(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 771 229**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **04.09.2017 E 17189163 (3)**

(97) Fecha y número de publicación de la concesión europea: **06.11.2019 EP 3451608**

(54) Título: **Sistema de comunicación de datos basado en la unidad de filtro que incluye una plataforma de cadena de bloques**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.07.2020

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München , DE

(72) Inventor/es:

FALK, RAINER

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Sistema de comunicación de datos basado en la unidad de filtro que incluye una plataforma de cadena de bloques

ANTECEDENTES

En el momento actual de una creciente demanda de soluciones TI entre compañías, la información entre compañías se debe transmitir en forma de transacciones. En varios casos, tales como en el caso de la tecnología Bitcoin o de los Contratos Inteligentes, estas transacciones se pueden basar en la tecnología de cadena de bloques, que ofrece una plataforma abierta o pública para compartir, ejecutar y revisar las respectivas transacciones.

En el caso de dichas plataformas de transacciones abiertas, existe el riesgo de que la información de la compañía involuntariamente sensible o las transacciones no publicadas o las transacciones no aprobadas debidamente se puedan transmitir a una base de datos de transacciones abiertas, por ejemplo, la base de datos de cadena de bloques. Esto se puede producir, por ejemplo, por el hecho de que los empleados usan un software de cadena de bloques, cuyo derecho no se confiere al uso, o al usar una plataforma de cadena de bloques usada por la compañía, que se usa de manera inadmisible.

El documento de patente US 2017/063789 divulga un procedimiento para la separación segura dentro de una red informática. El procedimiento incluye las etapas de: (i) proporcionar un módulo de separación segura entre una red informática de baja seguridad y una red informática de alta seguridad; (ii) interceptar, mediante el módulo de separación segura, cualquier dato dirigido desde la red informática de baja seguridad a la red informática de alta seguridad; (iii) enrutar, mediante el módulo de separación segura, los datos a un primer destino; (iv) autenticar la comunicación; (v) filtrar los datos usando uno o más filtros; y (vi) comunicar los datos, solo si pasan el uno o más filtros, a una red informática de destino.

SUMARIO

Por lo tanto, es necesario evitar el tráfico de datos inválidos y/o no deseados desde una primera red a una segunda red basada en la cadena de bloques.

Es un objetivo de la presente solicitud proporcionar un sistema y un respectivo procedimiento para realizar la comunicación de datos entre una primera red y una segunda red basada en la cadena de bloques, que está adaptada para evitar el tráfico de datos no válidos y/o no deseados.

Se proporcionan un sistema y un procedimiento de acuerdo con las reivindicaciones independientes. Otros modos de realización se definen en las reivindicaciones dependientes.

De acuerdo con un modo de realización, se divulga un sistema adaptado para realizar la comunicación de datos. El sistema comprende una primera interfaz adaptada para comunicarse con una primera red. El sistema comprende además una unidad de filtro. El sistema comprende además una segunda interfaz adaptada para comunicarse con una segunda red conectada a la primera red por medio de la unidad de filtro, en la que la segunda red está adaptada para funcionar como una plataforma de cadena de bloques. De acuerdo con esto, la unidad de filtro está adaptada para permitir selectivamente que los datos recibidos desde la primera red por medio de la primera interfaz se transmitan a la segunda red por medio de la segunda interfaz.

Dicho enfoque se puede basar en el descubrimiento de que la disposición de una unidad de filtro entre una primera red y una segunda red basada en la cadena de bloques puede proporcionar una implementación técnica que permita una restricción adicional del tráfico de datos que se origina en la primera red y llega a la segunda red. Dado que dicha segunda red basada en la cadena de bloques puede funcionar procesando datos de manera irreversible, dichos medios técnicos pueden ayudar a evitar la publicación de datos que de otro modo no se podrían eliminar, o a evitar el procesamiento de transacciones comprendidas dentro de los datos para los cuales el efecto del procesamiento podría no invertirse más. El filtrado que realiza la restricción adicional se puede definir independientemente de la lógica de cadena de bloques para verificar la validez de las transacciones. Esto permite definir de manera flexible qué transacciones se pueden enviar por una empresa a la segunda red basada en la cadena de bloques, por ejemplo, a una plataforma abierta o pública de cadena de bloques para su procesamiento. Las autorizaciones y las aprobaciones específicas de la empresa se pueden verificar de manera flexible, sin que se requiera que la plataforma de cadena de bloques procese la información de permisos internos de la compañía. Los servicios de autorización internos de la empresa y la información de autorización se pueden integrar fácilmente, sin exponer la información de autorización interna de la compañía a una plataforma de cadena de bloques pública o abierta. Los cambios dentro de la organización de la empresa se pueden reflejar mediante normas de filtro modificadas, es decir, sin requerir cambios en la plataforma de cadena de bloques o en los datos procesados por la infraestructura de cadena de bloques.

El filtrado de datos antes de enviarse a la segunda red basada en la cadena de bloques, por ejemplo, una plataforma de cadena de bloques o una infraestructura de cadena de bloques, para su procesamiento se requiere cuando una empresa o en entornos empresariales usan plataformas de cadena de bloques abiertas o públicas. A diferencia de un

firewall convencional, el propósito no es evitar ataques de red en la red de la compañía limitando la comunicación de red, sino hacer cumplir las normas sobre transacciones salientes que no se puedan eliminar o invertir una vez aceptadas y procesadas por la infraestructura de cadena de bloques. Entonces, la invención permite el uso seguro y controlado de una infraestructura de cadena de bloques abierta o pública. Las transacciones entrantes también se pueden filtrar antes de importar las transacciones en los sistemas TI internos de la compañía.

