

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

Esta solicitud se refiere y reivindica los beneficios de prioridad de la Solicitud Provisional de EE. UU. N.º 63/135,157, presentada el 8 de enero de 2021, titulada DISPOSITIVOS, SISTEMAS Y MÉTODOS DE CRIPTOMONEDAS y de la solicitud 63/271,545, presentada el 25 de octubre de 2021, DISPOSITIVOS, SISTEMAS Y MÉTODOS PARA LA AUTENTICACIÓN DE CLAVES PÚBLICAS O PRIVADAS, cuyo contenido se incorpora en el presente documento por referencia en su totalidad a todos los efectos.

ANTECEDENTES DE LA INVENCIÓN

En el ámbito de las criptomonedas (como las bitcoins, etc.), se necesita una clave privada (el código único, normalmente alfanumérico, que permite gastar la moneda) para acceder a la criptomoneda para fines de gasto. Específicamente, una clave pública identifica un destino para la moneda. Una transacción en criptomoneda normalmente necesita que el emisor y el receptor compartan sus direcciones que son las derivaciones de las claves públicas entre sí para completar la transacción, con la cadena de bloques asociada utilizada para certificar la validez de la transacción y para confirmar que el emisor tiene los fondos. Para otros tipos de autenticación (por ejemplo, FIDO o PGP), el emisor y el destinatario comparten sus claves públicas reales. Una vez que el pago ha llegado a la dirección, el receptor necesita la clave privada para acceder a los fondos. Mantener la clave privada segura es por lo tanto crítico, porque un usuario en posesión de la clave privada puede ser capaz de acceder y convertir la criptomoneda del titular sin autorización. Una ilustración de ejemplo de un proceso de derivación de la clave privada a la clave pública a la dirección se puede encontrar en <https://iancoleman.io/bip39/>, incorporado en el presente documento por referencia.

Una clave privada almacenada electrónicamente en un monedero digital conectado a Internet (es decir, un “monedero caliente”) es vulnerable a la piratería informática. Cuando se utiliza un monedero caliente, los pasos del método para realizar una transacción es decir, generar y almacenar claves privadas, así como firmar digitalmente las transacciones utilizando claves privadas suelen realizarse por un único dispositivo en línea, que difunde la transacción firmada a través de la red. Una transacción firmada difundida por la red es vulnerable a estos ataques.

El “almacenamiento en frío” impide los problemas anteriores al firmar la transacción utilizando las claves privadas en un entorno que no está conectado a Internet. Una transacción puede iniciarse en línea, pero luego se transfiere temporalmente a un monedero sin conexión como el almacenamiento electrónico en un USB, CD, disco duro o computadora sin conexión. La transacción se firma de forma digital fuera de línea antes de transmitirse a la red en línea. Dado que la clave privada nunca está presente en una ubicación en línea durante el proceso de firma, incluso si un pirata informático accede a los detalles de la transacción, la clave privada utilizada para realizar la transacción no puede descubrirse.

Aunque se conocen muchos sistemas y métodos para acceder al almacenamiento en frío, tienden a ser más fastidiosos que los sistemas y métodos para utilizar un monedero caliente, por lo que sigue existiendo una necesidad en la técnica de sistemas y métodos de uso de dispositivos de almacenamiento en frío que sean más eficientes.

