(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 809 202**

(51) Int. CI.:

G06Q 20/02	(2012.01)	***H04L 9/32***	(2006.01)
G06Q 20/04	(2012.01)		
G06Q 20/06	(2012.01)		
G06Q 20/36	(2012.01)		
G06Q 20/38	(2012.01)		
H04L 9/14	(2006.01)		
G06F 21/64	(2013.01)		
H04L 9/08	(2006.01)		
H04L 29/06	(2006.01)		
H04W 12/04	(2009.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.02.2018 PCT/US2018/019464**

(87) Fecha y número de publicación internacional: **30.08.2018 WO18156924**

(96) Fecha de presentación y número de la solicitud europea: **23.02.2018 E 18710609 (1)**

(97) Fecha y número de publicación de la concesión europea: **27.05.2020 EP 3555796**

(54) Título: **Método y aparato de establecimiento de clave y de envío de datos**

(30) Prioridad:

24.02.2017 CN 201710102824

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.03.2021

(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:

LI, YI

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y aparato de establecimiento de clave y de envío de datos

Reivindicación de prioridad

Esta solicitud reivindica prioridad a la Solicitud de Patente China No. 201710102824.3 presentada el 24 de febrero de 2017, cuyo contenido completo se incorpora aquí como referencia.

Campo técnico

La presente solicitud se refiere al campo de las tecnologías informáticas y, en particular, a un método y aparato de envío de datos.

Técnica anterior

Con el desarrollo de la tecnología de la información, la tecnología de la información ha aportado una gran comodidad al trabajo y la vida de las personas. En el campo de la tecnología de la información, la información se almacena y se transmite utilizando datos como un portador, y los datos se pueden almacenar como un número binario en un medio de almacenamiento de un dispositivo informático. Los datos mencionados aquí pueden ser texto, símbolo, vídeo o audio, y todos los demás elementos que pueden identificarse por el dispositivo informático.

Los datos, como portadores de información, generalmente tienen cierto valor. Especialmente en la era de los macrodatos, cada una de las unidades tiende a acumular una gran cantidad de datos en su proceso de operación o servicio, y los datos pueden tener cierto valor de uso para llevar a cabo algunos negocios. Para hacer un uso completo del valor de los datos, dos partes que poseen datos pueden intercambiar datos entre sí para tomar los datos requeridos por ellos mismos.

Para que sea conveniente para ambas partes del intercambio de datos encontrar un objeto de intercambio de datos apropiado, se creó una plataforma de intercambio de datos. La plataforma de intercambio de datos puede mostrar información de intercambio de datos emitida por un titular de datos, de modo que un solicitante de datos pueda encontrar fácilmente la información. Al mismo tiempo, en un proceso de intercambio de datos, la plataforma de intercambio de datos, como intermediario, puede recibir datos de un titular de datos y luego enviarlos a un solicitante de datos. De esta manera, es posible que la plataforma de intercambio de datos utilice los datos intercambiados entre ambas partes para otros fines, o cambie los datos sin autorización antes de enviarlos a un receptor, causando daños a los intereses de las partes del intercambio de datos. Es decir, en un proceso de intercambio de datos existente, la seguridad de los datos es relativamente baja. El documento XP055467436 de técnica anterior ha dado a conocer diferentes técnicas de gestión de claves que utilizan centros de distribución de claves y traducción de claves. En el documento WO2017027438, se ha dado a conocer el sistema y método para lograr la autorización en comunicaciones grupales confidenciales en términos de una lista ordenada de bloques de datos que representan una cuenta cronológica resistente a la manipulación de las actualizaciones de miembros del grupo, en donde las cadenas de bloques se utilizan contra la manipulación.

Resumen de la invención

Las realizaciones de la presente solicitud proporcionan un método de envío de datos para resolver el problema de baja seguridad de datos en el proceso de intercambio de datos existente.

La invención está definida por las reivindicaciones 1 y 15 independientes. Otras realizaciones están definidas por las reivindicaciones dependientes.

Las realizaciones de la presente solicitud proporcionan además un método de envío de datos para resolver el problema de baja seguridad de datos en el proceso de intercambio de datos existente.

Las realizaciones de la presente solicitud proporcionan además un aparato de envío de datos para resolver el problema de baja seguridad de datos en el proceso de intercambio de datos existente.

Al menos una de las soluciones técnicas anteriores adoptadas por las realizaciones de la presente solicitud puede lograr los siguientes efectos beneficiosos:
Durante el intercambio de datos, una plataforma de intercambio de datos escribe un acuerdo de intercambio de datos alcanzado entre un primer usuario y un segundo usuario que intercambian datos en una cadena de bloques. La plataforma de intercambio de datos luego recibe una primera clave, enviada por un primer terminal correspondiente al primer usuario, para descifrar los primeros datos cifrados. El primer terminal envía los primeros datos cifrados a un segundo terminal correspondiente al segundo usuario. La plataforma de intercambio de datos envía la primera clave al segundo terminal, y el segundo terminal descifra los primeros datos cifrados recibidos en base a la primera clave, con el fin de obtener los primeros datos. Es evidente que la plataforma de intercambio de datos se mantiene libre de

los primeros datos intercambiados en el proceso de intercambio de datos, evitando así el riesgo de que los primeros datos puedan utilizarse por la plataforma de intercambio de datos para otros fines, mejorando la seguridad de los datos en el proceso de intercambio de datos, y en paralelo la plataforma de intercambio de datos.

