(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 875 391**

(51) Int. CI.:

G06F 21/64 (2013.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
G06Q 30/00 (2012.01)
G06Q 50/18 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.03.2018 PCT/EP2018/056619**

(87) Fecha y número de publicación internacional: **20.09.2018 WO18167252**

(96) Fecha de presentación y número de la solicitud europea: **16.03.2018 E 18711920 (1)**

(97) Fecha y número de publicación de la concesión europea: **17.02.2021 EP 3596653**

(54) Título: **Expedición de documentos virtuales en una cadena de bloques**

(30) Prioridad:

17.03.2017 DE 102017204536

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.11.2021

(73) Titular/es:

BUNDESDRUCKEREI GMBH (100.0%)
Kommandantenstraße 18
10969 Berlin, DE

(72) Inventor/es:

RÜCKRIEMEN, JÖRG y
EHREKE, JENS

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Expedición de documentos virtuales en una cadena de bloques

La invención se refiere a un procedimiento para la expedición de un documento virtual en una cadena de bloques así como a un sistema para llevar a cabo el procedimiento.

Documentos tales como los certificados comprenden, en su mayoría, un cuerpo de documento, por ejemplo de papel, en el que se expiden y que pueden falsificarse fácilmente con modernos programas de procesamiento de imágenes e impresoras a color. En particular, el problema de la falta de protección contra la falsificación surge si, además de un original del documento, se requieren ejemplares adicionales, tales como fotocopias, duplicados y copias. Su autenticidad generalmente se verifica mediante legalización. Una legalización oficial es una certificación oficial que da fe de la exactitud de una fotocopia, duplicado, copia o similar de un documento. La legalización generalmente se basa únicamente en una breve inspección visual y ya por esta razón no es segura. A esto se añade que una legalización ya es correcta si la nota de legalización está provista de un sello oficial, por ejemplo, en forma de sello estampado, y si la persona que realiza la legalización ha firmado una nota de legalización. Una nota de legalización comprende, a este respecto, la afirmación de que la fotocopia/copia legalizada coincide con un documento original presentado. Además, la nota de legalización puede incluir una descripción precisa del documento original, cuya fotocopia/copia se está autentificando. Tal legalización también se puede falsificar fácilmente con programas modernos de procesamiento de imágenes.

Los procedimientos con un sello impreso legible por máquina en forma de código QR aumentan la seguridad, pero debido a la pequeña cantidad de datos que puede contener un código QR, solo se pueden usar para documentos a una cara con pocos datos.

Además, la aplicación de características de seguridad a los cuerpos de los documentos, por ejemplo, de papel, es logísticamente ineficaz. Las hojas en blanco con las características de seguridad adecuadas, como las que se utilizan para documentos de identidad o billetes de banco, deben distribuirse físicamente y protegerse contra el uso indebido o el robo. Además, los costes de implementación de las características de seguridad aumentan linealmente con el número de certificados. A este respecto, un principio fundamental de las características de seguridad utilizadas se basa en el hecho de que la seguridad se logra porque una copia 1:1 de las características de seguridad es demasiado cara y, por lo tanto, económicamente poco interesante. Después de todo, estos conceptos de seguridad no se pueden aplicar a los productos digitales.

El documento US 2016 / 0 261 685 A1 describe sistemas y procedimientos que hacen posible transmitir un mensaje independientemente de un recurso centralizado para su recuperación en un momento futuro. Un equipo informático recibe un mensaje relacionado con la configuración a través de una cadena de bloques gestionada por varios nodos descentralizados. El equipo, después de verificar la autenticidad del mensaje, ejecuta las instrucciones diferidas especificadas en el mensaje. Las instrucciones pueden permitir una funcionalidad o ninguna funcionalidad en el equipo. Las instrucciones indican que un paquete inteligente debe permitir al usuario final acceder al contenido del paquete o no permitir el acceso al contenido.

El documento WO 2016 / 170 538 A1 describe un sistema descentralizado y un procedimiento para gestionar documentos de título electrónicos (EDT). El procedimiento comprende: por parte de un nodo de salida: generar un objeto único raíz (RUO) asignado al nodo de salida y que se puede usar como puntero a una cadena de bloques administrada en la DTDB, con lo cual se inicia una cadena de propiedad para un EDT dado, que está caracterizada por un ID (RUOID) vinculado al RUO; e incrustar un objeto de datos con información sobre el RUOID en el EDT dado y firmar digitalmente el EDT con el objeto de datos incrustado de una manera que permita a un nodo autorizado verificar el EDT y extraer el objeto de datos, creando así un EDT generado; por parte de cada nodo actualmente en posesión del EDT generado: transferir la propiedad del EDT creado a un nodo receptor que será el próximo nodo en adquirir la propiedad del EDT creado, comprendiendo la transferencia de la propiedad: obtener la cadena de bloques un primer objeto único generado por un nodo que ha transferido la propiedad del EDT al primer nodo; usar el primer objeto único para generar un segundo objeto único que sea indicativo del primer objeto único, el nodo destinatario, y pueda agregarse a la cadena de bloques; permitir que el siguiente objeto único generado se agregue a la cadena de bloques; y reenviar el EDT generado al nodo destinatario a través de un medio digital; por parte de cada nodo, en respuesta a la obtención del EDT generado: validar el EDT generado recibido; usar un RUO_ID incrustado en el EDT generado para validar la cadena de propiedad; y transferir la propiedad del EDT creado al nodo destinatario.

El documento GB 2 539 430 A describe un sistema de cambio de moneda o de tokens digital y un procedimiento para codificar uno o más tokens digitales, comprendiendo el sistema una red de igual a igual (*peer-to-peer*) con una pluralidad de terminales de usuario operados por los respectivos usuarios y una pluralidad de servidores. Se instancia un correspondiente par de claves criptográficas con al menos una clave pública para cada usuario y servidor en el sistema. Cada usuario en el sistema registra su respectiva clave pública y un respectivo identificador único en al menos un servidor y solicita a este servidor la instanciación de uno o más tokens digitales. Los tokens digitales se instancian en el servidor y comprenden una pluralidad de códigos que definen una cadena de bloques. El servidor firma digitalmente tokens basándose en la pluralidad de códigos con su clave privada. Los tokens firmados digitalmente se

transmiten a la pluralidad de servidores remotos, donde la cadena de bloques del token transmitido se procesa en cada servidor para validar la transmisión. El procesamiento de la cadena de bloques comprende calcular un primer y un segundo *hash* y comparar el segundo *hash* con una firma digital. El token se instancia nuevamente cuando la cadena de bloques excede un determinado valor umbral.

El documento CN 106 412 037 A describe un procedimiento de procesamiento de archivos de seguridad electrónicos basado en una estructura de conexión de bloques. El procedimiento comprende las siguientes etapas: un nodo miembro en una conexión de bloques, que consta de un nodo principal y al menos un nodo miembro, crea una solicitud para generar un archivo de seguridad electrónico basándose en la ocurrencia de un evento desencadenante y envía la solicitud para generar el archivo de seguridad electrónico al nodo principal; el nodo principal genera un archivo de seguridad electrónico basándose en la solicitud de generación de archivo de seguridad electrónico recibida y transmite el archivo de seguridad electrónico generado al nodo miembro especificado por la solicitud de generación de archivo de seguridad electrónico.

El documento US 2016 / 0 212 146 A1 describe sistemas y procedimientos que utilizan una cadena de bloques (*blockchain*) para permitir la configuración de datos de archivo y la ausencia de manipulación, incluso para documentos confidenciales y para aquellos que se almacenan en entornos no controlados, pero para lo cual no se requiere confiar en una autoridad de sellado de fecha y hora o en un servicio de archivado de documentos. Se puede usar una autoridad de sellado de fecha y hora (TTSA) de confianza, pero incluso aunque la TTSA pierda su credibilidad o un impugnador se niegue a validar un sello de fecha y hora, aún se puede establecer una fecha para un documento electrónico. Se describen sistemas y procedimientos que permiten la detección de duplicaciones de archivos en grandes colecciones de documentos, lo que puede mejorar la búsqueda de documentos dentro de la gran colección.

El documento US 2017 / 0 033 932 A1 describe la ampliación de al menos un nodo en una infraestructura de verificación de árbol *hash* distribuida con un identificador de una entidad en una ruta de registro. Una firma de datos, que contiene parámetros para recalcular un valor de verificación y que está asignada a un registro de datos digitales de entrada también contiene, por lo tanto, datos que identifican al menos una entidad en la ruta del árbol *hash* que se utiliza para su registro inicial en la infraestructura. Un valor máximo de la infraestructura de verificación de árbol *hash* se introduce en una cadena de bloques como una transacción o como parte de una transacción.

El documento US 2016 / 0 330 035 A1 describe sistemas y procedimientos para gestionar la identidad de un usuario, para gestionar la identidad del usuario en un dispositivo de almacenamiento público y para certificar transacciones pendientes para un usuario. El procedimiento comprende recibir datos personales que identifican al usuario en un dispositivo de entrada. Los datos personales se representan como datos de entrada. El equipo de entrada está configurado de modo que procesa una función *hash* para proporcionar al dispositivo de almacenamiento público, por ejemplo, cadena de bloques, un valor *hash* y una interfaz accesible para el usuario para transmitir el valor *hash* y una clave pública del usuario, y para recibir del dispositivo de almacenamiento público un número de transacción correspondiente al valor *hash* y a la clave pública. El dispositivo de entrada está configurado para cifrar el valor *hash*, un sello de fecha y hora y el número de transacción con una clave pública de una unidad de certificación a fin de proporcionar a la unidad de certificación datos certificables por el usuario. La autoridad de certificación está configurada para acceder al dispositivo de almacenamiento público para verificar al usuario.

BERGMANN, Christoph: "Notare und Banken, Ausweise und Börsen" (Notarios y bancos, documentos de identidad y bolsas de valores), en Bitcoinblog, 8 de diciembre de 2015. URL: https://bitcoinblog.de/2015/12/08/notareundbanken-ausweise-und-boersen, describe proyectos que aplican el principio de cadena de bloques a diferentes ámbitos, a saber, notarios, bancos, bolsas de valores, identificación. Las identidades se gestionan mediante una cadena de bloques, almacenándose datos de identidad en la cadena de bloques a través de un protocolo Factom y poniéndose a disposición del cliente un carné de identidad digital.

"Does notarization on the blockchain actually work?" (¿Funciona realmente la notarización en la cadena de bloques?), en: Decentralize.today, 25 de enero de 2017. URL: https://decentralize.today/does-notarization-on-the-blockchain-actually-work-d8006443cOb9, describe servicios que describen una legalización de archivos utilizando una cadena de bloques.

CROSBY, M. *et al.*: "Blockchain Technology, Beyond Bitcoin" (Tecnología cadena de bloques, más allá de Bitcoin), en: Centro Sutardja de Emprendimiento y Tecnología, Informe técnico, 16 de octubre de 2015. URL: https://pdfs.semanticscholar.org/4b65/d3eda63fc18303dfbc071fe ceOe276a7a 16c.pdf, es un Libro Blanco que describe la tecnología de cadena de bloques y algunas aplicaciones específicas en los sectores financiero y no financiero.

En cambio, la invención se basa en el objetivo de crear un procedimiento eficaz y seguro para expedir una versión virtual de un documento.

El objetivo en el que se basa la invención se consigue en cada caso con las características de las reivindicaciones independientes. Formas de realización de la invención se especifican en las reivindicaciones dependientes.

Las formas de realización comprenden un procedimiento para la expedición de un documento virtual por medio de un primer sistema informático de un expedidor. El primer sistema informático comprende una memoria en la que está almacenada una clave criptográfica pública de un par de claves asimétricas asignadas al expedidor. Una clave criptográfica privada del par de claves asimétricas del expedidor está almacenada en un área de memoria protegida de la memoria. El primer sistema informático comprende, además, una interfaz de comunicación para la comunicación a través de una red.

El documento virtual se expide usando una cadena de bloques. La cadena de bloques comprende en un bloque un módulo de programa con primeras y segundas instrucciones de programa. Se generan entradas asignadas al módulo de programa en la cadena de bloques mediante la ejecución de las instrucciones de programa.

El procedimiento para la expedición del documento virtual comprende:

- crear una solicitud de registro por parte del primer sistema informático, comprendiendo la solicitud de registro la clave criptográfica pública del expedidor e identificando el módulo de programa,
- enviar la solicitud de registro por parte del primer sistema informático a través de la red a un primer servidor de cadena de bloques, estando configurado el primer servidor de cadena de bloques para generar bloques de la cadena de bloques,
- recibir la solicitud de registro por parte del primer servidor de cadena de bloques,
- ejecutar las primeras instrucciones de programa del módulo de programa identificado por la solicitud de registro por parte del primer servidor de cadena de bloques, comprendiendo la ejecución de las primeras instrucciones de programa verificar la validez de la solicitud de registro y, en el caso de una solicitud de registro válida, para registrar la clave criptográfica pública del expedidor, generar un primer bloque adicional de la cadena de bloques, comprendiendo el primer bloque generado una primera entrada asignada al módulo de programa con la clave criptográfica pública del expedidor.

El procedimiento comprende, además:

- recibir una solicitud por parte del primer sistema informático para la expedición del documento virtual,
- crear el documento virtual por parte del primer sistema informático,
- calcular un primer valor *hash* del documento virtual por parte del primer sistema informático,
- crear una solicitud de entrada firmada con la clave criptográfica privada del expedidor por parte del primer sistema informático, comprendiendo la solicitud de entrada el primer valor *hash* e identificando el módulo de programa,
- enviar la solicitud de entrada firmada por parte del primer sistema informático a través de la red a un segundo servidor de cadena de bloques, que está configurado para generar bloques de la cadena de bloques,
- recibir la solicitud de entrada firmada por parte del segundo servidor de cadena de bloques,
- ejecutar las segundas instrucciones de programa del módulo de programa identificado por la solicitud de entrada firmada por parte del segundo servidor de cadena de bloques, comprendiendo la ejecución de las segundas instrucciones de programa verificar la firma de la solicitud de entrada utilizando la clave criptográfica pública del expedidor registrada en la cadena de bloques, y, en el caso de una firma válida, para expedir el documento virtual, generar un segundo bloque adicional de la cadena de bloques, comprendiendo el segundo bloque generado una segunda entrada asignada al módulo de programa con el primer valor *hash*.

Las formas de realización pueden tener la ventaja de que permiten una expedición o legalización segura de documentos virtuales, tales como certificados u otros archivos. Se entiende por expedición de un documento virtual, en este caso, la creación de un archivo electrónico con todos los datos del documento correspondiente así como una prueba de la autenticidad de los datos correspondientes. Según las formas de realización, tal prueba de autenticidad para un documento virtual comprende un valor *hash* del documento virtual correspondiente introducido en una cadena de bloques. La protección de un documento virtual mediante una suma de comprobación basada en un *hash* y el almacenamiento en una cadena de bloques es eficaz y segura. En particular, de este modo se pueden impedir de manera eficaz las falsificaciones. Los costes resultantes apenas aumentan con la cantidad de documentos, ya que los costes para proteger los documentos individuales ya son bajos. Asimismo, las formas de realización pueden tener la ventaja de que mediante la cadena de bloques se confirma la autenticidad de todas las copias de un documento una vez introducido en la cadena de bloques. Por lo tanto, es posible autentificar un número ilimitado de copias con una única entrada en la cadena de bloques. Siempre que el contenido de las copias sea idéntico al documento original o al archivo original, de modo que el valor *hash* no cambie, la cadena de bloques puede servir para verificar que una copia correspondiente sea realmente una copia fiel al original. En el caso de documentos en papel convencionales, por ejemplo, cada copia individual tendría que estar certificada. El procedimiento es adecuado para todo tipo de documentos virtuales, es decir, objetos de datos o archivos. Pueden protegerse documentos de cualquier tamaño o número de páginas de manera eficaz y ahorrando espacio de almacenamiento. El procedimiento es fácil de usar. Finalmente, el uso de una cadena de bloques de una criptomoneda permite la implementación de un sistema de tasas implícito.

El valor *hash* resultante del documento queda almacenado de forma permanente y accesible públicamente. Según las formas de realización, el valor *hash* se introduce en la cadena de bloques junto con un sello de fecha y hora, de modo que en cualquier momento puede verificarse el instante en el que se expidió el documento. Independientemente de la

accesibilidad pública del valor *hash*, la cadena de bloques no comprende ningún dato personal accesible públicamente del titular del documento ni ningún otro dato incluido en el documento. Los datos personales del titular del documento, así como el documento en sí, están bajo el control exclusivo del titular del documento o del expedidor del documento. Solo quienes estén en posesión del documento pueden calcular su valor *hash* y verificar si hay depositado un valor *hash* idéntico en la cadena de bloques. Si este es el caso, este documento se considera auténtico. Sin embargo, no se puede obtener información sobre el tipo o el contenido del documento subyacente a partir de los valores *hash* accesibles públicamente de la cadena de bloques.

