(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 935 369**

(51) Int. CI.:

H04L 9/00 (2012.01)
G06Q 20/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.08.2016 PCT/CZ2016/000094**

(87) Fecha y número de publicación internacional: **23.02.2017 WO17028828**

(96) Fecha de presentación y número de la solicitud europea: **19.08.2016 E 16769847 (1)**

(97) Fecha y número de publicación de la concesión europea: **12.10.2022 EP 3350953**

(54) Título: **Transferencia de claves de cifrado de moneda digital a través del proceso de emisión, validación y devaluación de medio físico con autorización multifactorial, y el medio físico de claves de cifrado de moneda digital para realizar esta tecnología de transferencia**

(30) Prioridad:

20.08.2015 CZ 20150562

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.03.2023

(73) Titular/es:

SOBOTKA, PETR (100.0%)
Rozsirena 2039/19
182 00 Praha 8, CZ

(72) Inventor/es:

SOBOTKA, PETR

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Transferencia de claves de cifrado de moneda digital a través del proceso de emisión, validación y devaluación de medio físico con autorización multifactorial, y el medio físico de claves de cifrado de moneda digital para realizar esta tecnología de transferencia

Campo de la invención

La presente invención se refiere al campo de moneda digital y red de pago electrónico basada en criptografía y descentralización, tal como Bitcoin, Litecoin, etc. La invención se refiere a los métodos y procedimientos para transferir estos instrumentos financieros al mundo físico y para crear una realización física correspondiente de este medio de pago en forma de un medio de claves de cifrado para moneda digital.

Antecedentes de la invención

Desde el establecimiento de la criptomoneda digital Bitcoin a principios de 2008/2009, se han producido intentos de transferir esta moneda electrónica al mundo físico. La forma más fácil y común es crear una "billetera de papel" (figura 1). De hecho, este es el respaldo en papel de una clave de cifrado privada que se logra al usar equipo de oficina comúnmente disponible. La billetera de papel contiene una clave de cifrado privada en un texto legible para humanos y generalmente también en un código QR legible por máquina, una dirección de Bitcoin (nuevamente, en texto y código QR), y posiblemente una figura que muestra el saldo, o un recuadro donde se puede escribir la cantidad de saldo. Todo se proporciona con texto adicional, instrucciones y gráficos a color. La billetera de papel no contiene características de seguridad.

Hay varios servicios web/programas de software para generar billeteras de papel (Literatura 1, 2, 3). El titular de una billetera de papel realmente controla el saldo de moneda digital en una dirección relevante. El problema es que cada billetera de papel puede tener un número ilimitado de copias, por lo tanto, una billetera de papel, como un objeto físico, no refleja el valor de un saldo de moneda digital. Una billetera de papel tampoco puede servir para pagos, porque el destinatario nunca puede estar seguro de si el pagador conserva otra copia. Por lo tanto, esto es realmente solo un instrumento para el respaldo de una clave privada, de manera similar a anotar una contraseña para la banca electrónica en lápiz sobre papel. No lo compartimos con nadie, ni intentamos pagar con ello.

En 2011 aparecieron en el mercado monedas Bitcoin Casascius (figura 3) y tarjetas Bitbills de plástico (figura 2). Ambos productos representan objetos físicos que contienen una clave privada integrada cubierta con una etiqueta a prueba de manipulación. En 2013 aparecieron los certificados de Bitcoin de Bitcoin Suisse AG (figura 4) que tiene la clave privada pegada entre dos capas de papel sintético. Los tres productos sufren una deficiencia fundamental: el fabricante conoce las claves privadas de todas las piezas producidas de cada instrumento de pago. Por lo tanto, los titulares actuales no están en una posición exclusiva para controlar la moneda digital representada por objetos físicos; siempre hay un titular conjunto - el fabricante. Aunque los fabricantes se comprometen a haber destruido la información de clave privada, o presumen de altos estándares de seguridad en la producción que proporcionan garantías de ninguna fuga de información de claves privadas, este asunto no se puede verificar de forma independiente y siempre existe un cierto riesgo de que el respaldo de parte o todas las unidades producidas de un medio de pago tarde o temprano sea malversado por un fabricante inicialmente honesto, lo que equivale a robar a sus propios clientes. El modelo correspondiente de control financiero se muestra en la figura 6.

Hay intentos de prevenir esta situación mediante la especificación BIP 38 (Literatura 4), que permite generar una clave privada protegida por una contraseña. Durante un cierto período (2012-2013), el fabricante de monedas Casascius ofreció a los clientes pedir monedas hechas de acuerdo con esta especificación. El procedimiento fue como sigue: un cliente generó una clave privada protegida con contraseña y la envió al fabricante Casascius, que produjo una moneda para el cliente con la clave protegida integrada en la misma. La moneda se envió al cliente-cliente. En este modelo, al fabricante no se le dio la oportunidad de apropiarse indebidamente de los fondos porque el único que conocía la contraseña de la clave privada era el cliente. Este modelo corresponde al diagrama dibujado en la figura 7. El titular de moneda no tiene que preocuparse por la apropiación indebida del respaldo de moneda digital correspondiente. Sin embargo, esta moneda no se puede utilizar como un medio de pago por una simple razón: El receptor de nuevo no se convertiría en un titular exclusivo ya que el primer propietario, que había pedido la moneda, conoce tanto la clave privada como la contraseña. Por lo tanto, el problema no se resuelve, simplemente se desplaza un paso más en la cadena de titulares (ver figura 8). Excepto para el primer titular (Cliente), ningún otro titular actual puede controlar exclusivamente el respaldo por moneda digital. Los fabricantes de objetos basados en PIF38 son conscientes de este hecho, por lo que ofrecen sus productos, en lugar de como un medio de pago, para "almacenamiento fuera de línea" (almacenamiento en frío), es decir, como un depósito seguro de un saldo de criptomonedas digitales en forma física.

Por el momento, no existe una solución técnica conocida públicamente para producir y utilizar medios de pago físicos respaldados por moneda digital de manera que un titular actual tenga un control exclusivo sobre el respaldo correspondiente. Por lo tanto, una solución que satisfaría la esencia de los diagramas en la figura 7 y 9.

Por ejemplo, hay un documento de Christopher Mann et al. : Autenticación de dos factores para el protocolo Bitcoin "

IACR, International Association for Cryptologic research, vol. 20141104"132246, 4 de noviembre de 2014 (2014-11-04), páginas 1 a 18, XP061017249. Este documento describe cómo realizar la autenticación de dos factores para una billetera de Bitcoin que emplea el protocolo de firma de ECSDA de dos partes y un teléfono inteligente como segundo factor de autenticación.

La invención se define por las reivindicaciones independientes. Se establecen realizaciones preferidas en las reivindicaciones dependientes.

Breve descripción de la invención

Las desventajas mencionadas de las representaciones físicas existentes de moneda digital se eliminan mediante la transferencia de claves de cifrado de moneda digital a través del proceso de emisión, validación y devaluación de medio físico con autorización multifactorial. La idea básica de este proceso de transferencia es que un emisor, utilizando una aplicación de software para emisión de medio, carga un medio en blanco distribuido en el mercado, emparejado con el segundo factor de autorización almacenado de forma segura en el fabricante o integrado en el medio en forma de un recuadro a prueba de manipulación, y genera el primer factor de autorización. Con base en este primer factor de autorización, el identificador de medio y otros datos adquiere la dirección donde enviar el saldo de moneda digital en la cantidad equivalente a la denominación del medio. Habiendo inspeccionado todas las formalidades requeridas, en particular la autenticidad de la pieza de medio y la suma transferida del saldo de moneda digital que es igual a la denominación del medio, se emite una firma digital previa solicitud a través del servicio en línea. La aplicación de software para la emisión de medio combina la firma digital con el primer factor de autorización y el emisor completa el medio con estos datos especialmente mediante impresión, escritura a mano o una pegatina. De esa manera, el medio se activa y se puede pasar al siguiente titular, incluso repetidamente. El destinatario realiza una inspección visual y verifica el medio utilizando una aplicación de software para la verificación del medio, especialmente la cantidad del saldo de moneda digital. Luego esta aplicación SW verifica la autenticidad de la firma digital después de cargar el primer factor de autorización y la firma digital, se valida el primer factor de autorización y el receptor compara los datos firmados digitalmente con los datos visibles en el medio. Luego, el destinatario carga, utilizando la aplicación de software para el canje de moneda digital, todos los factores de autorización disponibles en este nuevo medio físico debidamente emitido en estado activo, posiblemente añade otros factores de autorización conocidos por él, y compila y autoriza una transacción electrónica en la red de moneda digital dada para canjear fondos en forma electrónica a la dirección privada del destinatario. El resultado es la transferencia de claves de cifrado de moneda digital a través del proceso de emisión, validación y devaluación de medio físico con autorización multifactorial, y efectuando así una transacción de pago entre el emisor y el destinatario final en moneda digital. Parte del resultado también es un medio visiblemente devaluado. Preferentemente, el último destinatario, que realiza el canje de fondos en moneda digital y la devaluación final del medio es su fabricante original, que utiliza para la compilación y autorización de la transacción en moneda digital también otros factores de autorización no presentes en el medio y conocidos solo por él.

Preferentemente, la aplicación SW para emisión de medio, la aplicación SW para verificación de medio y la aplicación SW para el canje de los fondos de moneda digital son aplicaciones de código abierto, accesibles públicamente en Internet. En el mejor de los casos, todas estas tres aplicaciones SW se representan por una sola aplicación de software.

Los inconvenientes anteriores de las representaciones físicas actuales de monedas digitales se eliminan mediante el medio físico de claves de cifrado para moneda digital diseñadas para la transferencia exitosa de claves de cifrado de moneda digital cuyo cuerpo base es un objeto plano de cualquier forma (en particular una figura geométrica), hecho de materiales compactos (especialmente plásticos, papel, metales y sus aleaciones) con una de sus superficies planas principales identificadas con el identificador alfanumérico único 1 y que contiene, dependiendo de un modelo particular, aplicaciones de características de protección contra la falsificación, con una o ambas superficies planas principales que tienen también recuadros para recibir el primer factor de autorización y la firma digital.

Preferentemente, el cuerpo base en forma de un objeto plano tiene la forma de un cuadrado, rectángulo o círculo.

Preferentemente, el cuerpo base tiene la forma de tarjetas de crédito estándar, monedas y billetes. Preferentemente, el cuerpo base lleva a cada lado información sobre la denominación y la unidad monetaria.

Preferentemente, las características de protección contra falsificación en caso de realización en forma de papel son en particular papel de seguridad especial con marcas de agua o tiras metálicas, elementos ópticamente variables, elementos gráficos muy finos llamados guillochés, gradaciones de color de iris, colores con luminiscencia UV o IR, colores de reactivos químicos o métodos de impresión inaccesibles.

Preferentemente, las características de protección contra falsificación en caso de realización en tarjetas de plástico son principalmente hologramas.

Preferentemente, las características de protección contra falsificación en caso de realización en monedas de metal son elementos de seguridad difractivos (kinegramas) o chips RFID electrónicos.

Preferentemente, el identificador alfanumérico único 1 se convierte en un elemento asegurado, es decir, revestido con

barniz iridiscente, perforado o un elemento ópticamente variable.

Preferentemente, solo hay un único recuadro utilizado para rellenar tanto el primer factor de autorización como la firma digital.

Preferentemente, cualquiera de las superficies de plano principales lleva otro recuadro que contiene el segundo factor de autorización en un modo a prueba de manipulación.

La tecnología propuesta para transferir claves de cifrado de moneda digital a través del proceso de emisión, validación y devaluación de medio físico con autorización multifactorial y el medio físico de claves de cifrado de moneda digital para realizar esta tecnología comparten las siguientes ventajas clave:

1. Esta forma física de moneda digital es muy difícil de falsificar.
2. Un titular actual está en una posición exclusiva para controlar la moneda digital utilizada para respaldar un determinado medio. En otras palabras, ninguno de los titulares anteriores ni el fabricante se pueden apropiar indebidamente del respaldo.
3. El respaldo (emisión) del medio físico es fácilmente factible utilizando equipos de computadora y oficina comúnmente disponibles y una conexión a Internet.
4. La verificación del medio físico es fácilmente factible utilizando equipos de computadora móviles y software preinstalado comúnmente disponibles, incluso sin conexión a Internet.
5. En caso de que un medio físico también contenga el segundo factor de autorización en un modo a prueba de manipulación, cualquiera puede cancelar el respaldo y canjear los fondos utilizando equipo de computadora (móviles) comúnmente disponibles y acceso a Internet, pero la devaluación /daño evidente al medio ocurrirá al mismo tiempo.

En comparación con los productos físicos actuales destinados a preservar el equilibrio de las monedas digitales, la invención significa un gran salto cualitativo hacia adelante, debido principalmente a los puntos 2 y 4.

