(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 942 758**

(51) Int. CI.:

H04L 9/40 (2012.01)
H04L 9/00 (2012.01)
G06Q 50/18 (2012.01)
G06Q 50/20 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.10.2019 E 19382933 (0)**

(97) Fecha y número de publicación de la concesión europea: **04.01.2023 EP 3817320**

(54) Título: **Sistema basado en cadenas de bloques para emitir y validar certificados**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.06.2023

(73) Titular/es:

UNIVERSIDAD INTERNACIONAL DE LA RIOJA (UNIR) (100.0%)
Avenida de la Paz, 137
26006 Logroño (La Rioja), ES

(72) Inventor/es:

PANIAGUA DÍEZ, FIDEL;
NOMBELA PÉREZ, JUAN JOSÉ;
GONZÁLEZ CRESPO, RUBÉN y
BURGOS SOLANS, DANIEL

(74) Agente/Representante:

ESCUDERO PRIETO, Nicolás

DESCRIPCIÓN

Sistema basado en cadenas de bloques para emitir y validar certificados

Campo de la invención

La presente invención se refiere en general a las tecnologías de la información (TI) y, más particularmente, a un sistema basado en cadenas de bloques para la emisión y validación de certificados, y preferiblemente certificados académicos. El sistema garantiza tanto la inmutabilidad como la validez de los certificados emitidos, independientemente de que exista o no una autoridad certificadora (por ejemplo, una institución académica), así como la confidencialidad de los datos y el control de acceso a los certificados por parte del usuario (por ejemplo, un estudiante).

Antecedentes de la invención

La falsificación de certificados académicos es un problema internacional y se han aplicado diversas soluciones técnicas para mitigarlo. En los últimos años, la base de estas soluciones de la técnica anterior se centra principalmente en añadir un código de barras, un código de respuesta rápida (QR), un localizador uniforme de recursos (URL), etc. al certificado académico, de forma que se pueda comprobar su validez con un dispositivo y/o servicio de validación remota. Todas estas soluciones dependen de un proveedor de servicios que realiza el servicio de validación, lo que genera problemas de confianza debido a la necesidad de un tercero para validar los certificados.

Una cadena de bloques puede definirse como una serie de registros de datos inmutables que se distribuyen en una red de pares (P2P) formada por nodos sin autoridades centrales. Cada nodo de la red tiene acceso a la información registrada en la cadena de bloques y la inmutabilidad de los datos almacenados se garantiza mediante criptografía. Más recientemente, la evolución de la tecnología de las cadenas de bloques ha permitido compartir no solo datos sino también programas, lo que se conoce como contratos inteligentes. Los contratos inteligentes pueden almacenarse en la cadena de bloques y ejecutarse por cualquiera de los nodos pertenecientes a la misma, garantizando que sus ejecuciones (comúnmente conocidas como “transacciones”) no puedan ser modificadas y evitando ataques de denegación de servicio (DoS). La verificación de transacciones en una cadena de bloques se logra a través de operaciones de consenso llevadas a cabo por los usuarios o los nodos en la red.

Las redes de cadenas de bloques se pueden clasificar generalmente en las siguientes categorías, según su política de acceso/permiso:

- Redes públicas sin permiso: las entidades que forman parte de la red (usuarios y nodos) no necesitan solicitar permiso para interactuar con la cadena de bloques. Además, cada entidad en la red puede ejecutar y verificar transacciones, que son públicas.

- Redes con permiso público: cada entidad debe estar identificada antes de que pueda participar en la red y solo los nodos de validación pueden verificar las transacciones, que son públicas.

- Redes privadas: las entidades tienen identidades conocidas y solo unos pocos nodos pueden verificar transacciones, que son privadas.

Las características y ventajas específicas de las tecnologías de cadena de bloques ya se han adoptado como una solución contra la falsificación de certificados académicos en la técnica anterior. En la actualidad existen varias plataformas y servicios conocidos para la emisión y validación de certificados académicos en base a esta tecnología. A continuación se enumeran algunos ejemplos relevantes:

- Los sistemas del École Supérieure d'Ingénieurs Leonard de Vinci, Holberton School, CESYT y MIT Media Lab utilizan la tecnología de cadena de bloques de Bitcoin y funciones de comprobación criptográfica (CHF, del inglés “cryptographic hash functions”) para mapear datos de tamaño arbitrario en una cadena de bits de un tamaño fijo (el “valor de comprobación” o “comprobación”, o “resumen de mensajes”) asociados a los certificados académicos. En estos sistemas, una operación de validación verifica si la comprobación de la copia digital del certificado académico es igual a la comprobación almacenada en Bitcoin.