Según las formas de realización, la entrada en la cadena de bloques con el valor *hash* comprende una firma del expedidor del documento. Por ejemplo, la transacción que contiene el valor *hash* se firma con la clave criptográfica privada del expedidor. Esta firma se puede verificar con la clave criptográfica pública asociada del expedidor. Dado que se ha dado a conocer la clave pública del expedidor, se puede comprobar que el documento también fue realmente expedido por un expedidor autorizado para ello. Por ejemplo, en el caso de un certificado, se puede comprobar si la escuela responsable también ha expedido realmente el certificado, es decir, lo ha insertado en la cadena de bloques.

Por ejemplo, la entrada en la cadena de bloques describe una transacción desde una dirección de origen hasta una dirección de destino, siendo la dirección de origen, por ejemplo, una dirección del expedidor, tal como una escuela, por ejemplo. Esta dirección de origen puede corresponder, por ejemplo, a la clave criptográfica pública del expedidor, de modo que se pueda comprobar el origen del valor *hash* en la cadena de bloques. Solo datos firmados con la clave criptográfica privada del expedidor pueden enviarse desde esta dirección de origen. Al entrar en la cadena de bloques, la solicitud de entrada identifica, por ejemplo, la dirección de origen correspondiente.

Según las formas de realización, se proporciona una cadena de bloques para expedir y verificar documentos virtuales, tales como, por ejemplo, certificados. Si un expedidor de documentos, tal como, por ejemplo, una autoridad, una universidad, una escuela, un instituto, una empresa privada, quiere utilizar la cadena de bloques, puede registrarse. En el transcurso del registro, por ejemplo, se autentifica al expedidor. Una vez registrado el expedidor, es decir, su clave criptográfica pública se ha depositado en la cadena de bloques, este puede expedir documentos virtuales y depositar sus valores *hash* en la cadena de bloques para fines de verificación. Este depósito de los valores *hash* en la cadena de bloques corresponde a una autentificación de los documentos virtuales correspondientes así como de todas las copias fieles al original de los mismos.

Por tanto, las formas de realización pueden hacer posible que documentos tales como, por ejemplo, certificados, se expidan exclusivamente, o además de ser expedidos en papel, en forma virtual como una estructura de datos para el procesamiento electrónico de datos. Tales documentos virtuales se pueden guardar y/o transportar en cualquier equipo electrónico con memorias adecuadas. Sin embargo, estos equipos electrónicos deben estar protegidos contra el acceso no autorizado. Por ejemplo, los documentos se pueden guardar en un área de almacenamiento protegida de la memoria correspondiente. Además, los documentos se pueden proteger criptográficamente, por ejemplo, usando un módulo de seguridad. Además, los documentos virtuales se pueden enviar fácilmente a través de enlaces de comunicación electrónica como, por ejemplo, Internet. Sin embargo, los enlaces de comunicación utilizados para el envío deben estar protegidas contra escuchas o intentos de manipulación por parte de terceros no autorizados. La protección criptográfica puede tener lugar, por ejemplo, mediante cifrado con una clave criptográfica simétrica y/o una clave criptográfica pública asignada al destinatario. Según las formas de realización, la transmisión tiene lugar a través de un enlace protegido por medio de un cifrado de extremo a extremo. Además, la transmisión del documento virtual se puede proteger, a este respecto, por medio de un cifrado de transporte adecuado, tal como HTTPS, por ejemplo.

Si el titular de un documento virtual de este tipo necesita el envío de una copia, por ejemplo, copias para una solicitud en línea en el caso de los certificados, puede crearla él mismo. Siempre que la copia no cambie con respecto al original, es decir, siempre que tenga el mismo valor *hash*, la copia resultante ya está autenticada por el valor *hash* introducido en la cadena de bloques. El destinatario de la copia correspondiente puede calcular su valor *hash* y con ayuda de la cadena de bloques verificar si una entidad autorizada para ello, es decir, el expedidor, ha depositado un valor *hash* idéntico. Por ejemplo, en el caso de una solicitud en línea, un solicitante puede enviar todos sus certificados en forma virtual y el destinatario puede hacer que un sistema informático verifique su autenticidad automáticamente. Esta automatización puede resultar especialmente beneficiosa para las grandes empresas internacionales con miles de solicitudes al mes. Las formas de realización implementan estándares de seguridad suficientemente altos como para descartar la falsificación. Esto puede ser una ventaja para los hospitales, por ejemplo, ya que se puede comprobar así de manera eficaz y efectiva si un solicitante presenta certificados falsificados, en particular una licencia falsificada para ejercer la medicina. La comprobación se puede implementar mediante el uso de una cadena de bloques centralizada, por ejemplo, de manera eficaz para todas las universidades nacionales y/o al menos una selección de universidades internacionales que ofrecen titulaciones en medicina reconocidas. Dado que la cadena de bloques solo contiene valores *hash* y no datos personales del titular del certificado, también se garantiza un alto nivel de protección de datos.

Según las formas de realización, hay asignada una entrada al módulo de programa, por ejemplo, si comprende un ID del módulo de programa.

Por "documento" se entiende, en particular, un acta, un certificado o un documento de identidad, de valor o de seguridad, en particular un documento soberano, en particular un documento en papel y/o plástico, tal como, por ejemplo, un documento de identidad electrónico, en particular, pasaporte, carné de identidad, visado, carné de conducir, ficha técnica del vehículo, permiso de circulación, tarjeta sanitaria o una identificación de empresa u otro documento de ID, una tarjeta chip, medios de pago, en particular billetes, tarjetas bancarias o tarjetas de crédito, albaranes u otra prueba de autorización. En particular, el documento puede ser un documento de viaje legible por máquina, estandarizado, por ejemplo, por la Autoridad de Aviación Internacional (OACI) y/o la BSI.

Se entiende por documento "virtual" una estructura de datos para el procesamiento electrónico de datos que comprende los mismos datos que un documento previamente definido, pero no un cuerpo de documento físico asignado de manera fija. Un documento virtual, también denominado documento electrónico, puede comprender, por ejemplo, un texto, una tabla de números, una imagen o una secuencia o combinación de textos, tablas o imágenes, que se crean o transfieren en forma de archivo por digitalización, es decir, conversión a un código binario. En particular, la validez de tal documento es independiente de la presencia de un cuerpo de documento asignado de manera fija. Un documento "virtual" puede ser un archivo electrónico de cualquier formato de archivo, en particular un archivo de texto o tabla no ejecutable. Además, un documento virtual también puede ser, por ejemplo, un archivo de vídeo, un archivo de canción, un código de programa, un archivo ejecutable, un fichero o similar.

Según las formas de realización, se puede crear un documento virtual, por ejemplo, generando un archivo con los datos del documento correspondiente en un ordenador. Además, también se puede crear un documento virtual, por ejemplo, escaneando o fotocopiando un documento físico, como por ejemplo un documento en papel. Sin embargo, si se expide un documento virtual utilizando un escaneo de este tipo, como resultado solo serán válidos el documento virtual en forma del archivo de escaneo específico, así como todos los duplicados o copias idénticas del archivo de escaneo específico. Un nuevo escaneo del mismo documento original físico generalmente dará como resultado un archivo de escaneo adicional que tendrá un valor *hash* diferente debido a variaciones menores en el proceso de escaneo. Por lo tanto, a partir de un valor *hash* ya introducido en la cadena de bloques de un archivo de escaneo creado previamente del mismo documento original no puede dar como resultado una prueba de autenticidad o validez para este archivo de escaneo adicional. Sin embargo, debido al uso de valores *hash*, la prueba de autenticidad o la validez de un documento virtual está vinculada a un archivo sin cambios de acuerdo con el procedimiento aquí descrito.

Un acta es una declaración en forma de texto o escrita, que fija un cierto hecho o circunstancia. Además, el acta puede identificar al expedidor de la misma. Un certificado puede ser, por ejemplo, certificados escolares o universitarios, certificaciones de participación satisfactoria en cursos o formación continua, justificantes de participación en cursos, certificaciones de prácticas o referencias laborales.

Un certificado puede ser, por ejemplo, un certificado de examen IHK, que es un acta que se expide a nombre de un titulado después de haber aprobado el examen final ante la Cámara de Industria y Comercio (IHK) en una profesión reconocida o curso de formación avanzada. Un certificado IHK incluye, por ejemplo, información sobre la profesión que ha aprendido, es decir, un título profesional y el examen final que ha aprobado. El certificado puede aparecer en un diseño uniforme y contener el título profesional así como el campo de especialización o especialidad. El resultado global con calificación y puntuación está por encima de los resultados de los exámenes individuales. A petición del participante en los exámenes, se puede mostrar una calificación del centro de formación profesional por debajo de los resultados de los exámenes individuales.

Además, un documento también puede ser, por ejemplo, un diploma de obrero especializado, un diploma de oficial, un diploma de maestro, un título de grado, un título de máster, un título de maestría, un título de diplomatura, un título de doctorado o una licencia para ejercer la medicina.

Por "cadena de bloques" se entiende aquí y en lo sucesivo una estructura de datos ordenada que comprende una pluralidad de bloques de datos concatenados. En particular, se entiende por cadena de bloques una estructura de datos ordenada en la que cada uno de los bloques (aparte del primer bloque) comprende un valor de comprobación, por ejemplo un valor *hash*, de su bloque precedente y, por tanto, con ayuda de cada bloque se puede comprobar la validez de todos sus bloques precedentes y, dado el caso, confirmar. Para ver ejemplos de cadena de bloques, véase https://en.wikipedia.org/wiki/Block_chain_(database) y "Mastering Bitcoin" (Dominar el Bitcoin), Capítulo 7, The Blockchain, páginas 161 y sigs. El concepto de cadena de bloques se describió, por ejemplo, en 2008 en un Libro Blanco sobre Bitcoin bajo el seudónimo de Satoshi Nakamoto ("Bitcoin: Peer-to-Peer Electronic Cash System" (Bitcoin: sistema de efectivo electrónico de igual a igual) (https://bitcoin.org/bitcoin.pdf)). La cadena de bloques descrita en el mismo consta de una serie de bloques de datos en los que se combinan en cada caso una o más entradas o transacciones y se les proporciona una suma de comprobación en forma de valor *hash*. Se generan bloques adicionales de la cadena de bloques, por ejemplo, en un proceso computacionalmente intensivo, que también se conoce como minería (*mining*). Estos bloques generados adicionalmente se agregan, a continuación, a la cadena de bloques y se distribuyen a través de una red a todos los abonados o nodos de la red.

Las formas de realización pueden tener la ventaja de que la cadena de bloques ofrece un alto grado de seguridad contra manipulaciones posteriores mediante el almacenamiento de sumas de comprobación criptográficas, es decir, valores *hash*, del bloque precedente en el bloque en cada caso siguiente. En una cadena de bloques, las entradas o

transacciones de un bloque se combinan en pares mediante función *hash*, por ejemplo, utilizando un árbol de Merkle, y solo el último valor *hash* del bloque obtenido de esta manera, el denominado valor *hash* raíz, se anota como suma de comprobación, por ejemplo, en un encabezado del bloque. A continuación, se puede comprobar la concatenación de los bloques utilizando estos valores *hash* raíz. Cada bloque de la cadena de bloques contiene en su encabezado el *hash* de todo el encabezado de bloque anterior. La secuencia de los bloques queda así claramente definida y se crea una estructura en cadena. Mediante la concatenación de los bloques individuales implementada de esta manera se consigue que una modificación posterior de bloques precedentes o transacciones individuales quede descartada en la práctica, ya que los valores *hash* de todos los bloques subsiguientes también tendrían que recalcularse en poco tiempo.

El primer bloque de la cadena de bloques está predefinido y se denomina bloque de génesis. Según las formas de realización, las claves criptográficas públicas de uno o más proveedores que están autorizados para crear módulos de programa están almacenadas en el bloque de génesis. Debido a la estructura en cadena descrita anteriormente, el bloque de génesis es el bloque cuyas entradas tienen el mayor nivel de seguridad, ya que para cambiarlo, toda la cadena de bloques tendría que ser reemplazada por una nueva cadena de bloques. Por lo tanto, la entrada de la clave criptográfica pública en el bloque de génesis puede representar un ancla de confianza con un grado de seguridad suficiente, de modo que, por ejemplo, no es necesaria ninguna comprobación PKI adicional para confiar en la autenticidad de la clave criptográfica pública. Esto puede aumentar aún más la seguridad del sistema en el modo fuera de línea.

Además, adaptando la intensidad computacional requerida para la creación de bloques en cada caso adicionales, la seguridad se puede incrementar adicionalmente. La intensidad computacional requerida para la creación de bloques adicionales se puede controlar a través de los requisitos para el valor *hash* del bloque adicional que se va a crear. El valor *hash* resultante es impredecible, más bien se trata de un número distribuido aleatoriamente. Sin embargo, se puede calcular cuánto tiempo es necesario en la media estadística para encontrar un bloque adicional válido, en función de la potencia de cálculo utilizada. El valor *hash* de un bloque se puede variar, por ejemplo, agregando y variando un *nonce.* Debido a la estructura en cadena, los datos almacenados una vez en una cadena de bloques ya no se pueden cambiar o eliminar sin reemplazar grandes partes de la cadena de bloques. Sin embargo, tal reemplazo se descarta como resultado de una generación de bloques adicionales suficientemente intensiva computacionalmente. Las formas de realización conocidas de una cadena de bloques, como por ejemplo en el caso de la criptomoneda Bitcoin, se basan en el anonimato de los socios involucrados en las transacciones. En cambio, mediante la firma descrita anteriormente de los valores *hash* introducidos en las transacciones, se puede acreditar su autenticidad y verificar su origen. De este modo se puede mejorar la seguridad contra la falsificación.

Un requisito para un bloque válido puede ser, por ejemplo, que el valor *hash* del encabezado del bloque sea menor o igual a un valor límite. El valor *hash* se puede calcular utilizando el algoritmo de *hash* seguro (SHA) SHA 256, por ejemplo. En este caso, el valor *hash* resultante es un número aleatorio entre 0 y 2^{256}-1. La probabilidad de que salga un determinado *hash* al aplicar el algoritmo de *hash* es (valor *hash* máximo+1)$^{-1}$, en el caso del algoritmo SHA 256 es, por tanto, 2^{-256}. La probabilidad de que el valor *hash* resultante sea menor o igual a un valor límite o valor objetivo (en inglés, *target*) es, por tanto, (objetivo)/(valor *hash* máx.). Para un valor límite máximo a modo de ejemplo de (2^{16}-1) 2^{208}, la probabilidad es de [(2^{16}-1) 2^{208}] / $2^{256} \approx 2^{-32}$. La dificultad S de obtener un valor *hash* que sea menor o igual a un valor límite u objetivo seleccionado se puede especificar de la siguiente manera, en función de un valor límite máximo u objetivo máximo: S = (objetivo máx.)/objetivo. Por lo tanto, la probabilidad de recibir un valor *hash* que sea menor o igual al valor límite seleccionado es, para el ejemplo anterior: 2^{-32}/S. Como ejemplo, considérese un sistema informático con una determinada tasa *hash* que, en promedio, cada x segundos encuentra un valor *hash* que es menor o igual al valor límite seleccionado. Si el sistema informático, en lugar de cada x segundos en promedio, debe encontrar un resultado cada y segundos, la dificultad se puede adaptar correspondientemente: $S_y=(x/y)\cdot S$. También pueden usarse adaptaciones apropiadas de la dificultad para mantener constante la tasa de resultados en caso de modificación del sistema informático, por ejemplo, modificaciones en la potencia computacional al aumentar o disminuir la cantidad de servidores de cadena de bloques. Si la dificultad se adapta de modo que cada y segundos se logra un resultado, la tasa *hash* R del sistema informático puede parametrizarse de la siguiente manera: R = ($2^{32}\cdot$S)/(y segundos).

Si los bloques válidos se generan mediante un procedimiento computacionalmente intensivo como el descrito anteriormente, los abonados de la red de cadena de bloques confían en la cadena de bloques válida más larga, ya que esta cuenta con la mayor potencia computacional y, por lo tanto, se puede suponer que esta será reconocida como válida por la mayoría de abonados. Si, por ejemplo, en la cadena de bloques surge una bifurcación, es decir, una ramificación, en algún momento prevalecerá la bifurcación con mayor longitud de cadena, ya que se puede suponer que la mayoría de los abonados están detrás de ella.

Una cadena de bloques también se puede implementar, por ejemplo, en forma de una cadena de bloques privada, en la que solo un grupo seleccionado de abonados está autorizado a agregar bloques válidos. Se puede comprobar una autorización correspondiente, por ejemplo, mediante una firma usando una clave criptográfica privada. La clave criptográfica privada puede pertenecer a un par de claves asimétricas, que también incluye una clave criptográfica pública con la que se puede verificar la firma. Al par de claves asimétricas también se le puede asignar, por ejemplo, un certificado que acredite la autorización para generar un bloque válido de la cadena de bloques. Este certificado también puede estar asignado a una PKI que acredite la autenticidad del certificado. Según una forma de realización

adicional, por ejemplo, puede estar depositada una clave pública en la cadena de bloques para cada abonado del grupo seleccionado, por ejemplo en un bloque de génesis. Esta clave pública se puede utilizar para comprobar si las firmas de los bloques y, por tanto, los propios bloques correspondientes son válidos.