De acuerdo con otro modo de realización, se divulga un procedimiento para realizar la comunicación de datos. El procedimiento comprende permitir selectivamente que los datos recibidos desde una primera red se transmitan a una segunda red. De acuerdo con este procedimiento, la segunda red se hace funcionar como una plataforma de cadena de bloques en base a los datos permitidos.

Dicho enfoque se puede basar en el filtrado selectivo de datos antes de llegar a la segunda red basada en la cadena de bloques. Por lo tanto, se puede evitar que los datos, que no se consideren adecuados para el procesamiento por la tecnología de cadena de bloques, lleguen a la segunda red, que puede funcionar de manera irreversible.

Una red con arreglo a la presente divulgación se puede referir a cualquier conjunto de nodos que permita a una pluralidad de participantes realizar la comunicación de datos entre sí. La red puede ser una red pública o una red privada. La red puede o no estar basada en una plataforma de cadena de bloques. La red puede estar conectada al menos a una red adicional. La red puede procesar irreversiblemente los datos en base a las técnicas de cadena de bloques.

Una unidad de filtro con arreglo a la presente divulgación se puede referir a cualquier unidad, que esté adaptada para separar el primer conjunto de datos de un segundo conjunto de datos. Los datos pueden comprender al menos una transacción que se procesará por una plataforma de cadena de bloques. La separación puede tener lugar porque el primer conjunto de datos puede pasar la unidad de filtro y el segundo conjunto de datos no puede pasar la unidad de filtro. Aquí, la separación se puede controlar por una entrada de usuario.

Una plataforma de cadena de bloques con arreglo a la presente divulgación se puede referir a cualquier base de datos implementada en una red, que se base al menos en parte en la técnica de cadena de bloques. La cadena de bloques puede comprender una pluralidad de bloques que comprendan datos relacionados con transacciones y/o Contratos Inteligentes. El encadenamiento de diferentes bloques se puede implementar mediante valores criptográficos hash almacenados en cada bloque, en el que cada valor hash se puede referir a datos de un bloque previo.

En un modo de realización del sistema, la unidad de filtro está adaptada para permitir selectivamente los datos en base a un contenido de datos y/o a una fuente de datos.

La provisión de una unidad adaptada para filtrar datos en base a su contenido de datos puede permitir de este modo controlar una distribución de información en base al nivel de confidencialidad de esta información. La provisión de una unidad adaptada para filtrar datos en base a su fuente de datos puede permitir de este modo distribuir los datos en base a reglamentos dados, tales como una política de empresa. Por ejemplo, una política se puede comparar con el contenido de datos y/o la fuente de datos para decidir si los permite o no.

En otro modo de realización, la unidad de filtro está adaptada para permitir selectivamente los datos en base a una entrada de usuario.

De este modo, los criterios de selección de una unidad de filtro se pueden adaptar de acuerdo con las circunstancias actuales y las necesidades del usuario.

En otro modo de realización, la unidad de filtro es parte de a) un firewall de red localizado en una transición entre la primera red y la segunda red o b) un servicio basado en la nube.

Con respecto al firewall de red, la unidad de filtro se puede implementar por medios técnicos preferentemente simples. Perteneciente al servicio basado en la nube, el tráfico de datos de filtrado se puede externalizar desde una conexión de red actual, ahorrando de este modo recursos de las redes actuales.

En otro modo de realización, los datos comprenden una transacción, que se puede procesar por la plataforma de cadena de bloques.

De este modo, la segunda red que comprende la plataforma de cadena de bloques se puede usar como una base de datos abiertamente accesible, permitiendo que cualquier participante comparta y revise las transacciones que se realizarán. La segunda red puede ser una plataforma de cadena de bloques autorizada a la que pueden acceder múltiples empresas.

En otro modo de realización, la unidad de filtro está adaptada para realizar el permiso selectivo de los datos que comprenden la transacción independientemente de o de otras transacciones, que se hayan recibido previamente por el dispositivo de filtro.

De este modo, se puede proporcionar un permiso confiable de transacciones que se procesarán por la plataforma de cadena de bloques independientemente de o de un protocolo de transacción.

En otro modo de realización, la unidad de filtro está adaptada para realizar el permiso selectivo de los datos que comprenden la transacción en base a otras transacciones, que se hayan recibido previamente por la unidad de filtro.

De este modo, por ejemplo, la cantidad de transacciones procesadas por la plataforma de cadena de bloques previamente se pueden tener en cuenta para proporcionar otras transacciones a la plataforma de cadena de bloques. Como consecuencia, el número de transacciones realizadas en un intervalo de tiempo predefinido puede ser limitado. También, se pueden tener en cuenta otras propiedades de las transacciones anteriores, por ejemplo, contenido de datos y/o fuente de datos, etc. Se pueden desarrollar conjuntos de normas heurísticas para permitir los datos.

