116, la clave pública P y una función de creación de códigos de comprobación H(Z) de la primera carga útil de datos. En algunas realizaciones, t indica un tiempo límite para que el remitente 112 o el destinatario 116 realicen una función de seguimiento. Por ejemplo, t puede indicar un tiempo límite para que el dispositivo informático 104 reciba una confirmación de recepción de la segunda carga útil de datos Y del segundo dispositivo informático 108. En otras realizaciones, t especifica un momento futuro después del cual el destinatario 116 no podrá restablecer la equidad de la transacción.

El dispositivo informático 104 transmite 216 la primera carga útil de datos Z y la segunda carga útil de datos Y a un dispositivo informático 108 asociado al destinatario 116. Al recibir los datos Y del dispositivo informático 104, en algunas realizaciones, el dispositivo informático 108 determina si el momento actual es suficientemente anterior al tiempo límite t, de modo que el dispositivo informático 108 pueda restablecer la equidad de la transacción si es necesario. El dispositivo informático 108 firma digitalmente los datos Y para generar los datos 136 ($SIG_B(Y)$). Los datos 136 se usan como recepción para indicar al dispositivo informático 104 que el dispositivo informático 108 recibió los datos 132. Los datos 132 y los datos 136 se ilustran y describen con más detalle con referencia a la FIG. 1.

El dispositivo informático 104 recibe 220 la versión firmada $SIG_B(Y)$ de la segunda carga útil de datos Y del dispositivo informático 108. La versión firmada $SIG_B(Y)$ de la segunda carga útil de datos Y se firma mediante el uso de la clave criptográfica B del destinatario 116. En algunas realizaciones, el paquete de datos (A, B, P, t, H(Z)) indica un tiempo límite (usando el valor de t) para que el dispositivo informático 104 reciba la versión firmada de la segunda carga útil de datos Y del dispositivo informático 108. Por ejemplo, si se incumple, la transacción se anulará o cancelará.

El dispositivo informático 104 determina 224 que la versión firmada $SIG_B(Y)$ de la segunda carga útil de datos Y ha sido publicada en la cadena de bloques 120 por el dispositivo informático 108. Cuando el remitente 112 recibe la recepción debidamente firmada (la versión firmada $SIG_B(Y)$ de la segunda carga útil de datos Y) del destinatario 116, se supone que el remitente 112 debe enviar los datos 140 (clave privada S) al destinatario 116. Los datos 140 se ilustran y describen con más detalle con referencia a la FIG. 1. Cuando el dispositivo informático 108 determina que el dispositivo informático 108 no ha podido recibir la clave privada S (datos 140) del dispositivo informático 104, el dispositivo informático 108 publica la versión firmada $SIG_B(Y)$ de la segunda carga útil de datos Y en la cadena de bloques 120.

En respuesta a la determinación de que la versión firmada de la segunda carga útil de datos Y se ha publicado en la cadena de bloques 120, el dispositivo informático 104 publica 228 la clave privada S en la cadena de bloques 120 para que el destinatario 116 desencripte el mensaje M. En algunas realizaciones, t indica un tiempo límite T2 para que el dispositivo informático 104 publique la clave privada S en la cadena de bloques 120 después de que el dispositivo informático 108 publique la versión firmada de la segunda carga útil de datos Y en la cadena de bloques 120. El dispositivo informático 104 debe, por lo tanto, publicar S en el bloque 128 antes del tiempo T2.

La FIG. 3 ilustra una máquina ejemplar. En la implementación de la FIG. 3, el sistema informático 300 es un dispositivo informático de propósito especial. El dispositivo informático de propósito especial está preprogramado para ejecutar protocolos de cadena de bloques, incluye dispositivos electrónicos digitales tales como uno o más circuitos integrados para aplicaciones específicas (ASIC) o matrices de puertas programables en campo (FPGA) que se programan de manera persistente para realizar las técnicas de esta invención o incluye uno o más procesadores de hardware de uso general programados para realizar las técnicas según las instrucciones del programa en firmware, memoria, otro almacenamiento o una combinación. En diversas implementaciones, los dispositivos informáticos de propósito especial son sistemas informáticos de escritorio, sistemas informáticos portátiles, dispositivos portátiles, dispositivos de red o cualquier otro dispositivo que incorpore lógica preprogramada o de programa para implementar las técnicas.