También se puede implementar un consenso en una cadena de bloques de otras formas. Por ejemplo, se puede llegar a un consenso votando sobre la inclusión de entradas propuestas en la cadena de bloques. Por ejemplo, cada abonado mantiene una lista unívoca de otros abonados en los que confía como grupo. Cada abonado puede sugerir entradas adicionales que deberían incluirse en un bloque adicional de la cadena de bloques. Se vota sobre la inclusión y, por tanto, el reconocimiento de la validez de las entradas propuestas. Por ejemplo, cada abonado solo vota las sugerencias que provienen de los abonados de su lista. En otras palabras, para decidir si una propuesta de entrada adicional se reconoce como válida, es decir, si existe un consenso entre los abonados con respecto a la validez de esta entrada, solo se tienen en cuenta los votos de aquellos abonados que están incluidos en la lista del abonado que hace la correspondiente propuesta. Para que una propuesta de entrada sea aceptada como válida, un cierto porcentaje mínimo de abonados con derecho a voto debe votar sí, por ejemplo el 80 %. Todas las entradas propuestas que cumplan con este criterio se agregarán a la cadena de bloques. Tal votación puede constar de varias rondas. Todas las demás propuestas que no cumplan con el criterio antes mencionado serán rechazadas o sometidas a votación nuevamente cuando se vote el siguiente bloque de la cadena de bloques. Las listas antes mencionadas representan subgrupos de la red de cadena de bloques en los que el abonado que mantiene la lista respectiva confía en conjunto como grupo, sin que esto requiera que confíe en cada abonado individual de la lista. Un ejemplo de un procedimiento de consenso de este tipo es el algoritmo de consenso del protocolo Ripple (David Schwartz *et al.*: "The Ripple Protocol Consensus Algorithm" (El algoritmo de consenso del protocolo Ripple), Ripple Labs Inc., 2014, https://ripple.com/files/ripple_consensus_whitepaper.pdf).

Para verificar las entradas en la cadena de bloques o para buscar valores *hash*, una entidad de gestión de la cadena de bloques puede proporcionar una GUI, por ejemplo en forma de sitio de Internet. Por ejemplo, la cadena de bloques puede ser una cadena de bloques privada, por ejemplo interna de una empresa o interna de un grupo, o pública. Por ejemplo, se trata de una cadena de bloques de Bitcoin, Litecoin o Ethereum.

Un "módulo de programa" designa aquí un programa independiente que está almacenado en una cadena de bloques. El módulo de programa puede estar configurado para controlar la creación de entradas asignadas al módulo de programa en la cadena de bloques. El módulo de programa puede estar almacenado en un bloque de la cadena de bloques o distribuido en varios bloques de la cadena de bloques. Por ejemplo, se asigna un módulo de programa individual a cada expedidor o a cada entidad de gestión de un grupo de expedidores o a todos los expedidores juntos. La cadena de bloques es, por ejemplo, una cadena de bloques de documentos o certificados especial. Un módulo de programa puede ser, por ejemplo, un "contrato inteligente" (*smart contract*) como el que se puede implementar en la cadena de bloques de Ethereum de código abierto.

Por "programa" o "instrucciones de programa" se entiende aquí, sin restricción, cualquier tipo de programa informático que comprenda instrucciones legibles por máquina para controlar una funcionalidad del ordenador.

Por "interfaz" se entiende aquí una interfaz a través de la cual se pueden recibir y enviar datos, pudiendo estar la interfaz de comunicación configurada con o sin contacto. La interfaz de comunicación puede ser una interfaz interna o una interfaz externa que se conecta a un equipo asignado, por ejemplo, mediante un cable o de manera inalámbrica.

La comunicación puede tener lugar, por ejemplo, a través de una red. Por "red" se entiende aquí cualquier medio de transmisión con una conexión para la comunicación, en particular una conexión local o una red local, en particular una red de área local (LAN), una red privada, en particular una intranet, y una red privada virtual (*virtual private network* - VPN). Por ejemplo, un sistema informático puede tener una interfaz de radio estándar para conectarse a una WLAN. También puede tratarse de una red pública, como Internet, por ejemplo. Dependiendo de la forma de realización, esta conexión también se puede establecer a través de una red de radiotelefonía móvil.

Se entiende aquí por "memoria" tanto memorias electrónicas volátiles y no volátiles como medios de almacenamiento digitales.

Se entiende aquí por "memoria no volátil" una memoria electrónica para el almacenamiento permanente de datos. Una memoria no volátil puede estar configurada como memoria no modificable, que también se denomina memoria de solo lectura (ROM, *read-only memory*), o como memoria modificable, que también se denomina memoria no volátil (NVM, *non-volatile memory*). En particular, puede tratarse a este respecto de una EEPROM, por ejemplo una Flash EEPROM, conocida como Flash para abreviar.

Una memoria no volátil se caracteriza por el hecho de que los datos almacenados en ella se conservan incluso después de que se apague la fuente de alimentación.

Una "memoria electrónica volátil" es una memoria para el almacenamiento temporal de datos, que se caracteriza por que todos los datos se pierden después de que se apague la fuente de alimentación. En particular, puede tratarse a

este respecto de una memoria volátil de acceso directo, que también se denomina memoria de acceso aleatorio (RAM, *random-access memory*), o una memoria volátil principal del procesador.

Por "área de memoria protegida" se entiende aquí un área de una memoria electrónica a la que el acceso, es decir, el acceso de lectura o el acceso de escritura, solo es posible a través de un procesador del módulo de seguridad. Según las formas de realización, el acceso desde el procesador acoplado a la memoria solo es posible si se cumple una condición requerida para ello. Puede tratarse, a este respecto, por ejemplo, de una condición criptográfica, en particular una autentificación satisfactoria y/o una comprobación de autorización satisfactoria.

Por "procesador" se entiende aquí y en lo sucesivo un circuito lógico que sirve para ejecutar instrucciones de programa. El circuito lógico puede estar implementado en uno o más componentes discretos, en particular en un chip. En particular, se entiende por "procesador" un microprocesador o un sistema de microprocesador compuesto por una pluralidad de núcleos de procesador y/o una pluralidad de microprocesadores.

Por "certificado" se entiende aquí un certificado digital, que también se denomina certificado de clave pública. A continuación, los objetos "digitales" también se denominan objetos "virtuales", es decir, estructuras de datos para el procesamiento electrónico de datos. La denominada Infraestructura de clave pública (PKI) se implementa a través de tales certificados sobre la base de pares de claves asimétricas. Un certificado de este tipo son datos estructurados que sirven para asignar una clave pública de un criptosistema asimétrico a una identidad, como una persona o un dispositivo, por ejemplo. Por ejemplo, un certificado puede incluir una clave pública y estar firmado. Alternativamente, también son posibles certificados basados en criptosistemas de conocimiento cero. Por ejemplo, el certificado puede cumplir con la norma X.509 o con otra norma. Por ejemplo, el certificado es un certificado CV o un certificado verificable por tarjeta (CVC, *card verifiable certificate*). Una implementación de tales CVC se especifica en la norma ISO/IEC 7816-8, por ejemplo.

La PKI proporciona un sistema para expedir, distribuir y verificar certificados digitales. Un certificado digital se utiliza en un criptosistema asimétrico para confirmar la autenticidad de una clave pública y su alcance permitido de aplicación y validez. El propio certificado digital está protegido por una firma digital, cuya autenticidad puede comprobarse con la clave pública del expedidor del certificado. Se vuelve a utilizar un certificado digital para comprobar la autenticidad de la clave del expedidor. De esta forma se puede configurar una cadena de certificados digitales, cada uno de los cuales confirma la autenticidad de la clave pública con la que se puede verificar el certificado precedente. Esta cadena de certificados forma una denominada ruta de validación o ruta de certificación. Los abonados de la PKI deben poder confiar en la autenticidad del último certificado, el llamado certificado raíz, y de la clave certificada por este certificado, sin otro certificado más. El certificado raíz es gestionado por una denominada entidad de certificación raíz, cuya autenticidad se supone que está asegurada y en la que se basa la autenticidad de todos los certificados de la PKI.

Cuando se trata de proteger la comunicación electrónica mediante procedimientos criptográficos asimétricos, los certificados digitales son un medio probado para verificar las autorizaciones. Los certificados son datos estructurados que documentan la autenticidad y/u otras propiedades/autorizaciones del propietario de una clave pública (clave de verificación de firma) y la confirman mediante una entidad independiente y de confianza (proveedor de servicios de certificación/ZDA), generalmente la autoridad de certificación que expide el certificado. Los certificados generalmente se ponen a disposición de un amplio grupo de personas para que puedan verificar la autenticidad y validez de firmas electrónicas.

Se puede asignar un certificado a una firma electrónica si la clave privada perteneciente a la clave pública se utilizó para generar la firma electrónica que se va a verificar. Debido a que un ZDA pone un certificado a disposición del público en general en asociación con una clave pública, un ZDA permite a los usuarios de criptosistemas asimétricos asignar la clave pública a una identidad, por ejemplo, a una persona, una organización, un sistema energético o informático.

Los pares de claves asimétricas se utilizan para una gran cantidad de criptosistemas y también desempeñan un papel importante en la firma de documentos electrónicos. Un par de claves asimétricas consta de una clave pública, que se utiliza para cifrar y/o descifrar datos y puede transmitirse a terceros, por ejemplo, a un proveedor de servicios, y una clave privada, que se utiliza para cifrar y/o descifrar datos y, por regla general, debe mantenerse secreta. La clave pública permite a cualquier persona cifrar los datos del titular de la clave privada, verificar firmas digitales de sus documentos o autentificarlo. Una clave privada permite a su titular descifrar datos cifrados con la clave pública o crear firmas digitales para documentos electrónicos. Una firma creada con una clave privada se puede verificar con la clave pública asociada.

La creación de una firma digital, también denominada únicamente como "firma" en lo sucesivo, es un procedimiento criptográfico en el que se calcula un valor de datos adicional, denominado "firma", para cualquier dato, por ejemplo, un documento electrónico. La firma puede ser, por ejemplo, un valor *hash* cifrado del documento electrónico, en particular un valor *hash* cifrado con una clave privada de un par de claves criptográficas asignado a un certificado. La peculiaridad de tal firma es que su autoría y afiliación a una determinada persona o entidad puede ser verificada por cualquier tercero.

Una firma digital también se entiende aquí como un sello digital que no está asignado a una persona física, sino a una persona jurídica. Por tanto, un sello digital no sirve para hacer una declaración de intenciones de un particular, sino que más bien le sirve a una institución como prueba de origen. De este modo, puede garantizar el origen y la integridad de documentos virtuales y demostrar que proceden de una persona jurídica concreta.

Por "enlace cifrado de extremo a extremo" o "canal de transmisión cifrado de extremo a extremo" se entiende aquí un enlace entre un remitente y un destinatario con cifrado de extremo a extremo, en el que los datos que va a transmitir el remitente se cifran y solo los vuelve a descifrar el destinatario. Por tanto, el cifrado de los datos transmitidos tiene lugar abarcando todas las estaciones de transmisión, de modo que las estaciones intermedias no pueden conocer el contenido de los datos transmitidos debido al cifrado. El enlace está protegido criptográficamente mediante el cifrado para evitar el espionaje y/o la manipulación de la transmisión, pudiendo utilizarse para ello un denominado procedimiento de mensajería segura. El cifrado de extremo a extremo se basa, por ejemplo, en dos claves criptográficas simétricas, sirviendo una primera de las claves simétricas para cifrar mensajes y una segunda de las claves simétricas para autentificar al remitente del mensaje.

Se puede utilizar una clave para autentificar al remitente de un mensaje en el transcurso de un procedimiento de mensajería segura, por ejemplo, para crear un código de autentificación de mensaje (*message authentication code*, MAC). Por medio de un MAC se puede obtener certeza acerca del origen de los mensajes y verificar su integridad. Los algoritmos MAC requieren dos parámetros de entrada, en primer lugar los datos que se van a proteger y en segundo lugar una clave secreta. A partir de ambos se calcula un código de autentificación de mensaje en forma de suma de comprobación. El remitente de un mensaje calcula un MAC para los datos del mensaje que van a transmitirse y envía el mensaje junto con el MAC al destinatario. El destinatario calcula el MAC para el mensaje recibido con su clave y compara el MAC calculado con el MAC recibido. Si ambos valores coinciden, se deduce que el mensaje fue enviado por una parte que tiene acceso a la clave secreta y que el mensaje no fue modificado durante la transmisión.

Según las formas de realización, la solicitud de registro comprende una contraseña de registro. La verificación de la validez de la solicitud de registro comprende verificar la validez de la contraseña de registro.

Las formas de realización pueden tener la ventaja de que se proporciona al expedidor, por ejemplo por una entidad de gestión de la cadena de bloques o del módulo de programa o del expedidor, una contraseña de registro para registrarse en la cadena de bloques. Con esta, al registrarse en la cadena de bloques, el expedidor puede activar la autorización para depositar valores *hash* utilizando el módulo de programa. Por ejemplo, el expedidor es una escuela que quiere registrarse para poder depositar valores *hash* de certificados. Para ello, la escuela solicita a la autoridad de gestión una contraseña de registro para el registro. Esto se puede hacer, por ejemplo, por escrito por correo postal, por correo electrónico o a través de un sitio de Internet. Una solicitud por vía electrónica puede estar protegida criptográficamente. La protección criptográfica puede tener lugar, por ejemplo, mediante cifrado con una clave criptográfica simétrica y/o una clave criptográfica pública asignada al destinatario. Según las formas de realización, la transmisión tiene lugar a través de un enlace protegido por medio de un cifrado de extremo a extremo. Además, la transmisión de la solicitud se puede proteger mediante un cifrado de transporte adecuado, tal como HTTPS, por ejemplo. Por ejemplo, la escuela se autentifica con ayuda de la solicitud. En el caso de una solicitud por vía electrónica, esta se puede firmar, por ejemplo, con un sello, es decir, una clave de firma criptográfica privada asignada a la escuela. En respuesta a la solicitud, la entidad de gestión envía a la escuela la contraseña de registro. Por ejemplo, el envío tiene lugar por correo postal. Esto puede servir como una medida de seguridad adicional, ya que la dirección postal de la escuela es pública y generalmente solo cambia si la escuela cambia de ubicación. Por lo tanto, se puede asumir con un alto grado de seguridad que el destinatario de la contraseña de registro enviada por correo postal es en realidad la escuela, incluso aunque la solicitud subyacente provenga de un tercero no autorizado que haya falsificado la identidad de la escuela. Alternativamente, la contraseña de registro se puede enviar por vía electrónica a través de un enlace de comunicación protegido criptográficamente, tal como se describió anteriormente.

La contraseña de registro puede ser, por ejemplo, una *"one-time-password*" u "OTP". Una OTP es una contraseña de un solo uso que solo será válida para un único uso.

Según las formas de realización, el procedimiento comprende, además, enviar el documento virtual a un segundo sistema informático en respuesta a la solicitud para expedir el documento virtual. Las formas de realización pueden tener la ventaja de que el documento virtual se pone a disposición de un segundo sistema informático, tal como un sistema informático del titular del documento. El titular del documento virtual obtiene así el control de la disponibilidad del documento y puede enviarlo a otros sistemas informáticos seleccionados, que pueden comprobar la autenticidad del documento virtual utilizando la cadena de bloques.

Según las formas de realización, la solicitud de registro también comprende un ID de expedidor. Si la contraseña de registro se verifica satisfactoriamente, el ID de expedidor se introduce junto con la clave criptográfica pública en el segundo bloque de la cadena de bloques. Las formas de realización pueden tener la ventaja de que la identidad del expedidor se puede determinar a partir de la cadena de bloques.

Un ID es un identificador, también denominado identificación, que comprende una característica vinculada a una identidad concreta para la identificación inequívoca de una persona o un objeto, por ejemplo, el expedidor de los

documentos virtuales al que está asignado el identificador. Un identificador puede incluir, por ejemplo, números, letras, caracteres especiales y combinaciones de los mismos. Por ejemplo, el ID de expedidor puede comprender el nombre del expedidor.

Según las formas de realización, la verificación de la contraseña de registro comprende:

- comparar la contraseña de registro recibida por parte del primer servidor de cadena de bloques con una contraseña de registro almacenada en la cadena de bloques,
- si la contraseña de registro recibida coincide con la contraseña de registro almacenada, confirmar la validez de la contraseña de registro recibida por parte del primer servidor de cadena de bloques.

Las formas de realización pueden tener la ventaja de que se proporciona un procedimiento eficaz para determinar la validez de una contraseña de registro presentada por un expedidor para el registro. Según las formas de realización, la contraseña de registro almacenada en la cadena de bloques es generada por un sistema informático de gestión de una entidad de gestión y almacenada en la cadena de bloques.

Según las formas de realización, si la contraseña de registro recibida coincide con la contraseña de registro almacenada, se almacena una nota en una entrada de la cadena de bloques que indica que la correspondiente contraseña de registro almacenada se ha agotado. Por tanto puede garantizarse que ya no sea posible realizar más registros usando la misma contraseña de registro. Se puede implementar así una contraseña de un solo uso.

Según las formas de realización, la contraseña de registro se proporciona en forma de un segundo valor *hash* almacenado firmado en la cadena de bloques. La comparación de la contraseña de registro recibida con la contraseña de registro almacenada comprende:

- verificar la validez de la firma del segundo valor *hash* almacenado,
- calcular un tercer valor *hash* de la contraseña de registro recibida,
- comparar el tercer valor *hash* calculado con el segundo valor *hash* almacenado.