5

BREVE DESCRIPCIÓN DE LA INVENCION

Un aspecto de la invención se refiere a un sistema para realizar transacciones de criptomonedas. El sistema comprende un dispositivo de almacenamiento en frío de criptomonedas con un circuito integrado que comprende un elemento seguro. El término “elemento seguro”, como se utiliza en el presente documento, se refiere no solo a microcontroladores específicamente diseñados mencionados en el campo o comercializados específicamente como elementos seguros (por ejemplo, para el uso en tarjetas de crédito y similares), sino también a cualquier microcontrolador programado con *software* de seguridad adecuado para realizar las funciones de un elemento seguro como se conoce en la técnica. El elemento seguro tiene un procesador, una memoria digital y una primera interfaz de comunicaciones de campo cercano (NFC, por sus siglas en inglés). La memoria digital del elemento seguro incluye instrucciones legibles por procesador del elemento seguro para provocar que el 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 firma y *hash*. En algunas modalidades, la clave pública puede ser compartida desde el elemento seguro, por conveniencia. El sistema incluye además un dispositivo de procesamiento, por ejemplo, un dispositivo móvil, como un teléfono inteligente, una tableta o una computadora portátil, los cuales tienen 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 programada con instrucciones legibles por procesador para provocar que el dispositivo de procesamiento establezca una conexión segura a través de NFC con la interfaz NFC del elemento seguro, para enviar información al elemento seguro para su procesamiento por el elemento seguro, y para establecer un monedero de criptomonedas operable para acceder a una red de criptomonedas a través de la red de comunicaciones global. Las instrucciones legibles por procesador del dispositivo de almacenamiento en frío y el procesador del dispositivo de procesamiento, cuando son leídas por los respectivos procesadores, son capaces de hacer que el sistema realice pasos predeterminados. Los pasos incluyen que el dispositivo de procesamiento recibe el inicio de una transacción a través de la interfaz de usuario, la transacción corresponde a un valor monetario o *token*. El dispositivo de procesamiento establece un enlace seguro de comunicaciones con el elemento seguro a través de las NFC, y envía información al elemento seguro para su procesamiento a través del enlace NFC. El elemento seguro recupera la clave privada, realiza operaciones *hash* utilizando la clave privada para generar una firma, descifra la clave privada utilizando la clave pública (es decir, comprueba una cadena asociada a la clave

pública para confirmar que la firma se ajusta a la 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. El dispositivo de procesamiento establece una sesión de comunicación a través de la red de comunicaciones global con un servidor de intercambio de criptomonedas de la red de criptomonedas y envía la información de transacción firmada al servidor de intercambio de criptomonedas (por ejemplo, un nodo de la cadena de bloques) para iniciar una transacción operativa para enviar el valor de divisa o *token* al servidor de intercambio. Por ejemplo, una vez que un bloque está firmado y listo para ser añadido a la cadena, el servidor de intercambio se comunica con un nodo para mandar la transacción al *mempool* (es decir, la zona de espera para transacciones no confirmadas).

El sistema puede estar configurado para recibir un depósito de criptomonedas, en donde el dispositivo de procesamiento está configurado para mostrar una dirección de criptomonedas asociada al monedero de criptomonedas de forma codificada para proporcionar a un pagador. El elemento seguro también puede comprender un módulo de pago configurado para intercambiar información de pago con un lector de tarjetas para realizar una transacción de compra. En un sistema con un elemento único seguro, el elemento único puede tener una división que separa el *software* para realizar las funciones de criptomonedas del *software* para realizar las funciones de pago. El *software* puede compartir información entre *applets*, como claves privadas o PIN. Cada aplicación suele estar en su propia “caja segura”. Compartir entre cada caja segura es posible, pero puede ser relativamente complicado. En otras modalidades, un primer elemento seguro puede dedicarse a realizar funciones de criptomonedas y un segundo elemento seguro puede dedicarse a realizar funciones de pago.

En algunas modalidades, el dispositivo de almacenamiento en frío comprende una tarjeta con dimensiones convencionales de una tarjeta de transacción de conformidad con la norma ISO/IEC 7810:2003 ID-1, como una tarjeta que comprende metal, cerámica, vidrio, o una combinación de los mismos. En algunas modalidades, la tarjeta no tiene módulo de pago ni banda magnética configurada para interactuar con un lector de tarjetas, mientras que en otras modalidades la tarjeta puede comprender además al menos uno de los módulos de pago y una banda magnética. En otras modalidades, el dispositivo de almacenamiento en frío puede tener la forma de un llavero de metal, cerámica, vidrio o una combinación de los mismos.

