(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 810 828**

(51) Int. CI.:

H04L 29/08 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.03.2018 PCT/CN2018/079416**

(87) Fecha y número de publicación internacional: **27.09.2018 WO18171539**

(96) Fecha de presentación y número de la solicitud europea: **19.03.2018 E 18770564 (5)**

(97) Fecha y número de publicación de la concesión europea: **29.07.2020 EP 3531668**

(54) Título: **Procedimiento y dispositivo para el procesamiento de una solicitud de servicio**

(30) Prioridad:

21.03.2017 CN 201710168014

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.03.2021

(73) Titular/es:

ADVANCED NEW TECHNOLOGIES CO., LTD. (100.0%)
Cayman Corporate Centre, 27 Hospital Road George Town, Grand Cayman KY1-9008, KY

(72) Inventor/es:

ZHUANG, WEIMING y
LI, NING

(74) Agente/Representante:

VIDAL GONZÁLEZ, Maria Ester

DESCRIPCIÓN

Procedimiento y dispositivo para el procesamiento de una solicitud de servicio

Campo técnico

La presente solicitud se refiere al campo de las tecnologías de la información y, en particular, a un procedimiento y a un dispositivo para el procesamiento de una solicitud de servicio.

Antecedentes

Una red de cadena de bloques también es conocida como una red distribuida de registro caracterizada por la descentralización y la transparencia. Una red de cadena de bloques incluye nodos de cadena de bloques, y cada nodo de cadena de bloques se usa para sincronizar una cadena de bloques.

En la tecnología existente, un procedimiento para el procesamiento de una solicitud de servicio es como sigue: Un determinado nodo de cadena de bloques que participa en un determinado servicio difunde una solicitud de servicio del servicio a cada nodo de consenso (un nodo de cadena de bloques responsable de la verificación de consenso) en una red de cadena de bloques. La solicitud de servicio incluye datos de servicio del servicio y un resumen de los datos de servicio. Los datos de servicio incluyen información detallada del servicio (por ejemplo, información privada del nodo de cadena de bloques que participa en el servicio). El resumen de los datos de servicio se genera en función de los datos de servicio y se puede utilizar para verificar la autenticidad de los datos de servicio. Después de que la solicitud de servicio pasa la verificación de consenso realizada por cada nodo de consenso, el nodo de consenso cifra los datos de servicio y almacena los datos de servicio cifrados y el resumen en una cadena de bloques, para evitar que un nodo de cadena de bloques irrelevante para el servicio obtenga cierta información privada en los de servicio del servicio cuando se sincroniza con la cadena de bloques.

Sin embargo, no solo la carga computacional en cada nodo de consenso se incrementa en gran medida si cada nodo de consenso encripta datos de servicio incluidos en cada solicitud de servicio que pasa una verificación de consenso, también se reduce la eficiencia de realizar la verificación de consenso a la solicitud de servicio por cada nodo de consenso.

El documento de patente CN 106 100 981 A de Bubi (Beijing) Network Tech Co Ltd, titulado "Social network data interaction method and device (Procedimiento y dispositivo de interacción de datos de redes sociales)", publicado el 9 de noviembre de 2016, divulga un procedimiento y un dispositivo de interacción de datos de redes sociales. El procedimiento se usa en una red social compuesta de múltiples nodos de red entre pares. El procedimiento incluye las siguientes etapas: un primer nodo de red publica información en uno o más nodos de red en la red social; el primer nodo de red participa en la verificación de consenso de toda la red de la red social sobre la información publicada por los nodos de red en línea en la red social; y el primer nodo de red escribe la información publicada pasando la verificación de consenso de toda la red en una cadena de bloques de la red social.

El documento de patente CN 106 230 851 A de Centrin Cloud Finance & Data Tech Co Ltd, titulado “Data preservation method and system based on blockchain (Procedimiento y sistema de preservación de datos basado en cadena de bloques)", publicado el 14 de diciembre de 2016, divulga un procedimiento y un sistema de preservación de datos basados en una cadena de bloques. El procedimiento incluye: una terminal de usuario específica que envía un archivo de destino a ser preservado a una terminal de servidor central, la terminal de servidor central realiza una operación de preservación de datos en los datos de origen de un archivo de destino para adquirir una huella digital de datos preservados de los datos de origen; la terminal de servidor central almacena un ID de archivo de destino correspondiente al archivo de destino y los datos de origen, envía el ID de archivo de destino correspondiente al archivo de destino y la huella digital de datos conservados a otra terminal de usuario y la terminal de usuario específica se conecta con la cadena de bloques; y la otra terminal de usuario y la terminal de usuario específica se conectan con la cadena de bloques y reciben y almacenan el ID de archivo de destino correspondiente al archivo de destino y la huella digital de datos conservada. Cada terminal de usuario conectada con la cadena de bloques únicamente guarda la información de huella digital y no guarda los datos de origen, y la terminal de servidor central únicamente guarda los datos de origen y no guarda la información de huella digital; por lo tanto, los datos de origen y la huella digital están separados.

El documento de patente CN 102 724 044 A de Dongfang Jindun Technology Co Ltd, titulado “Electronic evidence verification and preservation method (Procedimiento de verificación y preservación de evidencia electrónica)", publicado el 10 de octubre de 2012, divulga un procedimiento de verificación y preservación de evidencia electrónica que incluye: recolectar evidencia electrónica; operar en la evidencia electrónica recopilada para generar una serie de resúmenes digitales que se utiliza para verificar si la evidencia electrónica recopilada fue falsificada; y generar un paquete de evidencia de acuerdo con la evidencia electrónica recolectada y cargar el paquete de evidencia a un servidor de centro de datos especificado para almacenar el paquete de evidencia. Un

usuario puede solicitar al servidor del centro de datos que presente un informe de verificación del paquete de evidencia.

