

**ALMACENAMIENTO Y TRANSFERENCIA SEGUROS RESISTENTES A PÉRDIDA DE  
MÚLTIPLES PARTES DE CLAVES CRIPTOGRÁFICAS PARA SISTEMAS A BASE DE CADENA  
DE BLOQUES EN CONJUNTO CON UN SISTEMA DE ADMINISTRACIÓN DE BILLETERA**

5

**MEMORIA DESCRIPTIVA**

Esta invención se refiere generalmente a seguridad de computadoras y de datos, y más particularmente a manejo seguro de artículos de datos altamente sensibles tal como claves criptográficas. La invención proporciona un mecanismo de control de acceso. La invención es particularmente adecuada para, pero no está limitada a, uso con billeteras digitales (softwares). Esto puede incluir, por ejemplo, billeteras utilizadas con relación a criptodivisas tal como Bitcoin. La invención proporciona un mecanismo de control de acceso ventajoso.

La criptografía involucra técnicas para almacenamiento seguro de datos sensibles, así como su comunicación entre dos o más nodos en una red. Un nodo puede incluir un dispositivo de comunicación móvil, una computadora de tableta, una computadora laptop, de escritorio, otras formas de dispositivos de cómputo y dispositivos de comunicación, un dispositivo de servidor en una red, un dispositivo de cliente en una red, uno o más nodos en una red distribuida, etc. Los nodos pueden estar asociados con, por ejemplo, una persona física, un grupo de personas tal como empleados de una compañía, un sistema tal como un sistema bancario, o un libro de contabilidad distribuido, entre pares (es decir, cadena de bloques).

Dos o más nodos pueden estar enlazados por una red de comunicaciones que es insegura y vulnerable a interceptación o intercepción por terceras partes no autorizadas. Por lo tanto, mensajes enviados entre nodos frecuentemente son enviados en forma encriptada. Con la recepción, el receptor deseado descifra los mensajes con clave(s) de descifrado correspondientes u otros métodos de descifrado. De esa forma, la seguridad de tal comunicación puede ser dependiente en prevenir que la tercera parte determine la clave de descifrado correspondiente.

Un método criptográfico conocido incluye utilizar logaritmos de clave simétrica. Las claves son simétricas en el sentido de que la misma clave simétrica se utiliza tanto para encriptación de un mensaje de texto simple como para descifrado del mensaje de texto cifrado. Sin embargo, la clave simétrica debe transmitirse a ambos nodos en una forma segura para prevenir acceso no autorizado a ésta. Esto puede incluir, por ejemplo, entregar físicamente la clave simétrica a los nodos (autorizados) de manera que la clave simétrica nunca es transmitida por una red de comunicaciones insegura. Sin embargo, la entrega física no siempre es una opción práctica. Por lo tanto, un problema en tales sistemas criptográficos es el establecimiento de la clave simétrica (que puede basarse en un secreto común) entre los nodos a través de una red electrónica insegura tal

como el Internet. De esa forma, este paso de proporcionar una clave simétrica (el secreto común) es una vulnerabilidad potencialmente catastrófica. Ya que los algoritmos de clave simétrica y protocolos son simples y muy utilizados, existe una necesidad de dos nodos para determinar una clave simétrica basada en secreto común de manera segura a través de una red insegura.

5 El uso de claves asimétricas, también conocido como criptografía de clave pública, alivia este problema a cierto grado. Aunque la clave privada se mantiene secreta, su clave pública correspondiente puede hacerse públicamente disponible. Su intercepción en una red no es catastrófica. Protocolos existentes incluyen el Intercambio de Clave Diffie-Hellman y el Protocolo de Tres Pasos.

10 Sin embargo, el almacenamiento de la clave privada da origen a preocupaciones de seguridad significativas. Considerar, por ejemplo, una billetera digital tal como una billetera de Bitcoins. Las billeteras digitales comprenden software que permite a un usuario conectarse con otros nodos para realizar transacciones con sus activos electrónicos, por ejemplo, al utilizar fondos de Bitcoins para comprar artículos y servicios. La criptografía de clave pública frecuentemente se utiliza  
15 para proteger la información vital que es necesaria para tales conexiones y transacciones. La clave privada está almacenada ya sea por la billetera instalada en el dispositivo del usuario ('lado del cliente') o por un proveedor de servicio de billetera ('lado del servidor'). Sin embargo, si la clave privada es almacenada únicamente en el lado del cliente, la clave privada puede perderse a través de robo, pérdida o daño provocados por el hardware del usuario, por ejemplo, computadora, teléfono  
20 móvil, etc. Similarmente, si el usuario mueve o queda incapacitado, se puede perder el conocimiento de o acceso a la clave privada y de esa forma los fondos asociados con la billetera se vuelven inaccesibles. Aunque el almacenamiento del lado de servidor de la clave privada puede superar estos problemas, el usuario debe estar preparado para confiar en el proveedor de servicio para mantener su clave privada segura. Las violaciones de seguridad en el lado de servidor son un riesgo real y  
25 significativo.

De esa forma, es deseable proporcionar una solución que permita el manejo seguro de un secreto. Este secreto puede ser una clave criptográfica y/o algo que puede proporcionar acceso a la clave. Tal solución mejorada ahora se ha previsto. De conformidad con la presente invención se proporciona una solución mejorada como se define en las reivindicaciones anexas.

30 La invención puede proporcionar un método implementado por computadora. Puede permitir el control de acceso a un recurso. Puede llamarse un método de verificación o autenticación. Puede denominarse como una solución de administración de clave criptográfica. El recurso puede ser cualquier tipo de recurso físico o electrónico. En una modalidad, el recurso es una billetera digital o algún otro recurso que se refiere a una forma de divisa. Puede ser una billetera de  
35 Bitcoins u otra billetera para la administración de recursos de criptodivisa. La invención puede

proporcionar un método para controlar acceso a una billetera digital (y sistema correspondiente).

La invención puede utilizarse durante la configuración, registro o creación de una billetera digital a través de un canal de comunicación inseguro (tal como el Internet), para permitir operaciones relacionadas con billetera subsecuentes tal como transacciones que se van a manejar, comunicar y/o crear en una forma segura.

Una o más modalidades de la invención pueden comprender el paso de derivar la clave criptográfica de un par de claves criptográficas existente. Esto puede comprender los pasos de:

determinar una segunda clave privada de primera entidad con base en al menos una clave privada maestra de primera entidad y un valor de generador;

determinar una segunda clave privada de segunda entidad con base al menos en una clave privada maestra de segunda entidad y el valor de generador;

determinar un secreto común (CS, por sus siglas en inglés) en la primera entidad con base en la segunda clave privada de primera entidad y la segunda clave pública de segunda entidad, y determinar el secreto común (CS) en la segunda entidad con base en la segunda clave privada de segunda entidad y segunda clave pública de primera entidad; y

en donde:

la segunda clave pública de primera entidad y la segunda clave pública de segunda entidad se basan respectivamente al menos en la clave maestra de primera/segunda entidad y el valor de generador.

Adicional o alternativamente, la invención puede comprender un método para controlar acceso a una billetera digital, el método que comprende los pasos:

determinar una segunda clave privada de primera entidad con base al menos en una clave privada maestra de primera entidad y un valor de generador;

determinar una segunda clave privada de segunda entidad con base en al menos una clave privada maestra de segunda entidad y el valor de generador;

determinar un secreto común (CS) en la primera entidad con base en la segunda clave privada de primera entidad y la segunda clave pública de segunda entidad, y determinar el secreto común (CS) en la segunda entidad con base en la segunda clave privada de segunda entidad y segunda clave pública de primera entidad; y

en donde:

la segunda clave pública de primera entidad y la segunda clave pública de segunda entidad se basan respectivamente al menos en la clave maestra de primera/segunda entidad y el valor de generador.

Adicional o alternativamente, el método puede comprender los pasos:

dividir un elemento de verificación en una pluralidad de acciones;

determinar un secreto común en o sobre dos o más nodos en una red;

utilizar el secreto común para transmitir al menos una acción del elemento de verificación de un nodo en la red a al menos otro nodo.