El dispositivo de almacenamiento en frío y/o el dispositivo de procesamiento pueden incluir además un módulo lector biométrico conectado al procesador respectivo y configurado para restringir la actividad o el acceso al dispositivo de almacenamiento en frío con base en la información biométrica detectada por el lector biométrico.

Otro aspecto de la invención se refiere a un dispositivo de almacenamiento en frío de criptomonedas que tiene un circuito integrado que comprende un elemento seguro. El elemento seguro tiene un procesador, una memoria digital y una interfaz de comunicación de campo cercano (NFC), como, entre otros, una interfaz

configurada para la comunicación mediante la norma ISO 14443. La memoria digital del elemento seguro contiene instrucciones programadas legibles por procesador del elemento seguro para provocar que el 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 firma y *hash*. Las instrucciones programadas también hacen que el elemento seguro responda a la recepción de información de alto nivel procedente de un dispositivo móvil vinculado a través de un enlace seguro de comunicaciones con el elemento seguro a través de la interfaz NFC, la información de alto nivel relativa a una transacción correspondiente a un valor monetario o ficha. La respuesta incluye la recuperación de la clave privada, la modalidad de operaciones *hash* utilizando la clave privada para generar una firma, el descifrado de la clave privada utilizando la clave pública (es decir, la comprobación de 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), la firma de la transacción y el envío de la información de transacción firmada al dispositivo móvil.

En algunas modalidades, el dispositivo de almacenamiento en frío comprende una tarjeta con dimensiones convencionales de una tarjeta de transacción de conformidad con la norma ISO/IEC 7810:2003 ID-1, como una tarjeta de metal, cerámica, vidrio, o una combinación de los mismos. La tarjeta puede no tener módulo de pago ni banda magnética configurada para interactuar con un lector de tarjetas, o puede tener al menos un módulo de pago y una banda magnética. En otras modalidades, el dispositivo de almacenamiento en frío comprende un llavero de metal, cerámica, vidrio o una combinación de los mismos. El dispositivo de almacenamiento en frío puede incluir un módulo lector biométrico conectado al procesador y configurado para restringir la actividad del dispositivo de almacenamiento en frío basándose en la información biométrica detectada por el lector biométrico.

Aún otros aspectos de la invención se refieren a un dispositivo de procesamiento, como un dispositivo móvil, como un teléfono inteligente, que tiene una interfaz de usuario, una interfaz de comunicaciones de campo cercano (NFC), y una interfaz de comunicaciones configurada para la conexión a una red de comunicaciones global. El dispositivo de procesamiento tiene una memoria digital y un procesador, la memoria digital programada con instrucciones legibles por procesador del dispositivo de procesamiento para provocar que el dispositivo de procesamiento establezca una conexión segura a través de NFC con un elemento seguro de un dispositivo de almacenamiento en frío de criptomonedas, para enviar información al elemento seguro para ser procesado por el elemento seguro, y para establecer un monedero de criptomonedas operativa para acceder a una red de criptomonedas a través de la red de comunicaciones global. Las instrucciones legibles por procesador del dispositivo de procesamiento están 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, la transacción correspondiente a un valor monetario o *token*;

establecer un enlace seguro 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;

(e) establecer una sesión de comunicación a través de la red de comunicaciones global con un servidor de intercambio de criptomonedas de la red de criptomonedas y enviar la información de transacción firmada al

5 servidor de intercambio de criptomonedas para iniciar una transacción operativa para enviar el valor de divisa o *token* al servidor de intercambio.

BREVE DESCRIPCIÓN DE LAS FIGURAS

10 En la Figura 1 se muestra un sistema de ejemplo para realizar una transacción de criptomonedas de conformidad con aspectos de la invención.

En la Figura 2 se muestra un diagrama de flujo que representa pasos de ejemplo del proceso de conformidad con aspectos de la invención.