El sistema informático 300 incluye un bus 302 u otro mecanismo de comunicación para comunicar información y uno o más procesadores de hardware informático 304 acoplados al bus 302 para procesar información. En algunas implementaciones, los procesadores de hardware 304 son microprocesadores de uso general. El sistema informático 300 también incluye una memoria principal 306, tal como una memoria de acceso aleatorio (RAM) u otro dispositivo de almacenamiento dinámico, acoplado al bus 302 para almacenar información e instrucciones a ejecutar por los procesadores 304. En una implementación, la memoria principal 306 se usa para almacenar variables temporales u otra información intermedia durante la ejecución de las instrucciones a ejecutar por los procesadores 304. Tales instrucciones, cuando se almacenan en medios de almacenamiento no transitorios accesibles para los procesadores 304, convierten el sistema informático 300 en una máquina de propósito especial personalizada para realizar las operaciones especificadas en las instrucciones.

En una implementación, el sistema informático 300 incluye además una memoria de solo lectura (ROM) 308 u otro dispositivo de almacenamiento estático acoplado al bus 302 para almacenar información estática e instrucciones para los procesadores 304. Se proporciona un dispositivo de almacenamiento 312, tal como un disco magnético, un disco

óptico, una unidad de estado sólido o una memoria de punto de cruce tridimensional y se acopla al bus 302 para almacenar información e instrucciones.

En una implementación, el sistema informático 300 se acopla a través del bus 302 a una pantalla 310, tal como un tubo de rayos catódicos (CRT), una pantalla de cristal líquido (LCD), una pantalla de plasma, una pantalla de diodos emisores de luz (LED) o una pantalla de diodos emisores de luz orgánicos (OLED) para mostrar información a un usuario informático. Un dispositivo de entrada 314, que incluye teclas alfanuméricas y de otro tipo, está acoplado al bus 302 para comunicar la información y las selecciones de comandos a los procesadores 304. Otro tipo de dispositivo de entrada de usuario es un controlador de cursor 316, tal como un ratón, una bola de seguimiento, una pantalla táctil o teclas de dirección del cursor para comunicar la información de dirección y las selecciones de comandos a los procesadores 304 y para controlar el movimiento del cursor en la pantalla 310.

según una implementación, las técnicas de esta invención son realizadas por el sistema informático 300 en respuesta a que los procesadores 304 ejecuten una o más secuencias de una o más instrucciones contenidas en la memoria principal 306. Tales instrucciones se leen en la memoria principal 306 desde otro medio de almacenamiento, tal como el dispositivo de almacenamiento 312. La ejecución de las secuencias de instrucciones contenidas en la memoria principal 306 hace que los procesadores 304 realicen las etapas del método descritas en esta invención. En implementaciones alternativas, se usan circuitos preprogramados en lugar de instrucciones de software o en combinación con las mismas.

La expresión «medio de almacenamiento», como se emplea en esta memoria, se refiere a cualquier medio no transitorio que almacena tanto datos como instrucciones que hacen que una máquina funcione de una manera específica. Tales medios de almacenamiento incluyen tanto medios no volátiles como medios volátiles. Los medios no volátiles incluyen, tales como discos ópticos, discos magnéticos, unidades de estado sólido o memoria de punto de cruce tridimensional, tal como el dispositivo de almacenamiento 312. Las formas comunes de medios de almacenamiento incluyen, tales como un disquete, un disco flexible, un disco duro, una unidad de estado sólido, una cinta magnética o cualquier otro medio de almacenamiento de datos magnético, un CD-ROM, cualquier otro medio de almacenamiento de datos óptico, cualquier medio físico con patrones de orificios, una RAM, una PROM y una EPROM, una FLASH-EPROM, NV-RAM o cualquier otro chip o cartucho de memoria. Los medios de almacenamiento son distintos de, pero se usan junto con, los medios de transmisión. Los medios de transmisión participan en la transferencia de información entre los medios de almacenamiento. Los medios de transmisión incluyen cables coaxiales, alambres de cobre y fibra óptica, incluyendo los alambres que incluyen el bus 302.