El elemento de verificación puede ser una clave criptográfica. Puede ser una clave  
5 privada en un par de criptografía asimétrica. Adicional o alternativamente, puede ser una representación de una clave criptográfica, o algún artículo que puede utilizarse para acceder, calcular, derivar o recuperar una clave criptográfica. Pueden ser algún secreto o valor que puede utilizarse en un proceso de verificación tal como, por ejemplo, mnemotécnico o una semilla.

De esa forma, un aspecto de la invención puede referirse a dividir un secreto tal  
10 como una clave privada en acciones (única). El elemento de verificación puede estar dividido en una pluralidad de acciones de manera que el elemento de verificación pueda restaurarse o regenerarse de dos o más de las acciones. Puede utilizarse el Esquema de Distribución Secreta de Shamir para dividir el elemento de verificación en acciones.

Las acciones pueden dividirse de manera que cualquiera acción por sí misma no sea  
15 de ningún valor, lo que significa que no pueda utilizarse para llegar al elemento de verificación (original, no dividido). La división puede realizarse de manera que el elemento de verificación pueda restaurarse únicamente después de la combinación de un número predeterminado de acciones. En una modalidad, cualquiera de dos acciones puede ser suficiente para restauración del elemento de verificación.

Otro aspecto de la invención puede referirse a manejo o almacenamiento seguro de  
20 las acciones respectivas. Las acciones pueden ser enviadas a, y almacenadas por, diferentes partes. Algunas o todas estas partes pueden ser nodos sobre la red. En una modalidad, el método puede comprender el paso de almacenar al menos tres acciones del elemento de verificación en diferentes ubicaciones con relación una a la otra.

Al menos una de las acciones puede almacenarse en o sobre una instalación de  
25 respaldo o "de almacenamiento seguro". Esta puede estar separada, independiente y/o distinta de cualquier otra ubicación que almacena una acción. Esto proporciona una ventaja importante, debido a que permite restauración del elemento de verificación en el caso de que una de las otras acciones se vuelva no disponible. En tal situación, la acción puede recuperarse de la instalación de  
30 almacenamiento seguro.

Un proceso de verificación puede realizarse antes de la restauración del elemento de verificación al utilizar las acciones. El proceso de verificación puede comprender verificación de la identidad de un individuo predeterminado o designado, y/o un recurso de cómputo.

Otro aspecto de la invención puede referirse a la distribución segura de una o más  
35 de las acciones. Los métodos pueden comprender el paso de utilizar el secreto común para generar

una clave de encriptación, en donde la clave de encriptación se utiliza para encriptar al menos una acción del elemento de verificación o un mensaje que comprende dicha al menos una acción.

El secreto común puede determinarse en los por lo menos dos nodos independientemente uno de otro. De esa forma, cada nodo puede determinar o generar el secreto para ellos mismos, sin entrada de o comunicación con el otro nodo u otra parte. Esto significa que el secreto común puede no requerir transmisión sobre un canal de comunicaciones. Esto proporciona seguridad mejorada debido a que no puede interceptarse por partes no autorizadas. El secreto común puede ser común para (es decir, compartido por) únicamente los por lo menos dos nodos. El secreto común entonces puede utilizarse para generar una clave de encriptación, y esa clave de encriptación puede utilizarse para la transmisión segura de la(s) acción(acciones). Otros datos también pueden transmitirse al utilizar la clave de encriptación.

El método puede comprender el paso de determinar, en un primer nodo (C), un secreto común (CS) que es común con el primer nodo (C) y un segundo nodo (S), en donde el primer nodo (C) está asociado con un primer par de criptografía asimétrica que tiene una clave privada maestra del primer nodo ( $V_{1C}$ ) y una clave pública maestra del primer nodo ( $P_{1C}$ ), y el segundo nodo (S) está asociado con un segundo par de criptografía asimétrica que tiene una clave privada maestra del segundo nodo ( $V_{1S}$ ) y una clave pública maestra del segundo nodo ( $P_{1S}$ ), en donde el método comprende:

- determinar una segunda clave privada del primer nodo ( $V_{2C}$ ) con base al menos en la clave privada maestra del primer nodo ( $V_{1C}$ ) y un Valor de Generador (GV);
- determinar una segunda clave pública del segundo nodo ( $P_{2S}$ ) con base al menos en la clave pública maestra del segundo nodo ( $P_{1S}$ ) y el Valor de Generador (GV); y
- determinar el secreto común (CS) con base en la segunda clave privada del primer nodo ( $V_{2C}$ ) y la segunda clave pública del segundo nodo ( $P_{2S}$ ).

en donde el segundo nodo (S) tiene el mismo secreto común (S) con base en una segunda clave pública del primer nodo ( $P_{2C}$ ) y una segunda clave privada del segundo nodo ( $V_{2S}$ ), en donde: la segunda clave pública del primer nodo ( $P_{2C}$ ) se basa en al menos la clave pública maestra del primer nodo ( $P_{1C}$ ) y el Valor de Generador (GV); y la segunda clave privada del segundo nodo ( $V_{2S}$ ) se basa en al menos la clave privada maestra del segundo nodo ( $V_{1S}$ ) y el Valor de Generador (GV).

El Valor de Generador (GV) se puede basar en un mensaje (M). El método además puede comprender: generar un primer mensaje firmado (SM1) con base en el mensaje (M) y la segunda clave privada del primer nodo ( $V_{2C}$ ) y enviar, sobre la red de comunicaciones, el primer mensaje firmado (SM1) al segundo nodo (S), en donde el primer mensaje firmado (SM1) se puede validar con una segunda clave pública del primer nodo ( $P_{2C}$ ) para autenticar el primer nodo (C).

El método también puede comprender: recibir, sobre la red de comunicaciones, un segundo mensaje firmado (SM2) del segundo nodo (S); validar el segundo mensaje firmado (SM2) con la segunda clave pública del segundo nodo (P2S) y autenticar el segundo nodo (S) con base en el resultado de validar el segundo mensaje firmado (SM2), en donde el segundo mensaje firmado (SM2) se generó con base en el mensaje (M), o un segundo mensaje (M2), y la segunda clave privada del segundo nodo ( $V_{2S}$ ).

El método además puede comprender generar un mensaje (M); y enviar, sobre una red de comunicaciones, el mensaje (M) al segundo nodo (S). Alternativamente, el método puede comprender recibir el mensaje (M), sobre la red de comunicaciones, desde el segundo nodo (S). Incluso en otra alternativa, el método puede comprender recibir el mensaje (M) sobre la red de comunicaciones, desde otro nodo. Incluso en otra alternativa, el método puede comprender recibir el mensaje (M) de un almacenamiento de datos, y/o una interfaz de entrada asociada con el primer nodo (C).

La clave pública maestra del primer nodo ( $P_{1C}$ ), clave pública maestra del segundo nodo ( $P_{1S}$ ) puede basarse en multiplicación de punto de curva elíptica de la clave privada maestra del primer nodo ( $V_{1C}$ ) respectiva y clave privada maestra del segundo nodo ( $V_{1S}$ ) y un generador (G).

El método además puede comprender los pasos de: recibir, sobre la red de comunicaciones, la clave pública maestra del segundo nodo ( $P_{1S}$ ); y almacenar, en un almacenamiento de datos asociado con el primer nodo (C), la clave pública maestra del segundo nodo ( $P_{1S}$ ).

El método además puede comprender los pasos de: generar, en un primer nodo (C), la clave privada maestra del primer nodo ( $V_{1C}$ ) y la clave pública maestra del primer nodo ( $P_{1C}$ ); enviar, sobre la red de comunicaciones, la clave pública maestra del primer nodo ( $P_{1C}$ ) al segundo nodo (S) y/u otro nodo; y almacenar, en un primer almacenamiento de datos asociado con el primer nodo (C), la clave privada maestra del primer nodo ( $V_{1C}$ ).