En otro modo de realización, los datos comprenden una clasificación de la transacción y el permiso selectivo de la unidad de filtro se adapta para basarse en la clasificación de la transacción.

De este modo, en base a cualquier característica de transacción, las diferentes transacciones se pueden manejar de una manera diferente. La clasificación puede parametrizar determinados detalles de la transacción de modo que se pueden comparar fácilmente diferentes transacciones.

En otro modo de realización, la clasificación de la transacción comprende una etiqueta de seguridad de la transacción.

De este modo, el nivel de confidencialidad que se refiere a una transacción se puede tener en cuenta para una evaluación, si se proporciona una transacción para su procesamiento a la plataforma de cadena de bloques de la segunda red.

En otro modo de realización, la unidad de filtro está adaptada para recibir, desde una unidad de aprobación de transacción de la primera red, instrucciones para bloquear la transacción, por ejemplo, si la unidad de aprobación de transacción no recibe un número predeterminado de mensajes de aprobación desde los respectivos participantes.

De este modo, la unidad de filtro se adapta para controlarse, al menos en parte, por los reglamentos implementados en la primera red, que corresponden a las aprobaciones de los participantes que comparten la primera red. Estas aprobaciones que se darán para transmitir una transacción a una plataforma de cadena de bloques pueden representar la autoridad de los respectivos participantes en una comunidad, por ejemplo, una empresa. Como consecuencia, dicha adaptación puede implementar, por ejemplo, una política de empresa dada. La política de empresa también puede reflejar reglamentos que le permitan a la empresa cumplir con las normas de la compañía o con las limitaciones regulatorias.

En otro modo de realización, el sistema comprende además una unidad de etiquetado, que está adaptada para etiquetar los datos que comprenden la transacción permitida por la unidad de filtro usando una suma de verificación, en la que la etiqueta es indicativa de la respectiva unidad de filtro de una pluralidad de unidades de filtro. La unidad de etiquetado también puede etiquetar la transacción usando otra clave única, de forma alternativa o adicionalmente a la suma de verificación. La suma de verificación puede ser una suma de verificación criptográfica, por ejemplo, un código de autenticación de mensaje o una firma digital.

De este modo, cualquier dato recibido por la primera red se puede asignar a una unidad de filtro específica, que esté adaptada para controlar el permiso de los datos para llegar a la segunda red. Por lo tanto, estos medios pueden facilitar la inspección de los procesos de filtrado.

En otro modo de realización, el sistema comprende además una unidad de modificación, que está adaptada para modificar la transacción permitida por la unidad de filtro, en la que la transacción modificada se transmite a la segunda red por medio de la segunda interfaz y la transacción no modificada no se transmite a la segunda red por medio de la segunda interfaz.

De este modo, la transacción modificada, que puede llegar a la plataforma de cadena de bloques, y la transacción no modificada, que no puede llegar a la plataforma de cadena de bloques, puede contener información diferente. Como ejemplo, la información, que debe estar disponible para los participantes de la primera red, pero que no debe estar disponible para los participantes de la segunda red, simplemente se puede incluir en la transacción no modificada, pero no en la modificada. En consecuencia, estos medios pueden permitir una distribución deseada de información. La anonimización es posible. La información sensible a la privacidad se puede filtrar.

En otro modo de realización, la unidad de filtro está adaptada además para permitir selectivamente que los datos recibidos desde la segunda red se transmitan a la primera red.

De este modo, el malware que reside en la segunda red se puede bloquear para que no llegue a la primera red. Además, solo las transacciones que cumplan con las normas de filtro se pueden importar y procesar en los sistemas

TI internos de la compañía. En particular, solo las transacciones que cumplen con las normas de filtro se pueden importar automáticamente. Otras transacciones se pueden rechazar o pueden requerir una aprobación explícita antes de importarlas en un sistema TI interno de la compañía.

En otro modo de realización, la primera red es una red privada y/o la segunda red es una red pública.

De este modo, la unidad de filtro se puede implementar para filtrar el tráfico de datos que se origina en una primera red hasta una segunda red, en el que la primera red comprende un número menor de participantes que la segunda red. Por tanto, estos medios están adaptados para controlar el tráfico de datos a diferentes círculos de participantes.

En un modo de realización del procedimiento, el procedimiento se realiza por un sistema de acuerdo con cualquiera de los modos de realización anteriores.

De este modo, el procedimiento se puede realizar en base a una implementación técnica preferentemente simple.

Un firewall de red en el sentido de la presente divulgación se puede referir a un sistema de seguridad entre diferentes redes que controla el tráfico de datos entrantes y/o salientes en base a normas de seguridad predeterminadas. El tráfico de datos puede comprender transacciones que se procesarán por una plataforma de cadena de bloques. Las normas de seguridad se pueden controlar por una entrada de usuario.

Un servicio basado en la nube con arreglo a la presente divulgación se puede referir a cualquier concepto técnico implementado en una infraestructura informática en la nube. De este modo, se puede habilitar la capacidad informática para almacenar y procesar datos en una nube privada o en un servidor de terceros localizado en un centro de datos para que los mecanismos de acceso a datos sean más eficientes y confiables.