DESCRIPCIÓN DETALLADA DE LA INVENCION

15 En la Figura 1 se muestra un sistema de ejemplo (100) para realizar transacciones de criptomonedas de conformidad con aspectos de la invención. Un dispositivo de almacenamiento en frío de criptomoneda (110) se representa en la Figura 1 en la forma de una tarjeta de transacción, como una tarjeta de lujo que comprende metal, cerámica, vidrio, o una combinación de los mismos, con dimensiones convencionales de una tarjeta de transacción de conformidad con la norma ISO/IEC 7810:2003 ID-1, a saber, una longitud y

20 ancho de 85.6 x 53.98 mm (3.4 x 2.1 pulgadas) y un grosor de 0.76 milímetros ($\frac{1}{32}$ in). Sin embargo, a diferencia de una tarjeta de débito o crédito convencional, la tarjeta no necesita (y por tanto carece de este elemento) una banda magnética y contactos físicos asociados a las tarjetas de transacción configuradas para interactuar con un lector de tarjetas. Del mismo modo, no hay necesidad de un número de tarjeta, un nombre de usuario o un bloque de firma en la tarjeta. En otras modalidades, sin embargo, dados los riesgos

25 potenciales de pérdida y la naturaleza de la información almacenada en el dispositivo de almacenamiento en frío, las modalidades con información identificativa del usuario pueden tener ventajas. Por ejemplo, pueden incluirse características como el nombre del usuario (no se muestra, pero se conoce bien en la técnica), la foto del usuario (no se muestra, pero se conoce bien en la técnica), el bloque de firma del usuario (no se muestra, pero se conoce bien en la técnica) y un lector biométrico (12) (por ejemplo, un lector de huellas

30 dactilares o de pulgares para controlar el acceso al dispositivo de almacenamiento en frío). En otras modalidades, las tarjetas pueden estar configuradas para realizar transacciones rutinarias con tarjeta de crédito o débito, y pueden estar configuradas con todos los elementos típicos de una tarjeta de crédito, incluyendo un módulo de pago (10), banda magnética (no mostrada pero bien conocida en la técnica), y similares.

En algunas modalidades, puede ser ventajoso configurar la tarjeta u otro factor de forma (llavero, etc.) para el pago más la autenticación (por ejemplo, utilizando FIDO). Debe entenderse que, en algunas modalidades, la tarjeta/otro factor de forma puede presentar cualquier combinación de criptografía, FIDO, control de acceso/fidelidad y/o pago, dependiendo de la combinación de *software*.

5 Aunque se representa como un dispositivo del tamaño de una tarjeta de transacciones, que ofrece la ventaja de caber perfectamente en la cartera física del titular junto con las tarjetas de transacciones convencionales, la invención no se limita a ningún tamaño o forma en particular. Cualquier factor de forma configurado para las comunicaciones de NFC con un dispositivo móvil, como se describe en el presente documento, puede ser adecuado. Por ejemplo, el dispositivo de almacenamiento en frío puede ser un
10 llavero, una moneda o cualquier tipo de ficha física. Aunque se prefiere una construcción de metal, cerámica, vidrio, o una combinación de los mismos, por su durabilidad, los materiales de construcción no están limitados.

La tarjeta (110) incluye un elemento seguro (112), que comprende un circuito integrado que tiene un procesador (114), una memoria digital (116), y una interfaz de comunicaciones de campo cercano (NFC)
15 (118). La memoria digital (116) del elemento seguro (112) incluye un módulo criptográfico que incorpora instrucciones legibles por procesador (114) del elemento seguro para provocar que el 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 firma y *hash*.