El método también puede comprender: enviar, sobre la red de comunicaciones, al segundo nodo, una notificación indicativa de utilizar un sistema de criptografía de curva elíptica (ECC, por sus siglas en inglés) común con un punto base (G) para el método de determinar un secreto común (CS). El paso de generar la clave privada maestra del primer nodo ( $V_{1C}$ ) y la clave pública maestra del primer nodo ( $P_{1C}$ ) puede comprender: generar la clave privada maestra del primer nodo ( $V_{1C}$ ) con base en un número entero aleatorio en un intervalo permisible especificado en el sistema ECC común; y determinar la clave pública maestra del primer nodo ( $P_{1C}$ ) con base en multiplicación de punto de curva elíptica de la clave privada maestra del primer nodo ( $V_{1C}$ ) y el punto base (G) de conformidad con la siguiente fórmula:

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

El método además puede comprender: determinar el Valor de Generador (GV) con base en determinar una función hash del mensaje (M), en donde el paso de determinar una segunda clave privada del primer nodo (V<sub>2C</sub>) se basa en una suma escalar de la clave privada maestra del primer nodo (V<sub>1C</sub>) y el Valor de Generador (GV) de conformidad con la siguiente fórmula:

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

El paso de determinar una segunda clave pública del segundo nodo (P<sub>2S</sub>) se puede basar en la clave pública maestra del segundo nodo (P<sub>1S</sub>) con suma de punto de curva elíptica a la multiplicación de punto de curva elíptica del Valor de Generador (GV) y el punto base (G) de conformidad con la siguiente fórmula:

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

El Valor de Generador (GV) se puede basar en determinar una función hash de un Valor de Generador (GV) previo.

El primer par de criptografía asimétrica y el segundo par de criptografía asimétrica se pueden basar en una función de primer par de criptografía asimétrica previo respectivo y segundo par de criptografía asimétrica previo.

En una redacción alternativa, la invención puede proporcionar un método que comprende los pasos:

- dividir un elemento de verificación en una pluralidad de acciones;
- generar, en un primer nodo, una clave criptográfica privada derivada (o segunda) con base en un primer par de claves asimétricas maestro;
- utilizar la clave privada derivada para la encriptación y/o transmisión segura de al menos una acción del elemento de verificación.

El método también puede comprender el paso de generar, en un segundo nodo, la misma clave privada derivada, ésta siendo generalmente independiente del primer nodo y con base en un segundo par de claves asimétricas maestro.

La clave privada derivada puede ser parte de un par de claves asimétricas que comprende la clave privada y una clave pública. El primer y/o segundo nodos pueden utilizar una Criptografía de Curva Elíptica para generar la clave privada (y su clave pública correspondiente).

El método puede comprender las etapas:

- Acordar, entre el primer y segundo nodos, un sistema ECC estándar al utilizar un punto base (G); y/o
- generar, en el primer y/o segundo nodo, un par de clave pública/privada que utiliza el sistema SC estándar acordado y publicar la clave pública; esto puede significar hacerlo públicamente disponible; y/o
- registrar la clave pública maestra del primer nodo (P<sub>MC</sub>) en el segundo nodo

u otra ubicación; y/o registrar la clave pública maestra del segundo nodo ( $P_{MC}$ ) en el primer nodo u otra ubicación; y/o

- enviar un mensaje ( $M$ ) del primer nodo al segundo nodo y/o viceversa, y crear una función hash del mensaje; el mensaje puede ser firmado al utilizar la clave privada derivada; este paso puede representar la transmisión única requerida para 1) establecer un secreto compartido entre los nodos y 2) indica una sesión de comunicación asegurada entre ellas. El primer o segundo nodo pueden utilizar el mensaje  $M$  recibido para generar su propio par de claves públicas/privadas derivado (secundario). Esto puede permitir al nodo calcular la otra clave pública derivada del nodo; y/o

10                   • recibir el mensaje y calcular independientemente la función hash del mensaje  $M$  (por ejemplo,  $SHA-256(M)$ ); y/o

- calcular una clave pública ( $P_{2C}$ ) que se puede derivar de la clave maestra ( $P_{MC}$ ); y/o

- validar la firma ( $Sig-V_{2C}$ ) contra el  $P_{2C}$  calculado

15                   La clave privada derivada puede ser derivada de manera determinista de la clave pública maestra del primer o segundo nodo.

La invención también puede comprender un sistema implementado por computadora dispuesto y configurado para implementar cualquier modalidad del(de los) método(s) descrito(s) anteriormente. El sistema puede comprender o utilizar una red de plataforma de cadena de bloques.

20                   Adicional o alternativamente, puede comprender un proveedor de billetera digital o sistema de administración.

Cualquier característica descrita anteriormente con relación a un aspecto o modalidad de la invención también puede utilizarse con relación a cualquier otro aspecto o modalidad. Por ejemplo, una característica descrita con relación al método puede aplicar al sistema y viceversa.

25                   Éstos y otros aspectos de la invención serán evidentes a partir de y se aclararán con referencia a, la modalidad aquí descrita.

Una modalidad de la presente invención se describirá ahora, a manera de ejemplo únicamente, y con referencia a las figuras anexas, en donde:

30                   la Figura 1 es un diagrama esquemático de un sistema ilustrativo para determinar un secreto común para un primer nodo y un segundo nodo, según pueda utilizarse de conformidad con la presente invención para transmisión segura de información altamente sensible, tal como una acción de una clave privada;

35                   la Figura 2 es un cuadro de flujo de métodos implementados por computadora para determinar un secreto común según pueda utilizarse de conformidad con la presente invención para

transmisión segura de información altamente sensible, tal como una acción o una clave privada;

la Figura 3 es un cuadro de flujo de métodos implementados por computadora para registrar el primer y segundo nodos;

la Figura 4 es otro cuadro de flujo de métodos implementados por computadora para  
5 determinar un secreto común según pueda utilizarse de conformidad con la presente invención para asegurar transmisión de información altamente sensible, tal como una acción de una clave privada;

la Figura 5 es un cuadro de flujo de métodos implementados por computadora de comunicación segura entre el primer nodo y segundo nodo.

Como se explicó anteriormente, existe una necesidad de almacenamiento y/o  
10 intercambio mejorado de un secreto tal como una clave criptográfica, o un secreto que pueda utilizarse para generar una clave. El secreto puede ser una semilla para un mnemotécnico de billetera, u otro artículo relacionado con seguridad. La invención proporciona tal solución. Se describe una modalidad a continuación para los propósitos de ilustración, y usos del contexto de una billetera digital implementada en una cadena de bloques. Sin embargo, la invención no está limitada  
15 a tales implementaciones y podría implementarse con respecto a cualquier red o sistema implementado por computadora.

Como anteriormente, la criptografía de clave pública se utiliza frecuentemente con relación a billeteras digitales. Si el usuario final (que puede denominarse como un "cliente" o simplemente "usuario") es responsable de almacenar su clave privada, pueden surgir problemas  
20 cuando el usuario o su hardware se vuelven no disponibles ya que esto hace inaccesible la clave privada, y de esa forma los fondos de la billetera. Sin embargo, el almacenamiento de la clave en el extremo del proveedor de billetera (que puede denominarse como "lado de servidor") requiere un grado de confianza tanto en el proveedor como en sus mecanismos de seguridad. Así que existe una necesidad de almacenar la clave privada de tal forma que no pueda obtenerse por una parte no  
25 autorizada, sino que también pueda reproducirse cuando sea necesario. El término "usuario" puede ser un usuario humano o un recurso implementado por computadora.

Un algoritmo criptográfico conocido, conocido como "esquema de distribución de secreto de Shamir" (4S), enseña a dividir el secreto en partes o acciones únicas que entonces se distribuyen a diferentes partes. Las acciones pueden utilizarse para reconstruir el secreto en lo  
30 sucesivo. Cada acción individual no es de valor o uso en sí misma hasta que se combina con una o más de otras acciones. El número de acciones requeridas para reconstruir el secreto puede variar de conformidad con las necesidades de la situación. En algunos casos, pueden requerirse todas las acciones, mientras en otros casos únicamente se requiere un número suficiente. Esto es conocido como el esquema umbral, en donde cualquier  $k$  de acciones son suficientes para reconstruir el  
35 secreto original.

En la modalidad ilustrativa, 4S se utiliza para dividir un secreto tal como una red privada o una semilla mnemotécnica en un número de partes. Entonces también se utiliza para regenerar la clave o semilla mnemotécnica de cierto número de partes. El uso de mnemotécnicos es conocido en conjunto con billeteras digitales. El mnemotécnico es un código fácil de usar o grupo de palabras que pueden volverse una semilla binaria para la generación de una billetera o datos.