En comparación con los medios de pago actualmente disponibles como productos de bancos y estados (billetes, monedas, cheques), la invención presentada también aporta una innovación fundamental. Los medios de pago comúnmente disponibles se basan en la confianza directa (figura 5), y si la confianza en sus fabricantes se desvanece, los instrumentos de pago pierden inmediatamente su función y valor. El titular no puede controlar directamente (fácticamente) el respaldo relevante de un determinado instrumento de pago. Las posiciones del titular y del fabricante no son iguales, por lo tanto, en caso de quiebra del fabricante o de una reforma monetaria, el titular generalmente pierde el valor total representado por estos sustitutos.

La invención de medios físicos de claves de cifrado para moneda digital da nacimiento a un medio de pago que conserva su valor independientemente de la situación económica del fabricante. En caso de que los medios físicos que contienen también el segundo factor de autorización en un modo a prueba de manipulación, ni la quiebra ni la posible liquidación del fabricante tienen efecto sobre el valor de los medios emitidos.

El medio físico inventado de claves de cifrado para moneda digital lleva, a diferencia de los sustitutos monetarios mencionados, su valor intrínseco equivalente al saldo en la moneda digital. Este valor intrínseco es similar como si los medios de pago fueran directamente metales preciosos (oro, plata). Estas ofertas, generalmente monedas, también tienen su valor intrínseco, que es independiente de la entidad del fabricante.

La presente invención permite realizar la metamorfosis entre la forma electrónica y física del dinero en la comodidad del hogar y sin un intermediario (banco). Tener la cantidad necesaria de piezas no respaldadas de los medios descritos, equipos comunes de computadora y oficina y una conexión a Internet es suficiente para cambiar la representación electrónica a la física de la moneda. En el caso de medios físicos con el segundo factor de autorización 5A en un modo a prueba de manipulación, también es posible un cambio en la dirección opuesta, sin un intermediario y con solo una conexión a Internet y un teléfono móvil inteligente o tableta.

En resumen, la ventaja absoluta de esta invención es la posibilidad de crear un medio físico de claves de cifrado para moneda digital y usarlo para realizar la transferencia de las claves de cifrado de moneda digital a través del proceso de emisión, validación y devaluación del medio físico, en tanto que un titular actual tiene un control exclusivo sobre el respaldo de la moneda digital.

Leyenda de las figuras adjuntas (dibujos de la invención)

Figura 1 Billetera de papel
Figura 2 BitBills
Figura 3 Monedas de Casascius
Figura 4 Certificados de Bitcoin
Figura 5 Control indirecto del respaldo
Figura 6 Control no exclusivo del respaldo
Figura 7 Control exclusivo del respaldo

Figura 8 Titulares versus cotitulares
Figura 9 Control exclusivo del titular actual
Figura 10 La mera creación de la representación física
Figura 11 Transición entre la representación electrónica y física
Figura 12 Las formas de los medios de claves de cifrado
Figura 13 Moneda - el anverso
Figura 14 Moneda - el reverso
Figura 15 Billete
Figura 16 Tarjeta de plástico
Figura 17 El ciclo de vida del medio de claves de cifrado para moneda digital
Figura 18 El procedimiento de emisión de medio de claves de cifrado
Figura 19 El procedimiento de validación de medio de claves de cifrado
Figura 20 El procedimiento de devaluación del medio de claves de cifrado

Ejemplos de la invención

Definiciones de términos básicos

Para describir y explicar el uso de medios físicos con claves de cifrado para moneda digital es necesario definir o aclarar primero ciertos términos. **Bitcoin** es una moneda digital y una red de pago, a veces también conocida como moneda virtual, o más precisamente como criptomoneda. Funciona sobre la base de una red P2P descentralizada de programas de computadora con una estructura de datos distribuidos conocida como cadena de bloques (blockchain) y utiliza criptografía asimétrica para autorizar transacciones.

Las **monedas digitales (criptomonedas)** en este texto se refieren a toda la familia de sistemas tal como Bitcoin. Por lo tanto, todas las monedas y redes de pago que operan como Bitcoin, monedas y redes de pago derivadas de las mismas, y monedas y redes de pago basadas en los mismos principios, por ejemplo, Litecoin, DogeCoin, PrimeCoin y muchos otros.

Medio de pago - a menos que se especifique lo contrario, es un objeto físico presente en el mundo real, que sirve para mantener y transferir un cierto valor en el sistema de pago. Puede estar marcado con una denominación y una unidad monetaria. Los medios de pago típicos en el contexto de este documento son monedas, billetes, cheques o la invención descrita en sí.

Pago físico - un acto en el que dos entidades transfieren un medio tangible de pago de una determinada denominación, por ejemplo, un pago con un billete en una tienda.

Medio físico de claves de cifrado para moneda digital es un objeto conectado con un cierto saldo financiero en la red de pago de una moneda digital determinada. Por lo general, sólo es plenamente legítimo con garantías de ser el único instrumento existente para controlar el saldo adecuado, es decir, no hay más copias de este objeto con el mismo número de serie.

Dirección de moneda digital es equivalente al número de cuenta bancaria en el sistema financiero convencional.

Claves de cifrado públicas y privadas son dos piezas de información que permiten realizar criptografía asimétrica.

A prueba de manipulación es la designación de una calidad general y una familia de tecnologías que son capaces de detectar la penetración en un entorno protegido. Su objetivo no es impedir la penetración, sino detectarla de manera fiable, por ejemplo, sellos en las cartas, sellos utilizados por la policía para asegurar las puertas de bienes inmuebles, sellos utilizados por los fabricantes de productos electrónicos para detectar interferencia no autorizada con el dispositivo, boletos para raspar, etc.

Fabricante de medio físico de claves de cifrado para moneda digital es una entidad que lanza el medio en el mercado bajo su propio nombre/marca. Puede ser una empresa, un banco o una institución estatal.

Emisor es un usuario/titular que utiliza un medio físico no respaldado de claves de cifrado y lo emite; de manera similar a la emisión de cheques.

Ciclo de vida de un medio de pago

La transferencia de claves de cifrado de moneda digital a través del proceso de emisión, validación y devaluación de medio físico con una autorización multifactorial se puede demostrar en el ejemplo del ciclo de vida de un medio de pago en forma de un medio físico de claves de cifrado de moneda digital. Los medios de pago descritos se distribuyen en blanco (sin respaldo) en el mercado. Este estado es visible a primera vista, ya que el recuadro 2 para el primer factor de autorización 2A y el recuadro 3 para la firma digital 3A están en blanco, y posiblemente el recuadro 5 para el segundo factor de autorización 5A intacto. En esta condición, el valor de este medio es solo su precio de venta, que puede ser

proporcional en comparación con la denominación indicada. La mejor metáfora para este estado es la comparación con un cheque sin llenar.

Un cliente puede emitir un instrumento de pago, es decir, respaldarlo con saldo en moneda digital. Ver la sección emisión de medio físico de claves de cifrado. En ese momento el medio gana el valor correspondiente a su denominación. Dado que se añade la información sobre el primer factor de autorización 2A y la firma digital 3A, el medio se distingue ahora de su condición en blanco anterior a primera vista.

Un medio respaldado se puede usar para pagos, lo que requiere que el destinatario verifique su autenticidad y respaldo. Ver la sección verificación de medio físico de claves de cifrado.

Un medio se puede utilizar para pagos repetidamente. No hay ninguna modificación en curso.

Un titular que desee liberar los fondos de respaldo y continuar usándolos solo electrónicamente puede devaluar el medio. Este proceso se describe en la sección devaluación de medio físico de claves de cifrado. De esa manera el ciclo de vida de un medio es al final. En este sentido, es desechable sin posibilidad de reciclaje funcional. Dependiendo del material utilizado, se puede eliminar ecológicamente. El ciclo de vida se ilustra en el diagrama de estado en la figura 17.

Infraestructura de software necesaria

Para transferir un blanco (no respaldado) a un medio respaldado, para verificar un medio y para transferir un respaldado a un medio devaluado (más precisamente, para canjear el respaldo de un medio devaluado de claves de cifrado para moneda digital), se necesita la siguiente infraestructura de software auxiliar:

a) Aplicación SW para la emisión de medio físico de claves de cifrado. Ayuda a los clientes a crear el primer factor de autorización 2A, combinarlo con un identificador de medio y posiblemente otros datos para adquirir la dirección final a la que se depositará el saldo de moneda digital con la intención de respaldar un medio físico específico de claves de cifrado para moneda digital. La solicitud también se comunica con el servicio en línea para la emisión de firmas digitales 3A, y finalmente prepara el trabajo preliminar para una realización adecuada del primer factor de autorización 2A y la firma digital 3A (por ejemplo, compila datos para imprimir en un medio).
b) Servicio en línea para la emisión de firmas digitales 3A.
El fabricante de medios de claves de cifrado proporciona un servicio público de Internet para la emisión de firmas digitales 3A. Durante el proceso de emisión de medio, el cliente se comunica automáticamente con este servicio en línea y después de la verificación de todas las formalidades (autenticidad de un medio físico de claves de cifrado con un identificador específico, la cantidad real de respaldo, etc.), el fabricante produce la firma digital 3A y la envía a través de la red de Internet al cliente.
c) Aplicación SW para la verificación de medio físico de claves de cifrado.
Ayuda al beneficiario a verificar la autenticidad de un medio físico de claves de cifrado para moneda digital, así como el respaldo adecuado por un saldo correspondiente de moneda digital. Puede estar diseñado, por ejemplo, para dispositivos móviles (tal como un teléfono o una tableta) equipados con una cámara, o para las terminales de pago de los comerciantes equipados con un lector de código de barras, etc. Sirve para facilitar la carga de la máquina y un análisis de la información relevante de un medio físico específico de claves de cifrado en el momento del pago.
d) Aplicación SW para el canje de fondos de moneda digital.
Se utiliza para cargar el primero y, si está disponible, también el segundo factor de autorización 5A en un medio devaluado y para compilar una transacción electrónica específica en una red de moneda digital dada con el fin de canjear los fondos a la dirección privada del titular. La única tarea es ayudar y facilitar el cambio de moneda de la forma física a la forma electrónica.

Distribución de equipos SW

Se asume que el fabricante de medios físicos de claves de cifrado liberará una aplicación para la emisión, una aplicación para la verificación y una aplicación para el canje de fondos en el modo de código abierto, accesible públicamente en Internet, con el fin de lograr una mayor transparencia de todo el sistema y recibir posibles comentarios de expertos en software.

Se puede asumir además que una implementación públicamente independiente de esta funcionalidad puede aparecer de un tercero con el fin de diversificar la infraestructura de software. Este hecho no comprometerá la invención, por el contrario, puede fortalecer la robustez de todo el sistema.

La infraestructura de software no está sujeta a la protección de la propiedad industrial y no contiene una inventiva sustancial. Sirve principalmente para automatizar y facilitar operaciones con medios físicos de claves de cifrado - principalmente realiza operaciones informáticas rutinarias y bien documentadas tal como emisión de firma digital, verificación de firma digital 3A, comunicación con la red P2P de moneda digital, etc.

Tecnología de autorización de dos factores

Hay múltiples tecnologías que se van a utilizar. Ya sea la clave privada se divide en varias partes, o se genera a partir de más piezas de información (consultar el esquema de uso compartido de secretos de Shamir (Literatura 8)), o la llamada transacción multifirma (multisig) y/o P2SH (Literatura 9), que requiere el conocimiento de dos o más claves privadas para controlar el saldo de la moneda digital.

Cabe mencionar que la seguridad criptográfica de toda la solución no depende de la calidad del primer factor de autorización 2A generado por el emisor. Con la condición de que el fabricante garantice la fuerza criptográfica del segundo factor de autorización 5A, así como la unicidad del segundo factor de autorización 5A para cada artículo valioso, y siempre que la concatenación de estos dos factores 2A, 5A se defina de una sola manera posible, entonces incluso si el emisor aplica el mismo primer factor de autorización 2A para más piezas de medios de pago, o si utiliza información criptográficamente débil con baja entropía, no pondrá en peligro la seguridad de la tecnología en términos de un ataque potencial por parte de un tercero.

Tecnología de firma digital

El esquema de firma digital específico 3A no es esencial para la realización de la invención. Parece deseable utilizar la firma digital 3A basada en criptografía asimétrica y la llamada infraestructura de clave pública (PKI). Los algoritmos particulares pueden ser, por ejemplo, DSA, ECDSA.