La interfaz NFC puede incluir una o más antenas, incluyendo en algunas modalidades,
20 particularmente modalidades en donde la tarjeta está compuesta de metal, una primera antena integrada dentro de un procesador de circuito integrado (IC, por sus siglas en inglés) que contiene el elemento seguro, y una segunda antena (de refuerzo) que comprende una capa de la tarjeta. En algunas modalidades, una capa metálica de la propia tarjeta puede configurarse como antena. Las configuraciones de tarjetas metálicas con interfaces NFC operables se describen, por ejemplo, pero sin limitarse, en la patente de
25 EE. UU. N.º 10,318,859, titulado TARJETA INTELIGENTE DE METAL DE INTERFAZ DUAL CON ANTENA DE REFUERZO, y la patente de EE. UU. n.º 10,762,412, titulada TARJETA DE METAL INTEGRADA CAPACITIVA DI, ambos se incorporan en el presente documento por referencia. Aunque en lo que antecede se describen en el contexto de módulos de pago que comprenden elementos seguros para comunicarse con lectores de tarjetas, las interfaces NFC descritas en ellos son comparables a las que se utilizan entre las
30 tarjetas y los dispositivos de procesamiento que se examinan en el presente documento.

El dispositivo móvil (120), como un teléfono inteligente, una tableta u otro tipo de computadora, también denominada en el presente documento dispositivo de procesamiento (PD), incluye una interfaz de usuario (126), y está configurado para conectarse a una red de comunicaciones global (130). El dispositivo móvil tiene una memoria digital (122), un procesador (124) y una interfaz de comunicación NFC (128). La
35 memoria digital (122) del dispositivo móvil está programada con instrucciones legibles por procesador (124)

del dispositivo móvil para provocar que el dispositivo móvil establezca una conexión segura con la interfaz NFC (118) del elemento seguro utilizando la interfaz de comunicación NFC (128) del dispositivo móvil, y para enviar información al elemento seguro (112) para su procesamiento por el elemento seguro. El dispositivo móvil (120) también está configurado para establecer una cartera de criptomonedas (129) operable para acceder a una red de criptomonedas (150) a través de la red de comunicaciones global (130). El acceso a la red de criptomonedas puede ser directo o indirecto (es decir, la cartera puede interactuar directamente con una red de criptomonedas de segunda capa, como a través de *Lightning Network* o mediante protocolos de finanzas descentralizadas (DeFi) (por ejemplo, *Compound* o *Uniswap*) a través de sus respectivas cadenas, como ejemplos limitativos.

Las instrucciones legibles por procesador (114) del dispositivo de almacenamiento en frío y el procesador (124) del dispositivo móvil, cuando son leídas por los respectivos procesadores desde la memoria conectada a los mismos, son capaces de hacer que el sistema realice los pasos necesarios para procesar una transacción de criptomonedas. En un proceso típico (200), resumido en el diagrama de flujo representado en la Figura 2, una transacción, correspondiente a una transferencia de moneda que tiene un valor, es iniciada por un usuario a través de la interfaz de usuario (126) del dispositivo de procesamiento (PD, por sus siglas en inglés) (por ejemplo, el dispositivo móvil (120)), en el paso (210). El dispositivo móvil (120) establece un enlace de comunicaciones con el dispositivo de procesamiento. El dispositivo móvil (120) establece un enlace de comunicaciones, como un enlace seguro de comunicaciones (por ejemplo, cifrado), con el elemento seguro (SE) a través de NFC entre las respectivas interfaces NFC (118), (128) en el paso (220), a través del cual el dispositivo móvil en el paso (230) envía información de alto nivel al elemento seguro para su procesamiento en la comunicación (132). El procesador del elemento seguro (114), en el paso (240), recupera la clave privada de la memoria (116), realiza operaciones *hash* utilizando la clave privada para generar una firma, descifra la clave privada utilizando la clave pública almacenada en la memoria (116) (es decir, comprueba la cadena asociada a la clave pública para confirmar que la firma se ajusta a la firma de clave pública que solo podría haberse generado utilizando la clave privada específica), firma la transacción y envía la información de transacción firmada de vuelta al dispositivo móvil, por ejemplo, a través de una comunicación de NFC (136). Esta comunicación puede o no estar encriptada por el dispositivo móvil. Esta comunicación puede estar cifrada o no.

