(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 985 270**

(51) Int. Cl.:

H04L 9/00 (2012.01)
H04L 9/32 (2006.01)
G06Q 20/38 (2012.01)
G06F 21/62 (2013.01)
G06F 16/27 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.10.2019 PCT/CA2019/051439**

(87) Fecha y número de publicación internacional: **16.04.2020 WO20073124**

(96) Fecha de presentación y número de la solicitud europea: **09.10.2019 E 19871914 (8)**

(97) Fecha y número de publicación de la concesión europea: **08.05.2024 EP 3834118**

(54) Título: **Método y sistema para claves públicas de un solo propósito para los libros de registro público**

(30) Prioridad:

12.10.2018 US 201816158971

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.11.2024

(73) Titular/es:

MALIKIE INNOVATIONS LIMITED (100.0%)
The Glasshouses GH292 Georges Street Lower
Dun Laoghaire, Dublin A96 VR66, IE

(72) Inventor/es:

BROWN, DANIEL RICHARD L.

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y sistema para claves públicas de un solo propósito para los libros de registro público

Campo de la descripción

La presente descripción se refiere a libros de registro públicos que incluyen cadena de bloques y, en particular, se refiere a la seguridad de transacciones para libros de registro públicos.

Antecedentes

La banca se basa normalmente en un sistema de libro de registro. Un libro de registro es un registro de transacciones entre cuentas. Un libro de registro público hace que el libro de registro sea público en el sentido de que todas las transacciones están disponibles para el público. Además, un sistema de registro público es seudónimo si los números de cuenta son rastreables, pero no identifican individuos por nombre. Seudónimo, como se usa en el presente documento, significa que mientras que las transacciones asociadas con un número de cuenta pueden rastrearse, los propios números de cuenta no pueden necesariamente asociarse con una persona particular.

Una criptomoneda de libro de registro público es una moneda digital que usa criptografía para marcar transacciones. En tales sistemas, un número de cuenta puede ser una clave pública, y una transacción puede contener una firma digital. El libro de registro público puede ser usado por un destinatario de criptomoneda para confirmar que el titular de la cuenta tiene suficientes fondos en una cuenta antes de entrar en una transacción. Esto puede ayudar a evitar un doble gasto por un emisor de criptomoneda.

En los sistemas criptográficos de libro de registro público, cada titular de cuenta normalmente tiene una clave privada, que se usa para firmar transacciones. La clave privada se almacena a menudo en un módulo llamado cartera digital en un dispositivo informático. Sin embargo, un ladrón puede invadir el dispositivo que almacena la cartera digital y extraer una clave privada de firma del titular de la cuenta. El ladrón puede entonces transferir fondos del titular de la cuenta a otras cuentas.

Un destinatario honesto no desea recibir fondos robados. En criptomoneda, cada destinatario debe inspeccionar primero el libro de registro público para ver si lo está. Dicho emisor posee fondos suficientes. Esta inspección del libro de registro público da a un destinatario honesto una oportunidad limitada para contrarrestar algunas formas de robo y fraude. En particular, la comprobación del libro de registro público puede permitir que un destinatario honesto trace dónde han viajado los fondos. Un destinatario honesto puede ser capaz de detectar que la criptomoneda en cuestión ha seguido una ruta sospechosa. Por ejemplo, si los fondos se originan a partir de una cuenta cuyos fondos han sido reportados robados, y el destinatario honesto puede rechazar recibir los fondos y puede reportar un intento de transacción a las autoridades.

Sin embargo, existen problemas significativos con tales métodos. En particular, no hay forma de que un destinatario honesto evite recibir fondos antes de que el propietario verdadero de los fondos haya detectado una cartera digital robada. Además, no hay forma de que un destinatario honesto valide si un extraño es un propietario correcto de los fondos. Por lo tanto, hay poca defensa contra, por ejemplo, el lavado de dinero basado en fraudes. Esta falta de defensa disminuye la credibilidad de todo el libro de registro público.

Los documentos de patente CN 108 021 821 A, CN 107 240 017 A2, WO 2017/044554A1, US 2017/085562A1 y US 2009/281937 A1 son representativos de la técnica disponible.

Compendio

Por consiguiente, se proporciona un método, dispositivo informático y medio legible por ordenador como se detalla en las reivindicaciones que siguen.

Breve descripción de los dibujos

La presente invención se comprenderá mejor con referencia a los dibujos, en los cuales:

la Figura 1 es un diagrama de bloques de un sistema informático de ejemplo que puede usarse para transacciones criptográficas de libro de registro público;

la Figura 2 es un diagrama de proceso que muestra un proceso para la creación de claves públicas y privadas vinculadas a un mensaje en un Algoritmo de Firma Digital de Curva Elíptica;

la Figura 3 es un diagrama de proceso que muestra un proceso para la verificación de que un mensaje está vinculado a una clave pública;

la Figura 4 es un diagrama de proceso que muestra un proceso generalizado para la creación de claves públicas y privadas vinculadas a un mensaje;

la Figura 5 es un diagrama de proceso que muestra un proceso para la verificación de que un mensaje está vinculado a una clave pública;

la Figura 6 es un diagrama de flujo de datos que muestra el uso de una cadena de propósito para dirigir una transacción en un sistema criptográfico de libro de registro público; y

la Figura 7 es un diagrama de bloques de un dispositivo informático simplificado que puede usarse con los métodos y sistemas en el presente documento según una realización.

Descripción detallada de los dibujos

La presente descripción proporciona un método en un dispositivo informático en un sistema criptográfico de libro de registro público, comprendiendo el método: crear una cadena de propósito, definiendo la cadena de propósito parámetros de transacción para una cuenta dentro del sistema criptográfico de libro de registro público; usar la cadena de propósito para crear una clave privada y una clave publica asociada para una cuenta dentro del sistema criptográfico de libro de registro público; y proporcionar la cadena de propósito para su uso en la verificación de una transacción desde la cuenta dentro del sistema criptográfico de libro de registro público.

La presente descripción proporciona además un dispositivo informático en un sistema criptográfico de libro de registro público, comprendiendo el dispositivo informático: un procesador; y un subsistema de comunicaciones, en donde el dispositivo informático está configurado para: crear una cadena de propósito, definiendo la cadena de propósito parámetros de transacción para una cuenta dentro del sistema criptográfico de libro de registro público; usar la cadena de propósito para crear una clave privada y una clave publica asociada para una cuenta dentro del sistema criptográfico de libro de registro público; y proporcionar la cadena de propósito para su uso en la verificación de una transacción desde la cuenta dentro del sistema criptográfico de libro de registro público.

La presente descripción proporciona además un medio legible por ordenador para almacenar código de instrucción que, cuando se ejecuta por un procesador de un dispositivo informático en un sistema criptográfico de libro de registro público, hace que el dispositivo informático: cree una cadena de propósito, definiendo la cadena de propósito parámetros de transacción para una cuenta dentro del sistema criptográfico de libro de registro público; use la cadena de propósito para crear una clave privada y una clave publica asociada para una cuenta dentro del sistema criptográfico de libro de registro público; y proporcione la cadena de propósito para su uso en la verificación de una transacción desde la cuenta dentro del sistema criptográfico de libro de registro público.

De acuerdo con la presente descripción, se usará la terminología de la Tabla 1.

