(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 687 182**

(51) Int. CI.:

***G06Q 20/38*** (2012.01)
***H04L 9/30*** (2006.01)
***H04L 9/32*** (2006.01)
***H04L 9/08*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.02.2017 PCT/IB2017/050856**

(87) Fecha y número de publicación internacional: **31.08.2017 WO17145016**

(96) Fecha de presentación y número de la solicitud europea: **16.02.2017 E 17708586 (7)**

(97) Fecha y número de publicación de la concesión europea: **20.06.2018 EP 3268914**

(54) Título: **Determinar un secreto común para el intercambio seguro de información y claves criptográficas jerárquicas y deterministas**

(30) Prioridad:

**23.02.2016 GB 201603117**
**15.11.2016 GB 201619301**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**24.10.2018**

(73) Titular/es:

**NCHAIN HOLDINGS LIMITED (100.0%)**
**Fitzgerald House 44 Church Street**
**St. John's, AG**

(72) Inventor/es:

**WRIGHT, CRAIG STEVEN y**
**SAVANAH, STEPHANE**

(74) Agente/Representante:

**LEHMANN NOVO, María Isabel**

## DESCRIPCIÓN

Determinar un secreto común para el intercambio seguro de información y claves criptográficas jerárquicas y deterministas

Campo técnico

La presente divulgación se refiere a determinar un secreto común para dos nodos. En algunas aplicaciones, el secreto común puede usarse en la criptografía para permitir una comunicación segura entre dos nodos. La invención puede ser adecuada para usarse con, pero sin estar limitada a, carteras digitales, tecnologías de cadena de bloques (por ejemplo, Bitcoin) y seguridad de dispositivos personales.

Antecedentes

La criptografía implica técnicas para una comunicación segura entre dos o más nodos. Un nodo puede incluir un dispositivo de comunicación móvil, un ordenador de tipo tableta, un ordenador portátil, un ordenador de escritorio, otras formas de dispositivos informáticos y de dispositivos de comunicación, un dispositivo servidor en una red, un dispositivo cliente en una red, uno o más nodos en una red distribuida, etc. Los nodos pueden estar asociados a una persona natural, un grupo de personas tales como empleados de una empresa, un sistema tal como un sistema bancario, etc.

En algunos casos, los dos o más nodos pueden estar enlazados mediante una red de comunicaciones que no es segura. Por ejemplo, los dos nodos pueden estar enlazados mediante una red de comunicaciones en la que una tercera parte puede escuchar furtivamente la comunicación entre los nodos. Por lo tanto, los mensajes enviados entre nodos pueden enviarse de forma cifrada y, tras su recepción, los destinatarios previstos pueden descifrar los mensajes con claves de descifrado correspondientes (u otros procedimientos de descifrado). Por tanto, la seguridad de tal comunicación puede depender de impedir que la tercera parte determine la clave de descifrado correspondiente.

Un procedimiento de criptografía incluye usar algoritmos de clave simétrica. Las claves son simétricas en el sentido de que se usa la misma clave simétrica tanto para el cifrado de un mensaje de texto plano como el descifrado de texto cifrado. Una consideración a la hora de usar algoritmos de clave simétrica es cómo transmitir la clave simétrica a ambos nodos de manera segura para impedir que un intruso adquiera la clave simétrica. Esto puede incluir, por ejemplo, la entrega física de la clave simétrica a los nodos (autorizados), de manera que la clave simétrica nunca se transmite a través de una red de comunicaciones no segura. Sin embargo, la entrega física no es siempre una opción. Por lo tanto, un problema en tales sistemas criptográficos es el establecimiento de la clave simétrica (que puede estar basada en un secreto común) entre los nodos a través de una red no segura. En los últimos años, ciertas situaciones pueden hacer deseable que la transmisión de claves se realice normalmente de manera electrónica a través de sistemas de comunicación tal como Internet. Por tanto, esta etapa de proporcionar un secreto compartido (por ejemplo, la clave simétrica) es una vulnerabilidad potencialmente catastrófica. Puesto que los algoritmos (y protocolos) de clave simétrica son simples y se usan de manera generalizada, existe la necesidad de una capacidad para que dos nodos determinen de manera segura una clave secreta común a través de una red no segura.

Otros procedimientos de criptografía existentes incluyen usar claves asimétricas. Estas pueden usarse en criptografía de clave pública cuando las claves asimétricas incluyen una clave privada y una clave pública correspondiente. La clave pública puede volverse públicamente disponible mientras que la clave privada, como su nombre implica, se mantiene privada. Estas claves asimétricas pueden usarse en el cifrado de claves públicas y en la firma digital, entre otras cosas. Protocolos existentes, tales como el intercambio de claves de Diffie-Hellman y el Protocolo de Tres Pasadas, permiten la compartición segura de un secreto entre redes no seguras. Sin embargo, estos procedimientos son computacionalmente caros en algunos casos, por ejemplo cuando van a generarse y compartirse continuamente nuevos secretos.

Jerarquías de claves asimétricas alternativas (tales como las descritas en la Guía para Desarrolladores de Bitcoin) se basan en una semilla aleatoria y en una estructura de índices que da como resultado una mala gestión de claves. Por el contrario, las formas de realización de la presente invención pueden comprender el uso de ‘mensajes’ (M) provechosos, no solo para generar claves asimétricas, sino también secretos compartidos jerárquicos deterministas que están asociados, probablemente, a datos específicos.

Cualquier análisis de documentos, acciones, materiales, dispositivos, artículos o similares que se haya incluido en la presente memoria descriptiva no debe tomarse como la admisión de que alguno o todos estos contenidos forman parte de la base de la técnica anterior o del conocimiento general común en el campo pertinente a la presente divulgación que ya existiese antes de la fecha de prioridad de cada reivindicación de esta solicitud.

A lo largo de esta memoria descriptiva, debe entenderse que la palabra "comprender", o variaciones tales como "comprende" o "que comprende", implica la inclusión de un elemento, entero e etapa, o grupo de elementos, enteros

o etapas especificados, pero no la exclusión de cualquier otro elemento, entero o etapa, o grupo de elementos, enteros o etapas.

Resumen

El documento US 2015/213433 da a conocer un procedimiento según el preámbulo de la reivindicación 1.

Según un aspecto de la presente invención, se proporciona un procedimiento implementado por ordenador según la reivindicación 1.

Esto proporciona la ventaja de permitir que las segundas claves públicas se obtengan de manera independiente en cada nodo, aumentando de este modo la seguridad, mientras que también permite que una máquina genere subclaves automáticamente. También se proporciona la ventaja de tener entradas de transacción coincidentes que no pueden rastrearse, ya que la relación entre las claves públicas no puede determinarse por terceras partes. Por lo tanto, esto permite conseguir un mayor nivel de anonimato, mejorándose por tanto la seguridad.

La clave determinista (DK) puede estar basada en un mensaje (M). El procedimiento puede comprender además: generar un primer mensaje firmado (SM1) basado en el mensaje (M) y la segunda clave privada de primer nodo ($V_{2C}$); y enviar, a través de la red de comunicaciones, el primer mensaje firmado (SM1) al segundo nodo (S), donde el primer mensaje firmado (SM1) puede validarse con una segunda clave pública de primer nodo ($P_{2C}$) para autenticar el primer nodo (C).

El procedimiento puede comprender además: recibir, a través de la red de comunicaciones, un segundo mensaje firmado (SM2) desde el segundo nodo (S); validar el segundo mensaje firmado (SM2) con la segunda clave pública de segundo nodo ($P_{2S}$); y autenticar el segundo nodo (S) en función del resultado de validar el segundo mensaje firmado (SM2), donde el segundo mensaje firmado (SM2) se generó en función del mensaje (M), o un segundo mensaje (M2), y la segunda clave privada de segundo nodo ($V_{2S}$).

El procedimiento puede comprender además generar un mensaje (M); y enviar, a través de una red de comunicaciones, el mensaje (M) al segundo nodo (S). Como alternativa, el procedimiento puede comprender recibir el mensaje (M), a través de la red de comunicaciones, desde el segundo nodo (S). En otra alternativa adicional, el procedimiento puede comprender recibir el mensaje (M), a través de la red de comunicaciones, desde otro nodo. En otra alternativa adicional, el procedimiento puede comprender recibir el mensaje (M) desde una unidad de almacenamiento de datos y/o una interfaz de entrada asociadas al primer nodo (C).

La clave pública maestra de primer nodo ($P_{1C}$) y la clave pública maestra de segundo nodo ($P_{1S}$) pueden estar basadas en una multiplicación de puntos de curva elíptica de clave privada maestra de primer nodo ($V_{1C}$) y de clave privada maestra de segundo nodo ($V_{1S}$) respectivas y un generador (G).

El procedimiento puede comprender además las etapas de: recibir, a través de la red de comunicaciones, la clave pública maestra de segundo nodo ($P_{1S}$); y almacenar, en una unidad de almacenamiento de datos asociada al primer nodo (C), la clave pública maestra de segundo nodo ($P_{1S}$).

El procedimiento puede comprender además las etapas de: generar, en un primer nodo (C), la clave privada maestra de primer nodo ($V_{1C}$) y la clave pública maestra de primer nodo ($P_{1C}$); enviar, a través de la red de comunicaciones, la clave pública maestra de primer nodo ($P_{1C}$) al segundo nodo (S) y/u otro nodo; y almacenar, en una primera unidad de almacenamiento de datos asociada al primer nodo (C), la clave privada maestra de primer nodo ($V_{1C}$).

El procedimiento puede comprender además: enviar, a través de la red de comunicaciones, al segundo nodo, un aviso que indica el uso de un sistema de criptografía de curva elíptica (ECC) común con un generador (G) común para el procedimiento de determinar un secreto común (CS). La etapa de generar la clave privada maestra de primer nodo ($V_{1C}$) y la clave pública maestra de primer nodo ($P_{1C}$) puede comprender: generar la clave privada maestra de primer nodo ($V_{1C}$) en función de un entero aleatorio en un intervalo permitido especificado en el sistema ECC común; y determinar la clave pública maestra de primer nodo ($P_{1C}$) en función de la multiplicación de puntos de curva elíptica de la clave privada maestra de primer nodo ($V_{1C}$) y el generador (G) común según la siguiente fórmula:

$$P_{1C} = V_{1C} \times G$$

El procedimiento puede comprender además: determinar la clave determinista (DK) en función de determinar un elemento hash del mensaje (M), donde la etapa de determinar una segunda clave privada de primer nodo ($V_{2C}$) está basada en una suma escalar de la clave privada maestra de primer nodo ($V_{1C}$) y la clave determinista (DK) según la siguiente fórmula:

$$V_{2C} = V_{1C} + DK$$

La etapa de determinar una segunda clave pública de segundo nodo ($P_{2S}$) puede estar basada en la clave pública maestra de segundo nodo ($P_{1S}$) con la adición de puntos de curva elíptica a la multiplicación de puntos de curva elíptica de la clave determinista (DK) y el generador (G) común según la siguiente fórmula:

$$P_{2S} = P_{1S} + DK \times G.$$

La clave determinista (DK) puede basarse en determinar un elemento hash de una clave determinista anterior.

El primer par de criptografía asimétrica y el segundo par de criptografía asimétrica pueden estar basados en una función de un primer par de criptografía asimétrica anterior y un segundo par de criptografía asimétrica anterior.

Según otro aspecto de la presente invención, se proporciona un procedimiento según la reivindicación 7.

El procedimiento puede comprender además: recibir, a través de una red de comunicaciones, un segundo mensaje de comunicación cifrado desde el segundo nodo (S); y descifrar el segundo mensaje de comunicación cifrado, con la clave simétrica, para obtener un segundo mensaje de comunicación.

Según un aspecto adicional de la presente invención, se proporciona un procedimiento según la reivindicación 9. Según un aspecto adicional de la presente invención, se proporciona un dispositivo según la reivindicación 10.

Según un aspecto adicional de la presente invención, se proporciona un dispositivo según la reivindicación 11. El dispositivo puede comprender una primera unidad de almacenamiento de datos para almacenar una o más de la clave privada maestra de primer nodo ($V_{1C}$). La primera unidad de almacenamiento de datos también puede almacenar uno o más de la clave pública maestra de primer nodo ($P_{1C}$), la clave pública maestra de segundo nodo ($P_{1S}$) y el mensaje (M).

El dispositivo puede comprender además un módulo de comunicaciones para enviar y/o recibir, a través de una red de comunicaciones, uno o más del mensaje (M), la clave pública maestra de primer nodo ($P_{1C}$), la clave pública maestra de segundo nodo ($P_{1S}$), el primer mensaje firmado (SM1), el segundo mensaje firmado (SM2), y el aviso que indica el uso de un sistema de criptografía de curva elíptica (ECC) común con un generador (G) común.

Según un aspecto adicional de la presente invención, se proporciona un sistema según la reivindicación 14.

En el sistema, la clave determinista (DK) está basada en un mensaje (M), y el primer dispositivo de procesamiento está configurado además para: generar un primer mensaje firmado (SM1) basado en el mensaje (M) y la segunda clave privada de primer nodo ($V_{2C}$); y enviar, a través de la red de comunicaciones, el primer mensaje firmado (SM1) al segundo nodo (S). El segundo dispositivo de procesamiento puede estar configurado además para: recibir el primer mensaje firmado (SM1); validar el primer mensaje firmado (SM1) con la segunda clave pública de primer nodo ($P_{2C}$); y autenticar el primer nodo (C) en función del resultado del primer mensaje firmado (SM1) validado.

En el sistema, el segundo dispositivo de procesamiento puede estar configurado además para: generar un segundo mensaje firmado (SM2) basado en el mensaje (M), o un segundo mensaje (M2), y la segunda clave privada de segundo nodo ($V_{2S}$); enviar el segundo mensaje firmado (SM2) al primer nodo (C), donde el primer dispositivo de procesamiento está configurado además para: recibir el segundo mensaje firmado (SM2); validar el segundo mensaje firmado (SM2) con la segunda clave pública de segundo nodo ($P_{2S}$); autenticar el segundo nodo (S) en función de un resultado del segundo mensaje firmado (SM2) validado.

En el sistema, el primer dispositivo de procesamiento puede estar configurado además para: generar el mensaje (M); y enviar el mensaje (M), donde el segundo dispositivo de procesamiento está configurado para: recibir el mensaje (M). En una alternativa, el mensaje se genera mediante otro nodo, donde el primer dispositivo de procesamiento está configurado para: recibir el mensaje (M), y donde el segundo dispositivo de procesamiento está configurado para recibir el mensaje (M).

En otra alternativa adicional, el sistema comprende una unidad de almacenamiento de datos de sistema y/o una interfaz de entrada, donde el primer dispositivo de procesamiento y el segundo dispositivo de procesamiento reciben el mensaje (M), o el segundo mensaje (M2), desde la unidad de almacenamiento de datos de sistema y/o la interfaz de entrada.

El primer dispositivo de procesamiento puede recibir la clave pública maestra de segundo nodo ($P_{1S}$) desde la unidad de almacenamiento de datos de sistema y/o el dispositivo de entrada, y el segundo dispositivo de procesamiento puede recibir la clave pública maestra de primer nodo ($P_{1C}$) desde la unidad de almacenamiento de datos de sistema y/o el dispositivo de entrada.

La clave pública maestra de primer nodo ($P_{1C}$) y la clave pública maestra de segundo nodo ($P_{1S}$) pueden estar basadas en una multiplicación de puntos de curva elíptica de clave privada maestra de primer nodo ($V_{1C}$) y de clave privada maestra de segundo nodo ($V_{1S}$) respectivas y un generador (G).

El sistema puede comprender además: una primera unidad de almacenamiento de datos asociada al primer nodo (C) para almacenar la clave privada maestra de primer nodo ($V_{1C}$); y una segunda unidad de almacenamiento de datos asociada al segundo nodo (S) para almacenar la clave privada maestra de segundo nodo ($V_{1S}$).

En el sistema, el primer dispositivo de procesamiento puede estar configurado para: generar la clave privada maestra de primer nodo ($V_{1C}$) y la clave pública maestra de primer nodo ($P_{1C}$); enviar la clave pública maestra de primer nodo ($P_{1C}$); y almacenar la clave privada maestra de primer nodo ($V_{1C}$) en la primera unidad de almacenamiento de datos, donde el segundo dispositivo de procesamiento está configurado para: generar la clave privada maestra de segundo nodo ($V_{1S}$) y la clave pública maestra de segundo nodo ($P_{1S}$); enviar la clave pública maestra de segundo nodo ($P_{1S}$); y almacenar la clave privada maestra de segundo nodo ($V_{1S}$) en la segunda unidad de almacenamiento de datos.

En el sistema, la primera unidad de almacenamiento de datos puede recibir y almacenar la clave pública maestra de segundo nodo ($P_{1S}$); y la segunda unidad de almacenamiento de datos puede recibir y almacenar la clave pública maestra de primer nodo ($P_{1C}$).