En el paso (250), el dispositivo móvil (120) establece entonces una sesión de comunicación a través de la red de comunicaciones global (130) con un servidor de cambio de criptomonedas (152) de la red de criptomonedas (150) y envía la información de transacción firmada al cambio de criptomonedas, que inicia una transacción operativa para enviar el valor de divisa o *token* al servidor de cambio.

El sistema (100) puede estar configurado además para recibir un depósito de criptomonedas. Un método para facilitar dicho depósito puede incluir que el dispositivo móvil muestre en la pantalla (125) una dirección de criptomonedas asociada a la cartera de criptomonedas en una forma codificada para

proporcionar a un pagador. Por ejemplo, la dirección puede estar en forma de código de barras o código QR que el pagador puede capturar con el dispositivo móvil del pagador. El sistema también puede leer una dirección a partir de una señal NFC u otra señal inalámbrica. El sistema también puede estar configurado para llevar a cabo cualquier tipo de transacción de criptomonedas, como la compra de criptomonedas (es decir, el uso de moneda fiduciaria) o el intercambio de criptomonedas (es decir, el comercio de una cantidad de una criptomoneda por una cantidad equivalente de otra criptomoneda).

En algunas modalidades, el elemento seguro (112) también puede comprender un módulo de pago (10) configurado para intercambiar información de pago con un lector de tarjetas para llevar a cabo una transacción de compra. Dicho módulo de pago (10) puede no estar conectado a partes del elemento seguro para procesar transacciones de criptomonedas, o puede estar conectado y utilizarse para iniciar una transacción de pago utilizando el elemento seguro. En las modalidades en donde el módulo de pago está conectado a la parte del elemento seguro configurada para procesar transacciones de criptomonedas, en lugar de que la transacción se inicie por el dispositivo móvil, el dispositivo de almacenamiento en frío puede establecer la conexión con el dispositivo móvil. Esta conexión puede ocasionar el inicio de la transacción, y las partes restantes de la transacción pueden ocurrir como se describe anteriormente. En una modalidad en donde el módulo de pago no está conectado a la parte de procesamiento de criptomonedas del elemento seguro, el procesamiento de un pago utilizando el módulo de pago puede ser una tarjeta de crédito convencional o transacción con tarjeta de débito, con el módulo de pago ubicado en conjunto en el dispositivo de almacenamiento en frío únicamente por conveniencia. En otras modalidades, la transacción de pago puede solicitar una transacción de tarjeta de crédito o débito convencional que se comunica al dispositivo móvil para la autorización y la satisfacción de la transacción, en cuyo caso el dispositivo móvil puede entonces iniciar la transacción de criptomonedas como se ha descrito anteriormente para satisfacer el pago. Los sistemas configurados para realizar tanto las funciones de criptomonedas descritas en el presente documento como las transacciones de pago pueden presentar un único elemento seguro (SE, por sus siglas en inglés) o dos SE (por ejemplo, uno en el módulo de pago, como en un procesador de interfaz dual (DI, por sus siglas en inglés), y el otro incrustado en otro lugar de la tarjeta). Un único SE puede tener “cajas” seguras (es decir, divisiones de *hardware* o *software* dentro del procesador que aíslan el pago de las partes criptográficas del SE, de modo que un ataque informático del *software* de pago del SE no proporcionaría una vía de acceso al *software* criptográfico, y viceversa).

En las modalidades con un lector biométrico (10), el lector biométrico (10) puede estar conectado al procesador (114) y a la memoria (116), con el procesador configurado para recibir los datos biométricos detectados por el lector, compararlos con los datos biométricos almacenados, y permitir el procesamiento posterior solo cuando la comparación muestre una coincidencia entre los datos leídos y los almacenados con un grado predeterminado de similitud. En otras modalidades, puede implementarse un punto de control

biométrico en el dispositivo móvil en lugar de (o además de) el aseguramiento biométrico proporcionado en la tarjeta.

