

REIVINDICACIONES

1. Un sistema para realizar una transacción, que comprende:

un dispositivo de almacenamiento, el dispositivo de almacenamiento tiene un circuito integrado que
5 comprende al menos un primer elemento seguro, el primer elemento seguro tiene un procesador, una memoria digital y una primera interfaz de comunicaciones de campo cercano (NFC), el módulo de memoria digital del primer elemento seguro contiene instrucciones legibles por procesador del primer elemento seguro para provocar que el primer elemento seguro almacene una clave pública y una clave privada en estados cifrados en la memoria digital, genere una clave pública utilizando la clave privada y realice operaciones de
10 firma y *hash*;

un dispositivo de procesamiento que tiene una interfaz de usuario, una segunda interfaz NFC y una interfaz de comunicación configurada para conectarse a una red de comunicaciones global, el dispositivo de procesamiento tiene una memoria digital y un procesador, la memoria digital del dispositivo de procesamiento programada con instrucciones legibles por procesador del dispositivo de procesamiento para
15 provocar que el dispositivo de procesamiento establezca una conexión a través de NFC con la interfaz NFC del primer elemento seguro, para enviar información al primer elemento seguro para su procesamiento por el primer elemento seguro, y para establecer una interfaz de usuario operable para acceder a una red de transacciones a través de la red de comunicaciones global;

en donde las instrucciones legibles por procesador del dispositivo de almacenamiento y el
20 procesador del dispositivo de procesamiento, cuando son leídas por los respectivos procesadores, son capaces de hacer que el sistema realice los pasos de:

(a) el dispositivo de procesamiento recibe el inicio de una transacción a través de la interfaz de usuario;

(b) el dispositivo de procesamiento establece la conexión con el primer elemento seguro a través
25 de NFC;

(c) el dispositivo de procesamiento envía información al primer elemento seguro para su procesamiento a través del enlace NFC;

(d) el primer elemento seguro recupera la clave privada, realiza operaciones hash utilizando la clave privada para definir una firma, comprueba una cadena asociada a la clave pública para confirmar que
30 la firma se ajusta a una firma de clave pública que solo podría haberse generado utilizando la clave privada específica, firma la transacción y envía la información de transacción firmada al dispositivo de procesamiento;

(e) el dispositivo de procesamiento establece una sesión de comunicación a través de la red global de comunicaciones con un servidor de intercambio de la red de transacciones y envía la información
35 de transacción firmada al servidor de intercambio para iniciar la transacción.

2. El sistema de conformidad con la reivindicación 1, en donde la transacción comprende una transacción de criptomonedas correspondiente a un valor monetario o *token*, el dispositivo de almacenamiento comprende un dispositivo de almacenamiento en frío de criptomonedas, el primer módulo de memoria digital de elemento seguro comprende un módulo criptográfico, y la interfaz de usuario comprende una cartera virtual de criptomonedas.

3. El sistema de conformidad con la reivindicación 2, en donde la cartera virtual de criptomonedas está configurada para acceder a la red de transacciones indirectamente a través del acceso directo a una red de criptomonedas de segunda capa.

4. El sistema de conformidad con las reivindicaciones 2 o 3, en donde el sistema está configurado además para recibir un depósito de criptomonedas, en donde el dispositivo de procesamiento está configurado para mostrar una dirección de criptomonedas asociada a la cartera de criptomonedas en una forma codificada para proporcionar a un pagador.

5. El sistema de conformidad con cualquiera de las reivindicaciones 2 a 4, en donde el sistema está configurado además para comprar o intercambiar criptomonedas.

6. El sistema de conformidad con las reivindicaciones 2 a 5, en donde el primer elemento seguro también comprende un módulo de pago configurado para intercambiar información de pago con un lector de tarjetas para realizar una transacción de compra.

7. El sistema de conformidad con la reivindicación 6, en donde el módulo de pago está aislado del módulo de criptomonedas en el primer elemento seguro del dispositivo de almacenamiento en frío, que comprende un único elemento seguro en el dispositivo de almacenamiento en frío.

8. El sistema de conformidad con las reivindicaciones 2-5, en donde el dispositivo de almacenamiento en frío incluye un segundo elemento seguro que comprende un módulo de pago configurado para intercambiar información de pago con un lector de tarjetas para realizar una transacción de compra.