TABLA 1: Terminología

Término	Breve descripción
Libro de registro	Una lista de transacciones/transferencias de dinero entre cuentas
Libro de registro público	Un libro de registro que es visible públicamente
Dirección de seudónimo o cuenta	Un número trazable único adjunto a una cuenta: normalmente también una clave pública
Clave pública	Un valor usado para verificar una firma digital de un mensaje, para cada clave pública, existe una clave privada asociada
Firma digital	Un valor que es un valor verificable públicamente, dado un mensaje y una clave pública
Clave privada	Un valor usado para generar una firma digital de mensaje - para cada clave privada, hay una clave pública asociada
Prueba de generación	Prueba de que una entidad generó una clave pública - más precisamente esa clave pública se generó en combinación con un mensaje particular, llamado cadena de propósito en esta descripción. La entidad puede identificar públicamente el mensaje particular usado para la generación de clave pública.
Cadena de propósito	Un mensaje que puede usarse para crear un par de claves mutuamente asociadas, una clave privada y una clave pública, de modo que cada clave pública puede tener como máximo 1 cadena de propósito

Tal como se proporciona en el documento Tabla 1, un libro de registro público es un libro de registro que es visible públicamente. Un ejemplo de una criptomoneda de libro de registro público es Bitcoin, que usa tecnología de cadena de bloques para autenticar el libro de registro público. Este proceso se conoce como minera, y en su mayor parte descentraliza la autoridad del libro mayor público.

De acuerdo con realizaciones de la presente descripción, se describe un sistema de criptografía de libro de registro público. El libro de registro público puede, por ejemplo, usarse para criptomoneda. La criptomoneda usada con las realizaciones en el presente documento puede ser, por ejemplo, Bitcoin. Sin embargo, la presente descripción no se limita a Bitcoin y puede usarse cualquier criptomoneda adecuada.

La criptomoneda puede usarse en una variedad de entornos informáticos. Un ejemplo de entorno informático se muestra con respecto a la Figura 1.

En la realización de la Figura 1, un dispositivo 110 informático pertenece a un usuario con fondos en un libro de registro público. A este respecto, el dispositivo 110 informático puede incluir un procesador 112 y un subsistema 114 de comunicaciones, donde el procesador y el subsistema de comunicaciones cooperan para realizar los métodos descritos en el presente documento.

El Dispositivo 110 informático puede incluir además una memoria 116, que puede usarse para almacenar los datos o la lógica programable. La lógica programable puede ser ejecutada por el procesador 112. En otras realizaciones, se puede proporcionar lógica programable al dispositivo 110 informático a través del subsistema 114 de comunicaciones.

En el sistema informático de la Figura 1, el dispositivo 110 informático incluye una cartera 118 digital, que puede almacenar la clave privada para fondos dentro del libro de registro público. En particular, la clave pública para el usuario del dispositivo 110 informático asociada a la clave privada almacenada en la cartera 118 digital puede permitir que los fondos se usen con el registro público. La clave privada se almacena en la cartera 118 digital, que proporciona seguridad para almacenar tal clave privada.

La cartera 118 digital puede ser cualquier estructura de datos o estructura lógica usada para almacenar la clave privada y los datos asociados. En algunas realizaciones, la cartera 118 digital se implementa en software y hardware, o puede implementarse en hardware diseñado expeditamente, que almacena información que permite a un individuo realizar transacciones de comercio electrónico. En algunas realizaciones, la cartera digital puede proporcionarse utilizando dispositivos de hardware dedicados, tales como un módulo de seguridad de hardware. En otras realizaciones, la cartera 118 digital puede incluir memoria que está dedicada a la cartera digital, y puede ser interna o externa al dispositivo 110 informático.

El dispositivo 110 informático puede comunicarse, por ejemplo, a través de una red 120.

En algunas realizaciones, el dispositivo 110 informático puede comunicarse con una autoridad 130 certificadora que puede usarse para generar y autenticar certificados para el dispositivo informático, incluyendo certificados para el libro de registro público en algunos casos.

Además, la red 120 puede usarse para el dispositivo 110 informático para comunicarse con un libro de registro público o cadena 140 de bloques, que pueden estar almacenados en varios ordenadores y distribuidos en algunos casos.

Además, en algunas realizaciones, la red 120 puede usarse para comunicarse con una entidad receptora tal como un proveedor 150. El proveedor 150 puede incluir un dispositivo informático configurado para realizar las realizaciones en el presente documento, incluyendo la comunicación con el dispositivo 110 informático y el libro/cadena 140 de bloques público, así como la verificación como se describe a continuación.

El vendedor 150 puede proporcionar bienes o servicios a cambio de la criptomoneda asociada a la cartera 118 digital.

Sin embargo, en algunas realizaciones, el dispositivo 110 informático puede estar próximo a un proveedor 150 y en este caso es posible la comunicación directamente entre el dispositivo 110 informático y el proveedor 150.

Como se ha indicado anteriormente, debido a la naturaleza del libro de registro público, la detección de fraude puede ser posible en cierto grado. Las transacciones sospechosas pueden detectarse, por ejemplo, a partir de actividades sospechosas. Por ejemplo, las transacciones de gran valor, transacciones repentinas, compras hacia vendedores sospechosos o compras realizadas en ubicaciones inusuales podrían servir como indicadores de transacciones fraudulentas. La industria de las tarjetas de crédito ya usa tales medidas para bloquear transacciones sospechosas de tarjetas de crédito, o para solicitar información adicional antes de permitir que las transacciones sospechosas avancen. En Bitcoin, una respuesta recomendada al robo sospechado de una clave privada de una cartera digital es crear primero una nueva cuenta con una nueva clave pública, y luego transferir fondos restantes (si los hay) a la nueva cuenta. Sin embargo, en este punto, puede ya ser demasiado tarde, el atacante puede haber transferido ya los fondos a otra cuenta.

Bitcoin en sí no proporciona ningún medio para emitir un informe de robo. No hay mecanismo actual dentro del libro de registro público para señalar bitcoins robados. Sin embargo, es posible hacerlo fuera del mecanismo de registro

público, tal como en redes sociales, por las autoridades gubernamentales en contacto, entre otras opciones. Una vez que se ha realizado tal informe, se puede rastrear una ruta de los fondos robados a través del libro mayor.

En un libro de registro público, un vendedor honesto puede examinar transacciones sospechosas o usar informes de robo para detectar transacciones fraudulentas. Un vendedor honesto puede rechazar por lo tanto entrar en nuevas transacciones que creen que pueden implicar fondos robados o ser de otro modo fraudulentos. El vendedor honesto puede incluso revisar u seguir a través de transacciones pasadas para medir qué porcentaje de fondos en una cuenta son sospechosos o fraudulentos.

Los esfuerzos de un ladrón para evitar el sistema de detección de fraude se denomina blanqueo. Como primer paso del blanqueo, un ladrón puede transferir una gran cantidad de fondos de la víctima a su propia cuenta. El ladrón intentaría entonces gastar esta cantidad antes de que la víctima emita un informe de robo (que señala como robados los fondos de la cuenta del ladrón). Un sistema de detección de fraude puede por lo tanto ser diseñado para sospechar fondos gastados demasiado pronto después de una gran transferencia.

Un ladrón podría intentar también realizar muchas pequeñas transferencias en una pequeña cantidad de tiempo a múltiples cuentas. Este tipo de actividad puede ser nuevamente etiquetado como sospechoso.

En casos de robo o fraude de alto valor, las autoridades pueden intentar aprobar físicamente a las personas que pasan los fondos, por ejemplo, ofreciendo realizar una transacción personal con el ladrón.

