(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 729 312**

(51) Int. CI.:

G06F 21/60 (2013.01)
G06F 21/31 (2013.01)
G06F 21/62 (2013.01)
H04L 9/06 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.12.2017 E 17210750 (0)**

(97) Fecha y número de publicación de la concesión europea: **06.03.2019 EP 3343425**

(54) Título: **Sistema y procedimiento para la creación y la gestión de autorizaciones descentralizadas para objetos conectados**

(30) Prioridad:

28.12.2016 FR 1663485

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.10.2019

(73) Titular/es:

BULL SAS (100.0%)
Rue Jean Jaurès
78340 Les Clayes sous Bois, FR

(72) Inventor/es:

LEPORINI, DAVID y
PIRON, CHARLES

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema y procedimiento para la creación y la gestión de autorizaciones descentralizadas para objetos conectados

La presente invención se refiere al dominio de la identidad única de los objetos conectados y la gestión de sus autorizaciones de acceso. Más particularmente, la presente invención permite la identificación, la autentificación y la prestación de la autorización utilizando un sistema distribuido, descentralizado y auditable. La invención se refiere a un sistema informático de creación y de gestión de autorizaciones de acceso para objetos conectados, así como un procedimiento que pueda llevarse a cabo por dicho sistema.

[Arte anterior]

Existen numerosas soluciones informáticas que permiten la gestión de las autorizaciones y de las identidades de los objetos conectados. En general, estas soluciones están basadas en una plataforma de gestión única y centralizada. La confianza en esta solución está generalmente asegurada por la reputación y las reglas que se impone esta plataforma centralizada. Sin embargo, dicha centralización induce unas problemáticas de seguridad de los datos así como en términos de pérdida de datos como de modificación no autorizada de su integridad.

Existen bases de datos para asegurar el almacenamiento de autorizaciones donde los datos están repartidos entre algunos sitios o entre algunos actores, pero estas bases de datos se basan en el principio de una referencia única replicada en varios lugares. Por ejemplo, las bases de datos distribuidas como las bases NoSQL (por ejemplo, Cassandra) reposan sobre una base de referencia única, llamada “maestro”, que está replicada y por tanto compartida en cada uno de los sitios. Cuando el número de actores es importante, dicho mecanismo basado en la replicación se hace demasiado complejo para llevarlo a cabo y su rendimiento se reduce fuertemente o su coherencia no está garantizada. Así, esto no responde a la necesidad emergente ligada a la volumetría de objetos conectados, y unas necesidades de descentralización, de control y de auditoría de las autorizaciones de accesos que haría que las soluciones clásicas de replicación sean demasiado complejas para llevarlas a cabo. Además, el gobierno de este tipo de arquitectura es único: un actor que permanece como maestro y los otros esclavos. Por ello, el actor principal tiene un papel diferente del de los otros actores. Sin embargo, en determinadas situaciones, no es posible o deseable disponer de una plataforma centralizada, aunque esté replicada. Por ejemplo, en el caso de un proceso de múltiples actores, es decir que implica unas entidades jurídicas distintas (varias empresas, etcétera), no es siempre fácil, jurídicamente o comercialmente, decidir qué actor jugará el papel central de alojador de la plataforma.

La evolución exponencial del número de objetos conectados y de estas plataformas centralizadas conlleva una complejidad de la gestión de las identidades y de las autorizaciones tanto para los usuarios como para las plataformas. Sobre todo, porque los sistemas existentes están generalmente especializados en una categoría de objeto conectado para la que gestiona la identidad y las autorizaciones y porque estos sistemas controlados por un tercero no permiten a los usuarios migrar fácilmente su identidad y/o su prueba de utilización hacia otros sistemas.

La utilización de una cadena de bloques permite dar seguridad a los datos ya que a partir del momento donde han sido difundidos en la comunidad, estos datos no pueden ser reescritos, por tanto, falsificados. Este aspecto comunitario permite prescindir de un tercero de confianza único o de una autoridad de control, la validación sincronizada de los datos sirve de garantía. Así, existen sistemas informáticos de gestión de transacciones basados en cadenas de bloques tales como por ejemplo el sistema descrito en la solicitud de patente WO2016197055 o la solicitud de patente US20160261690. Sin embargo, estos sistemas se basan en una gestión de objetos conectados que se libran de una autoridad de control y hacen reposar la confianza en el sistema sobre un gran número de participantes y un consenso criptográficamente verificable de su contenido.

El documento “MedRec: Using Blockchain for Medical Data Access and Permission Management”,2016 2nd International Conference on Open and Big Data, describe la utilización de la tecnología de cadena de bloques para la gestión de autorizaciones en el dominio de los datos de salud.

Resulta que no existe ninguna solución satisfactoria que permite asegurar la gestión de las autorizaciones de acceso y de las identidades que implican varios actores. Así, existe la necesidad para nuevos sistemas y procedimientos de gestión de las autorizaciones para objetos conectados respondiendo a este problema.

[Problema técnico]

La invención tiene por tanto como objetivo remediar los inconvenientes del arte anterior proponiendo un sistema y un procedimiento de creación y de gestión de autorización para objetos conectados que estén descentralizados, distribuidos y auditables. En particular, la invención tiene como objetivo proponer un sistema, gestionado por un número controlado de entidades de gobierno, que permita gestionar las autorizaciones de acceso de un objeto conectado a un conjunto de servicios muy diversos. Este sistema y este procedimiento presenta numerosas ventajas tales como: fuerte interoperabilidad, fuerte resiliencia, confidencialidad, autonomía, aseguramiento de una integridad de los datos, y trazabilidad.

[Breve descripción de la invención]

A este efecto, la invención se refiere a un sistema informático de creación de autorizaciones, de atribuciones y de gestión de dichas autorizaciones para unos objetos conectados que incluyen:

- una pluralidad de servidores de almacenamiento que incluye una cadena de bloques distribuida con la forma de nudos de almacenamiento, dichos servidores de almacenamiento 20 son aptos para registrar un nuevo bloque 202 en la cadena de bloques 200;

- un módulo de control de acceso que está configurado para definir un derecho de acceso a la cadena de bloques, para un usuario del sistema, dicho derecho de acceso está seleccionado de entre una lista que incluye al menos:

  - un derecho de acceso que incluye únicamente un derecho de lectura, y

  - un derecho de acceso que incluye un derecho de grabación de nuevos bloques de la cadena de bloques sobre el nudo de almacenamiento, el usuario que posee dicho derecho que es llamado entidad de gobierno;

- un módulo de inscripción para la creación de autorización apto para:

  - recibir unos datos de ejecución del contrato inteligente, emitidos por una entidad de gobierno 70, dichos datos de ejecución del contrato inteligente incluyen un identificador único del contratante inteligente, unas condiciones de aplicación del contrato inteligente y al menos una autorización condicional asociada al contrato inteligente, e

  - inscribir dichos datos dados de ejecución del contrato inteligente sobre un nudo de almacenamiento de dicha cadena de bloques; y

-un módulo de conexión para la atribución de autorización apto para:

  - recibir datos de conexión entre un objeto conectado y una tercera entidad, dichos datos de conexión incluyen al menos una solicitud de autorización,

  - identificar sobre un nudo de almacenamiento de la cadena de bloques una autorización condicional complementaria a dicha solicitud de autorización,

  - verificar las condiciones de aplicación comprendidas en los datos de ejecución del contrato inteligente, y

  - generar una instrucción de atribución de autorización que da derecho a la solicitud de autorización únicamente si todas las condiciones de aplicación de dicha autorización condicional han sido verificadas.

Las soluciones anteriores que permiten la gestión de las autorizaciones de objetos conectados están generalmente centralizadas por el hecho de las necesidades de identificación controlada y centralizada para el acceso a determinadas funcionalidades o servicios. La presente invención va en contra de esto proponiendo un sistema en el que la gestión de las identidades está distribuida y descentralizada, permitiendo una gestión evolutiva de las autorizaciones de acceso a servicios ofrecidos por diferentes actores. Para ello, una cadena de bloques, habitualmente utilizada en un marco abierto, es llevada a cabo en un sistema modificable por un número controlado y limitado de usuarios que tienen derechos de grabación de nuevos bloques de la cadena de bloques y también llamados entidades de gobierno. Además, la cadena de bloques puede presentar la ventaja de incluir datos al menos parcialmente cifrados.