Breve descripción de los dibujos

Los dibujos adjuntos descritos en el presente documento se utilizan para proporcionar una comprensión adicional de la presente solicitud y construir una parte de la presente solicitud. Las realizaciones ejemplares de la presente solicitud y las ilustraciones de la misma se utilizan para explicar la presente solicitud, y no constituyen una limitación inadecuada de la presente solicitud. En los dibujos:

la FIG. 1 es un diagrama de flujo esquemático de la implementación de un método de envío de datos de acuerdo con una realización de la presente solicitud;

la FIG. 2 es un diagrama esquemático de un escenario de implementación de un método de envío de datos de acuerdo con una realización de la presente solicitud;

la FIG. 3 es un diagrama de flujo esquemático de implementación de un método de transacción de datos de acuerdo con una realización de la presente solicitud; y

la FIG. 4 es un diagrama estructural esquemático específico de un aparato de envío de datos de acuerdo con una realización de la presente solicitud.

La FIG. 5 es un diagrama de flujo que ilustra otro ejemplo de un método implementado por computadora para transacciones de datos seguras, de acuerdo con una realización de la presente solicitud.

Descripción detallada

Para hacer que los objetivos, las soluciones técnicas y las ventajas de la presente solicitud sean más comprensibles, las soluciones técnicas de la presente solicitud se describen clara y completamente a través de realizaciones específicas de la presente solicitud y los correspondientes dibujos adjuntos. Aparentemente, las realizaciones descritas son meramente algunas realizaciones en lugar de todas las realizaciones de la presente solicitud. En base a las realizaciones de la presente solicitud, todas las demás realizaciones derivadas sin esfuerzo creativo algunos por expertos en la técnica caerán dentro del alcance de protección de la presente solicitud.

Como se describe en la Técnica anterior, los datos, como portadores de información, generalmente tienen cierto valor. Especialmente, en la era de los macrodatos, los macrodatos son de gran valor para que el gobierno y las empresas lleven a cabo diversos tipos de trabajo. La información extraída de los macrodatos puede ayudar al gobierno y a las empresas a tomar mejores decisiones. Por ejemplo, los grandes sitios de redes sociales generalmente acumulan una gran cantidad de datos de usuarios, que no solo registran la información de identidad personal de los usuarios, sino que también reflejan, en cierta medida, sus pasatiempos personales, hábitos de vida, relaciones personales y otra información. La información contenida en los datos tiene un gran valor de uso para llevar a cabo negocios posteriores, y su valor de uso, por ejemplo, puede ayudar a las empresas de marketing para enviar con precisión anuncios a los usuarios.

Para aprovechar al máximo el valor de los datos, los titulares de datos pueden intercambiar datos entre ellos para extraer información valiosa de los datos intercambiados, promoviendo así el desarrollo de sus propios negocios. Por lo tanto, para que sea conveniente para los solicitantes de datos buscar datos útiles para ellos, ambas partes del intercambio de datos pueden intercambiar datos a través de una plataforma de intercambio de datos.

Sin embargo, debido a que los datos son reproducibles, la propiedad de los datos no es tan clara como la de un objeto real. Cuando un objeto real se transfiere de la parte A a la parte B, la parte A pierde la propiedad del objeto real. Sin embargo, cuando los datos se transfieren de una parte a otra, si los datos pasan a través de un tercero en este proceso, el tercero puede copiar los datos y, por lo tanto, ser propietario de los datos. Esto puede dañar los intereses de ambas partes del intercambio de datos.

La plataforma de intercambio de datos puede desempeñar no solo un papel de emparejar los datos de intercambio entre ambas partes, sino también un rol de garante, es decir, garantizar los intereses de ambas partes en el proceso de intercambio de datos. En el proceso de intercambio de datos existente, para evitar la situación de que, después de que una parte del intercambio de datos envíe datos, la otra parte no envíe sus propios datos, la plataforma de intercambio de datos puede adquirir primero los datos de ambas partes del intercambio de datos, y luego enviar los datos por separado a ambas partes del intercambio de datos, evitando así que cualquiera de las partes incumpla una promesa. De esta manera, la plataforma de intercambio de datos puede tener una posibilidad de utilizar datos para otros fines. Esto conducirá a una baja seguridad de datos durante el intercambio. Para resolver este problema, la presente solicitud proporciona un método de envío de datos. El método de envío de datos proporcionado en la presente solicitud puede ejecutarse por una plataforma de intercambio de datos, y la plataforma de intercambio de datos puede ser software, hardware o una combinación de software y hardware para implementar este método.

En lo sucesivo, la solución técnica proporcionada en cada una de las realizaciones de la presente solicitud se describe en detalle con referencia a los dibujos adjuntos.

Realización 1

Para resolver el problema de la baja seguridad de datos en el proceso de intercambio de datos existente, la Realización 1 de la presente solicitud proporciona un método de envío de datos. En esta realización de la presente solicitud, para facilitar la descripción, ambas partes del intercambio de datos se denominan primer usuario y segundo usuario. El primer usuario y el segundo usuario pueden ser cualquier organización o individuo. El primer usuario y el segundo usuario en el presente documento se utilizan para distinguir a ambas partes de la transacción de datos, y no debe entenderse como una limitación para ambas partes de la transacción de datos en la presente solicitud.