En el sistema, el primer dispositivo de procesamiento puede estar configurado además para: generar la clave privada maestra de primer nodo ($V_{1C}$) en función de un entero aleatorio en un intervalo permitido especificado en un sistema de criptografía de curva elíptica (ECC) común; y determinar la clave pública maestra de primer nodo ($P_{1C}$) en función de la multiplicación de puntos de curva elíptica de la clave privada maestra de primer nodo ($V_{1C}$) y un generador (G) común según la siguiente fórmula:

$$P_{1C} = V_{1C} \times G$$

El segundo dispositivo de procesamiento puede estar configurado además para: generar la clave privada maestra de segundo nodo ($V_{1S}$) en función de un entero aleatorio en un intervalo permitido especificado en el sistema ECC común; y determinar la clave pública maestra de segundo nodo ($P_{1S}$) en función de la multiplicación de puntos de curva elíptica de la clave privada maestra de segundo nodo ($V_{1S}$) y el generador (G) común según la fórmula:

$$P_{1S} = V_{1S} \times G.$$

En el sistema, el primer dispositivo de procesamiento puede estar configurado para: determinar la clave determinista (DK) en función de un elemento hash del mensaje (M), y donde: la segunda clave privada de primer nodo ($V_{2C}$) está basada en una suma escalar de la clave privada maestra de primer nodo ($V_{1C}$) y la clave determinista (DK) según la fórmula:

$$V_{2C} = V_{1C} + DK$$

y la segunda clave pública de segundo nodo ($P_{2S}$) está basada en la clave pública maestra de segundo nodo ($P_{1S}$) con la adición de puntos de curva elíptica a la multiplicación de puntos de curva elíptica de la clave determinista (DK) y el generador (G) común según la siguiente fórmula:

$$P_{2S} = P_{1S} + DK \times G$$

El segundo dispositivo de procesamiento puede estar configurado además para: determinar la clave determinista (DK) en función de un elemento hash del mensaje (M), y donde la segunda clave privada de segundo nodo ($V_{2S}$) está basada en una suma escalar de la clave privada maestro de segundo nodo ($V_{1S}$) y la clave determinista (DK) según la fórmula:

$$V_{2S} = V_{1C} + DK$$

y la segunda clave pública de primer nodo ($P_{2C}$) está basada en la clave pública maestra de primer nodo ($P_{1C}$) con la adición de puntos de curva elíptica a la multiplicación de puntos de curva elíptica de la clave determinista (DK) y el generador (G) común según la siguiente fórmula:

$$P_{2C} = P_{1C} + DK \times G$$

El sistema puede comprender además: un primer módulo de comunicaciones asociado al primer dispositivo de procesamiento para enviar y/o recibir, a través de una red de comunicaciones, uno o más del mensaje (M), la clave pública maestra de primer nodo ($P_{1C}$), la clave pública maestra de segundo nodo ($P_{1S}$), el primer mensaje firmado (SM1), el segundo mensaje firmado (SM2), y un aviso que indica el uso de un sistema de criptografía de curva elíptica (ECC) común con un generador (G) común; y un segundo módulo de comunicaciones asociado al segundo dispositivo de procesamiento para enviar y/o recibir, a través de una red de comunicaciones, uno o más de entre el mensaje (M), la clave pública maestra de primer nodo ($P_{1C}$), la clave pública maestra de segundo nodo ($P_{1S}$), el primer mensaje firmado (SM1), el segundo mensaje firmado (SM2), y el aviso que indica el uso de un sistema de criptografía de curva elíptica (ECC) común con un generador (G) común.

En el sistema, la clave determinista (DK) puede estar basada en determinar un elemento hash de una clave determinista anterior.

En el sistema, el primer par de criptografía asimétrica y el segundo par de criptografía asimétrica pueden estar basados en una función de un primer par de criptografía asimétrica anterior y un segundo par de criptografía asimétrica anterior respectivos.

Según un aspecto adicional de la presente invención, se proporciona un sistema según la reivindicación 17. En el sistema de comunicación segura, el segundo dispositivo de procesamiento puede estar configurado además para: cifrar un segundo mensaje de comunicación, con la clave simétrica, para obtener el segundo mensaje de comunicación cifrado; y enviar el segundo mensaje de comunicación cifrado. El primer dispositivo de procesamiento puede estar configurado además para: recibir el segundo mensaje de comunicación cifrado; descifrar el segundo mensaje de comunicación cifrado, con la clave simétrica, para obtener el segundo mensaje de comunicación.

En el sistema antes descrito, el primer y el segundo mensaje de comunicación pueden ser mensajes de transacción entre el primer nodo y el segundo nodo para una transacción en línea entre el primer nodo y el segundo nodo.

Según un aspecto adicional de la presente invención, se proporciona un programa informático según la reivindicación 18.

Breve descripción de los dibujos

Ejemplos de la presente divulgación se describirán con referencia a:

la Fig. 1 es un diagrama esquemático de un sistema de ejemplo para determinar un secreto común para un primer nodo y un segundo nodo;

la Fig. 2 es un diagrama de flujo de procedimientos implementados por ordenador para determinar un secreto común;

la Fig. 3 es un diagrama de flujo de procedimientos implementados por ordenador para registrar el primer y el segundo nodo;

la Fig. 4 es otro diagrama de flujo de procedimientos implementados por ordenador para determinar un secreto común;

la Fig. 5 es un diagrama de flujo de procedimientos implementados por ordenador de comunicación segura entre el primer nodo y el segundo nodo;

la Fig. 6 es un diagrama esquemático de un sistema de ejemplo para el alquiler de recursos electrónicos;

la Fig. 7 es un diagrama esquemático de un sistema de ejemplo que aplica los procedimientos a la sustitución de contraseñas;

la Fig. 8 es un diagrama de flujo de procedimientos implementados por ordenador para autenticar el primer nodo y el segundo nodo;

la Fig. 9 es un ejemplo de una estructura en árbol de diferentes claves que tienen diferentes fines;

la Fig. 10 es un ejemplo de una estructura en árbol que usa el procedimiento de generación de claves maestras, y

la Fig. 11 ilustra una representación esquemática de un dispositivo de procesamiento de ejemplo.

Descripción de formas de realización

Visión general

A continuación se describirá un procedimiento, un dispositivo y un sistema para determinar un secreto común (CS) en un primer nodo (C) que es el mismo secreto común en un segundo nodo (S). La Fig. 1 ilustra un sistema 1 que incluye un primer nodo 3 que está en comunicación con, a través de una red de comunicaciones 5, un segundo nodo 7. El primer nodo 3 tiene un primer dispositivo de procesamiento 23 asociado y el segundo nodo 5 tiene un segundo dispositivo de procesamiento 27 asociado. El primer y el segundo nodo 3, 7 pueden incluir un dispositivo electrónico, tal como un ordenador, un ordenador de tipo tableta, un dispositivo de comunicación móvil, un servidor informático, etc. En un ejemplo, el primer nodo 3 puede ser un dispositivo cliente y el segundo nodo 7 un servidor.

El primer nodo 3 está asociado a un primer par de criptografía asimétrica que presenta una clave privada maestra de primer nodo ($V_{1C}$) y una clave pública maestra de primer nodo ($P_{1C}$). El segundo nodo (7) está asociado a un

segundo par de criptografía asimétrica que presenta una clave privada maestra de segundo nodo ($V_{1S}$) y una clave pública maestra de segundo nodo ($P_{1S}$). El primer y el segundo par de criptografía asimétrica para el primer y el segundo nodo 3, 7 respectivos pueden generarse durante el registro. Procedimientos de registro 100, 200 realizados por el primer y el segundo nodo 3, 7 se describirán en mayor detalle posteriormente con referencia a la Fig. 3. La clave pública para cada nodo puede compartirse de manera pública, tal como a través de la red de comunicaciones 5.

Para determinar el secreto común (CS) tanto en el primer nodo 3 como en el segundo nodo 7, los nodos 3, 7 llevan a cabo etapas de procedimientos respectivos 300, 400 sin comunicar claves privadas a través de la red de comunicaciones 5.

El procedimiento 300 realizado por el primer nodo 3 incluye determinar 330 una segunda clave privada de primer nodo ($V_{2C}$) en función de al menos la clave privada maestra de primer nodo ($V_{1C}$) y una clave determinista (DK). La clave determinista puede estar basada en un mensaje (M) compartido entre el primer y el segundo nodo, lo que puede incluir compartir el mensaje a través de la red de comunicación 5 como se describe posteriormente en mayor detalle. El procedimiento 300 incluye además determinar 370 una segunda clave pública de segundo nodo ($P_{2S}$) en función de al menos la clave pública maestra de segundo nodo ($P_{1S}$) y la clave determinista (DK). El procedimiento 300 incluye determinar 380 el secreto común (CS) en función de la segunda clave privada de primer nodo ($V_{2C}$) y la segunda clave pública de segundo nodo ($P_{2S}$).

Cabe señalar que el mismo secreto común (CS) también puede determinarse en el segundo nodo 7 mediante el procedimiento 400. El procedimiento 400 determina 430 una segunda clave pública de primer nodo ($P_{2C}$) en función de la clave pública maestra de primer nodo ($P_{1C}$) y la clave determinista (DK). El procedimiento 400 incluye además determinar 470 una segunda clave privada de segundo nodo ($V_{2S}$) en función de la clave privada maestra de segundo nodo ($V_{1S}$) y la clave determinista (DK). El procedimiento 400 incluye determinar 480 el secreto común (CS) en función de la segunda clave privada de segundo nodo ($V_{2S}$) y la segunda clave pública de primer nodo ($P_{2C}$).

La red de comunicaciones 5 puede incluir una red de área local, una red de área extensa, redes celulares, una red de comunicación radioeléctrica, Internet, etc. Estas redes, donde los datos pueden transmitirse a través de un medio de comunicaciones tal como un cable eléctrico, fibra óptica o de manera inalámbrica, pueden ser susceptibles de ser escuchadas furtivamente, tal como mediante un intruso 11. El procedimiento 300, 400 puede permitir que el primer nodo 3 y el segundo nodo 7 determinen de manera independiente un secreto común sin transmitir el secreto común a través de la red de comunicaciones 5. Por tanto, una ventaja es que el secreto común (CS) puede determinarse de manera segura mediante cada nodo sin tener que transmitir una clave privada a través de una red de comunicaciones 5 potencialmente no segura. A su vez, el secreto común puede usarse como una clave secreta (o como base de una clave secreta) para la comunicación cifrada entre el primer y el segundo nodo 3, 7 a través de la red de comunicaciones 5.

Los procedimientos 300, 400 pueden incluir etapas adicionales. El procedimiento 300 puede incluir, en el primer nodo 3, generar un mensaje firmado (SM1) en función del mensaje (M) y la segunda clave privada de primer nodo ($V_{2C}$). El procedimiento 300 incluye además enviar 360 el primer mensaje firmado (SM1, a través de la red de comunicaciones, al segundo nodo 7. A su vez, el segundo nodo 7 puede realizar las etapas de recibir 440 el primer mensaje firmado (SM1). El procedimiento 400 incluye además la etapa de validar 450 el primer mensaje firmado (SM1) con la segunda clave pública de primer nodo ($P_{2C}$) y autenticar 460 el primer nodo 3 en función del resultado de validación del primer mensaje firmado (SM1). De manera ventajosa, esto permite que el segundo nodo 7 autentique que el presunto primer nodo (en el que se ha generado el primer mensaje firmado) sea el primer nodo 3. Esto se basa en la suposición de que solamente el primer nodo 3 tiene acceso a la clave privada maestra de primer nodo ($V_{1C}$) y, por lo tanto, solamente el primer nodo 3 puede determinar la segunda clave privada de primer nodo ($V_{2C}$) para generar el primer mensaje firmado (SM1). Debe apreciarse que, de manera similar, un segundo mensaje firmado (SM2) puede generarse en el segundo nodo 7 y enviarse al primer nodo 3, de manera que el primer nodo 3 puede autenticar el segundo nodo 7, tal como en un escenario de igual a igual.

La compartición del mensaje (M) entre el primer y el segundo nodo puede conseguirse de varias formas. En un ejemplo, el mensaje puede generarse en el primer nodo 3, mensaje que se envía después, a través de la red de comunicaciones 5, al segundo nodo 7. Como alternativa, el mensaje puede generarse en el segundo 7 y después enviarse, a través de la red de comunicaciones 5, al segundo nodo 7. En otro ejemplo adicional, el mensaje puede generarse en un tercer nodo 9 y enviarse al primer y al segundo nodo 3, 7. En otra alternativa adicional, un usuario puede introducir el mensaje a través de una interfaz de usuario 15 para recibirse mediante el primer y el segundo nodo 3, 7. En otro ejemplo adicional, el mensaje (M) puede recuperarse de una unidad de almacenamiento de datos 19 y enviarse al primer y al segundo nodo 3, 7. En algunos ejemplos, el mensaje (M) puede ser público y, por lo tanto, puede transmitirse a través de una red no segura 5.

En otros ejemplos, uno o más mensajes (M) pueden almacenarse en una unidad de almacenamiento de datos 13, 17, 19, donde el mensaje puede estar asociado a una sesión, transacción, etc. entre el primer nodo 3 y el segundo nodo 7. Por tanto, los mensajes (M) pueden recuperarse y usarse para recrear, en el primer y el segundo nodo 3, 7 respectivos, el secreto común (CS) asociado a esa sesión o transacción. De manera ventajosa, puede mantenerse

un registro para permitir la recreación del secreto común (CS) sin que el propio registro tenga que almacenarse de manera privada o transmitirse de manera segura. Esto puede ser ventajoso si se llevan a cabo numerosas transacciones en el primer y el segundo nodo 3, 7, y sería poco práctico almacenar todos los mensajes (M) en los propios nodos.

Procedimiento de registro 100, 200

Un ejemplo de un procedimiento de registro 100, 200 se describirá con referencia a la Fig. 3, donde el procedimiento 100 se lleva a cabo mediante el primer nodo 3 y el procedimiento 200 se lleva a cabo mediante el segundo nodo 7. Esto incluye establecer el primer y el segundo par de criptografía asimétrica para el primer y el segundo nodo 3, 7 respectivos.

Los pares de criptografía asimétrica incluyen claves privadas y públicas asociadas, tales como las usadas en el cifrado de claves públicas. En este ejemplo, los pares de criptografía asimétrica se generan usando criptografía de curva elíptica (ECC) y propiedades de operaciones de curva elíptica.

Normas de la ECC pueden incluir normas conocidas tales como las descritas mediante las normas del Grupo de Criptografía Eficiente (www.sceg.org). La criptografía de curva elíptica también se describe en los documentos US 5.600.725, US 5.761.305, US 5.889.865, US 5.896.455, US 5.933.504, US 6.122.736, US 6.141.420, US 6.618.483, US 6.704.870, US 6.785.813, US 6.078.667 y US 6.792.530.

En el procedimiento 100, 200, esto incluye el establecimiento 110, 210 del primer y del segundo nodo en un sistema ECC común y el uso de un generador (G) común. En un ejemplo, el sistema ECC común puede estar basado en secp256K1, que es un sistema ECC usado por Bitcoin. El generador (G) común puede seleccionarse, generarse de manera aleatoria o asignarse.

Haciendo referencia a continuación al primer nodo 3, el procedimiento 100 incluye el establecimiento 110 en el sistema ECC común y el generador (G) común. Esto puede incluir recibir el sistema ECC común y el generador común desde el segundo nodo 7 o un tercer nodo 9. Como alternativa, una interfaz de usuario 15 puede estar asociada al primer nodo 3, donde un usuario puede proporcionar de manera selectiva el sistema ECC común y/o un generador (G) común. En otra alternativa adicional, el sistema ECC común y/o el generador (G) común pueden seleccionarse de manera aleatoria por el primer nodo 3. El primer nodo 3 puede enviar, a través de la red de comunicaciones 5, un aviso que indica el uso del sistema ECC común con un generador (G) común al segundo nodo 7. A su vez, el segundo nodo 7 puede establecerse 210 enviando un aviso que indica un acuse de recibo para usar el sistema ECC común y el generador (G) común.

El procedimiento 100 también incluye que el primer nodo 3 genere 120 un primer par de criptografía asimétrica que incluye la clave privada maestra de primer nodo ($V_{1C}$) y la clave pública maestra de primer nodo ($P_{1C}$). Esto incluye generar la clave privada maestra de primer nodo ($V_{1C}$) en función de, al menos en parte, un entero aleatorio en un intervalo permitido especificado en el sistema ECC común. Esto también incluye determinar la clave pública maestra de primer nodo ($P_{1C}$) en función de la multiplicación de puntos de curva elíptica de la clave privada maestra de primer nodo ($V_{1C}$) y el generador (G) común según la fórmula:

$$P_{1C} = V_{1C} \times G \qquad \text{(Ecuación 1)}$$

Por tanto, el primer par de criptografía asimétrica incluye:

$V_{1C}$: La clave privada maestra de primer nodo que se mantiene secreta mediante el primer nodo.

$P_{1C}$: La clave pública maestra de primer nodo que se conoce públicamente.

El primer nodo 3 puede almacenar la clave privada maestra de primer nodo ($V_{1C}$) y la clave pública maestra de primer nodo ($P_{1C}$) en una primera unidad de almacenamiento de datos 13 asociada al primer nodo 3. Por seguridad, la clave privada maestra de primer nodo ($V_{1C}$) puede almacenarse en una parte segura de la primera unidad de almacenamiento de datos 13 para garantizar que la clave siga siendo privada.

El procedimiento 100 incluye además enviar 130 la clave pública maestra de primer nodo ($P_{1C}$), a través de la red de comunicaciones 5, al segundo nodo 7. El segundo nodo 7 puede, tras recibir 220 la clave pública maestra de primer nodo ($P_{1C}$), almacenar 230 la clave pública maestra de primer nodo ($P_{1C}$) en una segunda unidad de almacenamiento de datos 17 asociada al segundo nodo 7.

De manera similar al primer nodo 3, el procedimiento 200 del segundo nodo 7 incluye generar 240 un segundo par de criptografía asimétrica que incluye la clave privada maestra de segundo nodo ($V_{1S}$) y la clave pública maestra de segundo nodo ($P_{1S}$). La clave privada maestra de segundo nodo ($V_{1S}$) es también un entero aleatorio dentro del

intervalo permitido. A su vez, la clave pública maestra de segundo nodo ($P_{1S}$) se determina mediante la siguiente fórmula:

$$P_{1S} = V_{1S} \times G \qquad \text{(Ecuación 2)}$$

Por tanto, el segundo par de criptografía asimétrica incluye:

$V_{1S}$: La clave privada maestra de segundo nodo que se mantiene secreta mediante el primer nodo.