Las formas de realización pueden tener la ventaja de que la contraseña de registro no puede derivarse del segundo valor *hash*. Por lo tanto, la contraseña de registro puede mantenerse secreta, incluso aunque las entradas de la cadena de bloques y, en particular, el segundo valor *hash* sean accesibles públicamente. Mediante la firma también se puede verificar si la contraseña de registro la proporciona una entidad autorizada para ello.

Según las formas de realización, el módulo de programa comprende terceras instrucciones de programa. La provisión de la contraseña de registro comprende:

- calcular el segundo valor *hash* de la contraseña de registro por parte de un primer sistema informático de gestión de una primera entidad de gestión que gestiona el módulo de programa,
- firmar el segundo valor *hash* con una clave criptográfica privada de un par de claves asimétricas asignadas a la primera entidad de gestión,
- crear una solicitud de provisión por parte del primer sistema informático de gestión, comprendiendo la solicitud de provisión el segundo valor *hash* firmado e identificando el módulo de programa,
- enviar la solicitud de provisión por parte del primer sistema informático de gestión a un tercer servidor de cadena de bloques, que está configurado para generar bloques de la cadena de bloques,
- recibir la solicitud de provisión por parte del tercer servidor de cadena de bloques,
- ejecutar las terceras instrucciones de programa del módulo de programa identificado por la solicitud de provisión por parte del tercer servidor de cadena de bloques, comprendiendo la ejecución de las terceras instrucciones de programa verificar la firma del segundo valor *hash* por parte del tercer servidor de cadena de bloques utilizando una clave criptográfica pública del par de claves asimétricas asignadas a la primera entidad de gestión y, en el caso de una firma válida, generar un tercer bloque adicional de la cadena de bloques mediante el tercer servidor de cadena de bloques, comprendiendo el tercer bloque generado una tercera entrada asignada al módulo de programa con el segundo valor *hash* firmado.

Las formas de realización pueden tener la ventaja de que se proporciona un procedimiento eficaz y seguro para registrar uno o más expedidores proporcionando uno o más segundos valores *hash* para una o más contraseñas de registro.

Según las formas de realización, la clave criptográfica pública de la primera entidad de gestión está almacenada en la cadena de bloques y el tercer servidor de la cadena de bloques usa la clave criptográfica pública del primer sistema informático de gestión almacenada en la cadena de bloques para verificar la firma del segundo valor *hash*. Las formas de realización pueden tener la ventaja de que la clave criptográfica pública para verificar la validez de la firma del segundo valor *hash* es proporcionada por la cadena de bloques, lo que permite una verificación eficaz.

Según las formas de realización, un ID de la primera entidad de gestión está almacenado en la cadena de bloques junto con la clave criptográfica pública de la primera entidad de gestión. Las formas de realización pueden tener la ventaja de que la identidad de la entidad de gestión se puede determinar a partir de la cadena de bloques.

Según las formas de realización, el procedimiento comprende, además, enviar una solicitud de contraseña para obtener la contraseña de registro por parte del primer sistema informático al primer sistema informático de gestión. La solicitud de contraseña identifica al expedidor. El procedimiento comprende, además, por parte de la primera entidad de gestión, utilizando el primer sistema informático de gestión:

- recibir la solicitud de contraseña,
- identificar una dirección postal asignada al expedidor,
- crear un escrito de respuesta dirigido a la dirección postal identificada, que comprende la contraseña de registro,
- enviar el escrito de respuesta por correo postal.

Las formas de realización pueden tener la ventaja de que se implementa un procedimiento eficaz y seguro para proporcionar la contraseña de registro y, por lo tanto, para el registro de expedidores. Según las formas de realización, el procedimiento comprende, además, verificar la validez de la solicitud. Por ejemplo, se comprueba si la solicitud proviene de una institución, tal como una universidad o una escuela, que efectivamente está autorizada para expedir los documentos correspondientes, como por ejemplo certificados.

Según las formas de realización, el procedimiento comprende, además, por parte de la primera entidad de gestión, utilizando el primer sistema informático de gestión:

- recibir la solicitud de contraseña,
- crear una respuesta a la solicitud de contraseña, que comprende la contraseña de registro,
- enviar la respuesta en forma protegida criptográficamente al primer sistema informático del expedidor.

Las formas de realización pueden tener la ventaja de que se implementa un procedimiento eficaz y seguro para proporcionar la contraseña de registro y, por lo tanto, para el registro de expedidores. Según las formas de realización, el procedimiento comprende, además, verificar la validez de la solicitud. Por ejemplo, se comprueba si la solicitud proviene de una institución, tal como una universidad o una escuela, que efectivamente está autorizada para expedir los documentos correspondientes, como por ejemplo certificados.

Según las formas de realización, el documento virtual es un certificado virtual.

Según las formas de realización, el procedimiento comprende, además:

- crear el módulo de programa por parte del segundo sistema informático de gestión,
- crear una solicitud de inicialización firmada por parte del segundo sistema informático de gestión con el módulo de programa,
- enviar la solicitud de inicialización por parte del segundo sistema informático de gestión a un cuarto servidor de cadena de bloques, que está configurado para generar bloques de la cadena de bloques,
- recibir el módulo de programa por parte del cuarto servidor de cadena de bloques,
- verificar la firma de la solicitud de inicialización por parte del cuarto servidor de cadena de bloques utilizando la clave criptográfica pública del par de claves asimétricas asignadas a la segunda entidad de gestión y, en el caso de una firma válida, generar un cuarto bloque adicional de la cadena de bloques por parte del cuarto servidor de cadena de bloques, comprendiendo el cuarto bloque generado una cuarta entrada con el módulo de programa.

Las formas de realización pueden tener la ventaja de que el sistema informático de gestión puede proporcionar el módulo de programa para introducir valores *hash* por parte del expedidor o los expedidores de documentos virtuales. Este módulo de programa está previsto, por ejemplo, para la introducción de documentos de un expedidor o de un grupo de expedidores. Según las formas de realización, el sistema informático de gestión puede introducir una pluralidad de módulos de programa para introducir valores *hash* en la cadena de bloques.

Según las formas de realización, el módulo de programa comprende cuartas instrucciones de programa y el procedimiento comprende, además:

- recibir una primera confirmación de pago de una tasa de legalización por la expedición del documento virtual por parte del segundo sistema informático de gestión,
- crear una primera confirmación de legalización por parte del segundo sistema informático de gestión, comprendiendo la confirmación de legalización el primer valor *hash* firmado del documento virtual e identificando el módulo de programa,
- firmar la primera confirmación de legalización por parte del segundo sistema informático de gestión con la clave criptográfica privada de la entidad de gestión,

- enviar la primera confirmación de legalización firmada a un quinto servidor de cadena de bloques, que está configurado para generar bloques de la cadena de bloques,
- recibir la primera confirmación de legalización por parte del quinto servidor de cadena de bloques,
- ejecutar las cuartas instrucciones de programa del módulo de programa identificado por la confirmación de legalización por parte del quinto servidor de cadena de bloques, comprendiendo la ejecución de las cuartas instrucciones de programa verificar la firma de la primera confirmación de legalización por parte del quinto servidor de cadena de bloques utilizando la clave criptográfica pública de la segunda entidad de gestión y, en el caso de una firma válida, generar un quinto bloque adicional de la cadena de bloques por parte del quinto servidor de cadena de bloques, comprendiendo el quinto bloque generado una quinta entrada asignada al módulo de programa con la primera confirmación de legalización firmada.

Las formas de realización pueden tener la ventaja de que un documento virtual solo se considera autentificado y, por lo tanto, se puede utilizar realmente si hay una confirmación del pago de una tasa de legalización. Por tanto, las formas de realización ofrecen un procedimiento para garantizar de manera eficaz que un documento virtual solo se pueda utilizar una vez que se hayan abonado las tasas correspondientes.

Según las formas de realización, el usuario, es decir, el titular del documento, paga las tasas de legalización y, por lo tanto, financia el esfuerzo adicional para el expedidor y la entidad de gestión que resulta de la introducción del valor *hash* en la cadena de bloques y la provisión o gestión de la cadena de bloques.

Según las formas de realización, el módulo de programa comprende quintas instrucciones de programa y el procedimiento comprende, además:

- generar una instrucción de transacción por parte del segundo sistema informático de gestión para la transacción de al menos un importe parcial de la tasa de legalización en forma de criptomoneda implementada en la cadena de bloques desde una dirección de origen asignada a la segunda entidad de gestión hasta una dirección de destino asignada al expedidor,
- firmar la instrucción de transacción con una clave criptográfica privada de un par de claves asimétricas asignadas a la dirección de origen,
- enviar la instrucción de transacción a un sexto servidor de cadena de bloques, que está configurado para generar bloques de la cadena de bloques,
- recibir la instrucción de transacción por parte del sexto servidor de cadena de bloques,
- ejecutar las quintas instrucciones de programa del módulo de programa identificado por la solicitud de provisión por parte del sexto servidor de cadena de bloques, comprendiendo la ejecución de las quintas instrucciones de programa verificar la firma de la instrucción de transacción por parte del sexto servidor de cadena de bloques utilizando la dirección de origen y, en el caso de una firma válida, generar un sexto bloque adicional de la cadena de bloques por parte del sexto servidor de cadena de bloques, comprendiendo el sexto bloque generado una sexta entrada asignada al módulo de programa con la instrucción de transacción.

Las formas de realización pueden tener la ventaja de que la cadena de bloques proporciona un sistema numérico utilizando una criptomoneda tal como, por ejemplo, Bitcoin o Ethereum. A través de este sistema de pago se puede proporcionar un procedimiento para repartir la tasa de legalización entre la entidad de gestión y el expedidor de una manera eficaz y segura.

Según las formas de realización, el módulo de programa comprende sextas instrucciones de programa y el procedimiento comprende, además:

- recibir una segunda confirmación de pago de la tasa de legalización por la expedición del documento virtual por parte del primer sistema informático,
- crear una segunda confirmación de legalización por parte del primer sistema informático, comprendiendo la confirmación de legalización el primer valor *hash* firmado del documento virtual e identificando el módulo de programa,
- firmar la segunda confirmación de legalización por parte del primer sistema informático con la clave criptográfica privada del expedidor,
- enviar la segunda confirmación de legalización firmada a un séptimo servidor de cadena de bloques, que está configurado para generar bloques de la cadena de bloques,
- recibir la segunda confirmación de legalización por parte del séptimo servidor de cadena de bloques,
- ejecutar las sextas instrucciones de programa del módulo de programa identificado por la segunda confirmación de legalización por parte del séptimo servidor de cadena de bloques, comprendiendo la ejecución de las sextas instrucciones de programa verificar la firma de la segunda confirmación de legalización por parte del séptimo servidor de cadena de bloques utilizando la clave criptográfica pública del expedidor y, en el caso de una firma válida, generar un séptimo bloque adicional de la cadena de bloques por parte del séptimo servidor de cadena de bloques, comprendiendo el séptimo bloque generado una séptima entrada asignada al módulo de programa con la segunda confirmación de legalización firmada.

Las formas de realización pueden tener la ventaja de que un documento virtual solo se considera autentificado y, por lo tanto, se puede utilizar realmente si hay una confirmación del pago de una tasa de legalización. Por tanto, las formas

de realización ofrecen un procedimiento para garantizar de manera eficaz que un documento virtual solo se pueda utilizar una vez que se hayan abonado las tasas correspondientes.

Según las formas de realización, el procedimiento comprende, además:

- recibir el documento virtual por parte de un tercer sistema informático,
- calcular el primer valor *hash* del documento virtual por parte del tercer sistema informático,
- solicitar a la cadena de bloques una entrada con el primer valor *hash* del documento virtual por parte del tercer sistema informático,
- en el caso de la existencia de la primera entrada con el primer valor *hash* del documento virtual, sin que exista una entrada con una confirmación de legalización, confirmar la existencia del documento virtual.

Las formas de realización pueden tener la ventaja de que el documento virtual puede ser presentado a un tercer sistema informático por el segundo sistema informático y este puede comprobar eficazmente si el documento virtual correspondiente existe oficialmente en la cadena de bloques.

Según las formas de realización, la confirmación de la existencia del documento virtual comprende una indicación a una posible legalización mediante el pago de la tasa de legalización. Las formas de realización pueden tener la ventaja de que se proporciona así un procedimiento eficaz para pagar una tasa de legalización. Si es necesario, la tasa correspondiente puede ser pagada por el titular del documento o por un destinatario del documento virtual que requiera legalización.

Según las formas de realización, si existe la entrada con el primer valor *hash* del documento virtual y una entrada con una confirmación de legalización para el primer valor *hash*, el procedimiento comprende, además, confirmar la legalización del documento virtual. Las formas de realización pueden tener la ventaja de que se proporciona un procedimiento para una legalización eficaz de documentos virtuales. Esto puede permitir que cualquier persona que disponga del correspondiente documento virtual compruebe la autenticidad de los documentos digitales o virtuales. Si el valor *hash* del documento virtual coincide con un valor *hash* legalizado, depositado en la cadena de bloques, se deduce que el documento virtual es un documento auténtico.

Las formas de realización comprenden, además, un sistema que comprende un primer sistema informático asignado a un expedidor, que está configurado para llevar a cabo un procedimiento según una de las formas de realización descritas anteriormente.

Según las formas de realización, el sistema comprende, además, un primer sistema informático de gestión que está asignado a una primera entidad de gestión y que está configurado para llevar a cabo un procedimiento según una de las formas de realización descritas anteriormente.

Según las formas de realización, el sistema comprende, además, un segundo sistema informático de gestión que está asignado a una segunda entidad de gestión y que está configurado para llevar a cabo un procedimiento según una de las formas de realización descritas anteriormente.

Según las formas de realización, el sistema comprende, además, un tercer sistema informático que está configurado para llevar a cabo un procedimiento según una de las formas de realización descritas anteriormente.

Según las formas de realización, el sistema comprende, además, al menos un servidor de cadena de bloques, que está configurado para llevar a cabo un procedimiento según una de las formas de realización descritas anteriormente.

El uso de números ordinales como primero, segundo, tercero, etc. sirve aquí, a menos que el contexto concreto indique claramente lo contrario, únicamente para distinguir entre diferentes elementos y no pretende implicar un orden concreto.

En el caso de los servidores de cadena de bloques anteriormente mencionados, es decir, del primer al séptimo servidor de cadena de bloques, todos o una parte de los mismos pueden ser un mismo o diferentes servidores de cadena de bloques, según las formas de realización.

Los sistemas informáticos de gestión primero y segundo anteriormente mencionados de la entidad de gestión primera o segunda pueden ser, según las formas de realización, diferentes o un mismo sistema informático de gestión de diferentes o una misma entidad de gestión. Por ejemplo, la primera entidad de gestión es una entidad de gestión del expedidor, que gestiona el y/o un grupo de expedidores. Por ejemplo, la primera y/o segunda entidad de gestión es una entidad de gestión del módulo de programa y/o de la cadena de bloques, que gestiona el módulo de programa y/o la cadena de bloques.

A continuación, se explican con más detalle formas de realización de la invención con referencia a los dibujos. Muestran:

la Figura 1 diagramas de bloques esquemáticos de una primera forma de realización de un sistema de ejemplo para la expedición de un documento virtual,
la Figura 2 un diagrama de bloques esquemático de una segunda forma de realización de un sistema de ejemplo para la expedición de un documento virtual,
la Figura 3 un diagrama UML esquemático de una forma de realización de un procedimiento de ejemplo para la expedición de un documento virtual,
la Figura 4 un diagrama de flujo esquemático de una forma de realización de un procedimiento de ejemplo para la expedición de un documento virtual,
la Figura 5 un diagrama de flujo esquemático de una forma de realización de un procedimiento de ejemplo para la provisión de una contraseña de registro,
la Figura 6 un diagrama de flujo esquemático de una forma de realización de un procedimiento de ejemplo para la provisión de un módulo de programa,
la Figura 7 un diagrama de flujo esquemático de una forma de realización de un procedimiento de ejemplo para la autentificación de un documento virtual, y
la Figura 8 un diagrama de flujo esquemático de una forma de realización de un procedimiento de ejemplo para la verificación de la autenticidad de un documento virtual.

Los elementos de las siguientes formas de realización que se corresponden entre sí se identifican mediante las mismas referencias.