El documento de patente KR 101 712 726 B1 de Galaxia Communications Co Ltd, titulado “Method and system for verifying integrity and validity of contents using hash code (Procedimiento y sistema para verificar la integridad y la validez de los contenidos utilizando código *hash*)", publicado el 14 de marzo de 2017, divulga un procedimiento para verificar la integridad y validez del contenido utilizando un código *hash* que incluye generar, en un servidor, información adicional relacionada con el contenido basada en datos del contenido en respuesta al contenido que se está cargando; obtener un código *hash* de referencia correspondiente al contenido basado en la información adicional asociada con el contenido; almacenar el contenido en el que se inserta el código *hash* de referencia e información adicional relacionada con el contenido en una base de datos incluida en el servidor; distribuir el contenido, con el código *hash* de referencia insertado, en la terminal de usuario e información adicional relacionada con el contenido en respuesta a una solicitud de contenido recibida de una terminal de usuario en el que está preinstalada una aplicación de reproducción de contenido conectada con el servidor; generar, en la terminal de usuario, un código *hash* de comparación correspondiente al contenido distribuido basado en la información adicional relacionada con el contenido distribuido; extraer el código *hash* de referencia insertado en el contenido distribuido y compararlo con el código *hash* de comparación; y validar la integridad del contenido distribuido y si el contenido distribuido se distribuye a través del servidor en función del resultado de comparación.

Sumario

La invención se define por un procedimiento para el procesamiento de una solicitud de servicio de la reivindicación independiente 1 y un dispositivo correspondiente para el procesamiento de una solicitud de servicio de la reivindicación independiente 5. Detalles adicionales se definen en las reivindicaciones dependientes 2-4.

A partir de las soluciones técnicas proporcionadas en las implementaciones de la presente solicitud, puede apreciarse que, en las implementaciones de la presente solicitud, en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso, cada nodo de consenso almacena el resumen de los datos de servicio en la cadena de bloques, en lugar de almacenar los datos de servicio en la cadena de bloques. Como tal, el resumen de los datos de servicio se almacena en la cadena de bloques confiable, y la autenticidad de los datos de servicio aún se puede verificar. Además, los datos de servicio no se almacenan en la cadena de bloques, por lo que los datos de servicio no pueden ser obtenidos por un nodo de la cadena de bloques irrelevante para el servicio de destino. Por lo tanto, cada nodo de consenso ya no necesita consumir recursos informáticos para cifrar los datos de servicio, mejorando de esta forma la eficiencia de realizar la verificación de consenso en la solicitud de servicio por cada nodo de consenso.

Breve descripción de los dibujos

Para describir las soluciones técnicas en las implementaciones de la presente solicitud o en la tecnología existente con más claridad, la siguiente describe brevemente los dibujos adjuntos necesarios para la descripción de las implementaciones o la tecnología existente. De forma aparente, los dibujos que se acompañan en la siguiente descripción simplemente muestran algunas implementaciones de la presente solicitud, y una persona de habilidad ordinaria en la técnica todavía puede derivar otros dibujos de estos dibujos que se acompañan sin esfuerzos creativos.

La Figura 1 es un diagrama de flujo que ilustra un procedimiento para el procesamiento de una solicitud de servicio, de acuerdo con una implementación de la presente solicitud;

La Figura 2 es un diagrama de flujo que ilustra otro procedimiento para el procesamiento de una solicitud de servicio, de acuerdo con una implementación de la presente solicitud;

La Figura 3 es un diagrama esquemático que ilustra un sistema de cadena de bloques, de acuerdo con una implementación de la presente solicitud;

La Figura 4 es un diagrama esquemático que ilustra un dispositivo para el procesamiento de una solicitud de servicio, de acuerdo con una implementación de la presente solicitud; y

La Figura 5 es un diagrama esquemático que ilustra otro dispositivo para el procesamiento de una solicitud de servicio, de acuerdo con una implementación de la presente solicitud.

Descripción de implementaciones

Las implementaciones de la presente solicitud proporcionar un procedimiento y dispositivo para el procesamiento

de una solicitud de servicio.

Para hacer que una persona experta en la técnica entienda las soluciones técnicas en la presente solicitud mejor, la siguiente descripción describe de forma clara y amplia las soluciones técnicas en las implementaciones de la presente solicitud con referencia a los dibujos adjuntos, en las implementaciones de la presente solicitud. De forma aparente, las implementaciones descritas son simplemente algunas, pero no todas las implementaciones de la presente solicitud.

Las soluciones técnicas proporcionadas en las implementaciones de la presente solicitud se describen en detalle a continuación con referencia a los dibujos que se acompañan.

La Figura 1 es un diagrama de flujo que ilustra un procedimiento para el procesamiento de una solicitud de servicio, de acuerdo con una implementación de la presente solicitud. El procedimiento para el procesamiento de una solicitud de servicio incluye las siguientes etapas:

S101. Recibir una solicitud de servicio correspondiente a un servicio de destino.

El procedimiento puede ser ejecutado por un nodo de consenso. En una red de cadena de bloques, cada nodo de consenso es un nodo de cadena de bloques responsable de la verificación de consenso. Para el servicio de destino, un nodo de cadena de bloques que participa en el servicio de destino es un nodo de servicio. El nodo de servicio puede servir como un nodo de consenso para participar en la verificación de consenso en el servicio de destino.

En conclusión, el procedimiento es ejecutado por al menos un nodo de consenso responsable de la verificación de consenso, y el nodo de consenso puede ser además un nodo de servicio que participa en el servicio de destino. Esto no está limitado en la presente solicitud.

El nodo de consenso puede recibir una solicitud de servicio de radiodifusión por un nodo de servicio determinado (que puede ser un nodo de servicio que inicia un servicio de destino), o puede recibir una petición de servicio de difusión adicional mediante otro nodo de consenso (que es un nodo de manipulación para una solicitud de servicio) después de recibir la solicitud de servicio.

Vale la pena hacer notar que los nodos de consenso que participan en la verificación de consenso pueden recibir la solicitud de servicio de diferentes maneras. Algunos nodos de consenso pueden servir como nodos de manipulación para recibir directamente la solicitud de servicio enviada por el nodo de servicio, y algunos nodos de consenso pueden recibir la solicitud de servicio transmitida por el nodo de manipulación. Alternativamente, cada nodo de consenso puede recibir directamente una solicitud de servicio transmitida por un nodo de servicio. Esto no está limitado en la presente solicitud.

En esta implementación de la presente solicitud, la solicitud de servicio incluye datos de servicio del servicio de destino y un resumen de los datos de servicio.