Ambas partes del intercambio de datos, durante el intercambio de datos, pueden ejecutar algunas operaciones utilizando dispositivos terminales. Para facilitar la descripción, un terminal correspondiente a una operación ejecutada por el primer usuario se denomina primer terminal, y un terminal correspondiente a una operación ejecutada por el segundo usuario se denomina segundo terminal. Cabe señalar que, en todo el proceso de intercambio de datos, el mismo usuario puede utilizar el mismo terminal, y también puede utilizar terminales diferentes. Es decir, el primer terminal mencionado en cada uno de los procesos en la realización de la presente solicitud puede ser terminales diferentes, y el segundo terminal también puede ser terminales diferentes. El terminal aquí, por ejemplo, puede ser una computadora personal, un servidor, un terminal móvil u otros dispositivos informáticos, lo cual no está limitado en la presente solicitud.

Durante el intercambio de datos, ambas partes del intercambio de datos a menudo logran un acuerdo de intercambio de datos antes de intercambiar datos. El acuerdo de intercambio de datos aquí se refiere a un acuerdo sobre los detalles del intercambio de datos logrado por ambas partes del intercambio de datos antes de intercambiarse los datos. El acuerdo de intercambio de datos incluye disposiciones estipuladas por ambas partes del intercambio de datos para determinar sus respectivos derechos y obligaciones, y ambas partes acatan las disposiciones.

Cuando se alcanza el acuerdo de intercambio de datos, el primer usuario puede emitir información de datos en la plataforma de intercambio de datos a través del primer terminal. Después de recibir la información de datos emitida por el primer terminal, la plataforma de intercambio de datos puede publicar la información de datos. Por lo tanto, el segundo usuario que está interesado en la información de datos, después de ver la información de datos, puede enviar una solicitud de pedido para la información de datos a la plataforma de intercambio de datos a través del segundo terminal. La plataforma de intercambio de datos recibe la solicitud de pedido del segundo terminal para la información de datos publicada, y envía la solicitud al primer terminal. Después de que el primer terminal hace una confirmación, la plataforma de intercambio de datos puede recibir información de confirmación enviada por el primer terminal para la solicitud de pedido, logrando así el acuerdo de intercambio de datos.

Lo anterior describe brevemente un proceso para lograr el acuerdo. En aplicaciones reales, ambas partes del intercambio de datos pueden decidir los detalles del acuerdo a través de negociaciones repetidas. El acuerdo de intercambio de datos puede incluir específicamente información de identidad de ambas partes del intercambio de datos, información característica de los datos intercambiados, especificaciones de uso de datos y medidas punitivas en incumplimiento del acuerdo que cumplen ambas partes, y otra información. De esta manera, después de recibir los datos, el receptor puede tomar las correspondientes medidas sobre la base del acuerdo si encuentra que los datos no se ajustan a la descripción del acuerdo.

En el acuerdo, la información característica de los datos intercambiados entre ambas partes puede incluir al menos uno de los siguientes: un resumen del mensaje para verificar la integridad de los datos e información de referencia para resumir el contenido específico de los datos. Para los primeros datos, la información característica de los primeros datos incluye al menos uno de los siguientes: un resumen del mensaje para verificar la integridad de los primeros datos e información de referencia para resumir el contenido específico de los primeros datos.

El resumen del mensaje es un valor de longitud fija que corresponde de forma única a un mensaje o documento, el valor se determina en base a un algoritmo hash unidireccional. Por lo tanto, cuando se modifican los datos que se intercambiarán, el resumen del mensaje de los datos también se puede cambiar. Los algoritmos hash unidireccionales de uso común incluyen: un Algoritmo de resumen de mensaje 5 (MD5), un Algoritmo de hash seguro (SHA), un Código de autenticación de mensaje (MAC), etc.

En base al resumen del mensaje de los primeros datos contenidos en el acuerdo, después de recibir los datos cifrados, el segundo usuario puede llevar a cabo una verificación de integridad de los datos cifrados para juzgar si los datos recibidos han sido modificados. Mientras tanto, un valor de verificación de integridad también puede convertirse en una base para el uso en futuras disputas entre ambas partes del intercambio de datos.

La información de referencia para resumir el contenido específico de los primeros datos puede ser, por ejemplo, el tipo de datos que deben incluirse en los primeros datos, o algunas condiciones específicas que deben cumplir los datos en los primeros datos, o efectos que pueden lograrse por los datos en los primeros datos en la presente solicitud, etc. En base a la información, el segundo terminal puede verificar el contenido específico de los primeros datos, evitando así que el segundo usuario sea engañado y evitando pérdidas para sus propios intereses.

Lo anterior describe un proceso para lograr un acuerdo de intercambio de datos por ambas partes antes del envío de datos. A continuación, se introducirá en detalle un proceso de envío de datos por ambas partes del intercambio de datos en la presente solicitud, es decir, un método de envío de datos proporcionado en la presente solicitud. En la FIG. 1 se muestra un diagrama de flujo esquemático para implementar el método. El método incluye los siguientes pasos:

Paso 101: Una plataforma de intercambio de datos escribe un acuerdo de intercambio de datos logrado entre un primer usuario y un segundo usuario en una cadena de bloques y almacena el acuerdo.

En la era de la tecnología de la información, un acuerdo también puede almacenarse en un medio de almacenamiento de un dispositivo informático en forma de datos, y los datos almacenados en el medio de almacenamiento pueden tener el riesgo de ser modificados. Para evitar que ambas partes del intercambio de datos modifiquen el acuerdo sin autorización y mejorar la seguridad de los datos del acuerdo, la plataforma de intercambio de datos se puede utilizar como un tercero para guardar el acuerdo.