En una implementación, varias formas de medios están implicadas en el transporte de una o más secuencias de una o más instrucciones a los procesadores 304 para su ejecución. Las instrucciones se transportan inicialmente en un disco magnético o en una unidad de estado sólido de un ordenador remoto. El ordenador remoto carga las instrucciones en su memoria dinámica y envía las instrucciones a través de una línea telefónica mediante el uso de un módem. Un módem local del sistema informático 300 recibe los datos de la línea telefónica y usa un transmisor de infrarrojos para convertir los datos en una señal de infrarrojos. Un detector de infrarrojos recibe los datos transportados en la señal de infrarrojos y los circuitos apropiados colocan los datos en el bus 302. El bus 302 lleva los datos a la memoria principal 306, desde la que los procesadores 304 recuperan y ejecutan las instrucciones. Las instrucciones recibidas por la memoria principal 306 se almacenan opcionalmente en el dispositivo de almacenamiento 312 antes o después de la ejecución por parte de los procesadores 304.

El sistema informático 300 también incluye una interfaz de comunicación 318 acoplada al bus 302. La interfaz de comunicación 318 proporciona un acoplamiento de comunicación de datos bidireccional a un enlace de red 320 conectado a una red local 322. La interfaz de comunicación 318 es una tarjeta de red digital de servicios integrados (ISDN), un módem por cable, un módem por satélite o un módem para proporcionar una conexión de comunicación de datos a un tipo correspondiente de línea telefónica. En otra implementación, la interfaz de comunicación 318 es una tarjeta de red de área local (LAN) para proporcionar una conexión de comunicación de datos a una LAN compatible. En algunas implementaciones, también se implementan enlaces inalámbricos.

El enlace de red 320 normalmente proporciona comunicación de datos a través de una o más redes a otros dispositivos de datos. El enlace de red 320 proporciona una conexión a través de la red local 322 a un ordenador central 324 o a un centro de datos en la nube o equipo operado por un proveedor de servicios de Internet (ISP) 326. El ISP 326, a su vez, proporciona servicios de comunicación de datos a través de la red mundial de comunicación de paquetes de datos ahora denominada comúnmente «Internet» 328. Tanto la red local 322 como Internet 328 usan señales eléctricas, electromagnéticas u ópticas que transportan corrientes de datos digitales.

Cualquiera o todas las características y funciones descritas anteriormente pueden combinarse entre sí, excepto en la medida en que se indique lo contrario anteriormente o en la medida en que cualquiera de estas realizaciones pueda ser incompatible en virtud de su función o estructura, como resultará evidente para los expertos en la materia. A menos que sea contrario a la posibilidad física, se prevé que (i) los métodos/etapas descritos en esta invención pueden realizarse en cualquier secuencia y/o en cualquier combinación, y que (ii) los componentes de las respectivas realizaciones pueden combinarse de cualquier manera.

Aunque la materia objeto se ha descrito en un lenguaje específico para las características estructurales y/o actos, debe entenderse que la materia objeto definida en las reivindicaciones adjuntas no se limita necesariamente a las características o actos específicos descritos anteriormente. Más bien, las características y actos específicos descritos anteriormente se describen como ejemplos de implementación de las reivindicaciones y se pretende que otras características y actos equivalentes estén dentro del alcance de las reivindicaciones.

En los dibujos, se muestran disposiciones u ordenamientos específicos de elementos esquemáticos, tales como los que representan dispositivos, módulos, bloques de instrucciones y elementos de datos, para facilitar la descripción. Sin embargo, los expertos en la materia deben entender que el ordenamiento o disposición específica de los elementos esquemáticos en los dibujos no implica que se requiera un orden o secuencia de procesamiento particular o separación de procesos. Además, la inclusión de un elemento esquemático en un dibujo no implica que dicho elemento sea necesario en todas las realizaciones o que las características representadas por dicho elemento no puedan incluirse o combinarse con otros elementos en algunas realizaciones.