Un nivel de seguridad con arreglo a la presente divulgación se puede referir a una característica de una transacción, que se refiere al requisito de controlar una transacción cuando se transmita desde una primera red a una segunda red. El nivel de seguridad de la transacción se puede asignar por un participante de la primera red. El nivel de seguridad se puede referir a un nivel de confidencialidad de la transacción. Por ejemplo, la información restringida se puede diferenciar de la información de alto secreto, etc.

Una red privada con arreglo a la presente divulgación se puede referir a una red accesible para un número de participantes más pequeño o restringido que una red pública. Una red privada se puede referir a una red interna de la compañía. La red privada se puede adaptar para usarse para transmitir datos a los cuales se atribuya una mayor confidencialidad.

Una red pública en el sentido de la presente divulgación se puede referir a una red accesible a un número mayor de participantes que una red privada. Por ejemplo, se puede proporcionar acceso sin restricciones a la red pública. Una red pública se puede referir a una red abierta, pero también se puede referir a una red interna de la compañía. La red pública se puede referir para no usarse para transmitir datos a los cuales se atribuya una mayor confidencialidad.

De acuerdo con un modo de realización, un producto de programa informático comprende código de programa. El código de programa se puede ejecutar por al menos un procesador. La ejecución del código de programa causa que al menos un procesador realice un procedimiento para realizar la comunicación de datos. El procedimiento comprende permitir selectivamente que los datos recibidos desde una primera red se transmitan a una segunda red. La segunda red se hace funcionar como una plataforma de cadena de bloques en base a los datos permitidos.

De acuerdo con un modo de realización, un programa informático comprende código de programa. El código de programa se puede ejecutar por al menos un procesador. La ejecución del código de programa causa que al menos un procesador realice un procedimiento para realizar la comunicación de datos. El procedimiento comprende permitir selectivamente que los datos recibidos desde una primera red se transmitan a una segunda red. La segunda red se hace funcionar como una plataforma de cadena de bloques en base a los datos permitidos.

El sumario anterior está previsto simplemente para dar una breve descripción general de algunos rasgos característicos de algunos modos de realización e implementaciones y no debe interpretarse como limitante. Otros modos de realización pueden comprender otros rasgos característicos distintos de los explicados anteriormente.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los elementos anteriores, y otros, rasgos característicos, pasos y características de la presente divulgación serán más evidentes a partir de la siguiente descripción detallada de modos de realización con referencia a las siguientes figuras:

La Figura 1 ilustra esquemáticamente una sección de cadena de bloques, que se puede montar en base a un sistema y a un procedimiento de acuerdo con la presente divulgación.

La Figura 2 ilustra esquemáticamente otra sección de cadena de bloques, que se puede montar en base a un

sistema y a un procedimiento de acuerdo con la presente divulgación.

La Figura 3 ilustra esquemáticamente una unidad de filtro en base a un sistema de comunicación de acuerdo con diversos ejemplos.

La Figura 4 representa un diagrama de flujo de un procedimiento realizado por el sistema de comunicación de datos de acuerdo con diversos ejemplos.

DESCRIPCIÓN DETALLADA DE LOS MODOS DE REALIZACIÓN

En lo sucesivo, se describen en detalle modos de realización de la invención con referencia a los dibujos adjuntos. Debe entenderse que la siguiente descripción de modos de realización no debe tomarse en un sentido limitante. El alcance de la invención no está previsto para estar limitado por los modos de realización descritos a continuación en el presente documento o por los dibujos, que se consideran solo ilustrativos.

Los dibujos deben considerarse representaciones esquemáticas y elementos ilustrados en los dibujos, que no se muestran necesariamente a escala. Más bien, los diversos elementos están representados de modo que su función y propósito general resultan evidentes para un experto en la técnica. Cualquier conexión o acoplamiento entre bloques funcionales, dispositivos, componentes u otras unidades físicas o funcionales mostrados en los dibujos o descritos en el presente documento también se puede implementar mediante una conexión o acoplamiento indirecto. También se puede establecer un acoplamiento entre componentes a través de una conexión inalámbrica. Por ejemplo, los bloques funcionales se pueden implementar en hardware, firmware, software o una combinación de los mismos.

La Figura 1 ilustra esquemáticamente una sección de cadena de bloques, que se puede montar en base a un sistema 1 y a un procedimiento 100 de acuerdo con la presente divulgación.

De acuerdo con esto, dicha cadena de bloques 13 puede comprender una pluralidad de bloques 14a-14c conectados entre sí. En dicho montaje, cada bloque 14a, 14b, 14c se puede acoplar con dos bloques vecinos 14a-14c, en el que el acoplamiento se representa, de acuerdo con la Figura 1, como la cadena 16. Un nuevo bloque 14a-14c que se incluirá en la cadena de bloques 13 se puede montar en un extremo abierto de la cadena 16 de la cadena de bloques 13. Cada bloque 14a-14c puede comprender una pluralidad de transacciones 9 que se procesarán. La creación de la cadena 16 que acopla los bloques 14a-14c para montar la cadena de bloques 13 puede recibir soporte de los valores hash 15a-15c, implementado cada uno en su respectivo bloque 14a-14c. Por la presente, cada valor hash para 15a a 15c depende del bloque predecesor 14a a 14c. Específicamente, el respectivo valor hash 15a-15c se evalúa en base a los datos del respectivo bloque predecesor 14a-14c.