$P_{1S}$: La clave pública maestra de segundo nodo que se conoce públicamente.

El segundo nodo 7 puede almacenar el segundo par de criptografía asimétrica en la segunda unidad de almacenamiento de datos 17. El procedimiento 200 incluye además enviar 250 la clave pública maestra de segundo nodo ($P_{1S}$) al primer nodo 3. A su vez, el primer nodo 3 puede recibir 140 y almacenar 150 la clave pública maestra de segundo nodo ($P_{1S}$).

Debe apreciarse que, en algunas alternativas, las claves maestras públicas respectivas pueden recibirse y almacenarse en una tercera unidad de almacenamiento de datos 19 asociada al tercer nodo 9 (tal como una tercera parte fiable). Esto puede incluir una tercera parte que actúe como un directorio público, tal como una autoridad de certificación. Por tanto, en algunos ejemplos, la clave pública maestra de primer nodo ($P_{1C}$) puede solicitarse y recibirse por el segundo nodo 7 solamente cuando sea necesario determinar el secreto común (CS) (y viceversa).

Es posible que las etapas de registro solo tengan que llevarse a cabo una vez como una configuración inicial. Después, las claves maestras pueden reutilizarse de manera segura para generar secretos comunes que dependen, entre otras cosas, de la clave determinista (DK).

Inicio de sesión y determinación del secreto común mediante el primer nodo 3

A continuación se describirá un ejemplo de la determinación de un secreto común (CS) con referencia a la Fig. 4. El secreto común (CS) puede usarse durante una sesión, tiempo, transacción particulares, u otro fin, entre el primer nodo 3 y el segundo nodo 7, y puede no ser deseable, o seguro, usar el mismo secreto común (CS). Por tanto, el secreto común (CS) puede cambiarse entre diferentes sesiones, tiempos, transacciones, etc.

*Generación de un mensaje (M) 310*

En este ejemplo, el procedimiento 300 realizado por el primer nodo 3 incluye generar 310 un mensaje (M). El mensaje (M) puede ser aleatorio, seudoaleatorio o definido por el usuario. En un ejemplo, el mensaje (M) está basado en tiempo Unix y un *nonce* (un valor arbitrario). Por ejemplo, el mensaje (M) puede proporcionarse como:

$$\text{Mensaje}\ (M) = \text{TiempoUnix} + \text{nonce} \qquad \text{(Ecuación 3)}$$

En algunos ejemplos, el mensaje (M) es arbitrario. Sin embargo, debe apreciarse que el mensaje (M) puede tener valores selectivos (tales como tiempo Unix, etc.) que pueden ser útiles en algunas aplicaciones.

El procedimiento 300 incluye enviar 315 el mensaje (M), a través de la red de comunicaciones 3, al segundo nodo 7. El mensaje (M) puede enviarse a través de una red no segura ya que el mensaje (M) no incluye información acerca de las claves privadas.

*Determinación de una clave determinista 320*

El procedimiento 300 incluye además la etapa de determinar 320 una clave determinista (DK) en función del mensaje (M). En este ejemplo, esto incluye determinar un elemento hash criptográfico del mensaje. Un ejemplo de un algoritmo de hash criptográfico incluye SHA-256 para crear una clave determinista (DK) de 256 bits. Es decir:

$$DK = \text{SHA-256}(M) \qquad \text{(Ecuación 4)}$$

Debe apreciarse que pueden usarse otros algoritmos de hash. Esto puede incluir otros algoritmos de la familia de Algoritmo de Hash Seguro (SHA). Algunos ejemplos particulares incluyen instancias del subconjunto SHA-3, incluidos SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256. Otros algoritmos de hash pueden incluir los la de la familia de Primitivas de Integridad de Resumen de Mensaje (RIPEMD, *RACE Integrity Primitives Evaluation Message Digest*). Un ejemplo particular puede incluir RIPEMD-160. Otras funciones hash pueden incluir familias basadas en funciones hash de Zémor-Tillich y en funciones hash basadas en knapsack.

*Determinación de una segunda clave privada de primer nodo 330*

El procedimiento 300 incluye entonces la etapa 330 de determinar 330 la segunda clave privada de primer nodo ($V_{2C}$) en función de la clave privada maestra de segundo nodo ($V_{1C}$) y la clave determinista (DK). Esto puede basarse en una suma escalar de la clave privada maestra de primer nodo ($V_{1C}$) y la clave determinista (DK) según la siguiente fórmula:

$$V_{2C} = V_{1C} + DK \qquad \text{(Ecuación 5)}$$

Por tanto, la segunda clave privada de primer nodo ($V_{2C}$) no es un valor aleatorio, sino que, en cambio, se obtiene de manera determinista a partir de la clave privada maestra de primer nodo. La clave pública correspondiente en el par criptográfico, en concreto la segunda clave pública de primer nodo ($P_{2C}$), tiene la siguiente relación:

$$P_{2C} = V_{2C} \times G \qquad \text{(Ecuación 6)}$$

La sustitución de $V_{2C}$ de la ecuación 5 en la ecuación 6 proporciona:

$$P_{2C} = (V_{1C} + DK) \times G \qquad \text{(Ecuación 7)}$$

Donde el operador '+' se refiere a una suma escalar y el operador 'x' se refiere a la multiplicación de puntos de curva elíptica. Debe observarse que el álgebra de criptografía de curva elíptica es distributiva, por lo que la ecuación 7 puede expresarse como:

$$P_{2C} = V_{1C} \times G + DK \times G \qquad \text{(Ecuación 8)}$$

Finalmente, la Ecuación 1 puede sustituirse en la Ecuación 7 para proporcionar:

$$P_{2C} = P_{1C} + DK \times G \qquad \text{(Ecuación 9.1)}$$

$$P_{2C} = P_{1C} + \text{SHA-256}(M) \times G \qquad \text{(Ecuación 9.2)}$$

En las ecuaciones 8 a 9.2, el operador '+' se refiere a la suma de puntos de curva elíptica. Por tanto, la segunda clave pública de primer nodo ($P_{2C}$) correspondiente puede obtenerse conociendo la clave pública maestra de primer nodo ($P_{1C}$) y el mensaje (M). El segundo nodo 7 puede conocer esto para determinar de manera independiente la segunda clave pública de primer nodo ($P_{2C}$), como se describirá posteriormente en mayor detalle con respecto al procedimiento 400.

*Generación de un primer mensaje firmado (SM1) en función del mensaje y la segunda clave privada de primer nodo 350*

El procedimiento 300 incluye, además, generar 350 un primer mensaje firmado (SM1) en función del mensaje (M) y la segunda clave privada de primer nodo ($V_{2C}$). La generación de un mensaje firmado incluye aplicar un algoritmo de firma digital para firmar digitalmente el mensaje (M). En un ejemplo, esto incluye aplicar la segunda clave privada de primer nodo ($V_{2C}$) al mensaje en un Algoritmo de Firma Digital de Curva Elíptica (ECDSA) para obtener el primer mensaje firmado (SM1).

Ejemplos de ECDSA incluyen los basados en sistemas ECC con secp256k1, secp256r1, secp384r1, se3cp521r1.

El primer mensaje firmado (SM1) puede verificarse con la segunda clave pública de primer nodo ($P_{2C}$) en el segundo nodo 7. Esta verificación del primer mensaje firmado (SM1) puede usarse por el segundo nodo 7 para autenticar el primer nodo 3, lo que se describirá posteriormente en el procedimiento 400.

*Determinación de una segunda clave pública de segundo nodo 370'*

El primer nodo 3 puede determinar entonces, 370, una segunda clave pública de segundo nodo ($P_{2S}$). Como se ha descrito anteriormente, la segunda clave pública de segundo nodo ($P_{2S}$) puede estar basada al menos en la clave pública maestra de segundo nodo ($P_{1S}$) y la clave determinista (DK). En este ejemplo, puesto que la clave pública se determina 370' como la clave privada con multiplicación de puntos de curva elíptica con el generador (G), la segunda clave pública de segundo nodo ($P_{2S}$) puede expresarse, de manera similar a la Ecuación 6, como:

$$P_{2S} = V_{2S} \times G \qquad \text{(Ecuación 10.1)}$$

$$P_{2S} = P_{1S} + DK \times G \qquad \text{(Ecuación 10.2)}$$

La demostración matemática de la Ecuación 10.2 es la misma que la descrita anteriormente para obtener la Ecuación 9.1 referente a la segunda clave pública de primer nodo ($P_{2C}$). Debe apreciarse que el primer nodo 3 puede determinar 370 la segunda clave pública de segundo nodo independientemente del segundo nodo 7.

*Determinar el secreto común 380 en el primer nodo 3*

El primer nodo 3 puede determinar entonces, 380, el secreto común (CS) en función de la segunda clave privada de primer nodo ($V_{2C}$) determinada y la segunda clave pública de segundo nodo ($P_{2S}$) determinada. El secreto común (CS) puede determinarse por el primer nodo 3 mediante la siguiente fórmula:

$$S = V_{2C} \times P_{2S} \qquad \text{(Ecuación 11)}$$

Procedimiento 400 realizado en el segundo nodo 7

A continuación se describirá el procedimiento 400 correspondiente realizado en el segundo nodo 7. Debe apreciarse que algunas de estas etapas son similares a las descritas anteriormente llevadas a cabo por el primer nodo 3.

El procedimiento 400 incluye recibir 410 el mensaje (M), a través de la red de comunicaciones 5, desde el primer nodo 3. Esto puede incluir el mensaje (M) enviado por el primer nodo 3 en la etapa 315. El segundo nodo 7 determina entonces, 420, una clave determinista (DK) en función del mensaje (M). La etapa de determinar 420 la clave determinista (DK) mediante el segundo nodo 7 es similar a la etapa 320 realizada por el primer nodo descrito anteriormente. En este ejemplo, el segundo nodo 7 realiza esta etapa de determinación 420 independientemente del primer nodo 3.

La siguiente etapa incluye determinar 430 una segunda clave pública de primer nodo ($P_{2C}$) en función de la clave pública maestra de primer nodo ($P_{1C}$) y la clave determinista (DK). En este ejemplo, puesto que la clave pública se determina 430' como la clave privada con multiplicación de puntos de curva elíptica con el generador (G), la segunda clave pública de primer nodo ($P_{2C}$) puede expresarse, de manera similar a la Ecuación 9, como:

$$P_{2C} = V_{2C} \times G \qquad \text{(Ecuación 12.1)}$$

$$P_{2C} = P_{1C} + DK \times G \qquad \text{(Ecuación 12.2)}$$

La demostración matemática de las Ecuaciones 12.1 y 12.2 es la misma que la descrita anteriormente para las Ecuaciones 10.1 y 10.2.

*El segundo nodo 7 autentica el primer nodo 3*

El procedimiento 400 puede incluir etapas llevadas a cabo por el segundo nodo 7 para autenticar que el presunto primer nodo 3 es el primer nodo 3. Como se ha descrito anteriormente, esto incluye recibir 440 el primer mensaje firmado (SM1) desde el primer nodo 3. Después, el segundo nodo 7 puede validar 450 la firma del primer mensaje firmado (SM1) con la segunda clave pública de primer nodo ($P_{2C}$) que se determinó en la etapa 430.

La verificación de la firma digital puede realizarse según un Algoritmo de Firma Digital de Curva Elíptica (ECDSA), como se ha descrito anteriormente. Cabe señalar que el primer mensaje firmado (SM1) que se firmó con la segunda clave privada de primer nodo ($V_{2C}$) solo debería verificarse correctamente con la segunda clave pública de primer nodo ($P_{2C}$) correspondiente, ya que $V_{2C}$ y $P_{2C}$ forman un par criptográfico. Puesto que estas claves son deterministas en la clave privada maestra de primer nodo ($V_{1C}$) y en la clave pública maestra de primer nodo ($P_{1C}$) que se generaron en el registro del primer nodo 3, la verificación del primer mensaje firmado (SM1) puede usarse como base de la autenticación de que un supuesto primer nodo que envía el primer mensaje firmado (SM1) es el mismo primer nodo 3 durante el registro. Por tanto, el segundo nodo 7 puede llevar a cabo además la etapa de autenticar (460) el primer nodo 3 en función del resultado de validar (450) el primer mensaje firmado.

La autenticación anterior puede ser adecuada en escenarios en los que uno de los dos nodos es un nodo fiable y solamente es necesario autenticar uno de los nodos. Por ejemplo, el primer nodo 3 puede ser un cliente y el segundo nodo 7 puede ser un servidor del que se fía el cliente. Por tanto, el servidor (segundo nodo 7) puede necesitar autenticar los credenciales del cliente (primer nodo 3) con el fin de permitir que el cliente acceda al sistema servidor. Puede no ser necesario que el servidor autentique los credenciales del servidor con respecto al cliente. Sin embargo, en algunos escenarios, puede ser deseable que ambos nodos se autentiquen entre sí, tal como en un escenario de igual a igual que se describirá posteriormente en otro ejemplo.

*El segundo nodo 7 determina el secreto común*

El procedimiento 400 puede incluir además que el segundo nodo 7 determine 470 una segunda clave privada de segundo nodo ($V_{2S}$) en función de la clave privada maestra de segundo nodo ($V_{1S}$) y la clave determinista (DK). De

manera similar a la etapa 330 realizada por el primer nodo 3, la segunda clave privada de segundo nodo ($V_{2S}$) puede estar basada en una suma escalar de la clave privada maestra de segundo nodo ($V_{1S}$) y la clave determinista (DK) según las siguientes fórmulas:

$$V_{2S} = V_{1S} + DK \quad \text{( Ecuación 13.1)}$$

$$V_{2S} = V_{1S} + \text{SHA-256}(M) \quad \text{( Ecuación 13.2)}$$

Después, el segundo nodo 7 puede determinar 480, de manera independiente al primer nodo 3, el secreto común (CS) en función de la segunda clave privada de segundo nodo ($V_{2S}$) y la segunda clave pública de primer nodo ($P_{2C}$) según la siguiente fórmula:

$$S = V_{2S} \times P_{2C} \quad \text{( Ecuación 14)}$$

*Demostración del secreto común (CS) determinado por el primer nodo 3 y el segundo nodo 7*

El secreto común (CS) determinado por el primer nodo 3 es el mismo que el secreto común (CS) determinado en el segundo nodo 7. A continuación se describirá la demostración matemática de la Ecuación 11 y la Ecuación 14 proporcionan el mismo secreto común (CS).

Haciendo referencia al secreto común (CS) determinado por el primer nodo 3, la Ecuación 10.1 puede sustituirse en la Ecuación 11 de la siguiente manera:

$$S = V_{2C} \times P_{2S} \quad \text{( Ecuación 11)}$$
$$S = V_{2C} \times (V_{2S} \times G)$$

$$S = (V_{2C} \times V_{2S}) \times G \quad \text{( Ecuación 15)}$$

Haciendo referencia al secreto común (CS) determinado por el segundo nodo 7, la Ecuación 12.1 puede sustituirse en la Ecuación 14 de la siguiente manera:

$$S = V_{2S} \times P_{2C} \quad \text{( Ecuación 14)}$$
$$S = V_{2S} \times (V_{2C} \times G)$$

$$S = (V_{2S} \times V_{2C}) \times G \quad \text{( Ecuación 16)}$$

Puesto que el álgebra ECC es conmutativa, la Ecuación 15 y la Ecuación 16 son equivalentes, puesto que:

$$S = (V_{2C} \times V_{2S}) \times G = (V_{2S} \times V_{2C}) \times G \quad \text{( Ecuación 17)}$$

*El secreto común (CS) y la clave secreta*

El secreto común (CS) puede usarse como una clave secreta o como base de una clave secreta en un algoritmo de clave simétrica para garantizar la comunicación entre el primer nodo 3 y el segundo nodo 7.

El secreto común (CS) puede estar en forma de un punto de curva elíptica ($x_S$, $y_S$). Éste puede convertirse en un formato de clave estándar usando operaciones estándar públicamente conocidas acordadas por los nodos 3, 7. Por ejemplo, el valor $x_S$ puede ser un entero de 256 bits que pueden usarse como una clave para el cifrado $AES_{256}$. También puede convertirse en un entero de 160 bits usando RIPEMD 160 en cualquier aplicación que requiera esta clave de longitud.

El secreto común (CS) puede determinarse según sea necesario. Cabe señalar que el primer nodo 3 no tiene que almacenar el secreto común (CS) ya que éste puede volverse a determinar en función del mensaje (M). En algunos ejemplos, el/los mensaje(s) (M) usado(s) puede(n) almacenarse en una unidad de almacenamiento de datos 13, 17, 19 (o en otras unidades de almacenamiento de datos) sin el mismo nivel de seguridad que el requerido para las claves privadas maestras. En algunos ejemplos, el mensaje (M) puede estar públicamente disponible.

Sin embargo, dependiendo de algunas aplicaciones, el secreto común (CS) podría almacenarse en la primera unidad de almacenamiento de datos (X) asociada al primer nodo siempre que el secreto común (CS) se mantenga seguro como clave privada maestra de primer nodo ($V_{1C}$).

Además, el sistema dado a conocer puede permitir la determinación de múltiples secretos comunes que pueden corresponder a múltiples claves secretas seguras basadas en un único par de criptografía de claves maestras. Una ventaja de esto puede ilustrarse mediante el siguiente ejemplo.