La invención se refiere además a un procedimiento de creación y de gestión de autorizaciones para objetos conectados, llevada a cabo por un sistema informático que incluye una cadena de bloques distribuida con la forma de nudos de almacenamiento, dichos servidores de almacenamiento son aptos para grabar un nuevo bloque en la cadena de bloques, un módulo de control de acceso, un módulo de inscripción, y un módulo de conexión, dicho procedimiento incluye las etapas de:

- Definición, mediante el módulo de control de acceso, de un derecho de acceso a la cadena de bloques, para un usuario, dicho derecho de acceso está seleccionado de entre una lista que incluye al menos:

  - un derecho de acceso que incluye únicamente un derecho de lectura y

  - un derecho de acceso que incluye un derecho de grabación de nuevos bloques de la cadena de bloques, el usuario que posee dicho derecho es llamado entidad de gobierno;

- Recepción, mediante el módulo de inscripción, de datos de ejecución del contratante inteligente, emitidos por una entidad de gobierno, dichos datos de ejecución del contrato inteligente incluyen un identificador único, unas condiciones de aplicación del contrato inteligente y al menos una autorización condicional asociada al contrato inteligente,

- Inscripción de dichos datos ejecución del contrato inteligente en un nudo de almacenamiento de dicha cadena de bloques,

- Recepción, mediante un módulo de conexión, de datos de conexión, dichos datos de conexión incluyen al menos una solicitud de autorización,

- Identificación de una autorización condicional complementaria a dicha solicitud de autorización en los datos ejecución del contrato inteligente inscritos sobre un nudo de almacenamiento de la cadena de bloques, dicha autorización condicional está asociada a unas condiciones de aplicación,

- Verificación de dichas condiciones de aplicación incluidas en los datos ejecución del contrato inteligente, y

- Generación de una instrucción de atribución de autorización aceptando la solicitud de autorización únicamente si todas las condiciones de aplicación de dicha autorización condicional han sido verificadas.

Otras ventajas y características de la invención aparecerán con la lectura de la siguiente descripción dada a título de ejemplo ilustrativo y no limitativo, haciendo referencia las figuras adjuntas que representan:

• Figura 1, un esquema de sistema informático de creación y de gestión de autorizaciones para objetos conectados según la invención.

• Figura 2, un esquema de la organización de los servidores de almacenamiento y del contenido de la cadena de bloques según la invención.

• Figura 3, las diferentes etapas del procedimiento de creación y de gestión de las autorizaciones según la invención. Las etapas en punteados son opcionales

• Figura 4, un esquema de un modo de realización según la invención que trata sobre la creación y la gestión de autorización de acceso para un vehículo conectado.

[Descripción de la invención]

En la continuación de la descripción, se hablará indiferentemente de “autorización de acceso” y para simplificar de “autorización”. Así, se entiende por autorización un dato o un conjunto de datos que especifican un derecho de comunicación, de vinculación, de intercambio o de acceso a un recurso. El recurso puede por ejemplo ser un dato, un fichero, un conjunto de ficheros, una aplicación, un servicio, material o un dispositivo tal como un objeto conectado. Una “autorización condicional” es una autorización asociada a unas condiciones de aplicación. Las condiciones de aplicación se corresponden con reglas de control utilizados para validar o no una solicitud de autorización.

Se entiende por “solicitud de autorización” una solicitud de acceso a un recurso. Esta solicitud está generalmente generada durante una conexión entre un objeto conectado y una tercera entidad.

Se entiende por “objeto conectado” cualquier dispositivo electrónico apto para conectarse a una red de comunicación. La red de comunicación puede ser por ejemplo una red de Internet o una red intranet. La conexión puede estar realizada por numerosos medios de comunicación tales como las conexiones cableadas o las conexiones inalámbricas (por ejemplo, Wi-Fi o Bluetooth).

Se entiende por “bloque” un conjunto de datos validados relativos por ejemplo a unas autorizaciones, unos contratos inteligentes, unos objetos o unos terceros. Cada bloque tiene una marca de tiempo y hacer referencia a un bloque anterior (excepto el primer bloque). Esta referencia se hace generalmente mediante la inclusión, en el seno de los datos del bloque, de una huella correspondiente al bloque anterior, la huella será designada en lo que sigue mediante el término “hash” más clásicamente utilizado. Esto permite asegurar que los datos de un bloque anterior no han sido modificados y que, en el marco de una cadena de bloques, los bloques se suceden en un orden cronológico. Así, se entiende por “cadena de bloques”, un encadenamiento de bloques.

Se entiende por “Hash” el resultado de una función de hash. Es una huella que permite identificar rápidamente el dato fuente. La función de hash permite reducir el tamaño de un conjunto de datos fuente mediante un procedimiento criptográfico y atribuirle, una huella única, un hash, que únicamente puede corresponder a este conjunto particular de datos fuente. En cambio, no es posible deducir el conjunto de datos fuente a partir de un hash.

Se entiende por “nudos de almacenamiento” unas réplicas de la cadena de bloques almacenadas en servidores de almacenamiento.

Se entiende por “servidor de almacenamiento” un dispositivo que incluye una memoria no transitoria y que es apta para conectarse a una red de comunicación.

Se entiende por “contrato inteligente” un conjunto de datos más conocido bajo la terminología anglosajona de “Smart contract”. Este conjunto de datos corresponde más particularmente a un conjunto de datos de ejecución y permite definir al menos las condiciones de atribución de una autorización. En lo que sigue, los datos de ejecución relativos a un contrato inteligente incluyen un identificador único del contrato inteligente, unas condiciones de aplicación del contrato inteligente y al menos una autorización condicional asociada al contrato inteligente.

Se entiende por “instrucción” o instrucción informática, unos datos que definen una o varias acciones que pueden realizarse por un dispositivo electrónico.

Se entiende por “usuario”, un usuario del sistema informático.

Se entiende por “conexión” una comunicación, un acceso, o más generalmente una vinculación entre dos recursos sometida a autorización y condiciones.

En la continuación de la descripción, las mismas referencias son utilizadas para designar los mismos elementos.

La Figura 1 esquematiza el sistema informático 1 de creación y de gestión de autorización para objetos conectados según la invención.

Este sistema reposa sobre una pluralidad de servidores de almacenamiento 20 que incluye una cadena de bloques 200 distribuida con la forma de nudos de almacenamiento 201.

Esta pluralidad de servidores de almacenamiento 20 puede encontrarse en numerosos sistemas incluyendo cadenas de bloques. La distribución de la cadena de bloques 200 con la forma de nudos de almacenamiento 201 presenta la ventaja de conferir a dicha cadena de bloques 200 unas propiedades de resiliencia en caso de ataque a uno de los nodos de almacenamiento 201. Dicha distribución que incluye una sucesión de bloques 202 permite igualmente al sistema tener una resistencia importante a la falsificación de datos. Estos servidores de almacenamiento 20 graban generalmente los datos en memorias no volátiles y pueden igualmente incluir memorias transitorias.

Tal y como se ha detallado en la figura 2, la cadena de bloques 200 está compuesta por una pluralidad de bloques 202 ordenados de forma cronológica. Los servidores de almacenamiento 20 son aptos para grabar un nuevo bloque 202 en la cadena de bloques 200. En el marco de la invención, este almacenamiento puede estar condicionado a la recepción de una instrucción de almacenamiento emitida por un usuario que tenga los derechos adecuados. Tal y como se detallará a continuación, dicho usuario es llamado entidad de gobierno. Cada uno de los bloques 202 puede ser utilizado para almacenar una gran diversidad de datos. En el marco de la invención, la cadena de bloques 200 y más particularmente los bloques 202 de la cadena de bloques 200 pueden ser utilizados para almacenar unos datos de objeto 210 relativos a los objetos conectados 10, unos datos de terceros 280 relativos a las entidades de terceros 80, unos datos de ejecución de contrato inteligente 240 relativos a los contratos inteligentes.

Los datos de objeto 210 pueden incluir al menos: un identificador único de objeto 211 y un perfil de objeto 212. Por ejemplo, el perfil de objeto 212 puede incluir los datos que pueden ser seleccionados de entre su estatus, su origen, su propietario inicial, sus características físicas, sus funcionalidades o sus permisos. Los datos de objeto 210 pueden igualmente incluir unos datos de contexto 213 tales como por ejemplo la localización geográfica del objeto. El objeto conectado 10 puede ser cualquier dispositivo electrónico apto para conectarse a una red de comunicación. El objeto conectado 10 puede incluir un controlador de acceso lógico y/o un controlador de acceso físico apto para dar acceso a un recurso conforme a una instrucción de atribución de autorización 220. Preferentemente, el objeto conectado 10 incluye un controlador de acceso físico. De forma particular, el objeto conectado 10 es apto, a partir de un derecho de acceso lógico tal como una instrucción de atribución de autorización 220, a inducir la materialización de un derecho de acceso físico a través de un controlador de acceso físico. Así, de forma preferida el objeto conectado 10 incluye un accionador físico asociado a un controlador de acceso físico. De forma más preferida, el objeto conectado 10 es seleccionado de entre: una válvula conectada, un vehículo conectado, una barrera de acceso a un aparcamiento, un interruptor conectado. La válvula conectada es un dispositivo destinado a controlar el flujo de un fluido tal como un líquido o un gas. Puede por ejemplo ser una válvula industrial o un contador de agua o de gas particularmente. De forma particular, el objeto conectado 10 incluye al menos un controlador lógico o físico y está seleccionado de entre: una válvula conectada, un vehículo conectado y un interruptor conectado. De forma preferida, el objeto conectado 10 es seleccionado de entre: una válvula conectada, un vehículo conectado y un interruptor conectado.

Los datos de terceros 280 puede incluir al menos: un identificador único de tercero 281 y un perfil de tercero 282. Por ejemplo, el perfil de tercero 282 incluye unos datos que pueden ser seleccionados de entre su estatus, su origen, sus características físicas, sus funcionalidades o sus permisos. La entidad tercero está generalmente seleccionada de entre: otro objeto conectado, un utilizador, un dato, un fichero o un conjunto de fichero o un servicio por ejemplo con la forma de una aplicación. Los datos de terceros 280 pueden igualmente incluir datos de contexto 283 tales como por ejemplo la localización geográfica de la entidad tercero.