Con respecto a las transacciones 9 implementadas en cada bloque 14a-14c, el código de programa se puede implementar como un contrato inteligente. El código de programa puede contener información con respecto a si una transacción 9 es admisible. De acuerdo con esto, una infraestructura común de cadena de bloques se puede realizar de manera flexible mediante diferentes procesos comerciales. Normalmente, se puede usar un árbol de hash, por ejemplo, un árbol de Merkle o un árbol de Patricia, para almacenar los respectivos valores de hash en cada uno de los bloques 14a-14c.

La Figura 2 ilustra esquemáticamente otra sección de cadena de bloques, que se puede montar en base a un sistema y a un procedimiento de acuerdo con la presente divulgación.

De acuerdo con esto, la cadena de bloques 13 comprende bloques 14a-14c, que están conectados por la cadena 16. La creación de la cadena de bloques 13 mediante el montaje de los bloques 14a-14c por la cadena 16 recibe soporte por la presente de los valores hash 15a-15c, cada uno de ellos se implementa en el respectivo bloque 14a-14c.

Específicamente, cada uno de los bloques 14a a 14c comprende configuraciones específicas de las transacciones 9. Como ejemplo, las transacciones 9 se pueden configurar como la transacción de pago 17, la transacción de transferencia de propiedad 18 y el contrato inteligente de registro 19. Por la presente, la transacción 9 puede comprender atributos adicionales, que se puedan adaptar, por ejemplo, para indicar un receptor de un pago, un objeto y su nuevo propietario o un código de programa de un contrato inteligente. Las transacciones de cadena de bloques se pueden usar también para controlar una red de automatización de energía. Una transacción puede causar que un generador de energía alimente una determinada cantidad de energía eléctrica a la red de energía, cause que un consumidor de energía limite el consumo de energía o realice una operación de conmutación en la red de energía. Los atributos de una transacción de cadena de bloques pueden indicar un dispositivo eléctrico y la acción que se realizará por el dispositivo.

La Figura 3 ilustra esquemáticamente un sistema de comunicación de datos basado en unidad de filtro 1 de acuerdo con diversos ejemplos.

De acuerdo con esto, el sistema 1 comprende al menos una primera interfaz 2 adaptada para comunicarse con una primera red 3. La primera red 3 puede ser una red privada 11, tal como una red de empresas. El acceso a la red

privada 11 puede estar restringido. La primera red 3 puede proporcionar cualquier número arbitrario de primeros nodos de red 22.

Además, el sistema 1 también comprende al menos una segunda interfaz 5 adaptada para comunicarse con una segunda red 6. La segunda red 6 puede ser una red pública 12, tal como Internet o cualquier otra red disponible para diferentes empresas y/o comunidades. Por la presente, la segunda red 6 se puede adaptar para funcionar como una plataforma de cadena de bloques 7. La segunda red 6 puede proporcionar cualquier número arbitrario de segundos nodos de red 23.

La primera red 3 y la segunda red 6 se conectan entre sí por medio de una unidad de filtro 4. La unidad de filtro 4 se puede adaptar para permitir selectivamente que los datos recibidos desde la primera red 3 por medio de la primera interfaz 2 se transmitan a la segunda red 6 por medio de la segunda interfaz 5. Estos datos pueden comprender al menos una transacción 9, que se puede procesar por la plataforma de cadena de bloques 7.

La unidad de filtro 4 se puede implementar en un firewall de red 8, como se representa en la Figura 3. Dicho firewall de red 8 puede comprender adicionalmente una memoria 21 para almacenar normas. Además, la unidad de filtro 4 también se puede implementar en un servicio basado en la nube. Además, para filtrar datos, también se puede usar una solución de seguridad entre dominios.

La unidad de filtro 4 se puede adaptar para permitir selectivamente los datos en base a un contenido de datos. Dicho contenido de datos se puede referir, por ejemplo, al contenido de la transacción 9. La unidad de filtro 4 también se puede adaptar para permitir selectivamente los datos en base a una fuente de datos. Dicha fuente de datos se puede referir a una fuente de una transacción 9, por ejemplo, un ordenador desde el cual se transmita la transacción 9 o un usuario ha iniciado sesión en el respectivo ordenador. Estos datos de transacción se pueden referir a atributos y/o contratos inteligentes.

Además, la unidad de filtro 4 también se puede adaptar para permitir selectivamente los datos en base a una entrada de usuario, lo que puede cambiar los criterios de filtro en base a circunstancias modificadas, tales como una política de empresa modificada o reglamentos públicos modificados.

La unidad de filtro 4 se puede adaptar además para realizar el permiso selectivo de los datos que comprenden la transacción 9 independientemente de otras transacciones 9, que se hayan recibido previamente por la unidad de filtro 4. Además, la unidad de filtro 4 también se puede adaptar para realizar el permiso selectivo de los datos que comprenden la transacción 9 en base a otras transacciones 9, que se hayan recibido previamente por la unidad de filtro 4. En este último caso, estos medios se pueden implementar en acciones de pago, que solo puedan ser admisibles en el caso de que una cantidad total de dinero gastado durante un intervalo de tiempo permanezca por debajo de un valor umbral predeterminado admisible.