Además, en los dibujos, donde se usan elementos de conexión, tales como líneas continuas o discontinuas o flechas, para ilustrar una conexión, relación o asociación entre o entre dos o más elementos esquemáticos diferentes, la ausencia de cualquiera de dichos elementos de conexión no implica que no pueda existir ninguna conexión, relación o asociación. En otras palabras, algunas conexiones, relaciones o asociaciones entre elementos no se muestran en los dibujos para no complicar la descripción. De manera adicional, para facilitar la ilustración, se usa un único elemento de conexión para representar múltiples conexiones, relaciones o asociaciones entre elementos. Por ejemplo, cuando un elemento de conexión representa una comunicación de señales, datos o instrucciones, los expertos en la materia deben entender que dicho elemento representa una o múltiples rutas de señal (por ejemplo, un bus), según pueda ser necesario, para afectar a la comunicación.

En la descripción anterior, las realizaciones se han descrito con referencia a numerosos detalles específicos que pueden variar de una implementación a otra. Por consiguiente, la descripción y los dibujos deben considerarse en un sentido ilustrativo más que restrictivo. El único y exclusivo indicador del alcance de las realizaciones, y lo que los solicitantes pretenden que sea el alcance de las realizaciones, es el alcance literal y equivalente del conjunto de reivindicaciones que se derivan de esta solicitud, en la forma específica en que se derivan dichas reivindicaciones, incluyendo cualquier corrección posterior. Cualquier definición que se exponga expresamente en esta invención para los términos contenidos en dichas reivindicaciones regirá el significado de dichos términos como se usan en las reivindicaciones. De manera adicional, cuando se usa el término «que incluye además», en la descripción anterior o en las siguientes reivindicaciones, lo que se deduce en esta expresión puede ser una etapa o entidad adicional o una subetapa/subentidad de una etapa o entidad anteriormente mencionada.

REIVINDICACIONES

1. Un método que comprende:

generar (204), por un primer dispositivo informático, una clave pública y una clave privada correspondiente, la clave pública para transmitir un mensaje de un remitente a un destinatario, el primer dispositivo informático asociado al remitente;

encriptar (208), por el primer dispositivo informático, el mensaje usando la clave pública y una clave criptográfica del destinatario para generar una primera carga útil de datos, indicando la clave criptográfica del destinatario una identidad del destinatario;

firmar (212), por el primer dispositivo informático, un paquete de datos usando una clave criptográfica del remitente para generar una segunda carga útil de datos, indicando la clave criptográfica del remitente una identidad del remitente, comprendiendo el paquete de datos la identidad del remitente, la identidad del destinatario, la clave pública y una función de creación de códigos de comprobación de la primera carga útil de datos;

transmitir (216), por el primer dispositivo informático, la primera carga útil de datos y la segunda carga útil de datos a un segundo dispositivo informático asociado al destinatario;

recibir (220), por el primer dispositivo informático, una versión firmada de la segunda carga útil de datos del segundo dispositivo informático, usando la versión firmada de la segunda carga útil de datos firmada la clave criptográfica del destinatario;

determinar (224), por el primer dispositivo informático, que la versión firmada de la segunda carga útil de datos se ha publicado en una cadena de bloques; caracterizado por que el método comprende además:

en respuesta a la determinación de que la versión firmada de la segunda carga útil de datos se ha publicado en la cadena de bloques, publicar (228), por el primer dispositivo informático, la clave privada en la cadena de bloques para desencriptar el mensaje por parte del destinatario.

2. El método de la reivindicación 1, en donde el paquete de datos indica un tiempo límite para que el primer dispositivo informático reciba la versión firmada de la segunda carga útil de datos del segundo dispositivo informático.

3. El método de la reivindicación 1, en donde el paquete de datos indica un tiempo límite para que el segundo dispositivo informático publique la versión firmada de la segunda carga útil de datos en la cadena de bloques, y en donde el primer dispositivo informático publica la clave privada en la cadena de bloques en respuesta a la determinación de que la versión firmada de la segunda carga útil de datos se publica en la cadena de bloques antes del tiempo límite.