Los datos ejecución del contrato inteligente 240 incluyen al menos: un identificador único 241 del contrato inteligente, unas condiciones de aplicación 242 del contrato inteligente y al menos una autorización condicional 243 asociada al contrato inteligente. Por ejemplo, las condiciones de aplicación 242 del contrato inteligente pueden incluir condiciones seleccionadas de entre: una condición de pago, una condición temporal, una condición de localización y una condición de seguridad. La autorización puede en cuanto a ella por ejemplo hacer referencia al derecho de acceder a una aplicación, al derecho de acceder a un dato o un fichero, autorizar el acceso mediante el objeto a un servicio de la entidad tercero, autorizar el acceso por la entidad tercero a una funcionalidad o datos del objeto. La invención permite, por ejemplo, cuando define las interacciones entre un objeto y un usuario, autorizar un usuario a utilizar determinadas funcionalidades del objeto conectado, administrarlas, o cambiar el usuario

“propietario”. La invención permite, por ejemplo, cuando define las interacciones entre objetos, atribuir una autorización de forma que asegure los intercambios de datos en confidencialidad e integridad. La invención puede igualmente ser utilizada para verificar las condiciones de seguridad necesarias para el acceso a un servicio mediante el objeto, y notificar de las condiciones no satisfechas en caso de rechazo.

De forma ventajosa, la autorización condicional puede incluir un límite en el tiempo.

Preferentemente, la cadena de bloques 200 incluye unos datos cifrados y unos datos no cifrados. Por ejemplo, al menos una parte de los datos del tercero 280, de ejecución del contrato inteligente 240 y/o del objeto 210 están cifrados antes de la grabación en un nudo de almacenamiento 201 de la cadena de bloques 200. Preferentemente, los datos cifrados lo han sido mediante métodos de cifrado asimétrico.

Los nudos de almacenamiento 201 corresponden a copias de la cadena de bloques 200. Cada uno de los nudos de almacenamiento 201 presenta preferentemente una importancia equivalente y no existe relación maestro-esclavo entre estos nudos de almacenamiento. Sin embargo, el sistema puede incluir nudos de almacenamiento 201, gestionados por entidades de gobierno 70, que tienen la posibilidad de introducir nuevos bloques 202 en la cadena de bloques 200 así como unos nudos de almacenamiento 201, que nuestra gestionados por unas entidades de gobierno 70, y por tanto son incapaces de introducir nuevos bloques 202 en la cadena de bloques 200. Los servidores de almacenamiento 20 incluyen unos nudos de almacenamiento 201, que no están gestionados por unas entidades de gobierno 70, permiten asegurar una replicación de la cadena de bloques 200 y mejoran así la resiliencia del sistema. Por ejemplo, una parte de los objetos conectados 10 pueden estar asociados a un nudo de almacenamiento 201 dedicado. Los servidores de almacenamiento 20 incluyen unos nudos de almacenamiento 201 gestionados por unas entidades de gobierno 70, que permiten asegurar una replicación de la cadena de bloques 200 pero sobre todo la integración de nuevos datos en la carrera de bloques 200 gracias a la grabación de nuevos bloques 202 por sentido del gobierno 70. Además, en el marco de la invención, el sistema informático 1 incluye un numero restringido de nudos de almacenamiento 201 gestionados por unas entidades de gobierno 70. En efecto, una de las particularidades de la invención es el de salirse de los sistemas clásicos de cadenas de bloques que reposa sobre una confianza general por presencia de una multitud de nudos almacenamiento 201 que tienen la capacidad de inscribir nuevos bloques 202, cada uno teniendo una escasa probabilidad de ser el nudo de almacenamiento implementando un nuevo bloque 202 en la cadena de bloques 200. Así, preferentemente, el sistema informático 1 según la invención incluye entre 2 y 2000 servidores de almacenamiento 20 gestionados por unas entidades de gobierno 70, de forma más preferida entre 2 y 1000 servidores de almacenamiento 20 gestionados por unas entidades de gobierno 70, y de forma también preferida entre 2 y 500 servidores de almacenamiento 20 gestionados por unas entidades de gobierno 70.

Clásicamente, los almacenamientos, de las cadenas de bloques puede ser anónimos y están abiertos a todos los usuarios. Cuando un nudo de almacenamiento recibe una nueva transacción, lo almacena en un soporte de memoria que incluye un conjunto de transacciones no confirmadas. Aunque las transacciones no confirmadas sean propagadas sobre la red de comunicación, este conjunto puede diferir de un nudo al otro, por el hecho del tiempo de propagación de las transacciones sobre la red. Así, los sistemas anteriores están basados en transacciones y cualquier nudo puede colectar un determinado número de solicitudes de inscripción de transacción en su lista y posteriormente formar un bloque. La confianza es aportada por el hecho de que ninguna entidad dispone de una autoridad superior sobre el sistema, que la grabación de un bloque está sometida a una variable aleatoria y que existe un control recíproco realizado por los mineros. Los mineros son las entidades encargadas en los sistemas clásicos de la actualización de la base de datos descentralizada, precisando esta actualización la resolución de un problema matemático que requiere mucho tiempo por los que albergan nudos de almacenamiento completos.

Contrariamente a los sistemas anteriores, el sistema incluye ventajosamente unas entidades de gobierno 70 que son las únicas que poseen el derecho de almacenar un nuevo bloque 202 sobre la cadena de bloques 200. Esta particularidad es la base de la confianza en el sistema 1 según la invención. Así, cada entidad de gobierno 70 administra un soporte memoria que incluye un conjunto de datos no confirmados. Estos datos pueden corresponder por ejemplo a datos de objeto 210, a datos de terceros 280 o a datos de ejecución de contrato inteligente 240. Estos datos no confirmados pueden ser compartidos entre las entidades de gobierno 70.

La entidad de gobierno 70 controla la validez de los datos no confirmados y una vez el bloque validado, se le añade una marca de tiempo y es añadido a la cadena de bloques. El contenido de este bloque 202 es entonces accesible a los usuarios según las modalidades definidas por el módulo de control de acceso.

Las reglas de validación del bloque 202 pueden ser variables en función de los modos de realización y de establecimiento del consenso. Por ejemplo, un bloque 202 puede ser validado por una entidad de gobierno 70 sin que sea preciso buscar un número aleatorio (Nonce) que tenga un valor tal que el hash del bloque a validar responda a unas reglas particulares. Al contrario, puede ser necesaria una prueba de trabajo como esto es visible en otros sistemas que utilizan las cadenas de bloques. Según otro modo de realización, un bloque puede también ser validado mediante el acuerdo de al menos dos, preferentemente al menos cuatro entidades de gobierno 70 y esto sin que una prueba de trabajo haya sido exigida, o también por un voto mayoritario.

Tal y como se presenta en la figura 2, un bloque 202 validado incluye el Hash del bloque anterior sobre la cadena de bloques (HASH n-1), y puede igualmente contener una firma (Sig.), una marca de tiempo (Horodat.), y/o un número aleatorio (Nonce). Una vez validado, el contenido de este bloque es entonces accesible a los usuarios 60 según las modalidades definidas por el módulo de control de acceso 30.

Estos modos de validaciones particulares son posibles ya que el sistema está basado en la confianza entre las entidades de gobierno 70 y la confianza de los usuarios 60 frente a las entidades de gobierno 70. Así, el sistema según la invención agrupa las ventajas de descentralización y de distribución de las cadenas de bloques mientras conserva la seguridad de los sistemas centralizados.

Así, preferentemente, el sistema informático 1 según la invención está conectado a, entre 2 y 2000 entidades de gobierno 70, de forma preferida entre 2 y 1000 entidades de gobierno 70 y de forma todavía más preferida entre 2 y 500 entidades de gobierno 70.

Al contrario, los sistemas clásicos que utilizan cadenas de bloques 200 para hacer el seguimiento de transacciones están conectados a varios miles de mineros encargados de validar los bloques 202.

Como complemento de las entidades de gobierno 70, el sistema 1 según la invención es preferentemente apto para comunicar con unas entidades de auditoría 90. Las entidades de auditoría 90 poseen un derecho de acceso que incluye un derecho de lectura y un acceso a unas claves de descifrado de forma que pueda auditar todos o parte de los datos cifrados. De forma particular, una entidad de auditoría 90 puede poseer un derecho de acceso que incluye un derecho de lectura y un acceso a unas claves de descifrado de forma que pueda auditar todos los datos cifrados.

Con el fin de permitir la atribución de derechos particulares a los diferentes usuarios del sistema 1 según la invención, la invención reposa sobre una arquitectura tal que, aunque el sistema sea descentralizado y beneficia así las ventajas clásicas de las cadenas de bloques distribuidas, el sistema según la invención incluye un módulo de control de acceso 30 configurado para definir los derechos de acceso de un usuario 60 a la cadena de bloques 200.