Además, la unidad de filtro 4 se puede adaptar para permitir selectivamente que los datos recibidos desde la segunda red 6 se transmitan a la primera red 3. En dicho caso, el respectivo mecanismo de filtrado puede funcionar de manera bidireccional. Dicho mecanismo se puede usar, por ejemplo, para bloquear el tráfico de datos que se origina desde la red pública 12 y fluye hacia la red privada 11. Dicho tráfico de datos bloqueado puede ser, por ejemplo, constructivo con respecto al malware adaptado para dañar la red privada 11, tal como una red de empresas. Además, la unidad de filtro 4 también se puede adaptar para recibir, desde una unidad de aprobación de transacción 10 de la primera red 3, instrucciones para bloquear la transacción 9, si la unidad de aprobación de transacción 10 no recibe un número predeterminado de mensajes de aprobación desde los respectivos participantes.

Como se puede deducir de la Figura 3, la primera red 3 configurada como una red privada 11 puede proporcionar adicionalmente una unidad de clasificación de transacciones 20. En base a esta unidad, los datos pueden comprender una clasificación de la transacción 9, y el permiso selectivo de la unidad de filtro 4 se puede adaptar para basarse en la clasificación de la transacción. Dicha clasificación puede comprender, por ejemplo, una etiqueta de seguridad de la transacción 9 y se puede usar para atribuir un nivel de confidencialidad a las respectivas transacciones 9. Además, la primera red 3 configurada como una red privada 11 puede proporcionar adicionalmente una unidad de aprobación de transacción 10 adaptada para recibir una pluralidad de aprobaciones de diferentes participantes de la red privada 11 antes de que se permita que una transacción 9 llegue a la plataforma de cadena de bloques 7.

La Figura 4 representa un diagrama de flujo de un procedimiento 100 realizado por el sistema de comunicación de datos 1 de acuerdo con diversos ejemplos, en el que, de acuerdo con este ejemplo, los datos comunicados corresponden a una transacción 9. En el presente documento, 110, 150, 160, 165 y 170 se refieren al manejo común de las transacciones 9 que se realizarán en un entorno de cadena de bloques.

En 110, un participante de la primera red 3, por ejemplo, una red privada 11, libera una transacción 9.

Posteriormente en 120, la transacción 9 liberada se recibe por una unidad de filtro 4 conectada a la primera red 3 por medio de la primera interfaz 2.

Posteriormente, en 130, la unidad de filtro 130 examina si se debe permitir que la transacción 9 recibida llegue a la plataforma de cadena de bloques 7. De acuerdo con esto, la unidad de filtro 4 permite selectivamente las transacciones 9 recibidas desde una primera red 3 por medio de una primera interfaz 2.

En caso de que, en base a 130, la transacción 9 no pueda llegar a la plataforma de cadena de bloques 7, la transacción de cadena de bloques se bloquea en 145, por ejemplo, se descarta o se rechaza. De otro modo y con respecto a 140, la transacción 9 se reenvía a la plataforma de cadena de bloques 7 por medio de una segunda interfaz 5.

En la plataforma de cadena de bloques 7, se realiza el manejo de la transacción común 9. La plataforma de cadena de bloques 7 verifica la validez de la transacción 7 antes de incluir la transacción 9 en un bloque de cadena de bloques, confirmando que la transacción sea válida. En 150, la plataforma de cadena de bloques 7 examina si la transacción 9 es válida. Para este propósito, los valores hash 15a-15c se pueden tener en cuenta y los contratos inteligentes se pueden procesar de acuerdo con los procedimientos comunes.

En caso de que, en base a 150, la transacción 9 no se pueda validar, la transacción no válida 9 se rechazará en 165. De otro modo, un bloque que comprende la transacción validada 9 se une a la cadena de bloques 13 en 160 y se realiza la transacción 9.

Posteriormente en 170, se detiene el procedimiento 100.

REIVINDICACIONES

1. Sistema (1) adaptado para realizar la comunicación de datos, que comprende

una primera interfaz (2) adaptada para comunicarse con una primera red (3);

una unidad de aprobación de transacción (10) de la primera red (3); una unidad de filtro (4); y

una segunda interfaz (5) adaptada para comunicarse con

una segunda red (6) conectada a la primera red (3) por medio de la unidad de filtro (4),

en el que la unidad de filtro (4) está adaptada para permitir selectivamente que los datos recibidos desde la primera red (3) por medio de la primera interfaz (2) se transmitan a la segunda red (6) por medio de la segunda interfaz (5);

caracterizado por que:

la segunda red (6) está adaptada para funcionar como una plataforma de cadena de bloques (7);

los datos comprenden al menos una transacción (9) que se procesará por la plataforma de cadena de bloques; y

la unidad de filtro (4) está adaptada para recibir, desde la unidad de aprobación de transacción (10) de la primera red (3), instrucciones para bloquear la transacción (9), si la unidad de aprobación de transacción (10) no recibe un número predeterminado de mensajes de aprobación desde los respectivos participantes.

2. Sistema (1) de acuerdo con la reivindicación 1, en el que la unidad de filtro (4) está adaptada para permitir selectivamente los datos en base a un contenido de datos y/o a una fuente de datos.

3. Sistema (1) de acuerdo con cualquiera de las reivindicaciones 1 y 2, en el que la unidad de filtro (4) está adaptada para permitir selectivamente los datos en base a una entrada de usuario.