Emisión de medio físico de claves de cifrado

El procedimiento se muestra en la figura 18. Un cliente-emisor debe tener un medio en blanco (no respaldado) de claves de cifrado, equipos informáticos con acceso a Internet y una aplicación de software para su emisión. Utilizando este SW genera, o carga desde otra fuente, el primer factor de autorización. Luego carga el identificador desde el medio físico de claves de cifrado para la moneda digital y posiblemente también otra información auxiliar necesaria para la compilación de la dirección para el respaldo. La aplicación deriva la dirección de respaldo y la comunica al emisor. Posteriormente, envía a esta dirección la cantidad de respaldo correspondiente (igual a la denominación del instrumento de pago). Luego, utilizando la aplicación de emisión, solicita al servicio en línea del fabricante la firma digital 3A. Si se cumplen todas las formalidades (es un medio de pago auténtico, la cantidad enviada para el respaldo corresponde a la denominación, etc.), se genera la firma digital 3A. La aplicación de emisión luego la combina adecuadamente con el primer factor de autorización 2A y produce un formato para facilitar al emisor una terminación adecuada del medio, por ejemplo, versión impresa.

Una vez que se completa la información necesaria en el medio, el proceso de emisión es al final, y hay un nuevo medio físico debidamente respaldado de claves de cifrado. Si se desea, el emisor puede verificarlo (ver más adelante).

En este punto, el emisor no puede controlar los fondos utilizados para el respaldo a menos que el medio esté devaluado (ver más adelante). Los mismos fondos no se pueden utilizar para respaldar otro medio u otro pago en forma digital. Los fondos están estrechamente vinculados a un medio específico cuyo titular actual está en una posición exclusiva para controlar el respaldo relevante en moneda digital.

Verificación de medio físico de claves de cifrado

El procedimiento de verificación se muestra en la figura 19. El verificador (generalmente el destinatario de un medio físico de claves de cifrado) utiliza una aplicación de software para la verificación, que se puede descargar libremente en Internet. Sin embargo, al momento de la verificación, independientemente del número de medios verificados, ya no existe la necesidad de estar en línea. En primer lugar, el verificador comprueba visualmente el medio para ver si está respaldado (es decir, si el recuadro para el primer factor de autorización 2A y el recuadro 3 para la firma digital 3A no están en blanco). Un medio aparentemente en blanco y sin respaldo se debe rechazar como medio de pago inmediatamente. Para completar la inspección visual, las características de seguridad también se deben verificar dependiendo de la realización particular de la invención, por ejemplo, en caso de papel de la marca de agua, holograma, etc. Luego el verificador inicia la aplicación de software, carga el primer factor de autorización 2A y la firma digital 3A desde el medio, y la aplicación verifica si la firma digital 3A es genuina y a qué medio y denominación se refiere. El verificador comprueba visualmente si el medio en sus manos está marcado con una denominación correcta y equipado con un identificador apropiado, y en caso de conformidad, acepta el medio. Si descubre alguna diferencia en el identificador o la denominación, se niega a aceptar el medio de pago.

Parte de la inspección con el uso de la aplicación de software es la validación del primer factor de autorización 2A. Si el medio contiene un primer factor de autorización 2A defectuoso, dañado o totalmente inadecuado, la aplicación notifica al verificador de este hecho y la verificación termina con un resultado negativo.

Devaluación de medio físico de claves de cifrado

El procedimiento de devaluación se muestra en la figura 20. En este punto nos referimos a la devaluación con la intención de transferir el respaldo correspondiente a la forma electrónica. Por supuesto, hay muchas posibilidades de destruir el instrumento de pago dependiendo del material utilizado, por ejemplo, por calor, disolventes químicos, etc. Sin embargo, su mera destrucción física sin carga previa del primer 2A y posiblemente el segundo factor de autorización 5A, causaría

una destrucción irreversible completa de las unidades monetarias digitales correspondientes (similar a la quema de un billete válido). Esperamos que la mayoría de los usuarios se guíen por motivos racionales y lleven a cabo la destrucción con el fin de obtener la moneda digital utilizada.

El usuario carga el primer factor de autorización 2A. En caso de que también exista el segundo factor de autorización 5A en un modo a prueba de manipulación, elimina la protección a prueba de manipulación para obtener la información sobre el segundo factor de autorización 5A. En realidad, puede ser rascar un recuadro, despegar una pegatina destructiva, romper o rasgar el cuerpo de los medios de pago, etc. Luego el usuario canjea los fondos a su dirección privada utilizando una aplicación de software.

Naturaleza de construcción de la tecnología propuesta de medio físico

En primer lugar se introduce en el texto y las figuras adjuntas es el elemento básico de la transferencia de claves de cifrado de moneda digital a través del proceso de emisión, validación y devaluación de medio físico con autorización multifactorial, por lo tanto, la construcción de un medio físico de claves de cifrado de moneda digital. Está hecho de un cuerpo base plano de cualquier forma (en particular una figura geométrica) y materiales compactos (especialmente plásticos, papel, metales y sus aleaciones) con una de sus superficies planas principales identificadas con el identificador alfanumérico único 1. Este medio físico de claves de cifrado para moneda digital contiene, dependiendo de un modelo particular, aplicaciones de características de protección contra falsificación, con una o ambas superficies planas principales que tienen el recuadro 2 para recibir el primer factor de autorización 2A. recuadro 3 para agregar la firma digital 3A, y, si es el caso, también el recuadro 5 para el segundo factor de autorización 5A en un modo evidente.

El cuerpo base, un objeto plano, tiene preferentemente la forma de un cuadrado, rectángulo o círculo, o la forma de una tarjeta de crédito, moneda o billete estándar. A cada lado proporciona información sobre la denominación y la unidad monetaria.

Los medios físicos de claves de cifrado incorporados en forma de papel tienen aplicaciones con características de protección contra falsificación, en particular papel de seguridad especial con marcas de agua y/o tiras metálicas, elementos ópticamente variables, gráficos muy finos llamados guillochés, gradaciones de color de iris, colores con luminiscencia UV o IR, colores de reactivos químicos o métodos de impresión inaccesibles.

En caso de realización en tarjetas de plástico, las características de protección contra falsificación son principalmente hologramas, y en caso de realización en monedas de metal las características de protección contra falsificación son preferentemente elementos de seguridad difractivos (kinegramas) o chips RFID electrónicos. El identificador alfanumérico único 1 se convierte en un elemento asegurado, es decir, en particular, revestido con barniz iridiscente, perforado o un elemento ópticamente variable.

Una de las soluciones trae el recuadro 2 para el primer factor de autorización 2A y el recuadro 3 para la firma digital 3A en un recuadro compartido.

La tecnología de medio físico de claves de cifrado para moneda digital se basa en los siguientes bloques de construcción: características de impresión de seguridad, autorización multifactorial, firma digital y posiblemente también características a prueba de manipulación. La presente invención es un objeto físico que está protegido contra falsificación con características de seguridad e identificado por el identificador alfanumérico único 1. En seguida, contiene el recuadro 2 para recibir el primer factor de autorización 2A, que hace, después de una emisión adecuada del medio, como máximo la mitad de la cantidad de información necesaria para el control del respaldo digital. El objeto contiene además el recuadro 3 para añadir la firma digital 3A. Estas dos piezas de información se deben proporcionar por el cliente, junto con los fondos en moneda digital necesarios para respaldar el medio. También es preferible si el medio físico de las claves de cifrado contiene el recuadro 5 con el segundo factor de autorización 5A protegido por una característica de seguridad de naturaleza a prueba de manipulación, en otras palabras, legible solo con una devaluación/daño evidente de todo el objeto.

Descripción detallada del medio

Dimensiones, peso, material y forma: la realización del medio de claves de cifrado para moneda digital puede ser teóricamente de cualquier tamaño, sin embargo, para hacer que su uso en transacciones de pago físico entre individuos sea práctico y cómodo, presumiblemente el tamaño de cada pieza individual debe variar de unidades a decenas de centímetros, con su volumen minimizado por la razón de almacenamiento que ahorra espacio.

Del mismo modo, el peso del medio no debe exceder varias unidades de gramos, ya que la manipulación con medios mucho más masivos de claves de cifrado sin duda conduciría a una reducción en la ergonomía de pago. Sin embargo, teóricamente, se puede producir un medio de cualquier peso. El material del medio tampoco se da con precisión. Es deseable utilizar un material que proporcione durabilidad, resistencia al desgaste razonable y costos de producción aceptables incluso en lotes de gran cantidad, típicamente papel, plástico o metal. Tampoco se especifica la forma de la presente invención, preferentemente debe ser una forma plana (plana).

Las dimensiones, el peso, el material y la forma no son esenciales para la realización de la invención, pero no deben

impedir el uso de los elementos clave antes mencionados, que debe contener el medio físico de las claves de cifrado.

En este texto trabajamos con tres posibles realizaciones físicas, en su tamaño, peso, material y forma que se asemejan más a los medios de pago bien establecidos actuales, es decir, una moneda, un billete y una tarjeta de plástico (figura 12). Sin embargo, se debe señalar nuevamente que las posibles realizaciones de la presente invención no se limitan a estas tres opciones, y se pueden producir combinaciones teóricamente completamente diferentes de materiales, pesos, tamaños y formas.

Protección contra falsificación e imitación

El medio de claves de cifrado debe, en última instancia, obstaculizar cualquier intento de falsificación. En el caso de una realización de papel/polímero, se debe utilizar impresión de seguridad, es decir, tecnologías que conducen a la producción y aplicación de una variedad de características de seguridad típicas en la producción de billetes. Estos incluyen, por ejemplo, papel de seguridad especial con marcas de agua y/o tiras metálicas, los llamados elementos ópticamente variables ("hologramas", barniz iridiscente, colores especiales), métodos de impresión comúnmente inaccesibles tal como huecograbado o impresión offset de alta precisión, elementos geométricos muy finos llamados guillochés, gradaciones de color de iris, colores con luminiscencia UV o IR, colores termocrómicos o reactivos químicos, etc. Hay muchas características de protección y tecnologías de producción, y su selección particular depende de la elección y las posibilidades de producción del fabricante de medios de pago.

Las tarjetas de plástico también se pueden equipar con elementos ópticamente variables ("hologramas"), impresos en colores especiales, grabados en relieve, etc.

Las monedas de metal se pueden equipar con un elemento ópticamente variable KINEGRAM (Literatura 5), o un chip RFID electrónico (Literatura 6).

Distinguibilidad y unicidad

Cada medio debe estar marcado con el identificador alfanumérico único 1. La unicidad está asegurada por el fabricante que selecciona un conjunto adecuado de identificadores, que no necesitan formar una serie continua, por el contrario, parece preferible usar cadenas suficientemente largas que se ven al azar a primera vista. Por ejemplo:

4DaFvf3RumoW67B2rXAMdx72VycebHksU

KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM

NH9od4H3XQupviN8pRGQ6uteVm1qd9KF4, etc.

Estos identificadores, si son de longitud suficiente y por lo tanto de espacio combinatorio suficientemente grande, básicamente eliminan la posibilidad de que un falsificador potencial los adivine y produzca falsificaciones de piezas no disponibles. La autenticación (ver más adelante) incluye una inspección automatizada del identificador, es decir, se detectaría inmediatamente una falsificación con un identificador no conforme, por ejemplo, inventado.

En las Figuras 13, 15 y 16 se proporcionan ejemplos del uso de identificadores alfanuméricos 1.

Protección contra modificaciones del identificador

Con respecto a la naturaleza de la invención, cuando el mercado libre ofrece medios sin respaldo (en blanco) y debidamente respaldados, es decir, no todos los medios tienen siempre el valor correspondiente a la denominación indicada, es necesario obstaculizar en última instancia cualquier esfuerzo para modificar el identificador para evitar la falsificación convirtiendo una pieza sin respaldo en una respaldada. El siguiente ejemplo demuestra que si un identificador estuviera en forma de un número ordinario de una serie continua impresa en una tecnología convencional, un falsificador necesitaría obtener solo dos piezas originales sin respaldo con números de identificación consecutivos. Después de respaldar adecuadamente uno con la moneda digital, es decir, emitir un medio válido de claves de cifrado, modificaría la segunda pieza para que el identificador fuera idéntico al primero y transfiriera allí también otros elementos clave (ver más adelante). De esa manera recibiría una falsificación muy exitosa. En el caso del identificador numérico de una serie continua, es de hecho suficiente alterar uno (el último) dígito de cualquiera de los dos números consecutivos. Por el contrario, con el uso de identificadores alfanuméricos largos 1 de una serie discontinua, como se describió anteriormente, un falsificador tendría que alterar una gran cantidad de caracteres, a menudo toda la cadena. Además, si el identificador se convierte en una característica protegida, por ejemplo, revestido con barniz iridiscente, composición tipográfica, perforado o variable ópticamente, entonces cualquier esfuerzo de un falsificador potencial para modificar el identificador se vuelve mucho más difícil y no habrá posibilidad de llevar a cabo un ataque contra los medios valiosos por la modificación del identificador.