En efecto, contrariamente a la mayoría de las cadenas de bloques, en el sistema 1 según la invención, la cadena de bloques 200 presenta unos derechos de acceso diferentes en función del usuario 60. Así, el módulo de control de acceso 30 está configurado para definir un derecho de acceso, dicho derecho de acceso está seleccionado de entre una lista de derecho de acceso que incluye al menos:

- un derecho de acceso que incluye únicamente un derecho de lectura. Este derecho puede estar acordado con una mayoría de usuarios.

- un derecho de acceso que incluye un derecho de grabación de nuevos bloques 202 de la cadena de bloques 200. La grabación de nuevos bloques 202 de la cadena de bloques 200 permite validar las autorizaciones y/o los datos en espera. Es esta grabación quien confirma la validez de estos datos y su aceptación. Este derecho de grabación en el marco de la presente invención puede estar dado a varias entidades de gobierno 70. De forma preferida, el sistema según la invención incluye un número controlado de entidades de gobierno 70, garantes de una parte importante de la confianza acordada al sistema. En cambio, el número de entidades de gobierno 70 que tienen derechos de grabación es más pequeño que el observado en numerosos sistemas basados sobre una cadena de bloques. Así, preferentemente, el módulo de control de acceso 30 según la invención está configurado para conceder entre 2 y 2000 derechos de grabación de nuevos bloques 202 de la cadena de bloques 200, de forma más preferida entre 2 y 1000 y de forma todavía más preferida entre 2 y 500. Esto corresponde a un derecho concedido a las entidades de gobierno 70.

Unos derechos de acceso suplementarios pueden estar concedidos por este módulo de control de acceso 30. Así, la lista de derechos de acceso puede incluir igualmente:

- un derecho de acceso que incluye un derecho de escritura. Este derecho permite por ejemplo al usuario que pueda inscribir nuevos datos de objeto 210, de terceros 280 o de ejecución de control inteligente 240 sobre la cadena de bloques 200, y/o,

- un derecho de acceso que incluye un derecho de lectura y un acceso a unas claves de descifrado. Este derecho puede estar concedido a una entidad de auditoría 90 de forma que verifique al menos una parte de las autorizaciones concedidas y más generalmente de los datos almacenados en la cadena de bloques 200.

El módulo de acceso 30 puede estar configurado de manera que conceda un derecho de acceso que incluye únicamente un derecho de lectura incluso si el usuario no está autentificado.

Además, el módulo de control de acceso 30 puede estar configurado para conceder un número limitado de derechos de acceso que incluye un derecho de escritura. Por ejemplo, el módulo de control de acceso 30 está configurado para conceder menos de 1000 derechos de acceso que incluya un derecho de escritura, preferentemente menos de 500. Esto permite principalmente limitar el número de usuarios que pueden escribir en la referencia y así reforzar la seguridad.

El derecho de escritura permite al usuario que lo dispone inscribir nuevos datos sobre la cadena de bloques 200. En cambio, este derecho no permite hacer que sus datos sean perennes y grabar un nuevo bloque 202 en la cadena de bloques 200. Así, después de la inscripción, estos nuevos datos son situados en la cadena de bloques 200 en el seno de un conjunto de datos no confirmados. Una entidad de gobierno 70 controla la validez de los datos no confirmados y una vez estos datos han sido validados son grabados sobre un nuevo bloque 202 con huella de tiempo de la cadena de bloques 200. El contenido de este bloque 202 es entonces accesible a los usuarios según las modalidades definidas por el módulo de control 30.

Preferentemente, además de un derecho de grabación de nuevos bloques 202 de la cadena de bloques 200, una entidad de gobierno 70 posee igualmente, la cadena de bloques 200, un derecho de escritura y de lectura.

Los derechos de acceso concedidos a las entidades de auditoría 90 permiten controlar y auditar la cadena de bloques 200 y principalmente las autorizaciones de acceso sobre la cadena de bloques distribuida y compartida. Preferentemente, el derecho de acceso incluye un derecho de lectura y un acceso a unas claves de descifrado necesita una autentificación de la entidad de auditoría 90 y el módulo de control de acceso 30 no concede ningún derecho de acceso a claves de descifrado y a la cadena de bloques 200 a dicha entidad de auditoría 90 no autentificada.

De la misma manera, preferentemente, la grabación de nuevos bloques 202 de la cadena de bloques 200 necesita una autentificación de la entidad de gobierno 70 y el módulo de control de acceso 30 no concede ningún derecho de acceso que incluya un derecho de grabación a dicha entidad de gobierno 70 no autentificada.

Del mismo modo que el sistema según la invención permite un control del acceso a los datos de la cadena de bloques 200, la invención se basa en una arquitectura tal que la inscripción de datos de ejecución del contrato inteligente sobre la cadena de bloques 200 está controlada por un módulo de inscripción 40 configurado para recibir y posteriormente escribir los datos ejecución del contrato inteligente 240 sobre un nudo de almacenamiento 201. Así, el módulo de inscripción 40 es apto para:

- recibir unos datos ejecución del contrato inteligente 240, emitidos por una entidad de gobierno 70, dichos datos de ejecución del contrato inteligente 240 incluyen un identificador único 241 del contrato inteligente, unas condiciones de aplicación 242 del contrato inteligente y al menos una autorización condicional 243 asociada al contrato inteligente,

- inscribir dichos datos de ejecución del contrato inteligente 240 sobre un nudo de almacenamiento 201 de dicha cadena de bloques 200.

Así, el módulo de inscripción 40 permite gestionar las autorizaciones de acceso entre usuarios y objetos, entre objetos y para los objetos en sí mismos.

De forma preferida, el módulo de inscripción 40 es apto para inscribir dichos datos ejecución del contrato inteligente 240 sobre un nudo de almacenamiento 201 de dicha cadena de bloques 200 únicamente si los datos ejecución del contrato inteligente 240 son emitidos por una entidad de gobierno 70.

Además, el módulo de inscripción 40 está igualmente configurado para recibir y posteriormente inscribir los datos de objeto 210 y los datos de terceros 280 sobre un nudo de almacenamiento 201. Así, el módulo de inscripción 40 es apto para:

- recibir unos datos de objeto 210 y/o de terceros 280,

- inscribir dichos datos de objeto 210 y/o de terceros 280 sobre un nudo de almacenamiento 201 de dicha cadena de bloques 200.

Así, el módulo de inscripción 40 permite igualmente gestionar las identidades y los perfiles de objeto conectados y unos terceros interactúan con estos objetos conectados.

Más particularmente, el módulo de inscripción 40 es apto para recibir unos datos de objeto 210, y/o de terceros 280 emitidos por un usuario 60 y para inscribir dichos datos de objeto 210 y/o de terceros 280 sobre un nudo de almacenamiento 201 de dicha cadena de bloques 200 únicamente si los datos son emitidos por un usuario que posea derechos escritura sobre la cadena de bloques 200.

De forma ventajosa, el módulo de inscripción 40 es apto para autentificar la identidad de la fuente de los datos. Esto permite asegurar que la identidad y el perfil de un objeto inscrito en la cadena de bloques proviene de un usuario autorizado a dichas inscripciones y refuerza sí la confianza que pueda darse a estas informaciones.

Una vez inscritos los datos de objeto 210, del tercero 280 y/o de ejecución del contrato inteligente 240 sobre un nudo de almacenamiento 201 de dicha cadena de bloques 200, el servidor de almacenamiento 20 que alberga dicho nudo de almacenamiento 201 es apto para grabar un nuevo bloque 202 sobre la cadena de bloques 200. Este bloque incluye dichos datos de objeto 210, del tercero 280 y/o de ejecución del contrato inteligente 240. Con el fin de reforzar la seguridad del sistema, de forma ventajosa, el servidor de almacenamiento 20 que alberga dicho nudo de

almacenamiento 201 es apto para grabar un nuevo bloque 202 en la cadena de bloques 200 únicamente se recibieron instrucción de validación de dichos datos, dicha instrucción de validación está emitida por una entidad de gobierno 70.

Una vez los datos inscritos en la cadena de bloques mediante el módulo de inscripción 40, estos nuevos datos son situados en la cadena de bloques 200 en el seno de un conjunto de datos no confirmados. Una entidad de gobierno 70 controla la validez de los datos no confirmados y una vez estos datos han sido validados son grabados sobre un nuevo bloque 202 con marca de tiempo de la cadena de bloques 200.

La entidad de gobierno 70 controla la validez de los datos no confirmados y una vez el bloque 202 validado, se le añade una marca de tiempo y es añadido a la cadena de bloques 200. El contenido de este bloque 202 es entonces accesible a los usuarios según las modalidades definidas por el módulo de control de acceso 30.

Además, el módulo de inscripción 40 permite una gestión evolutiva de las autorizaciones de acceso a unos servicios ofrecidos por diferentes actores. En efecto, el módulo de inscripción 40 es apto para inscribir nuevos datos que vienen a completar o modificar unos relativos a datos de objeto 210, de terceros 280 y/o de ejecución de contrato inteligente 240 ya grabados en la cadena de bloques 200.

De forma particular, el módulo de inscripción 40 es igualmente apto para inscribir en la cadena de bloques 200 unos datos inicialmente externos a la cadena de bloques 200 que pueden ser relativos a servicios y que serán necesarios para la ejecución de determinados contratos inteligentes 240 ya que permitirán verificar las condiciones de aplicación 242 comprendidas en los datos de ejecución del contrato inteligente 240.