- El sistema de la Red Griega de Investigación y Tecnología (GRNET) sigue la misma idea que las soluciones anteriores, almacenando la comprobación del certificado académico en cadenas de bloques, pero utilizando Cardano (una red de cadenas de bloques diferente) en lugar de Bitcoin. Además, este sistema también registra toda la cadena de etapas de verificación en la cadena de bloques, lo que permite rastrear evidencias de un título y el estado de concesión pasado o actual del mismo.

- Blockcerts es un estándar abierto para administrar certificados en una cadena de bloques. Originalmente se basó en la tecnología Bitcoin “Mit Media Lab”, pero hoy en día también es compatible con las redes Ethereum.

• Smartdegrees utiliza Quorum, basado en Ethereum, para crear cadenas de bloques privadas y para registrar en las mismas los certificados digitales.

Aunque hay muchos otros ejemplos de soluciones de cadenas de bloques para verificar certificados académicos, todos comparten que los datos (por ejemplo, los valores de comprobación) asociados a los certificados se almacenan en una red privada. Por tanto, la información generada no puede gestionarse dentro de una red de cadenas de bloques pública (sin permiso o con permiso), por razones de confidencialidad o de seguridad. Esta es una limitación no deseada en las operaciones de validación del mundo real, donde el acceso público y privado y la gestión de datos necesariamente deben coexistir. Por ejemplo, en el contexto de las instituciones académicas, naturalmente tanto los estudiantes como las propias instituciones están sujetos a solicitudes y envíos de información tanto públicos como privados.

Incluso si se intentara implementar una cadena de bloques con permiso público (por ejemplo, en una cadena de bloques de Quorum) para validar certificados, con el fin de garantizar la privacidad y cumplir con los requisitos legales de confidencialidad y protección de datos, también surgen las siguientes limitaciones:

- Los datos de los certificados solo se pondrán a disposición de su titular o de la institución académica que los ha emitido. Compartir certificados, por ejemplo con empresas, solo puede realizarse utilizando servicios externos, como un servidor web, pero nunca dentro de la propia red de cadenas de bloques.

- No es posible utilizar los datos de los certificados en otros procesos implementados dentro de la red de cadenas de bloques, como por ejemplo, un sistema de registro universitario.

- No brinda la opción de crear relaciones de confianza entre instituciones académicas para compartir las cuentas de los estudiantes, por lo que requiere que los estudiantes tengan una cuenta para cada institución académica registrada en la cadena de bloques.

Un sistema basado en cadenas de bloques conocido para emitir certificados se describe en la solicitud de patente US 2018/082256 A1. Sin embargo, este sistema requiere almacenar la información asociada a los certificados (contratos inteligentes) en una base de datos asociada a la billetera digital de cada usuario. Esta propuesta consume muchos recursos, ya que los certificados deben copiarse de manera proporcional al número de usuarios, por lo que carece de escalabilidad. El sistema también implica un alto riesgo de datos que también es proporcional al número de usuarios, por ejemplo cuando terceros necesitan acceder a sus certificados para su verificación.

Dadas las limitaciones anteriores en las técnicas conocidas, existe la necesidad de una cadena de bloques con permiso público que pueda validar de manera eficaz los certificados, al tiempo que garantice la confidencialidad, la protección de datos y la facilidad de uso incluso cuando varias entidades de certificación participan en el sistema. La presente invención propone una solución a dicha necesidad, a través de un novedoso sistema basado en cadenas de bloques para la emisión y validación de certificados, que resulta especialmente ventajoso para la validación de certificados académicos.

Breve descripción de la invención

Un primer objeto de la presente invención se refiere, sin carácter limitativo, al desarrollo de un sistema para la emisión y validación de certificados, que comprende:

- una red de cadenas de bloques con permiso público, configurada con:

◦ una pluralidad de nodos conectados a través de una red de comunicación;

◦ un repositorio de servicios de certificados que comprende los datos de los certificados y la lógica de emisión/revocación de los mismos; y

◦ lógica de control de acceso que comprende uno o más contratos inteligentes para gestionar el control de acceso a la información privada almacenada en el repositorio de servicios de certificados.