4. El método de la reivindicación 1, en donde la función de creación de códigos de comprobación es una función de creación de códigos de comprobación resistente a colisiones, y en donde un primer tamaño de la primera carga útil de datos es superior a un segundo tamaño de la segunda carga útil de datos.

5. El método de la reivindicación 1, en donde la segunda carga útil de datos indica un tiempo límite para que el primer dispositivo informático publique la clave privada en la cadena de bloques después de que el segundo dispositivo informático publique en la cadena de bloques la versión firmada de la segunda carga útil de datos.

6. El método de la reivindicación 1, en donde la primera carga útil de datos comprende además la clave criptográfica del destinatario y la clave criptográfica del remitente.

7. Un método que comprende:

recibir, por un primer dispositivo informático asociado al destinatario de un mensaje, una primera carga útil de datos y una segunda carga útil de datos de un segundo dispositivo informático asociado al remitente del mensaje, excluyendo la primera carga útil de datos una clave privada para desencriptar el mensaje, la segunda carga útil de datos generada al firmar un paquete de datos usando una clave criptográfica del remitente que indica una identidad del remitente, comprendiendo el paquete de datos la identidad del remitente, una identidad del destinatario, una clave pública para transmitir el mensaje y una función de creación de códigos de comprobación del primera carga útil de datos;

transmitir, por el primer dispositivo informático, una versión firmada de la segunda carga útil de datos al segundo dispositivo informático, usando la segunda carga útil de datos una clave criptográfica del destinatario que indica la identidad del destinatario;

determinar, por el primer dispositivo informático, un fallo del primer dispositivo informático al recibir la clave privada del segundo dispositivo informático; caracterizado por que el método comprende además:

en respuesta a la determinación del fallo de recepción de la clave privada, publicar, por parte del primer dispositivo informático, la versión firmada de la segunda carga útil de datos en una cadena de bloques, indicando la publicación de la versión firmada de la segunda carga útil de datos, al segundo dispositivo informático, el fallo del primer dispositivo informático a la hora de recibir la clave privada del segundo dispositivo informático.

8. El método de la reivindicación 7, en donde la primera carga útil de datos se genera encriptando el mensaje usando la clave pública y la clave criptográfica del destinatario.

9. El método de la reivindicación 7, en donde la función de creación de códigos de comprobación de la primera carga útil de datos es una función de creación de códigos de comprobación resistente a colisiones, y en donde un primer tamaño de la primera carga útil de datos es superior a un segundo tamaño de la segunda carga útil de datos.

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

determinar, por el primer dispositivo informático, que la clave privada es publicada en la cadena de bloques por el segundo dispositivo informático; y

desencriptar, por el primer dispositivo informático, la primera carga útil de datos usando la clave privada para obtener el mensaje.