Sin embargo, si la plataforma de intercambio de datos almacena el acuerdo, habrá un riesgo de que la plataforma de intercambio de datos pueda modificar el acuerdo. Si la plataforma de intercambio de datos confabula con una de las partes del intercambio de datos para modificar el acuerdo, los intereses de la otra parte se dañarán. Para mejorar aún más la seguridad de los datos del acuerdo y mejorar la credibilidad de la plataforma de intercambio de datos, durante el almacenamiento del acuerdo, se puede utilizar una tecnología de cadena de bloques para almacenar el acuerdo de intercambio de datos alcanzado entre el primer usuario y el segundo usuario.

La tecnología de cadena de bloques es una tecnología de almacenamiento de datos distribuida descentralizada, confiable y a prueba de manipulaciones. Una estructura de datos almacenada utilizando la tecnología de cadena de bloques es una estructura de datos encadenada. Los datos en la estructura de datos encadenada solo se pueden cambiar de forma incremental. Los datos ya registrados mantendrán el estado inicial y no serán cubiertos.

Mientras tanto, la cadena de bloques sigue un mecanismo de consenso al registrar datos. Cuando un nodo registra datos, los datos registrados pueden registrarse en cada uno de los nodos de la cadena de bloques solo después de obtener el consenso de la mayoría de los nodos en la cadena de bloques. Esto reduce en gran medida la posibilidad de que los datos almacenados sean datos ilegales, lo que reduce en gran medida la posibilidad de que el acuerdo sea manipulado.

El mecanismo de consenso utilizado en la tecnología de cadena de bloques puede ser, por ejemplo, un mecanismo de prueba de trabajo, un mecanismo de prueba de participación, un mecanismo de prueba de participación delegada, un mecanismo de grupo de verificación, etc. Si se pretende cambiar los datos existentes en la cadena de bloques, la única opción es reemplazar los datos originales forjando una cadena lateral. Los costos de manipulación son enormes en términos de dificultad técnica, consumo de tiempo y mano de obra. Es casi imposible lograr esto bajo el mecanismo de consenso de la cadena de bloques.

A través del análisis anterior, se puede concluir que la realización de la presente solicitud almacena un acuerdo de intercambio de datos por medio de una tecnología de cadena de bloques, que puede evitar efectivamente la posibilidad de que el acuerdo se altere, y mejorar en gran medida la seguridad del acuerdo de intercambio de datos.

Paso 102: La plataforma de intercambio de datos recibe una primera clave enviada por un primer terminal y utilizada para descifrar los primeros datos cifrados.

Los primeros datos mencionados aquí son datos que el primer usuario espera enviar al segundo usuario. Por lo tanto, el primer usuario aquí es un emisor de los primeros datos, y el segundo usuario es un receptor de los primeros datos. Por supuesto, en el campo de la informática, los expertos en la técnica deben tener claro que el llamado envío de datos entre usuarios, en operaciones reales, puede ser un usuario que envía datos a un terminal de otro usuario a través de un terminal del mismo.

Para evitar que una tercera parte distinta de ambas partes del intercambio robe los datos, los primeros datos pueden cifrarse y luego enviarse al segundo terminal. En criptografía, el cifrado se utiliza para ocultar información de texto plano, de modo que la información no sea legible en ausencia de una clave de descifrado, mejorando así la seguridad en la transmisión de datos.

Los datos se transmiten a través de la plataforma de interacción de datos después de cifrarse, pero esto aún no puede evitar por completo que los primeros datos cifrados se utilicen por la plataforma de intercambio de datos. Por ejemplo, la plataforma de intercambio de datos puede descifrar los datos. Los primeros datos cifrados pueden luego enviarse directamente mediante el primer terminal al segundo terminal, y la plataforma de intercambio de datos se mantiene libre de los datos intercambiados, mejorando así la seguridad en la transmisión de datos.

Los datos pueden cifrarse mediante el primer terminal utilizando una variedad de métodos de cifrado. Por ejemplo, los primeros datos pueden cifrarse utilizando un algoritmo de cifrado simétrico. En este caso, la primera clave aquí es una clave utilizada para cifrar los primeros datos. De esta manera, la plataforma de intercambio de datos determina una clave para descifrar los primeros datos cifrados al recibir la clave que se envía por el primer terminal y utilizada para

cifrar los primeros datos. O bien, el primer terminal también puede cifrar los primeros datos utilizando un algoritmo de cifrado asimétrico y cifrar los primeros datos con una clave pública enviada mediante la plataforma de intercambio de datos. De esta manera, la plataforma de intercambio de datos solo necesita determinar una clave privada para descifrar los datos cifrados.

Para restringir a ambas partes del intercambio de datos, se prefiere que la primera clave se envíe por la plataforma de intercambio de datos en el momento adecuado en lugar de enviarse directamente por el primer terminal al segundo terminal. Es decir, después de que el primer terminal cifra los primeros datos utilizando un algoritmo de cifrado simétrico, la primera clave utilizada en el cifrado puede enviarse a la plataforma de intercambio de datos. Después de recibir la clave enviada por el primer terminal, la plataforma de intercambio de datos puede enviar la clave al segundo terminal realizando el paso 103.

Paso 103: La plataforma de intercambio de datos envía la primera clave al segundo terminal.

De esta manera, el segundo terminal, después de recibir los primeros datos enviados por el primer terminal, puede descifrar los primeros datos cifrados recibidos en base a la primera clave para obtener los primeros datos. El segundo terminal es un terminal correspondiente al segundo usuario.