Sin embargo, en todos estos casos, se necesita conocimiento previo de las transacciones y en algunos casos conocimiento de que los fondos son robados.

Por lo tanto, de acuerdo con las realizaciones de la presente descripción descritas a continuación, un concepto titulado "Prueba de Generación" puede utilizarse con claves públicas para proporcionar una "cadena de propósito" para la verificación de la transacción.

La prueba de generación permite la vinculación de un mensaje a una clave pública. La clave pública puede verificarse entonces contra el mensaje para garantizar que la clave pública esté asociada con el mensaje. Esto se describe, por ejemplo, en la patente de los EE.UU. número 9,240,884, 19 de enero 2016.

En particular, la prueba de generación se usa para generar una clave pública con un mensaje adjunto. Típicamente, usando la prueba de generación, cuando se genera la clave pública, se vincula un mensaje a la clave pública. La vinculación de este mensaje a la clave pública puede ser verificada por cualquier persona.

Además, el vínculo es único, ya que es imposible tener dos mensajes diferentes vinculados a una clave pública. Incluso una entidad maliciosa que genera la clave privada y la clave pública no puede crear dos mensajes diferentes vinculados a la misma clave pública.

Una clave pública con un mensaje de prueba de generación puede usarse como cualquier clave pública y no tiene limitaciones distintas de estar vinculada a un único mensaje de prueba de generación. Por ejemplo, una clave pública de prueba de generación puede ser usada para firmas digitales y para intercambio de claves, o para cualquier otro tipo de criptografía de clave pública.

En lo anterior, cuando se hace referencia a la vinculación, la prueba de generación permite que cada clave pública se vincula a un mensaje. Sin embargo, esto no significa una unión uno a uno. Un mensaje puede estar vinculado a muchas claves públicas diferentes.

La prueba de generación puede ser autenticada o no autenticada, como se explica a continuación.

En la prueba de generación no autenticada, el mensaje vinculado no está autenticado. En particular, no hay nada que deje de crear otra clave pública vinculada al mismo mensaje.

En la prueba de generación autenticada, el mensaje vinculado se autentica de alguna manera. Por ejemplo, el mensaje vinculado puede contener una firma digital de una autoridad de certificación, o alguna otra parte confiable. Por ejemplo, para certificados implícitos descritos en las Normas para Criptografía Eficiente 4 (SEC 4), la prueba de generación es autenticada debido a la participación de la autoridad de certificación.

Si se usa con las realizaciones de la presente descripción, una clave pública puede reconstruirse a partir de certificados implícitos. Además, cualquiera puede crear un certificado implícito, a partir del cual se puede reconstruir una clave pública. Sin embargo, la única manera en que alguien puede conocer la clave privada para una clave pública reconstruida es si participa con la autoridad de certificación en la creación del par de claves pública/privada. Por lo tanto, para que certificados implícitos proporcionen una seguridad completa, incluyendo la prueba de generación, el propietario de la clave pública reconstruida debe demostrar de alguna manera la posesión de la clave privada correspondiente. Esta prueba de posesión se demuestra típicamente firmando un mensaje o desencriptando un texto cifrado. En el contexto de la prueba de generación, la prueba de generación no se completa hasta que se proporciona la prueba de posesión. Hasta la prueba de posesión, la seguridad se considera implícita. Esto significa que es normalmente relativamente seguro usar el certificado implícito incluso antes de recibir la posesión de la prueba, porque

si el certificado implícito es falso, será inútil con una clave privada desconocida. Específicamente, en algún punto de la transacción, la clave privada necesitará usarse para la prueba de posesión, y por lo tanto el uso del certificado implícito puede hacerse antes de la prueba de posesión, ya que eventualmente se detectará un certificado falso. En el contexto de criptomoneda de libro de registro público, una de las principales formas en las que se usan claves públicas es verificar firmas, que proporcionan prueba de posesión. Por lo tanto, de acuerdo con las realizaciones descritas a continuación, la fase de seguridad implícita no se evita, ya que la prueba de posesión aún puede usarse con los métodos y sistemas descritos en el presente documento.

Por ejemplo, se hace referencia ahora a la Figura 2, que muestra un método para generar claves pública y privada utilizando un mensaje *m* en un Algoritmo de Firma Digital de Curva Elíptica (ECDSA).

El procedimiento de la Figura 2 comienza en el bloque 210 y procede al bloque 212 en el que se elige un mensaje. Como apreciarán los expertos en la técnica, el mensaje podría ser cualquiera. En particular, de acuerdo con las realizaciones descritas a continuación, el mensaje puede ser una cadena de propósito que indica el propósito de la cuenta de criptomoneda.

El proceso pasa entonces al bloque 214 en el que se calcula un resumen de mensaje e con ayuda de una función hash sobre el mensaje m. En este caso, la función hash es una función hash criptográfica que da un resultado entero.

El correspondiente puede entonces calcular una clave privada a partir del resumen de mensaje e usando una fórmula d=(sk - e)/r mod n en el bloque 216. En este caso, s es un número entero en el intervalo [0, n-1], y es preferiblemente aleatorio. El valor k es un número entero elegido al azar en el intervalo [0, n-1]. El valor n es el tamaño del campo para la criptografía. El valor r es un valor entero correspondiente a un punto R de curva elíptica, donde R se denomina clave pública efímera de firma y k se denomina clave privada efímera.

El procedimiento de la Figura 2 entonces procede al bloque 218 en la que se encuentra una clave Q pública se calcula usando la fórmula Q=dG, donde G es un punto de orden n en una curva elíptica.

De esta manera, una clave Q pública y una clave d privada están vinculadas a un mensaje m. Dichas claves pública y privada pueden usarse entonces para un sistema criptográfico de libro de registro público.

Al recibir una clave pública, un dispositivo informático puede verificar que la clave pública se genera basándose en el mensaje m. En particular, se hace referencia ahora a la Figura 3. En la realización de la Figura 3, el proceso comienza en el bloque 310 y procede al bloque 312 en la que el dispositivo informático verificador recibe la clave pública Q y el mensaje m.

El proceso pasa entonces al bloque 314. En el bloque 314, el verificador calcula en primer lugar un punto de curva elíptico R'= (1/s mod n n)(eG + rQ), que es parte del proceso de verificación de ECDSA.

El verificador también necesitará saber cómo la clave R pública efímera de firma se convirtió en valor r entero . Esto puede implicar conocer el valor A salino, junto con la función hash u otra función usada para calcular r. Por ejemplo, si r=Hash (A||R||A||R||...||A||R) entonces r' puede calcularse como r'=Hash (A||R'||A||R'||...||A||R').

El verificador podría comparar entonces r' y r en el bloque 316, y si los dos coinciden, esto indica que la clave pública se generó usando el mensaje m.

Del proceso procede entonces al bloque 320 y finaliza.

En otra forma de realización, mostrada con la Figura 4, Se proporciona un método más general que no usa necesariamente criptografía de curva elíptica. En particular, el procedimiento de la Figura 4 empieza en el bloque 410 y procede al bloque 412 en la que se selecciona un valor k entero . El valor k es un número entero en el intervalo [0, n-1].

El proceso pasa entonces al bloque 414 en el que se genera una clave R pública de semilla usando la fórmula R=kG, donde G es de nuevo un punto de orden n en una curva.

Del bloque 414, el resumen del mensaje f se calcula como f = SHA-1 (m,R) en el bloque 416.

Del bloque 416 el proceso pasa al bloque 418 en el que se calcula la clave privada d=kf.