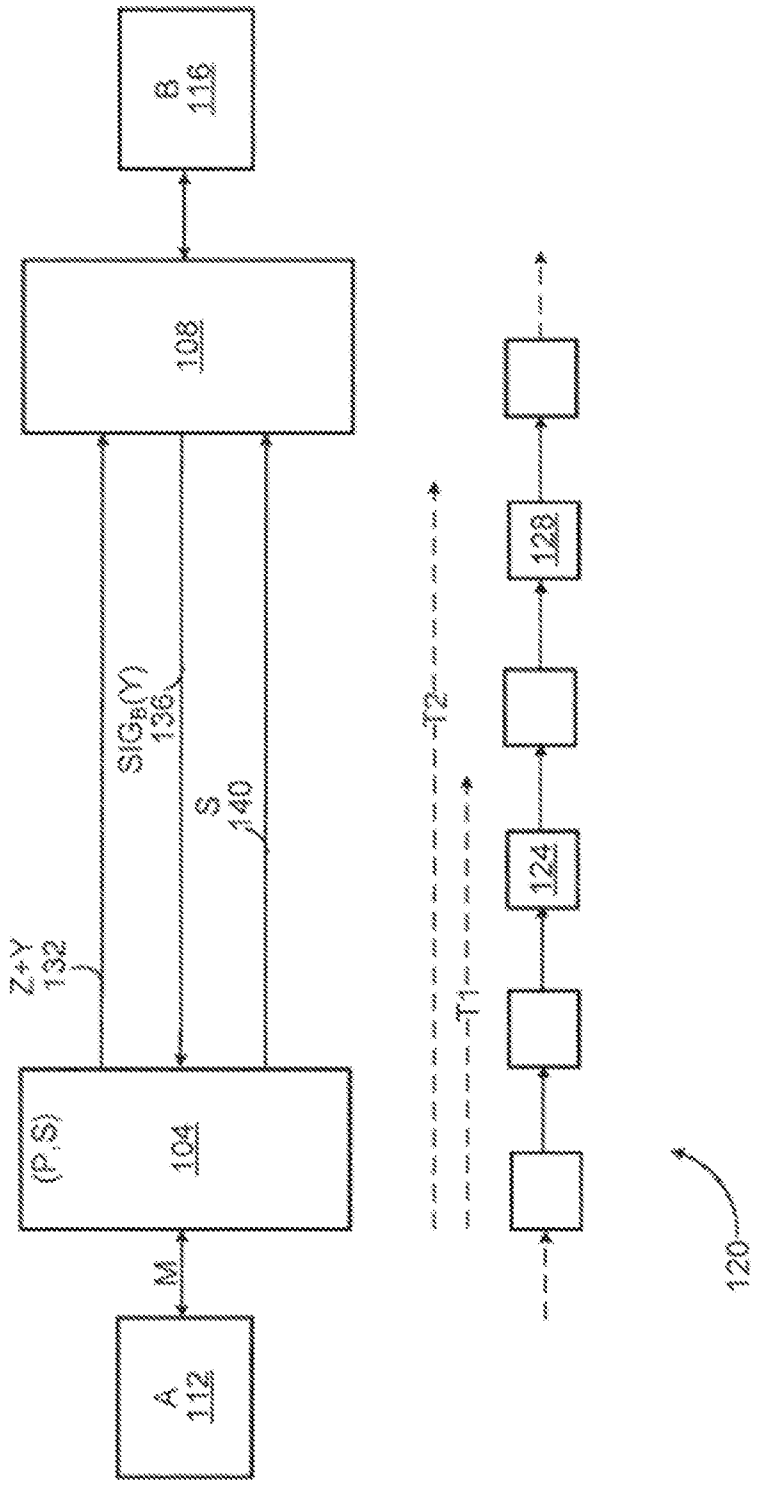

FIG. 1

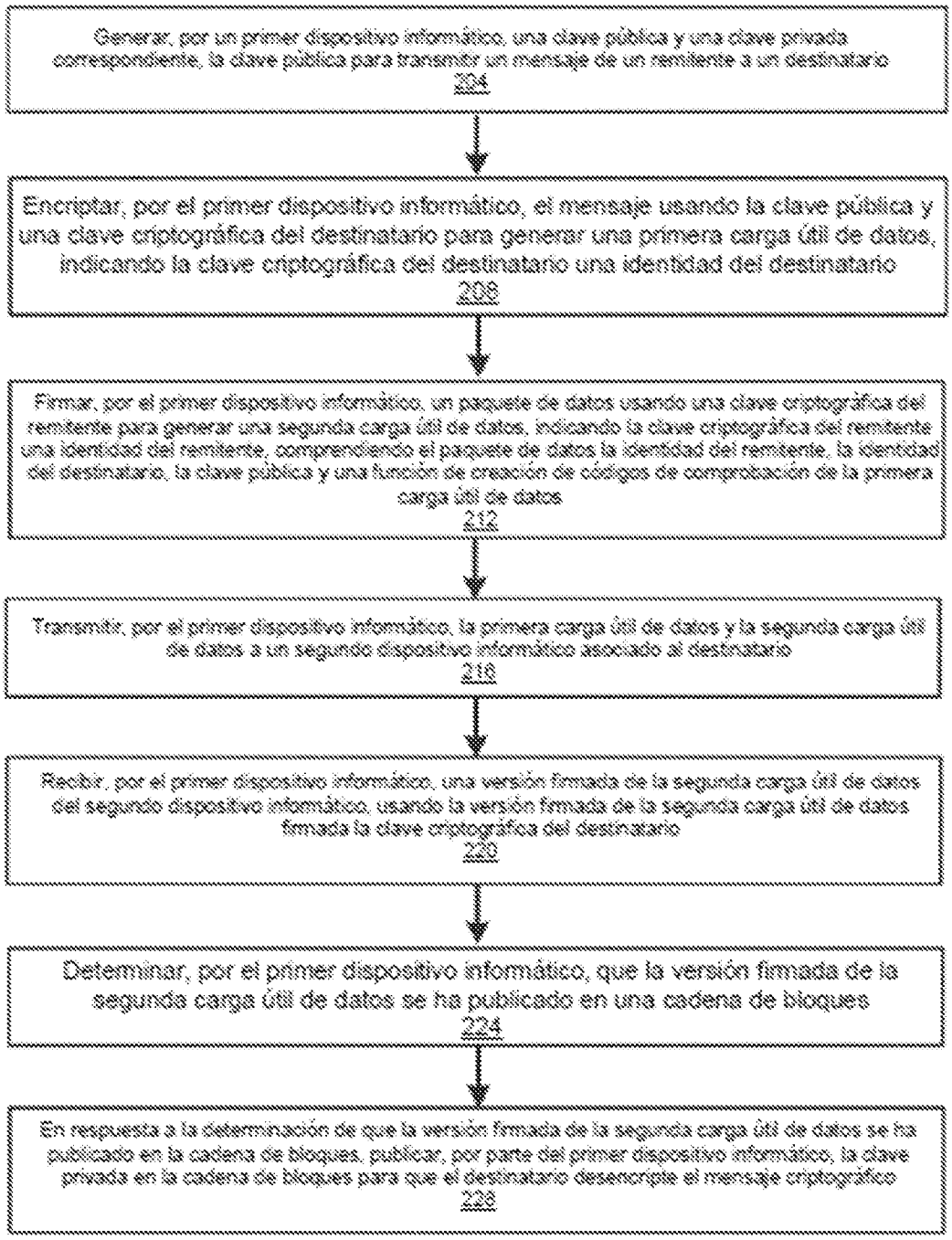
Generar, por un primer dispositivo informático, una clave pública y una clave privada correspondiente, la clave pública para transmitir un mensaje de un remitente a un destinatario
204
Encriptar, por el primer dispositivo informático, el mensaje usando la clave pública y una clave criptográfica del destinatario para generar una primera carga útil de datos, indicando la clave criptográfica del destinatario una identidad del destinatario
208
Firmar, por el primer dispositivo informático, un paquete de datos usando una clave criptográfica del remitente para generar una segunda carga útil de datos, indicando la clave criptográfica del remitente una identidad del remitente, comprendiendo el paquete de datos la identidad del remitente, la identidad del destinatario, la clave pública y una función de creación de códigos de comprobación de la primera carga útil de datos
212
Transmitir, por el primer dispositivo informático, la primera carga útil de datos y la segunda carga útil de datos a un segundo dispositivo informático asociado al destinatario
216
Recibir, por el primer dispositivo informático, una versión firmada de la segunda carga útil de datos del segundo dispositivo informático, usando la versión firmada de la segunda carga útil de datos firmada la clave criptográfica del destinatario
220
Determinar, por el primer dispositivo informático, que la versión firmada de la segunda carga útil de datos se ha publicado en una cadena de bloques
224
En respuesta a la determinación de que la versión firmada de la segunda carga útil de datos se ha publicado en la cadena de bloques, publicar, por parte del primer dispositivo informático, la clave privada en la cadena de bloques para que el destinatario desencripte el mensaje criptográfico
228