Ventajosamente, el sistema comprende además:

- una red de institución certificadora, que comprende uno o más medios informáticos conectados a una red de comunicación y configurados con una pluralidad de procesos y operaciones informáticas, donde la red de institución certificadora comprende además:

◦ un nodo de cadena de bloques con permiso público de la red de cadena de bloques con permiso, administrado por una institución certificadora;

◦ una plataforma de distribución de contenido/almacenamiento distribuido de pares;

donde dicho nodo de cadena de bloques está configurado para permitir tanto la interacción con la red de cadena de bloques a través de la ejecución de contratos inteligentes como el almacenamiento de copias de los certificados en la plataforma de distribución de contenido/almacenamiento distribuido;

◦ uno o más medios informáticos configurados con un servicio de gestión de certificados adaptado para la emisión y revocación de certificados por parte de la institución certificadora, en el que el servicio de gestión de certificados está conectado a través de una red de comunicación con la red de cadena de bloques con permiso público, a través del nodo de cadena de bloques con permiso público y la plataforma de distribución de contenido/almacenamiento distribuido;

◦ uno o más medios informáticos configurados con una pluralidad de servicios fuera de cadena utilizados por la institución certificadora para gestionar el acceso a los certificados por parte de usuarios no conectados a la red de cadena de bloques con permiso público, donde los servicios fuera de cadena también están conectados con la red de cadena de bloques con permiso público, a través del nodo de cadena de bloques con permiso público y la plataforma de distribución de contenido/almacenamiento distribuido;

- una red externa que comprende una pluralidad de dispositivos informáticos utilizados por usuarios u otros proveedores de servicios a terceros no conectados al entorno de cadena de bloques, configurados para interactuar con los certificados almacenados en la plataforma de distribución de contenido/almacenamiento a través de los servicios fuera de cadena.

En una realización preferida de la invención, al menos parte de la información comprendida en el repositorio está encriptada.

En una realización preferida adicional de la invención, la lógica de control de acceso se configura a través de una jerarquía de información de usuarios, información de grupos e información de recursos, donde la información de recursos está encriptada en el repositorio de servicio de certificados.

En todavía otra realización preferida adicional de la invención, la información de recursos se encripta a través de una clave de encriptado con un secreto compartido obtenido como resultado de un protocolo Elliptic-Curve Diffie Hellman (ECDH). Más preferiblemente, las curvas elípticas del protocolo comprenden la curva Secp256k1.

En una realización preferida adicional de la invención, los dispositivos informáticos de la red externa comprenden al menos un dispositivo móvil conectado al servicio fuera de cadena a través de una red de comunicación.

En una realización preferida adicional de la invención, los servicios fuera de cadena están configurados para realizar una o más de las siguientes operaciones, a través de uno o más dispositivos informáticos:

- emitir certificados: la institución certificadora puede emitir certificados académicos y registrar en la red de cadena de bloques, por medio del nodo de cadena de bloques con permiso público y la plataforma de distribución de contenido/almacenamiento distribuido (preferiblemente, el resultado de la operación de emisión está adaptado para generar una URL única del certificado académico);

- establecer permisos: los usuarios o la institución certificadora pueden gestionar los permisos de los certificados;

- listar certificados: la institución certificadora puede listar certificados emitidos;

- revocar certificados: la institución certificadora puede revocar certificados;

- visualizar certificados: la institución certificadora, los usuarios u otros proveedores de servicios a terceros pueden visualizar un certificado académico.

Descripción de los dibujos

Las características y las ventajas de esta invención resultarán más evidentes a partir de la siguiente descripción detallada, cuando se lea junto con los dibujos adjuntos, en los que:

La figura 1 representa la arquitectura de un sistema según una realización preferida de la invención, en donde se muestran sus elementos esenciales, a saber, sus entornos, servidores y servicios.

La figura 2 representa los participantes que pueden interactuar con el sistema de la invención y sus operaciones principales, para una realización preferida del mismo.