Una vez los contratos inteligentes inscritos en la cadena de bloques 200, el sistema según la invención permite, gracias al módulo de conexión 50, la gestión de las autorizaciones y principalmente la atribución de una autorización para definida y condicional posterior a la conexión entre un objeto conectado 10 y una entidad tercera 80.

En efecto, contrariamente a la mayoría de las cadenas de bloques, el sistema 1 no gestiona transacciones según la invención sino autorizaciones, más particularmente autorizaciones relativas a un objeto conectado 10. Por ejemplo, una autorización relativa a una interacción entre un objeto conectado 10 y una entidad tercera 80. Para ello, el módulo de conexión 50 está configurado para:

- recibir unos datos de conexión 250 entre un objeto conectado 10 y una entidad tercera 80, dichos datos de conexión 250 incluyen al menos una solicitud de autorización 253,

- identificar en un nudo de almacenamiento 201 de la cadena de bloques 200 una autorización condicional 243 complementaria a dicha solicitud de autorización 253,

- verificar las condiciones de aplicación 242 incluidas en los datos de ejecución del contrato inteligente 240,

- generar una instrucción de atribución de autorización 220 que tiene derecho a la solicitud de autorización 253 únicamente si todas las condiciones de aplicación 242 de dicha autorización condicional 243 son verificadas.

Además, el módulo de conexión 50 puede estar configurado para grabar en un nudo de almacenamiento 201 de la cadena de bloques 200 los datos de conexión 250. En caso contrario esto permite asegurar la estabilidad de las conexiones efectuadas y la auditabilidad del sistema. Los datos de conexión pueden igualmente incluir un identificador único 251 así como unas informaciones de contexto 252 a saber por ejemplo las entidades implicadas en la solicitud de autorización 253.

La cadena de bloques 200 incluye todos los datos de ejecución del contrato inteligente validados por las entidades de gobierno 70 y, a pesar de la imposibilidad de modificar los bloques 202 anteriores de la cadena de bloques 200, el sistema según la invención permite ventajosamente una actualización de las autorizaciones de acceso. Para ello, de forma preferida, el módulo de conexión 50 es apto para verificar con prioridad las condiciones de aplicación 242 más recientes.

La instrucción de atribución de autorización 220 puede ser seleccionada de entre: ruptura de la asociación entre el objeto conectado 10 y la entidad tercera 80 asociada, autorizar el acceso mediante el objeto conectado 10 a un servicio de entidad tercera 80, y autorizar el acceso por la entidad tercera 80 a una funcionalidad o unos datos del objeto conectado 10.

De forma preferida, el módulo de conexión 50 es apto para permitir la instrucción de atribución de autorización a una máquina virtual para su ejecución.

Además, ventajosamente, el módulo de conexión 50 es además apto para grabar la instrucción de atribución de autorización 220 sobre la cadena de bloques 200. En efecto, el módulo de conexión 50 posee ventajosamente unos derechos de acceso correspondientes a los derechos de las entidades de gobierno 70 y por tanto un derecho de acceso que incluye un derecho de grabación de nuevos bloques 202 de la cadena de bloques 200. En caso contrario esto permite asegurar la profundidad de las autorizaciones concedidas y la auditabilidad del sistema.

De forma particular, el módulo de conexión 50 es apto para acceder a unos datos exteriores 280, que no están inscritos o grabados en la cadena de bloques 200 pero sin embargo necesarios para la verificación de las condiciones de aplicación 242 incluidos en los datos ejecución del contrato inteligente 240.

Los módulos de control de acceso 30, de inscripción 40 y de conexión 50 pueden ventajosamente estar albergados en unos entornos de ejecución seguros. Esto es particularmente ventajoso en el marco de la realización de operaciones de descifrado de datos (por ejemplo, con fines de auditoría) por el módulo de control de acceso 30 o en el marco de operaciones de cifrado de datos por el módulo de inscripción 40. Los entornos de ejecución seguros pueden ser lógicos (del tipo Trusted Execution Environnement, Secure Excecution Environnement, o SGX de Intel). Los entornos de ejecución seguros pueden ser físicos (típicamente en el seno de aplicaciones de seguridad o de Hardware Security Modules).

Según otro aspecto, la invención trata sobre un procedimiento 2 de creación y de gestión de autorizaciones para objetos conectados 10.

Este procedimiento puede ser realizado mediante un sistema informático que incluye una cadena de bloques 200 apta para almacenar datos ejecución de contrato inteligente 240, un módulo de control de acceso 30, un módulo de inscripción 40, y un módulo de conexión 50.

Las diferentes etapas de este procedimiento están representadas en las figuras 3A a 3C. Este procedimiento incluye una serie de etapas que pueden estar agrupadas en al menos tres etapas principales:

- la atribución de derechos de acceso,

- la creación o la modificación del contrato inteligente 240, y

- la atribución de autorización.

El procedimiento según la invención se distingue dos procedimientos clásicos principalmente por la instauración de un alto nivel de control sobre la creación y la gestión de las autorizaciones. Para realizar dicho control, el procedimiento 2 según la invención incluye las siguientes etapas relativas al atribución de los derechos de acceso:

- Recepción 310 de una solicitud de acceso a la cadena de bloques 200 emitida por un usuario 60,

- Atribución 320, al usuario 60 mediante el módulo de control de acceso 30 de un derecho de acceso a la cadena de bloques 200, dicho derecho de acceso está seleccionado de entre una lista que incluye al menos:

  - un derecho de acceso con únicamente un derecho de lectura, y

  - un derecho de acceso que incluye un derecho de grabación de nuevos bloques de la cadena de bloques.

Preferentemente, el derecho de acceso puede estar seleccionado de entre una lista que incluye igualmente:

- un derecho de acceso con un derecho de escritura, y

- un derecho de acceso con un derecho de lectura y un acceso a unas claves de descifrado.

El procedimiento según la invención incluye igualmente las siguientes etapas relativas la creación o la modificación del contrato inteligente 240:

- Recepción 410, por el módulo de inscripción, de los datos ejecución del contrato inteligente 240 emitidos por un usuario 60, dichos datos ejecución del contrato inteligente 240 incluyen un identificador único 241 del contrato inteligente, unas condiciones de aplicación 242 del contrato inteligente y al menos una autorización condicional 243 asociada al contrato inteligente, e

- Inscripción 430 de dichos datos ejecución del contrato inteligente sobre un nudo de almacenamiento 201 de dicha cadena de bloques 200 únicamente el derecho de acceso del usuario 60 incluye un derecho de escritura,

El procedimiento según la invención incluye las siguientes etapas relativas a la atribución de autorizaciones:

- Recepción 510, mediante un módulo de conexión 50, de datos de conexión 250, dichos datos de conexión 250 incluyen al menos una solicitud de autorización 253,

- Identificación 530 de una autorización condicional 243 complementaria a dicha solicitud de autorización 253 en los datos de ejecución del contrato inteligente 240 inscritos en un nudo de almacenamiento 201 de la cadena de bloques 200, dicha autorización condicional 243 está asociada a unas condiciones de aplicación 242,

- Verificación 540 de dichas condiciones de aplicación 242 incluidas en los datos de ejecución del contrato inteligente 240, y

- Generación 550 de una instrucción de atribución de autorización 220 que da derecho a la solicitud de autorización 253 únicamente si todas las condiciones de aplicación 242 de dicha autorización condicional 243 son verificadas.

Preferentemente, el procedimiento puede igualmente incluir una grabación 520 de datos de conexión 250, sobre un nudo de almacenamiento 201 de la cadena de bloques 200.

El procedimiento según la invención puede incluir unas etapas suplementarias tales que:

- la inscripción 200 de los usuarios 60,

- la grabación 600 de bloques 202 sobre la cadena de bloques 200,

- la revocación 700 de una autorización, y

- la auditoría 900 de los datos la cadena de bloques 200.

La revocación 700 de una autorización incluye las siguientes etapas:

- la generación 710, por una entidad de gobierno 70, de los datos de revocación de la asociación entre un objeto 10 y en entidad tercera 80, dichos datos de revocación incluyen una fecha y al menos una regla de compra por también todo que prohíbe el acceso del objeto 10 y a dicha entidad tercera 80,

- la inscripción 720, por dicha entidad de gobierno 70, sobre la cadena de bloques 200, de dichos datos de revocación, y

- la grabación 730 por dicha entidad de gobierno 70 de un nuevo bloque 202 sobre la cadena de bloques distribuida que incluye los datos de revocación.

La auditoría 900 de datos de la cadena de bloques 200 incluye las siguientes etapas:

- Emisión 910 de una solicitud de auditoría para una entidad de auditoría 90,

- Autentificación 920 por el módulo de control de acceso 30 de la entidad auditoría 90, y

- Transmisión 930 a la entidad de auditoría 90 por el módulo de control de acceso 30 de las claves de descifrado para un descifrado parcial o total de la cadena de bloques 200 si los derechos de acceso de la entidad de auditoría 90 han sido confirmados durante la autentificación 920.