FIG. 2

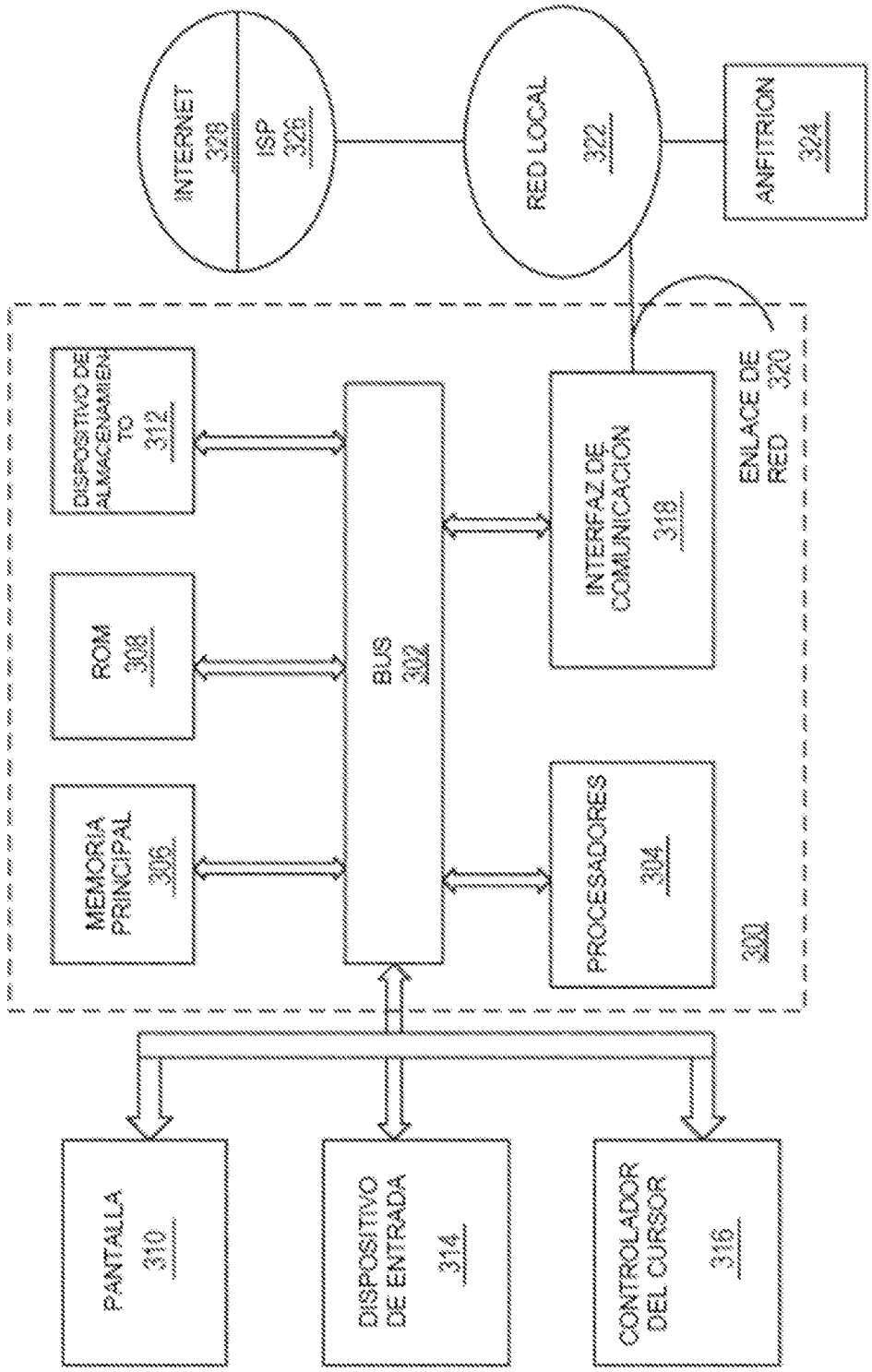
INTERNET
328
ISP
326
RED LOCAL
322
ANFITRIÓN
324
DISPOSITIVO DE ALMACENAMIENTO
312
ROM
308
MEMORIA PRINCIPAL
306
BUS
302
INTERFAZ DE COMUNICACIÓN
318
ENLACE DE RED
320
PROCESADORES
304
301
PANTALLA
310
DISPOSITIVO DE ENTRADA
314
CONTROLADOR DEL CURSOR
316

FIG. 3