La solicitud de servicio correspondiente al servicio de destino es solicitar cada nodo de consenso para realizar la verificación de consenso sobre los datos de servicio del servicio de destino y el resumen de los datos de servicio, específicamente, para verificar si los datos de servicio fueron falsificados (si los datos de servicio son consistentes con el resumen) y si los datos de servicio que no fueron falsificados son auténticos y confiables (por ejemplo, si el saldo de una cuenta es suficiente para el pago, por ejemplo, si existen gastos duplicados).

En el campo de las tecnologías de cadena de bloques, un resumen es una cadena de caracteres generados sobre la base de datos de servicio, un resumen se puede utilizar como una "huella digital de datos" de los datos de servicio y los datos de servicio y del resumen de los datos de servicio son siempre estrictamente consistentes entre sí. En otras palabras, los datos de servicio de texto sin formato no se pueden inferir en función del resumen, un ligero cambio en los datos de servicio provoca un cambio correspondiente en el resumen generado en función de los datos de servicio. El resumen de los datos de servicio se puede generar en función de una función *hash* unidireccional (por ejemplo, MD5 o SHA-1), o se puede generar en función de otra función, siempre que los datos de servicio no se puedan inferir en función del resumen.

S102. Realizar una verificación de consenso en la solicitud de servicio.

S103. Almacenar un resumen en una cadena de bloques en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso.

En esta implementación de la presente solicitud, cada nodo de consenso realiza una verificación de consenso a la solicitud de servicio después de recibir la solicitud de servicio. En respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso (en otras palabras, los datos de servicio no son falsificados

y los datos de servicio son auténticos y confiables), cada nodo de consenso almacena el resumen incluido en la solicitud de servicio en la cadena de bloques, en lugar de almacenar los datos de servicio en la cadena de bloques.

En esta implementación de la presente solicitud, cada nodo de consenso almacena el resumen verificado de los datos de servicio en la cadena de bloques. En otras palabras, la cadena de bloques respalda que los datos de servicio de destino son auténticos y confiables. Los datos de servicio no se almacenan en la cadena de bloques para evitar que un nodo de la cadena de bloques irrelevante para el servicio de destino vea los datos de servicio.

Cuando la autenticidad de los datos de servicio declarada por un cierto nodo de servicio necesita ser verificada, un resumen se puede obtener de los datos de servicio declarado por el nodo de servicio y, a continuación, el resumen obtenido se compara con el resumen almacenado en la cadena de bloques. Si no es coherente, indica que los datos de servicio declarados por el nodo de servicio no son confiables. Dicho mecanismo se puede usar para evitar efectivamente un caso en el que un nodo de servicio niega el servicio de destino después de que el servicio de destino pasa la verificación de consenso realizada por cada nodo de consenso y es reconocido por la cadena de bloques.

En base al procedimiento para el procesamiento de una solicitud de servicio que se muestra en La Figura 1, en esta implementación de la presente solicitud, en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso, cada nodo de consenso almacena el resumen de los datos de servicio en la cadena de bloques, en lugar de almacenar los datos de servicio en la cadena de bloques. Como tal, el resumen de los datos de servicio se almacena en la cadena de bloques confiable, y la autenticidad de los datos de servicio aún se puede verificar. Además, los datos de servicio no se almacenan en la cadena de bloques, por lo que los datos de servicio no pueden ser obtenidos por un nodo de la cadena de bloques irrelevante para el servicio de destino. Por lo tanto, cada nodo de consenso ya no necesita consumir recursos informáticos para cifrar los datos de servicio, mejorando de esta forma la eficiencia de realizar la verificación de consenso en la solicitud de servicio por cada nodo de consenso.

Además, en esta implementación de la presente solicitud, a pesar de que los datos de servicio no se almacenan en la cadena de bloques, cada nodo de servicio puede almacenar los datos de servicio por sí mismo en su propia base de datos privada, ya que cada nodo de servicio se encuentra al tanto de los datos de servicio. Vale la pena hacer notar que cada nodo de cadena de bloques puede tener su propia base de datos privada, o los nodos de cadena de bloques pueden compartir una base de datos privada, pero cada nodo de cadena de bloques solo puede acceder a los datos relacionados. Como tal, los datos de servicio almacenados en la base de datos privada del nodo de servicio pueden ser preservados por el nodo de servicio. Además, los datos de servicio no se filtran a un nodo de cadena de bloques irrelevante para el servicio de destino (cada nodo de cadena de bloques está autorizado para acceder únicamente a los datos almacenados en la cadena de bloques, pero no puede acceder a una base de datos privada de otro nodo de cadena de bloques).

Por supuesto, los datos almacenados en la base de datos privada del nodo de cadena de bloques pueden no ser respaldados por cada nodo de consenso. Teóricamente, el nodo de cadena de bloques puede modificar los datos almacenados en la base de datos privada de sí mismo a voluntad. Sin embargo, la cadena de bloques almacena el resumen correspondiente al servicio de destino. En este caso, todas las partes que participan en el servicio de destino pueden reconocer los datos de servicio del servicio de destino propugnado por cualquier nodo de cadena de bloques (incluido el nodo de servicio) únicamente si los datos de servicio son consistentes con el resumen almacenado en la cadena de bloques.

En esta implementación de la presente solicitud, en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso, uno o más nodos de consenso puede ser responsable de enviar los datos de servicio al nodo de servicio para almacenar y ordenar al nodo de servicio que almacene los datos de servicio. El nodo de consenso, un ejecutor del presente procedimiento, puede realizar este trabajo en nombre de cada nodo de consenso.

Para ser específico, en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso, el nodo de consenso puede enviar los datos de servicio al menos a un nodo de servicio de modo que el nodo de servicio almacena los datos de servicio en la base de datos privada correspondiente al nodo de servicio.

O bien, el nodo de consenso puede enviar una instrucción de almacenamiento al menos a un nodo de servicio para que el nodo de servicio almacene los datos de servicio en la base de datos privada correspondiente al nodo de servicio.