El proceso pasa entonces al bloque 420 en el que se calcula la clave pública Q=fR.

El proceso pasa entonces al bloque 430 y finaliza.

Dichas claves pública y privada pueden usarse entonces para un sistema criptográfico de libro de registro público.

[0064] Un verificador puede verificar que la clave pública está vinculada al mensaje m que utiliza el procedimiento de la Figura 5. En particular, el procedimiento de la Figura 5 comienza en el bloque 510 y procede al bloque 512 en el que el verificador recibe un triple exponencial con hash (m, R, Q).

El proceso pasa entonces al bloque 514 en el que se calcula un resumen de mensaje f=SHA-1 (m, R).

El proceso pasa entonces al bloque 516 en el que un valor T se calcula como T=fR.

El proceso pasa entonces al bloque 518 en el que un verificador puede comprobar que Q=T. En caso afirmativo, la clave pública se vincula al mensaje.

El proceso pasa entonces al bloque 520 y finaliza.

Utilizando este concepto, las realizaciones a continuación incluyen una "cadena de propósito" que se usa como parte del mensaje para generar la clave pública. En particular, una cadena de propósito identifica el propósito de la cuenta dentro del libro de registro público.

Un receptor honesto de fondos puede pedir a un supuesto titular de cuenta la cadena de propósito en algunos casos. En otros casos, la cadena de propósito puede ser voluntaria por el supuesto titular de la cuenta. En otros casos adicionales, la cadena de propósito puede estar disponible a través de una base de datos publica, o a través del propio libro de registro.

Un receptor honesto intentará entonces prescindir de la cadena de propósito e intentará garantizar que la cuenta se usa sólo para el propósito designado.

Esto puede disuadir o impedir que un ladrón que ha robado la clave privada para que una cuenta use fondos con un propósito incorrecto.

Por lo tanto, la cadena de propósito se usa como una prevención contra el fraude y se establece en el momento en que se crea la cuenta, antes de que ocurra cualquier fraude.

Por lo tanto, de acuerdo con las realizaciones de la presente descripción, la prueba de generación se usa para proporcionar un propósito para la cuenta. El propósito puede verificarse entonces durante una transacción en el libro de registro público.

Como se ha descrito anteriormente, en prueba de generación, una vez que se genera una clave pública, se vincula a un mensaje único. La unión puede verificarse por cualquier persona. En todos los demás aspectos, la clave pública es normal y puede usarse para generar firmas digitales de arbitrariamente muchos mensajes, tal como se usa en la criptomoneda.

Por lo tanto, de acuerdo con las realizaciones en el presente documento, el mensaje al que está vinculada una clave pública se vuelve a designar para ser una cadena de propósito.

La cadena de propósito puede incluir datos arbitrarios. El contenido específico de la cadena de propósito se analiza a continuación.

En las realizaciones en el presente documento, se proporciona un proceso sobre cómo usar una cadena de propósito en el contexto de la criptomoneda. Cuando un supuesto propietario de clave pública Alice usa su clave pública con otra parte honesta Bob, la otra parte Bob puede solicitar ver la cadena de propósito. Alice puede proporcionar la cadena de propósito y Bob puede inspeccionar la cadena de propósito. Bob da cuenta de la cadena de propósito, asegurando que la transacción se ajuste a los detalles contenidos en la cadena de propósito.

Si la supuesta parte Alice no logra suministrar la cadena de propósito, o la supuesta Alice o la naturaleza de la transacción de algunas maneras no logra cumplir con la cadena de propósito, Bob puede rechazar entrar en la transacción. Al rechazar así la transacción, Alice no puede obtener ningún producto o servicio de Bob. Si un adversario Eve ha robado la clave privada de Alice y está intentando impersonar fraudulentamente a Alice, entonces Bob puede haber frustrado los intentos de Eve para aprovechar el robo de las claves privadas de Alice.

Una propiedad clave de la cadena de propósito es que puede haber como máximo una cadena de propósito por clave pública. Esta propiedad es una consecuencia del método de generación de pruebas como se ha descrito anteriormente. No es factible generar la misma clave pública con dos cadenas de propósito diferentes.

En el presente documento se aclaran varias propiedades de las series de propósito. En particular:

- La cadena de propósito no revela la clave privada.
- La clave pública no revela la cadena de propósito.
- No se requiere que la cadena de propósito sea secreta.
- La cadena de propósito puede mantenerse privada entre Alice y Bob, si se desea.

- La cadena de propósito se puede mantener publica, tal como en una base de datos publica, tal vez integrada en el libro de registro público.
- Se puede usar una clave pública sin una cadena de propósito.
- Un destinatario deshonesto de la cadena de propósito puede elegir ignorar su propósito, o no pedir en absoluto la cadena de propósito.
- La cadena de propósito, si se origina a partir de un método de prueba de generación no autentificado, puede ser común a muchas claves publicas diferentes, por lo que no establece uniformidad de la clave publica
- La cadena de propósito proporciona una manera de identificar un propósito único para una clave pública dada.

En una criptomoneda, un propietario de clave pública honesto puede crear a su clave pública una cadena de propósito honesto. Los destinatarios honestos pueden solicitar la cadena de propósito, bajo demanda, y sólo aceptar transacciones con una clave pública si las transacciones cumplen con el contenido encontrado en la cadena de propósito.

Por lo tanto, ahora se hace referencia a la Figura 6. En la realización de la Figura 6, un dispositivo 610 informático de cliente teniendo una cartera digital asociada con una criptomoneda de libro de registro público puede intentar comprar bienes o servicios de un vendedor 612.

A este respecto, el dispositivo 610 informático de cliente puede intentar la transacción usando un libro de registro público, como se muestra con el mensaje 620 entre el cliente y el vendedor 612. El mensaje 620 puede enviarse, por ejemplo, a través de una red, o puede basarse en una comunicación de corto alcance entre el dispositivo 610 informático de cliente y un dispositivo de cálculo para el proveedor 612.

El vendedor 612 puede entonces verificar que el cliente está asociado al dispositivo 610 informático tiene fondos suficientes, como se muestra en el bloque 622. La verificación en el bloque 622 puede consultar el registro para garantizar que se asocian fondos suficientes al cliente 610.

Suponiendo que hay fondos suficientes, el dispositivo informático del vendedor 612 puede entonces solicitar la cadena de propósito para la cuenta, como se muestra con el mensaje 630. El mensaje 630 en la realización de la Figura 4 se envía al dispositivo 610 informático de cliente.

En realizaciones alternativas, en lugar de solicitar la cadena de propósito al dispositivo 610 informático de cliente, el dispositivo informático del proveedor 612 puede solicitar la cadena de propósito del registro. En otras realizaciones, el dispositivo informático del proveedor 612 puede solicitar la cadena de propósito de otras bases de datos que pueden contener dicha cadena de propósito.

En respuesta a la solicitud de la cadena de propósito en el mensaje 630, Se puede proporcionar una cadena de propósito al dispositivo informático del proveedor 612 en el mensaje 632. El mensaje 632, en la realización de la Figura 6, se origina a partir del dispositivo 610 informático de cliente. Sin embargo, si la solicitud de mensaje 630 de cadena de propósito fuera a un dispositivo informático diferente, entonces el mensaje 632 puede provenir de ese dispositivo informático diferente.

El dispositivo informático del proveedor 612 puede entonces verificar que la clave pública está asociada al cliente, como se muestra en bloque 640. La verificación puede realizarse de acuerdo con la Figura 3 o la Figura 5 antes, por ejemplo. Esto asegura que la clave pública esté asociada con la cadena de propósito que se proporcionó en el mensaje 632.