9. El sistema de conformidad con cualquiera de las reivindicaciones anteriores, en donde el dispositivo de procesamiento comprende un dispositivo móvil.

10. El sistema de conformidad con la reivindicación 9, en donde el dispositivo móvil comprende uno de los siguientes: un teléfono inteligente, una tableta o una computadora portátil.

11. El sistema de conformidad con cualquiera de las reivindicaciones anteriores, en donde el dispositivo de almacenamiento comprende una tarjeta con las dimensiones convencional de una tarjeta de transacción de conformidad con la norma ISO/IEC 7810:2003 ID-1.

12. El sistema de conformidad con la reivindicación 11, en donde la tarjeta comprende metal, cerámica, vidrio o una combinación de los mismos.

13. El sistema de conformidad con la reivindicación 2, en donde el dispositivo de almacenamiento comprende una tarjeta con dimensiones convencionales de una tarjeta de transacción de conformidad con la norma ISO/IEC 7810:2003 ID-1, y la tarjeta no tiene módulo de pago ni banda magnética configurada para interactuar con un lector de tarjetas.

14. El sistema de conformidad con la reivindicación 13, en donde la tarjeta comprende además al menos uno de un módulo de pago y una banda magnética configurada para interactuar con un lector de tarjetas.

15. El sistema de conformidad con cualquiera de las reivindicaciones 1 a 10, en donde el dispositivo de almacenamiento comprende un llavero de metal, cerámica, vidrio o una combinación de los mismos.

16. El sistema de conformidad con cualquiera de las reivindicaciones anteriores, en donde el dispositivo de almacenamiento comprende además un módulo lector biométrico conectado al procesador y configurado para restringir la actividad del dispositivo de almacenamiento con base en la información biométrica detectada por el lector biométrico.

17. El sistema de conformidad con cualquiera de las reivindicaciones anteriores, en donde el dispositivo de procesamiento comprende además un módulo lector biométrico conectado al procesador del dispositivo de procesamiento y configurado para restringir el acceso al dispositivo de almacenamiento desde el dispositivo de procesamiento con base en la información biométrica detectada por el lector biométrico.

18. El sistema de conformidad con cualquiera de las reivindicaciones anteriores, en donde la conexión entre el dispositivo de procesamiento y el primer elemento seguro es un enlace seguro de comunicación NFC.

19. Un dispositivo de almacenamiento, el dispositivo tiene un circuito integrado que comprende al menos un primer elemento seguro, el primer elemento seguro tiene un procesador, una memoria digital, y una interfaz de comunicaciones de campo cercano (NFC), la memoria digital del primer elemento seguro que comprende un módulo que incorpora instrucciones legibles por procesador del primer elemento seguro para provocar que el primer elemento seguro almacene una clave pública y una clave privada en estados cifrados en la memoria digital, generar una clave pública utilizando la clave privada, y realizar operaciones de firma y *hash*, y para provocar que el primer elemento seguro, en respuesta a la recepción de información de alto nivel de un dispositivo móvil vinculado a través de un enlace de comunicaciones con el primer elemento seguro a través de la interfaz NFC, la información de alto nivel relativa a una transacción, realice los pasos de:

recuperar la clave privada, realizar operaciones *hash* utilizando la clave privada para definir una firma, comprobar una cadena asociada a la clave pública para confirmar que la firma se ajusta a una firma de clave pública que solo podría haberse generado utilizando la clave privada específica que firma la transacción, y enviar la información de transacción firmada al dispositivo móvil.

20. El dispositivo de almacenamiento de conformidad con la reivindicación 19, en donde el dispositivo de almacenamiento comprende una tarjeta con dimensiones convencional de una tarjeta de transacción de conformidad con la norma ISO/IEC 7810:2003 ID-1.

5 21. El dispositivo de almacenamiento de conformidad con la reivindicación 20, en donde la tarjeta comprende metal, cerámica, vidrio o una combinación de los mismos.

 22. El dispositivo de almacenamiento de conformidad con cualquiera de las reivindicaciones 17 a 19, en donde el dispositivo de almacenamiento comprende un dispositivo de almacenamiento en frío de criptomonedas, la transacción corresponde a un valor monetario o *token*, y el módulo comprende un módulo
10 criptográfico.

 23. El dispositivo de almacenamiento de conformidad con la reivindicación 22, en donde la tarjeta no tiene módulo de pago ni banda magnética configurada para interactuar con un lector de tarjetas.