Referencias numéricas utilizadas en los dibujos

Para facilitar una mejor comprensión de las características técnicas de la invención, las Figuras 1-2 a las que se hace referencia van acompañadas de una serie de referencias numéricas que, con carácter ilustrativo y no limitativo, se representan a continuación:

(1)	Red de cadena de bloques con permiso público
(2)	Repositorio de servicios de certificados
(3)	Lógica de control de acceso
(4)	Red de institución certificadora
(5)	Institución certificadora
(6)	Nodo de cadena de bloques
(6')	Plataforma de distribución de contenido/almacenamiento distribuido
(7)	Gestión de certificados
(8)	Fuera de cadena
(9)	Entorno de red externo
(10)	Usuario
(11)	Otra entidad
(12)	Emitir certificado
(13)	Establecer permisos
(14)	Listar certificados
(15)	Revocar certificado
(16)	Visualizar certificado

Descripción detallada de la invención

En la siguiente descripción, con fines explicativos y no limitativos, se exponen detalles para proporcionar una comprensión exhaustiva de la presente invención. Sin embargo, resultará evidente para los expertos en la técnica que la presente invención puede llevarse a la práctica en otras realizaciones que se alejen de estos detalles y descripciones sin alejarse del alcance de la invención. A continuación, se describirán determinadas realizaciones con referencia a los dibujos (Figuras 1-2) en las que las características ilustrativas se indican mediante números de referencia.

A continuación se muestra una descripción detallada de la invención, cuya arquitectura se muestra en la Figura 1. El propósito y la utilidad de los diferentes ambientes representados en la figura son:

- Red de cadena de bloques con permiso público (1): comprende una pluralidad de nodos (es decir, procesos informáticos configurados en uno o más medios informáticos, donde los nodos están conectados a una red de comunicación), donde cada nodo almacena al menos una parte de una cadena de bloques (es decir, datos distribuidos a lo largo de los nodos) y uno o más procesos o contratos inteligentes, configurados con operaciones sobre dicha cadena de bloques. Preferiblemente, la cadena de bloques comprende además:

◦ Repositorio de servicios de certificados (2): contiene la información de los certificados y su lógica de emisión/revocación. Más preferiblemente, al menos parte de la información comprendida en el repositorio (2) está encriptada para preservar su confidencialidad.

◦ Lógica de control de acceso (3): comprende uno o más contratos inteligentes para gestionar el control de acceso a la información privada almacenada en el repositorio de servicios de certificados (2). La lógica de control de acceso (3) se configura preferiblemente a través de una jerarquía de usuarios, grupos y recursos (de manera similar al control de acceso en los sistemas operativos Linux). Los recursos se refieren preferiblemente a la información encriptada en el repositorio de servicios de certificados (2) y se pueden asignar permisos a los usuarios, grupos u otros (análogo a titular, grupo y otros en un sistema de archivos de Linux). Los contratos inteligentes de la lógica de control de acceso (3) brindan funciones para la creación, mantenimiento y eliminación de usuarios, grupos y recursos (por ejemplo, "useradd", "adduser", "groupadd", "ls", "touch", "cat", u otras funciones similares utilizadas en los sistemas Linux), incluida la definición de permisos ("chown", "chgrp", "chmod", etc.). Preferiblemente, las características de estos tres elementos se pueden resumir en:

- Usuario: se representa en el sistema mediante un identificador y una clave pública. Los usuarios tienen un grupo predeterminado y hay un usuario raíz que puede crear usuarios y grupos y establecer permisos globalmente.

- Grupo: se representa en el sistema por una clave pública, una clave privada encriptada con una clave de grupo, y un identificador de la cuenta del grupo. Los usuarios con permisos en el grupo pueden usar la clave de grupo e

interactuar en el sistema con la identidad de grupo.

- Recurso: se define con permisos de titular, grupo y otros. Además, las claves de encriptado solo están disponibles para aquellos usuarios y grupos que tienen permisos para el recurso. Los recursos también permiten definir listas de control de acceso para conceder permisos adicionales a usuarios y grupos.

Preferiblemente, el sistema encripta las claves de encriptado de recursos y grupos con un secreto compartido obtenido como resultado de un protocolo Elliptic-Curve Diffie Hellman (ECDH) entre los usuarios o grupos con permisos y los usuarios raíz. Garantiza que cada recurso y grupo en el sistema pueda administrarse por el usuario raíz. Más preferiblemente, las curvas elípticas utilizadas comprenden la curva Secp256k1.