En situaciones en las que hay múltiples sesiones, cada una asociada a múltiples secretos comunes (CS) respectivos, puede ser deseable tener un registro asociado a esas múltiples sesiones de manera que los secretos comunes (CS) respectivos puedan volver a determinarse en el futuro. En sistemas conocidos, esto puede requerir que se almacenen múltiples claves secretas en una unidad de almacenamiento de datos segura, que puede ser cara o engorrosa de mantener. Por el contrario, el presente sistema mantiene seguras las claves privadas maestras en el primer y el segundo nodo respectivos, mientras que las otras claves deterministas, o el mensaje (M), pueden almacenarse de manera segura o no. A pesar de que las claves deterministas (DK), o el mensaje (M), se almacenen de manera no segura, los múltiples secretos comunes (CS) se mantienen seguros ya que las claves privadas maestras requeridas para determinar los secretos comunes siguen siendo seguras.

El procedimiento también puede usarse para generar "claves de sesión" para enlaces de comunicación temporales, tales como para transmitir de manera segura contraseñas de acceso al sistema.

Aplicaciones de ejemplo

Los procedimientos, dispositivos y sistemas de la presente divulgación pueden tener diversas aplicaciones, incluidas, pero sin limitarse a, las descritas a continuación.

Cifrado de mensajes

La presente divulgación puede usarse para facilitar una comunicación segura, en particular el envío y la recepción de mensajes de comunicación, entre el primer nodo 3 y el segundo nodo 7 a través de una red de comunicaciones 5 potencialmente no segura. Esto puede conseguirse usando el secreto común (CS) como la base para una clave simétrica. Este procedimiento de determinar un secreto común (CS) y usar la clave simétrica para el cifrado y descifrado de los mensajes de comunicación puede ser más eficiente desde un punto de vista computacional en comparación con los procedimientos conocidos de cifrado de clave pública.

A continuación se describirán procedimientos 500, 600 de comunicación segura entre el primer nodo 3 y el segundo nodo 7 con referencia a la Fig. 5. El primer nodo 3 determina 510 una clave simétrica basándose en el secreto común (CS) determinado en el procedimiento anterior. Esto puede incluir convertir el secreto común (CS) en un formato de clave estándar. Asimismo, el segundo nodo 7 también puede determinar 610 la clave simétrica basándose en el secreto común (CS).

Para enviar un primer mensaje de comunicación de manera segura desde el primer nodo 3, a través de la red de comunicaciones, al segundo nodo, el primer mensaje de comunicación tiene que cifrarse. Por tanto, el primer nodo usa la clave simétrica para cifrar 520 un primer mensaje de comunicación para formar un primer mensaje de comunicación cifrado, que se envía después, 530, a través de la red de comunicaciones 5, al segundo nodo 7. A su vez, el segundo nodo 7 recibe 620 el primer mensaje de comunicación cifrado 620 y descifra 630 el primer mensaje de comunicación cifrado, con la clave simétrica, para obtener el primer mensaje de comunicación.

Asimismo, el segundo nodo 7 puede cifrar 640 un segundo mensaje de comunicación, con la clave simétrica, para obtener un segundo mensaje de comunicación cifrado, que se envía después, 650, al primer nodo 3. Después, el primer nodo 3 puede recibir 540 el segundo mensaje de comunicación cifrado y descifrarlo 550 para obtener el segundo mensaje de comunicación.

Cartera de criptomonedas

En otro ejemplo, el procedimiento puede usarse para la generación y gestión de secretos comunes (CS) tales como claves secretas para transacciones de criptomonedas. Las claves de criptomonedas, tales como las usadas en transacciones de Bitcoin, están asociadas normalmente a fondos y activos que pueden intercambiarse por un valor.

Alquiler de recursos electrónicos

Haciendo referencia a la Fig. 6 se describirá un ejemplo que usa el procedimiento y el sistema para facilitar el alquiler de recursos electrónicos. Se ilustra un sistema 701 en el que el primer nodo 3 está asociado a un cliente 703 y el segundo nodo 7 está asociado a un recurso electrónico, tal como un superordenador 707. Por tanto, el cliente 504 puede desear usar el superordenador 707 ubicado de manera remota para procesar grandes cantidades de datos confidenciales.

El superordenador 707 puede alquilar el tiempo de CPU de superordenador por ciclo de tiempo y/o por ciclo de CPU. El cliente 703 puede registrarse en el superordenador depositando su clave pública, tal como enviando 130, a través de una red de comunicaciones 5, la clave pública maestra de primer nodo ($P_{1C}$) al segundo nodo 7.

El superordenador 707 puede proporcionar entonces software al cliente 703 para llevar a cabo procesos en segundo plano, tal como establecer conexiones seguras usando cifrado AES, y para facilitar las etapas del procedimiento 300 descrito anteriormente.

Cuando se lleva a cabo el procedimiento 300, el primer nodo 3 puede enviar 360 un primer mensaje firmado (SM1) que, en parte, está basado en un mensaje (M) que incluye el tiempo Unix concatenado con un *nonce*.

El segundo nodo 7 puede recibir 440 el primer mensaje firmado (SM1). El segundo nodo 7 puede llevar a cabo, además, la etapa de determinar si el tiempo Unix en el mensaje (M) está dentro de un valor permitido para el tiempo Unix. Por ejemplo, el valor permitido para el tiempo Unix puede fijarse según las condiciones establecidas entre el cliente 703 y el superordenador 707. Por ejemplo, puede ser necesario que el tiempo Unix (del mensaje) esté dentro de un periodo fijado (por ejemplo, 300 segundos) referente a cuándo el superordenador recibe 440 el primer mensaje firmado (SM1). Si el tiempo Unix en el mensaje (M) está fuera del tiempo permitido, no se aceptará el intercambio de datos confidenciales.

Las etapas anteriores pueden garantizar que la clave de sesión resultante, que está basada en el secreto común (CS) determinado en las etapas 380, 480, no pueda reproducirse nunca posteriormente y sea única a la sesión que está estableciéndose. Un protocolo puede usarse entonces para establecer una clave de sesión simétrica, tal como una clave de cifrado/descifrado AES, durante toda la sesión. La clave de sesión se usa en todas las comunicaciones entre el primer nodo 3 y el segundo nodo 7 durante toda la sesión. Esto permite al cliente cifrar código y/o grandes cantidades de datos, enviarlos al superordenador 707 para su procesamiento y recibir resultados cifrados desde el superordenador 707.

Sustitución, complemento o alternativa a las contraseñas

El sistema y procedimiento también puede usarse como una sustitución, complemento o alternativa a las contraseñas. Haciendo referencia a la Fig. 7 se proporciona un sistema que incluye un primer nodo 3 asociado a un usuario y una pluralidad de nodos adicionales 7', 7", 7"'. Cada nodo de la pluralidad de nodos adicionales puede estar asociado a instituciones respectivas que participan en el mismo protocolo. Por ejemplo, las instituciones pueden incluir bancos, proveedores de servicio, servicios gubernamentales, agencias de seguros, proveedores de telecomunicación, minoristas, etc.

El usuario 803 puede desear comunicarse con estas instituciones, de manera segura, para acceder a servicios. En sistemas conocidos, esto puede requerir que el usuario tenga múltiples contraseñas para registrarse en cada una de las respectivas instituciones. Usar la misma contraseña para registrarse en múltiples instituciones no es deseable por motivos de seguridad.

En este ejemplo, el usuario y las múltiples instituciones se establecen usando el mismo protocolo. Esto puede incluir establecerse en el sistema ECC (tal como los basados en secp256k1, secp256r1, secp384r1, secp521r1) y un generador (G). El usuario puede registrar y compartir entonces la clave pública maestra de primer nodo ($P_{1C}$) con la pluralidad de instituciones y nodos adicionales asociados 7', 7", 7"'. Cada nodo adicional 7', 7", 7"' puede llevar a cabo las etapas del procedimiento de manera similar al segundo nodo 7 descrito anteriormente.

Cada vez que el usuario 803 desea registrarse en uno de los sitios web de una institución participante no necesita usar una contraseña. En cambio, el protocolo elimina la necesidad de contraseñas en cada institución. Todo lo que se necesita en el primer nodo 3 es la clave pública de la institución, que está siempre disponible, y que el usuario se registre en las instituciones (incluido el registro de la clave pública maestra de primer nodo ($P_{1C}$) en la institución). Puesto que el registro por parte del usuario en una institución es una práctica habitual para usar servicios basados en web, esto no supone una carga para el usuario 803. Una vez que ha finalizado el registro, puede determinarse un secreto común (CS) y usarse y reutilizarse en lugar de una contraseña. Por ejemplo, al inicio de cada sesión, el primer nodo 3 puede generar 310 un mensaje (M) que se envía al nodo adicional 7', 7", 7"' implicado en la sesión. El mensaje (M) se usa para determinar 320, 420 una clave determinista correspondiente que es usada después tanto por el primer nodo 3 como por el nodo adicional 7', 7", 7"' para determinar el secreto común (CS) como se ha descrito en los procedimientos anteriores. Como alternativa, el mensaje (M) puede generarse o recibirse desde el nodo adicional 7', 7", 7". En otra alternativa adicional, el mensaje (M) puede ser un mensaje predeterminado almacenado en una unidad de almacenamiento de datos 13, 17, 19 accesible por el primer nodo 3 y/o el nodo adicional 7', 7", 7"'.

Esta técnica mitiga una considerable carga en la seguridad de las instituciones. En particular, ya no tienen que mantener un archivo de contraseñas (registro secreto de contraseñas o elementos hash de contraseñas) ya que el secreto común puede recalcularse a partir de información no secreta. En cambio, la institución solo necesita mantener segura su propia clave privada maestra. Además, el usuario no tiene que memorizar o almacenar de

manera segura muchas contraseñas (una para cada institución) siempre que pueda mantener segura su clave privada maestra de primer nodo ($V_{1C}$).

Variaciones

A continuación se describirán algunas variaciones con los siguientes ejemplos.

Autenticación de igual a igual

En un escenario de igual a igual, puede ser necesario que el primer nodo 3 y el segundo nodo 7 autentiquen las credenciales del otro. A continuación se describirá un ejemplo de esto con referencia a la Fig. 8. En este ejemplo, las etapas del procedimiento 300, 400 para autenticar el primer nodo 3 en función del primer mensaje firmado validado (SM1) son similares a las descritas anteriormente.

Sin embargo, el procedimiento 400 realizado por el segundo nodo 7 incluye además generar 462 un segundo mensaje firmado (SM2) en función del mensaje (M) y la clave privada de segundo nodo ($V_{2S}$). En algunas alternativas, el segundo mensaje firmado (SM2) puede estar basado en un segundo mensaje (M2) y en la clave privada de segundo nodo ($V_{2S}$), donde el segundo mensaje (M2) es compartido con el primer nodo 3. El procedimiento 400 incluye además enviar 464 el segundo mensaje firmado (SM2), a través de la red de comunicaciones 5, al primer nodo 3.

En el primer nodo 3, el procedimiento 300 incluye recibir el segundo mensaje firmado (SM2) desde el segundo nodo 7. El procedimiento incluye validar 374 la firma en el segundo mensaje firmado (SM2) con la segunda clave pública de segundo nodo ($P_{2S}$) que se determinó en la etapa 370. El procedimiento 300 puede incluir entonces autenticar 376 el segundo nodo 7 en función del resultado de validar el segundo mensaje firmado (SM2). Esto da como resultado que el primer y el segundo nodo 3, 7 se autentiquen entre sí.

Jerarquía de claves deterministas

En un ejemplo, puede determinarse una serie de claves deterministas sucesivas, donde cada clave sucesiva puede determinarse en función de la clave determinista anterior.

Por ejemplo, en lugar de repetir las etapas 310 a 370 y 410 a 470 para generar claves sucesivas de una sola finalidad, mediante un acuerdo previo entre los nodos, la clave determinista (DK) usada anteriormente puede someterse a algoritmos de hash de manera repetida por ambas partes para establecer una jerarquía de claves deterministas. En efecto, la clave determinista, en función del elemento hash de un mensaje (M), puede ser un mensaje de nueva generación (M') para la nueva generación de la clave determinista (DK'). Esto permite calcular generaciones sucesivas de secretos compartidos sin necesidad de transmisiones adicionales de establecimiento de protocolo, en particular la transmisión de múltiples mensajes para cada generación de secretos comunes. El secreto común de nueva generación (CS') puede calcularse de la siguiente manera.

En primer lugar, tanto el primer nodo 3 como el segundo nodo 7 determinan de manera independiente la nueva generación de la clave determinista (DK'). Esto es similar a las etapas 320 y 420, pero adaptadas a las siguientes fórmulas:

$$M' = \text{SHA-256}(M) \qquad (\text{Ecuación } 18)$$

$$DK' = \text{SHA-256}(M') \qquad (\text{Ecuación } 19.1)$$

$$DK' = \text{SHA-256}(\text{SHA-256}(M)) \qquad (\text{Ecuación } 19.2)$$

El primer nodo 3 puede determinar entonces la nueva generación de la segunda clave pública de segundo nodo ($P_{2S}$') y de la segunda clave privada de primer nodo ($V_{2C}$') de manera similar a las etapas 370 y 330 descritas anteriormente, pero adaptadas con las siguientes fórmulas:

$$P_{2S}' = P_{1S} + DK' \times G \qquad (\text{Ecuación } 20.1)$$

$$V_{2C}' = V_{1C} + DK' \qquad (\text{Ecuación } 20.2)$$

El segundo nodo 7 puede determinar entonces la nueva generación de la segunda clave pública de primer nodo ($P_{2C}$') y de la segunda clave privada de segundo nodo ($V_{2S}$') de manera similar a las etapas 430 y 470 descritas anteriormente, pero adaptadas con las siguientes fórmulas:

$$P_{2C}' = P_{1C} + DK' \times G \qquad (\text{Ecuación } 21.1)$$

$$V_{2S}' = V_{1S} + DK' \quad \text{(Ecuación 21.2)}$$

Después, tanto el primer nodo 3 como el segundo nodo 7 pueden determinar el secreto común de nueva generación (CS').

En particular, el primer nodo 3 determina el secreto común de nueva generación (CS') con la fórmula:

$$CS' = V_{2C}' \times P_{2S}' \quad \text{(Ecuación 22)}$$

El segundo nodo 7 determina el secreto común de nueva generación (CS') con la fórmula:

$$CS' = V_{2S}' \times P_{2C}' \quad \text{(Ecuación 23)}$$

Generaciones adicionales (CS", CS"', etc.) pueden calcularse de la misma manera para crear una jerarquía de cadena. Esta técnica requiere que tanto el primer nodo 3 como el segundo nodo 7 realicen un seguimiento del mensaje original (M) o de la clave determinista (DK) calculada originalmente y a la que hace referencia el nodo. Puesto que esto es información conocida públicamente, no hay problemas de seguridad referentes a la conservación de esta información. Por consiguiente, esta información puede mantenerse en "tablas hash" (correlación entre valores hash y claves públicas) y distribuirse libremente a través de la red 5 (por ejemplo, usando Torrent). Además, si algún secreto común (CS) individual de la jerarquía queda revelado alguna vez, esto no afecta a la seguridad de ningún otro secreto común de la jerarquía siempre que las claves privadas $V_{1C}$, $V_{1S}$ sigan siendo seguras.

Estructura en árbol de claves

Al igual que una jerarquía de cadena (lineal) descrita anteriormente, puede crearse una jerarquía en forma de estructura en árbol.

Con una estructura en árbol pueden determinarse varias claves de diferentes finalidades, tales como claves de autenticación, claves de cifrado, claves de firma, claves de pago, etc., de modo que todas estas claves están vinculadas a una única clave maestra mantenida de manera segura. Esto se ilustra mejor en la Fig. 9, que muestra una estructura en árbol 901 con varias claves diferentes. Cada una de las mismas puede usarse para crear un secreto compartido con otra parte.

La ramificación del árbol puede conseguirse de varias maneras, tres de las cuales se describen a continuación.

*(i) Generación de clave maestra*

En la jerarquía de cadena, cada nuevo "enlace" (par de clave pública/privada) se crea añadiendo a la clave maestra original un mensaje sometido a múltiples algoritmos de hash. Por ejemplo, (solo se muestra por claridad la clave privada del primer nodo 3):

$$V_{2C} = V_{1C} + \text{SHA-256}(M) \quad \text{(Ecuación 24)}$$

$$V_{2C}' = V_{1C} + \text{SHA-256}(\text{SHA-256}(M)) \quad \text{(Ecuación 25)}$$

$$V_{2C}'' = V_{1C} + \text{SHA-256}(\text{SHA-256}(\text{SHA-256}(M))) \quad \text{(Ecuación 26)}$$

... y así sucesivamente.

Para crear una rama puede usarse cualquier clave como una clave submaestra. Por ejemplo, $V_{2C}'$ puede usarse como una clave submaestra ($V_{3C}$) añadiendo el elemento hash a la misma como se realiza para la clave maestra convencional:

$$V_{3C} = V_{2C}' + \text{SHA-256}(M) \quad \text{(Ecuación 27)}$$

La propia clave submaestra ($V_{3C}$) puede tener una clave de nueva generación ($V_{3C}'$), por ejemplo:

$$V_{3C}' = V_{2C}' + \text{SHA-256}(\text{SHA-256}(M)) \quad \text{(Ecuación 28)}$$

Esto proporciona una estructura en árbol 903 usando el procedimiento de generación de clave maestra mostrado en la Fig. 10.

*(ii) Asociación lógica*

En este procedimiento, todos los nodos del árbol (pares de clave pública/privada) se generan como una cadena (o de otra manera) y las relaciones lógicas entre los nodos del árbol se mantienen mediante una tabla en la que cada nodo del árbol está simplemente asociado a su nodo padre del árbol usando un puntero. Por tanto, el puntero puede usarse para determinar los pares de clave pública/privada pertinentes para determinar la clave secreta común (CS) para la sesión.

*(iii) Multiplicidad de mensajes*

Nuevos pares de clave privada/pública pueden generarse introduciendo un nuevo mensaje en cualquier punto de la cadena o árbol. El propio mensaje puede ser arbitrario o puede llevar cierto significado o función (por ejemplo, puede estar relacionado con un número de cuenta bancaria "real", etc.). Puede ser deseable que tales nuevos mensajes que forman los nuevos pares de clave privada/pública se conserven de manera segura.