Recuadro 2 para el primer factor de autorización 2A

En un medio de claves de cifrado para moneda digital, hay un recuadro claramente visible 2 para completar el primer factor de autorización 2A, es decir, la primera parte de la información que se necesita para controlar la cantidad de moneda digital utilizada para respaldar el medio. No es importante de qué manera se añade el primer factor de autorización 2A: se puede imprimir en el medio, pegarse, escribirse a mano, grabarse, perforarse, quemarse con láser, cortarse, etc.

El primer factor de autorización 2A no necesita estar protegido por características de seguridad, solo debe ser legible y razonablemente duradero y resistente para el propósito de pagos físicos. Por lo tanto, el recuadro 2 para completar el primer factor de autorización 2A no requiere ninguna tecnología especial.

El elemento se muestra en las figuras 14, 15 y 16.

Recuadro 3 para firma digital 3A

En el medio de claves de cifrado para moneda digital, hay un recuadro 3 claramente visible para completar la firma digital 3A. No es importante de qué manera se añade la firma digital 3A: se puede imprimir en el medio, pegar, escribir a mano, grabar, perforar, grabar con láser, cortar, etc.

La firma digital 3A no necesita estar protegida por características de seguridad, solo debe ser legible y razonablemente duradera y resistente para fines de pagos físicos. Por lo tanto, el recuadro 3 para rellenar la firma digital 3A no requiere ninguna tecnología especial.

La firma digital 3A en este punto significa una representación física de los datos generados por la tecnología de firma digital. Los datos se pueden representar en sistema binario, octal, decimal, hexadecimal u otro sistema adecuado y formar una cadena alfanumérica legible a simple vista o gráficos legibles por máquina (código de barras, código QR), o ambos juntos.

En determinadas circunstancias, puede ser práctico combinar el primer factor de autorización 2A y la firma digital 3A en un único recuadro, y así simplificar el proceso de emisión y verificación de medio. Por lo tanto, esta versión del medio de claves de cifrado tiene solo un recuadro para completar ambas piezas de información a la vez como se muestra en la figura 14 y 16.

Segundo factor de autorización 5A

La segunda información que protege el respaldo de moneda digital se proporciona por el fabricante del medio y se denomina segundo factor de autenticación 5A. Dependiendo de si el segundo factor de autorización 5A está integrado en el medio, hay dos formas diferentes de realización.

a) Preferentemente, el segundo factor de autorización 5A se incorpora en un medio en forma de un recuadro protegido a prueba de manipulación para detectar de forma confiable la penetración, lo que en este caso sucede simplemente al leer el segundo factor de autorización. Por lo tanto, hay un objetivo de añadir el segundo factor de autorización 5A al medio de tal manera que una vez leído, habrá un cambio visible (evidente) del elemento, o todo el medio, en el sentido de que a primera vista parecerá devaluado. Un ejemplo podría ser boletos raspables o pegatinas destructivas utilizadas por las corporaciones bancarias para enviar PIN a tarjetas de pago por correo. Opcionalmente, el segundo factor de autorización 5A se puede encapsular dentro del cuerpo de un medio de pago de modo que sea necesario desmontar/dividir los medios en dos partes para leerlo. Este enfoque se utiliza en la Literatura 7. Es importante que el proceso de modificación sea irreversible y fiable, es decir, que no se eluda la información obtenida sin una modificación/devaluación evidente del medio al mismo tiempo, ni siquiera mediante tecnologías físicas o químicas sofisticadas.
Si un medio de claves de cifrado para moneda digital contiene el segundo factor de autorización 5A en forma de un recuadro a prueba de manipulación, no hay necesidad de un intermediario para un cambio inverso de la moneda de la representación física a la electrónica, y el último titular puede canjear los fondos utilizados para respaldar el medio utilizando solo un teléfono móvil o tableta "inteligente" con el equipo SW relevante y una conexión a Internet. Al mismo tiempo, esta opción de solución es técnica y financieramente más exigente para los fabricantes de medios.

b) Más simple, así como más barato para producir puede ser la opción de solución donde el segundo factor de autorización no está integrado en el medio de claves de cifrado, pero todo el tiempo se conoce solo por el fabricante del medio. Al mismo tiempo, sin embargo, el fabricante se convierte en la única entidad que es capaz de cambiar la representación física de la moneda digital (un medio de claves de cifrado) de nuevo a una representación electrónica, es decir, para canjear el respaldo. De hecho, esto significa que si un titular actual de un medio debidamente emitido (respaldado) decide cambiar la representación de la moneda física a la forma electrónica, debe devolver el medio al fabricante para recibir los fondos relevantes. Al mismo tiempo, el fabricante debe garantizar que el medio retirado sufrirá una destrucción definitiva.

La necesidad de devolver el medio al fabricante para cancelar el respaldo hace que este modelo sea logística y procedimentalmente desafiante, y al mismo tiempo el fabricante se convierte en el punto central para posibles ataques de falsificadores, sin embargo, este modelo elimina los costos de las tecnologías a prueba de manipulación, lo que puede hacer que la producción de medios físicos de claves de cifrado sea significativamente más barata.

Denominación

El medio de claves de cifrado para moneda digital en un estado respaldado siempre debe contener una información claramente legible 4 sobre la denominación y la unidad monetaria, o el nombre de la moneda en sí.

El medio se puede producir ya con esta información y comercializar en varias denominaciones diferentes, o la elección del valor nominal puede permanecer con el emisor (de manera similar a los cheques). En ese caso, el medio debe ofrecer un recuadro adecuado para completar esta información (figura 16).

Diseño de elementos

Dentro del medio de claves de cifrado para moneda digital, los elementos se distribuyen de acuerdo con la ergonomía de uso, en tanto que se tiene en cuenta en particular el procedimiento de verificación de medio, que se supone que es la actividad más común realizada con un medio. En segundo lugar, también se tienen en cuenta los procedimientos de emisión y devaluación. Sin embargo, teóricamente, la disposición particular de los elementos no es importante ya que el núcleo de la presente invención no se ve afectado, por ejemplo, una realización de papel (figura 15) no necesita tener todos los elementos colocados en el lado facial, pero ambas cajas para imprimir se pueden mover al lado opuesto. Existe una amplia gama de posibles modificaciones.

El resumen de innovación

La naturaleza del medio físico de las claves de cifrado y la transferencia de las claves de cifrado de moneda digital a través del proceso de emisión, validación y devaluación del medio físico con autorización multifactorial

El medio propuesto de claves de cifrado para moneda digital es de la siguiente naturaleza:

1. Esta representación física de la moneda digital es muy difícil de falsificar.
2. Un titular actual está en una posición exclusiva para controlar la moneda digital utilizada para respaldar un determinado medio. En otras palabras, ninguno de los titulares anteriores ni el fabricante se pueden apropiar indebidamente del respaldo.
3. El respaldo (emisión) del medio físico es fácilmente factible utilizando equipos de computadora y oficina comúnmente disponibles y una conexión a Internet.
4. La verificación del medio físico es fácilmente factible utilizando equipos de computadora móviles y software preinstalado comúnmente disponibles, incluso sin conexión a Internet.
5. En caso de que un medio físico también contenga el segundo factor de autorización en un modo a prueba de manipulación, cualquiera puede cancelar el respaldo y canjear los fondos utilizando equipo de computadora (móviles) comúnmente disponibles y acceso a Internet, pero la devaluación /daño evidente al medio ocurrirá al mismo tiempo.

En comparación con los productos físicos actuales destinados a preservar el equilibrio de las monedas digitales, la invención significa un gran salto cualitativo hacia adelante, debido principalmente a los puntos 2 y 4 de este capítulo.

En comparación con los medios de pago actualmente disponibles como productos de bancos y estados (billetes, monedas, cheques), la presente invención también aporta una innovación fundamental. Los medios de pago comúnmente disponibles se basan en la confianza directa (figura 5), y si la confianza en sus fabricantes se desvanece, los instrumentos de pago pierden inmediatamente su función y valor. El titular no puede controlar directamente (fácticamente) el respaldo relevante de un determinado instrumento de pago. Las posiciones del titular y del fabricante no son iguales, por lo tanto, en caso de quiebra del fabricante o de una reforma monetaria, el titular generalmente pierde el valor total representado por estos sustitutos.

Por el contrario, la presente solución técnica da nacimiento a un medio de pago que conserva su valor independientemente de la situación económica del fabricante. En caso de que los medios físicos contengan también el segundo factor de autorización en un modo a prueba de manipulación, ni la quiebra ni la posible liquidación del fabricante pueden afectar el valor de los medios emitidos de claves de cifrado para la moneda digital como instrumentos de pago. Todavía se utilizan para almacenar el valor y facilitar los pagos.

Este medio de claves de cifrado para moneda digital lleva, a diferencia de los sustitutos monetarios mencionados, su valor intrínseco equivalente al saldo en la moneda digital. Este valor intrínseco es similar como si los medios de pago fueran directamente metales preciosos (oro, plata). Estas ofertas, generalmente monedas, también tienen sus valores intrínsecos, que son independientes de la entidad del fabricante.

El medio de claves de cifrado para moneda digital utilizado como medio de pago conserva las ventajas idénticas a los medios de pago físicos modernos convencionales: bajo peso y tamaño pequeño. Se introdujeron los billetes, entre otras razones, porque la manipulación con grandes cantidades de oro físico parecía poco práctica. Asimismo, el medio inventado de claves criptográficas representa una herramienta que debería facilitar los pagos a personas para las que la manipulación con moneda digital en su forma electrónica nativa no es práctica. Al mismo tiempo, sin embargo, conserva su valor intrínseco, por lo que no es un sustituto, sino más bien un "sobre" físico para una moneda electrónica.

La presente invención se puede ver como un instrumento para la metamorfosis de la moneda digital desde el mundo electrónico al mundo físico y viceversa (figura 11), con un hecho importante de que una vez que la moneda se transfiere al mundo físico, ya no hay nadie que pueda usarla en el mundo electrónico original. De esta manera se puede describir el mencionado principio de control exclusivo de un titular actual. Los productos físicos actuales relacionados con las monedas digitales, es decir, utilizan el diagrama de la figura 6, es decir, hay dos entidades para controlar los medios de pago en el momento de su emisión, el fabricante y el titular. Por lo tanto, en cualquier momento en el futuro, puede ocurrir la situación que se muestra en la figura 10, es decir, el "titular electrónico" continúa utilizando los recursos financieros y el "titular físico" descubre, cuando intenta devaluar el objeto y transferir el respaldo nuevamente al entorno electrónico, que ya no es el titular actual, y que se le había robado.

La metamorfosis entre la representación electrónica y física del dinero se realiza regularmente al llevar efectivo al banco/cajero automático y depositarlo en la cuenta o, a la inversa, al retirar dinero de una cuenta en un banco/cajero automático y llevarlo a casa como efectivo.

La presente invención permite realizar esta metamorfosis en la comodidad del hogar y sin un intermediario (banco). Con la cantidad necesaria de piezas no respaldadas de los medios descritos de claves de cifrado para la moneda digital, y mediante equipos comunes de computadora y oficina y una conexión a Internet, la representación electrónica de la moneda se puede cambiar a la física. En el caso de medios físicos con el segundo factor de autorización 5A en un modo a prueba de manipulación, también es posible un cambio en la dirección opuesta, con solo una conexión a Internet y un teléfono móvil inteligente o tableta.

Al mismo tiempo, la invención presentada no carece de la función secundaria de un almacenamiento seguro sin conexión de moneda digital, es decir, puede reemplazar billeteras de papel y otras formas de respaldos de claves privadas. Por lo tanto, incluso si no se utiliza en el sistema de pago, conserva su función como un depósito de valor.