Las figuras 1A y 1B muestran diagramas de bloques de una primera forma de realización de un sistema de ejemplo para la expedición de un documento virtual. El documento virtual es, por ejemplo, un certificado virtual 210 y el expedidor es, por ejemplo, una escuela. El certificado 210 es generado por el sistema informático escolar 200 ejecutando las instrucciones de programa 214 y es almacenado en la memoria 202 del sistema informático escolar 200. Las instrucciones de programa 214 son ejecutadas por un procesador del sistema informático escolar 200. La memoria 202 del sistema informático escolar 200 comprende, además, un área de memoria protegida 204 con la clave criptográfica privada 206 de un par de claves asimétricas, que están asignadas a la escuela como expedidor de certificados, tal como el certificado 210 asignado al certificado 210. Además, la memoria 202 comprende una clave criptográfica pública 208. El sistema informático escolar 200 utiliza la clave criptográfica privada 206, por ejemplo, para firmar objetos de datos, como por ejemplo un valor *hash* 104 del certificado 210, con el fin de acreditar su autenticidad. Finalmente, el sistema informático escolar 200 comprende una interfaz de comunicación para la comunicación a través de la red 160. La red 160 es, por ejemplo, Internet. La comunicación a través de la red 160 puede, adicional o alternativamente a una firma con una clave criptográfica privada del remitente, por ejemplo, protegerse criptográficamente mediante cifrado de los datos transmitidos con una clave criptográfica simétrica y/o una clave criptográfica pública asignada al destinatario. Por ejemplo, se utiliza una clave simétrica que se calcula utilizando el número pseudoaleatorio. La distribución de la clave criptográfica simétrica se puede proteger, por ejemplo, en forma de un esquema de cifrado híbrido utilizando un par de claves asimétricas. El cifrado híbrido comprende una combinación de cifrado asimétrico y cifrado simétrico. A este respecto, el remitente selecciona una clave simétrica aleatoria, por ejemplo, un número pseudoaleatorio, denominado clave de sesión. Los datos que se van a proteger se cifran simétricamente con esta clave de sesión. La clave de sesión se cifra asimétricamente con la clave pública del destinatario. Este procedimiento puede combinar la ventaja de una distribución segura de claves utilizando claves asimétricas con la ventaja de la velocidad del cifrado simétrico. Según las formas de realización, la transmisión tiene lugar a través de un enlace protegido por medio de un cifrado de extremo a extremo. Además, la transmisión se puede proteger, por ejemplo, mediante un cifrado de transporte adecuado, como por ejemplo HTTPS.

El sistema informático escolar 200 también calcula un valor *hash* 104 del certificado 210 y lo envía a través de la red 160 a uno de los servidores cadena de bloques 100, 130 de la red de cadena de bloques 170. Para calcular el valor *hash*, el sistema informático escolar 200 puede, por ejemplo, recurrir a su propio algoritmo *hash*, incluido en las instrucciones 214 de programa, o a un algoritmo *hash* proporcionado por el servidor de cadena de bloques 100. Según las formas de realización, la red de cadena de bloques 170 comprende un servidor de cadena de bloques 100; según formas de realización adicionales, la red de cadena de bloques 170 comprende una pluralidad de servidores de cadena de bloques 100, 130. Según las formas de realización, la red 160 comprende la red de cadena de bloques 170.

El servidor de cadena de bloques 100 comprende la cadena de bloques 110 en su memoria 108. La cadena de bloques 110 comprende una pluralidad de bloques 112, 116. Según las formas de realización, los bloques 112, 116 comprenden en cada caso una indicación de fecha y hora que indica el instante en el que se creó el bloque 112, 116 correspondiente. Por ejemplo, la indicación de fecha y hora comprende una fecha y una hora. Según las formas de realización, los bloques 112, 116 comprenden en cada caso una o más entradas 114, 118. Las entradas 114, 118 comprenden en cada caso, por ejemplo, una dirección que identifica la entrada en la cadena de bloques. Las entradas 114, 118 también pueden estar constituidas, por ejemplo, como transacciones y especifican en cada caso una dirección de origen "In" y una dirección de destino "Out" de la transacción correspondiente. La entrada 118 incluye además el módulo de programa (PM) 148, que incluye instrucciones de programa. Al ejecutar estas instrucciones de programa, se crean entradas 114 asignadas al módulo de programa 148 en la cadena de bloques 110 o se consultan y evalúan correspondientes entradas 114. Según las formas de realización, el módulo de programa 148 también puede estar almacenado distribuido en una pluralidad de entradas 118. Al ejecutar las instrucciones de programa del módulo de programa 148 por parte del procesador 102, el *hash* 104 del certificado 210 se almacena en la entrada 114 de la

cadena de bloques 110, por ejemplo. Al ejecutar las instrucciones de programa, el sistema informático escolar 200 y/o un sistema informático de gestión 600 de una entidad de gestión, tal como una autoridad escolar o una asociación, también pueden registrarse. El registro comprende, por ejemplo, crear una entrada en la cadena de bloques con una clave criptográfica pública de un par de claves asimétricas asignadas al correspondiente sistema informático 200, 600. Además, al ejecutar las instrucciones de programa, las contraseñas de registro para los correspondientes registros se pueden depositar en la cadena de bloques. Al ejecutar las instrucciones de programa, la entrada del *hash* 104 también puede legalizarse y las tasas abonadas para la legalización pueden repartirse a las partes involucradas a través de transacciones. Finalmente, la autenticidad de un certificado 210 se puede verificar comparando un valor *hash* calculado para el certificado con el valor *hash* 104 depositado en la cadena de bloques. En caso de coincidencia, el certificado 210 es auténtico.

El servidor de cadena de bloques 100 comprende, además, instrucciones de programa 106 que, por ejemplo, controlan la comunicación por medio de una interfaz de comunicación 120 a través de la red 160 y/o la red de cadena de bloques 170. Además, las instrucciones de programa 106 controlan, por ejemplo, el almacenamiento y la consulta de la cadena de bloques 110. Además, el servidor de cadena de bloques 100 comprende, por ejemplo, un par de claves asimétricas (no mostradas) para firmar datos y/o cifrar datos.

Los servidores de cadena de bloques 130 adicionales de la red de cadena de bloques 170 también comprenden procesadores 132, memorias 138 con la cadena de bloques y el módulo de programa 148, así como interfaces de comunicación 150. Además, los servidores de cadena de bloques 130 comprenden, por ejemplo, en cada caso un par de claves asimétricas (no mostradas) para firmar datos y/o cifrar datos.

El sistema informático 300 es, por ejemplo, un sistema informático de un titular del certificado 210. El certificado virtual 210 se envía al sistema informático 300 desde el sistema informático escolar 200 a través de la red 160. Un procesador 312 del sistema informático 300 está configurado, por ejemplo, para ejecutar instrucciones de programa 314. La ejecución de las instrucciones de programa 314 controla, por ejemplo, la recepción y/o un reenvío del certificado 210. El sistema informático 300 almacena el certificado 210 recibido en su memoria 302, por ejemplo. Para la comunicación a través de la red 160, el sistema informático 300 comprende una interfaz de comunicación 316. Además, el sistema informático 300 comprende, por ejemplo, un par de claves asimétricas (no mostradas) para firmar datos y/o cifrar datos.

El sistema informático 400 es, por ejemplo, un sistema informático de un destinatario del certificado 210. El destinatario del certificado 210 puede ser, por ejemplo, un empleador potencial del titular del certificado ante el que el titular del certificado desea postularse con el certificado 210. El certificado virtual 210 se envía al sistema informático 400 desde el sistema informático 300 a través de la red 160. Un procesador 412 del sistema informático 300 está configurado, por ejemplo, para ejecutar instrucciones de programa 414. La ejecución de las instrucciones de programa 414 controla la recepción del certificado 210, por ejemplo. El sistema informático 400 almacena el certificado 210 recibido en su memoria 402, por ejemplo. Para la comunicación a través de la red 160, el sistema informático 400 comprende una interfaz de comunicación 346. Además, el sistema informático 400 comprende, por ejemplo, un par de claves asimétricas (no mostradas) para firmar datos y/o cifrar datos.

Al ejecutar las instrucciones de programa 414 puede calcularse, además, un valor *hash* del certificado 210 y compararse con el valor *hash* 104 depositado en la cadena de bloques 110. Si ambos valores *hash* coinciden, el certificado 210 que envió el titular del certificado es un certificado auténtico. Para calcular el valor *hash*, el sistema informático 400 puede, por ejemplo, recurrir a su propio algoritmo *hash*, incluido en las instrucciones 414 de programa, o a un algoritmo *hash* proporcionado por el servidor de cadena de bloques 100.

El sistema informático de gestión 500 es, por ejemplo, un sistema informático de una entidad de gestión de la cadena de bloques 110 o del módulo de programa 148. Por ejemplo, se trata de un proveedor de la cadena de bloques 110 o del módulo de programa 148. Un procesador 512 del sistema informático de gestión 500 está configurado para ejecutar instrucciones de programa 514. Al ejecutar las instrucciones de programa 514 se crea, por ejemplo, el módulo de programa 148 y se envía a través de la red 160 a los servidores de cadena de bloques para su entrada en la cadena de bloques 110. Para la comunicación a través de la red 160, el sistema informático de gestión 500 comprende una interfaz de comunicación 516. La memoria 502 comprende, además, una clave criptográfica pública 508 de un par de claves asimétricas asignadas al proveedor. Además, el sistema informático de gestión 500 puede almacenar una clave criptográfica privada 504 del par de claves asimétricas en un área de memoria protegida 604. La clave criptográfica privada 504 se puede utilizar, por ejemplo, para firmar el módulo de programa 148, pudiendo verificarse la firma resultante con la clave criptográfica pública 508. Por un lado, la firma puede servir como prueba de la autenticidad del módulo de programa 148; por otro lado, la firma puede servir como prueba de autorización del sistema informático de gestión 500 para introducir el módulo de programa en la cadena de bloques 110.

Además, puede estar previsto un sistema informático de gestión 600 de una entidad de gestión, tal como una autoridad escolar o una asociación. Por ejemplo, los datos 610 de la escuela con el sistema informático escolar 200, tales como su dirección, están almacenados en una memoria 602 del sistema informático de gestión 600. La memoria 602 comprende, además, una clave criptográfica pública 608 de un par de claves asimétricas asignadas a la entidad de gestión. Además, el sistema informático de gestión 600 puede almacenar una clave criptográfica privada 604 del par

de claves asimétricas en un área de memoria protegida 604. Un procesador 612 del sistema informático de gestión 600 está configurado para ejecutar instrucciones de programa 614. Al ejecutar las instrucciones de programa 614 tiene lugar, por ejemplo, una provisión de una contraseña de registro para registrar el sistema informático escolar 200 en una entrada en la cadena de bloques 110. La clave criptográfica privada 604 se puede utilizar, por ejemplo, para firmar la contraseña de registro, pudiendo verificarse la firma resultante con la clave criptográfica pública 608. Además, se proporciona la correspondiente contraseña de registro al sistema informático escolar 200 para el registro. Finalmente, el sistema informático de gestión 600 comprende una interfaz de comunicación 616 para la comunicación a través de la red 160.

La figura 2 muestra un diagrama de bloques de una segunda forma de realización de un sistema de ejemplo para la expedición de un documento virtual 210. Los sistemas informáticos mostrados, es decir, el sistema informático escolar 200, el servidor de cadena de bloques 100, el sistema informático 300 y el sistema informático 400, están diseñados de manera análoga a los correspondientes sistemas informáticos de la figura 1A. La figura 2 ilustra la comunicación entre los sistemas informáticos con más detalle. El sistema informático escolar 200 genera un documento virtual en forma de certificado 210. Se calcula un valor *hash* 104 para el certificado 210 creado. Para ello, el sistema informático escolar 200 consulta, por ejemplo, un algoritmo *hash* 119 proporcionado por el servidor de cadena de bloques 100 en un navegador. El valor *hash* 104 calculado se transmite al servidor de cadena de bloques 100 y este último lo introduce en una entrada 114 de un bloque 112 adicional de la cadena de bloques 110.

El certificado 210 creado se envía desde el sistema informático escolar 200 al sistema informático 300 del titular del certificado. El titular del certificado reenvía el certificado 210 a un sistema informático 400, por ejemplo. Si el sistema informático 400 desea comprobar la autenticidad del certificado 210 recibido desde el sistema informático 300 del titular del certificado, el sistema informático 400 calcula el valor *hash* 104 con un algoritmo *hash* 119 proporcionado por el servidor de cadena de bloques 100 y lo compara con el valor *hash* almacenado en la entrada 114 de la cadena de bloques 110. Si los dos valores *hash* coinciden, el certificado 210 presentado es un documento auténtico.

La figura 3 muestra un diagrama UML de una forma de realización de un procedimiento de ejemplo para la expedición de un documento virtual 210. En la etapa ⓐ, el proveedor 500 genera un módulo de programa 148 que se almacena en la cadena de bloques 110. En la etapa ⓑ, una entidad de gestión 600, tal como una autoridad escolar o una asociación, se registra con una contraseña de registro 1234. La entidad de gestión 600 recibe la correspondiente contraseña de registro del proveedor 500, por ejemplo, por correo postal a petición. En el transcurso del registro, por ejemplo, una clave criptográfica pública asignada a la entidad de gestión 600 se almacena en una entrada 114 de la cadena de bloques 110. Con esta clave criptográfica pública se pueden verificar las firmas de la entidad de gestión 600, que fueron creadas con una clave criptográfica privada asignada a la clave criptográfica pública. Si las entradas en la cadena de bloques tienen lugar en forma de transacciones con direcciones de origen y de destino, esta clave criptográfica pública también puede servir como la dirección de recepción de la entidad de gestión 600. En la etapa ⓒ, una contraseña de registro 1111 para el registro de la escuela 200 por medio del módulo de programa 148 en la cadena de bloques 110 se envía a la escuela 200, que está subordinada a la entidad de gestión 600. Esto puede tener lugar, por ejemplo, por correo postal para aumentar la seguridad. En la etapa ⓓ, la escuela se registra con la contraseña de registro 1111 recibida desde la entidad de gestión 600 a través del módulo de programa 148 en la cadena de bloques 110. En este caso, por ejemplo, se genera una entrada 114 con una clave criptográfica pública en la cadena de bloques 110. Con esta clave criptográfica pública se pueden verificar las firmas de la escuela 200, que fueron creadas con una clave criptográfica privada asignada a la clave criptográfica pública. Si las entradas en la cadena de bloques tienen lugar en forma de transacciones con direcciones de origen y de destino, esta clave criptográfica pública también puede servir como la dirección de recepción de la escuela 200. Una vez registrada, la escuela 200 puede registrar certificados. Para ello, en la etapa ⓔ se calcula un valor *hash* 5555 para un certificado y el certificado con este valor *hash* 5555 se registra en una entrada 114 de la cadena de bloques 110 usando el módulo de programa 148. Dado que la escuela 200 está registrada, se acepta la entrada. Sin embargo, con este registro, el certificado aún no está legalizado. En la etapa ⓕ, la escuela envía además el certificado al titular del certificado 300. Por ejemplo, cualquier usuario 300, 400, 600, 200 puede verificar el estado del certificado. Por ejemplo, recibe a este respecto la respuesta: El certificado se puede legalizar. Por ejemplo, el titular del certificado 300 paga mediante transferencia la tasa de legalización, por ejemplo, 5 €, al proveedor 500. Según formas de realización alternativas, la transferencia también se puede realizar a la escuela 200 o a la entidad de gestión 600. La transferencia se puede realizar a través de la cadena de bloques, por ejemplo, si esta proporciona una opción para transacciones en una criptomoneda. Como alternativa, la tasa de legalización también se puede pagar mediante transferencia a través de una cuenta corriente habitual proporcionada por el proveedor 500, por ejemplo. Por ejemplo, la transferencia menciona el *hash* 5555 como concepto. Un script del proveedor 500 verifica el recibo de las tasas y, en la etapa ⓖ, cambia el estado del certificado en la cadena de bloques 110 de registrado a pagado, es decir, legalizado. En este caso, se almacena una confirmación de legalización en una entrada 114 de la cadena de bloques 110. A partir de este instante, un usuario que compruebe el estado del certificado recibirá la respuesta de que el certificado está legalizado. En la etapa ⓗ, la tasa de legalización recibida se reparte a la escuela 200, la entidad de gestión 600 y el proveedor 500, por ejemplo, según una clave predefinida. Esto puede tener lugar, por ejemplo, mediante transacciones utilizando la cadena de bloques 110. En la etapa ⓙ, el titular del certificado 300 envía al usuario 400, por ejemplo. Este puede verificar, en la etapa ⓙ, el estado del certificado calculando su valor *hash* y comparando el valor *hash* calculado

usando el módulo de programa 148 con el valor *hash* almacenado en una entrada 114 de la cadena de bloques 110. Si ambos valores *hash* coinciden, el usuario recibe la información de que el certificado es auténtico y está legalizado.

La figura 4 muestra un diagrama de flujo de una forma de realización de un procedimiento de ejemplo para la expedición de un documento virtual. En el bloque 700, la escuela envía una solicitud de registro a un servidor de cadena de bloques. En el bloque 702, la solicitud de registro se envía al servidor de cadena de bloques. En el bloque 704, el servidor de cadena de bloques recibe la solicitud de registro y verifica la validez de la solicitud de registro utilizando un módulo de programa proporcionado por la cadena de bloques. Por ejemplo, la escuela se registra utilizando una contraseña de registro. Por ejemplo, la solicitud de registro es válida si la contraseña de registro es válida. En respuesta a una solicitud de registro válida, el módulo de programa en la cadena de bloques registra la escuela, en el bloque 706. Por ejemplo, una clave criptográfica pública de la escuela se almacena en este caso en la cadena de bloques. En el bloque 708, la escuela recibe una solicitud para expedir un documento, por ejemplo, un certificado. En el bloque 710, la escuela crea el certificado. En el bloque 712, la escuela calcula un valor *hash* del documento creado. En el bloque 714, se crea una solicitud de entrada para introducir el valor *hash* en la cadena de bloques. En el bloque 716, la solicitud de entrada se envía desde la escuela a un servidor de cadena de bloques, que recibe la solicitud de entrada, en el bloque 718. Si se trata de una solicitud de entrada válida, que comprende, por ejemplo, una firma válida con una clave criptográfica privada de la escuela, se introduce el valor *hash*, en el bloque 720, en la cadena de bloques y se registra así el certificado. Luego, la escuela envía el certificado registrado al titular del certificado, por ejemplo.