Aquí, pueden utilizarse los siguientes términos.

- “Secreto” (S) es un secreto (por ejemplo, un número o valor) que necesita compartirse de manera segura entre partes.
- “Acción” es una pieza del secreto. El secreto está dividido en piezas y cada pieza es llamada una acción. Se calcula a partir del secreto dado. Con el fin de recuperar el secreto, uno debe obtener cierto número de acciones.
- “Umbral” (k) es el número mínimo de acciones que uno necesita para regenerar o recuperar el secreto. El secreto puede ser regenerado únicamente cuando tiene  $\geq k$  acciones.

- “Primo” (p) es un número primo aleatorio.

Desde una perspectiva amplia, una modalidad ilustrativa puede comprender un método como a continuación. En este ejemplo, utilizamos un esquema ‘2 de 3’ (es decir  $k = 2$ );

- Un usuario se registra con un proveedor de billetera para generar y configurar una nueva billetera asociada con ese usuario. En este ejemplo, la billetera es una billetera de Bitcoins, que utiliza la Cadena de Bloques
- Un par de clave pública-privada se genera y asocia con la billetera del usuario;
- La clave privada está dividida en acciones, que utiliza 4S
- Una acción de la clave privada se envía a través de una transmisión segura al usuario
- Otra acción de la clave privada se retiene por el proveedor de servicio y se almacena en un servidor
- Otra acción se envía a través de una transmisión segura a una ubicación remota para almacenamiento seguro. El término ‘remota’ no implica cualquier distancia geográfica o ubicación particular. En lugar de esto, se utiliza aquí para significar que la acción se retiene dentro, en o sobre una instalación de almacenamiento seguro o recurso que es independiente en algún sentido del proveedor de billetera o el usuario, preferiblemente ambos. “Independiente” puede incluir físico, lógico, financiero, político y/o independiente por organización. Por ejemplo, el almacenamiento seguro puede subcontratar una entidad comercial que proporciona el servicio de almacenamiento seguro por una cuota; o puede celebrarse por el apoderado del usuario, o alguna

otra parte elegida (y confiada) que acepta responsabilidad para almacenar la acción y suministrarla a demanda si es necesario;

- El proveedor de billetera puede destruir cualquier o todas las copias de la clave privada completa, debido a que ya no es necesaria. Cuando es necesaria la clave privada para autorización subsecuente del usuario (por ejemplo, debido a que el usuario ahora desea hacer una transacción) la clave puede ser reconstruida de la acción del usuario, que el usuario proporciona al proveedor de billetera como y cuando sea necesario, y la acción de proveedor de billetera.

Una ventaja de esto es que incluso si se viola la seguridad del proveedor de billetera, la parte no autorizada no puede obtener acceso a la clave privada del usuario debido a que no está almacenada en ninguna parte en el sistema de proveedor de billetera y el sistema del proveedor de billetera sólo no contiene suficientes acciones para permitir reconstrucción de la clave privada. Esta misma ventaja aplica en situaciones en donde se viola la seguridad del cliente.

Otra ventaja es que, al almacenar una acción en una ubicación de almacenamiento segura, la clave privada puede ser reconstruida al recuperar esa acción de almacenamiento seguro y al combinarla con la acción de proveedor de billetera. De esa forma, si el usuario muere o queda incapacitado, o si se pierde, daña o es robado el hardware del usuario (y de esa forma la acción), aún se puede acceder a los fondos en la billetera. En tal situación, se verificaría la identidad del usuario. En algunos casos, la identidad de una parte probada, confiada tal como una albacea de una propiedad o apoderado se verificaría. Esto puede lograrse, por ejemplo, tras la producción de evidencia tal como un certificado de muerte, pasaporte, un documento legal u otra forma de identificación. Tras la verificación de identidad autorizada, la acción del secreto se recuperaría de almacenamiento seguro. Por lo tanto, el almacenamiento seguro sirve como un tipo de instalación de respaldo que puede utilizarse en circunstancias excepcionales o predeterminadas.

De esa forma, la invención proporciona una combinación ventajosa de sistema mejorado/conveniencia extra de seguridad de datos. Proporciona una solución simple, efectiva y segura para control de acceso.

Se debe observar que, en el ejemplo anterior, la clave privada se genera por el proveedor de servicio de billetera y partes respectivas envían al usuario y recurso de almacenamiento seguro. Sin embargo, éste puede no ser el caso en otras modalidades. Es importante observar que la transmisión de partes entre las partes, que pueden denominarse como 'nodos', debe realizarse en una forma segura debido a que cualquier intersección no autorizada de múltiples acciones podría permitir que el interceptor reconstruya el secreto (por ejemplo, mnemotécnico o clave). Este problema de intercambio también se aborda por la invención, como se describe a continuación.

Más aspectos detallados de la invención se describen ahora para el propósito de

ilustración. Se debe observar que el Esquema de Distribución de Secreto de Shamir es una técnica que es conocida en la técnica y el experto en la técnica estaría consciente de cómo entender y sería capaz de utilizarla. Por lo tanto, se proporciona lo siguiente para el propósito de integridad únicamente.

### 5 **Dividir el Secreto en Acciones**

Dado un secreto  $S$ , un número de participantes  $n$ , un número umbral  $k$ , y algún número primo  $p$ , construimos un polinomio:

$$y = f(x) \text{ de grado } k - 1 \text{ (nuestro primo } p \text{ en módulos)}$$

con término constante  $S$ .

10 Después, elegimos  $n$  números enteros aleatorios únicos entre 1 y  $p-1$ , inclusive, y evaluamos el polinomio en esos  $n$  puntos. Cada uno de los  $n$  participantes se proporciona con un par  $(x, y)$ . Esto puede lograrse por los siguientes pasos.

#### 1. Convertir en un Número Entero

15 Para el algoritmo 4S, el secreto necesita ser un número entero. Por ello, si el secreto está en algún otro formato (por ejemplo, secuencia, hexadecimal, etc. debe convertirse en un número entero primero. Si el secreto ya es un número entero, este paso puede omitirse. Para este ejemplo, permitir  $S = 1234$ .

#### 2. Decidir número de acciones ( $n$ ) y umbral ( $k$ )

20 Observar que se requerirán partes para regenerar el secreto. Por ello, elegir  $S$  y  $k$  de manera que  $k$  partes pueden siempre obtenerse mientras se recupera el secreto. Para este ejemplo, permitir  $n = 6$ ,  $k = 3$ .

#### 3. Crear el polinomio

Necesitamos crear un polinomio de la forma:  $y = f(x) \bmod p$

i. Determinar término y grado constante del polinomio

25  $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots + a_{k-1}x^{k-1}$

- El término constante  $a_0 = S$

- grado del polinomio =  $k-1$

Por ello, para  $k = 3$  y  $S = 1234$ , necesitamos construir un polinomio con *grado* 2 y  $a_0 = 1234$

30  $f(x) = 1234 + a_1x + a_2x^2$

ii. Determinar coeficientes

Elegir  $k-1$  números aleatorios (utilizar un Generador de Número Aleatorio (o pseudo aleatorio)) de manera que:

$$0 < a_i \leq S$$

35 Permitir  $a_1 = 166$ ;  $a_2 = 94$

Por ello,  $f(x) = 1234 + 166x + 94x^2$

iii. Seleccionar un número primo aleatorio

Elegir un número primo aleatorio ( $p$ ) de manera que:

$$p > \max(S, n)$$

5

Sea  $p = 1613$

iv. Polinomio final

$$y = f(x) \bmod p$$

$$y = (1234 + 166x + 94x^2) \bmod 1613$$

### Crear las acciones

10

Para dividir el secreto en  $n$  acciones, necesitamos construir  $n$  puntos (acciones) al utilizar el polinomio:

$$y = (1234 + 166x + 94x^2) \bmod 1613$$

Ya que  $n = 6$  para este ejemplo, tendremos seis puntos. Observar que iniciamos con  $x = 1$  y NO  $x = 0$ .