Opciones de solución

(1) Los medios físicos de claves de cifrado para moneda digital pueden perder la parte de la firma digital 3A, es decir, en una situación en la que solo el destinatario del instrumento de pago tiene una conexión a Internet, no el pagador, por ejemplo, en tanto que compra en una tienda física. El destinatario puede poseer una terminal conectada a Internet y utilizarla para verificar directamente el respaldo de piezas individuales de un medio de pago.
(2) En determinadas circunstancias, puede ser preferible dejar el segundo factor de autorización al fabricante, pero integrar una "contraseña" secreta a prueba de manipulación en el soporte, lo que demostrará a distancia que la parte comunicante es el beneficiario efectivo del instrumento de pago. Por lo tanto, esta modificación requiere la cooperación del fabricante incluso en el canje del respaldo, pero puede tener lugar a distancia sin un contacto físico del fabricante con los medios de pago. Hay algunas motivaciones para optar por esta opción, por ejemplo, reducir el volumen de información protegida en un modo a prueba de manipulación en caso de que los costos de producción y/o la vulnerabilidad aumenten con el volumen de información protegida y todo el segundo factor de autorización criptográficamente fuerte sea difícil de integrar.
(3) Los medios emitidos también pueden estar respaldados teóricamente por un tercero. Durante el proceso de emisión, la entidad emisora debe informar a este tercero sobre la dirección para depositar los fondos y luego obtener el identificador de esta transacción. El respaldo también se puede proporcionar por el fabricante porque en ciertos casos puede acelerar el proceso de emisión, más precisamente el proceso de generación de la firma digital 3A. Esta modificación se basa en la presunción de que el emisor había depositado previamente una cierta cantidad de dinero por parte del fabricante, que luego se retira mediante la emisión de medios de pago, es decir, una cierta forma de fondos predepositados.
(4) La protección contra la falsificación de medios de claves de cifrado para moneda digital se podría mejorar significativamente teóricamente al usar una tecnología llamada función física inclonable (PUF), que actualmente es el nombre colectivo para las tecnologías utilizadas para producir un objeto que no se puede copiar, duplicar o falsificar funcionalmente (Literatura 10, 11, 12, 13) incluso mediante las tecnologías físicas y químicas más avanzadas. Las cualidades únicas se logran mediante la producción de un dispositivo electrónico con cualidades electromagnéticas únicas que se derivan de la disposición de moléculas y átomos, y por lo tanto es técnicamente imposible hacer una copia idéntica. En realidad, significaría equipar el medio de claves de cifrado para moneda digital con un chip electrónico con implementación PUF, y así reemplazar el identificador alfanumérico único 1 descrito en el texto anterior. Para esta opción sería natural utilizar el formulario electrónico también para completar el primer factor de autorización 2A y la firma digital 3A por parte del emisor, es decir, se podría integrar un chip de memoria regrabable. Una mayor protección de los medios de pago contra la falsificación se vería compensada por mayores demandas en el equipo del verificador, ya que tendría que utilizar equipos más avanzados para comunicarse con la electrónica incorporada en el medio de claves de cifrado para moneda digital. Por lo tanto, el producto resultante no sería tan universalmente aplicable. Al mismo tiempo, se plantearían otras cuestiones y problemas relacionados con la aplicación, ya que el área de tarjetas de pago de contacto y sin contacto equipadas con un chip es conocida por una gran cantidad de ataques potenciales y vulnerabilidad.

Aplicabilidad industrial

La transferencia de claves de cifrado de moneda digital a través del proceso de emisión, validación y devaluación de medio físico con autorización multifactorial y el medio físico de claves de cifrado de moneda digital para realizar esta tecnología de transferencia son aplicables en el área de preservación y transferencia de valores en el sistema de pago.

La literatura utilizada en textos y otras fuentes de información

Literatura 1. Bitaddress. [En línea] https://www.bitaddress.org.
Literatura 2. BitcoinPaperwallet.com. [En línea] https://bitcoinpaperwallet.com/.
Literatura 3. Wallet Generator. [En línea] https://walletgenerator.net.
Literatura 4. BIP 38: Passphrase-protected private key. [En línea]https://github.com/bitcoin/bips/blob/master/bip-0038.mediawiki.
Literatura 5. OVD Kinegram AG. [En línea] http://www.kinegram.com/.
Literatura 6. Soheil Hamedani, Gregor Innitzer. Coin having integrated rfid identification device and method for the production thereof. US 20120055996 3 8, 2012.
Literatura 7. Swiss Bitcoin Certificates. [En línea] https://www.bitcoinsuisse.ch/en/about-certificates/.
Literatura 8. Shamir, Adi. How to share a secret. Communications of the ACM. 1979, Vol. 22. Literatura 9. BIP 16: Pay to Script Hash. [En línea] https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki.
Literatura 10. Christoph, Böhm, Maximilian, Hofer. Physical Unclonable Functions in Theory and Practice. Lugar desconocido: Springer, 2012.
Literatura 11. Pappu, R., et al. Physical one-way functions. Science. 2002, 297.
Literatura 12. Naccache David, Frémanteau Patrice. Unforgeable identification device, identification device reader and method of identification. EP0583709 1992.
Literatura 13. Roel, Maes. Physically Unclonable Functions: Constructions, Properties and Applications. Lugar desconocido: Escuela de Doctorado en Ciencias, Ingeniería y Tecnología de Arenberg, 2012.
Literatura 14. Feigelson, Douglas. Creating and using digital currency. US 20130166455 6 27, 2013.

Signos de referencia:

1	Identificador alfanumérico
2	Recuadro para rellenar el primer factor de autorización
2A	El primer factor de autorización
3	Recuadro para rellenar la firma digital
3A	Firma digital
4	Información sobre la denominación y la unidad monetaria
5	Recuadro para rellenar el segundo factor de autorización
5A	El segundo factor de autorización
6	Recuadro para rellenar la denominación
7	Símbolo de la moneda digital

REIVINDICACIONES

1. Un método de transferencia de claves de cifrado de moneda digital al menos entre un primer titular y un siguiente titular, incluso repetidamente, a través de un proceso de emisión, validación y devaluación de un medio físico con una autorización multifactorial, el medio físico se distribuye en el mercado como blanco, es decir, sin respaldo, y a él pertenece un segundo factor de autorización (5A), el segundo factor de autorización (5A) que se almacena de forma segura con el fabricante del medio físico o se integra en el medio físico en forma de un recuadro a prueba de manipulación;
el método que comprende:

respaldar el medio físico por el primer titular usando una aplicación SW,
donde la aplicación SW está adaptada para la emisión, es decir, el respaldo del medio físico de claves de cifrado por la moneda digital, y también está adaptada para comunicarse con un servicio en línea para la emisión de firmas digitales, generando un primer factor de autorización (2A) por el primer titular;
con base en el primer factor de autorización (2A) y en un identificador del medio físico, una dirección final a la que se va a depositar el saldo de moneda digital con la intención de respaldar este medio físico se deriva de la aplicación SW y se pasa al primer titular;
el primer titular envía el saldo de la moneda digital en una cantidad equivalente a la denominación del medio físico a la dirección final y luego, a través del servicio en línea para la emisión de firmas digitales, el primer titular recibe la firma digital previa solicitud después de cumplir todos los requisitos sobre la autenticidad del medio físico y si la suma transferida del saldo de moneda digital es igual a la denominación del medio físico, luego el primer titular combina la firma digital con el primer factor de autorización utilizando la aplicación de software para la emisión de medio físico y añade estos datos al medio físico mediante impresión, escritura a mano o como una pegatina y, por lo tanto, el medio físico se activa y se puede pasar a un siguiente titular, el siguiente titular realiza una inspección visual de las características de protección contra falsificación presentes en el medio físico para asegurar que el medio no es falso, es decir, mediante la inspección visual de una recuadro (2) para el primer factor de autorización (2A) y un recuadro (3) para la firma digital (3A) y luego verifica el respaldo del medio físico utilizando una aplicación de software para la verificación de medio físico para verificar el saldo de moneda digital;
luego esta aplicación SW verifica la autenticidad de la firma digital (3A) después de cargar el primer factor de autorización (2A) y la firma digital (3A), se valida el primer factor de autorización (2A) y el siguiente titular que desea canjear el respaldo del medio físico compara los datos firmados digitalmente con los datos visibles en el medio físico y luego se cargan, utilizando una aplicación de software para el canje de la moneda digital, todos los factores de autorización (2A y/o 5A) disponibles en este medio físico en estado activo, posiblemente añade otros factores de autorización conocidos por él, y compila y autoriza una transacción electrónica en la red de moneda digital para canjear fondos en forma electrónica a una dirección privada del próximo titular que desea canjear el respaldo del medio físico que da como resultado la transferencia de claves de cifrado de moneda digital a través del proceso de emisión, validación y devaluación del medio físico con autorización multifactorial, y efectuando así una transacción de pago por moneda digital entre el primer titular y el siguiente titular que quiera canjear el respaldo del medio físico y como parte del resultado el medio físico también está visiblemente devaluado.

2. El método de acuerdo con la reivindicación 1, donde el siguiente titular que desea canjear el respaldo del medio físico es el fabricante original del medio físico, que utiliza para la compilación y autorización de la transacción en moneda digital también otros factores de autorización no presentes en el medio físico y conocidos solo por él.

3. El método de acuerdo con la reivindicación 1, donde la aplicación SW para emisión de medio físico, la aplicación SW para verificación de medio físico y la aplicación SW para el canje de los fondos de moneda digital son aplicaciones de código abierto, accesibles públicamente en Internet.

4. El método de acuerdo con la reivindicación 1 o 2, donde la aplicación SW para emisión de medio físico, la aplicación SW para verificación de medio físico y la aplicación SW para el canje de los fondos de moneda digital de hecho solo forman una aplicación SW.

5. Un sistema adaptado para realizar el método de la reivindicación 1,
donde el medio físico está hecho de un cuerpo base plano de cualquier forma y materiales compactos, una de las superficies planas principales del cuerpo base plano que está provista de un identificador alfanumérico único (1) para su identificación y contiene características de protección contra la falsificación; una o ambas superficies planas principales del cuerpo plano del medio físico que tienen un recuadro (2) para recibir el primer factor de autorización (2A) y un recuadro (3) para añadir la firma digital (3A).

6. El sistema de acuerdo con la reivindicación 5, donde el cuerpo base en forma de un objeto plano tiene la forma de un cuadrado, rectángulo o círculo.

7. El sistema de acuerdo con la reivindicación 5 o 6, donde el medio tiene la forma de tarjetas de crédito estándar, monedas o billetes.

8. El sistema de acuerdo con la reivindicación 5, donde el medio lleva a cada lado información (4) sobre la denominación y unidad monetaria.

9. El sistema de acuerdo con la reivindicación 5, donde las aplicaciones de características de protección contra falsificación en caso de una realización de papel son papel de seguridad con marcas de agua o tiras metálicas, elementos ópticamente variables, elementos gráficos muy finos llamados guillochés, gradaciones de color de iris, colores con luminiscencia UV o IR, colores de reactivos químicos.

10. El sistema de acuerdo con la reivindicación 5, donde las aplicaciones de características de protección contra falsificación en caso de realización en tarjetas de plástico son principalmente hologramas.

11. El sistema de acuerdo con la reivindicación 5, donde las aplicaciones de las características de protección contra falsificación en caso de realización en monedas de metal son elementos de seguridad difractivos (kinegramas) o chips RFID electrónicos.

12. El sistema de acuerdo con la reivindicación 5, donde el identificador alfanumérico único (1) se convierte en un elemento asegurado, es decir, revestido con barniz iridiscente, perforado o como un elemento ópticamente variable.

13. El sistema de acuerdo con la reivindicación 5, donde el recuadro (2) para recibir el primer factor de autorización (2A) y el recuadro (3) para agregar la firma digital (3A) forman de hecho un recuadro compartido.

14. El sistema de acuerdo con la reivindicación 5, donde cualquiera de las superficies de plano principales lleva otro recuadro (5) para el segundo factor de autorización (5A) en un modo a prueba de manipulación.

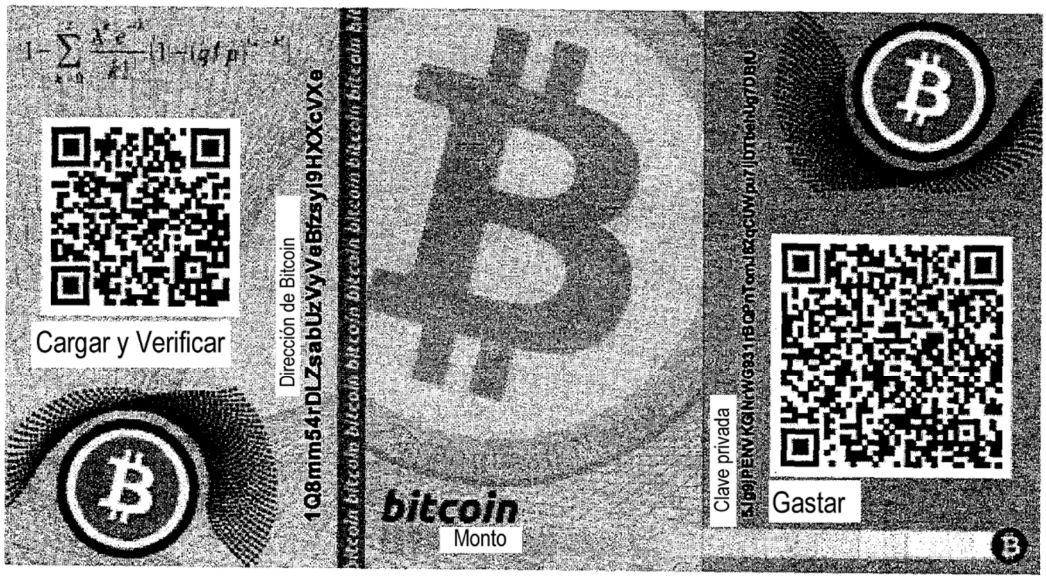
Cargar y Verificar
Dirección de Bitcoin
1Q8mm54rDLZsabUzVyVaBrzsyj9HXGcVXe
bitcoin
Monto
Clave privada
Gastar