O bien, el nodo de consenso puede enviar una instrucción de confirmación a un nodo de servicio que inicia el servicio de destino, por lo que el nodo de servicio almacena los datos de servicio en la base de datos privada correspondiente al nodo de servicio, y envía los datos de servicio a otro nodo de servicio para que el otro nodo

de servicio almacene los datos de servicio en una base de datos privada correspondiente al otro nodo de servicio.

Debido a que el nodo de servicio que inicia el servicio de destino puede transmitir los datos de servicio al otro nodo de servicio con antelación, el nodo de consenso a veces no tiene que enviar los datos de servicio al nodo de servicio, únicamente tiene que enviar una instrucción de almacenamiento de notificación o una instrucción de confirmación.

En conclusión, en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso, cada nodo de servicio puede aprender de esta información y optar por almacenar los datos de servicio por sí mismo. La presente solicitud no se limita a una implementación específica.

La Figura 2 es un diagrama de flujo que ilustra otro procedimiento para el procesamiento de una solicitud de servicio, de acuerdo con una implementación de la presente solicitud. El procedimiento para el procesamiento de una solicitud de servicio incluye las siguientes etapas:

S201. Un nodo de consenso recibe una solicitud de servicio correspondiente a un servicio de destino, en el que la solicitud de servicio incluye datos de servicio del servicio de destino y un resumen de los datos de servicio.

S202. Realizar una verificación de consenso en la solicitud de servicio basada en el servicio de datos y el resumen.

S203. Indicar a cada nodo sin consenso que almacene el resumen en una cadena de bloques en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso.

En esta implementación de la presente solicitud, el nodo de consenso puede ser únicamente responsable de la verificación de consenso, y no sirve como un nodo de servicio para participar en el servicio de destino. El nodo sin consenso no puede participar en la verificación de consenso, y puede servir solo como un nodo de servicio para participar en el servicio de destino.

En esta implementación de la presente solicitud, el nodo de consenso no puede mantener una cadena de bloques, y sólo es responsable de realizar la verificación de consenso a una solicitud de servicio. El nodo sin consenso mantiene una cadena de bloques y almacena, en la cadena de bloques, el resumen incluido en la solicitud de servicio que aprueba la verificación de consenso.

Para ser específicos, el nodo de consenso instruye a cada nodo sin consenso para que almacene el resumen en la cadena de bloques en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso.

Si cada nodo sin consenso ha recibido un resumen de difusión mediante un nodo sin consenso que inicia un servicio de destino antes de la verificación de consenso, el nodo sin consenso puede almacenar directamente el resumen en la cadena de bloques después de recibir una notificación del nodo de consenso.

Si el nodo sin consenso no obtiene el resumen antes de la verificación de consenso, el nodo de consenso puede enviar el resumen al nodo sin consenso después de que la solicitud de servicio pasa la verificación de consenso, de tal forma que el nodo sin consenso almacena el resumen en la cadena de bloques.

Además, el nodo de consenso puede enviar adicionalmente los datos de servicio al menos a un nodo de servicio de modo que el nodo de servicio almacena los datos de servicio en una base de datos privada correspondiente al nodo de servicio.

O, bien el nodo de consenso envía una instrucción de almacenamiento al menos a un nodo de servicio, de modo que el nodo de servicio almacena los datos de servicio en una base de datos privada correspondiente al nodo de servicio.

O bien, el nodo de consenso puede enviar una instrucción de confirmación a un nodo de servicio que inicia el servicio de destino para que el nodo de servicio almacene los datos de servicio en la base de datos privada correspondiente al nodo de servicio, y puede enviar los datos de servicio a otro nodo de servicio por lo que el otro nodo de servicio almacena los datos de servicio en una base de datos privada correspondiente al otro nodo de servicio.

Vale la pena hacer notar que el nodo de servicio es un nodo de cadena de bloques que participa en el servicio de destino.

La Figura 3 es un diagrama esquemático que ilustra un sistema de cadena de bloques, de acuerdo con una implementación de la presente solicitud. Como se muestra en la Figura 3, cada nodo de consenso (un nodo en blanco) es responsable de proporcionar un servicio de verificación de consenso para cada nodo sin consenso (un nodo sombreado). Cada nodo sin consenso mantiene una cadena de bloques y su propia base de datos privada.

Cada nodo de consenso proporciona un servicio de consenso en el siguiente procedimiento: realizar la verificación de consenso en los datos de servicio incluida en una petición de servicio recibida y un resumen de los datos de servicio; y almacenar el resumen en una cadena de bloques después de que la solicitud de servicio pasa la verificación para que el nodo de servicio almacene los datos de servicio (el nodo de servicio no puede almacenar los datos de servicio).

Como tal, una red de consenso confiable proporciona un respaldo para cada servicio de destino aprueba la verificación de consenso, y el servicio de destino correspondiente al resumen almacenado en la cadena de bloques es auténtico y confiable para cada nodo de cadena de bloques en toda la red de cadena de bloques. Si surgen disputas entre nodos de servicio que participan en un mismo servicio de destino, un resumen correspondiente al servicio de destino y almacenado en la cadena de bloques siempre puede evitar la negación de nodos de servicio maliciosos.

En base al procedimiento para el procesamiento de una solicitud de servicio que se muestra en La Figura 1, una implementación de la presente solicitud además proporciona un dispositivo correspondiente para el procesamiento de una solicitud de servicio. Como se muestra en la Figura 4, el dispositivo para el procesamiento de una solicitud de servicio incluye un módulo de recepción 401, un módulo de verificación de consenso 402 y un módulo de almacenamiento 403.

El módulo de recepción 401 está configurado para recibir una solicitud de servicio que corresponde a un servicio de destino. La solicitud de servicio incluye datos de servicio del servicio de destino y un resumen de los datos de servicio.

El módulo de verificación de consenso 402 está configurado para realizar una verificación de consenso a la solicitud de servicio en base a los datos de servicio y el resumen.

El módulo de almacenamiento 403 está configurado para almacenar el resumen en una cadena de bloques en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso.