La figura 5 muestra un diagrama de flujo de una forma de realización de un procedimiento de ejemplo para la provisión de una contraseña de registro. En el bloque 800, una entidad de gestión responsable de la escuela, o un proveedor de la cadena de bloques o el módulo de programa, calcula una contraseña de registro. En el bloque 802, se calcula un valor *hash* de la contraseña de registro. En el bloque 804, el valor *hash* se cifra con una clave criptográfica privada de la entidad de gestión o del proveedor. Se crea una solicitud de provisión, en el bloque 806, y se envía a un servidor de cadena de bloques, en el bloque 808. El servidor de cadena de bloques recibe la solicitud de provisión, en el bloque 810, y almacena la contraseña de registro, en el bloque 812, usando el módulo de programa en una entrada en la cadena de bloques, si la solicitud de provisión es válida. La solicitud de provisión es válida, por ejemplo, si la entidad de gestión o el proveedor están registrados por el módulo de programa, es decir, una entrada de la cadena de bloques asignada al módulo de programa comprende una clave criptográfica pública de la entidad de gestión o del proveedor, y la solicitud de provisión comprende una firma con una clave criptográfica privada asignada a la clave criptográfica pública.

La figura 6 muestra un diagrama de flujo de una forma de realización de un procedimiento de ejemplo para la provisión de un módulo de programa. En el bloque 900, un proveedor crea un módulo de programa. En el bloque 902, se crea una solicitud de inicialización para el módulo de programa y, en el bloque 904, se envía a un servidor de cadena de bloques. En el bloque 906, se recibe la solicitud de inicialización y se introduce en la cadena de bloques, en el bloque 908. Según ejemplos de realización, la entrada tiene lugar si la solicitud de inicialización comprende una firma del proveedor.

La figura 7 muestra un diagrama de flujo de una forma de realización de un procedimiento de ejemplo para legalizar un documento virtual. En el bloque 1000, se paga una tasa de legalización para un certificado registrado en la cadena de bloques. Esto puede tener lugar, por ejemplo, mediante criptomonedas o de manera convencional mediante transferencia, pago con tarjeta de crédito o un servicio de pago como PayPal®. En el bloque 1002, por ejemplo, el proveedor recibe una confirmación de pago de la tasa de legalización. Luego, el proveedor crea, en el bloque 1004, una confirmación de legalización firmada, que envía a un servidor de cadena de bloques, en el bloque 1006. En el bloque 1008, el servidor de cadena de bloques recibe la confirmación de legalización y, en el bloque 1010, la introduce usando el módulo de programa en la cadena de bloques. Según las formas de realización, la entrada tiene lugar si la firma de la confirmación de legalización es válida. En el bloque 1012, se generan además una o más instrucciones de transacción con las que se transfieren partes de la tasa de legalización, por ejemplo conforme a una clave de reparto predefinida, a la escuela que expidió el certificado y, dado el caso, a una entidad de gestión de orden superior a la escuela, usando una criptomoneda. En el bloque 1014, la instrucción de transacción se envía desde el proveedor a un servidor de cadena de bloques y, en el bloque 1016, es recibida por este último. Si la instrucción de la transacción es válida, es decir, por ejemplo, está incluida con una firma del proveedor, y el proveedor está autorizado a transferir los importes especificados, en el bloque 1018 tiene lugar una entrada de las transacciones en la cadena de bloques.

La figura 8 muestra un diagrama de flujo de una forma de realización de un procedimiento de ejemplo para verificar la autenticidad de un documento virtual. En el bloque 1100, el certificado virtual se recibe de un usuario. Por ejemplo, el usuario sería un futuro empleador potencial ante el que se postula el titular del certificado. Para verificar la validez del certificado presentado, el usuario calcula un valor *hash* del certificado, en el bloque 1102. En el bloque 1104, se envía una solicitud de verificación con el valor *hash* a un servidor de cadena de bloques, que recibe la solicitud de verificación, en el bloque 1106. En el bloque 1108, usando el módulo de programa se verifica si el valor *hash* calculado está introducido en la cadena de bloques del certificado. Además, en la etapa 1110 se verifica si el certificado también está legalizado, es decir, si hay una nota acerca del pago de las tasas de legalización. Sobre la base de los resultados de la verificación, en el bloque 1112, se crea una respuesta a la solicitud de verificación y, en el bloque 1114, se envía

desde el servidor de cadena de bloques al usuario. En el bloque 1116, el usuario recibe la respuesta. Si el certificado está introducido y legalizado, la respuesta le informará de ello.

Lista de referencias

100	servidor de cadena de bloques
102	procesador
104	valor *hash*
106	instrucciones de programa
108	memoria
110	cadena de bloques
112	bloque
114	entrada
116	bloque
118	entrada
119	algoritmo *hash*
120	interfaz de comunicación
130	servidor de cadena de bloques
132	procesador
138	memoria
148	módulo de programa
150	interfaz de comunicación
160	red
170	red de cadena de bloques
200	sistema informático escolar
202	memoria
204	área de memoria protegida
206	clave privada
208	clave pública
210	testigo
212	procesador
214	instrucciones de programa
216	interfaz de comunicación
300	sistema informático (titular del certificado)
302	memoria
312	procesador
314	instrucciones de programa
316	interfaz de comunicación
400	sistema informático (destinatario del certificado)
402	memoria
412	procesador
414	instrucciones de programa
416	interfaz de comunicación
500	sistema informático de gestión (cadena de bloques)
502	memoria
504	área de memoria protegida
506	clave privada
508	clave pública
512	procesador
514	instrucciones de programa
516	interfaz de comunicación
600	sistema informático de gestión (escuelas)
602	memoria
604	área de memoria protegida
606	clave privada
608	clave pública
612	procesador
614	instrucciones de programa
616	interfaz de comunicación

REIVINDICACIONES

1. Procedimiento para la expedición de un documento virtual (210) por medio de un primer sistema informático (200) de un expedidor, comprendiendo el primer sistema informático (200) una memoria (202), estando almacenada en la memoria (202) una clave criptográfica pública (208) de un par de claves asimétricas asignadas al expedidor, estando almacenada una clave criptográfica privada (206) del par de claves asimétricas del expedidor en un área de memoria protegida (204) de la memoria (202), comprendiendo el primer sistema informático (200) una interfaz de comunicación (216) para la comunicación a través de una red (160),
en donde el documento virtual (210) se expide utilizando una cadena de bloques (110), comprendiendo la cadena de bloques (110) en un bloque (116) un módulo de programa (148) con primeras y segundas instrucciones de programa, generándose mediante la ejecución de las instrucciones de programa entradas (112) asignadas al módulo de programa (148) en la cadena de bloques (110),
comprendiendo el procedimiento:

• crear una solicitud de registro por parte del primer sistema informático (200), comprendiendo la solicitud de registro la clave criptográfica pública (208) del expedidor e identificando el módulo de programa (148),
• enviar la solicitud de registro por parte del primer sistema informático (200) a través de la red a un primer servidor de cadena de bloques (100, 130), estando configurado el primer servidor de cadena de bloques (100, 130) para generar bloques de la cadena de bloques (110),
• recibir la solicitud de registro por parte del primer servidor de cadena de bloques (100, 130),
• ejecutar las primeras instrucciones de programa del módulo de programa (148) identificado por la solicitud de registro por parte del primer servidor de cadena de bloques (100, 130), comprendiendo la ejecución de las primeras instrucciones de programa verificar la validez de la solicitud de registro y, en el caso de una solicitud de registro válida, para registrar la clave criptográfica pública (208) del expedidor, generar un primer bloque adicional de la cadena de bloques (110), comprendiendo el primer bloque generado una primera entrada asignada al módulo de programa (148) con la clave criptográfica pública (208) del expedidor,
• recibir una solicitud por parte del primer sistema informático (200) para la expedición del documento virtual (210),
• crear el documento virtual (210) por parte del primer sistema informático (200),
• calcular un primer valor *hash* (104) del documento virtual (210) por parte del primer sistema informático (200),
• crear una solicitud de entrada firmada con la clave criptográfica privada (206) del expedidor por parte del primer sistema informático (200), comprendiendo la solicitud de entrada el primer valor *hash* (104) e identificando el módulo de programa (148),
• enviar la solicitud de entrada firmada por parte del primer sistema informático (200) a través de la red a un segundo servidor de cadena de bloques (100, 130), que está configurado para generar bloques de la cadena de bloques (110),
• recibir la solicitud de entrada firmada por parte del segundo servidor de cadena de bloques (100, 130),
• ejecutar las segundas instrucciones de programa del módulo de programa (148) identificado por la solicitud de entrada firmada por parte del segundo servidor de cadena de bloques (100, 130), comprendiendo la ejecución de las segundas instrucciones de programa verificar la firma de la solicitud de entrada utilizando la clave criptográfica pública (208) del expedidor registrada en la cadena de bloques (110), y, en el caso de una firma válida, para expedir el documento virtual (210), generar un segundo bloque (112) adicional de la cadena de bloques (110), comprendiendo el segundo bloque (114) generado una segunda entrada asignada al módulo de programa (148) con el primer valor *hash* (104).

2. Procedimiento según la reivindicación 1, en donde la solicitud de registro comprende una contraseña de registro y en donde la verificación de la validez de la solicitud de registro comprende verificar la validez de la contraseña de registro.

3. Procedimiento según una de las reivindicaciones anteriores, en donde el procedimiento comprende, además:
enviar el documento virtual (210) a un segundo sistema informático (300) en respuesta a la solicitud de expedición del documento virtual (210), y/o
en donde la solicitud de registro comprende, además, un ID de expedidor que, si la contraseña de registro se ha verificado con éxito, se introduce en el segundo bloque (112) de la cadena de bloques (110) junto con la clave criptográfica pública (208), y/o
en donde la verificación de la contraseña de registro comprende:

• comparar la contraseña de registro recibida por parte del primer servidor de cadena de bloques (100, 130) con una contraseña de registro almacenada en la cadena de bloques (110),
• si la contraseña de registro recibida coincide con la contraseña de registro almacenada, confirmar la validez de la contraseña de registro recibida por parte del primer servidor de cadena de bloques (100, 130), y/o

en donde el documento virtual (210) es un certificado virtual.

4. Procedimiento según una de las reivindicaciones anteriores, en donde la contraseña de registro se proporciona en forma de un segundo valor *hash* almacenado firmado en la cadena de bloques (110), comprendiendo la comparación de la contraseña de registro recibida con la contraseña de registro almacenada:

• verificar la validez de la firma del segundo valor *hash* almacenado,
• calcular un tercer valor *hash* de la contraseña de registro recibida,
• comparar el tercer valor *hash* calculado con el segundo valor *hash* almacenado.

5. Procedimiento según la reivindicación 4, en donde el módulo de programa (148) comprende terceras instrucciones de programa, y en donde la provisión de la contraseña de registro comprende:

• calcular el segundo valor *hash* de la contraseña de registro por parte de un primer sistema informático de gestión (500, 600) de una primera entidad de gestión,
• firmar el segundo valor *hash* con una clave criptográfica privada (506, 606) de un par de claves asimétricas asignadas a la primera entidad de gestión,
• crear una solicitud de provisión por parte del primer sistema informático de gestión (500, 600), comprendiendo la solicitud de provisión el segundo valor *hash* firmado e identificando el módulo de programa (148),
• enviar la solicitud de provisión por parte del primer sistema informático de gestión (500, 600) a un tercer servidor de cadena de bloques (100, 130), que está configurado para generar bloques de la cadena de bloques (110),
• recibir la solicitud de provisión por parte del tercer servidor de cadena de bloques (100, 130),
• ejecutar las terceras instrucciones de programa del módulo de programa (148) identificado por la solicitud de provisión por parte del tercer servidor de cadena de bloques (100, 130), comprendiendo la ejecución de las terceras instrucciones de programa verificar la firma del segundo valor *hash* por parte del tercer servidor de cadena de bloques (100, 130) utilizando una clave criptográfica pública (508, 608) del par de claves asimétricas asignadas a la primera entidad de gestión y, en el caso de una firma válida, generar un tercer bloque adicional de la cadena de bloques (110) mediante el tercer servidor de cadena de bloques (100, 130), comprendiendo el tercer bloque generado una tercera entrada asignada al módulo de programa (148) con el segundo valor *hash* firmado.

6. Procedimiento según la reivindicación 5, en donde la clave criptográfica pública (508, 608) de la primera entidad de gestión está almacenada en la cadena de bloques (110) y el tercer servidor de cadena de bloques (100, 130) utiliza, para verificar la firma del segundo valor *hash*, la clave criptográfica pública (508, 608) del primer sistema informático de gestión (500, 600) almacenada en la cadena de bloques (110).

7. Procedimiento según una de las reivindicaciones 5 a 6, en donde el procedimiento comprende, además:

• enviar una solicitud de contraseña para obtener la contraseña de registro por parte del primer sistema informático (200) al primer sistema informático de gestión (500, 600), identificando la solicitud de contraseña al expedidor,

en donde el procedimiento comprende, además, por parte de la primera entidad de gestión, utilizando el primer sistema informático de gestión (500, 600):

• recibir la solicitud de contraseña,
• identificar una dirección postal asignada al expedidor,
• crear un escrito de respuesta dirigido a la dirección postal identificada, que comprende la contraseña de registro,
• enviar el escrito de respuesta por correo postal,

o en donde el procedimiento comprende, además:

• enviar una solicitud de contraseña para obtener la contraseña de registro por parte del primer sistema informático (200) al primer sistema informático de gestión (500, 600), identificando la solicitud de contraseña al expedidor,

en donde el procedimiento comprende, además, por parte de la primera entidad de gestión, utilizando el primer sistema informático de gestión (500, 600):

• recibir la solicitud de contraseña,
• crear una respuesta a la solicitud de contraseña, que comprende la contraseña de registro,
• enviar la respuesta en forma protegida criptográficamente al primer sistema informático (200) del expedidor.

8. Procedimiento según una de las reivindicaciones anteriores, en donde el procedimiento comprende, además:

• crear el módulo de programa (148) por parte de un segundo sistema informático de gestión (500) de una segunda entidad de gestión,
• crear una solicitud de inicialización firmada por parte del segundo sistema informático de gestión (500) con el módulo de programa (148),
• enviar la solicitud de inicialización por parte del segundo sistema informático de gestión (500) a un cuarto servidor de cadena de bloques (100, 130), que está configurado para generar bloques de la cadena de bloques (110),
• recibir el módulo de programa (148) por parte del cuarto servidor de cadena de bloques (100, 130),
• verificar la firma de la solicitud de inicialización por parte del cuarto servidor de cadena de bloques (100, 130) utilizando la clave criptográfica pública (508, 608) del par de claves asimétricas asignadas a la segunda entidad de gestión y, en el caso de una firma válida, generar un cuarto bloque (116) adicional de la cadena de bloques (110) por

parte del cuarto servidor de cadena de bloques (100, 130), comprendiendo el cuarto bloque generado (116) una cuarta entrada (118) con el módulo de programa (148).

9. Procedimiento según una de las reivindicaciones anteriores, en donde el módulo de programa (148) comprende cuartas instrucciones de programa y en donde el procedimiento comprende, además:

• recibir una primera confirmación de pago de una tasa de legalización por la expedición del documento virtual (210) por parte del segundo sistema informático de gestión (500),
• crear una primera confirmación de legalización por parte del segundo sistema informático de gestión (500), comprendiendo la confirmación de legalización el primer valor *hash* (104) firmado del documento virtual (210) e identificando el módulo de programa (148),
• firmar la primera confirmación de legalización por parte del segundo sistema informático de gestión (500) con la clave criptográfica privada (506) de la segunda entidad de gestión,
• enviar la primera confirmación de legalización firmada a un quinto servidor de cadena de bloques (100, 130), que está configurado para generar bloques de la cadena de bloques (110),
• recibir la primera confirmación de legalización por parte del quinto servidor de cadena de bloques (100, 130),
• ejecutar las cuartas instrucciones de programa del módulo de programa (148) identificado por la confirmación de legalización por parte del quinto servidor de cadena de bloques (100, 130), comprendiendo la ejecución de las cuartas instrucciones de programa verificar la firma de la primera confirmación de legalización por parte del quinto servidor de cadena de bloques (100, 130) utilizando la clave criptográfica pública (508) de la segunda entidad de gestión y, en el caso de una firma válida, generar un quinto bloque adicional de la cadena de bloques (110) por parte del quinto servidor de cadena de bloques (100, 130), comprendiendo el quinto bloque generado una quinta entrada asignada al módulo de programa (148) con la primera confirmación de legalización firmada.