Fig. 1


฿1
bitbills
bitbills beta
dirección
bitbills.com
contiene 1 bitcoin // no aceptar si la tarjeta se ha abierto // v0 07
฿5
bitbills
bitbills beta
dirección
bitbills.com
contiene 5 bitcoins // no aceptar si la tarjeta se ha abierto // v0 07
฿10
bitbills
bitbills beta
dirección
bitbills.com
contiene 10 bitcoins // no aceptar si la tarjeta se ha abierto // v0 07
฿20
bitbills
bitbills beta
dirección
bitbills.com
contiene 20 bitcoins // no aceptar si la tarjeta se ha abierto // v0 07

Fig. 2

Fig. 3

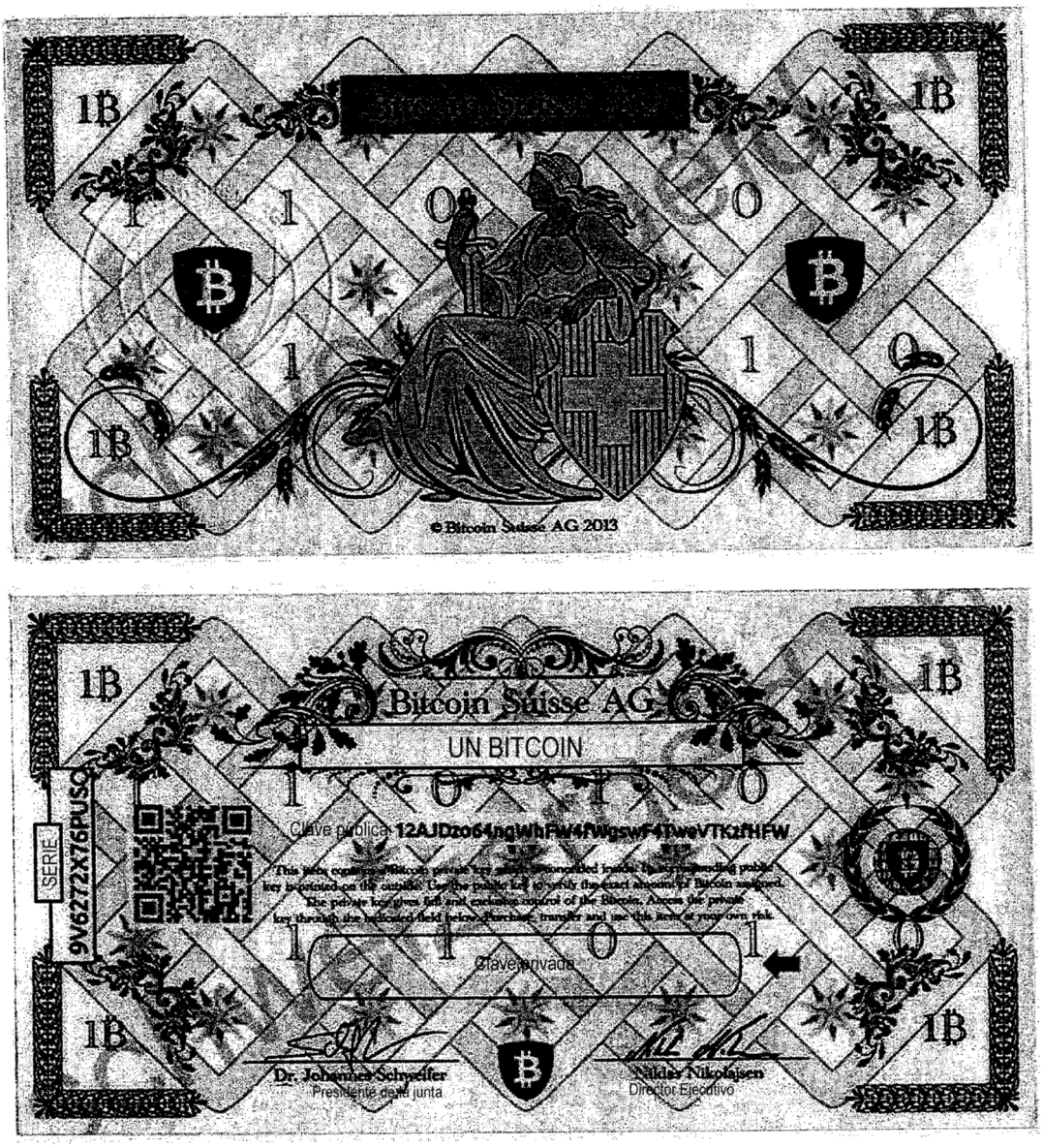
1Ƀ
1Ƀ
1Ƀ
1Ƀ
© Bitcoin Suisse AG 2013
Bitcoin Suisse AG
UN BITCOIN
SERIE
9V6Z72X76PUSO
Clave pública 12AJDzo64ngWhFw4fWgswF4TweVTKzfHFW
Clave privada
Dr. Johannes Schneider
Presidente de la junta
Niklas Nikolajsen
Director Ejecutivo

Fig. 4

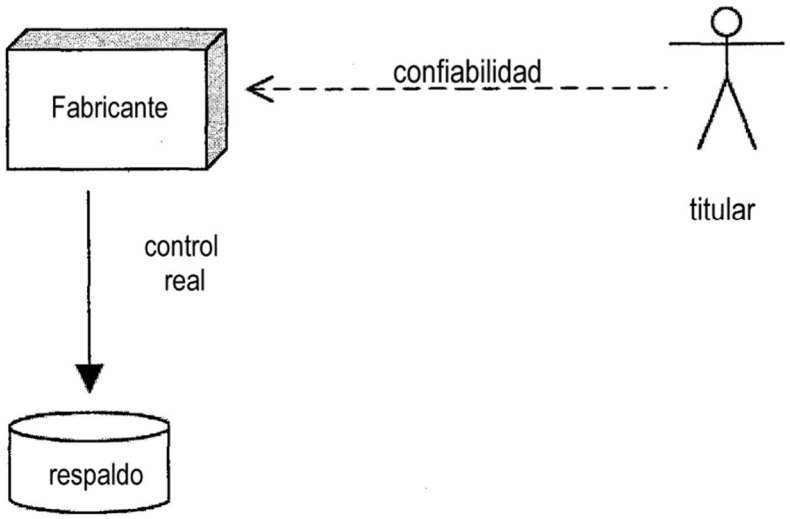
Fabricante
confiabilidad
titular
control
real
respaldo

Fig. 5

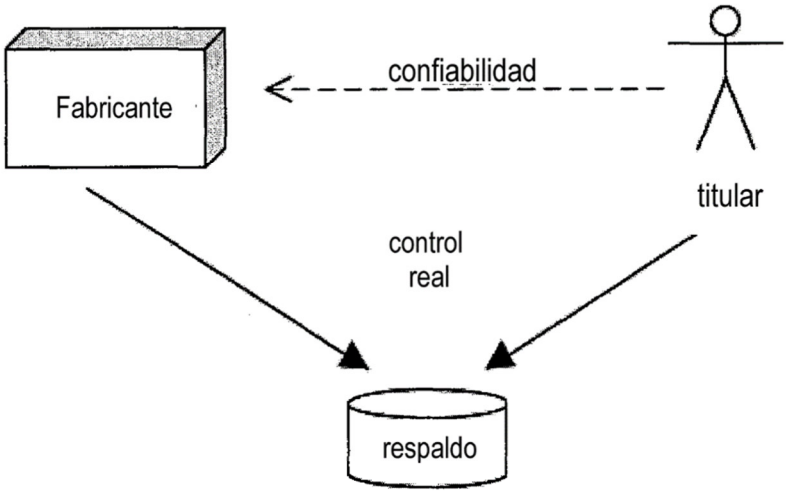
Fabricante
confiabilidad
titular
control
real
respaldo

Fig. 6

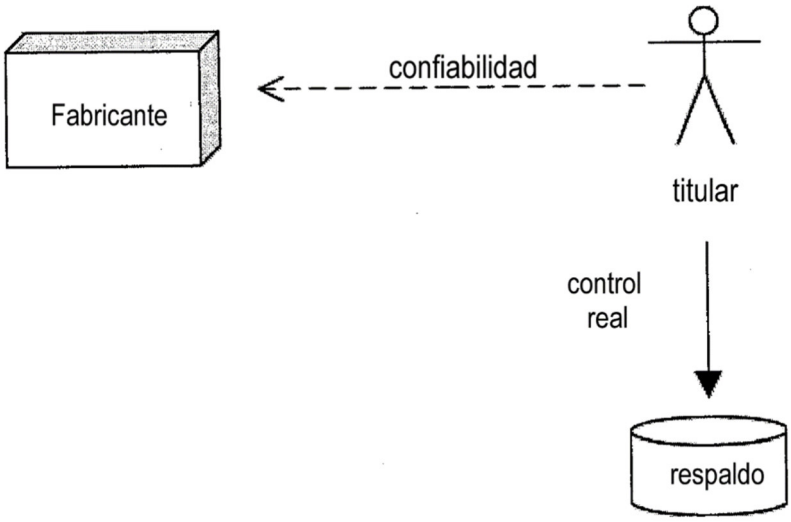
Fabricante
confiabilidad
titular
control
real
respaldo

Fig. 7

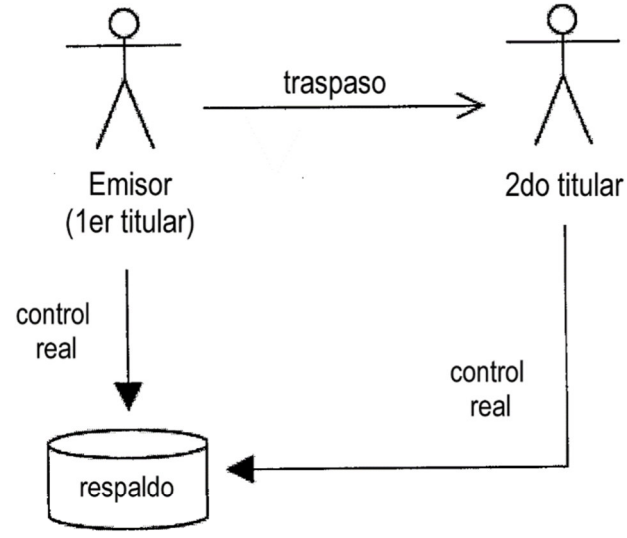
traspaso
Emisor
(1er titular)
2do titular
control
real
control
real
respaldo

Fig. 8

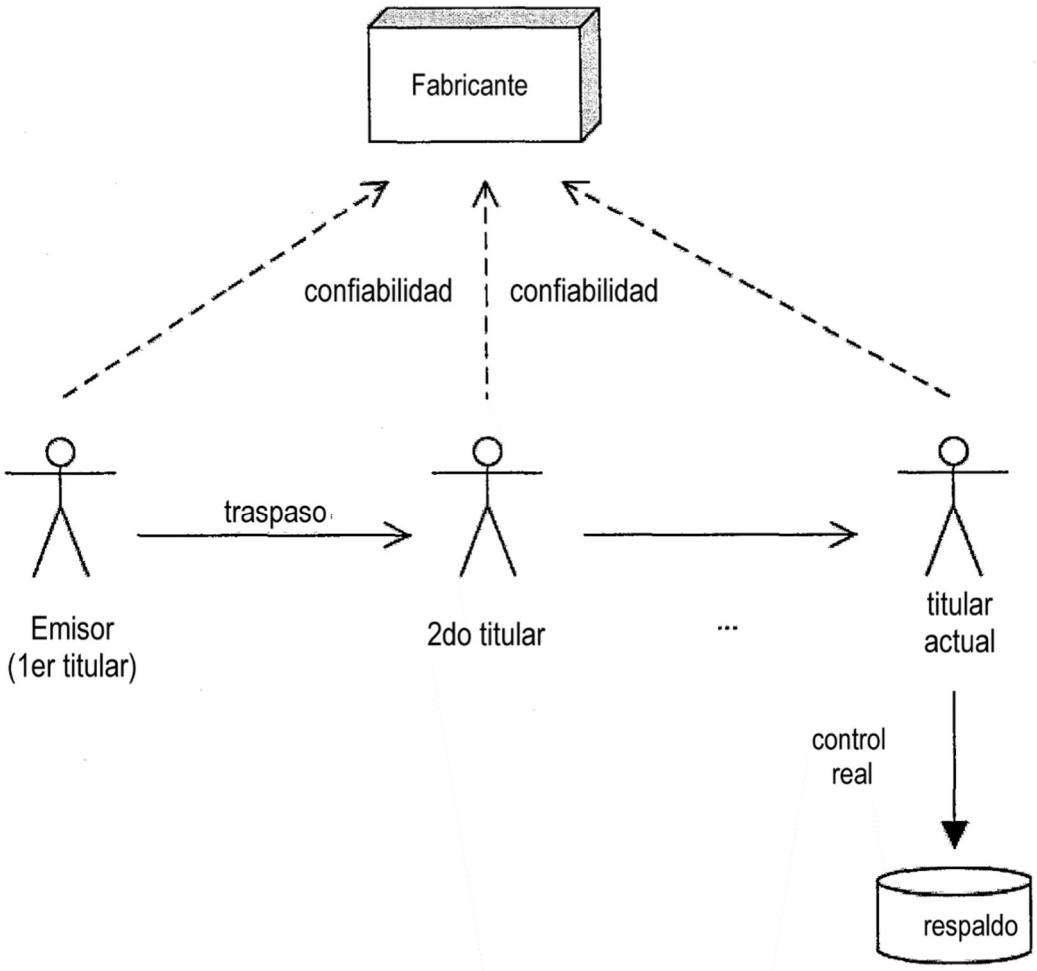
Fabricante
confiabilidad
confiabilidad
traspaso
Emisor
(1er titular)
2do titular
...
titular
actual
control
real
respaldo