• Red de institución certificadora (4): comprende una pluralidad de operaciones y procesos informáticos configurados en uno o más medios informáticos, conectados a una red de comunicación. Preferiblemente, la red de institución certificadora (4) representa una institución certificadora, tal como una institución académica y además comprende:

◦ Un nodo de cadenas de bloques con permiso público (6) y una plataforma de distribución de contenido/almacenamiento distribuido (6'): la red de institución certificadora (4) comprende un nodo habitual (6) de la cadena de bloques, controlado por la institución certificadora (5). Este nodo (6) permite tanto la interacción con la cadena de bloques (a través de la ejecución de contratos inteligentes) como el almacenamiento de copias (preferiblemente encriptadas) de los certificados en una plataforma de distribución de contenido/almacenamiento distribuido (6'), como Swarm. Swarm es una infraestructura de almacenamiento y comunicación descentralizada y sin permisos, basada en la contabilidad de pares de los recursos, que permite a los nodos en una cadena de bloques intercambiar "recurso por recurso", pero que ofrece una compensación a los nodos que consumen menos de lo que sirven.

◦ Servicio de gestión de certificados (7): comprende uno o más medios informáticos configurados con una pluralidad de servicios utilizados por la institución certificadora (5) para la emisión y revocación de los certificados. Este servicio (7) está conectado a través de una red de comunicación con la red de cadena de bloques con permiso público (1), a través del nodo de cadena de bloques con permiso público (6) y la plataforma de distribución de contenido/almacenamiento distribuido (6').

◦ Fuera de cadena (8): comprende uno o más medios informáticos configurados con una pluralidad de servicios utilizados por la institución certificadora (5) para gestionar el acceso a los certificados por parte de usuarios no conectados a la red de cadena de bloques con permiso público (1). Los servicios fuera de cadena (8) también están conectados con la red de cadena de bloques con permiso público (1), a través del nodo de cadena de bloques con permiso público (6) y la plataforma de distribución de contenido/almacenamiento distribuido (6'). Por medio del servicio fuera de cadena (8), cualquier usuario que no esté conectado al entorno de cadena de bloques (1) podrá acceder al mismo utilizando este servicio (por ejemplo, implementándolo como un servicio web en el que el usuario puede acceder al certificado introduciendo una URL del mismo). Esto permite la posibilidad de compartir certificados con otros usuarios o entidades a terceros, concediendo o revocando una opción de compartir por parte del titular del certificado en cualquier momento.

• Entorno de red externa (9): representa la pluralidad de dispositivos informáticos utilizados por los usuarios (10) (por ejemplo, estudiantes) y otras entidades (11) no conectados al entorno de cadena de bloques (1), para interactuar con los certificados almacenados en la plataforma de distribución de contenido/almacenamiento distribuido (6') a través del servicio fuera de cadena (8). Los dispositivos informáticos utilizados por los usuarios (10) y otras entidades pueden comprender cualquier ordenador o dispositivo móvil conectado al servicio fuera de cadena (8) a través de una red de comunicación. En una realización preferida de la invención, las operaciones que pueden realizar estas entidades (10, 11) son una o más de las siguientes:

◦ Usuarios (10) (por ejemplo, estudiantes):

- Pueden visualizar y compartir sus propios certificados mediante un servicio web, por ejemplo, por medio de una URL impredecible. La URL contiene un ID único e impredecible resultante de aplicar la función de comprobación KECCAK-256 al resultado de firmar los parámetros del certificado con una función de algoritmo de firma digital de curva elíptica (ECDSA).

- Pueden conceder o revocar el acceso al certificado académico mediante el uso de una URL.

- Pueden estar conectados a la red de cadena de bloques (1) a través de una cuenta generada por una institución certificadora (5) a la que están conectados, por medio del nodo de cadena de bloques con permiso público (6) y la plataforma de distribución de contenido/almacenamiento distribuido (6'). De esta forma, la información asociada a los certificados puede sincronizarse con un navegador web y almacenarse en un espacio de almacenamiento temporal del mismo. La conexión entre los usuarios (10) y la red de cadena de bloques (1) puede establecerse por uno o más servicios web, a través de un navegador web.

◦ Otras entidades (11) (por ejemplo, proveedores de servicios a terceros, como gerentes de recursos humanos):

- Pueden visualizar los certificados con una URL única, si los usuarios conceden el permiso (10). El acceso se establece preferiblemente a través del servicio fuera de cadena (8).