 24. El dispositivo de almacenamiento de conformidad con las reivindicaciones 20 a 22, en donde la tarjeta comprende además una banda magnética configurada para interactuar con un lector de tarjetas.

15 25. El dispositivo de almacenamiento de conformidad con las reivindicaciones 19 a 22, en donde la tarjeta comprende además un módulo de pago.

 26. El dispositivo de almacenamiento de conformidad con la reivindicación 25, en donde el módulo de pago está aislado del módulo en el primer elemento seguro del dispositivo de almacenamiento, que comprende un único elemento seguro en el dispositivo de almacenamiento en frío.

20 27. El dispositivo de almacenamiento de conformidad con la reivindicación 25, en donde el dispositivo de almacenamiento incluye un segundo elemento seguro que comprende el módulo de pago configurado para intercambiar información de pago con un lector de tarjetas para realizar una transacción de compra.

 28. El dispositivo de almacenamiento de conformidad con la reivindicación 19, en donde el
25 dispositivo de almacenamiento en frío comprende un llavero de metal, cerámica, vidrio o una combinación de los mismos.

 29. El dispositivo de almacenamiento de conformidad con cualquiera de las reivindicaciones 19 a 28, en donde el dispositivo de almacenamiento comprende además un módulo lector biométrico conectado al procesador y configurado para restringir la actividad del dispositivo de almacenamiento basándose en la
30 información biométrica detectada por el lector biométrico.

 30. El dispositivo de almacenamiento de conformidad con cualquiera de las reivindicaciones 19 a 29, en donde el enlace de comunicaciones es un enlace seguro de comunicaciones.

 31. Un dispositivo de procesamiento que tiene una interfaz de usuario de dispositivo, una interfaz de comunicaciones de campo cercano (NFC), y una interfaz de comunicaciones configurada para la
35 conexión a una red de comunicaciones global, el dispositivo de procesamiento que tiene una memoria digital

y un procesador, la memoria digital del dispositivo de procesamiento programado con instrucciones legibles por procesador del dispositivo de procesamiento para provocar que el dispositivo de procesamiento para establecer una conexión a través de NFC con un elemento seguro de un dispositivo de almacenamiento, para enviar información al elemento seguro para su procesamiento por el elemento seguro, y para establecer una interfaz de usuario de aplicación de transacciones operable para acceder a una red de transacciones a través de la red global de comunicaciones, las instrucciones legibles por procesador del dispositivo de procesamiento configuradas además para provocar que el dispositivo de procesamiento realice los pasos de:

- (a) recibir el inicio de una transacción a través de la interfaz de usuario del dispositivo;
- (b) establecer un enlace de comunicaciones con el elemento seguro a través de NFC;
- (c) enviar información de alto nivel al elemento seguro para su procesamiento a través del enlace NFC;
- (d) recibir del elemento seguro información firmada sobre la transacción;
- (e) establecer una sesión de comunicación a través de la red global de comunicaciones con un servidor de intercambio de la red de transacciones y enviar la información de transacción firmada al servidor de intercambio para iniciar una transacción.

31. El dispositivo de procesamiento de conformidad con la reivindicación 30, en donde el dispositivo de almacenamiento es un dispositivo de almacenamiento en frío de criptomonedas, la interfaz de usuario de la aplicación de transacción comprende una cartera de criptomonedas, la red de transacción es una red de criptomonedas, y la transacción corresponde a un valor de moneda o *token*.

32. El dispositivo de procesamiento de conformidad con la reivindicación 30 o con la reivindicación 31, en donde el dispositivo de procesamiento comprende un dispositivo móvil.

33. El dispositivo de procesamiento de conformidad con la reivindicación 32, en donde el dispositivo móvil comprende un teléfono inteligente.

34. El dispositivo de procesamiento de conformidad con cualquiera de las reivindicaciones 19 a 33, que comprende además un módulo lector biométrico conectado al procesador y configurado para restringir el acceso al dispositivo de almacenamiento desde el dispositivo de procesamiento con base en la información biométrica detectada por el lector biométrico.

35. El dispositivo de procesamiento de conformidad con cualquiera de las reivindicaciones 19 a 34, en donde la conexión a través de NFC con el elemento seguro es una comunicación segura.