El dispositivo además incluye un módulo de envío 404 configurado para: en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso, enviar los datos de servicio al menos a un nodo de servicio de modo que el nodo de servicio almacena los datos de servicio en una base de datos privada correspondiente al nodo de servicio; o enviar una instrucción de almacenamiento al menos a un nodo de servicio para que el nodo emisor almacene los datos de servicio en una base de datos privada correspondiente al nodo de servicio; o enviar una instrucción de confirmación a un nodo de servicio que inicia el servicio de destino para que el nodo de servicio almacene los datos de servicio en una base de datos privada correspondiente al nodo de servicio, y enviar los datos de servicio a otro nodo de servicio para que el otro nodo de servicio almacene los datos de servicio en una base de datos privada correspondiente al otro nodo de servicio.

El nodo de servicio es un nodo de cadena de bloques que participa en el servicio de destino.

En base al procedimiento para el procesamiento de una solicitud de servicio que se muestra en La Figura 2, una implementación de la presente solicitud además proporciona un dispositivo correspondiente para el procesamiento de una solicitud de servicio. Como se muestra en la Figura 5, el dispositivo para el procesamiento de una solicitud de servicio incluye un módulo de recepción 501, un módulo de consenso 502 y un módulo de almacenamiento 503.

El módulo de recepción 501 está configurada para recibir una solicitud de servicio que corresponde a un servicio de destino. La solicitud de servicio incluye datos de servicio del servicio de destino y un resumen de los datos de servicio.

El módulo de consenso 502 está configurado para realizar la verificación de consenso a la solicitud de servicio en base a los datos de servicio y el resumen.

El módulo de almacenamiento 503 está configurado para instruir a cada nodo sin consenso para almacenar el resumen en una cadena de bloques en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso.

El módulo de almacenamiento 503 está configurado para enviar el resumen a cada nodo sin consenso de manera que cada nodo sin consenso almacena el resumen en la cadena de bloques.

El dispositivo además incluye un módulo de envío 504 configurado para enviar los datos de servicio al menos a un nodo de servicio de modo que el nodo de servicio almacena los datos de servicio en una base de datos privada correspondiente al nodo de servicio; o enviar una instrucción de almacenamiento al menos a un nodo de servicio para que el nodo de servicio almacene los datos de servicio en una base de datos privada correspondiente al nodo de servicio; o enviar una instrucción de confirmación a un nodo de servicio que inicia el servicio de destino para que el nodo de servicio almacene los datos de servicio en una base de datos privada correspondiente al nodo de servicio, y enviar los datos de servicio a otro nodo de servicio para que el otro nodo de servicio almacene los datos de servicio en una base de datos privada correspondiente al otro nodo de servicio.

El nodo de servicio es un nodo de cadena de bloques que participa en el servicio de destino.

En la década de 1990, ya sea una mejora técnica sea una mejora de hardware (por ejemplo, una mejora de una estructura de circuito, tal como un diodo, un transistor, o un conmutador) o una mejora del software (una mejora a un procedimiento) se puede distinguir claramente. Sin embargo, a medida que se desarrollan las tecnologías, las mejoras actuales de muchos procedimientos podrían considerarse como mejoras directas a las estructuras de circuitos de hardware. Un diseñador generalmente programa un procedimiento mejorado en un circuito de hardware, para obtener una estructura de circuito de hardware correspondiente. Por lo tanto, un procedimiento puede mejorarse utilizando un módulo de entidad de hardware. Por ejemplo, un dispositivo lógico programable (PLD) (por ejemplo, un arreglo de compuertas programables en campo (FPGA)) es un circuito integrado y el usuario determina la función lógica del PLD a través de la programación del dispositivo. El diseñador realiza la programación para "integrar" un sistema digital a un PLD sin solicitar a un fabricante de chips que diseñe y produzca un chip de circuito integrado de aplicación específica. Además, en la actualidad, en lugar de fabricar manualmente un chip de circuito integrado, este tipo de programación se implementa principalmente mediante el uso de software de "compilador lógico". La programación es similar a un compilador de software utilizado para desarrollar y escribir un programa. El código original debe ser escrito en un lenguaje de programación particular para la compilación. El lenguaje se conoce como lenguaje de descripción de hardware (HDL). Hay muchos tipos de HDL, como el lenguaje de expresión booleana avanzada (ABEL), el lenguaje de descripción de hardware Altera (AHDL), Confluence, el lenguaje de programación de la Universidad de Cornell (CUPL), HDCal, el lenguaje de descripción de hardware Java (JHDL), Lava, Lola, MyHDL, PALASM y Lenguaje de descripción de hardware Ruby (RHDL). El lenguaje de descripción de hardware de circuito integrado de muy alta velocidad (VHDL) y Verilog se usan más comúnmente en la actualidad. Una persona experta en la técnica también debe comprender que un circuito de hardware que implementa un procedimiento lógico puede obtenerse fácilmente una vez que el procedimiento se programa lógicamente utilizando los diversos lenguajes de descripción de hardware descritos y se programa en un circuito integrado.

Un controlador puede implementarse usando cualquier procedimiento apropiado. Por ejemplo, el controlador puede ser un microprocesador o un procesador, o un medio legible por ordenador que almacena código de programa legible por ordenador (como software o firmware) que puede ser ejecutado por el microprocesador o el procesador, una puerta lógica, un interruptor, un circuito integrado de aplicación específica (ASIC), un controlador lógico programable o un microprocesador incorporado. Los ejemplos del controlador incluyen, entre otros, los siguientes microprocesadores: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20 y Silicone Labs C8051F320. El controlador de memoria también se puede implementar como parte de la lógica de control de la memoria. Una persona experta en la técnica también sabe que, además de implementar el controlador mediante el uso del código de programa legible por ordenador, la programación lógica se puede realizar en las etapas del procedimiento para permitir que el controlador implemente la misma función en formas de la puerta lógica, el interruptor, el circuito integrado aplicación específica, el controlador lógico programable, el microcontrolador incorporado, etc. Por lo tanto, el controlador puede ser considerado como un componente de hardware, y un dispositivo configurado para implementar diversas funciones en el controlador también puede ser considerado como una estructura en el componente de hardware. O el dispositivo configurado para implementar diversas funciones puede incluso ser considerado como un módulo de software que implementa el procedimiento y una estructura en el componente de hardware.