De manera similar, cuando se envían datos al primer terminal, el segundo terminal también puede cifrar los datos utilizando una clave. Aquí, los datos a ser intercambiados retenidos por el segundo usuario se denominan segundos datos. Después de cifrar los segundos datos, el segundo terminal envía los segundos datos cifrados al primer terminal y luego envía una segunda clave para descifrar los datos cifrados a la plataforma de intercambio de datos. Luego, la plataforma envía la clave al primer terminal, de manera que el primer terminal puede descifrar los segundos datos cifrados utilizando la clave para obtener los segundos datos, implementando así el intercambio de datos entre ambas partes. En este proceso, los datos intercambiados entre ambas partes no pasan la plataforma de intercambio de datos, mejorando así la seguridad de los datos intercambiados.

Debe observarse que, en la realización de la presente solicitud, para facilitar la descripción, los datos retenidos por el primer usuario se denominan los primeros datos, los datos retenidos por el segundo usuario se denominan los segundos datos, y el proceso de intercambio de datos por ambas partes es un proceso de intercambio de los primeros datos y los segundos entre sí. Puede entenderse que los términos “primero” y “segundo” utilizados en la realización de la presente solicitud se utilizan para distinguir diferentes objetos descritos, y no se refieren a objetos particulares.

Para mejorar aún más la seguridad de los datos y evitar daños a los intereses de cualquiera de las partes, después de recibirse las claves enviadas por ambas partes para los datos cifrados, también es posible enviar las claves a ambas partes después de recibirse la información de confirmación enviada por ambas partes para los datos, con el fin de evitar el caso de que una parte no envíe la clave después de recibir los datos, lo que perjudica en gran medida los intereses de la otra parte. Por ejemplo, después de enviar la primera clave al segundo terminal, la plataforma de intercambio de datos envía la segunda clave al primer terminal después de recibir la información de confirmación enviada por el segundo terminal para los primeros datos. La información de confirmación para los primeros datos indica que el segundo usuario determina que los primeros datos se ajustan a la descripción en el acuerdo, protegiendo efectivamente los intereses del segundo usuario. Del mismo modo, después de recibir la información de confirmación enviada por el segundo usuario para los primeros datos, la plataforma de intercambio de datos también puede recibir información de confirmación enviada por el primer terminal para los segundos datos. La información de confirmación para los segundos datos indica que el primer usuario determina que los segundos datos se ajustan a la descripción en el acuerdo.

Algunos tipos de datos pueden intercambiarse a través de una plataforma. Los datos pueden ser, por ejemplo, datos que al usuario no le importa si los obtiene un tercero, o datos cuyo valor de datos no puede adquirirse por duplicación. No es necesario cifrar estos tipos de datos, lo que ahorra recursos de computación y recursos de almacenamiento. Para facilitar la descripción, los datos que pueden intercambiarse a través de una plataforma se denominan terceros datos.

En lo sucesivo, un método de intercambio de datos proporcionado en la presente solicitud se ilustra en detalle utilizando un ejemplo en el que los datos a ser intercambiados del segundo usuario son los terceros datos que se pueden intercambiar a través de la plataforma de intercambio de datos y la tecnología para cifrar los primeros datos a ser intercambiados es una tecnología de cifrado simétrico. Incluye los siguientes pasos:

Paso 201: Una plataforma de intercambio de datos escribe un acuerdo de intercambio de datos logrado entre un primer usuario y un segundo usuario en una cadena de bloques y almacena el acuerdo.

Paso 202: La plataforma de intercambio de datos recibe una primera clave enviada por un primer terminal y utilizada para descifrar los primeros datos cifrados.

Paso 203: El primer terminal envía los primeros datos cifrados a un segundo terminal.

Paso 204: El segundo terminal envía los terceros datos a la plataforma de intercambio de datos.

Debe observarse que la presente solicitud no limita la secuencia de ejecución del paso 202, del paso 203 y del paso 204.

Paso 205: La plataforma de intercambio de datos envía la primera clave recibida al segundo terminal.

Debido a que el segundo usuario envía directamente los terceros datos a la plataforma de intercambio de datos, la plataforma de intercambio de datos puede verificar los terceros datos y puede no enviar la primera clave al segundo terminal si encuentra que los terceros datos no se ajustan al acuerdo alcanzado por ambas partes, con el fin de evitar daños a los intereses del primer usuario. Por lo tanto, un proceso de implementación específico de este paso puede ser: enviar la primera clave recibida al segundo terminal cuando se determina que los terceros datos cumplen con el acuerdo de ambas partes.

Paso 206: El segundo terminal descifra los primeros datos cifrados recibidos de acuerdo con la primera clave recibida para obtener los primeros datos.

Paso 207: La plataforma de intercambio de datos envía los terceros datos al primer terminal.

Para los primeros datos obtenidos mediante el segundo usuario, debido a que la plataforma se mantiene libre de los primeros datos, la plataforma no podrá verificar la autenticidad de los mismos. En este caso, el primer terminal verifica los primeros datos. Durante la verificación, el segundo terminal puede adquirir información característica de los primeros datos acordados por ambas partes en el acuerdo de transacción. Específicamente, la información característica se puede adquirir a partir del acuerdo almacenado en una cadena de bloques. Definitivamente, cuando ambas partes negocian el acuerdo, el segundo terminal generalmente también almacena el acuerdo localmente. Por lo tanto, el segundo terminal también puede adquirir la información característica a partir del acuerdo almacenado mediante el segundo terminal. Después de adquirir la información característica de los primeros datos en el acuerdo, el segundo terminal puede verificar si los primeros datos adquiridos se ajustan a un registro en el acuerdo de acuerdo con la información característica adquirida.