15

Para  $x = 1$  a  $6$ , los 6 puntos son como a continuación:

$$(1, 1494); (2, 329); (3, 965); (4, 176); (5, 1188); (6, 775)$$

De estos  $n$  (6) puntos, cualquier  $k$  (3) puntos puede utilizarse para regenerar la clave secreta.

### Reconstruir el Secreto a partir de un número dado de acciones

20

i. Obtener el número entero secreto

Para reconstruir el secreto, necesitamos la siguiente información:

$$n = 6, k = 3, p = 1613$$

$k$  acciones:

$$(x_0, y_0) = (1, 1494); (x_1, y_1) = (2, 329); (x_2, y_2) = (3, 965)$$

25

Una vez que tenemos la información anterior, podemos utilizar una técnica tal como una Interpolación de Lagrange que se conoce en la técnica y se aprecia fácilmente por el técnico en la materia. Al utilizar esta técnica podemos reconstruir el todo el polinomio. Los coeficientes pueden calcularse de conformidad con la fórmula a continuación:

$$a_i(x) = \left[ \sum_{i=0}^{k-1} y_i \prod_{0 \leq j < k-1, j \neq i} (x - x_j) / (x_i - x_j) \right] \bmod p$$

30

pero ya que  $S = a_0$ , sólo necesitamos encontrar  $a_0 = a_0$

(0)

$$a_0 = \left[ \sum_{i=0}^{k-1} y_i \prod_{0 \leq j < k-1, j \neq i} \frac{-x_j}{x_i - x_j} \right] \bmod p$$

35

en donde  $x_i - x_j \neq 0$

El experto la técnica entenderá que, en lo anterior, el exponente -1 significa tomar la inversa multiplicativa. La mayoría de los lenguajes de programación comprenden paquetes incorporados para realizar operaciones matemáticas tal como inversa multiplicativa.

ii. Convertir número entero a formato deseado

5 Si se realizó el Paso 1 para convertir un formato específico a un número entero, seguimos el procedimiento inverso para convertir el número entero de nuevo al formato deseado.

### **Transmisión segura de las acciones**

10 Como se mencionó anteriormente, es importante que las acciones del secreto se transmitan a los receptores respectivos en una forma segura para prevenir que las partes no autorizadas sean capaces de reconstruir el secreto. En una modalidad preferida, la transmisión segura puede lograrse como se describe a continuación.

Un secreto común (CS) puede establecerse en dos partes y entonces utilizarse para generar una clave de encriptación segura para transmisión de una o más de las acciones. Este secreto común (CS) no se debe confundir con el secreto (S) indicado anteriormente. El Secreto  
15 Común (CS) se genera y utiliza para permitir intercambio seguro del Secreto (S) por ejemplo, clave o acción del mismo.

Las dos partes podrían ser cualquiera de dos del proveedor de servicio de billetera, el usuario, el recurso de almacenamiento seguro o alguna otra parte legítima. Después de eso, para la búsqueda de conveniencia, se denominarán como un primer nodo (C) un segundo nodo (S). El  
20 propósito es generar un secreto común (CS) que ambos nodos conocen, pero sin que ese secreto común haya sido enviado a través de un canal de comunicación, eliminando de esa forma la posibilidad de su descubrimiento no autorizado. La técnica de almacenamiento seguro adicional de división de secreto, en combinación con una técnica de transmisión segura tal como se describe a continuación, proporciona una solución de administración de clave segura.

25 La técnica de transmisión segura de la presente invención involucra el CS que se genera en cada extremo de la transmisión en una forma independiente, de manera que aunque ambos nodos saben que el CS no ha viajado sobre canales de comunicación potencialmente inseguros. Una vez que se ha establecido CS en ambos extremos, puede utilizarse para generar una clave de encriptación segura que ambos nodos pueden utilizar para comunicación después de eso.  
30 Esto es de beneficio particular durante el proceso de registro de billetera, para transmisión de la clave privada de división de una parte a otra.

La Figura 1 ilustra un sistema que incluye un primer nodo 3 que está en comunicación con un segundo nodo 7 sobre una red de comunicaciones 5. El primer nodo 3 tiene un primer dispositivo de procesamiento asociado 23 y el segundo nodo 5 tiene un segundo dispositivo  
35 de procesamiento asociado 27. El primer y segundo nodos 3, 7 pueden incluir un dispositivo

electrónico, tal como una computadora, teléfono, computara de tableta, dispositivo de comunicación móvil, servidor de computadora, etc. En un ejemplo, el primer nodo 3 puede ser un dispositivo de cliente (usuario) y el segundo nodo 7 puede ser un servidor. El servidor puede ser un servidor de proveedor de billetera digital.

5 El primer nodo 3 está asociado con un primer par de criptografía asimétrica que tiene una clave privada maestra del primer nodo ( $V_{1C}$ ) y una clave pública maestra del primer nodo ( $P_{1C}$ ). El segundo nodo (7) está asociado con un segundo par de criptografía asimétrica que tiene una clave privada maestra del segundo nodo ( $V_{1S}$ ) y una clave pública maestra del segundo nodo ( $P_{1S}$ ). En otras palabras, el primer y segundo nodos están cada uno en posesión de pares de clave  
10 pública-privada respectivos.

El primer y segundo pares de criptografía asimétrica para el primer y segundo nodos respectivos 3, 7 pueden generarse durante un proceso de registro, tal como registro para una billetera. La clave pública para cada nodo puede compartirse públicamente, tal como sobre la red de comunicaciones 5.

15 Para determinar el secreto común (CS) en ambos del primer nodo 3 y segundo nodo 7, los nodos 3, 7 realizan pasos de método respectivos 300, 400 sin comunicar claves privadas sobre la red de comunicaciones 5.

El método 300 realizado por el primer nodo 3 incluye determinar 330 una segunda clave privada del primer nodo ( $V_{2C}$ ) con base al menos en la clave privada maestra del primer nodo ( $V_{1C}$ ) y un Valor de Generador (GV). El Valor de Generador se puede basar en un mensaje (M) que es uno compartido entre el primer y segundo nodos, que pueden incluir compartir el mensaje sobre la red de comunicaciones 5 como se describe en detalle adicional a continuación. El método 300 también incluye determinar 370 una segunda clave pública del segundo nodo ( $P_{2S}$ ) con base en al menos la clave pública maestra del segundo nodo ( $P_{1S}$ ) y el Valor de Generador (GV). El método 300  
20 incluye determinar 380 el secreto común (CS) con base en la segunda clave privada del primer nodo ( $V_{2C}$ ) y la segunda clave pública del segundo nodo ( $P_{2S}$ ).

De forma importante, el secreto común (CS) también puede determinarse en el segundo nodo 7 por el método 400. El método 400 incluye determinar 430 una segunda clave pública del primer nodo ( $P_{2C}$ ) con base en la clave pública maestra del primer nodo ( $P_{1C}$ ) y el Valor de Generador (GV). El método 400 además incluye determinar 470 una segunda clave privada del segundo nodo ( $V_{2S}$ ) con base en la clave privada maestra del segundo nodo ( $V_{1S}$ ) y el Valor de Generador (GV). El método 400 incluye determinar 480 el secreto común (CS) con base en la segunda clave privada del segundo nodo ( $V_{2S}$ ) y la segunda clave pública del primer nodo ( $P_{2C}$ ).  
30

La red de comunicaciones 5 puede incluir una red de área local, una red de área  
35 ancha, redes celulares, red de radio comunicación, el Internet, etc. Estas redes, en donde pueden

transmitirse datos a través del medio de comunicaciones tal como cable eléctrico, fibra óptica, o inalámbricamente pueden ser susceptibles a interceptación, tal como por un espía 11. El método 300, 400 puede permitir que el primer nodo 3 y segundos nodos 7 ambos determinen independientemente un secreto común sin transmitir el secreto común sobre la red de comunicaciones 5.

De esa forma, una ventaja es que el secreto común (CS) pueda determinarse de manera segura e independiente por cada nodo sin tener que transmitir una clave privada sobre una red de comunicaciones potencialmente insegura 5. A su vez, el secreto común puede utilizarse como una clave secreta (o como la base de una clave secreta) para comunicación encriptada entre el primer y segundo nodos 3, 7 sobre la red de comunicaciones 5.