Fig. 9

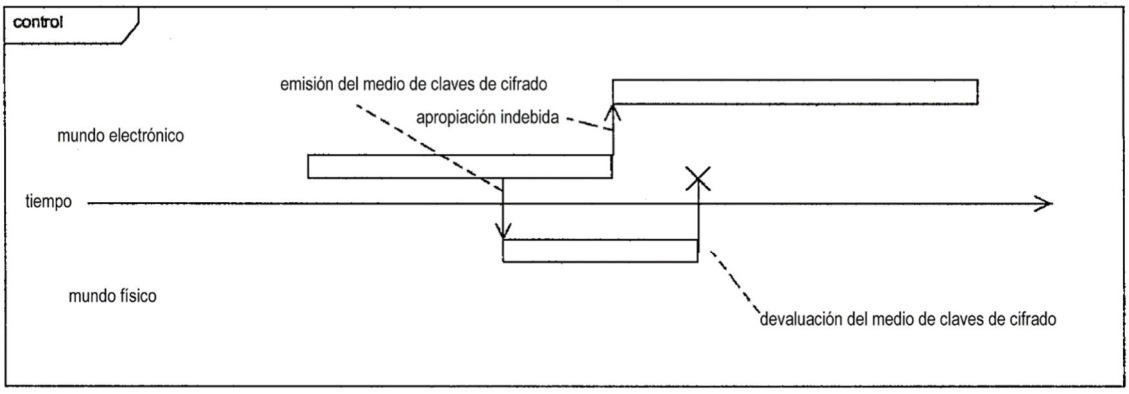
control
emisión del medio de claves de cifrado
apropiación indebida
mundo electrónico
tiempo
mundo físico
devaluación del medio de claves de cifrado

Fig. 10

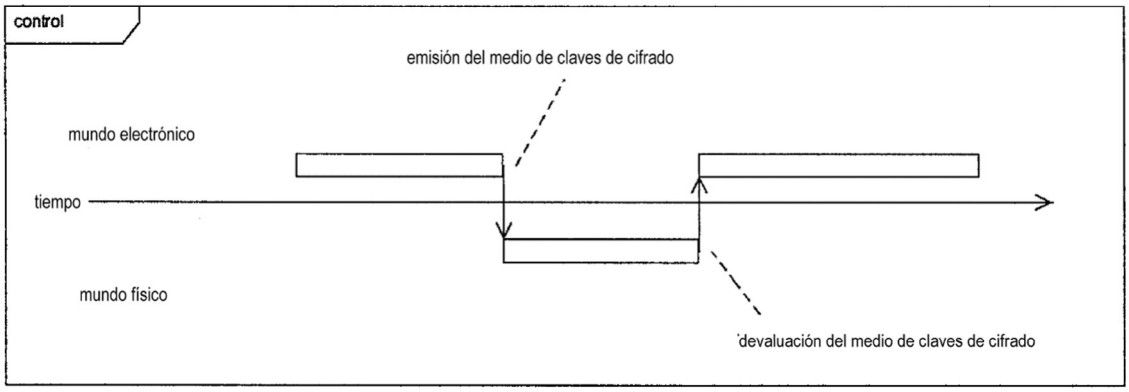
control
emisión del medio de claves de cifrado
mundo electrónico
tiempo
mundo físico
devaluación del medio de claves de cifrado

Fig. 11

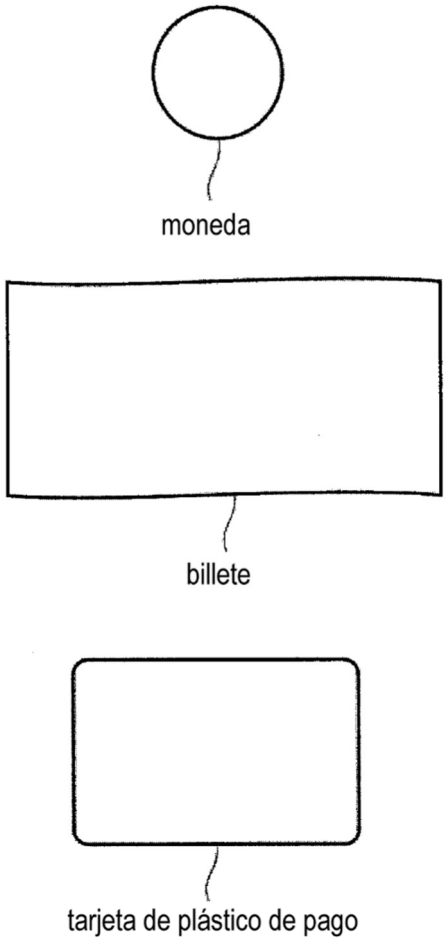

Fig. 12

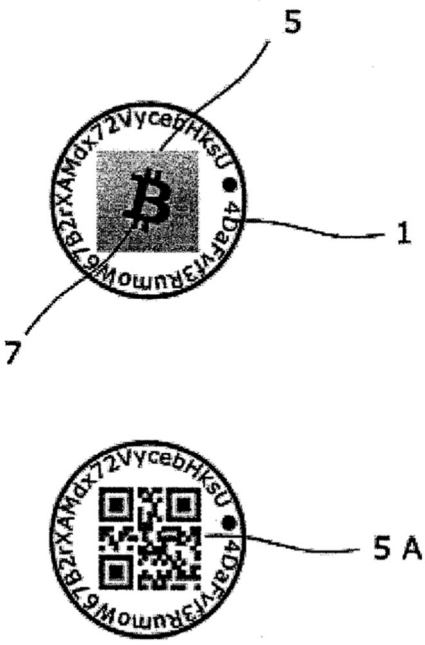

Fig. 13

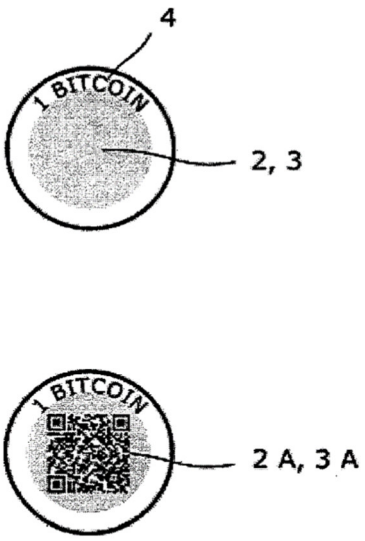

Fig. 14

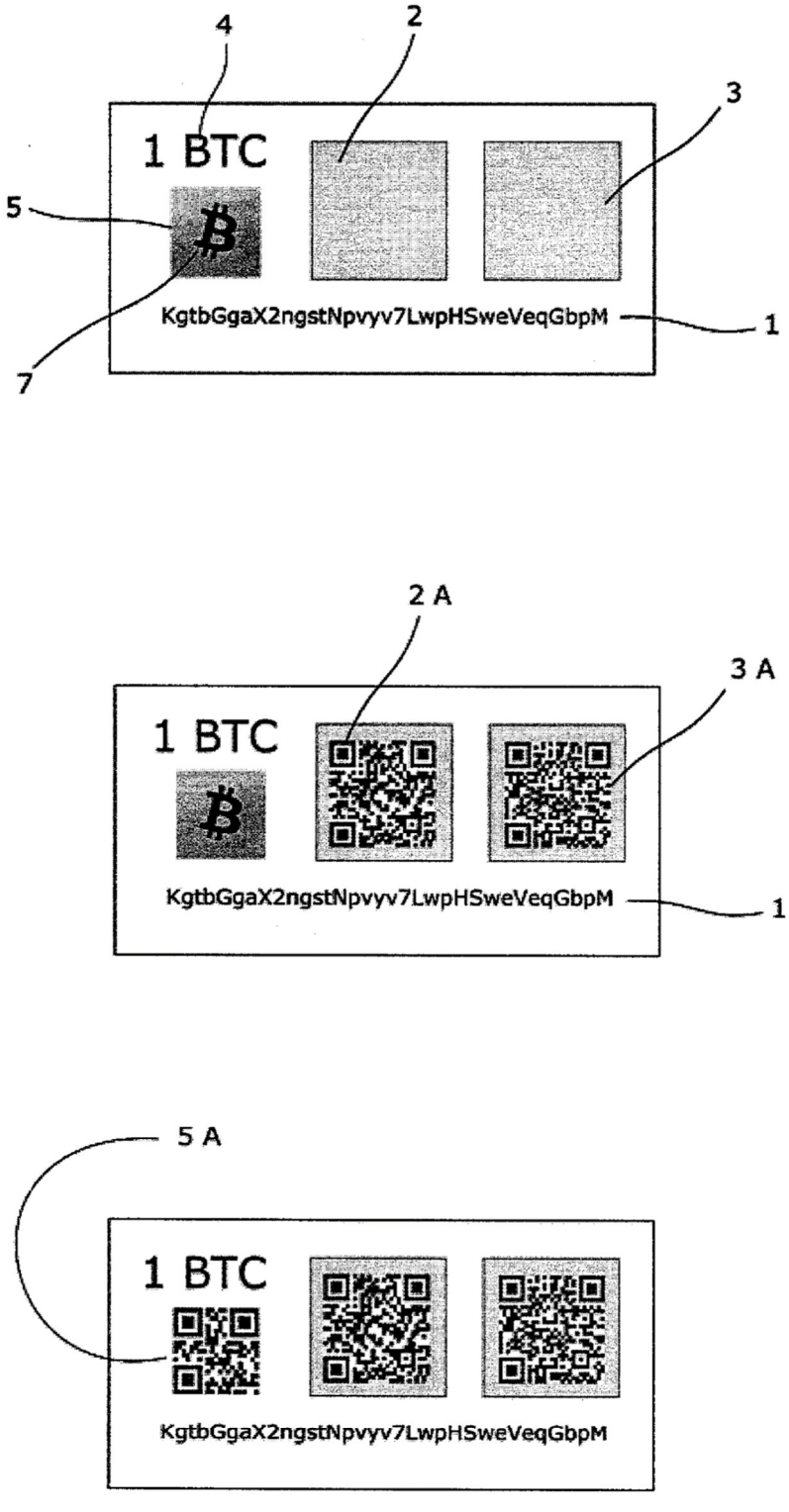
4
2
3
1 BTC
5
KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM
1
7
2 A
3 A
1 BTC
KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM
1
5 A
1 BTC
KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM

Fig. 15

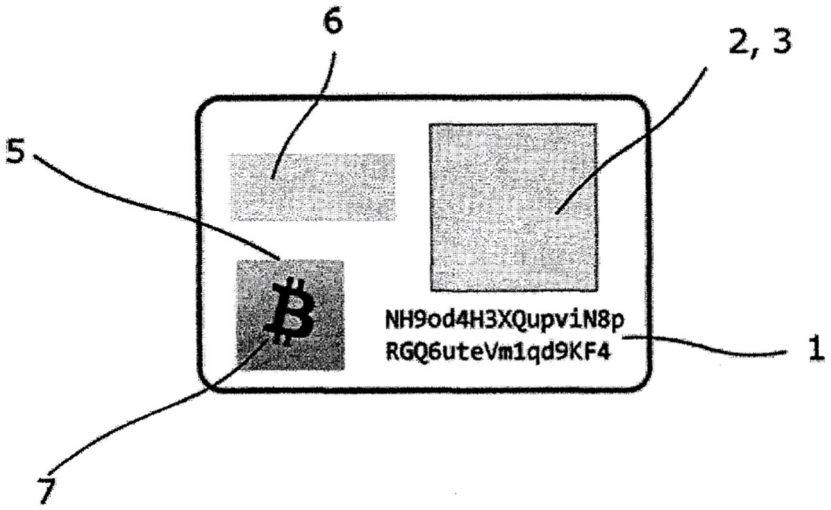
6
2, 3
5
NH9od4H3XQupviN8p
RGQ6uteVm1qd9KF4
1
7