Dispositivo de procesamiento

Como se ha indicado anteriormente, el primer y el segundo nodo 3, 7 pueden ser un dispositivo electrónico, tal como un ordenador, un ordenador de tipo tableta, un dispositivo de comunicaciones móviles, un servidor informático, etc. El dispositivo electrónico puede incluir un dispositivo de procesamiento 23, 27, una unidad de almacenamiento de datos 13, 17 y una interfaz de usuario 15.

La Fig. 11 ilustra un ejemplo de un dispositivo de procesamiento 23, 27. El dispositivo de procesamiento 23, 27 puede usarse en el primer nodo 3, el segundo nodo 7 u otros nodos 9. El dispositivo de procesamiento 23, 27 incluye un procesador 1510, una memoria 1520 y un dispositivo de interfaz 1540 que se comunican entre sí a través de un bus 1530. La memoria 1520 almacena instrucciones y datos para implementar el procedimiento 100, 200, 300, 400 descrito anteriormente, y el procesador 1510 lleva a cabo las instrucciones de la memoria 1520 para implementar el procedimiento 100, 200, 300, 400. El dispositivo de interfaz 1540 puede incluir un módulo de comunicaciones que facilita la comunicación con la red de comunicaciones 5 y, en algunos ejemplos, con la interfaz de usuario 15 y dispositivos periféricos tales como la unidad de almacenamiento de datos 13, 17, 19. Debe observarse que aunque el dispositivo de procesamiento 1501 puede ser un elemento de red independiente, el dispositivo de procesamiento 501 también puede ser parte de otro elemento de red. Además, algunas funciones llevadas a cabo por el dispositivo de procesamiento 1501 pueden estar distribuidas entre múltiples elementos de red. Por ejemplo, el primer nodo 3 puede tener múltiples dispositivos de procesamiento 23 para llevar a cabo el procedimiento 100, 300 en una red de área local segura asociada al primer nodo 3.

Cuando esta divulgación describe que un usuario, expedidor, mercante, proveedor u otra entidad lleva a cabo una acción particular (incluidos la firma, emisión, determinación, cálculo, envío, recepción, creación, etc.), esto se usa para facilitar la presentación. Debe entenderse que estas acciones se llevan a cabo mediante los dispositivos informáticos controlados por estas entidades.

La firma puede comprender ejecutar una función criptográfica. La función criptográfica tiene una entrada para un texto sin cifrar y una entrada para una clave, tal como una clave privada. Un procesador puede ejecutar la función para calcular un número o cadena que puede usarse como firma. La firma se proporciona posteriormente junto con el texto sin cifrar para proporcionar un texto firmado. La firma cambia completamente si el texto de mensaje o la clave cambia en un único bit. Aunque calcular la firma requiere poca potencia computacional, recrear un mensaje que tiene una firma dada es prácticamente imposible. De esta manera, el texto sin cifrar solo puede cambiarse y estar acompañado de una firma válida si la clave privada está disponible. Además, otras entidades pueden verificar fácilmente la firma usando la clave pública disponible públicamente.

En la mayoría de los casos, el cifrado y el descifrado comprende que un procesador ejecute una función criptográfica para calcular una cadena de salida que representa el mensaje cifrado o un mensaje de texto sin cifrar, respectivamente.

Claves, testigos, metadatos, transacciones, ofertas, contratos, firmas, secuencias de comandos, metadatos, invitaciones y similares hacen referencia a datos representados como números, texto o cadenas almacenadas en una memoria de datos, tales como variables en un código de programa de tipo "cadena" o "entero" u otros tipos o archivos de texto.

Un ejemplo del libro mayor en una comunicación de igual a igual es la cadena de bloques de Bitcoin. La transferencia de fondos o el pago de cuotas en moneda de tipo Bitcoin comprende crear una transacción en la cadena de bloques de Bitcoin, donde los fondos o cuotas se proporcionan a partir de la transacción. Un ejemplo de una transacción con Bitcoin incluye un elemento hash de transacción de entrada, una cantidad de transacción, uno o más destinos, una clave pública de un beneficiario o beneficiarios y una firma creada usando la transacción de entrada como el mensaje de entrada y una clave privada de un pagador para calcular la firma. La transacción puede verificarse comprobando que el elemento hash de transacción de entrada existe en una copia de la cadena de bloques de Bitcoin y que la firma es correcta usando la clave pública. Para garantizar que el mismo elemento hash de transacción de entrada no se ha usado todavía en otro sitio, la transacción se difunde a una red de nodos

informáticos ("mineros"). Un minero acepta y registra la transacción en la cadena de bloques solamente si el elemento hash de transacción de entrada no se ha conectado todavía y las firmas son válidas. Un minero rechaza la transacción si el elemento hash de transacción de entrada ya se ha vinculado a una transacción diferente.

Asignar una criptomoneda a un testigo comprende crear una transacción con la criptomoneda asignada y el testigo representado en un campo de metadatos en la transacción.

Cuando dos elementos están asociados, esto significa que hay una conexión lógica entre estos elementos. En una base de datos, por ejemplo, los identificadores de los dos elementos pueden almacenarse en los mismos registros para hacer que los dos elementos estén asociados entre sí. En una transacción, los identificadores de los dos elementos pueden estar incluidos en la cadena de transacción para hacer que los dos elementos estén asociados entre sí.

Usando el protocolo de Bitcoin, redimir una secuencia de comandos y/o desbloquear un testigo comprende calcular una cadena de firmas de la secuencia de comandos y/o de la transacción usando la clave privada. La secuencia de comandos puede requerir más de una firma obtenida a partir de diferentes claves privadas u otras condiciones. La salida de esta transacción se proporciona después a un minero.

Autorizar otra entidad puede comprender calcular una cadena de firmas de una transacción usando una clave privada y proporcionar la cadena de firmas a la entidad para permitir que la entidad use la firma para verificar la transacción.

Un usuario que tiene una cuenta con otra entidad puede comprender que la entidad almacene información acerca del usuario, tal como una dirección de correo electrónico, el nombre y, posiblemente, claves públicas. Por ejemplo, la entidad puede mantener una base de datos, tal como SQL, OrientDB, MongoDB u otras. En algunos ejemplos, la entidad también puede almacenar una o más de las claves privadas del usuario.

Los expertos en la técnica apreciarán que la presente invención proporciona numerosos beneficios técnicos y ventajas con respecto a la técnica anterior. Por ejemplo, el protocolo BIP32 (por ejemplo, como se describe en la guía para desarrolladores de Bitcoin) usa una semilla aleatoria para generar las subclaves. Esto da lugar a la necesidad de mantener una base de datos de índices. Sin embargo, según la presente invención, un mensaje M provechoso se usa para generar las subclaves (y, por lo tanto, también los secretos subcompartidos). De manera ventajosa, esto elimina la necesidad de una base de datos de índices y, por tanto, proporciona una técnica de seguridad más sencilla que es más eficaz en lo que respecta a los recursos informáticos necesarios para su ejecución. Además, permite la asociación de información provechosa con las subclaves. Por ejemplo, las subclaves reutilizables pueden usarse para representar cuentas bancarias específicas o códigos de cliente, etc. Como alternativa, pueden generarse subclaves de un solo uso basadas en la aplicación de un algoritmo de hash en un archivo específico de factura o de vídeo (u otros datos), etc.

Los expertos en la técnica apreciarán que pueden realizarse numerosas variaciones y/o modificaciones en las formas de realización antes descritas sin apartarse del alcance general de la presente divulgación definido por las reivindicaciones adjuntas. Por lo tanto, se considera que las presentes formas de realización, en todos los aspectos, son ilustrativas y no restrictivas.

**REIVINDICACIONES**

1. Un procedimiento implementado por ordenador que determina, en un primer nodo (C), un secreto común (CS) que es común con el primer nodo (C) y un segundo nodo (S), donde el primer nodo (C) está asociado a un primer par de criptografía asimétrica que presenta una clave privada maestra de primer nodo ($V_{1C}$) y una clave pública maestra de primer nodo ($P_{1C}$), y el segundo nodo (S) está asociado a un segundo par de criptografía asimétrica que presenta una clave privada maestra de segundo nodo ($V_{1S}$) y una clave pública maestra de segundo nodo ($P_{1S}$), donde la clave pública maestra de primer nodo ($P_{1C}$) y la clave pública maestra de segundo nodo ($P_{1S}$) están basadas en una multiplicación de puntos de curva elíptica de la clave privada maestra de primer nodo ($V_{1C}$) y de la clave privada maestra de segundo nodo ($V_{1S}$) y un generador (G) común, donde el primer y el segundo nodo usan un sistema de criptografía de curva elíptica común con el primer y el segundo nodo, y donde el procedimiento comprende:

- determinar (330) una segunda clave privada de primer nodo ($V_{2C}$);

- determinar (370, 370') una segunda clave pública de segundo nodo ($P_{2S}$); y

- determinar (380) el secreto común (CS) en función de la multiplicación de puntos de curva elíptica de la segunda clave privada de primer nodo ($V_{2C}$) y de la segunda clave pública de segundo nodo ($P_{2S}$) usando el sistema de criptografía de curva elíptica común,

donde el segundo nodo (S) tiene el mismo secreto común (CS) basado en la multiplicación de puntos de curva elíptica de una segunda clave pública de primer nodo ($P_{2C}$) y de una segunda clave privada de segundo nodo ($V_{2S}$) usando el sistema de criptografía de curva elíptica común,
caracterizado por que la segunda clave privada de primer nodo ($V_{2C}$) se determina en función de al menos una suma escalar de la clave privada maestra de primer nodo ($V_{1C}$) y una clave determinista (DK) común con el primer y el segundo nodo;

- la segunda clave pública de segundo nodo ($P_{2S}$) se determina en función de al menos la clave pública maestra de segundo nodo ($P_{1S}$) con la suma de puntos de curva elíptica a la multiplicación de puntos de curva elíptica del generador (G) común y la clave determinista (DK) usando el sistema de criptografía de curva elíptica común;

- la segunda clave pública de primer nodo ($P_{2C}$) está basada en al menos la clave pública maestra de primer nodo ($P_{1C}$) con la suma de puntos de curva elíptica a la multiplicación de puntos de curva elíptica del generador (G) común y la clave determinista (DK) usando el sistema de criptografía de curva elíptica común; y

- la segunda clave privada de segundo nodo ($V_{2S}$) está basada en al menos una suma escalar de la clave privada maestra de segundo nodo ($V_{1S}$) y la clave determinista (DK).

2. Un procedimiento según la reivindicación 1, que incluye una o más de las siguientes características:

(i) en el que la clave determinista (DK) está basada en un mensaje (M);

(ii) que comprende además las etapas de:

- recibir (130), a través de la red de comunicaciones, la clave pública maestra de segundo nodo ($P_{1S}$); y
- almacenar, en una unidad de almacenamiento de datos asociada al primer nodo (C), la clave pública maestra de segundo nodo ($P_{1S}$); o

(iii) que comprende además las etapas de:

- generar (120), en un primer nodo (C), la clave privada maestra de primer nodo ($V_{1C}$) y la clave pública maestra de primer nodo ($P_{1C}$);

- enviar (130), a través de la red de comunicaciones, la clave pública maestra de primer nodo ($P_{1C}$) al segundo nodo (S) y/u otro nodo; y

- almacenar, en una primera unidad de almacenamiento de datos asociada al primer nodo (C), la clave privada maestra de primer nodo ($V_{1C}$).

3. Un procedimiento según la reivindicación 2, que incluye una o más de las siguientes características:

(i) que comprende además:

- generar (350) un primer mensaje firmado (SM1) en función del mensaje (M) y la segunda clave privada de primer nodo ($V_{2C}$); y

- enviar (360), a través de la red de comunicaciones, el primer mensaje firmado (SM1) al segundo nodo (S), donde el primer mensaje firmado (SM1) puede validarse con una segunda clave pública de primer nodo ($P_{2C}$) para autenticar el primer nodo (C);

(ii) que comprende además:
- recibir, a través de la red de comunicaciones, un segundo mensaje firmado (SM2) desde el segundo nodo (S);

- validar el segundo mensaje firmado (SM2) con la segunda clave pública de segundo nodo (P2S); y

- autenticar el segundo nodo (S) en función del resultado de validar el segundo mensaje firmado (SM2), donde el segundo mensaje firmado (SM2) se ha generado en función del mensaje (M), o un segundo mensaje (M2), y la segunda clave privada de segundo nodo ($V_{2S}$);

(iii) que comprende además:

- generar (310) un mensaje (M); y

- enviar (315), a través de una red de comunicaciones, el mensaje (M) al segundo nodo (S);

(iv) que comprende además:

- recibir el mensaje (M), a través de la red de comunicaciones, desde el segundo nodo (S);

(v) que comprende además:

- recibir el mensaje (M), a través de la red de comunicaciones, desde otro nodo; o

(vi) que comprende además:

- recibir el mensaje (M) desde una unidad de almacenamiento de datos y/o una interfaz de entrada asociada al primer nodo (C).

4. Un procedimiento según la reivindicación 2 o 3, que comprende además:

- enviar (110), a través de la red de comunicaciones, al segundo nodo, un aviso que indica el uso de un sistema de criptografía de curva elíptica común con un generador (G) común para el procedimiento de determinar un secreto común (CS), y

en el que la etapa de generar la clave privada maestra de primer nodo ($V_{1C}$) y la clave pública maestra de primer nodo ($P_{1C}$) comprende:

- generar la clave privada maestra de primer nodo ($V_{1C}$) en función de un entero aleatorio en un intervalo permitido especificado en el sistema de criptografía de curva elíptica común; y

- determinar la clave pública maestra de primer nodo ($P_{1C}$) en función de la multiplicación de puntos de curva elíptica de la clave privada maestra de primer nodo ($V_{1C}$) y el generador (G) común según la siguiente fórmula:

$$P_{1C} = V_{1C} \times G.$$

5. Un procedimiento según la reivindicación 4, que comprende además:

- determinar la clave determinista (DK) en función de determinar un elemento hash del mensaje (M), y
en el que la etapa de determinar una segunda clave privada de primer nodo (V2C) está basada en una suma escalar de la clave privada maestra de primer nodo ($V_{1C}$) y la clave determinista (DK) según la siguiente fórmula:

$$V_{2C} = V_{1C} + DK \text{ ,y}$$

en el que la etapa de determinar una segunda clave pública de segundo nodo ($P_{2S}$) está basada en la clave pública maestra de segundo nodo ($P_{1S}$) con la suma de puntos de curva elíptica a la multiplicación de puntos de curva elíptica de la clave determinista (DK) y el generador (G) común según la siguiente fórmula:

$$P_{2S} = P_{1S} + DK \times G.$$

6. Un procedimiento según una cualquiera de las reivindicaciones anteriores, que incluye una o más de las siguientes características:

(i) en el que la clave determinista (DK) está basada en determinar un elemento hash de una clave determinista anterior; o

(ii) en el que el primer par de criptografía asimétrica y el segundo par de criptografía asimétrica están basados en una función de un primer par de criptografía asimétrica anterior y un segundo par de criptografía asimétrica anterior respectivos.

7. Un procedimiento de comunicación segura entre un primer nodo y un segundo nodo con un algoritmo de clave simétrica, donde el procedimiento comprende:

- determinar un secreto común mediante un procedimiento según una cualquiera de las reivindicaciones anteriores;

- determinar (510) una clave simétrica en función del secreto común;

- cifrar (520) un primer mensaje de comunicación, con la clave simétrica, para obtener un primer mensaje de comunicación cifrado; y

- enviar (530), a través de una red de comunicaciones, el primer mensaje de comunicación cifrado desde el primer nodo (C) al segundo nodo (S).

8. Un procedimiento según la reivindicación 7, en el que el procedimiento comprende además:

- recibir (540), a través de una red de comunicaciones, un segundo mensaje de comunicación cifrado desde el segundo nodo (S); y

- descifrar (550) el segundo mensaje de comunicación cifrado, con la clave simétrica, para obtener un segundo mensaje de comunicación.

9. Un procedimiento para llevar a cabo una transacción en línea entre un primer nodo y un segundo nodo, donde el procedimiento comprende:

- determinar un secreto común mediante un procedimiento según una cualquiera de las reivindicaciones 1 a 6;

- determinar una clave simétrica en función del secreto común;

- cifrar un primer mensaje de transacción, con la clave simétrica, para obtener un primer mensaje de transacción cifrado;

- enviar, a través de una red de comunicaciones, el primer mensaje de transacción cifrado desde el primer nodo (C) al segundo nodo (S);

- recibir, a través de una red de comunicaciones, un segundo mensaje de transacción cifrado desde el segundo nodo (S); y

- descifrar el segundo mensaje de transacción cifrado, con la clave simétrica, para obtener un segundo mensaje de transacción.

10. Un dispositivo para determinar, en un primer nodo (C), un secreto común (CS) que es común con un segundo nodo (S), donde el primer nodo (C) está asociado a un primer par de criptografía asimétrica que presenta una clave privada maestra de primer nodo ($V_{1C}$) y una clave pública maestra de primer nodo ($P_{1C}$), y el segundo nodo (S) está asociado a un segundo par de criptografía asimétrica que presenta una clave privada maestra de segundo nodo ($V_{1S}$) y una clave pública maestra de segundo nodo ($P_{1S}$), donde el dispositivo comprende un primer dispositivo de procesamiento para llevar a cabo el procedimiento según una cualquiera de las reivindicaciones 1 a 6 para determinar el secreto común.