36. Un dispositivo de autenticación, el dispositivo tiene un circuito integrado que comprende al menos un primer elemento seguro, el primer elemento seguro tiene un procesador, una memoria digital, y una interfaz de comunicaciones de campo cercano (NFC), la memoria digital del primer elemento seguro que comprende un módulo que incorpora instrucciones legibles por procesador del primer elemento seguro para provocar que el primer elemento seguro almacene un código de autenticación en la memoria digital, y para transmitir la información de autenticación a un dispositivo móvil en respuesta a la recepción de una

comunicación desde el dispositivo móvil vinculado a través de un enlace de comunicaciones con el primer elemento seguro a través de la interfaz NFC, la información relativa a una transacción.

5 37. El dispositivo de autenticación, en donde el dispositivo de autenticación es un dispositivo de autenticación de criptomonedas, el módulo comprende un módulo criptográfico, y la transacción corresponde a un valor monetario o *token*.

38. Un sistema para realizar transacciones, que comprende:

10 un dispositivo de autenticación, el dispositivo de autenticación tiene un circuito integrado que comprende al menos un primer elemento seguro, el primer elemento seguro tiene un procesador, una memoria digital y una primera interfaz de comunicaciones de campo cercano (NFC), la memoria digital del primer elemento seguro comprende un módulo de transacción que incorpora instrucciones legibles por procesador del primer elemento seguro para provocar que el primer elemento seguro almacene un código de autenticación en la memoria digital;

15 un dispositivo de procesamiento que tiene una interfaz de usuario, una segunda interfaz NFC y una interfaz de comunicación configurada para la conexión a una red de comunicaciones global, el dispositivo de procesamiento que tiene una memoria digital y un procesador, la memoria digital del dispositivo de procesamiento programada con instrucciones legibles por procesador del dispositivo de procesamiento para provocar que el dispositivo de procesamiento establezca una conexión a través de NFC con la interfaz NFC
20 del primer elemento seguro, para enviar una comunicación al primer elemento seguro, para establecer una interfaz de usuario de aplicación de transacción operable para acceder a una cuenta de transacción en línea a través de la red de comunicaciones global;

25 la cuenta de transacciones en línea que comprende una clave pública y una clave privada en estados cifrados almacenados en la memoria digital de la cuenta de transacciones e instrucciones legibles por un procesador de la cuenta de transacciones para almacenar y generar una clave pública utilizando la clave privada, realizar operaciones de firma y *hash*, y transmitir información de transacciones firmadas a un servidor de intercambio de transacciones de una red de transacciones;

30 en donde las instrucciones legibles por procesador del dispositivo de autenticación y el procesador del dispositivo de procesamiento, cuando son leídas por los respectivos procesadores, son capaces de hacer que el sistema realice los pasos de:

(a) el dispositivo de procesamiento recibe el inicio de una transacción a través de la interfaz de usuario;

(b) el dispositivo de procesamiento establece la conexión con el primer elemento seguro a través de NFC;

(c) el dispositivo de procesamiento envía una comunicación al primer elemento seguro a través del enlace NFC;

(d) el primer elemento seguro envía el código de autenticación al dispositivo de procesamiento;

5

(e) el dispositivo de procesamiento establece una sesión de comunicación a través de la red global de comunicaciones con la cuenta de transacciones en línea y envía el código de autenticación a la cuenta de transacciones en línea; y

(f) la cuenta de transacciones en línea recupera la clave privada, realiza operaciones *hash* con la clave privada para generar una firma, comprueba una cadena asociada a la clave pública para confirmar que la firma se ajusta a una firma de clave pública que solo podría haberse generado utilizando la clave privada, firma la transacción y envía la información de transacción firmada al servidor de intercambio de transacciones para iniciar una transacción.

39. El sistema de conformidad con la reivindicación 38, en donde el sistema comprende un sistema de transacción de criptomonedas, el dispositivo de autenticación comprende un dispositivo de autenticación de criptomonedas, el módulo comprende un módulo de criptomonedas, la interfaz de usuario de la aplicación de transacción comprende una cartera de criptomonedas, la cuenta de transacción en línea comprende una cuenta de criptomonedas, la red de transacción es una red de criptomonedas, el servidor de intercambio es un servidor de intercambio de criptomonedas, y la transacción comprende una transacción de criptomonedas operativa para enviar un valor de moneda o *token* al servidor de intercambio.

25

30