En el marco de un modo de realización particular, ilustrado en la figura 4, donde el objeto conectado 10 es un vehículo conectado, la invención puede ponerse al servicio de un consorcio de sociedades que proponen unos accesos a aparcamiento 80 donde cada una de las sociedades es una entidad de gobierno 70 apta para modificar la cadena de bloques 200. A este consorcio pueden añadirse otras sociedades que proponen otros servicios adaptados a un vehículo conectado, por ejemplo, unas compañías de seguros. Así, cada sociedad propone servicios de aparcamiento y las compañías aseguradoras miembros pueden disponer del servidor de almacenamiento 20 que incluye un nudo de almacenamiento 201.

Los datos de objeto 210 han sido inscritos en la cadena de bloques mediante el objeto conectado 10. El perfil de objeto 212 puede incluir unos datos tales que la identificación del constructor, el modelo, el año de construcción del vehículo, pero igualmente un identificador relativo al propietario y/o al usuario del vehículo, así como datos relativos a servicios a los que el vehículo está abonado. La entidad tercera 80 puede por ejemplo ser un aparcamiento y los datos de terceros 280 han sido inscritos en la cadena de bloques 200 por una sociedad de gestión del aparcamiento 70. El perfil del tercero 282 puede incluir unos datos sobre el número de plazas, las restricciones a la entrada para este aparcamiento (autorizaciones, alturas del vehículo…), y/o la sociedad que se encarga de la gestión del aparcamiento. Estos datos de objeto 210 y de terceros 280 han sido, después de la variación por una entidad de gobierno, inscritos en la cadena de bloques 200.

En el marco de este modo de realización particular donde el objeto conectado es un vehículo conectado, el aparcamiento se beneficia de un derecho de acceso que incluye únicamente un derecho de lectura de la cadena de bloques 200, el vehículo se beneficia de un derecho de acceso que incluye un derecho, en la cadena de bloques 200 de lectura y de escritura mientras que una sociedad 70 que pertenece al consorcio de la sociedad propone los servicios de aparcamiento se beneficia de un derecho de acceso que incluye un derecho de grabación de nuevos bloques 202 de la cadena de bloques 200.

Durante la creación o la modificación 400 del contrato inteligente 240, la sociedad de gestión del servicio de aparcamiento envía al módulo de inscripción 40 unos datos de ejecución del contrato inteligente 240 que incluyen el identificador del contrato inteligente 241, las condiciones de aplicación 242 que incluyen por ejemplo una verificación de la tasa de ocupación del aparcamiento, la verificación del estatus del abono del vehículo al servicio del aparcamiento y al menos una autorización condicional 243 correspondiente por ejemplo a la autorización para qué el vehículo que entra en el aparcamiento.

Una vez que los datos ejecución del contrato inteligente 240 han sido recibidos, el módulo de inscripción 40 procede a una autentificación 420 de la identidad de la sociedad de gestión del aparcamiento. Y si esta identidad es validada procede a la inscripción de dichos datos ejecución del contrato inteligente 430 sobre un nudo de almacenamiento 201 de dicha cadena de bloques 200. Después, el servidor de almacenamiento que alberga el nudo de almacenamiento 201 graba un nuevo bloque 202 sobre la cadena de bloques 200. Este bloque incluye dichos datos de ejecución del contrato inteligente 240.

En el marco de este modo de realización particular, el vehículo conectado 10 puede ya beneficiarse de un abono sobre una sociedad de gestión de servicio de aparcamiento. En este caso, durante una conexión entre el vehículo conectado 10 y el aparcamiento 80, un módulo de conexión 50 recibe los datos de conexión 250 incluyendo al menos una solicitud de autorización 253. Estos datos pueden ser enviados por ejemplo por el vehículo conectado 10 o el aparcamiento 80. El módulo de conexión 50, que tiene acceso la cadena de bloques 200, identifica 530, en los datos ejecución del contrato inteligente 240 inscritos en la cadena de bloques 200, una autorización condicional 243 complementaria a la solicitud de autorización 253. El módulo de conexión 50 verifica después si las condiciones de aplicación han sido verificadas (por ejemplo, la tasa de ocupación del aparcamiento y el estatus del abono del vehículo al servicio de aparcamiento) y en caso contrario genera una instrucción de atribución de autorización 220 con derecho a la solicitud de autorización de acceso al aparcamiento.

De forma alternativa, el vehículo puede desear entrar en un aparcamiento sin tener previamente suscrito un servicio de abono. En este caso, después de la conexión entre el vehículo conectado 10 y el aparcamiento 80, el vehículo o un tercero procede a un pago (PAI) a la sociedad de gestión del servicio de aparcamiento 70. Este pago es inscrito en un nudo de la cadena de bloques y se graba un nuevo bloque que incluye esta inscripción (INS). El módulo de conexión 50 recibe los datos de conexión 250 incluyendo al menos una solicitud de autorización 253. El módulo de conexión 50, que tiene acceso a la cadena de bloques 200, identifica 530, en los datos ejecución del contrato inteligente 240 inscritos en la cadena de bloques 200, una autorización condicional 243 complementaria a la solicitud de autorización 253. El módulo de conexión 50 verifica después si las condiciones de aplicación han sido verificadas (aquí por ejemplo el pago) y en caso contrario genera una instrucción atribución de autorización 220 que da derecho a la solicitud de autorización de acceso al aparcamiento.

Así, el sistema según la invención agrupa las ventajas de descentralización y de distribución de las cadenas de bloques mientras conserva la seguridad de los sistemas centralizados. Por el hecho de todas estas ventajas, es posible establecer la confianza entre varios actores que tienen intereses y un gobierno propio en el seno de una referencia distribuida y compartida.

REIVINDICACIONES

1. Sistema informático (1) de creación de autorizaciones, de atribuciones y de gestión de dichas autorizaciones para unos objetos conectados (10) que incluye:

- una pluralidad de servidores de almacenamiento (20) que incluyen una cadena de bloques (200) distribuida con la forma de nudos de almacenamiento (201), dichos servidores de almacenamiento son aptos para grabar un nuevo bloque (202) en la cadena de bloques (200);

- un módulo de control de acceso (30) que está configurado para crear un derecho de acceso a la cadena de bloques (200), para un usuario (60) del sistema, dicho derecho de acceso está seleccionado de entre una lista que incluye al menos:

  - un derecho de acceso que incluye únicamente un derecho de lectura, y

  - un derecho de acceso que incluye un derecho de grabación de nuevos bloques (202) de la cadena de bloques (200) sobre un nudo de almacenamiento (201), el usuario (60) que posee dicho derecho es llamado una entidad de gobierno (70);

- un módulo de inscripción (40) para la creación de autorización apto para:

  - recibir datos ejecución del contrato inteligente (240), emitidos por una entidad de gobierno (70), dichos datos de ejecución del contrato inteligente (240) incluyen un identificador único (241) de dicho contrato inteligente, unas condiciones de aplicación (242) del contrato inteligente y al menos una autorización condicional (243) asociada al contrato inteligente, y

  - inscribir dichos datos de ejecución del contrato inteligente (240) sobre un nudo de almacenamiento (201) de dicha cadena de bloques (200); y

- un módulo de conexión (50) para la atribución de autorización apto para:

  - recibir unos datos de conexión (250) entre un objeto conectado (10) y una tercera entidad (80), dichos datos de conexión (250) incluyen al menos una solicitud de autorización (253),

  - identificar sobre un nudo de almacenamiento (201) de la cadena de bloques (200) una autorización condicional (243) complementaria a dicha solicitud de autorización (253),

  - verificar las condiciones de aplicación (242) incluidas en los datos ejecución del contrato inteligente (240), y

  - generar una instrucción de atribución de autorización (220) que da derecho a la solicitud de autorización (253) únicamente si todas las condiciones de aplicación (242) de dicha autorización condicional (243) han sido verificadas.

2. Sistema según la reivindicación 1 caracterizado porque el módulo de conexión (50) es además apto para grabar la instrucción de atribución de autorización (220) en la cadena de bloques (200).

3. Sistema según una de las reivindicaciones 1 o 2 caracterizado porque el módulo de conexión (50) es apto para transmitir la instrucción de atribución de autorización a una máquina virtual para su ejecución.

4. Sistema según una cualquiera de las reivindicaciones 1 a 3 caracterizado porque la cadena de bloques (200) incluye unos datos cifrados y unos datos no cifrados.

5. Sistema según una cualquiera de las reivindicaciones 1 a 4 caracterizado porque la cadena de bloques (200) incluye unos datos de objeto (210) relativos a dicho objeto conectado (10), dichos datos de objeto incluyen al menos: un identificador único de objeto (211) y un perfil de objeto (212).

6. Sistema según una cualquiera de las reivindicaciones 1 a 5 caracterizado porque el perfil del objeto (212) incluye unos datos que pueden ser seleccionados de entre su estatus, su origen, sus características físicas, sus funcionalidades o sus permisos.

7. Sistema según una cualquiera de las reivindicaciones 1 a 6 caracterizado por que la cadena de bloques (200) incluye unos datos de un tercero (280) relativos a dicha entidad tercero (80), dichos datos de tercero incluyen al menos: un identificador único de tercero (281) y un perfil de tercero (282).