Los métodos 300, 400 pueden incluir pasos adicionales. El método 300 puede incluir, en el primer nodo 3, generar un mensaje firmado (SM1) con base en el mensaje (M) y la segunda clave privada del primer nodo ( $V_{2c}$ ). El método 300 además incluye enviar 360 el primer mensaje firmado (SM1) sobre la red de comunicaciones, al segundo nodo 7. A su vez, el segundo nodo 7 puede realizar los pasos de recibir 440 el primer mensaje firmado (SM1). El método 400 también incluye el paso de validar 450 el primer mensaje firmado (SM2) con la segunda clave pública del primer nodo ( $P_{2c}$ ) y autenticar 460 el primer nodo 3 con base en el resultado de validar el primer mensaje firmado (SM1). Ventajosamente, esto permite que el segundo nodo 7 autentique que el supuesto primer nodo (en donde se generó el primer mensaje firmado) sea el primer nodo 3. Esto se basa en la suposición que únicamente el primer nodo 3 tiene acceso a la clave privada maestra del primer nodo ( $V_{1c}$ ) y por lo tanto únicamente el primer nodo 3 puede determinar la segunda clave privada del primer nodo ( $V_{2c}$ ) para generar el primer mensaje firmado (SM1). Se apreciará que similarmente, 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 pueda autenticar el segundo nodo 7, tal como en un escenario entre pares.

Compartir el mensaje (M) entre el primer y segundo nodos puede lograrse en una variedad de formas. En un ejemplo, el mensaje puede generarse en el primer nodo 3 que entonces se envía, sobre la red de comunicaciones 5, al segundo nodo 7. Alternativamente, el mensaje puede generarse en el segundo nodo 7 y entonces enviarse, sobre la red de comunicaciones 5, al segundo nodo 7. Incluso en otro ejemplo, el mensaje puede generarse en un tercer nodo 9 y el mensaje enviarse tanto al primer como al segundo nodos 3, 7. Incluso en otra alternativa, un usuario puede ingresar el mensaje a través de una interfaz de usuario 15 para recibirse por el primer y segundo nodos 3, 7. Incluso en otro ejemplo, el mensaje (M) puede recuperarse de un almacenamiento de datos 19 y enviarse al primer y segundo nodos 3, 7. En algunos ejemplos, el mensaje (M) puede ser público y por lo tanto puede transmitirse sobre una red insegura 5.

En ejemplos adicionales, uno o más mensajes (M) pueden almacenarse en un almacenamiento de datos 13, 17, 19, en donde el mensaje puede estar asociado con alguna entidad tal como una billetera digital, o una sesión de comunicación establecida entre el primer nodo 3 y el segundo nodo 7. De esa forma, los mensajes (M) pueden recuperarse y utilizarse para recrear, en el primer y segundo nodos respectivos 3, 7, el secreto común (CS) asociado con esa billetera o sesión.

Ventajosamente, un registro para permitir recreación del secreto común (CS) puede mantenerse sin el registro por sí mismo que ha sido almacenado de manera privada o transmitido de manera segura. Esto puede ser ventajoso si se realizan numerosas transacciones en el primer y segundo nodos 3, 7 y sería impráctico almacenar todos los mensajes (M) en los mismos nodos.

#### 10 Método de registro 100, 200

Un ejemplo de un método de registro 100, 200 se describirá con referencia a la Figura 3, en donde el método 100 se realiza por el primer nodo 3 y el método 200 se realiza por el segundo nodo 7. Esto incluye establecer el primer y segundo pares de criptografía asimétrica para el primer y segundo nodos respectivos 3, 7.

15 Los pares de criptografía asimétrica incluyen claves privadas y públicas asociadas, tal como aquellas utilizadas en encriptación de clave pública. En este ejemplo, los pares de criptografía asimétrica se generan al utilizar Criptografía de Curva Elíptica (SC) y propiedades de operaciones de curva elíptica.

Estándares para SC pueden incluir estándares conocidos tal como aquellos descritos por los Estándares para Grupo de Criptografía Eficiente ([www.sceg.org](http://www.sceg.org)). La criptografía de curva elíptica también se describe en 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, US 6,792,530.

En el método 100, 200, esto incluye el primer y segundo nodos que acuerdan 110, 210 un sistema SC común y que utilizan un punto base (G). (Observar: el punto base podría denominarse como un Generador Común, pero el término 'punto base' se utiliza para evitar confusión con el Valor de Generador GV). En un ejemplo, el sistema SC común se puede basar en secp256K1 que es un sistema SC utilizado por Bitcoin. El punto base (G) puede seleccionarse, generarse aleatoriamente, o asignarse.

30 Al cambiar ahora al primer nodo 3, el método 100 incluye establecer 110 en el sistema SC común y punto base (G). Esto puede incluir recibir el sistema SC común y punto base desde el segundo nodo 7, o un tercer nodo 9. Alternativamente, una interfaz de usuario 15 puede estar asociada con el primer nodo 3, por lo cual un usuario puede proporcionar selectivamente el sistema SC común y/o punto base (G). Incluso en otra alternativa, uno o ambos del sistema SC 35 común y/o punto base (G) pueden seleccionarse aleatoriamente por el primer nodo 3. El primer

nodo 3 puede enviar, sobre la red de comunicaciones 5, una notificación indicativa de utilizar el sistema SC común con un punto base (G) al segundo nodo 7. A su vez, el segundo nodo 7 puede establecer 210 al enviar una notificación indicativa de un conocimiento para utilizar el sistema SC común y punto base (G).

- 5 El método 100 también incluye el primer nodo 3 que genera 120 un primer par de criptografía asimétrica que incluye la clave privada maestra del primer nodo ( $V_{1C}$ ) y la clave pública maestra del primer nodo ( $P_{1C}$ ). Esto incluye generar la primera clave privada maestra ( $V_{1C}$ ) con base, al menos en parte, en un número entero aleatorio en un intervalo permisible especificado en el sistema SC común. Esto también incluye determinar la clave pública maestra del primer nodo ( $P_{1C}$ ) con base en multiplicación de punto de curva elíptica de la clave privada maestra del primer nodo ( $P_{1C}$ ) y el punto base (G) de conformidad con la fórmula:

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

De esa forma, el primer par de criptografía asimétrica incluye:

- 15  $V_{1C}$ : La clave privada maestra del primer nodo que se mantiene secreta por el primer nodo.

$P_{1C}$ : La clave pública maestra del primer nodo que se hace públicamente conocida.

- El primer nodo 3 puede almacenar la clave privada maestra del primer nodo ( $V_{1C}$ ) y la clave pública maestra del primer nodo ( $P_{1C}$ ) en un primer almacenamiento de datos 13 asociado con el primer nodo 3. Para seguridad, la clave privada maestra del primer nodo ( $V_{1C}$ ) puede almacenarse en una porción segura del primer almacenamiento de datos 13 para asegurar que la clave permanece privada.

- 20 El método 100 además incluye enviar 130 la clave pública maestra del primer nodo ( $P_{1C}$ ), sobre la red de comunicaciones 5, al segundo nodo 7. El segundo nodo 7 puede, al recibir 220 la clave pública maestra del primer nodo ( $P_{1C}$ ), almacenar 230 la clave pública maestra del primer nodo ( $P_{1C}$ ) en un segundo almacenamiento de datos 17 asociado con el segundo nodo 7.

- 25 Similar al primer nodo 3, el método 200 del segundo 7 incluye generar 240 un segundo par de criptografía asimétrica que incluye la clave privada maestra del segundo nodo ( $V_{1S}$ ) y la clave pública maestra del segundo nodo ( $P_{1S}$ ). La clave privada maestra del segundo nodo ( $V_{1S}$ ) también es un número entero aleatorio dentro del intervalo permisible. A su vez, la clave pública maestra del segundo nodo ( $P_{1S}$ ) se determina por la siguiente fórmula:

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

De esa forma, el segundo par de criptografía asimétrica incluye:

- 30  $V_{1S}$ : La clave privada maestra del segundo nodo que se mantiene secreta por el segundo nodo.