En una realización preferida de la invención aplicada a los certificados académicos (representados en la Figura 2), las funcionalidades que pueden ejecutar las entidades existentes (5, 10, 11) (instituciones académicas, estudiantes y otras entidades, respectivamente) que participan en el sistema son una o más de las siguientes:

• Emitir certificado (12): la institución académica (5) puede emitir certificados académicos y estos se registrarán en la red de cadena de bloques (1), por medio del nodo de cadena de bloques con permiso público (6) y la plataforma de distribución de contenido/almacenamiento distribuido (6'). El resultado de la operación de emisión (12) preferiblemente genera también una URL única del certificado académico y una notificación al estudiante (5) con un enlace y una contraseña para descargar una cuenta creada por la institución académica (10) al que puede accederse a través de un navegador web.

• Establecer permisos (13): los estudiantes (10) o la institución académica (5) pueden gestionar los permisos de los certificados. Por ejemplo, pueden activar o desactivar la URL para visualizarla.

• Listar certificados (14): la institución académica (5) puede listar todos los certificados emitidos. La información que se muestra puede ordenarse usando múltiples criterios y buscarse usando los campos de información de los certificados académicos.

• Revocar certificado (15): la institución académica (5) puede revocar un certificado académico.

• Visualizar certificado (16): cualquier entidad (5, 10, 11) puede visualizar un certificado académico si tiene la URL de este certificado académico y está activada.

REIVINDICACIONES

1. Sistema para la emisión y validación de certificados, que comprende:

- una red de cadena de bloques con permiso público (1), configurada con:

◦ una pluralidad de nodos conectados a través de una red de comunicación;

◦ un repositorio de servicios de certificados (2) que comprende los datos de los certificados y la lógica de emisión/revocación de los mismos;

◦ lógica de control de acceso (3) que comprende uno o más contratos inteligentes para gestionar el control de acceso a la información privada almacenada en el repositorio de servicios de certificados (2);

en el que el sistema comprende además:

- una red de institución certificadora (4), que comprende uno o más medios informáticos conectados a una red de comunicación y configurados con una pluralidad de procesos y operaciones informáticas, donde la red de institución certificadora (4) comprende además:

◦ un nodo de cadena de bloques con permiso público (6) de la red de cadena de bloques con permiso (1) gestionado por una institución certificadora (5);

◦ una plataforma de distribución de contenido/almacenamiento distribuido de pares (6');

donde dicho nodo de cadena de bloques (6) está configurado para permitir tanto la interacción de la red de institución certificadora con la red de cadena de bloques (1) a través de la ejecución de contratos inteligentes como el almacenamiento de copias de los certificados en la plataforma de distribución de contenido/almacenamiento distribuido de pares (6');

◦ uno o más medios informáticos configurados con un servicio de gestión de certificados (7) adaptado para la emisión y revocación de certificados por parte de la institución certificadora (5), en el que el servicio de gestión de certificados (7) está conectado a través de una red de comunicación con la red de cadena de bloques con permiso público (1), a través del nodo de cadena de bloques con permiso público (6) y la plataforma de distribución de contenido/almacenamiento distribuido de pares (6');

◦ uno o más medios informáticos configurados con una pluralidad de servicios fuera de cadena (8) utilizados por la institución certificadora (5) para gestionar el acceso a los certificados por parte de usuarios no conectados a la red de cadena de bloques con permiso público (1), donde los servicios fuera de cadena (8) también están conectados con la red de cadena de bloques con permiso público (1), a través del nodo de cadena de bloques con permiso público (6) y la plataforma de distribución de contenido/almacenamiento distribuido de pares (6');

- una red externa (9) que comprende una pluralidad de dispositivos informáticos utilizados por usuarios (10) u otros proveedores de servicios a terceros (11) no conectados directamente al entorno de cadena de bloques (1), configurados para interactuar con los certificados almacenados en la plataforma de distribución de contenido/almacenamiento distribuido de pares (6') a través de los servicios fuera de cadena (8).

2. Sistema según la reivindicación anterior, en el que al menos parte de la información comprendida en el repositorio (2) está encriptada.

3. Sistema según cualquiera de las reivindicaciones anteriores, en el que la lógica de control de acceso (3) está configurada a través de una jerarquía de información de usuarios, información de grupos e información de recursos, donde la información de recursos está encriptada en el repositorio de servicios de certificados (2).

4. Sistema según la reivindicación anterior, en el que la información de recursos está encriptada a través de una clave de encriptado con un secreto compartido obtenido como resultado de un protocolo Elliptic-Curve Diffie Hellman (ECDH).

5. Sistema según la reivindicación anterior, en el que las curvas elípticas del protocolo comprenden la curva Secp256k1.

6. Sistema según cualquiera de las reivindicaciones anteriores, en el que los dispositivos informáticos de la red externa (9) comprenden un dispositivo móvil conectado al servicio fuera de cadena (8) a través de una red de comunicación.