Si se verifica que la clave pública está asociada con la cadena de propósito, entonces el dispositivo informático del proveedor 612 puede intentar verificar la transacción en el bloque 650. Verificar la transacción significa que la transacción cae dentro de los límites de la cadena de propósito.

El vendedor puede entonces permitir o denegar la transacción, como se muestra con el mensaje 660. La habilitación o denegación puede realizarse automáticamente en un dispositivo informático en algunas realizaciones. En las otras realizaciones, la autorización o denegación puede basarse en la entrada de usuario a un dispositivo informático con base en la información presentada en el dispositivo informático.

Como apreciarán los expertos en la técnica, si la clave pública no está asociada con la cadena de propósito que se proporcionó en el mensaje 632, entonces un mensaje 660 puede enviarse inmediatamente después del bloque 640, denegando la transacción.

Como se indicó anteriormente para el bloque 650, la transacción puede verificarse contra la cadena de propósito. Hay varias opciones para tal verificación.

En una primera opción, se pueden colocar diversas limitaciones de transacción dentro de la cadena de propósito. Por ejemplo, en una realización, la cadena de propósito puede contener información que limita qué tipo de transacciones se permiten para la cuenta.

Al configurar la cuenta, el titular de la cuenta puede limitar la cantidad o valor máximo de una única transferencia, por ejemplo. El soporte también puede limitar el número total de transferencias en un período de tiempo dado, tal como por día.

Un receptor honesto puede por lo tanto comprobar la cadena de propósito en el bloque 650 y respetar estas limitaciones. En particular, el dispositivo informático del proveedor 612 puede referirse al libro de registro público para ver cuántas transacciones han ocurrido desde dicha cuenta y ver si la transacción actual superaría el límite de transacción dentro de la cadena de propósito.

En otros casos, el dispositivo informático del proveedor 612 puede verificar que la cantidad de transferencia propuesta está por debajo del valor en la cadena de propósito.

En algunos casos, la cadena de propósito puede tener un formato específico que facilitaría el análisis sintáctico de la cadena de propósito por un dispositivo informático asociado con el proveedor 612, permitiendo así al dispositivo informático realizar la verificación en bloque 640. En otros casos, el procesamiento del lenguaje natural puede usarse para encontrar limitaciones dentro de la cadena de propósito.

Por lo tanto, la cadena de propósito puede proporcionar una forma de añadir limitaciones de transacción a la criptomoneda del libro de registro público.

La cadena de propósito también puede usarse para limitar el tipo de artículos para los que los fondos pueden usarse para comprar. Por ejemplo, los fondos pueden limitarse a ser usados únicamente para comprar comestibles. Tal limitación puede hacer que sea menos eficiente para un ladrón blanquee fondos robados, porque los fondos robados tendrían que ser intercambiados por algo que es más difícil de volver a ser vendido, es más voluminoso y tiene una vida útil corta, perdiendo por ello rápidamente valor.

De nuevo, los tipos de bienes o servicios para los que las transacciones están limitadas pueden tener texto estandarizado para permitir el análisis sintáctico de dicha cadena de propósito en algunos casos. En otros casos, podría utilizarse el procesamiento de lenguaje natural.

En otros casos más, la cadena de propósito solo puede permitir una transacción cuando el titular de la cuenta está físicamente presente y no en línea.

En otros casos, la cadena de propósito puede limitar las transacciones durante una cierta ventana de tiempo. Por ejemplo, las transacciones pueden limitarse a entre 7 am y 9 pm de Zona Horaria Estándar Oriental. Por lo tanto, si se hace un intento de comprar algo de un vendedor fuera de la ventana de tiempo especificada, entonces se puede denegar la transacción.

En realizaciones adicionales, la cadena de propósito puede contener límites geográficos para donde puede ocurrir la transacción. Por lo tanto, los fondos pueden ser usados solamente dentro de dicha área geográfica, tal como una ciudad, provincia, estado o país.

En otros casos, puede requerirse que la transacción se realice en un lugar público. Por lo tanto, un sistema de posicionamiento asociado con el dispositivo informático del vendedor 612 puede determinar si el dispositivo está en un espacio público o en un espacio privado y, por lo tanto, permitir o denegar la transacción.

Son posibles otras opciones.

Además, en algunos casos, la cadena de propósito puede limitarse a solo uno de los propósito anteriores. En otros casos, la cadena de propósito puede contener múltiples limitaciones. Por lo tanto, la cadena de propósito puede indicar que un puede darse límite de transacción de 1000 $ por transacción solo entre 7 am y 9 pm de Zona Horaria Estándar Oriental. El número o tipos de propósito no están limitados para una cadena de propósito.

En otras realizaciones adicionales, la cadena de propósito puede contener un identificador para un cliente. En particular, en esta realización, la cadena de propósito incluye datos que pueden usarse para identificar el titular de cuenta verdadero. Los datos pueden estar en una forma que permita al receptor honesto verificar la identificación.

Mientras que en muchas criptomonedas, los titulares de cuenta son seudónimos, o incluso anónimos, una cadena de propósito con un identificador revierte parcialmente esta propiedad seudónimo. La pérdida de seudónimo tiene algunas desventajas, tales como privacidad más débil, tales desventajas pueden verse compensadas por las protecciones o descentivos contra el robo de carteras digitales.

Por ejemplo, en un caso, la cadena de propósito puede proporcionar el nombre del titular de cuenta verdadera, en forma de texto. En este caso, un vendedor honesto puede tener algún medio para verificar el nombre de la persona que intenta realizar la transacción. En algunos casos, el vendedor puede conocer el titular de la cuenta, por ejemplo,

a través de una relación preexistente. En otros casos, el destinatario o vendedor honesto puede solicitar ver otras formas autenticadas de identificación, tales como un permiso de conducir o pasaporte. El receptor honesto puede comprobar el nombre en el documento oficial para encontrar si coincide con el nombre en la cadena de propósito. La fuerza de la identificación depende de la fuerza del documento oficial o de la relación existente.

En otra realización más, el cambio de propósito puede ser datos que proporcionan datos biométricos tales como una imagen del titular de cuenta verdadera. En este caso, el receptor honesto puede comparar la imagen en la cadena de propósito con una imagen del supuesto titular de cuenta. Por ejemplo, esto puede usarse cuando las transacciones se realizan en personas, o usando una cámara web, entre otras opciones.

En realizaciones adicionales, en lugar de una imagen, se podría usar otra información de identificación y difícil de falsificar. Esto podría incluir, por ejemplo, datos biométricos tales como una huella dactilar, un patrón de voz, entre otras opciones.

De manera similar, la cadena de propósito puede contener una imagen de la licencia de conducir de los titulares de cuenta. Esto podría incluir una imagen del titular de cuenta real, la firma manuscrita del titular, entre otra información. Esta información puede entonces ser emparejada contra la licencia real del conductor, así como una imagen directa del supuesto titular de la cuenta y la supuesta firma del titular de la cuenta. En otra realización más, que puede ser adecuada para transacciones en línea, es si la cadena de propósito es autenticada por una autoridad de certificación. Por ejemplo, el método de prueba de generación subyacente podría ser un certificado implícito, o el propósito podría contener un mensaje similar a un certificado de clave pública tradicional. Como es habitual, la autoridad de certificación verifica la identidad del titular de cuenta verdadero en el momento de la creación de la cuenta. Sin embargo, en la situación en la que un ladrón ha fijado la clave privada, es probable que la información puramente digital que se usa normalmente para la autenticación pueda haber sido comprometida. Para superar esta amenaza, en un entorno en línea, se podría poder simular el entorno minorista, tal como proporcionar una conexión de vídeo entre el destinatario honesto y el supuesto titular de la cuenta. En esta conexión de vídeo, el receptor honesto puede usar los diversos métodos basados en imágenes descritos anteriormente para intentar verificar la identidad.