10. Procedimiento según la reivindicación 9, en donde el módulo de programa (148) comprende quintas instrucciones de programa, y en donde el procedimiento comprende, además:

• generar una instrucción de transacción por parte del segundo sistema informático de gestión (500) para la transacción de al menos un importe parcial de la tasa de legalización en forma de criptomoneda implementada en la cadena de bloques (110) desde una dirección de origen asignada a la segunda entidad de gestión hasta una dirección de destino asignada al expedidor,
• firmar la instrucción de transacción con una clave criptográfica privada (506) de un par de claves asimétricas asignadas a la dirección de origen,
• enviar la instrucción de transacción a un sexto servidor de cadena de bloques (100, 130), que está configurado para generar bloques de la cadena de bloques (110),
• recibir la instrucción de transacción por parte del sexto servidor de cadena de bloques (100, 130),
• ejecutar las quintas instrucciones de programa del módulo de programa (148) identificado por la solicitud de provisión por parte del sexto servidor de cadena de bloques (100, 130), comprendiendo la ejecución de las quintas instrucciones de programa verificar la firma de la instrucción de transacción por parte del sexto servidor de cadena de bloques (100, 130) utilizando la dirección de origen y, en el caso de una firma válida, generar un sexto bloque adicional de la cadena de bloques (110) por parte del sexto servidor de cadena de bloques (100, 130), comprendiendo el sexto bloque generado una sexta entrada asignada al módulo de programa (148) con la instrucción de transacción.

11. Procedimiento según una de las reivindicaciones 1 a 8, en donde el módulo de programa (148) comprende sextas instrucciones de programa, y en donde el procedimiento comprende, además:

• recibir una segunda confirmación de pago de la tasa de legalización por la expedición del documento virtual (210) por parte del primer sistema informático (200),
• crear una segunda confirmación de legalización por parte del primer sistema informático (200), comprendiendo la confirmación de legalización el primer valor *hash* (104) firmado del documento virtual (210) e identificando el módulo de programa (148),
• firmar la segunda confirmación de legalización por parte del primer sistema informático (200) con la clave criptográfica privada (206) del expedidor,
• enviar la segunda confirmación de legalización firmada a un séptimo servidor de cadena de bloques (100, 130), que está configurado para generar bloques de la cadena de bloques (110),
• recibir la segunda confirmación de legalización por parte del séptimo servidor de cadena de bloques (100, 130),
• ejecutar las sextas instrucciones de programa del módulo de programa (148) identificado por la segunda confirmación de legalización por parte del séptimo servidor de cadena de bloques (100, 130), comprendiendo la ejecución de las sextas instrucciones de programa verificar la firma de la segunda confirmación de legalización por parte del séptimo servidor de cadena de bloques (100, 130) utilizando la clave criptográfica pública (208) del expedidor y, en el caso de una firma válida, generar un séptimo bloque adicional de la cadena de bloques (110) por parte del séptimo servidor de cadena de bloques (100, 130), comprendiendo el séptimo bloque generado una séptima entrada asignada al módulo de programa (148) con la segunda confirmación de legalización firmada.

12. Procedimiento según una de las reivindicaciones anteriores, en donde el procedimiento comprende, además:

• recibir el documento virtual (210) por parte de un tercer sistema informático (400),
• calcular el primer valor *hash* (104) del documento virtual (210) por parte del tercer sistema informático,
• solicitar a la cadena de bloques (110) una entrada con el primer valor *hash* (104) del documento virtual (210) por parte del tercer sistema informático (400),
• en el caso de la existencia de la primera entrada con el primer valor *hash* (104) del documento virtual (210), sin que exista una entrada con una confirmación de legalización, confirmar la existencia del documento virtual (210).

13. Procedimiento según la reivindicación 12, en donde la confirmación de la existencia del documento virtual (210) comprende una indicación a una posible legalización mediante el pago de la tasa de legalización, y/o en donde el procedimiento comprende, además:
si existe la entrada con el primer valor *hash* (104) del documento virtual (210) así como una entrada con una confirmación de legalización para el primer valor *hash* (104), confirmar la legalización del documento virtual (210).

14. Sistema que comprende un primer sistema informático (200) asignado a un expedidor y que está configurado para llevar a cabo un procedimiento según una de las reivindicaciones 1 a 13.

15. Sistema según la reivindicación 14, que comprende, además, un primer sistema informático de gestión (500, 600) que está asignado a una primera entidad de gestión y está configurado para llevar a cabo un procedimiento según una de las reivindicaciones 5 a 13, y/o que comprende, además, un segundo sistema informático de gestión (500), que está asignado a una segunda entidad de gestión y está configurado para llevar a cabo un procedimiento según una de las reivindicaciones 8 a 13, y/o
que comprende, además, un tercer sistema informático (400) que está configurado para llevar a cabo un procedimiento según una de las reivindicaciones 12 a 13, y/o
que comprende, además, al menos un servidor de cadena de bloques (100, 130) que está configurado para llevar a cabo un procedimiento según una de las reivindicaciones 1 a 13.

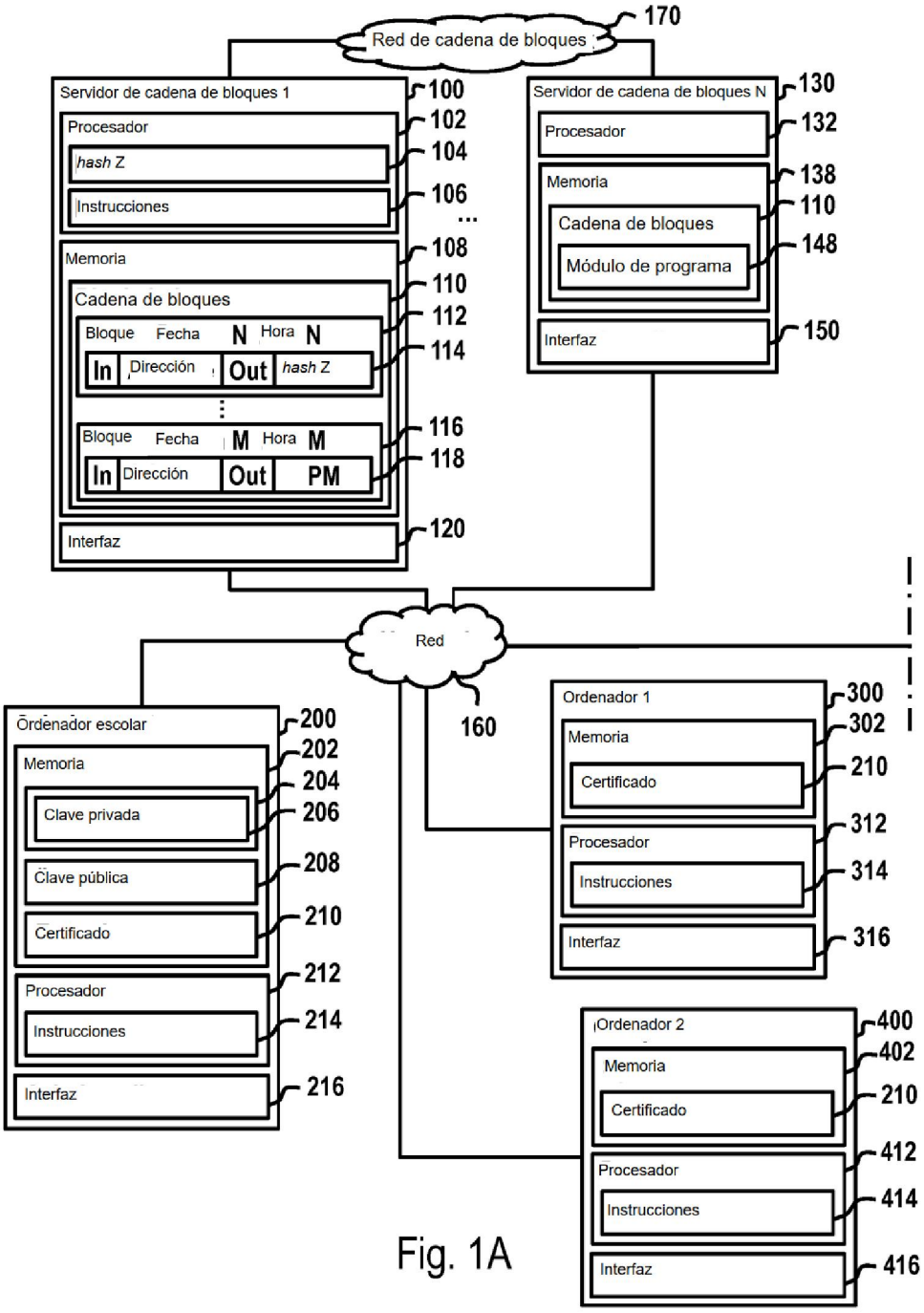
Red de cadena de bloques
170
Servidor de cadena de bloques 1
100
Procesador
102
hash Z
104
Instrucciones
106
Memoria
108
Cadena de bloques
110
Bloque Fecha N Hora N
112
In Dirección Out hash Z
114
Bloque Fecha M Hora M
116
In Dirección Out PM
118
Interfaz
120
Servidor de cadena de bloques N
130
Procesador
132
Memoria
138
Cadena de bloques
110
Módulo de programa
148
Interfaz
150
Red
160
Ordenador escolar
200
Memoria
202
Clave privada
204
Clave pública
206
Certificado
208
Procesador
210
Instrucciones
212
Interfaz
214
216
Ordenador 1
300
Memoria
302
Certificado
210
Procesador
312
Instrucciones
314
Interfaz
316
Ordenador 2
400
Memoria
402
Certificado
210
Procesador
412
Instrucciones
414
Interfaz
416

Fig. 1A

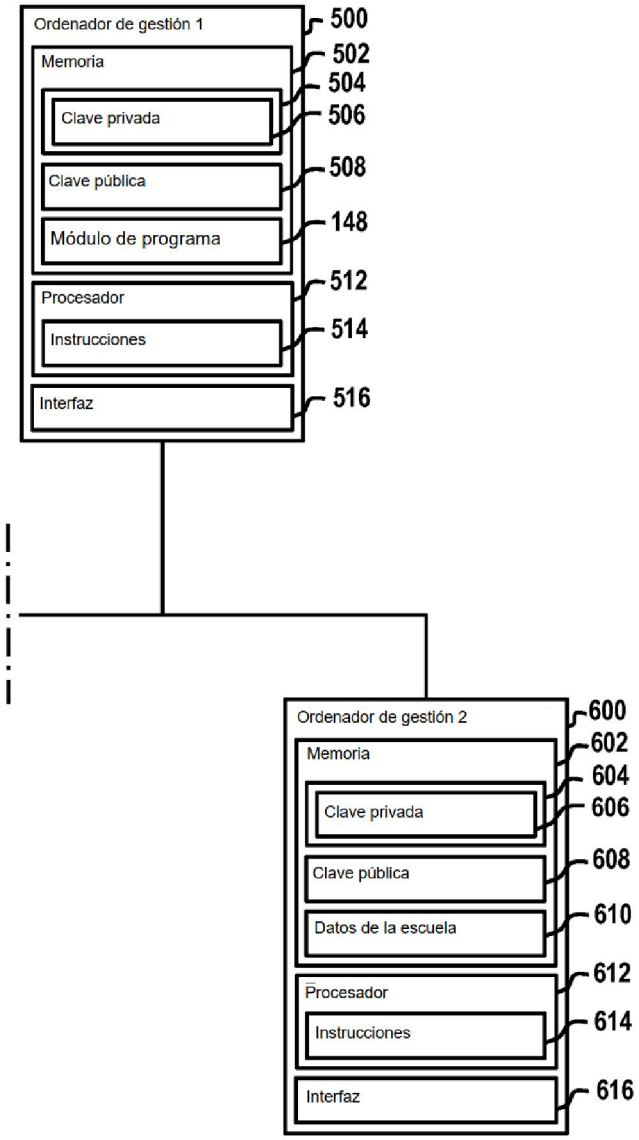
Ordenador de gestión 1
500
Memoria
502
Clave privada
504
506
Clave pública
508
Módulo de programa
148
Procesador
512
Instrucciones
514
Interfaz
516
Ordenador de gestión 2
600
Memoria
602
Clave privada
604
606
Clave pública
608
Datos de la escuela
610
Procesador
612
Instrucciones
614
Interfaz
616

Fig. 1B

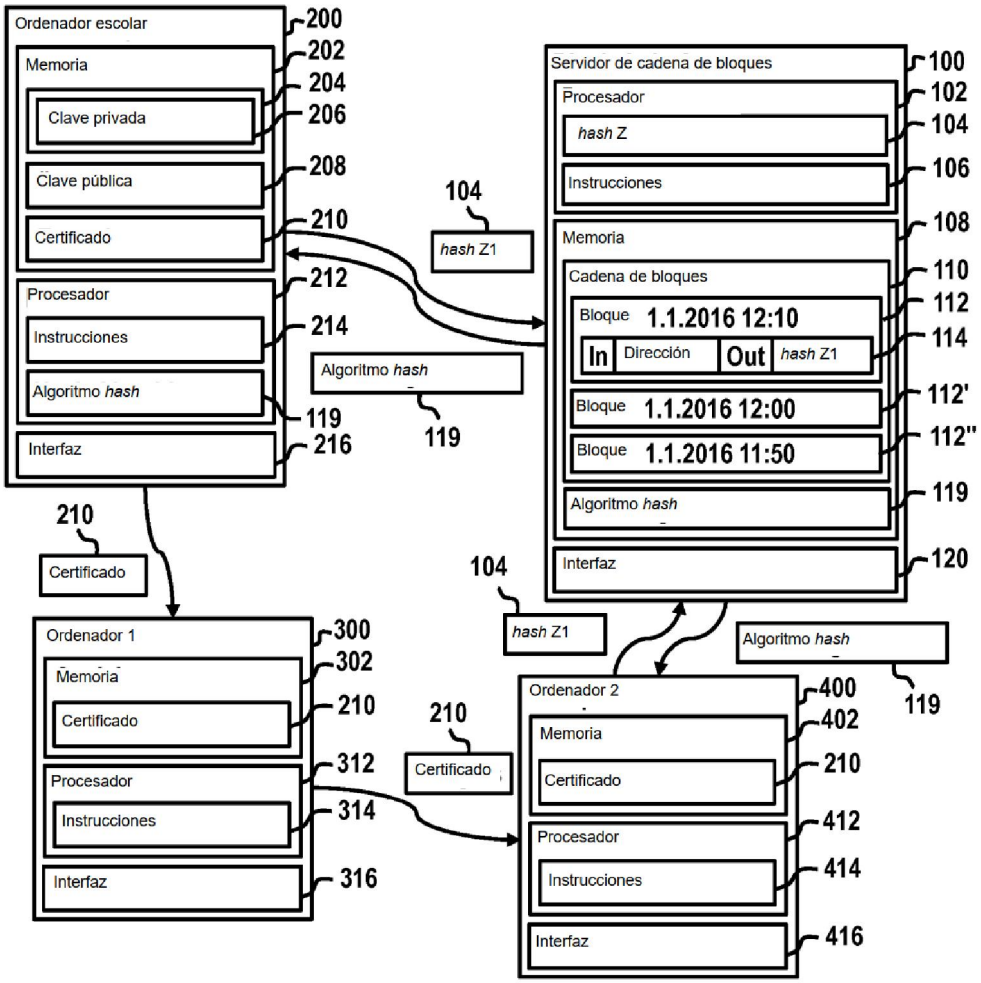
Ordenador escolar
200
Memoria
202
Clave privada
204
206
Clave pública
208
Certificado
210
Procesador
212
Instrucciones
214
Algoritmo hash
119
Interfaz
216
104
hash Z1
Algoritmo hash
119
Servidor de cadena de bloques
100
Procesador
102
hash Z
104
Instrucciones
106
Memoria
108
Cadena de bloques
110
Bloque 1.1.2016 12:10
112
In
Dirección
Out
hash Z1
114
Bloque 1.1.2016 12:00
112'
Bloque 1.1.2016 11:50
112"
Algoritmo hash
119
Interfaz
120
210
Certificado
104
hash Z1
Algoritmo hash
119
Ordenador 1
300
Memoria
302
Certificado
210
Procesador
312
Instrucciones
314
Interfaz
316
210
Certificado
Ordenador 2
400
Memoria
402
Certificado
210
Procesador
412
Instrucciones
414
Interfaz
416

