

## **REIVINDICACIONES**

1. Un método implementado por computadora para controlar acceso a un recurso, el método comprende los pasos: dividir un elemento de verificación en una pluralidad de acciones; determinar un secreto común en dos o más nodos en una red; utilizar el secreto común para transmitir al menos una acción del elemento de verificación entre los dos o más nodos.

2. El método de conformidad con la reivindicación 1, caracterizado además porque el elemento de verificación es una clave criptográfica, una representación de una clave criptográfica, o algún elemento que puede utilizarse para acceder, calcular o recuperar la clave criptográfica.

3. El método de conformidad con la reivindicación 1 ó 2, y caracterizado además porque comprende adicionalmente el paso de utilizar el secreto común para generar una clave de encriptación, preferiblemente en donde la clave de encriptación se utiliza para encriptar la por lo menos una acción del elemento de verificación o un mensaje que comprende o que se relaciona con dicha al menos una acción.

4. El método de conformidad con cualquier reivindicación anterior y caracterizado además porque comprende adicionalmente el paso de: almacenar al menos tres acciones del elemento de verificación en diferentes ubicaciones con relación una a la otra; preferiblemente en donde al menos una de las tres acciones se almacena en o sobre una instalación de respaldo o almacenamiento seguro que está separada, independiente y/o distinta de las por lo menos dos otras ubicaciones.

5. El método de conformidad con cualquier reivindicación anterior, caracterizado además porque el recurso es una billetera digital u otro recurso que se relaciona con alguna forma de divisa.

6. El método de conformidad con cualquier reivindicación anterior, caracterizado además porque el elemento de verificación está dividido en una pluralidad de acciones de manera que el elemento de verificación pueda restaurarse o regenerarse de dos o más de las acciones; preferiblemente en donde el elemento de verificación está dividido en una pluralidad de acciones que utilizan el Esquema de distribución de secreto de Shamir.

7. El método de conformidad con cualquier reivindicación anterior, caracterizado además porque el secreto común es: i) determinado en los por lo menos dos nodos independientemente entre sí, de manera que el secreto común no requiera transmisión sobre un canal de comunicaciones entre los nodos; y/o ii) compartido únicamente por los al menos dos nodos.

8. El método de conformidad con cualquier reivindicación anterior y caracterizado además porque comprende el paso de configurar, crear o registrar una billetera digital, en donde el elemento de verificación está asociado con la billetera digital.

9. El método de conformidad con cualquier reivindicación anterior, caracterizado además porque el secreto común se determina por los nodos primero (C) y segundo (S) en la red, 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 además comprende los pasos: - determinar una

segunda clave privada del primer nodo ( $V_{2C}$ ) con base en al menos 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 en al menos 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).

10. El método de conformidad con la reivindicación 9, caracterizado además porque el Valor de Generador (GV) se basa en un mensaje (M).

11. El método de conformidad con la reivindicación 10 y caracterizado además porque comprende adicionalmente los pasos de - 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) puede validarse con una segunda clave pública del primer nodo ( $P_{2C}$ ) para autenticar el primer nodo (C).

12. El método de conformidad con cualquiera de las reivindicaciones 10 u 11 y caracterizado además porque comprende adicionalmente: - 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 ( $P_{2S}$ ); 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 ( $V_{2S}$ ).

13. El método de conformidad con cualquiera de las reivindicaciones 9 a 12 y caracterizado además porque comprende adicionalmente: - generar un mensaje (M); y - enviar, sobre una red de comunicaciones, el mensaje (M) al segundo nodo (S).

14. El método de conformidad con cualquiera de las reivindicaciones 10 a 13, caracterizado además porque comprende adicionalmente: - recibir el mensaje (M), sobre la red de comunicaciones, desde el segundo nodo (S).

15. El método de conformidad con cualquiera de las reivindicaciones 10 a 14 y caracterizado además porque comprende adicionalmente: - recibir el mensaje (M), sobre la red de comunicaciones, desde otro nodo.

16. El método de conformidad con cualquiera de las reivindicaciones 9 a 15, caracterizado además porque la clave pública maestra del primer nodo ( $P_{1C}$ ), clave pública maestra del segundo nodo ( $P_{1S}$ ) se basan en multiplicación de punto de curva elíptica de la clave privada maestra primer nodo ( $V_{1C}$ ) respectivas y clave maestra privada del segundo nodo ( $V_{1S}$ ) y un punto base (G).

17. El método de conformidad con cualquiera de las reivindicaciones 9 a 16 y caracterizado además porque comprende adicionalmente 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 ( $P_{1S}$ ).

18. El método de conformidad con cualquiera de las reivindicaciones 9 a 17 y caracterizado además porque comprende adicionalmente las etapas 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 ( $V_{1C}$ ).

19. El método de conformidad con cualquiera de las reivindicaciones 9 a 18, caracterizado además porque el Valor de Generador (GV) se basa en determinar una función hash de un Valor de Generador (GV) previo.

20. El método de conformidad con cualquiera de las reivindicaciones 9 a 19, caracterizado además porque el primer par de criptografía asimétrica y el segundo par de criptografía asimétrica se basan en una función del primer par de criptografía asimétrica previo respectivo y segundo par de criptografía asimétrica previo.

21. Un sistema a base de computadora dispuesto para realizar los pasos de cualquier reivindicación anterior.

22. El sistema de conformidad con la reivindicación 21, caracterizado además porque: el recurso es una billetera digital u otro recurso que se relaciona con alguna forma de divisa.

23. El sistema de conformidad con la reivindicación 20 a 22, caracterizado además porque el sistema comprende software dispuesto para permitir la configuración, creación o registro de una billetera digital, en donde el elemento de verificación está asociado con la billetera digital.

24. Un sistema implementado por computadora dispuesto para controlar acceso a una billetera digital, el sistema es operativo para: 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 al menos en 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 en al menos la clave maestra de primera/segunda entidad y el valor de generador.

25. Un método para controlar acceso a una billetera digital, el método comprende los pasos de: 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 al menos en 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.