Un receptor honesto puede verificar una entidad en diferentes grados. En algunos casos, el viraje del supuesto titular de la cuenta puede ser proporcional al nivel de riesgo de la transacción. Por lo tanto, de acuerdo con las realizaciones descritas anteriormente, una o más cadenas de propósito pueden incrustarse en el mensaje que se usa para generar una clave pública. El uso de tal cadena de propósito puede permitir entonces que un destinatario vea una transacción antes de permitir que la transacción proceda.

Los expertos en la materia apreciarán que el uso de una cadena de propósito en la generación de las claves pública y privada asociadas con la criptografía de libro de registro público no limita otras funciones criptográficas para tales claves o libros de registro. Por ejemplo, el uso de una autoridad certificadora para comprobar que una clave pertenece a un propietario no se cambia mediante el uso de una cadena de propósito. De manera similar, la funcionalidad de infraestructura de clave pública (PKI) para el intercambio de claves no se ve afectada por el uso de cadenas de propósito.

Los módulos y equipos de usuario y dispositivos que realizan los métodos descritos anteriormente pueden ser cualquier dispositivo electrónico o nodo de red. Tal dispositivo informático o nodo de red puede incluir cualquier tipo de dispositivo informático, incluyendo, pero sin limitarse a, dispositivos móviles tales como teléfonos inteligentes o teléfonos móviles. Los ejemplos pueden incluir además equipos de usuario fijos o móviles, tales como dispositivos de Internet de las cosas (IoT), puntos finales, dispositivos de automatización del hogar, equipos médicos en entornos hospitalarios o domésticos, dispositivos de rastreo de inventario, dispositivos de monitorización ambiental, dispositivos de gestión de energía, dispositivos de gestión de infraestructuras, vehículos o dispositivos para vehículos, dispositivos electrónicos fijos, entre otros. Los vehículos incluyen vehículos a motor (por ejemplo, automóviles, coches, camiones, autobuses, motocicletas, etc.), aviones (por ejemplo, aviones, vehículos aéreos no tripulados, sistemas de aviones no tripulados, drones, helicópteros, etc.), naves espaciales (por ejemplo, naves espaciales, lanzaderas espaciales, cápsulas espaciales, estaciones espaciales, satélites, etc.), embarcaciones (por ejemplo, barcos, botes, aerodeslizadores, submarinos, etc.), vehículos ferroviarios (por ejemplo, trenes y tranvías, etc.), y otros tipos de vehículos que incluyen cualquier combinación de cualquiera de los anteriores, ya sea que exista actualmente o después de surgir.

Por ejemplo, el dispositivo informático puede estar asociado con un propietario de una cuenta de libro de registro público o asociado con un destinatario de transacción. Un diagrama simplificado de un dispositivo informático se muestra con respecto a la Figura 7.

En la Figura 7, el dispositivo 710 incluye un procesador 720 y un subsistema 730 de comunicaciones, donde el procesador 720 y el subsistema de comunicaciones 730 cooperan para realizar los procedimientos de los modos de realización descritos anteriormente. El subsistema 720 de comunicaciones puede comprender, en algunas realizaciones, múltiples subsistemas, por ejemplo para diferentes tecnologías de radio.

El procesador 720 está configurado para ejecutar lógica programable, que puede almacenarse, junto con datos, en el dispositivo 710, y se muestra en el ejemplo de la Figura 7 como memoria 740. La memoria 740 puede ser cualquier

medio de almacenamiento legible por ordenador tangible no transitorio. El medio de almacenamiento legible por ordenador puede ser un medio tangible o transitorio/no transitorio, tal como óptico (por ejemplo, CD, DVD, etc.), magnético (por ejemplo, cinta), unidad flash, disco duro u otra memoria conocida en la técnica.

De manera alternativa, o además de la memoria 740, el dispositivo 710 puede acceder a datos o lógica programable desde un medio de almacenamiento externo, por ejemplo a través de un subsistema 730 de comunicaciones.

El subsistema 730 de comunicaciones - permite al dispositivo 710 comunicarse con otros dispositivos o elementos de red y puede variar con base en el tipo de comunicación que se está realizando. Además, el subsistema 730 de comunicaciones puede comprender una pluralidad de tecnologías de comunicaciones, incluyendo cualquier tecnología de comunicaciones cableada o inalámbrica.

Las comunicaciones entre los diversos elementos del dispositivo 710 puede ser a través de un bus 760 interno en una realización. Sin embargo, son posibles otras formas de comunicación.

Las realizaciones descritas en el presente documento son ejemplos de estructuras, sistemas o métodos que tienen elementos correspondientes a elementos de las técnicas de esta solicitud. Esta descripción escrita puede permitir a los expertos en la técnica realizar y usar realizaciones que tienen elementos alternativos que corresponden igualmente a los elementos de las técnicas de esta solicitud. El alcance previsto de las técnicas de esta solicitud incluye, por tanto, otras estructuras, sistemas o métodos que no difieren de las técnicas de esta solicitud como se describe en el presente documento, e incluye además otras estructuras, sistemas o métodos con diferencias insustanciales de las técnicas de esta solicitud como se describe en el presente documento.

Aunque las operaciones se representan en los dibujos en un orden particular, esto no debe entenderse como que requiere que tales operaciones se realicen en el orden particular mostrado o en orden secuencial, o que se realicen todas las operaciones ilustradas, para lograr resultados deseables. En ciertas circunstancias, se pueden emplear tareas múltiples y procesamiento paralelo. Además, la separación de diversos componentes del sistema en la implementación descrita anteriormente no debe entenderse como que requiere tal separación en todas las implementaciones, y debe entenderse que los componentes y sistemas de programa descritos pueden integrarse generalmente entre sí en un producto de software de señal o empaquetarse en múltiples productos de software.

Además, las técnicas, sistemas, subsistemas y métodos descritos e ilustrados en las diversas implementaciones como discretos o separados pueden combinarse o integrarse con otros sistemas, módulos, técnicas o métodos. Otros elementos mostrados o analizados como acoplados o directamente acoplados o en comunicación entre sí pueden estar indirectamente acoplados o en comunicación a través de alguna interfaz, dispositivo o componente intermedio, ya sea eléctrica, mecánica o de otro modo. Otros ejemplos de cambios, sustituciones y alteraciones son determinables por un experto en la técnica y pueden realizarse.

Aunque la descripción detallada anterior ha mostrado, descrito y señalado las características novedosas fundamentales de la descripción como se aplica a diversas implementaciones, se entenderá que los expertos en la técnica pueden realizar diversas omisiones, sustituciones y cambios en la forma y detalles del sistema ilustrado. Además, el orden de los pasos del método no está implícito en el orden en el que aparecen en las reivindicaciones.