11. Un dispositivo de comunicación segura o para llevar a cabo una transacción en línea segura entre un primer nodo y un segundo nodo, donde el dispositivo incluye un primer dispositivo de procesamiento para:

- llevar a cabo el procedimiento según una cualquiera de las reivindicaciones 7 a 9.

12. Un dispositivo según la reivindicación 10 u 11, que incluye una o más de las siguientes características:

(i) que comprende además una primera unidad de almacenamiento de datos para almacenar una o más de la clave privada maestra de primer nodo ($V_{1C}$); o

(ii) que comprende además un módulo de comunicaciones para enviar y/o recibir, a través de una red de comunicaciones, uno o más del mensaje (M), la clave pública maestra de primer nodo ($P_{1C}$), la clave pública maestra de segundo nodo ($P_{1S}$), el primer mensaje firmado (SM1), el segundo mensaje firmado (SM2), el aviso que indica el uso de un sistema de criptografía de curva elíptica común con un generador (G) común.

13. Un dispositivo según la reivindicación 12, en el que la primera unidad de almacenamiento de datos almacena además uno o más de la clave pública maestra de primer nodo ($P_{1C}$), la clave pública maestra de segundo nodo ($P_{1S}$) y el mensaje (M).

14. Un sistema para determinar un secreto común entre un primer nodo (C) y un segundo nodo (S), en el que:

- el primer nodo (C) está asociado a un primer par de criptografía asimétrica que presenta una clave privada maestra de primer nodo ($V_{1C}$) y una clave pública maestra de primer nodo ($P_{1C}$); y
- el segundo nodo (S) está asociado a un segundo par de criptografía asimétrica que presenta una clave privada maestra de segundo nodo ($V_{1S}$) y una clave pública maestra de segundo nodo ($P_{1S}$), donde la clave pública maestra de primer nodo ($P_{1C}$) y la clave pública maestra de segundo nodo ($P_{1S}$) están basadas en una multiplicación de puntos de curva elíptica de clave privada maestra de primer nodo ($V_{1C}$) y de clave privada maestra de segundo nodo ($V_{1S}$) y un generador (G) común con el primer y el segundo nodo usando un sistema de criptografía de curva elíptica común con el primer y el segundo nodo, y en el que el sistema comprende:

  - un primer dispositivo de procesamiento, asociado al primer nodo (C), configurado para:

    - determinar una segunda clave privada de primer nodo ($V_{2C}$);

    - determinar una segunda clave pública de segundo nodo ($P_{2S}$); y

    - determinar el secreto común (CS) en función de la multiplicación de puntos de curva elíptica de la segunda clave privada de primer nodo ($V_{2C}$) y de la segunda clave pública de segundo nodo ($P_{2S}$) usando el sistema de criptografía de curva elíptica común; y

  - un segundo dispositivo de procesamiento, asociado al segundo nodo (S), configurado para:

    - determinar una segunda clave pública de primer nodo ($P_{2C}$); y

    - determinar una segunda clave privada de segundo nodo ($V_{2S}$); y

    - determinar el secreto común en función de la multiplicación de puntos de curva elíptica de la segunda clave pública de primer nodo ($P_{2C}$) y de la segunda clave privada de segundo nodo ($V_{2S}$) usando el sistema de criptografía de curva elíptica común;

en el que el primer dispositivo de procesamiento y el segundo dispositivo de procesamiento determinan el mismo secreto común;
caracterizado por que el primer dispositivo de procesamiento está configurado para:

- determinar la segunda clave privada de primer nodo ($V_{2C}$) en función de al menos una suma escalar de la clave privada maestra de primer nodo ($V_{1C}$) y una clave determinista (DK) común con el primer y el segundo nodo; y

- determinar la segunda clave pública de segundo nodo ($P_{2S}$) en función de al menos la clave pública maestra de segundo nodo ($P_{1S}$) con la suma de puntos de curva elíptica a la multiplicación de puntos de curva elíptica del generador (G) común y la clave determinista (DK) usando el sistema de criptografía de curva elíptica común;

y el segundo dispositivo de procesamiento está configurado para:

- determinar la segunda clave pública de primer nodo ($P_{2C}$) en función de al menos la clave pública maestra de primer nodo ($P_{1C}$) con la suma de puntos de curva elíptica a la multiplicación de puntos de

curva elíptica del generador (G) común y la clave determinista (DK) usando el sistema de criptografía de curva elíptica común; y

- determinar la segunda clave privada de segundo nodo ($V_{2S}$) en función de al menos una suma escalar de la clave privada maestra de segundo nodo ($V_{1S}$) y la clave determinista (DK).

15. Un sistema según la reivindicación 14, que incluye una o más de las siguientes características:

(i) en el que la clave determinista (DK) está basada en un mensaje (M), y el primer dispositivo de procesamiento está configurado además para:

- generar un primer mensaje firmado (SM1) en función del mensaje (M) y la segunda clave privada de primer nodo ($V_{2C}$); y

- enviar, a través de la red de comunicaciones, el primer mensaje firmado (SM1) al segundo nodo (S),

en el que el segundo dispositivo de procesamiento está configurado además para:

- recibir el primer mensaje firmado (SM1);

- validar el primer mensaje firmado (SM1) con la segunda clave pública de primer nodo ($P_{2C}$); y

- autenticar el primer nodo (C) en función de un resultado del primer mensaje firmado validado (SM1);

(ii) en el que el segundo dispositivo de procesamiento está configurado además para:

- generar un segundo mensaje firmado (SM2) en función del mensaje (M), o un segundo mensaje (M2), y la segunda clave privada de segundo nodo ($V_{2S}$); y

- enviar el segundo mensaje firmado (SM2) al primer nodo (C),

en el que el primer dispositivo de procesamiento está configurado además para:

- recibir el segundo mensaje firmado (SM2);

- validar el segundo mensaje firmado (SM2) con la segunda clave pública de segundo nodo ($P_{2S}$); y

- autenticar el segundo nodo (S) en función de un resultado del segundo mensaje firmado validado (SM2);

(iii) en el que el primer dispositivo de procesamiento está configurado para:

- generar el mensaje (M); y

- enviar el mensaje (M),

en el que el segundo dispositivo de procesamiento está configurado para:

- recibir el mensaje (M);

(iv) en el que el mensaje se genera mediante otro nodo, donde el primer dispositivo de procesamiento está configurado para:

- recibir el mensaje (M),

en el que el segundo dispositivo de procesamiento está configurado para:

- recibir el mensaje (M);

(v) que comprende además una unidad de almacenamiento de datos de sistema y/o una interfaz de entrada, donde el primer dispositivo de procesamiento y el segundo dispositivo de procesamiento reciben el mensaje (M) o el segundo mensaje (M2) desde la unidad de almacenamiento de datos de sistema y/o la interfaz de entrada;

(vi) que comprende además:

- una primera unidad de almacenamiento de datos asociada al primer nodo (C) para almacenar la clave privada maestra de primer nodo ($V_{1C}$); y

- una segunda unidad de almacenamiento de datos asociada al segundo nodo (S) para almacenar la clave privada maestra de segundo nodo ($V_{1S}$);

(vii) en el que el primer dispositivo de procesamiento está configurado además para:

- generar la clave privada maestra de primer nodo ($V_{1C}$) en función de un entero aleatorio en un intervalo permitido especificado en un sistema de criptografía de curva elíptica común; y

- determinar la clave pública maestra de primer nodo ($P_{1C}$) en función de la multiplicación de puntos de curva elíptica de la clave privada maestra de primer nodo ($V_{1C}$) y un generador (G) común según la fórmula:

$$P_{1C} = V_{1C} \times G$$

y en el que el segundo dispositivo de procesamiento está configurado además para:

- generar la clave privada maestra de segundo nodo ($V_{1S}$) en función de un entero aleatorio en el intervalo permitido especificado en el sistema de criptografía de curva elíptica común; y

- determinar la clave pública maestra de segundo nodo ($P_{1S}$) en función de la multiplicación de puntos de curva elíptica de la clave privada maestra de segundo nodo ($V_{1S}$) y el generador (G) común según la fórmula:

$$P_{1S} = V_{1S} \times G;$$

(viii) en el que el primer dispositivo de procesamiento está configurado para:

- determinar la clave determinista (DK) en función de un elemento hash del mensaje (M), y en el que:

  - la segunda clave privada de primer nodo ($V_{2C}$) está basada en una suma escalar de la clave privada maestra de primer nodo ($V_{1C}$) y de la clave determinista (DK) según la fórmula:

$$V_{2C} = V_{1C} + DK \text{ ; y}$$

  - la segunda clave pública de segundo nodo ($P_{2S}$) está basada en la clave pública maestra de segundo nodo ($P_{1S}$) con la suma de puntos de curva elíptica a la multiplicación de puntos de curva elíptica de la clave determinista (DK) y el generador (G) común según la siguiente fórmula:

$$P_{2S} = P_{1S} + DK \times G$$

y en el que el segundo dispositivo de procesamiento está configurado para:

- determinar la clave determinista (DK) en función de un elemento hash del mensaje (M), y en el que:

  - la segunda clave privada de segundo nodo ($V_{2S}$) está basada en una suma escalar de la clave privada maestra de segundo nodo ($V_{1S}$) y de la clave determinista (DK) según la fórmula:

$$V_{2S} = V_{1C} + DK \text{ ; y}$$

  - la clave pública de primer nodo ($P_{2C}$) está basada en la clave pública maestra de primer nodo ($P_{1C}$) con la suma de puntos de curva elíptica a la multiplicación de puntos de curva elíptica de la clave determinista (DK) y el generador (G) común según la siguiente fórmula:

$$P_{2C} = P_{1C} + DK \times G;$$

(ix) que comprende además:

- un primer módulo de comunicaciones asociado al primer dispositivo de procesamiento para enviar y/o recibir, a través de una red de comunicaciones, uno o más del mensaje (M), la clave pública maestra de primer nodo ($P_{1C}$), la clave pública maestra de segundo nodo ($P_{1S}$), el primer mensaje

firmado (SM1), el segundo mensaje firmado (SM2) y un aviso que indica el uso de un sistema de criptografía de curva elíptica común con un generador (G) común; y

- un segundo módulo de comunicaciones asociado al segundo dispositivo de procesamiento para enviar y/o recibir, a través de una red de comunicaciones, uno o más del mensaje (M), la clave pública maestra de primer nodo ($P_{1C}$), la clave pública maestra de segundo nodo ($P_{1S}$), el primer mensaje firmado (SM1), el segundo mensaje firmado (SM2) y el aviso que indica el uso de un sistema de criptografía de curva elíptica común con un generador (G) común;

(x) en el que la clave determinista (DK) está basada en determinar un elemento hash de una clave determinista anterior; o

(xi) en el que el primer par de criptografía asimétrica y el segundo par de criptografía asimétrica están basados en una función de un primer par de criptografía asimétrica anterior y un segundo par de criptografía asimétrica anterior respectivos.

16. Un sistema según la reivindicación 15, que incluye una o más de las siguientes características:

(i) en el que el primer dispositivo de procesamiento recibe la clave pública maestra de segundo nodo ($P_{1S}$) desde la unidad de almacenamiento de datos de sistema y/o un dispositivo de entrada, y el segundo dispositivo de procesamiento recibe la clave pública maestra de primer nodo ($P_{1C}$) desde la unidad de almacenamiento de datos de sistema y/o el dispositivo de entrada;

(ii) en el que el primer dispositivo de procesamiento está configurado para:

- generar la clave privada maestra de primer nodo ($V_{1C}$) y la clave pública maestra de primer nodo ($P_{1C}$);

- enviar la clave pública maestra de primer nodo ($P_{1C}$); y

- almacenar la clave privada maestra de primer nodo ($V_{1C}$) en la primera unidad de almacenamiento de datos,

en el que el segundo dispositivo de procesamiento está configurado para:

- generar la clave privada maestra de segundo nodo ($V_{1S}$) y la clave pública maestra de segundo nodo ($P_{1S}$);

- enviar la clave pública maestra de segundo nodo ($P_{1S}$); y

- almacenar la clave privada maestra de segundo nodo ($V_{1S}$) en la segunda unidad de almacenamiento de datos; o

(iii) en el que:

- la primera unidad de almacenamiento de datos recibe y almacena la clave pública maestra de segundo nodo ($P_{1S}$); y

- la segunda unidad de almacenamiento de datos recibe y almacena la clave pública maestra de primer nodo ($P_{1C}$).

17. Un sistema de comunicación segura entre un primer nodo y un segundo nodo con un algoritmo de clave simétrica, donde el sistema comprende:

- un sistema según una cualquiera de las reivindicaciones 14 a 16 para determinar un secreto común con el primer dispositivo de procesamiento y el segundo dispositivo de procesamiento, donde el primer dispositivo de procesamiento está configurado además para:

- determinar una clave simétrica en función del secreto común;
- cifrar un primer mensaje de comunicación, con la clave simétrica, para obtener un primer mensaje de comunicación cifrado; y
- enviar el primer mensaje de comunicación cifrado;

en el que el segundo dispositivo de procesamiento está configurado además para:

- determinar la misma clave simétrica en función del secreto común;

- recibir el primer mensaje de comunicación cifrado; y
- descifrar el primer mensaje de comunicación cifrado, con la clave simétrica, para obtener el primer mensaje de comunicación.

18. Un programa informático que comprende instrucciones legibles por máquina para hacer que un dispositivo de procesamiento implemente el procedimiento según una cualquiera de las reivindicaciones 1 a 9.

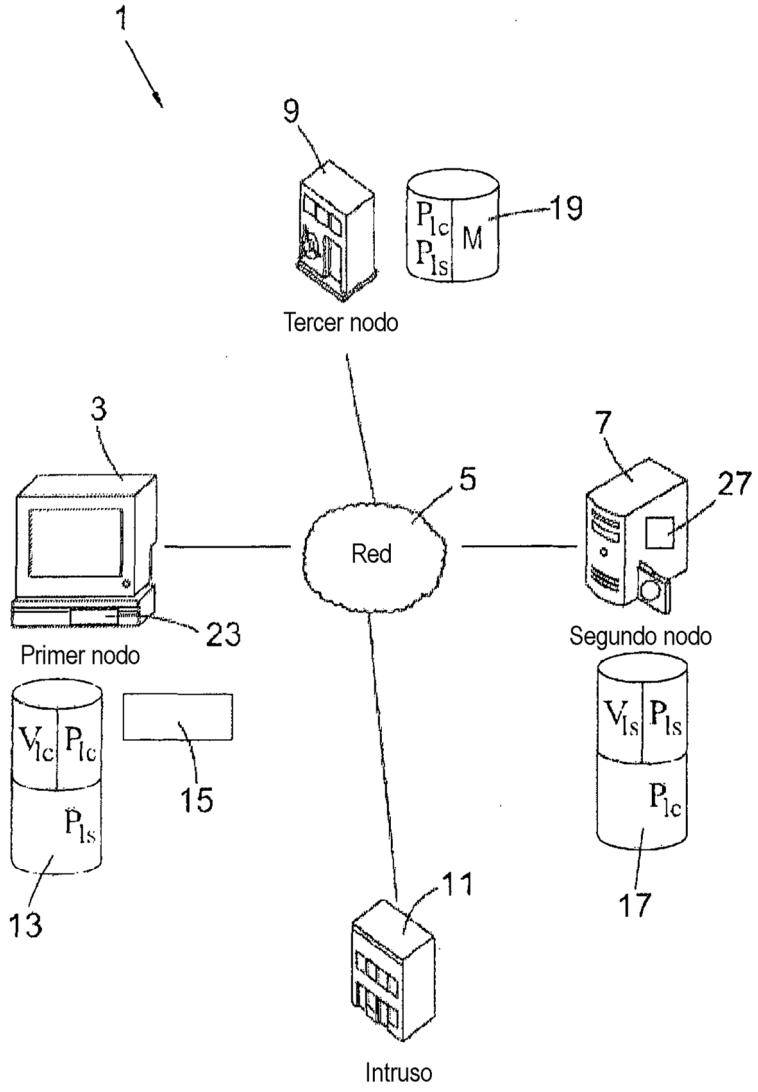
1
9
19
Tercer nodo
3
7
5
27
Red
Primer nodo
23
Segundo nodo
15
13
17
11
Intruso