- 35  $P_{1S}$ : La clave pública maestra del segundo nodo que se hace públicamente conocida.

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

5 Se apreciará que, en algunas alternativas, las claves maestras públicas respectivas pueden recibirse y almacenarse en un tercer almacenamiento de datos 19 asociado con el tercer nodo 9 (tal como una tercera parte confiada). Esto puede incluir una tercera parte que actúa como un directorio público, tal como una autoridad de certificación. De esa forma, en algunos ejemplos, la clave pública maestra del primer nodo ( $P_{1C}$ ) puede solicitarse y recibirse por el segundo nodo 7  
10 únicamente cuando determina que se requiere el secreto común (CS) (y viceversa).

Los pasos de registro pueden necesitar ocurrir solamente una vez como un arranque inicial de, por ejemplo, la billetera digital.

#### Inicio de sesión y determinar el secreto común por el tercer nodo 3

Un ejemplo para determinar un secreto común (CS) se describirá ahora con  
15 referencia a la Figura 4. El secreto común (CS) puede utilizarse para una sesión, tiempo, transacción particular u otro propósito entre el primer nodo 3 y el segundo nodo 7 y puede no ser deseable, o seguro, para utilizar el mismo secreto común (CS). De esa forma, el secreto común (CS) puede cambiar entre diferentes sesiones, tiempo, transacciones, etc.

Lo siguiente se proporciona para ilustración de la técnica de transmisión segura que  
20 ha sido descrita anteriormente.

#### Generar un mensaje (M) 310

En este ejemplo, el método 300 realizado por el primer nodo 3 incluye generar 310 un mensaje (M). El mensaje (M) puede ser aleatorio, pseudo aleatorio, o definido por usuario. En un ejemplo, el mensaje (M) se basa en tiempo Unix y un código generado al azar (y valor arbitrario).  
25 Por ejemplo, el mensaje (M) puede proporcionarse como:

$$\text{Mensaje (M)} = \text{Tiempo Unix} + \text{código generado al azar} \quad (\text{Ecuación 3})$$

En algunos ejemplos, el mensaje (M) es arbitrario. Sin embargo, se apreciará que el mensaje (M) puede tener valores selectivos (tal como Tiempo Unix, etc.) que puede ser útil en algunas aplicaciones.

30 El método 300 incluye enviar 315 el mensaje (M) sobre la red de comunicaciones 3, al segundo nodo 7. El mensaje (M) puede enviarse sobre una red insegura ya que el mensaje (M) no incluye información sobre las claves privadas.

#### Determinar un Valor de Generador (GV) 320

El método 300 además incluye el paso de determinar 320 un Valor de Generador  
35 (GV) con base en el mensaje (M). En este ejemplo, esto incluye determinar una función hash

criptográfica del mensaje. Un ejemplo de un algoritmo de función hash criptográfico incluye SHA-256 para crear un Valor de Generador (GV) de 256 bits. Es decir:

$$GV = \text{SHA} - 256(M) \quad (\text{Ecuación 4})$$

Se apreciará que pueden utilizarse otros algoritmos de función hash. Esto puede  
 5 incluir otro que tiene algoritmos en la familia de Algoritmos de Función Hash Segura (SHA, por sus siglas en inglés). Algunos ejemplos particulares incluyen casos en el subconjunto SHA-3, que incluyen SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256. Otros algoritmos de función hash pueden incluir aquellos en la familia de Compendio de Mensaje de Evaluación de Primitivos de Integridad de RACE (RIPEMD, por sus siglas en inglés). Un ejemplo particular puede  
 10 incluir RIPEMD-160. Otras funciones hash pueden incluir familias con base en función hash Zémor-Tillich y funciones hash con base mochila.

*Determinar una segunda clave privada de un primer nodo 330*

El método 300 entonces incluye el paso 330 de determinar 330 la segunda clave privada del primer nodo ( $V_{2C}$ ) con base en la clave privada del segundo nodo ( $V_{1C}$ ) y el Valor de Generador (GV). Esto se puede basar en una suma escalar de la clave privada maestra del primer  
 15 nodo ( $V_{1C}$ ) y el Valor de Generador (GV) de conformidad con la siguiente fórmula:

$$V_{2C} = V_{1C} + GV \quad (\text{Ecuación 5})$$

De esa forma, la segunda clave privada del primer nodo ( $V_{2C}$ ) es un valor aleatorio pero su vez se deriva de manera determinística de la clave privada maestra del primer nodo. La  
 20 clave pública correspondiente en el par criptográfico, principalmente la segunda clave pública del primer nodo ( $P_{2C}$ ), tiene la siguiente relación:

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

Sustitución de  $V_{2C}$  de la Ecuación 5 en la Ecuación 6 proporciona:

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

25 en donde el operador '+' se refiere a suma de punto de curva elíptica. Observar que el álgebra de criptografía de curva elíptica se puede distribuir, Ecuación 7 puede expresarse como:

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

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

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

$$30 \quad P_{2C} = P_{1C} + \text{SHA-256}(M) \times G \quad (\text{Ecuación 9.2})$$

De esa forma, la segunda clave pública del primer nodo ( $P_{2C}$ ) correspondiente se puede derivar dado el conocimiento de la clave pública maestra del primer nodo ( $P_{1C}$ ) y el mensaje (M). El segundo nodo 7 puede tener tal conocimiento para determinar independientemente la segunda clave pública del primer nodo ( $P_{2C}$ ) como se discutirá en detalle adicional a continuación con  
 35 respecto al método 400.

Generar un primer mensaje firmado (SM1) con base en el mensaje y la segunda clave privada del primer nodo 350

El método 300 además incluye generar 350 un primer mensaje firmado (SM1) con base en el mensaje (M) y la segunda clave privada del primer nodo determinada ( $V_{2C}$ ). Generar un  
5 mensaje firmado que incluye aplicar un algoritmo de firma digital para firmar digitalmente el mensaje (M). En un ejemplo, esto incluye aplicar la segunda clave privada del 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 aquellos con base en sistemas SC con secp256k1, secp256r1, secp384r1, secp521r1.  
10

El primer mensaje firmado (SM1) puede verificarse con la segunda clave pública del primer nodo ( $P_{2C}$ ) correspondiente en el segundo nodo 7. Esta verificación del primer mensaje firmado (SM1) puede utilizarse por el segundo nodo 7 para autenticar el primer nodo 3, que se discutirá en el método 400 a continuación.

15 Determinar una segunda clave pública del segundo nodo 370'

El primer nodo 3 entonces puede determinar 370 una segunda clave pública del segundo nodo ( $P_{2S}$ ). Como se discutió anteriormente, la segunda clave pública del segundo nodo ( $P_{2S}$ ) se puede basar al menos en la clave pública maestra del segundo nodo ( $P_{1S}$ ) y el Valor de Generador (GV). En este ejemplo, ya que la clave pública se determina 370' como la clave privada  
20 con multiplicación de punto de curva elíptico con el punto base (G), la segunda clave pública del segundo nodo ( $P_{2S}$ ) puede expresarse, en una forma similar a la Ecuación 6, como:

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

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

La prueba matemática para la Ecuación 10.2 es la misma como se describió  
25 anteriormente para derivar la Ecuación 9.1 para la segunda clave pública del primer nodo ( $P_{2C}$ ). Se apreciará que el primer nodo 3 puede determinar 370 la segunda clave pública del segundo nodo independientemente del segundo nodo 7.

Determinar el secreto común 380 en el primer nodo 3

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

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

Método 400 realizado en el segundo nodo 7

35 El método 400 correspondiente realizado en el segundo nodo 7 se describirá ahora.

Se apreciará que algunos de estos pasos son similares a aquellos discutidos anteriormente que fueron realizados por el primer nodo 3.

El método 400 incluye recibir 410 el mensaje (M) sobre la red de comunicaciones 5, desde el primer nodo 3. Esto puede incluir el mensaje (M) enviado por el primer nodo 3 en el paso 315. El segundo nodo 7 entonces determina 420 a un Valor de Generador (GV) con base en el mensaje (M). El paso de determinar 420 el Valor de Generador (GV) por el segundo nodo 7 es similar al paso 320 realizado por el primer nodo descrito anteriormente. En este ejemplo, el segundo nodo 7 realiza este paso de determinación 420 independiente del primer nodo 3.