Cuando se envían mensajes a/desde un dispositivo electrónico, tales operaciones pueden no ser inmediatas o desde el servidor directamente. Pueden entregarse de manera síncrona o asíncrona, desde un servidor u otra infraestructura de sistema informático que soporte los dispositivos/métodos/sistemas descritos en el presente documento. Los pasos anteriores pueden incluir, en su totalidad o en parte, comunicaciones síncronas/asíncronas hacia/desde el dispositivo/infraestructura. Además, la comunicación desde el dispositivo electrónico puede ser a uno o más puntos finales en una red. Estos puntos extremos pueden ser atendidos por un servidor, un sistema informático distribuido, un procesador de flujo, etc. Las Redes de Entrega de Contenido (CDN) también pueden proporcionar la comunicación a un dispositivo electrónico. Por ejemplo, en lugar de una respuesta de servidor típica, el servidor también puede proporcionar o indicar datos para que la Red de Entrega de Contenido (CDN) espere la descarga por el dispositivo electrónico en un momento posterior, tal como una actividad posterior del dispositivo electrónico. Por lo tanto, los datos pueden enviarse directamente desde el servidor, u otra infraestructura, tal como una infraestructura distribuida, o una CDN, como parte de o separada del sistema.

Típicamente, los medios de almacenamiento pueden incluir cualquiera o alguna combinación de los siguientes: un dispositivo de memoria semiconductor tal como una memoria de acceso aleatorio dinámica o estática (una DRAM o SRAM), una memoria de solo lectura borrable y programable (EPROM), una memoria de solo lectura borrable y programable eléctricamente (EEPROM) y memoria flash; un disco magnético tal como un disco fijo, flexible y extraíble; otro medio magnético que incluye cinta; un medio óptico tal como un disco compacto (CD) o un disco de vídeo digital (DVD); u otro tipo de dispositivo de almacenamiento. Obsérvese que las instrucciones analizadas anteriormente pueden proporcionarse en un medio de almacenamiento legible por ordenador o legible por máquina, o alternativamente, pueden proporcionarse en múltiples medios de almacenamiento legibles por ordenador o legibles por máquina distribuidos en un sistema grande que tiene posiblemente una pluralidad de nodos. Dicho medio o medios de almacenamiento legibles por ordenador o legibles por máquina se consideran parte de un artículo (o artículo de fabricación). Un artículo o artículo de fabricación puede referirse a cualquier componente único fabricado o

componentes múltiples. El medio o medios de almacenamiento pueden estar ubicados en la máquina que ejecuta las instrucciones legibles por máquina, o ubicados en un sitio remoto desde el que pueden descargarse instrucciones legibles por máquina a través de una red para su ejecución.

En la descripción anterior, se exponen numerosos detalles para proporcionar una comprensión del objeto descrito en el presente documento. Sin embargo, las implementaciones pueden ponerse en práctica sin algunos de estos detalles. Otras implementaciones pueden incluir modificaciones y variaciones de los detalles analizados anteriormente. Se pretende que las reivindicaciones adjuntas cubran tales modificaciones y variaciones.

REIVINDICACIONES

1. Un método en un dispositivo (110; 610; 710) informático en un sistema criptográfico de libro de registro público, comprendiendo el método:

crear una cadena de propósito, definiendo la cadena de propósito parámetros de transacción para una cuenta dentro del sistema criptográfico de libro de registro público;

crear una clave privada y una clave pública asociada para la cuenta dentro del sistema criptográfico de libro de registro público, usando la creación la cadena de propósito, en donde la clave pública está vinculada exclusivamente a la cadena de propósito;

recibir (630) una solicitud desde un segundo dispositivo (612) informático en el sistema criptográfico de libro de registro público para la cadena de propósito; y

proporcionar (632) la cadena de propósito al segundo dispositivo (612) informático para su uso en la verificación de prueba de generación de la clave publica durante una transacción desde la cuenta dentro del sistema criptográfico de libro de registro público.

2. El método de la reivindicación 1, en donde la cadena de propósito define al menos un parámetro de transacción seleccionado de: un límite de valor de transacción; un límite de frecuencia de transacción; un límite de geografía de transacción; un límite de período de tiempo de transacción; un límite de ubicación de transacción; un límite en una ubicación de un titular de cuenta de la cuenta dentro del sistema criptográfico de libro de registro público con respecto a un destinatario durante la transacción; y un límite en bienes o servicios permitidos en una transacción.

3. El procedimiento de la reivindicación 1, en donde la cadena de propósito proporciona un identificador para un titular de cuenta de la cuenta dentro del sistema criptográfico de registro público.

4. El método de la reivindicación 3, en donde el identificador son datos biométricos para el titular de la cuenta.

5. El método de la reivindicación 3, en donde el identificador es un nombre del titular de la cuenta.

6. El método de la reivindicación 3, en donde el identificador es una imagen de un documento para el titular de la cuenta.

7. El método de la reivindicación 1, en donde la provisión se realiza al crear la cuenta con un elemento de red.

8. El procedimiento de la reivindicación 7, en donde el elemento de red está asociado con el sistema criptográfico de libro de registro público.

9. Un dispositivo (110; 610; 710) informático en un sistema criptográfico de libro de registro público, comprendiendo el dispositivo informático:

un procesador (720); y

un subsistema (730) de comunicaciones,

en donde el dispositivo informático está configurado para llevar a cabo el método de una cualquiera reivindicación anterior.

10. Un medio legible por ordenador para almacenar código de instrucción que, cuando se ejecuta por un procesador (720) de un dispositivo (730) informático en un sistema criptográfico de libro de registro público, hace que el dispositivo (730) informático lleve a cabo el método de una cualquiera de las reivindicaciones 1 a 8.

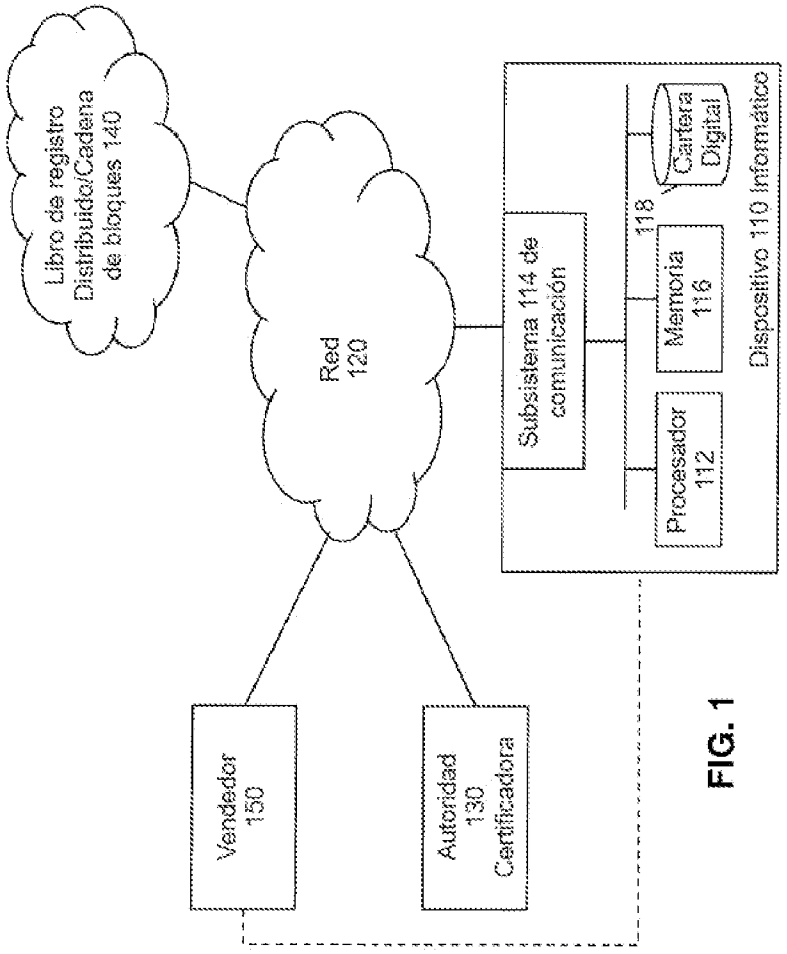
Libro de registro Distribuido/Cadena de bloques 140
Red 120
Vendedor 150
Autoridad 130 Certificadora
Subsistema 114 de comunicación
Procesador 112
Memoria 116
118
Cartera Digital
Dispositivo 110 Informático