4. Sistema (1) de acuerdo con cualquiera de las reivindicaciones precedentes, en el que la unidad de filtro (4) es parte de a) un firewall de red (8) localizado en una transición entre la primera red (3) y la segunda red (6) o b) un servicio basado en la nube.

5. Sistema (1) de acuerdo con cualquiera de las reivindicaciones precedentes, en el que la unidad de filtro (4) está adaptada para realizar el permiso selectivo de los datos que comprenden la transacción (9) independientemente de otras transacciones (9), que se hayan recibido por la unidad de filtro (4) previamente.

6. Sistema (1) de acuerdo con cualquiera de las reivindicaciones 1 a 4, en el que la unidad de filtro (4) está adaptada para realizar el permiso selectivo de los datos que comprenden la transacción (9) en base a otras transacciones (9), que se hayan recibido por la unidad de filtro (4) previamente.

7. Sistema (1) de acuerdo con cualquiera de las reivindicaciones precedentes, en el que los datos comprenden una clasificación de la transacción (9), y en el que el permiso selectivo de la unidad de filtro (4) está adaptado para basarse en la clasificación de la transacción (9).

8. Sistema (1) de acuerdo con la reivindicación 7, en el que la clasificación de la transacción (9) comprende una etiqueta de seguridad de la transacción (9).

9. Sistema (1) de acuerdo con cualquiera de las reivindicaciones precedentes, que comprende además una unidad de etiquetado, que está adaptada para etiquetar los datos que comprenden la transacción (9) permitida por la unidad de filtro (4) usando una suma de verificación, en el que la etiqueta es indicativa de la respectiva unidad de filtro (4) de una pluralidad de unidades de filtro (4).

10. Sistema (1) de acuerdo con cualquiera de las reivindicaciones precedentes, que comprende además una unidad de modificación, que está adaptada para modificar la transacción (9) permitida por la unidad de filtro (4), en el que la transacción modificada se transmite a la segunda red (6) por medio de la segunda interfaz (5) y la transacción no modificada no se transmite a la segunda red (6) por medio de la segunda interfaz (5).

11. Sistema (1) de acuerdo con cualquiera de las reivindicaciones precedentes, en el que la unidad de filtro (4) está adaptada además para permitir selectivamente que los datos recibidos desde la segunda red (6) se transmitan a la primera red (3).

12. Sistema (1) de acuerdo con cualquiera de las reivindicaciones precedentes, en el que la primera red (3) es una

red privada (11) y/o la segunda red (6) es una red pública (12).

13. Procedimiento (100) para realizar la comunicación de datos, que comprende:

permitir selectivamente (130) que los datos recibidos desde una primera red (3) se transmitan a una segunda red (6);

caracterizado por que:

la segunda red (6) se hace funcionar como una plataforma de cadena de bloques (7) en base a los datos permitidos;

los datos comprenden al menos una transacción (9) que se procesará por la plataforma de cadena de bloques; y

bloquear la transacción (9), si no se recibe un número predeterminado de mensajes de aprobación para la transacción (9).

14. Procedimiento de acuerdo con la reivindicación 13, que se realiza mediante un sistema (1) de acuerdo con cualquiera de las reivindicaciones 1 a 12.

FIG 1

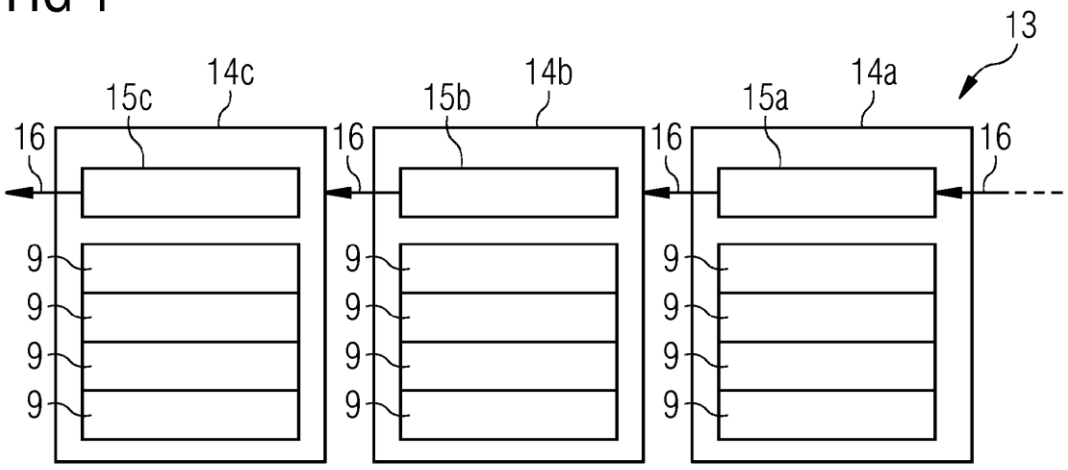
13
14c
15c
14b
15b
14a
15a
16
16
16
16
9
9
9
9
9
9
9
9
9
9
9
9