8. Sistema según una cualquiera de las reivindicaciones 1 a 7 caracterizado por que la entidad tercero (80) es seleccionada de entre: otro objeto conectado, un usuario, un dato, un fichero o un conjunto de fichero o un servicio por ejemplo con la forma de una aplicación.

9. Sistema según una cualquiera de las reivindicaciones 1 a 8 caracterizado por que el objeto conectado (10) incluye al menos un controlador lógico o físico y está seleccionado de entre: una válvula conectada, un vehículo conectado y un interruptor conectado.

10. Sistema según una cualquiera de las reivindicaciones 1 a 9 caracterizado por que al menos una parte de los datos del tercero (280), de ejecución del contrato inteligente (240) y/o de los datos del objeto (210) están cifrados antes de la grabación en un nudo de almacenamiento (201) de la cadena de bloques (200).

11. Sistema según una cualquiera de las reivindicaciones 1 a 10 caracterizado por que las condiciones de aplicación (242) incluyen unas condiciones seleccionadas de entre: una condición de pago, una condición temporal, una condición de localización y una condición de seguridad.

12. Sistema según una cualquiera de las reivindicaciones 1 a 11 caracterizado por que el módulo de conexión (50) es apto para verificar con prioridad las condiciones de aplicación (242) más recientes.

13. Sistema según una cualquiera de las reivindicaciones 1 a 12 caracterizada por que la instrucción de atribución de autorización (220) es seleccionada de entre: ruptura de la asociación entre el objeto conectado (10) y la entidad tercero (80) asociada, autorizar el acceso mediante el objeto conectado (10) a un servicio de la entidad tercero (80), y autorizar el acceso mediante la entidad tercero (80) a una funcionalidad o unos datos del objeto conectado (10).

14. Procedimiento (2) de creación y de gestión de autorizaciones para objetos conectados (10), realizado por un sistema informático que incluye una cadena de bloques (200) distribuida con la forma de nudos de almacenamiento (201), dichos servidores de almacenamiento (20) son aptos para grabar un nuevo bloque (202) sobre la cadena de bloques (200), un módulo de control de acceso (30), un módulo de inscripción (40), y un módulo de conexión (50), dicho procedimiento incluye las etapas de:

- Definición (320), mediante el módulo de control de acceso (30), de un derecho de acceso la cadena de bloques (200), para un usuario (60), dicho derecho de acceso está seleccionado de entre una lista que incluye al menos:

  - un derecho de acceso que incluye únicamente un derecho de lectura, y

  - un derecho de acceso que incluye un derecho de grabación de nuevos bloques (202) de la cadena de bloques (200), el usuario (60) que tiene tal derecho es llamado una entidad de gobierno (70);

- Recepción (410), mediante el módulo de inscripción (40), de datos de ejecución del contrato inteligente (240) emitidos por una entidad de gobierno (70), dichos datos ejecución del contrato inteligente (240) incluyen un identificador único (241) del contrato inteligente, unas condiciones de aplicación (242) del contrato inteligente y al menos una autorización condicional (243) asociada al contrato inteligente,

- Inscripción (430) de dichos datos ejecución del contrato inteligente (240) sobre un nudo de almacenamiento (201) de dicha cadena de bloques (200),

- Recepción (510), mediante el módulo de conexión (50), de datos de conexión (250), dichos datos de conexión (250 a) incluyen al menos una solicitud de autorización (253),

- Identificación (530) de una autorización condicional (243) complementaria a dicha solicitud de autorización (253) en los datos ejecución del contrato inteligente (240), inscritos en un modo de almacenamiento (201) de la cadena de bloques (200), dicha autorización condicional (243) está asociada a unas condiciones de aplicación (242),

- Verificación (540) de dichas condiciones de aplicación (242) incluidas en los datos ejecución del contrato inteligente (240), y

- Generación (550) de una instrucción de atribución de autorización (220) que da derecho a la solicitud de autorización (253) únicamente si todas las condiciones de aplicación (242) de dicha autorización condicional (243) han sido verificadas.

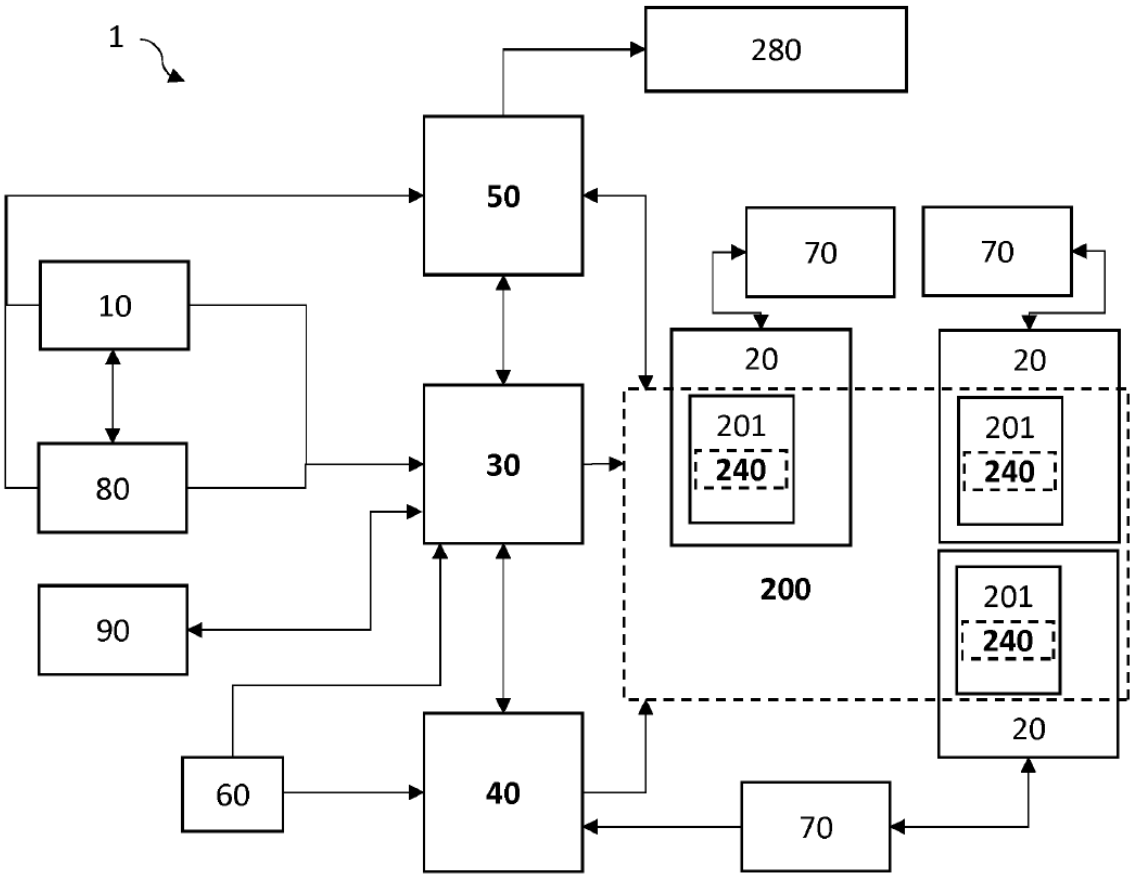
1
280
50
70
70
10
20
20
201
240
201
240
30
80
200
201
240
90
20
60
40
70