El siguiente paso incluye determinar 430 una segunda clave pública del primer nodo ( $P_{2C}$ ) con base en la clave pública maestra del primer nodo ( $P_{1C}$ ) y el Valor de Generador (GV). En este ejemplo, ya que la clave pública se determina 430' como la clave privada con multiplicación de punto de curva elíptica con el punto base (G), la segunda clave pública del primer nodo ( $P_{2C}$ ) puede expresarse, en una forma similar a la Ecuación 9, como:

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

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

La prueba matemática para las Ecuaciones 12.1 y 12.2 es la misma que aquellas discutidas anteriormente para Ecuaciones 10.1 y 10.2.

### El segundo nodo 7 que autentifica el primer nodo 3

El método 400 puede incluir pasos realizados por el segundo nodo 7 para autenticar que el supuesto primer nodo 3, es el primer nodo 3. Como se discutió previamente, esto incluye recibir 440 el primer mensaje firmado (SM1) del primer nodo 3. El segundo nodo 7 entonces puede validar 450 la firma sobre el primer mensaje firmado (SM1) con la segunda clave pública del primer nodo ( $P_{2C}$ ) que se determinó en el paso 430.

Verificar la firma digital puede hacerse de conformidad con un Algoritmo de firma digital de curva elíptica (ECDSA) como se discutió anteriormente. De forma importante, el primer mensaje firmado (SM1) que se firmó con la segunda clave privada del primer nodo ( $V_{2C}$ ) únicamente debe verificarse de forma correcta con la segunda clave pública del primer nodo ( $P_{2C}$ ) correspondiente, ya que  $V_{2C}$  y  $P_{2C}$  forman un par criptográfico. Ya que estas claves son deterministas en la clave privada maestra del primer nodo ( $V_{1C}$ ) y la clave pública maestra del primer nodo ( $P_{1C}$ ) que se generaron en el registro del primer nodo 3, verificar el primer mensaje firmado (SM1) que puede utilizarse como una base para autenticar que un supuesto primer nodo que envía el primer mensaje firmado (SM1) es el mismo primer nodo 3 durante registro. De esa forma, el segundo nodo 7 además puede realizar el paso de autenticar (460) el primer nodo 3 con base en el resultado de validar (450) el primer mensaje firmado.

La autenticación anterior puede ser adecuada para escenarios en donde uno de los

dos nodos es un nodo confiado y únicamente uno de los nodos necesita autenticarse. Por ejemplo, el primer nodo 3 puede ser un cliente y el segundo nodo 7 puede ser un servidor confiado por el cliente tal como un proveedor de billetera. De esa forma, el servidor (segundo nodo 7) puede necesitar autenticar las credenciales del cliente (primer nodo 3) con el fin de permitir que el cliente  
 5 acceda al sistema de servidor. Puede no ser necesario que el servidor autentique las credenciales del servidor para el cliente. Sin embargo, en algunos escenarios, puede ser deseable que ambos nodos sean autenticados entre sí, tal como en un escenario entre pares.

El segundo nodo 7 que determina el secreto común

El método 400 además puede incluir el segundo nodo 7 que determina 470 una  
 10 segunda clave privada del segundo nodo ( $V_{2S}$ ) con base en la clave privada maestra del segundo nodo ( $V_{1S}$ ) y el Valor de Generador (GV). Similar al paso 330 realizado por el primer nodo 3, la segunda clave privada del segundo nodo ( $V_{2S}$ ) se puede basar en una suma escalar de la clave privada maestra del segundo nodo ( $V_{1S}$ ) el Valor de Generador (GV) de conformidad con las siguientes fórmulas:

15 
$$V_{2S} = V_{1S} + GV \quad \text{(Ecuación 13.1)}$$

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

El segundo nodo 7 entonces puede, independiente del primer nodo 3, determinar  
 480 el secreto común (CS) con base en la segunda clave privada del segundo nodo ( $V_{2S}$ ) y la segunda clave pública del primer nodo ( $P_{2C}$ ) con base en la siguiente fórmula:

20 
$$S = V_{2S} \times P_{2C} \quad \text{(Ecuación 14)}$$

Prueba del secreto común (CS) determinado por el primer nodo 3 y 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. Se describirá ahora la prueba matemática que la Ecuación 11 y Ecuación 14 proporcionan el mismo secreto común (CS).

25 Al cambiar al secreto común (CS) determinado por el primer nodo 3, la Ecuación 10.1 puede sustituirse en la Ecuación 11 como a continuación:

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

$$S = V_{2C} \times (V_{2S} \times G)$$

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

30 Al cambiar al secreto común (CS) determinado por el segundo nodo 7, la Ecuación 12.1 puede sustituirse en la Ecuación 14 como a continuación:

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

$$S = V_{2S} \times (V_{2C} \times G)$$

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

35 Ya que el álgebra ECC es conmutativa, la Ecuación 15 y Ecuación 16 son

equivalentes, ya 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 clave secreta

El secreto común (CS) puede utilizarse ahora como una clave secreta, o como la base de una clave secreta en un algoritmo de clave simétrica para comunicación segura entre el primer nodo 3 y segundo nodo 7. Esta comunicación puede utilizarse para transmitir parte de una clave privada, una representación de o identificador para una clave privada, o mnemotécnico para una clave privada. Por lo tanto, una vez que se ha utilizado la invención durante el arranque de, por ejemplo, una billetera digital u otro recurso controlado, comunicación segura entre las partes puede realizarse en lo sucesivo.

El secreto común (CS) puede estar en la forma de un punto de curva elíptica ( $x_s, y_s$ ). Esto puede convertirse en un formato de clave estándar que utiliza operaciones estándares públicamente conocidas acordadas por los nodos 3, 7. Por ejemplo, el valor  $x_s$  puede ser un número entero de 256 bits que podría utilizarse como una clave para encriptación AES<sub>256</sub>. Por lo tanto, podría convertirse en un número entero de 160 bits que utiliza RIPEMND160 para cualquier aplicación que requiera esta longitud de clave.

El secreto común (CS) puede determinarse como se requiera. De forma importante, el primer nodo 3 no necesita almacenar el secreto común (ES) ya que éste puede volverse a determinar con base en el mensaje (M). En algunos ejemplos, el(los) mensaje(s) (M) utilizado(s) puede(n) almacenarse en el almacenamiento de datos 13, 17, 19 (u otro almacenamiento de datos) sin el mismo nivel de seguridad como se requiere para las claves privadas maestras. En algunos ejemplos, el mensaje (M) puede estar públicamente disponible. Sin embargo, dependiendo de alguna aplicación, el secreto común (CS) podría almacenarse en el primer almacenamiento de datos (x) asociado con el primer nodo proporcionado por el secreto común (CS) que se mantiene tan seguro como la clave privada maestra del primer nodo ( $V_{1C}$ ).

Se debe observar que las modalidades mencionadas anteriormente ilustran más bien limitar la invención, y que aquellos expertos en la técnica serán capaces de diseñar muchas modalidades alternativas sin apartarse del alcance de la invención como se define por las reivindicaciones anexas. En las reivindicaciones, cualquier signo de referencia colocado entre paréntesis no debe interpretarse como limitando las reivindicaciones. La palabra "que comprende" y "comprende", y similares, no excluye la presencia de elementos o pasos diferentes de aquellos enlistados en cualquier reivindicación o la especificación como un todo. En la presente especificación, "comprende" significa "incluye o consiste de" y "que comprende" significa "que incluye o que consiste de". La referencia singular de un elemento no excluye la referencia plural de tales elementos y viceversa. La invención puede implementarse por medio de hardware que comprende

- varios elementos distintos, o por medio de una computadora adecuadamente programada. En una reivindicación de dispositivo que enumera varios medios, varios de estos medios pueden representarse por uno y el mismo artículo de hardware. El simple hecho que ciertas medidas se mencionen en reivindicaciones dependientes mutuamente diferentes no indica que una combinación
- 5 de estas medidas no pueda utilizarse para tomar ventaja.