En modalidades de ejemplo, el almacenamiento y las funciones relacionadas a las claves pública y privada pueden comprender un primer *applet*, y uno o más segundos *applets* de pago convencional también pueden asentarse en el elemento seguro sin ninguna interacción entre los respectivos *applets*.

La mayor parte de la secuencia relacionada a las transacciones de criptomonedas es bien conocida, como la definida por el protocolo Bitcoin o las actualizaciones BIP32/39: "Protocolo de mejora de Bitcoin" En una modalidad, los pasos se implementan dentro de un *applet* de Java que se ejecuta en el elemento seguro. Las claves se generan dentro del elemento seguro, que puede ser, por ejemplo, un microcontrolador de seguridad SLC37 de Infineon Technologies, y se almacenan cifradas en una clave segura. Las claves no salen de la tarjeta y se conocen en el exterior por sus índices lógicos, pero no por sus valores reales. Todas las operaciones de firma y *hash* se realizan utilizando el elemento seguro. En esencia, el *software* integrado en la tarjeta gestiona todas las criptográficas antiguas de la criptomoneda. Un *applet* móvil en el dispositivo móvil (por ejemplo, ejecutado en un sistema operativo Android/iOS) envía la información importante de alto nivel a la tarjeta para su procesamiento. A continuación, una vez que el *applet* móvil recibe la transacción firmada de la tarjeta, establece una sesión de comunicación con un criptointercambio y envía estos datos para iniciar una transacción.

Aunque la invención se ilustra y describe en el presente documento con referencia a modalidades específicas, la invención no pretende limitarse a los detalles mostrados. Por el contrario, pueden realizarse diversas modificaciones en los detalles dentro del alcance y el rango de equivalencias de las reivindicaciones y sin apartarse de la invención.

En particular, aunque se ilustra con respecto a las transacciones de criptomonedas, los métodos, sistemas, dispositivo de almacenamiento y dispositivos de procesamiento como se discute en el presente documento, pueden utilizarse en relación con la modalidad de cualquier tipo de transacción (no limitado a las transacciones financieras), y puede incluir cualquier tipo de autenticación de clave pública/clave privada conocida en la técnica. Por ejemplo, el dispositivo de almacenamiento descrito en el presente documento puede emparejarse con una aplicación de transacciones en un dispositivo móvil para realizar cualquier tipo de transacción, incluidas las autenticaciones que utilizan la norma FIDO®. El inicio de la transacción puede adoptar cualquier forma, como una pulsación desde un primer dispositivo conectado a una red que solicita a un segundo dispositivo conectado a la red, la provisión de un código (por ejemplo, un código QR) mostrado por un primer dispositivo (o plasmado en una manifestación física como un documento impreso) leído por un segundo dispositivo, o puede ser iniciada por el usuario utilizando la interfaz de usuario de la aplicación de transacciones en el dispositivo, o por el usuario utilizando el dispositivo de almacenamiento colocado en una proximidad de activación al dispositivo móvil capaz de intercambiar información con el dispositivo de almacenamiento. El inicio no se limita a ningún método en particular. En algunas modalidades, la tarjeta

puede también o en su lugar ser utilizado como un *token* de autenticación para carteras calientes u otras cuentas en línea utilizando el mismo o similares criptográficas antiguas como se ha descrito anteriormente. En tales modalidades, el elemento seguro de la tarjeta puede intercambiar credenciales de cifrado a través del dispositivo móvil que aloja la cuenta en línea. Este intercambio puede producirse durante la configuración inicial. Por ejemplo, se puede realizar un intercambio de claves PGP entre los dos dispositivos a través de un *applet*. Un simple *token* de reconocimiento puede entonces verificarse a través de un canal encriptado durante las transacciones posteriores que coincida con el *token* durante el registro inicial. Una tarjeta así configurada puede funcionar como un factor independiente de autenticación, pero no firma ninguna transacción de criptomonedas ya que no mantiene las claves. Las claves pueden asociarse a través de varias plataformas con otras interacciones de *software*.

15

20

25

30