El sistema, dispositivo, módulo o unidad ilustrada en las implementaciones anteriores pueden implementarse mediante el uso de un chip de ordenador o una entidad, o puede ser implementado mediante el uso de un producto que tiene una cierta función. Un dispositivo de implementación típico es un ordenador. El ordenador puede ser, por ejemplo, un ordenador personal, un ordenador portátil, un teléfono celular, un teléfono con cámara, un teléfono inteligente, un asistente digital personal, un reproductor multimedia, un dispositivo de navegación, un dispositivo de correo electrónico, una consola de juegos, una tableta, un dispositivo usable, o una combinación de cualquiera de estos dispositivos.

Para facilitar la descripción, el dispositivo anterior se describe dividiendo funciones en varias unidades. Ciertamente, cuando se implementa la presente solicitud, se puede implementar una función de cada unidad en una o más piezas de software y/o hardware.

Un experto en la técnica entenderá que una implementación de la presente invención se puede proporcionar como un procedimiento, un sistema, o un producto de programa de ordenador. Por lo tanto, la presente invención puede usar una forma de implementaciones que utilizan únicamente hardware, implementaciones que utilizan únicamente software o implementaciones con una combinación de software y hardware. Además, la presente invención puede usar una forma de un producto de programa informático que se implementa en uno o más medios de almacenamiento utilizables por ordenador (que incluyen, entre otros, una memoria de disco, un CD-ROM, una memoria óptica, etc.) que incluyen código de programa utilizable por ordenador.

La presente invención se describe con referencia a los diagramas de flujo y/o diagramas de bloques del procedimiento, el dispositivo (sistema), y el producto de programa de ordenador basado en las implementaciones de la presente invención. Vale la pena hacer notar que las instrucciones del programa de ordenador se pueden usar para implementar cada procedimiento y/o cada bloque en los diagramas de flujo y/o los diagramas de bloque y una combinación de un procedimiento y/o un bloque en los diagramas de flujo y/o los diagramas de bloque. Estas instrucciones de programa de ordenador se pueden proporcionar para un ordenador de propósito general, un ordenador dedicado, un procesador incorporado o un procesador de otro dispositivo de procesamiento de datos programable para generar una máquina de modo que las instrucciones ejecutadas por el ordenador o el procesador del otro dispositivo programable de procesamiento de datos genera un dispositivo para implementar una función específica en uno o más procedimientos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones de programa de ordenador se pueden almacenar en un equipo de memoria legible que puede dar instrucciones al ordenador o al dispositivo de procesamiento otros datos programables para el trabajo de una manera específica de manera que las instrucciones almacenadas en la memoria legible por ordenador generen un artefacto que incluye un dispositivo de instrucción. El dispositivo de instrucción implementa una función específica en uno o más procedimientos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones de programa informático pueden cargarse en el ordenador o en otro dispositivo de procesamiento de datos programables de manera que una serie de operaciones y operaciones y etapas se llevan a cabo en el ordenador o el otro dispositivo programable, generando de ese modo el procesamiento implementado por ordenador. Por lo tanto, las instrucciones ejecutadas en el ordenador u otro dispositivo programable proporcionan etapas para implementar una función específica en uno o más procedimientos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

En una configuración típica, un dispositivo informático incluye uno o más procesadores (CPU), una o más interfaces de entrada/salida, una o más interfaces de red, y una o más memorias.

La memoria puede incluir una memoria no persistente, una memoria de acceso aleatorio (RAM), una memoria no volátil, y/u otra forma que se consiste en un medio legible por ordenador, por ejemplo, una memoria de sólo lectura (ROM) o una memoria flash (flash RAM). La memoria es un ejemplo del medio legible por ordenador.

El medio legible por ordenador incluye medios persistentes, no persistentes, móviles, e inamovibles que puede almacenar información mediante el uso de cualquier procedimiento o tecnología. La información puede ser una instrucción legible por ordenador, una estructura de datos, un módulo de programa u otros datos. Los ejemplos de un medio de almacenamiento de ordenador incluyen, entre otros: una memoria de acceso aleatorio de parámetros (PRAM), una memoria de acceso aleatorio estática (SRAM), una memoria de acceso aleatorio dinámica (DRAM) u otro tipo de memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una memoria de solo lectura programable y borrable eléctricamente (EEPROM), una memoria flash u otra tecnología de memoria, una memoria de solo lectura de disco compacto (CD-ROM), un disco versátil digital (DVD) u otro almacenamiento óptico, un casete magnético, una cinta magnética, una cinta magnética/memoria de disco magnético u otro dispositivo de almacenamiento magnético, o cualquier otro medio sin transmisión que pueda usarse para almacenar información a la que puede acceder un dispositivo informático. En base a la definición de la presente especificación, el medio legible por ordenador no incluye medios transitorios legibles por ordenador (medios transitorios) tales como una señal de datos modulada y una portadora.

Vale la pena hacer notar además que, los términos "incluye", "comprende", o sus otras variantes están destinados a cubrir una inclusión no exclusiva, de modo que un procedimiento, un procedimiento, un producto o un dispositivo que incluye una lista de elementos que no solo incluye esos elementos, sino que también incluye otros elementos que no están expresamente listados, o incluye elementos inherentes a dicho procedimiento, producto o dispositivo. Sin más restricciones, un elemento precedido por "que incluye un..." no excluye la existencia de elementos idénticos adicionales en el procedimiento, producto o dispositivo que incluye el elemento.

El alcance de la protección está definido por las reivindicaciones.