De esta manera, si el segundo usuario encuentra que los primeros datos no se ajustan al acuerdo original, la plataforma no puede enviar los terceros datos al primer terminal, con el fin de evitar daños a los intereses del segundo usuario.

Por lo tanto, los terceros datos pueden enviarse al primer terminal cuando se recibe una instrucción de envío de datos enviada por el segundo terminal. La instrucción de envío de datos aquí es una instrucción para instruir a la plataforma de intercambio de datos para que envíe los terceros datos al primer usuario. Por ejemplo, la instrucción puede ser la información de confirmación mencionada anteriormente para los primeros datos, que indica que los terceros datos se envían al primer terminal solo después de que el segundo usuario envía y determina que los primeros datos se ajustan a la descripción en el acuerdo.

Sin embargo, si el usuario no envía la instrucción de envío de datos a la plataforma, el primer usuario no puede recibir los terceros datos. Para evitar daños a los intereses de los primeros datos, en algunos casos, los terceros datos también pueden enviarse al primer usuario. Por ejemplo, si el primer usuario aún no envía la información de confirmación para los primeros datos después de la duración preestablecida ya que la primera clave se envía al segundo usuario, los terceros datos pueden enviarse al primer usuario en este momento.

En base a lo anterior, un proceso de implementación específico del paso 207 puede ser: enviar los terceros datos al primer usuario cuando se determina que se cumple una condición preestablecida. Aquí, el momento en que se cumple la condición preestablecida puede ser después de que se recibe la instrucción de envío de datos enviada por el segundo terminal, o después de la duración preestablecida ya que la clave se envía al segundo terminal.

Hasta ahora, se implementa el intercambio de los primeros datos y los terceros entre los usuarios. Este método puede evitar la situación de que una parte no envíe datos a la otra parte después de adquirir los datos enviados por la otra parte, protegiendo así los intereses de ambas partes del intercambio de datos.

Después de completar el intercambio de datos, la plataforma de intercambio de datos también puede escribir un registro de que el intercambio se lleva a cabo como resultado del acuerdo de cambio de datos en la cadena de bloques y almacenar el registro para su uso posterior.

En la realización de la presente solicitud, también se puede determinar un estado de transmisión de los datos cifrados para evitar que el segundo usuario reciba los datos cifrados, pero afirme que los datos cifrados no se reciben, y para evitar que el primer terminal no envíe datos al segundo terminal, pero el primer usuario afirme haber enviado los datos al segundo terminal. Los datos cifrados aquí son los datos intercambiados cifrados, por ejemplo, los primeros datos cifrados y los segundos datos cifrados mencionados anteriormente. El estado de transmisión incluye uno de los siguientes: los datos cifrados no se han transmitido, los datos cifrados se están transmitiendo y los datos cifrados se han transmitido al segundo terminal.

Una forma específica de determinar el estado de transmisión de los datos cifrados puede ser la siguiente: la plataforma de interacción de datos adquiere el estado de transmisión de los datos cifrados a través de un programa de monitorización predeterminado. El programa de monitorización puede ser un programa utilizado para transmitir datos

entre ambas partes del intercambio de datos. O, una forma específica para determinar el estado de transmisión de los datos cifrados también puede ser: recibir el estado de transmisión de los datos cifrados informados activamente mediante el primer terminal y el segundo terminal.

Los datos cifrados enviados por el primer terminal no pasan la plataforma de intercambio de datos. Por lo tanto, si el primer terminal necesita realizar el intercambio de datos con múltiples terminales diferentes, debido a que diferentes terminales pueden soportar diferentes modos de transmisión de datos, el primer terminal necesita desarrollar diferentes interfaces de transmisión de datos para los diferentes terminales. Esto no solo consumirá más recursos humanos, sino que también ocupará demasiados recursos de almacenamiento. La plataforma de transmisión de datos puede entonces elaborar una especificación utilizada durante la transmisión de datos y definir una interfaz de transmisión estándar utilizada durante la transmisión de datos. La interfaz de transmisión estándar es una interfaz universal utilizada durante la transmisión de datos entre terminales.

Mientras un terminal de un usuario que realiza el intercambio de datos a través de la plataforma de transmisión de datos implemente la interfaz de transmisión estándar, el terminal puede transmitir datos a cualquier terminal que implemente la interfaz estándar. En la interfaz de transmisión estándar definida por la plataforma de transmisión de datos, por ejemplo, se puede definir información tal como un protocolo de transmisión de datos durante la transmisión de datos entre ambas partes del intercambio de datos. Los detalles no se describen aquí.

La función de la interfaz estándar definida también puede incluir una función de enviar un estado de transmisión de datos a la plataforma de intercambio de datos. De esta manera, después de terminar de enviar los datos cifrados, la plataforma de interacción de datos puede determinar que los datos cifrados se han enviado con éxito al segundo terminal, y luego se realiza una operación correspondiente.

En base a la realización de la presente solicitud, la FIG. 2 muestra un diagrama esquemático de un escenario de implementación de un método de envío de datos. Después de que ambas partes logran un acuerdo de intercambio de datos, un proceso específico de transmisión, mediante un primer terminal, de los primeros datos a un segundo terminal es el siguiente:

Paso 301: El primer terminal cifra los primeros datos para obtener datos cifrados.

Paso 302: El primer terminal envía los datos cifrados al segundo terminal a través de una interfaz de transmisión estándar implementada.

Definitivamente, el segundo terminal también implementa la interfaz de transmisión estándar.