Fig. 1

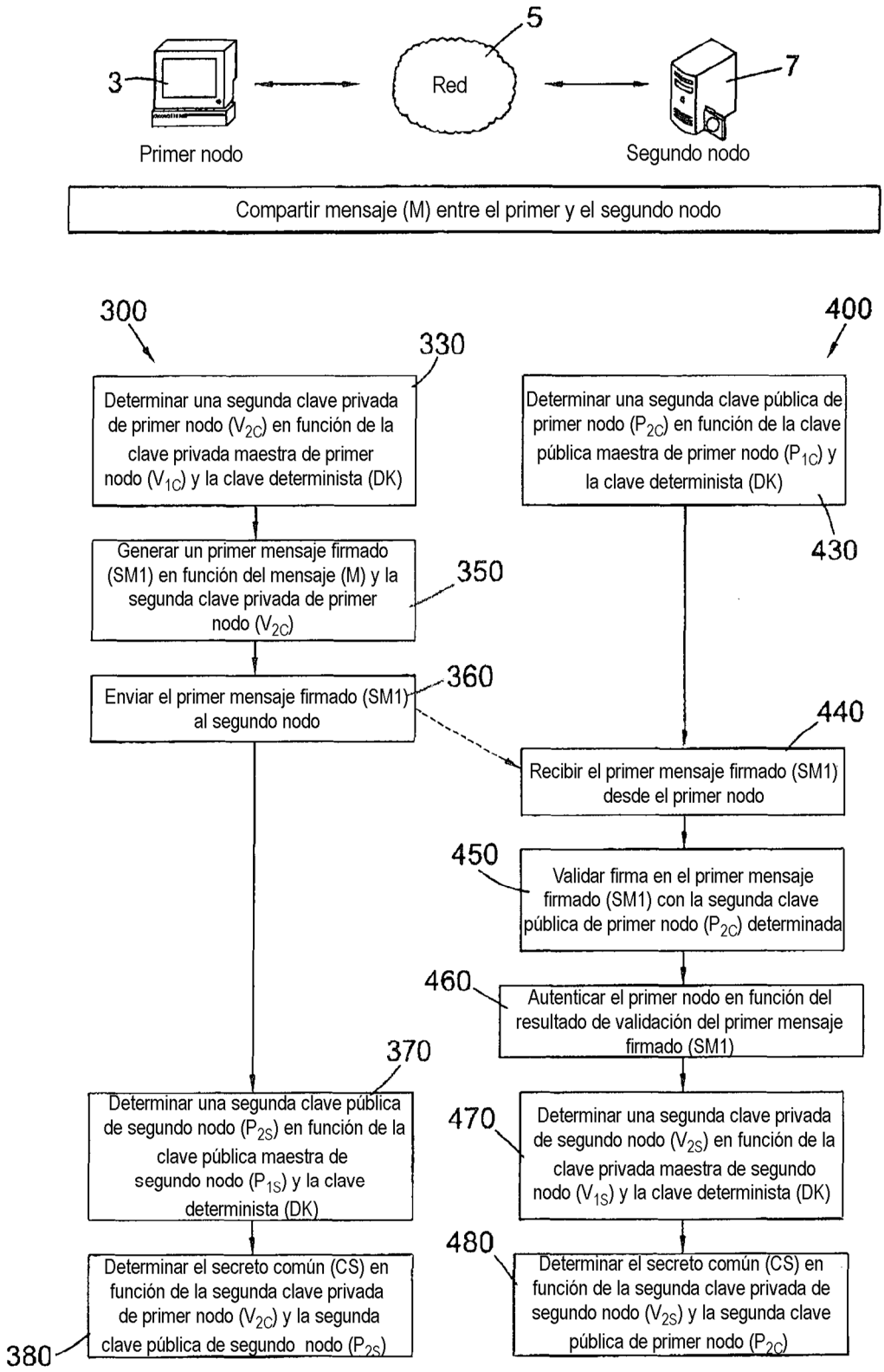
5
3
Red
7
Primer nodo
Segundo nodo
Compartir mensaje (M) entre el primer y el segundo nodo
300
330
Determinar una segunda clave privada de primer nodo ($V_{2C}$) en función de la clave privada maestra de primer nodo ($V_{1C}$) y la clave determinista (DK)
Generar un primer mensaje firmado (SM1) en función del mensaje (M) y la segunda clave privada de primer nodo ($V_{2C}$)
350
Enviar el primer mensaje firmado (SM1) al segundo nodo
360
Determinar una segunda clave pública de segundo nodo ($P_{2S}$) en función de la clave pública maestra de segundo nodo ($P_{1S}$) y la clave determinista (DK)
370
Determinar el secreto común (CS) en función de la segunda clave privada de primer nodo ($V_{2C}$) y la segunda clave pública de segundo nodo ($P_{2S}$)
380
400
Determinar una segunda clave pública de primer nodo ($P_{2C}$) en función de la clave pública maestra de primer nodo ($P_{1C}$) y la clave determinista (DK)
430
440
Recibir el primer mensaje firmado (SM1) desde el primer nodo
450
Validar firma en el primer mensaje firmado (SM1) con la segunda clave pública de primer nodo ($P_{2C}$) determinada
460
Autenticar el primer nodo en función del resultado de validación del primer mensaje firmado (SM1)
470
Determinar una segunda clave privada de segundo nodo ($V_{2S}$) en función de la clave privada maestra de segundo nodo ($V_{1S}$) y la clave determinista (DK)
480
Determinar el secreto común (CS) en función de la segunda clave privada de segundo nodo ($V_{2S}$) y la segunda clave pública de primer nodo ($P_{2C}$)

Fig. 2

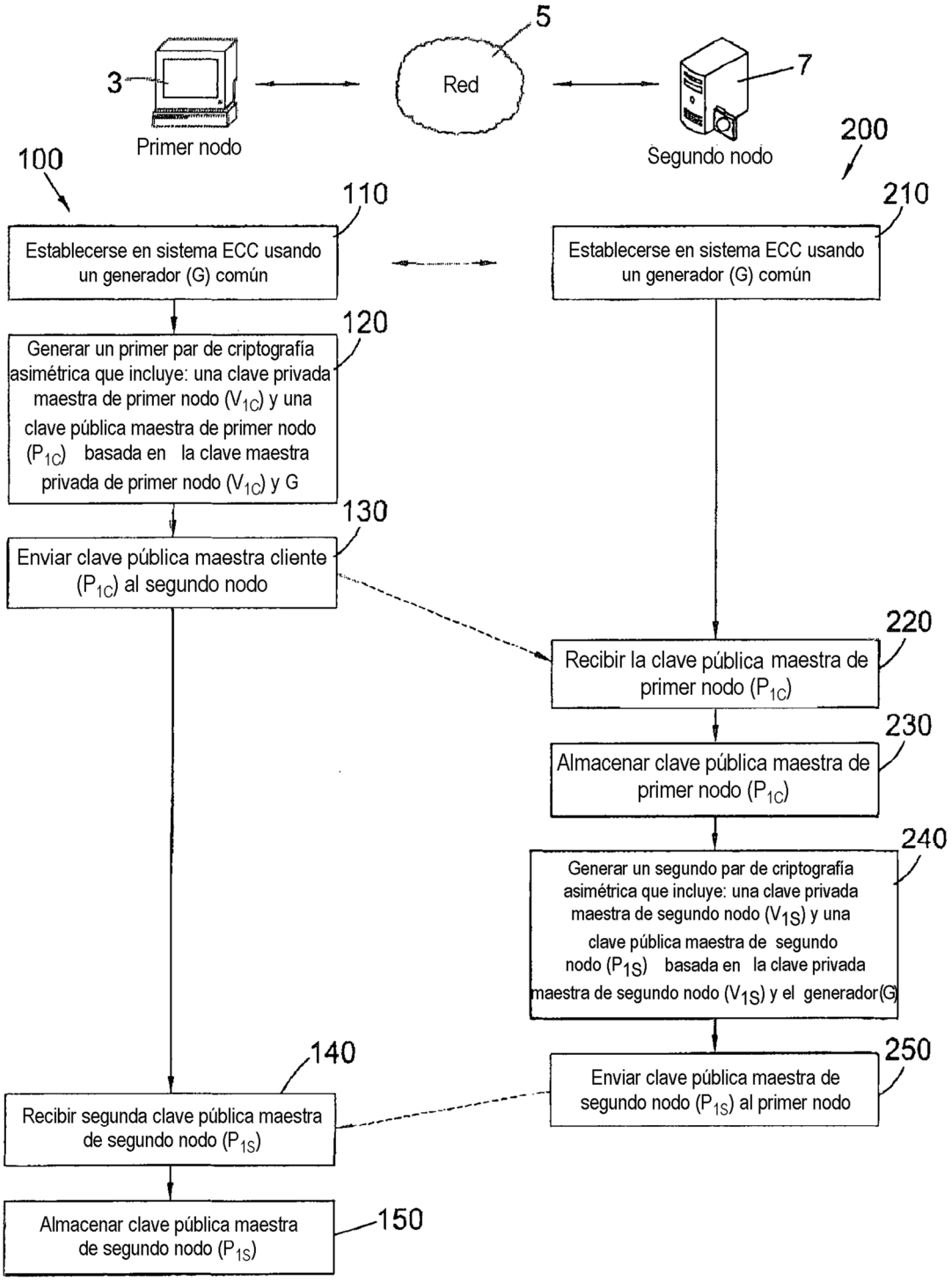
3
Primer nodo
5
Red
7
Segundo nodo
100
200
110
Establecerse en sistema ECC usando un generador (G) común
210
Establecerse en sistema ECC usando un generador (G) común
120
Generar un primer par de criptografía asimétrica que incluye: una clave privada maestra de primer nodo ($V_{1C}$) y una clave pública maestra de primer nodo ($P_{1C}$) basada en la clave maestra privada de primer nodo ($V_{1C}$) y G
130
Enviar clave pública maestra cliente ($P_{1C}$) al segundo nodo
220
Recibir la clave pública maestra de primer nodo ($P_{1C}$)
230
Almacenar clave pública maestra de primer nodo ($P_{1C}$)
240
Generar un segundo par de criptografía asimétrica que incluye: una clave privada maestra de segundo nodo ($V_{1S}$) y una clave pública maestra de segundo nodo ($P_{1S}$) basada en la clave privada maestra de segundo nodo ($V_{1S}$) y el generador(G)
250
Enviar clave pública maestra de segundo nodo ($P_{1S}$) al primer nodo
140
Recibir segunda clave pública maestra de segundo nodo ($P_{1S}$)
150
Almacenar clave pública maestra de segundo nodo ($P_{1S}$)

Fig. 3

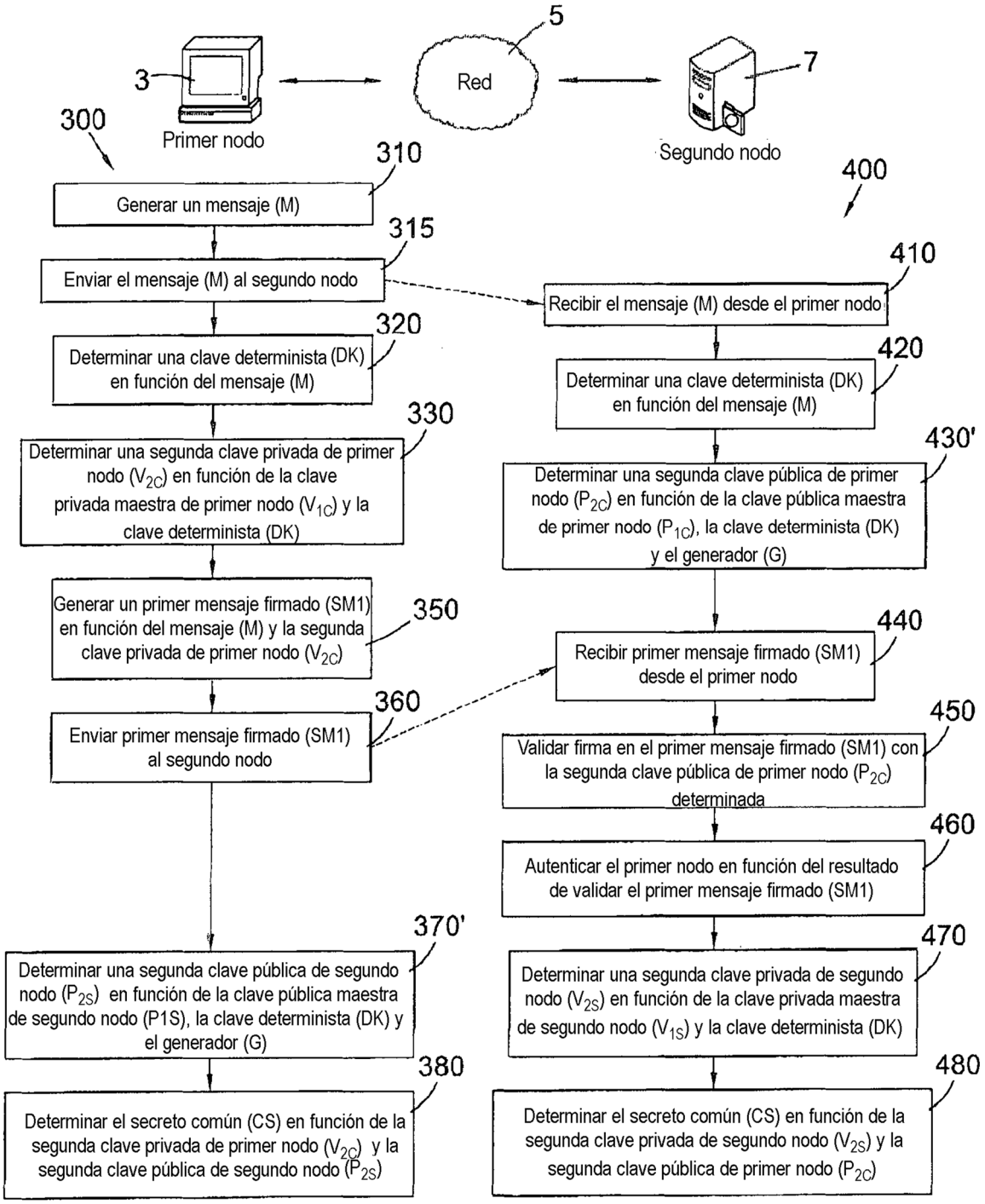
5
Red
3
7
300
Primer nodo
Segundo nodo
400
310
Generar un mensaje (M)
315
Enviar el mensaje (M) al segundo nodo
410
Recibir el mensaje (M) desde el primer nodo
320
Determinar una clave determinista (DK) en función del mensaje (M)
420
Determinar una clave determinista (DK) en función del mensaje (M)
330
Determinar una segunda clave privada de primer nodo ($V_{2C}$) en función de la clave privada maestra de primer nodo ($V_{1C}$) y la clave determinista (DK)
430'
Determinar una segunda clave pública de primer nodo ($P_{2C}$) en función de la clave pública maestra de primer nodo ($P_{1C}$), la clave determinista (DK) y el generador (G)
Generar un primer mensaje firmado (SM1) en función del mensaje (M) y la segunda clave privada de primer nodo ($V_{2C}$)
350
440
Recibir primer mensaje firmado (SM1) desde el primer nodo
360
Enviar primer mensaje firmado (SM1) al segundo nodo
450
Validar firma en el primer mensaje firmado (SM1) con la segunda clave pública de primer nodo ($P_{2C}$) determinada
460
Autenticar el primer nodo en función del resultado de validar el primer mensaje firmado (SM1)
370'
Determinar una segunda clave pública de segundo nodo ($P_{2S}$) en función de la clave pública maestra de segundo nodo (P1S), la clave determinista (DK) y el generador (G)
470
Determinar una segunda clave privada de segundo nodo ($V_{2S}$) en función de la clave privada maestra de segundo nodo ($V_{1S}$) y la clave determinista (DK)
380
Determinar el secreto común (CS) en función de la segunda clave privada de primer nodo ($V_{2C}$) y la segunda clave pública de segundo nodo ($P_{2S}$)
480
Determinar el secreto común (CS) en función de la segunda clave privada de segundo nodo ($V_{2S}$) y la segunda clave pública de primer nodo ($P_{2C}$)

Fig. 4

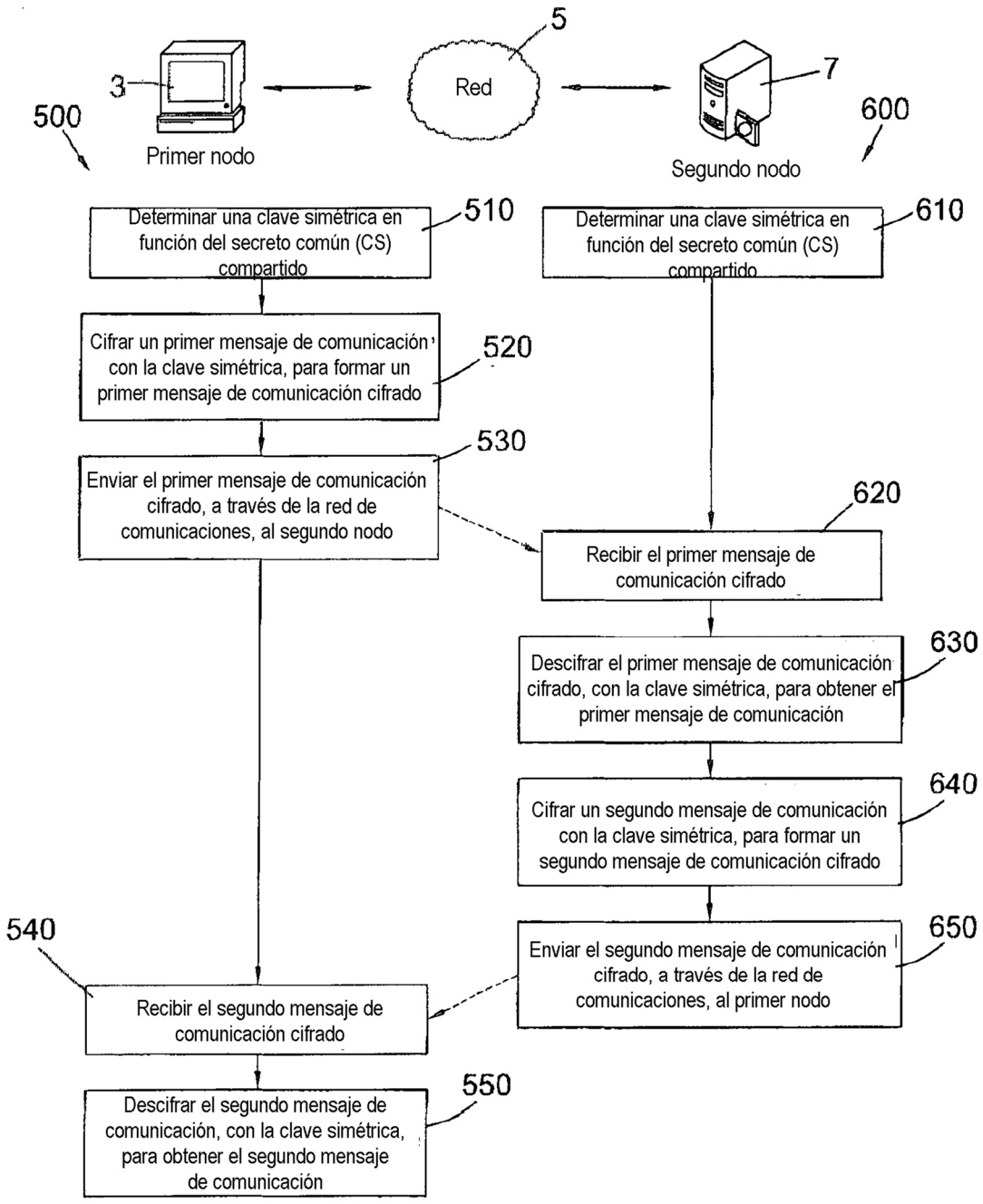
5
3
Red
7
500
600
Primer nodo
Segundo nodo
Determinar una clave simétrica en función del secreto común (CS) compartido
510
Determinar una clave simétrica en función del secreto común (CS) compartido
610
Cifrar un primer mensaje de comunicación con la clave simétrica, para formar un primer mensaje de comunicación cifrado
520
Enviar el primer mensaje de comunicación cifrado, a través de la red de comunicaciones, al segundo nodo
530
620
Recibir el primer mensaje de comunicación cifrado
Descifrar el primer mensaje de comunicación cifrado, con la clave simétrica, para obtener el primer mensaje de comunicación
630
Cifrar un segundo mensaje de comunicación con la clave simétrica, para formar un segundo mensaje de comunicación cifrado
640
540
Enviar el segundo mensaje de comunicación cifrado, a través de la red de comunicaciones, al primer nodo
650
Recibir el segundo mensaje de comunicación cifrado
Descifrar el segundo mensaje de comunicación, con la clave simétrica, para obtener el segundo mensaje de comunicación
550