REIVINDICACIONES

1. Un procedimiento para el procesamiento de una solicitud de servicio, comprendiendo el procedimiento:

recibir (S201), mediante un nodo de consenso, una solicitud de servicio correspondiente a un servicio de destino, en el que la solicitud de servicio comprende datos de servicio del servicio de destino y un resumen de los datos de servicio, en el que el resumen de los datos de servicio comprende una cadena de caracteres generada en base a los datos de servicio, y en el que la solicitud de servicio se recibe desde un nodo sin consenso que inicia el servicio de destino;
realizar (S202), mediante el nodo de consenso, una verificación de consenso a la solicitud de servicio en base a los datos de servicio y el resumen para determinar una autenticidad de los datos de servicio, en el que realizar la verificación de consenso verifica si los datos de servicio son consistentes con el resumen;
ordenar (S203), mediante el nodo de consenso, a cada nodo sin consenso para almacenar el resumen en una cadena de bloques, en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso; y
adicionalmente, en respuesta a la determinación de que la solicitud de servicio pasa la verificación de consenso:

enviar, mediante el nodo de consenso, los datos de servicio al menos a un nodo de servicio para que el nodo de servicio almacene los datos de servicio en una base de datos privada correspondiente al nodo de servicio; o
enviar, mediante el nodo de consenso, una instrucción de almacenamiento al menos a un nodo de servicio para que el nodo de servicio almacene los datos de servicio en una base de datos privada correspondiente al nodo de servicio; o
enviar, mediante el nodo de consenso, una instrucción de confirmación a un nodo de servicio que inicia el servicio de destino para que el nodo de servicio almacene los datos de servicio en una base de datos privada correspondiente al nodo de servicio, y enviar los datos de servicio a otro nodo de servicio para que el otro nodo de servicio almacene los datos de servicio en una base de datos privada correspondiente al otro nodo de servicio, en el que el nodo de servicio es un nodo de cadena de bloques que participa en el servicio de destino;

en el que:

el nodo de consenso únicamente es responsable de realizar la verificación de consenso en las solicitudes de servicio y no sirve como un nodo de servicio para participar en el servicio de destino y no mantiene una cadena de bloques; y
un nodo sin consenso no participa en la verificación de consenso, únicamente puede servir como un nodo de servicio para participar en el servicio de destino y mantiene la cadena de bloques.

2. El procedimiento de acuerdo con la reivindicación 1, en el que ordenar (S203) a cada nodo sin consenso que almacene el resumen en la cadena de bloques comprende:

enviar el resumen a cada nodo sin consenso para que cada nodo sin consenso almacene el resumen en la cadena de bloques.

3. El procedimiento de acuerdo con la reivindicación 1, en el que el resumen de los datos de servicio se genera en base a una función *hash* unidireccional.

4. El procedimiento de acuerdo con la reivindicación 1, en el que realizar (S202) la verificación de consenso comprende:

verificar si los datos de servicio que no son falsificados son auténticos y confiables.

5. Un dispositivo para el procesamiento de una solicitud de servicio, comprendiendo el dispositivo una pluralidad de módulos (401, 402, 403; 501, 502, 503) configurados para realizar el procedimiento de una cualquiera de las reivindicaciones 1 a 4.

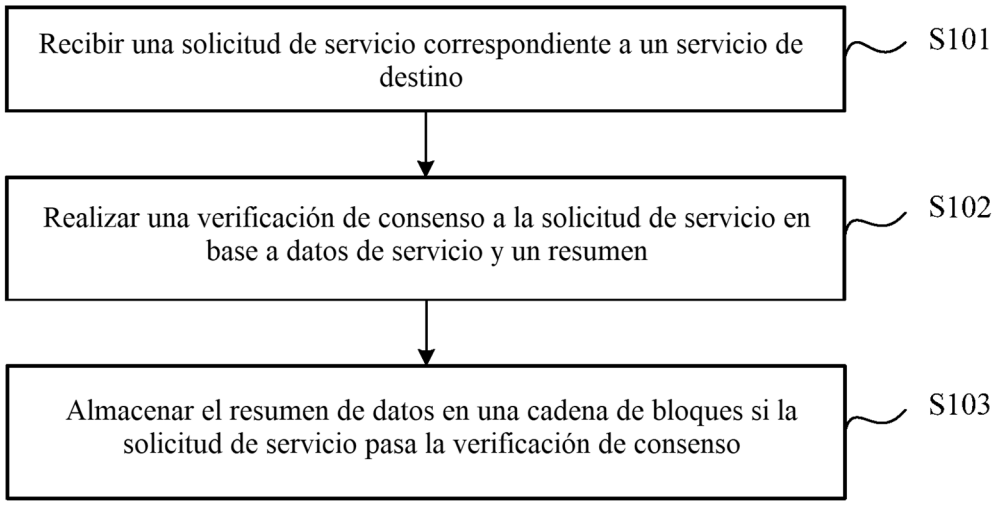
Recibir una solicitud de servicio correspondiente a un servicio de destino
S101
Realizar una verificación de consenso a la solicitud de servicio en base a datos de servicio y un resumen
S102
Almacenar el resumen de datos en una cadena de bloques si la solicitud de servicio pasa la verificación de consenso
S103

FIG. 1

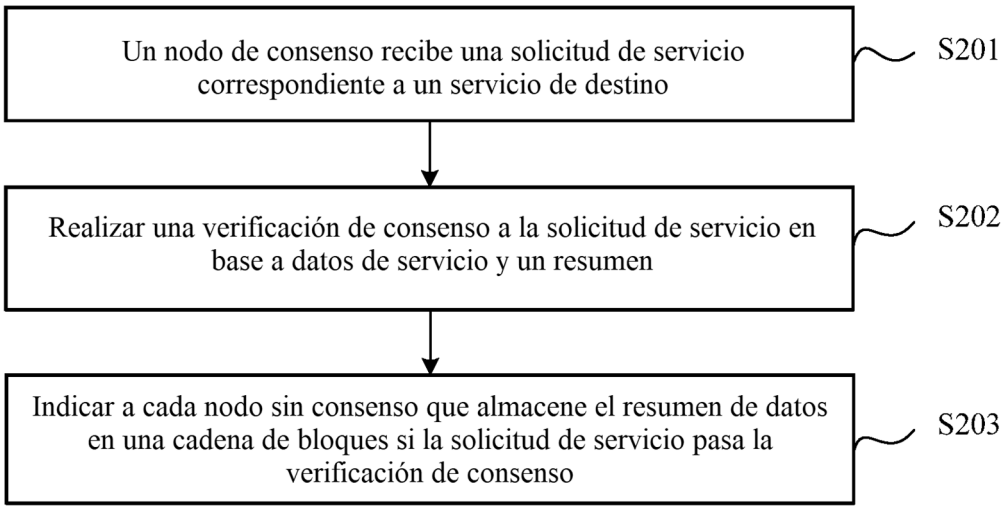
Un nodo de consenso recibe una solicitud de servicio correspondiente a un servicio de destino
S201
Realizar una verificación de consenso a la solicitud de servicio en base a datos de servicio y un resumen
S202
Indicar a cada nodo sin consenso que almacene el resumen de datos en una cadena de bloques si la solicitud de servicio pasa la verificación de consenso
S203