FIG. 1

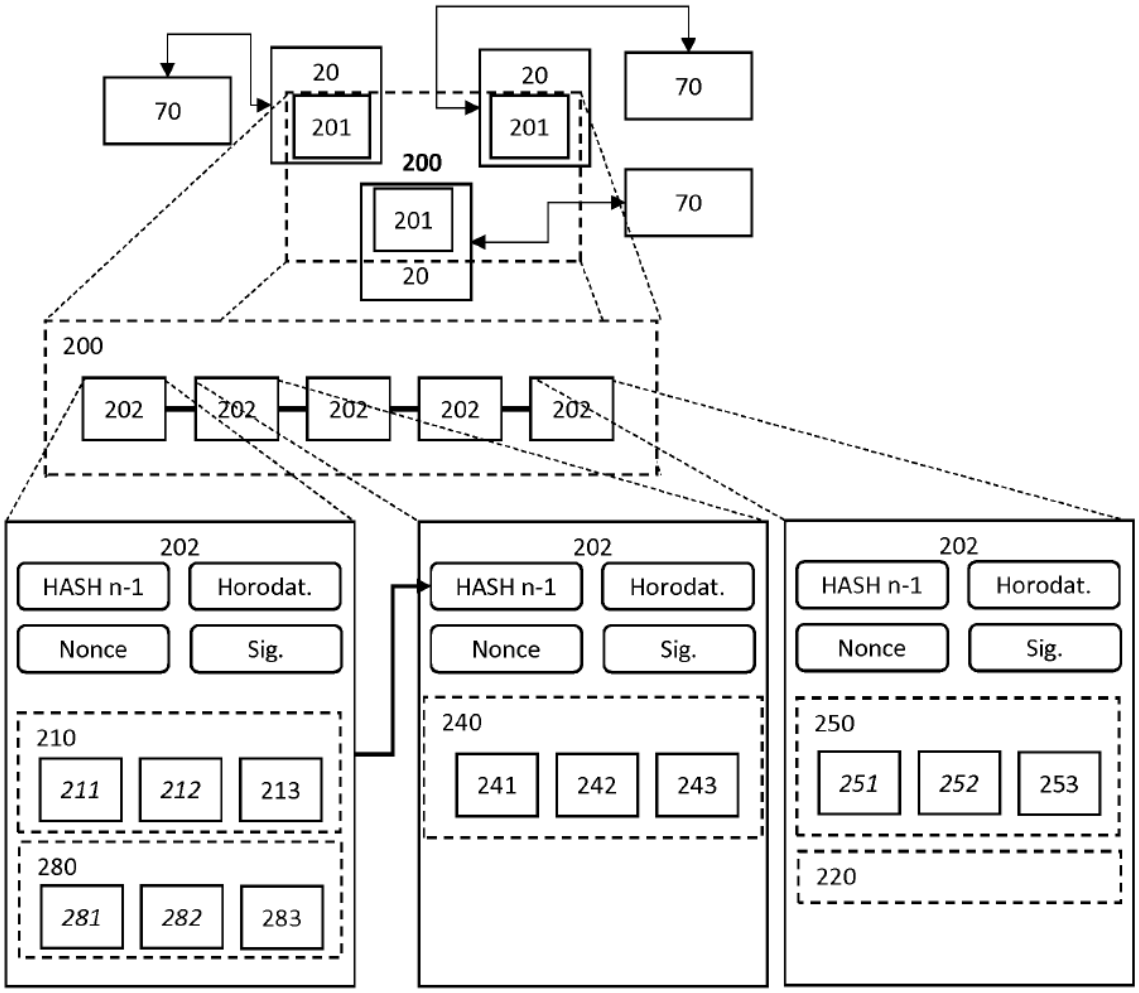
70
20
201
20
201
70
200
201
70
20
200
202
202
202
202
202
202
HASH n-1
Horodat.
Nonce
Sig.
210
211
212
213
280
281
282
283
202
HASH n-1
Horodat.
Nonce
Sig.
240
241
242
243
202
HASH n-1
Horodat.
Nonce
Sig.
250
251
252
253
220

FIG. 2

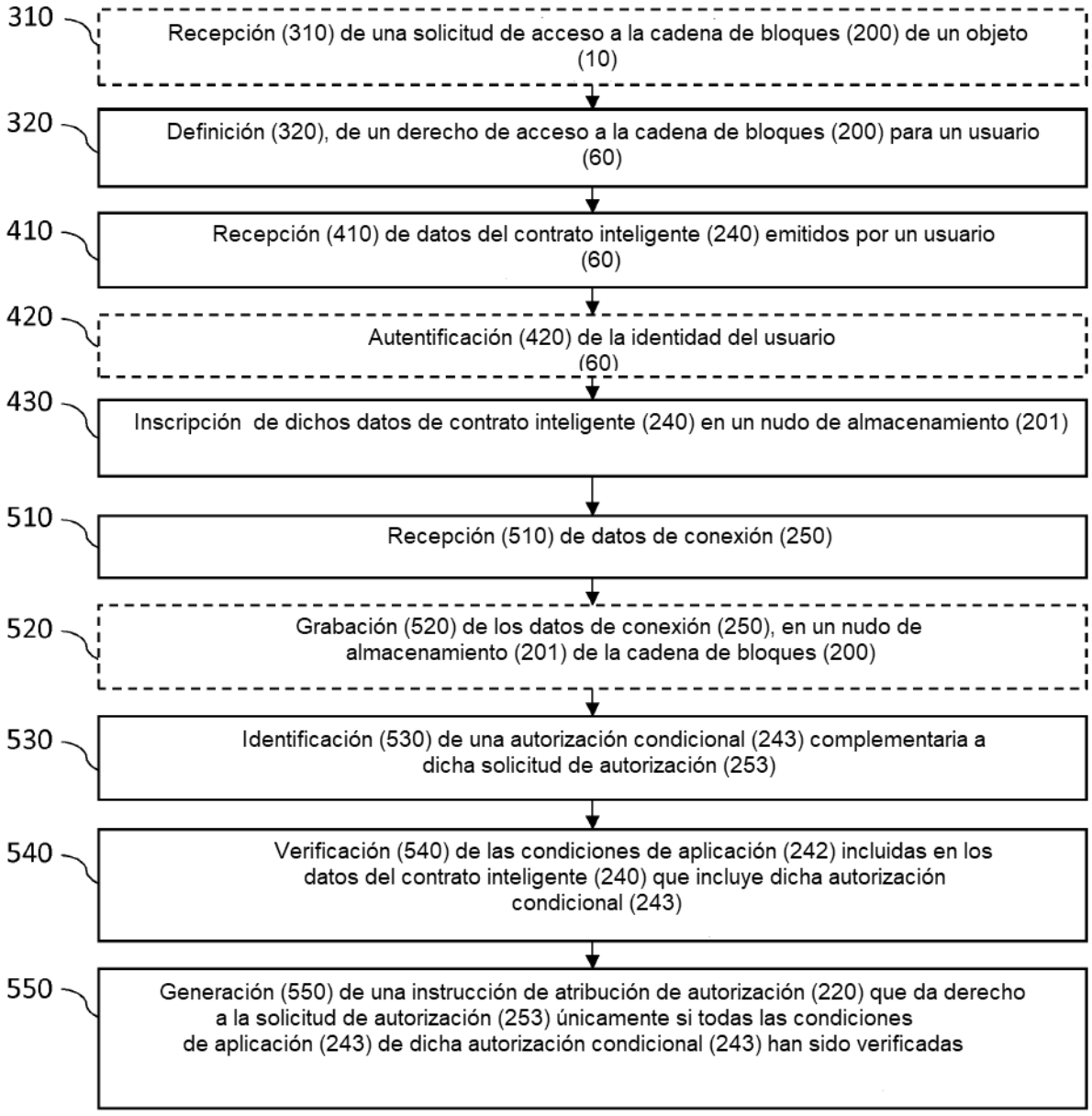
310
Recepción (310) de una solicitud de acceso a la cadena de bloques (200) de un objeto (10)
320
Definición (320), de un derecho de acceso a la cadena de bloques (200) para un usuario (60)
410
Recepción (410) de datos del contrato inteligente (240) emitidos por un usuario (60)
420
Autentificación (420) de la identidad del usuario (60)
430
Inscripción de dichos datos de contrato inteligente (240) en un nudo de almacenamiento (201)
510
Recepción (510) de datos de conexión (250)
520
Grabación (520) de los datos de conexión (250), en un nudo de almacenamiento (201) de la cadena de bloques (200)
530
Identificación (530) de una autorización condicional (243) complementaria a dicha solicitud de autorización (253)
540
Verificación (540) de las condiciones de aplicación (242) incluidas en los datos del contrato inteligente (240) que incluye dicha autorización condicional (243)
550
Generación (550) de una instrucción de atribución de autorización (220) que da derecho a la solicitud de autorización (253) únicamente si todas las condiciones de aplicación (243) de dicha autorización condicional (243) han sido verificadas

FIG. 3

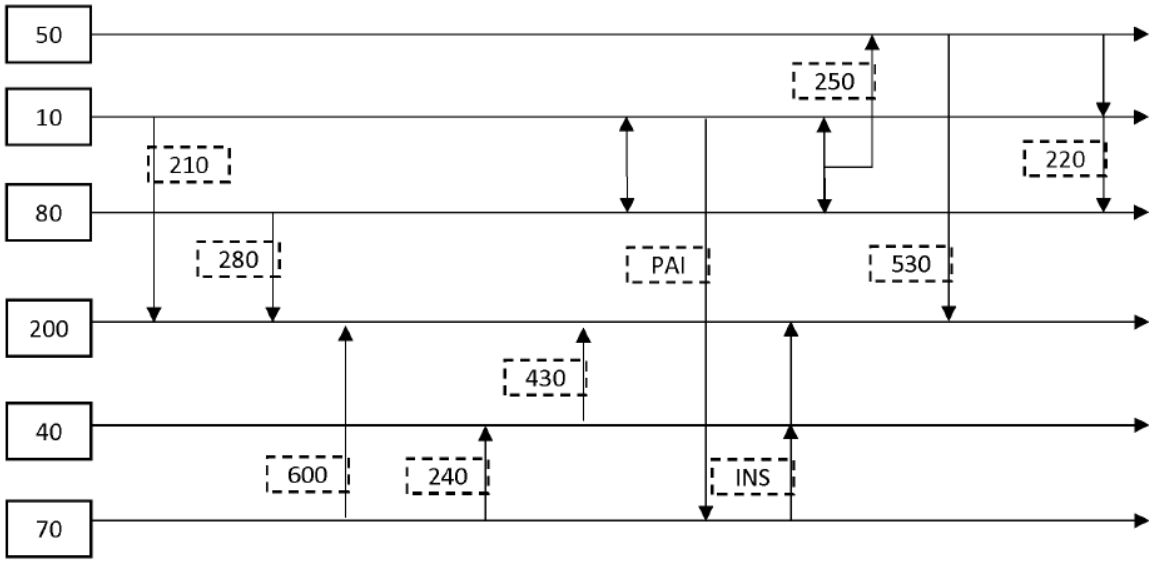

FIG. 4