7. Sistema según cualquiera de las reivindicaciones anteriores, en el que los servicios fuera de cadena (8) están configurados para realizar una o más de las siguientes operaciones a través de uno o más dispositivos informáticos:

- emitir certificados (12): la institución certificadora (5) puede emitir certificados académicos y registrar en la red de cadena de bloques (1), por medio del nodo de cadena de bloques con permiso público (6) y la plataforma de distribución de contenido/almacenamiento distribuido (6');

- establecer permisos (13): los usuarios (10) o la institución certificadora (5) pueden gestionar los permisos de los certificados;

- listar certificados (14): la institución certificadora (5) puede listar certificados emitidos;

- revocar certificados (15): la institución certificadora (5) puede revocar certificados;

- visualizar certificados (16): la institución certificadora (5), los usuarios (10) u otros proveedores de servicios a terceros (11) pueden visualizar un certificado académico.

8. Sistema según la reivindicación anterior, en el que el resultado de la operación de emisión (12) está adaptado para generar una URL única del certificado académico.

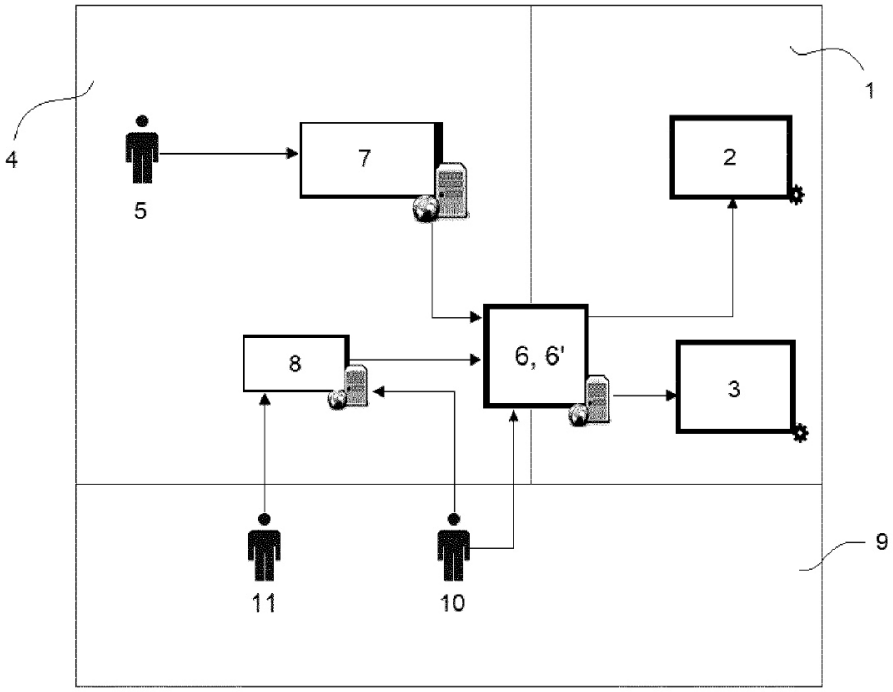

FIG. 1

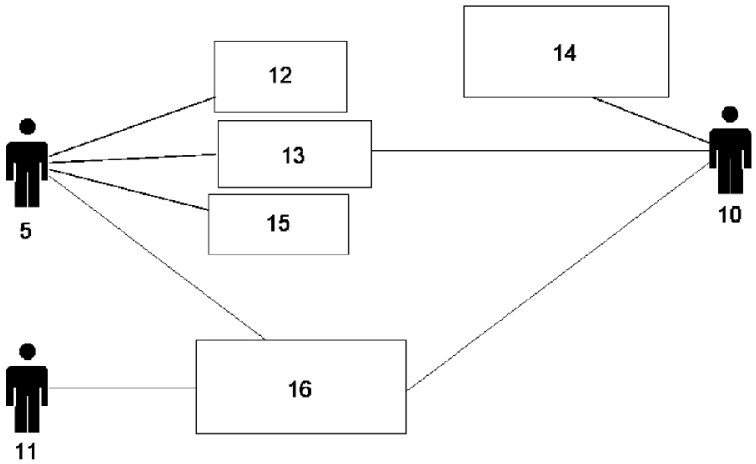

FIG. 2