FIG 2

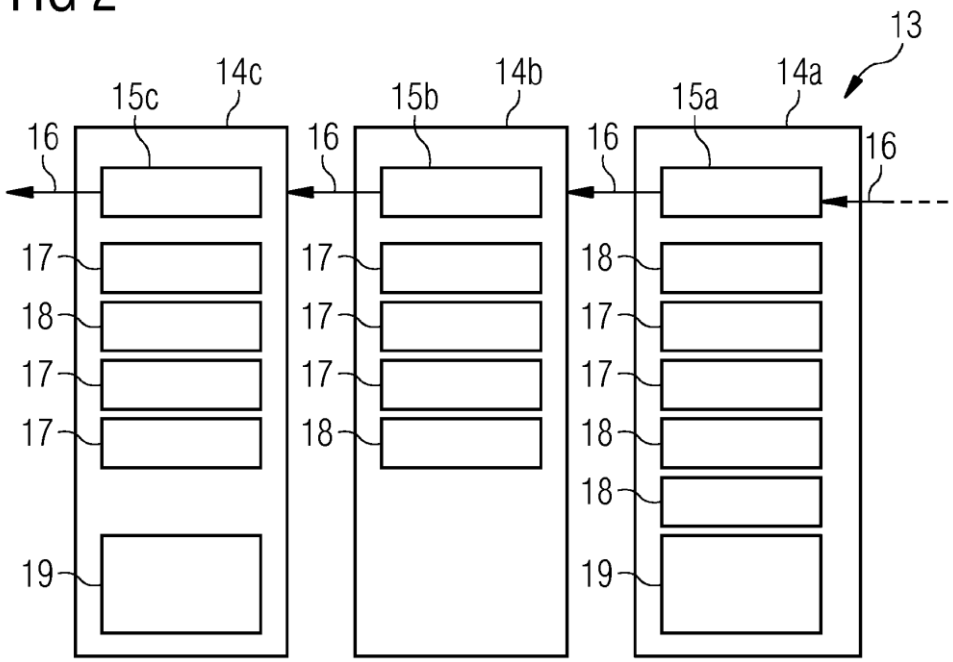
13
14c
15c
14b
15b
14a
15a
16
16
16
16
17
18
17
17
17
17
17
18
18
17
17
17
18
18
18
19
19

FIG 3

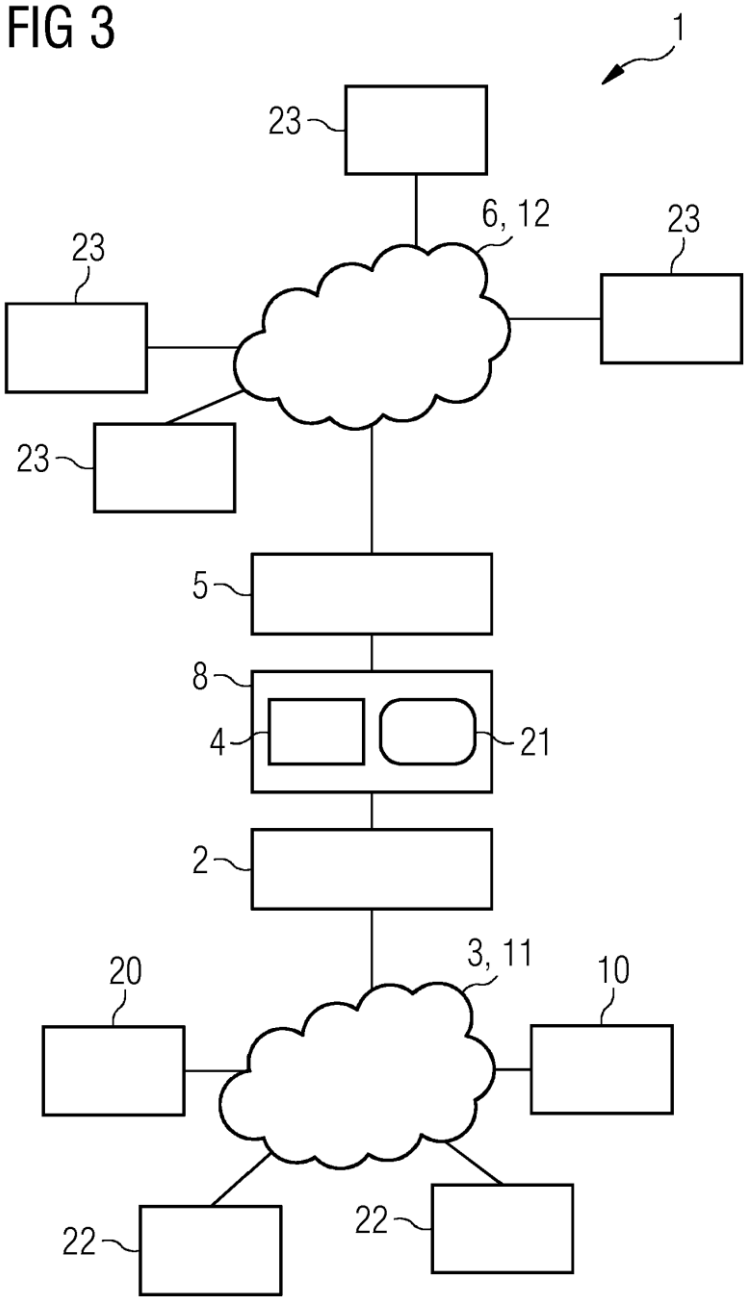

FIG 4