FIG. 2

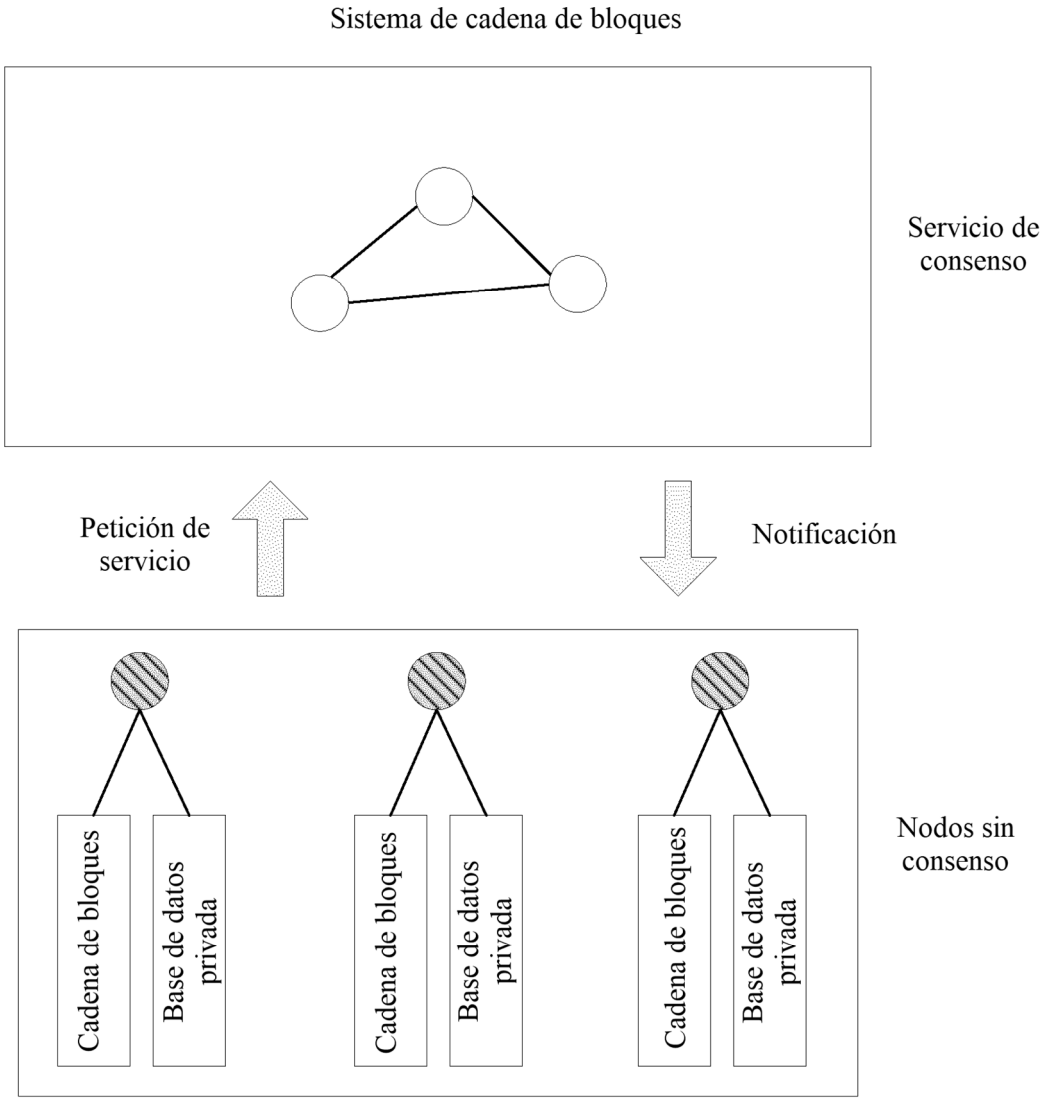
Sistema de cadena de bloques
Servicio de consenso
Petición de servicio
Notificación
Cadena de bloques
Base de datos privada
Cadena de bloques
Base de datos privada
Cadena de bloques
Base de datos privada
Nodos sin consenso

FIG. 3

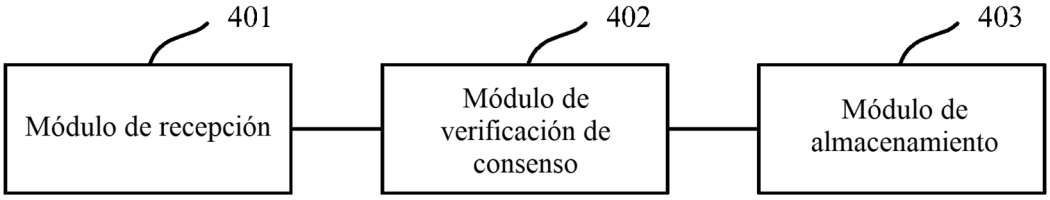
401
402
403
Módulo de recepción
Módulo de verificación de consenso
Módulo de almacenamiento

FIG. 4

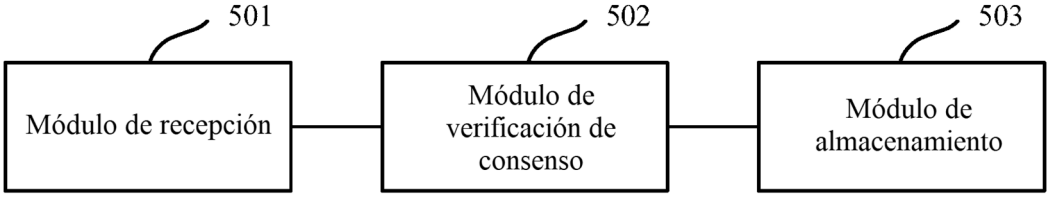
501
502
503
Módulo de recepción
Módulo de verificación de consenso
Módulo de almacenamiento

FIG. 5