Fig. 5

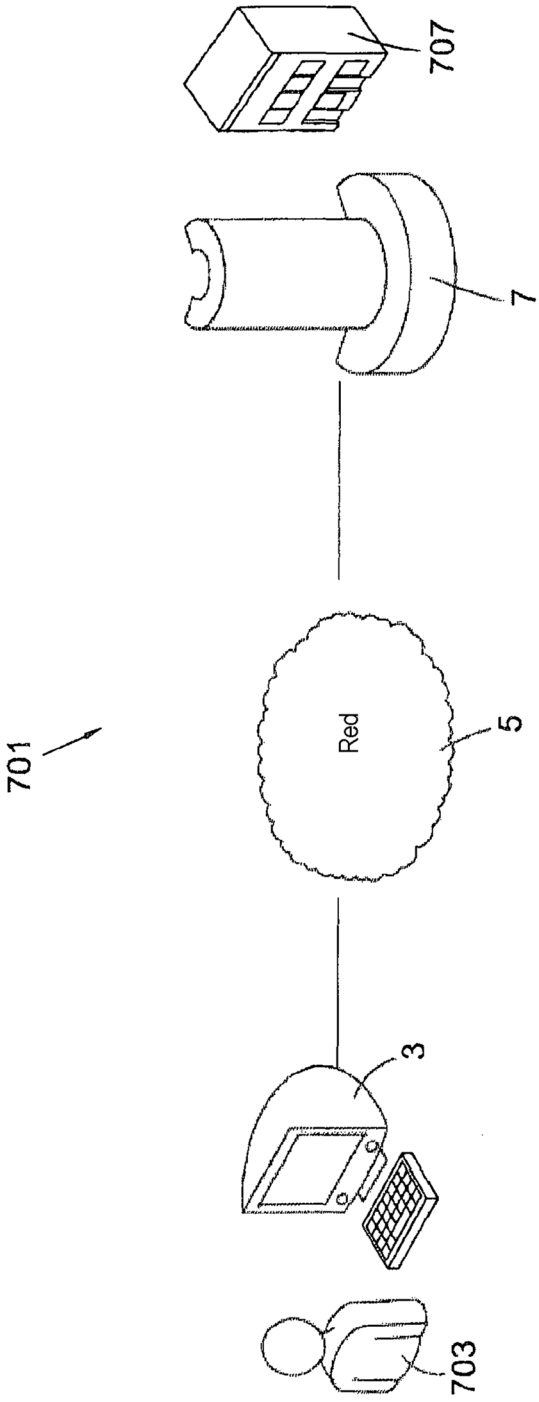


Fig. 6

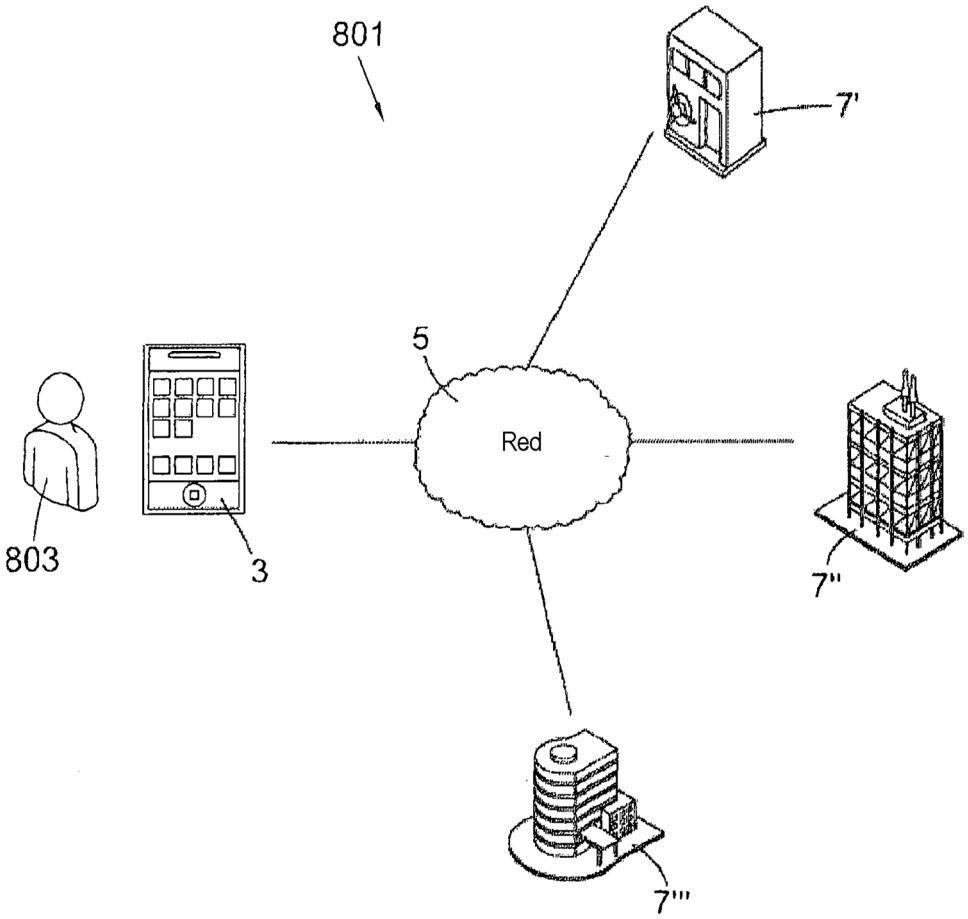


Fig. 7

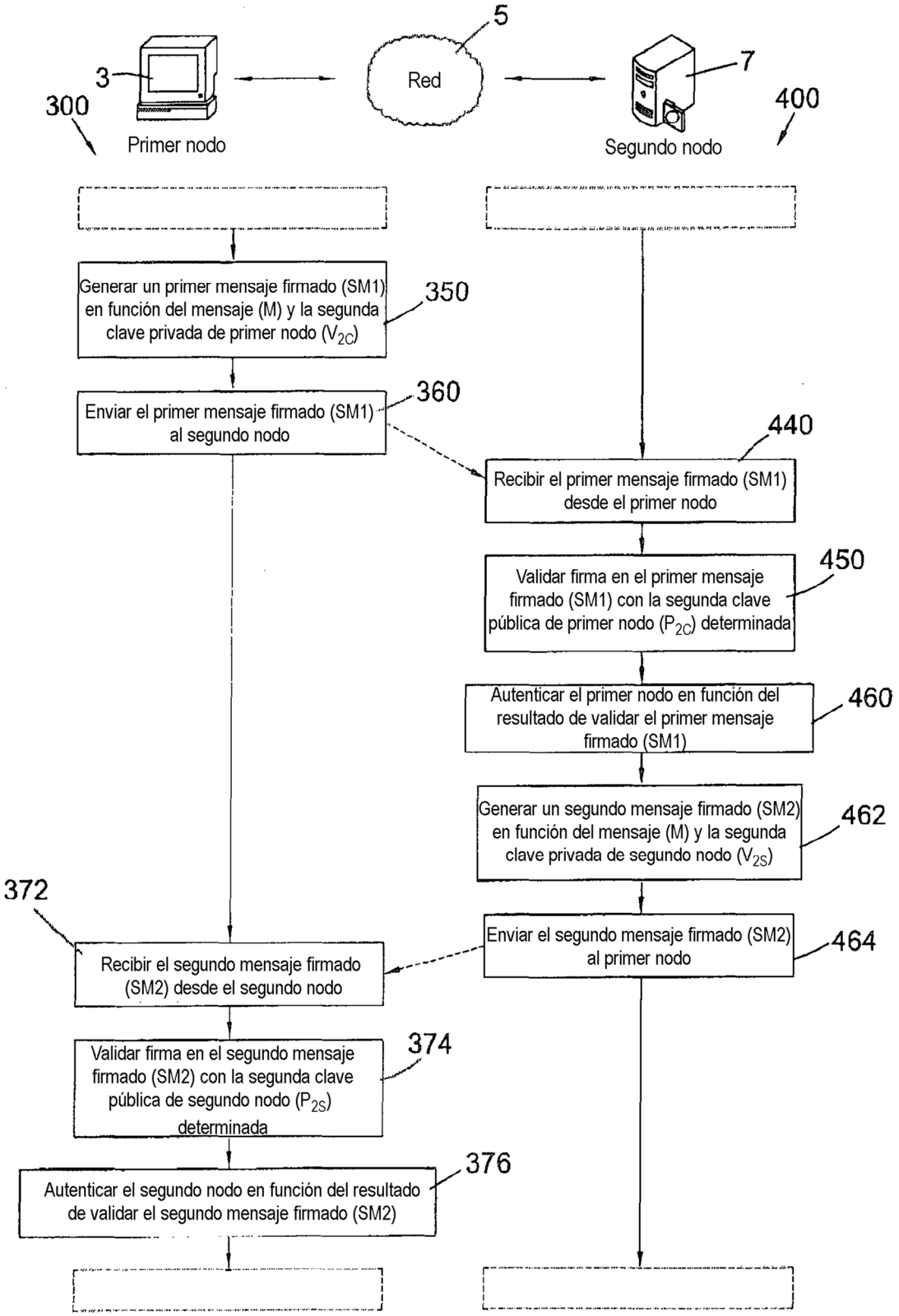
5
Red
3
7
300
400
Primer nodo
Segundo nodo
Generar un primer mensaje firmado (SM1) en función del mensaje (M) y la segunda clave privada de primer nodo ($V_{2C}$)
350
Enviar el primer mensaje firmado (SM1) al segundo nodo
360
440
Recibir el primer mensaje firmado (SM1) desde el primer nodo
Validar firma en el primer mensaje firmado (SM1) con la segunda clave pública de primer nodo ($P_{2C}$) determinada
450
Autenticar el primer nodo en función del resultado de validar el primer mensaje firmado (SM1)
460
Generar un segundo mensaje firmado (SM2) en función del mensaje (M) y la segunda clave privada de segundo nodo ($V_{2S}$)
462
372
Enviar el segundo mensaje firmado (SM2) al primer nodo
464
Recibir el segundo mensaje firmado (SM2) desde el segundo nodo
Validar firma en el segundo mensaje firmado (SM2) con la segunda clave pública de segundo nodo ($P_{2S}$) determinada
374
Autenticar el segundo nodo en función del resultado de validar el segundo mensaje firmado (SM2)
376

Fig. 8

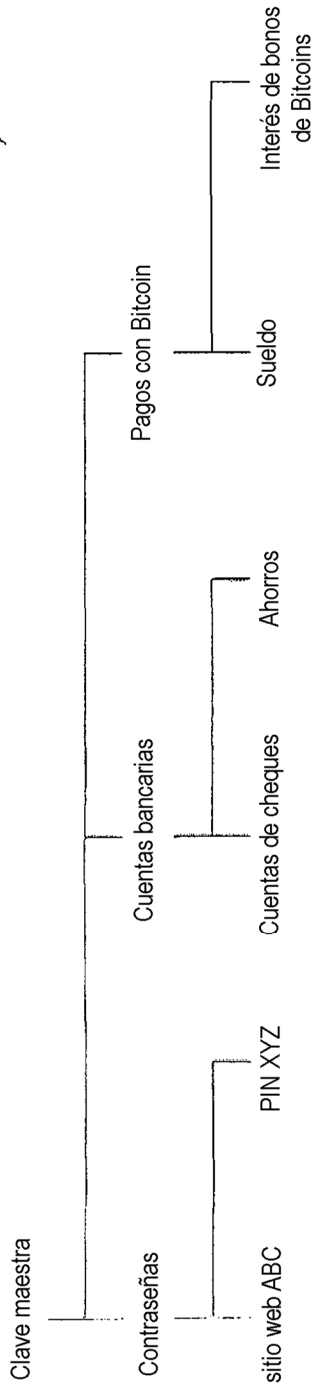
901
Clave maestra
Contraseñas
sitio web ABC
PIN XYZ
Cuentas bancarias
Cuentas de cheques
Ahorros
Pagos con Bitcoin
Sueldo
Interés de bonos de Bitcoins

Fig. 9

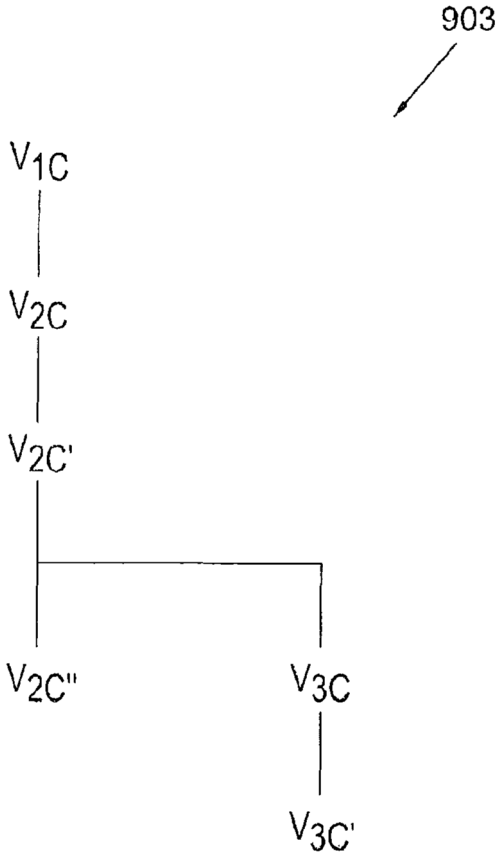


Fig. 10

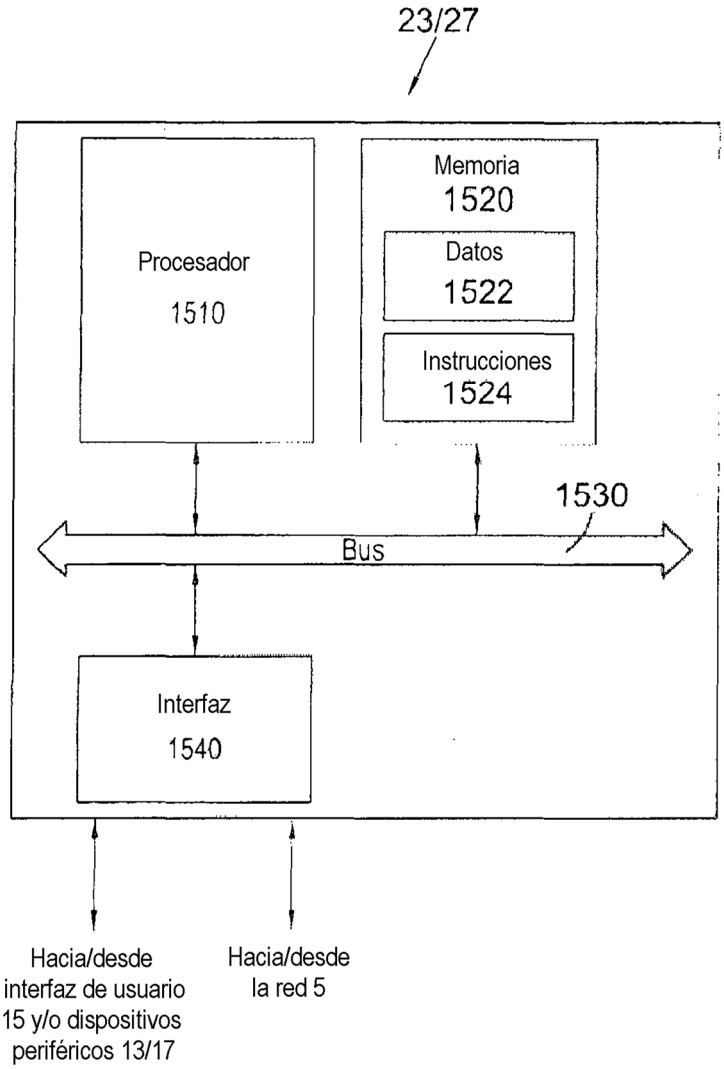
23/27
Procesador
1510
Memoria
1520
Datos
1522
Instrucciones
1524
1530
Bus
Interfaz
1540
Hacia/desde interfaz de usuario 15 y/o dispositivos periféricos 13/17
Hacia/desde la red 5

Fig. 11