FIG. 1

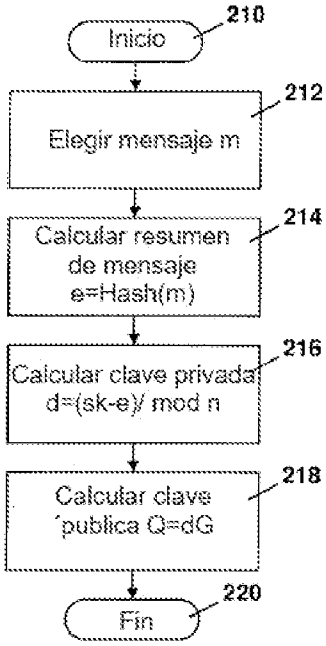
Inicio
210
Elegir mensaje m
212
Calcular resumen de mensaje e=Hash(m)
214
Calcular clave privada d=(sk-e)/ mod n
216
Calcular clave ´publica Q=dG
218
Fin
220

FIG. 2

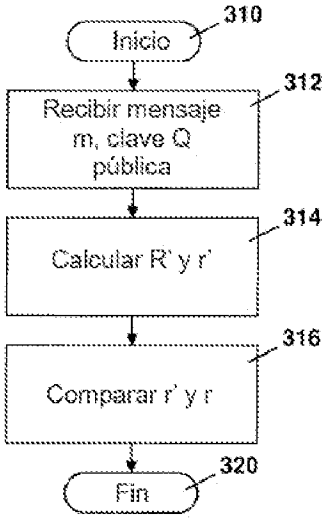
Inicio
310
Recibir mensaje m, clave Q pública
312
Calcular R' y r'
314
Comparar r' y r
316
Fin
320

FIG. 3

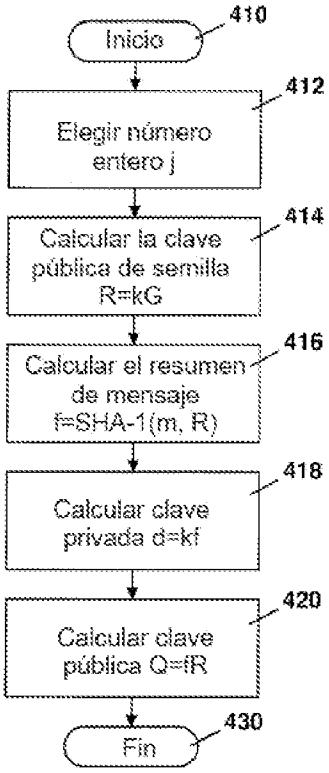
Inicio
410
Elegir número entero j
412
Calcular la clave pública de semilla R=kG
414
Calcular el resumen de mensaje f=SHA-1(m, R)
416
Calcular clave privada d=kf
418
Calcular clave pública Q=fR
420
Fin
430

FIG. 4

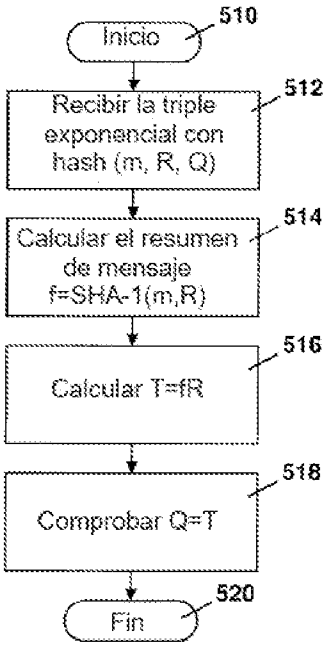
Inicio
510
Recibir la triple exponencial con hash (m, R, Q)
512
Calcular el resumen de mensaje f=SHA-1(m,R)
514
Calcular T=fR
516
Comprobar Q=T
518
Fin
520

FIG. 5

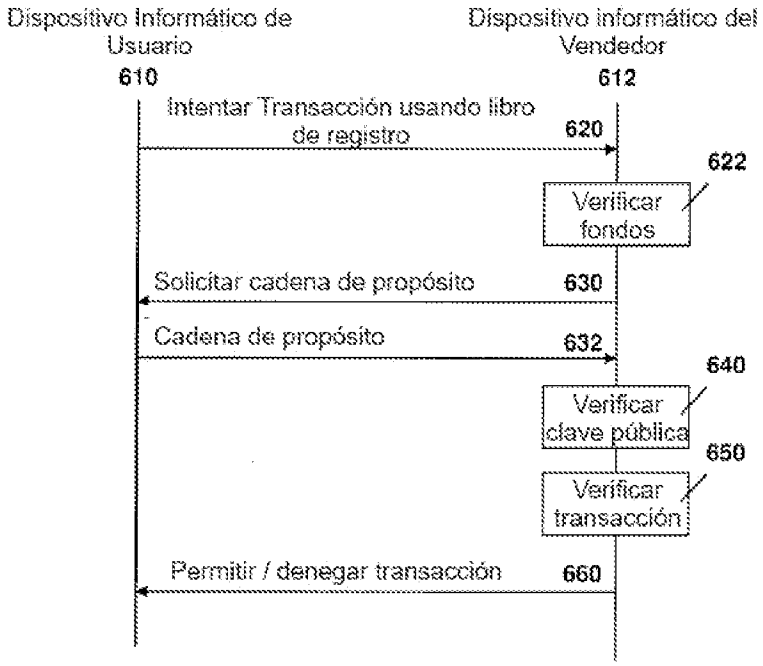
Dispositivo Informático de Usuario
610
Dispositivo informático del Vendedor
612
Intentar Transacción usando libro de registro
620
622
Verificar fondos
Solicitar cadena de propósito
630
Cadena de propósito
632
640
Verificar clave pública
650
Verificar transacción
Permitir / denegar transacción
660

FIG. 6

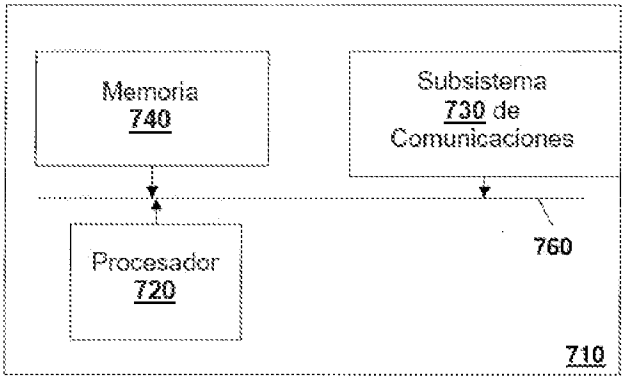
Memoria
740
Subsistema
730 de
Comunicaciones
760
Procesador
720
710

FIG. 7