Fig. 2

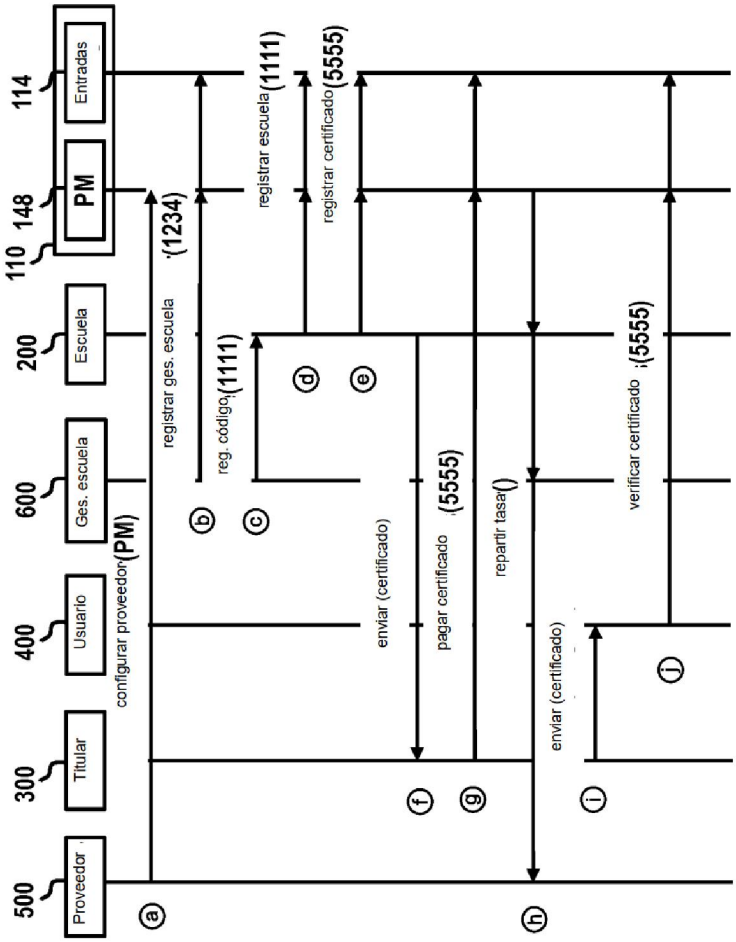
114
Entradas
148
PM
110
200
Escuela
600
Ges. escuela
400
Usuario
300
Titular
500
Proveedor
configurar proveedor(PM)
registrar ges. escuela (1234)
reg. código(1111)
registrar escuela(1111)
registrar certificado(5555)
enviar (certificado)
pagar certificado (5555)
repartir tasa()
enviar (certificado)
verificar certificado (5555)
a
b
c
d
e
f
g
h
i
j

Fig. 3

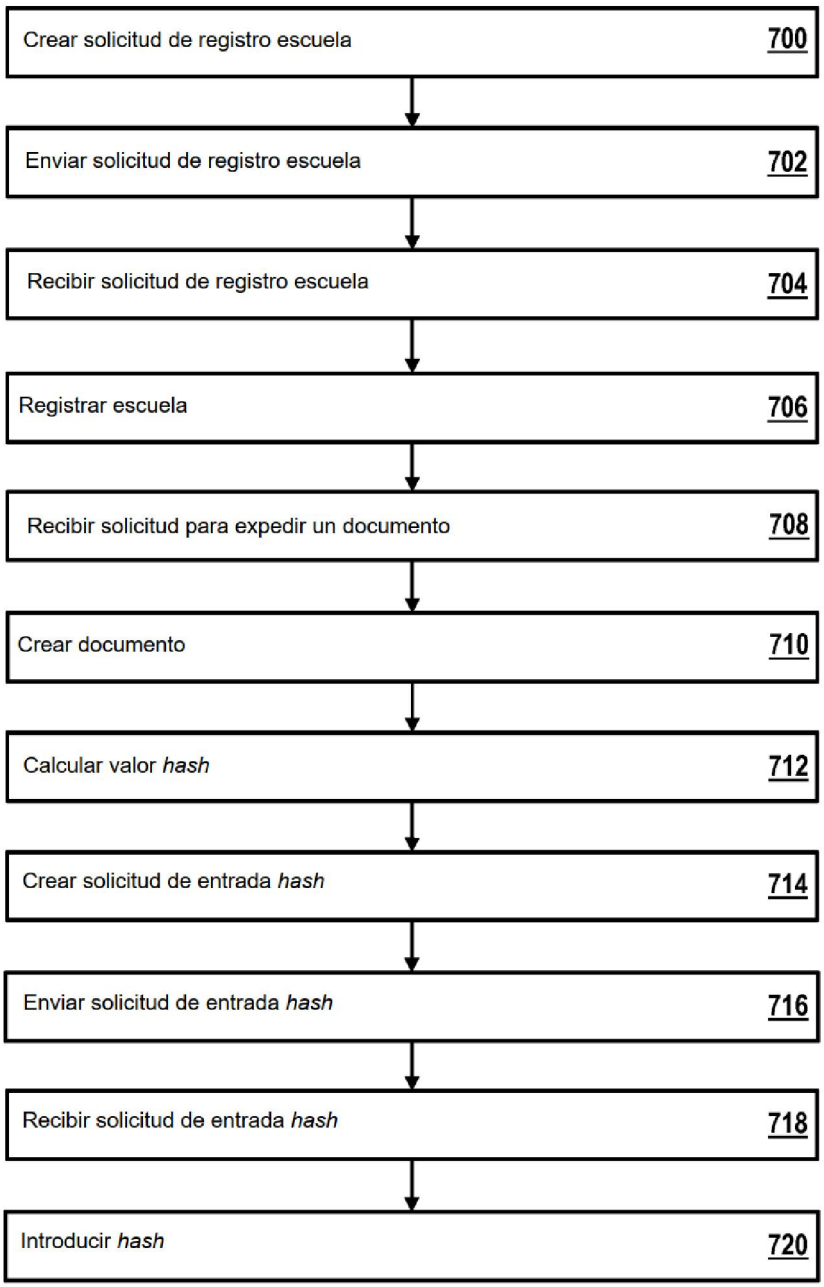
Crear solicitud de registro escuela 700
Enviar solicitud de registro escuela 702
Recibir solicitud de registro escuela 704
Registrar escuela 706
Recibir solicitud para expedir un documento 708
Crear documento 710
Calcular valor *hash* 712
Crear solicitud de entrada *hash* 714
Enviar solicitud de entrada *hash* 716
Recibir solicitud de entrada *hash* 718
Introducir *hash* 720

Fig. 4

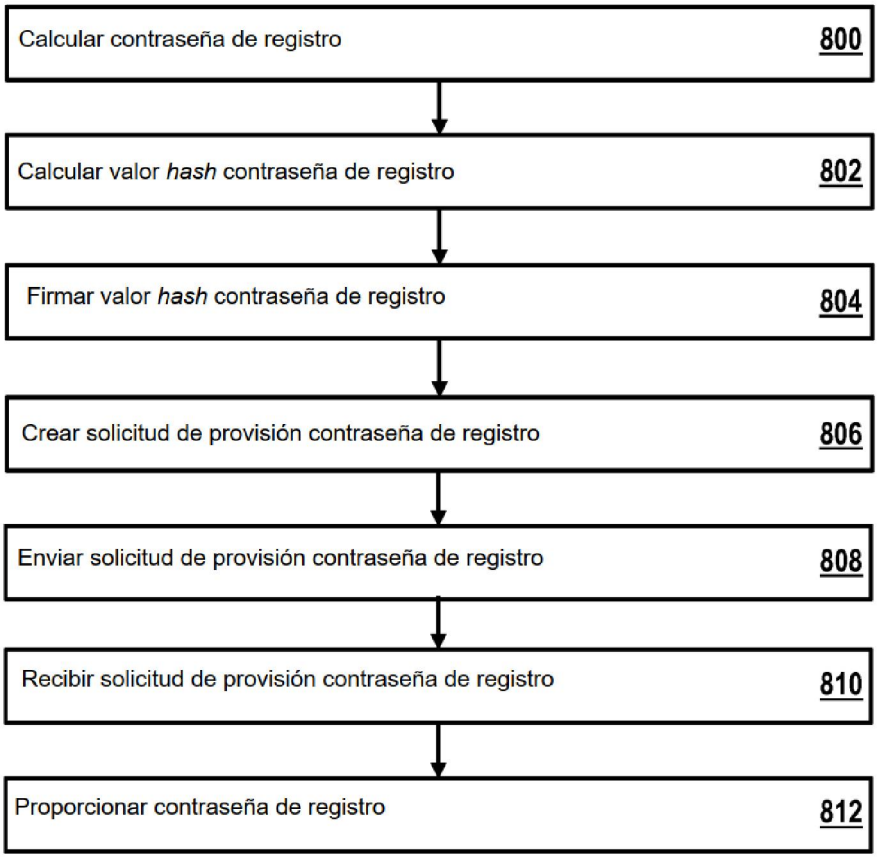
Calcular contraseña de registro
800
Calcular valor *hash* contraseña de registro
802
Firmar valor *hash* contraseña de registro
804
Crear solicitud de provisión contraseña de registro
806
Enviar solicitud de provisión contraseña de registro
808
Recibir solicitud de provisión contraseña de registro
810
Proporcionar contraseña de registro
812

Fig. 5

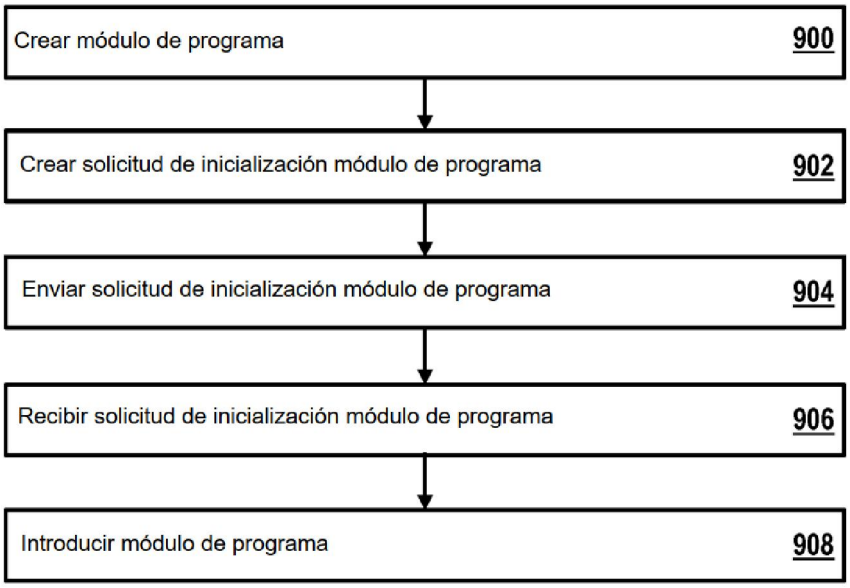
Crear módulo de programa
900
Crear solicitud de inicialización módulo de programa
902
Enviar solicitud de inicialización módulo de programa
904
Recibir solicitud de inicialización módulo de programa
906
Introducir módulo de programa
908

Fig. 6

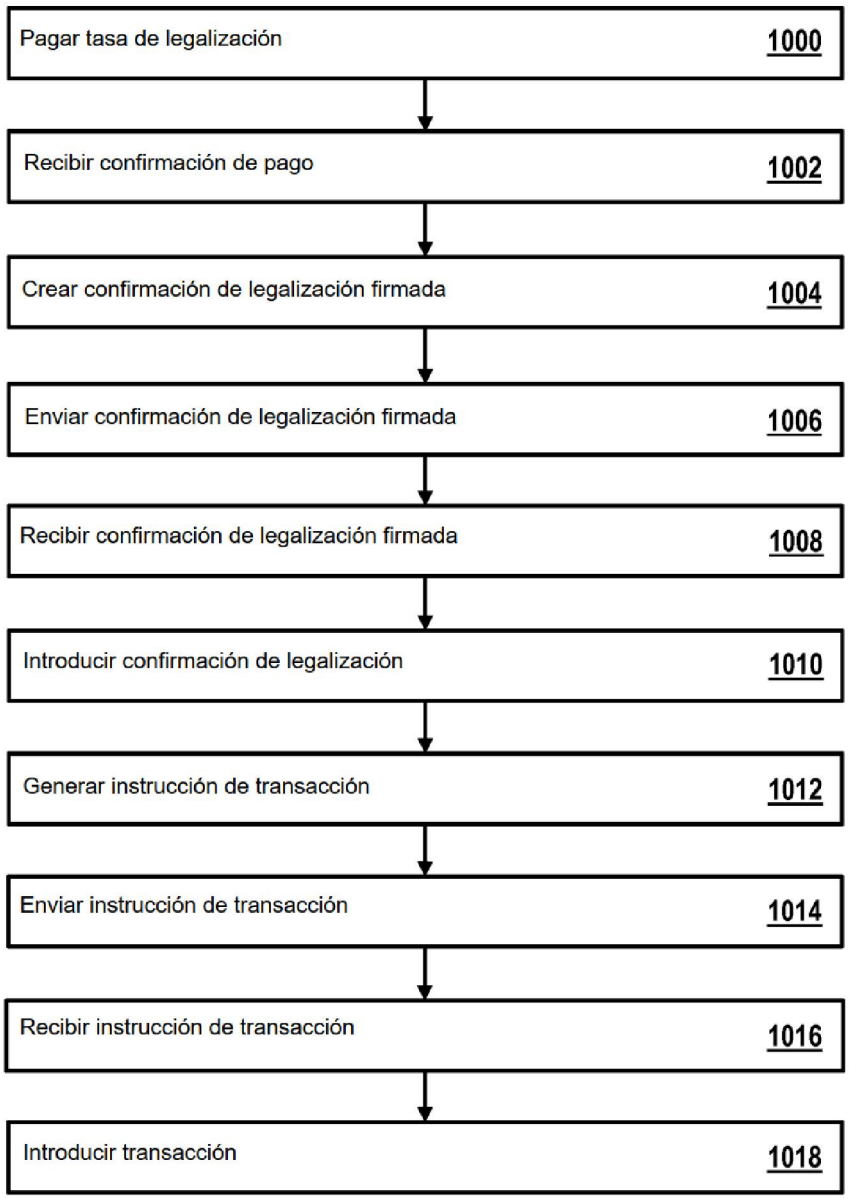
Pagar tasa de legalización
1000
Recibir confirmación de pago
1002
Crear confirmación de legalización firmada
1004
Enviar confirmación de legalización firmada
1006
Recibir confirmación de legalización firmada
1008
Introducir confirmación de legalización
1010
Generar instrucción de transacción
1012
Enviar instrucción de transacción
1014
Recibir instrucción de transacción
1016
Introducir transacción
1018

Fig. 7

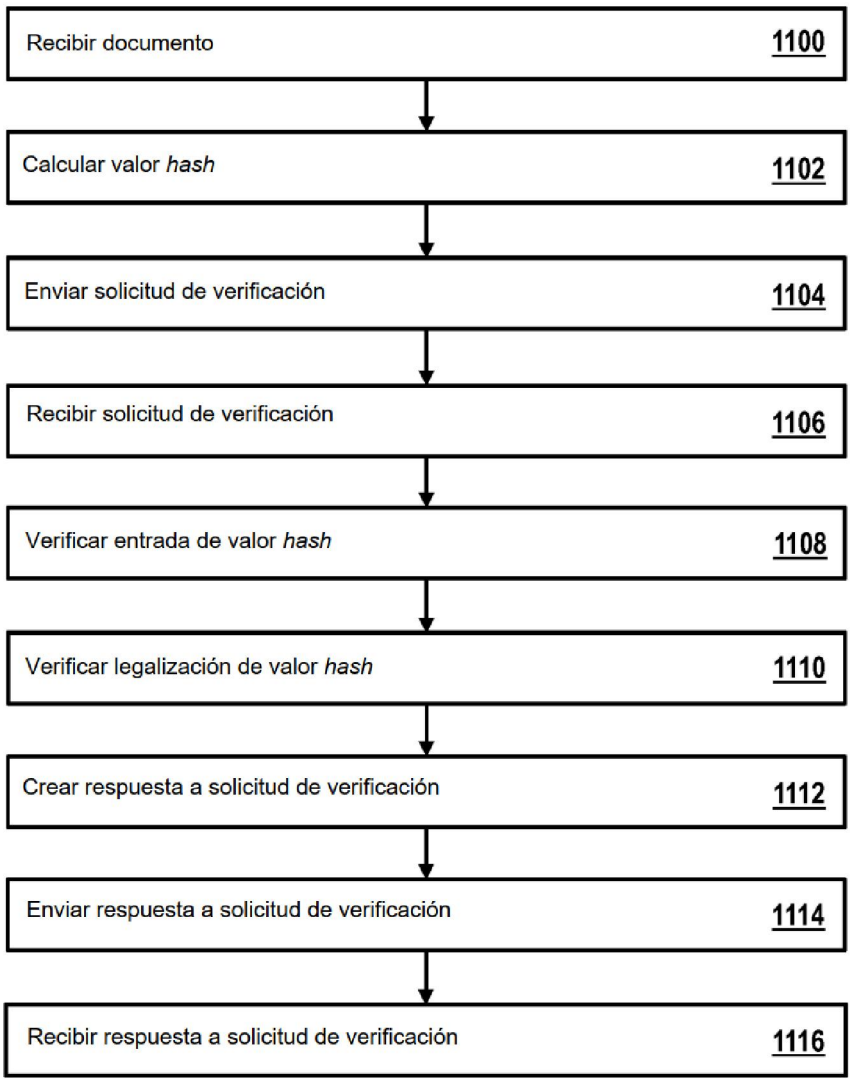
Recibir documento
1100
Calcular valor *hash*
1102
Enviar solicitud de verificación
1104
Recibir solicitud de verificación
1106
Verificar entrada de valor *hash*
1108
Verificar legalización de valor *hash*
1110
Crear respuesta a solicitud de verificación
1112
Enviar respuesta a solicitud de verificación
1114
Recibir respuesta a solicitud de verificación
1116

Fig. 8