Paso 303: El primer terminal envía una clave a una plataforma de intercambio de datos.

Paso 304: La plataforma de intercambio de datos envía la clave recibida al segundo terminal.

Paso 305: El segundo terminal descifra los datos cifrados de acuerdo con la clave recibida para obtener los primeros datos.

En el método de envío de datos proporcionado en la Realización 1 de la presente solicitud, durante el intercambio de datos, una plataforma de intercambio de datos escribe en una cadena de bloques un acuerdo de intercambio de datos alcanzado entre un primer usuario y un segundo usuario que intercambian datos. La plataforma de intercambio de datos luego recibe una primera clave, enviada por un primer terminal correspondiente al primer usuario, para descifrar los primeros datos cifrados. El primer terminal envía los primeros datos cifrados a un segundo terminal correspondiente al segundo usuario. La plataforma de intercambio de datos envía la primera clave al segundo terminal, y el segundo terminal descifra los primeros datos cifrados recibidos en base a la primera clave para obtener los primeros datos. Es evidente que la plataforma de intercambio de datos se mantiene libre de los primeros datos intercambiados en el proceso de intercambio de datos, evitando así el riesgo de que los primeros datos puedan utilizarse por la plataforma de intercambio de datos para otros fines, mejorando la seguridad de los datos en el proceso de intercambio de datos, y en paralelo la plataforma de intercambio de datos.

Cabe señalar que, para facilitar la descripción, se introduce una implementación del método de envío de datos utilizando un ejemplo en el que la plataforma de intercambio de datos ejecuta el método de datos. Se puede entender que el método que ejecuta la plataforma de intercambio de datos es una ilustración ejemplar, y no debe entenderse como una limitación de este método. A continuación, los pasos del método proporcionado en la Realización 1 pueden ejecutarse por un mismo dispositivo, o el método puede ejecutarse por diferentes dispositivos. Por ejemplo, el paso 101 y el paso 102 pueden ejecutarse por el dispositivo 1; para dar otro ejemplo, el paso 101 puede ejecutarse por el dispositivo 1, y el paso 102 puede ejecutarse por el dispositivo 2; etc.

Realización 2

El concepto inventivo de la presente solicitud se describe en detalle en base a la Realización 1 anterior. Para una mejor comprensión de las características técnicas, los medios y los efectos de la presente solicitud, el método de envío de datos de la presente solicitud se ilustra adicionalmente a continuación, formando así otra realización de la presente solicitud.

El proceso de intercambio de datos en la Realización 2 de la presente solicitud es similar al proceso de intercambio de datos en la Realización 1 y, para algunos pasos que no se introducen en la Realización 2, se puede hacer referencia a la descripción relevante en la Realización 1. Los detalles no se describen aquí de nuevo.

Antes de que la implementación de la solución se introduzca en detalle, primero se presenta brevemente un escenario de implementación de la solución.

En el Internet, el dinero también está presente en forma de datos. Por lo tanto, un valor de datos que representa dinero puede ser un valor del dinero representado por los datos. En el Internet, la transferencia de datos que representan dinero generalmente se implementa, en una operación real, cambiando los valores numéricos que identifican el dinero. Por ejemplo, si se transfieren 100 yuanes de la cuenta A a la cuenta B, la transferencia de datos es en realidad cambios correspondientes a valores numéricos que representan dinero en la cuenta A y la cuenta B.

Como se describe en la Realización 1, los valores de datos de algunos tipos de datos no pueden adquirirse por duplicación, y dichos datos pueden transmitirse a través de una plataforma. Por lo tanto, en la Realización 2, un proceso de implementación específico del método de envío de datos proporcionado en la presente solicitud se ilustra en detalle utilizando un ejemplo en el que los terceros datos son datos que representan dinero. Para facilitar la descripción, a continuación, los terceros datos para representar dinero se denominan dinero para abreviar. Por lo tanto, el proceso de intercambio de datos puede interpretarse como un proceso de transacción de datos, el primer usuario en la Realización 1 es un vendedor de datos, el segundo usuario es un comprador de datos, la plataforma de intercambio de datos es una plataforma de transacción de datos que puede proporcionar un servicio de transacción de datos para los usuarios.

En base a escenario anterior, en la FIG. 3 se muestra el proceso de implementación de transacción de datos en la Realización 2, que incluye los siguientes pasos:
Paso 401: Un vendedor de datos emite información de datos en venta a través de una plataforma de transacción de datos.

La plataforma de transacción de datos puede ayudar a los usuarios que tienen una demanda de venta de datos a emitir información de datos para la venta, de manera que los usuarios que tienen una demanda de consumo de datos pueden encontrar la información requerida en la plataforma de transacción de datos.

Paso 402: Un consumidor de datos y el vendedor de datos logran un acuerdo de transacción de datos.

El consumidor de datos puede comunicar acerca de detalles específicos de la transacción y, finalmente, lograr el acuerdo de transacción de datos. La función del acuerdo de transacción de datos es similar a la función del acuerdo de transacción de datos descrita en la Realización 1 y, por lo tanto, no se describe aquí en detalle de nuevo.

Paso 403: La plataforma de transacción de datos escribe el acuerdo de transacción de datos alcanzado por ambas partes en una cadena de bloques.

Una vez que el acuerdo de transacción de datos se escribe en la cadena de bloques, la posibilidad de manipular el acuerdo puede reducirse en gran medida y, por lo tanto, se mejora la seguridad del acuerdo.

Paso 404: El consumidor de datos paga una cantidad de dinero acordada en el acuerdo a la plataforma.