Fig. 16

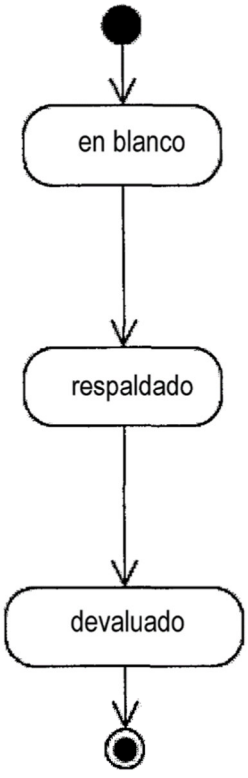
en blanco
respaldado
devaluado

Fig. 17

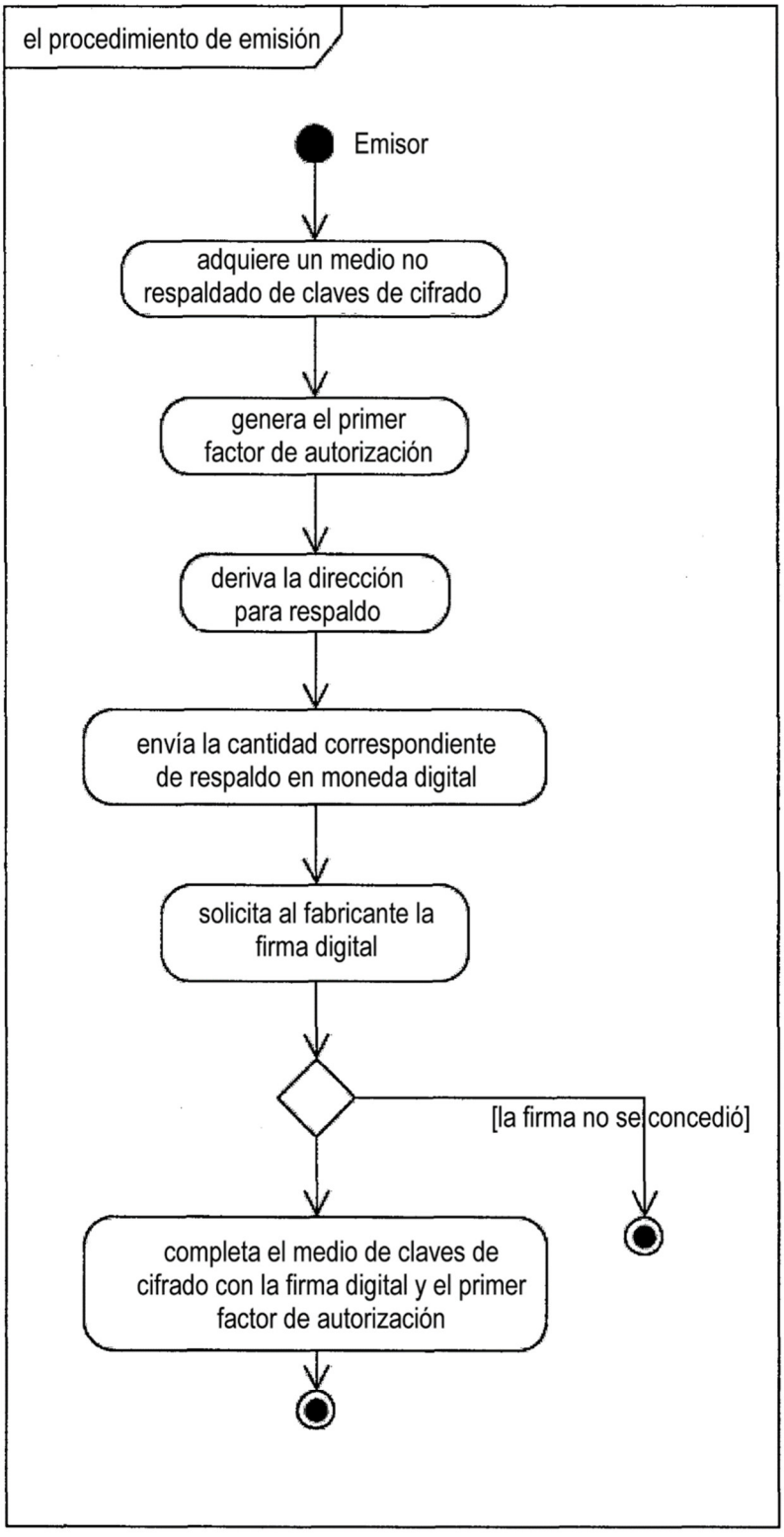
el procedimiento de emisión
Emisor
adquiere un medio no respaldado de claves de cifrado
genera el primer factor de autorización
deriva la dirección para respaldo
envía la cantidad correspondiente de respaldo en moneda digital
solicita al fabricante la firma digital
[la firma no se concedió]
completa el medio de claves de cifrado con la firma digital y el primer factor de autorización

Fig. 18

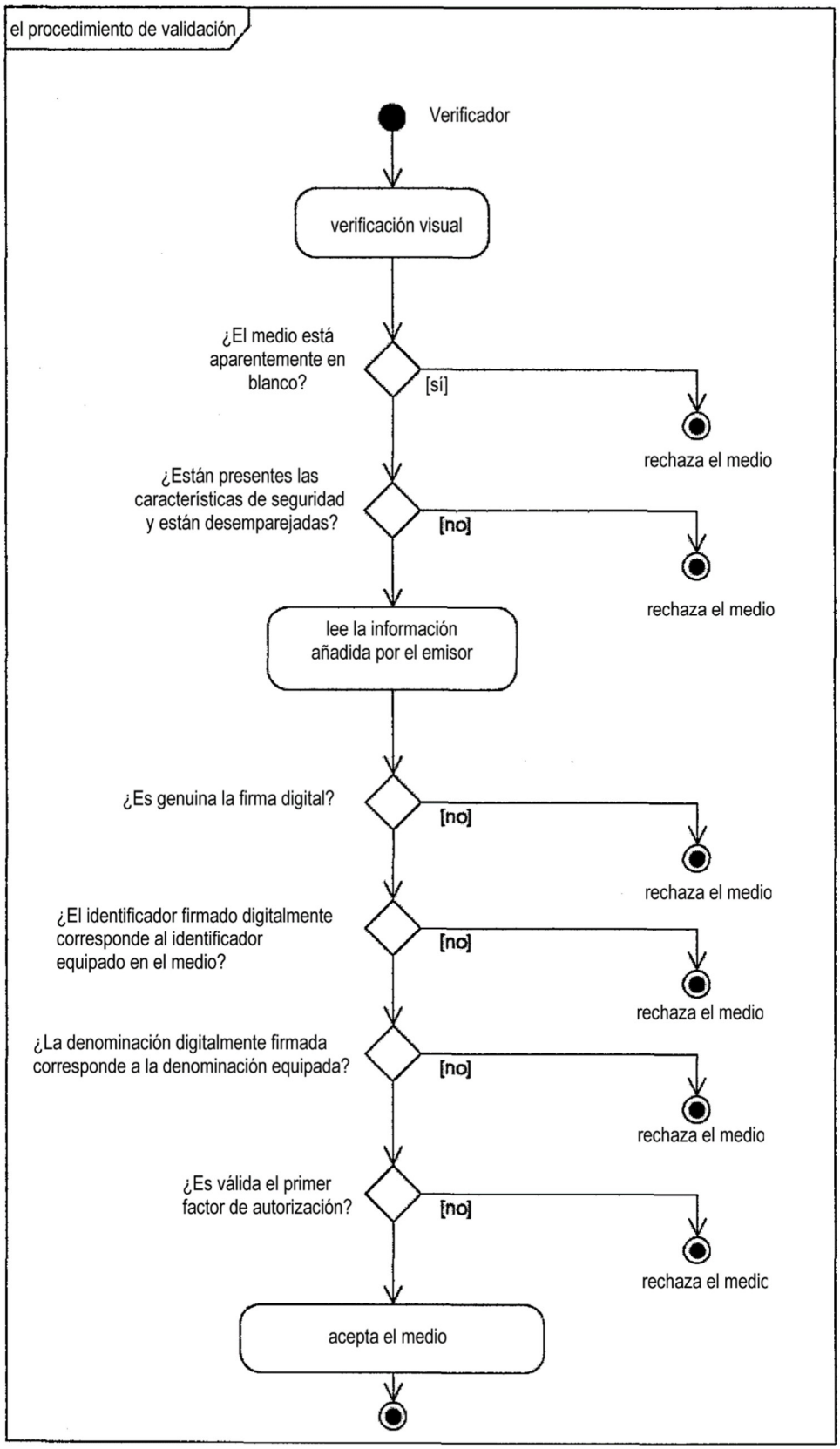
el procedimiento de validación
Verificador
verificación visual
¿El medio está aparentemente en blanco?
[sí]
rechaza el medio
¿Están presentes las características de seguridad y están desemparejadas?
[no]
rechaza el medio
lee la información añadida por el emisor
¿Es genuina la firma digital?
[no]
rechaza el medio
¿El identificador firmado digitalmente corresponde al identificador equipado en el medio?
[no]
rechaza el medio
¿La denominación digitalmente firmada corresponde a la denominación equipada?
[no]
rechaza el medio
¿Es válida el primer factor de autorización?
[no]
rechaza el medic
acepta el medio

Fig. 19

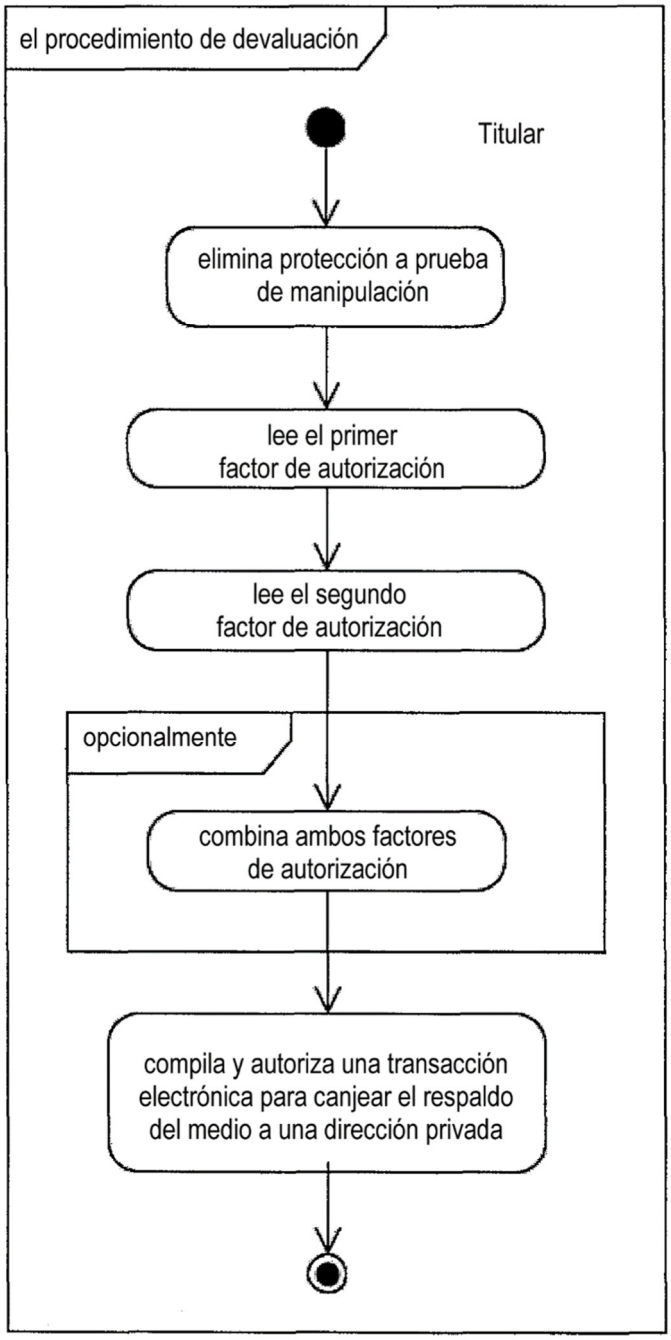
el procedimiento de devaluación
Titular
elimina protección a prueba de manipulación
lee el primer factor de autorización
lee el segundo factor de autorización
opcionalmente
combina ambos factores de autorización
compila y autoriza una transacción electrónica para canjear el respaldo del medio a una dirección privada

Fig. 20