En el Internet, la transferencia de dinero es en realidad la transferencia de datos que representan el dinero. En una operación real, esto generalmente se implementa cambiando los valores de los datos que identifican el dinero en las cuentas.

Paso 405: El vendedor de datos cifra los datos en venta para obtener datos cifrados y luego envía una clave para el cifrado a la plataforma de transacción de datos.

Los datos pueden cifrarse utilizando una tecnología de cifrado simétrico, de manera que la clave para el cifrado sea la misma que la clave para el descifrado.

Debe observarse que la realización de la presente solicitud no limita la secuencia de ejecución del paso 404 y del paso 405.

Paso 406: El vendedor de datos transmite los datos cifrados a un terminal del consumidor de datos a través de un terminal que implementa una interfaz de transmisión estándar.

Como se describe en la Realización 1, la interfaz de transmisión estándar aquí es una interfaz universal definida por la plataforma de intercambio de datos y utilizada durante la transmisión de datos entre terminales. El terminal del consumidor de datos también debe implementar la interfaz de transmisión estándar con el fin de recibir datos. De esta manera, cuando el consumidor de datos y el vendedor de datos realizan además el intercambio de datos con otros

usuarios de la plataforma, no hay necesidad de desarrollar otras interfaces de transmisión, lo que ahorra recursos humanos y recursos de almacenamiento.

Paso 407: la plataforma de transacción de datos determina que los datos cifrados se han transmitido al terminal del consumidor de datos.

Un método específico para determinar que los datos cifrados se han transmitido al terminal del consumidor de datos es similar a la descripción relevante en la Realización 1 y, por lo tanto, no se describe aquí en detalle de nuevo.

Paso 408: La plataforma de transacción de datos envía una clave al consumidor de datos después de determinar que la cantidad de dinero pagada por el consumidor de datos se ajusta a la registrada en el acuerdo.

Debe observarse que la realización de la presente solicitud no limita la secuencia de ejecución del paso 407 y del paso 408.

Paso 409: el consumidor de datos descifra los datos cifrados utilizando la clave recibida y verifica si los datos descifrados se ajustan a la descripción en el acuerdo.

Paso 410: El consumidor de datos envía una instrucción de confirmación de recibo a la plataforma de transacción de datos a través del terminal después de determinar que los datos recibidos se ajustan a la descripción en el acuerdo.

La función de la instrucción de confirmación de recibo es similar a la función de la instrucción de envío de segundos datos descrita en la Realización 1 y, por lo tanto, no se describe en detalle aquí de nuevo.

Paso 411: La plataforma de transacción de datos, después de recibir la instrucción de confirmación de recibo, transfiere la cantidad de dinero pagada por el consumidor de datos a una cuenta del vendedor de datos.

Si el vendedor de datos y el consumidor de datos posteriormente tienen disputas sobre los datos en la transacción, pueden salvaguardar sus derechos de acuerdo con el acuerdo en la cadena de bloques.

En el método de transacción de datos proporcionado en la Realización 2 de la presente solicitud, una plataforma de transacción de datos recibe una clave enviada por un consumidor y utilizada para cifrar datos en venta, y luego envía la clave a un terminal del consumidor de datos después de recibir el dinero pagado por el consumidor de datos a través del terminal. De esta manera, después de recibir los datos cifrados enviados por el vendedor de datos, el consumidor de datos puede descifrar los datos cifrados utilizando la clave para obtener los datos vendidos por el vendedor de datos. Por lo tanto, en el proceso de transacción de datos, la plataforma de intercambio de datos se mantiene libre de los datos vendidos, evitando así el riesgo de que la plataforma de intercambio de datos pueda utilizar los datos vendidos para otros fines, y mejorando la seguridad de los datos en el proceso de transacción de datos.

Realización 3

Para resolver el problema de baja seguridad de datos en el proceso de intercambio de datos existente, la Realización 1 de la presente solicitud proporciona un aparato de envío de datos. Un diagrama estructural esquemático del aparato de envío de datos, como se muestra en la FIG. 4, incluye principalmente las siguientes unidades funcionales:

una unidad 501 de escritura configurada para escribir en una cadena de bloques un acuerdo de intercambio de datos logrado entre un primer usuario y un segundo usuario, y almacenar el acuerdo;

una primera unidad 502 de recepción configurada para recibir una primera clave enviada por un primer terminal y utilizada para descifrar los primeros datos cifrados, siendo el primer terminal un terminal correspondiente al primer usuario;

una primera unidad 503 de envío configurada para enviar la primera clave a un segundo terminal, de manera que el segundo terminal, después de recibir los primeros datos enviados por el primer terminal, descifra los primeros datos cifrados recibidos en base a la primera clave para obtener los primeros datos, siendo el segundo terminal un terminal correspondiente al segundo usuario.

En la realización de la presente solicitud, hay muchas otras implementaciones específicas para el intercambio de datos. En una implementación, el aparato incluye además una tercera unidad 504 de recepción configurada para, antes de que la primera unidad 503 de envío envíe la primera clave al segundo terminal, recibir una segunda clave enviada por el segundo terminal y utilizada para descifrar los segundos datos cifrados; y

una tercera unidad 505 de envío configurada para enviar la segunda clave al primer terminal después de que la primera unidad 503 de envío envíe la primera clave al segundo terminal, de manera que el primer terminal, después de recibir los segundos datos cifrados enviados por el segundo terminal, descifre los segundos datos cifrados recibidos en base a la segunda clave para obtener los segundos datos.

Para garantizar los intereses del segundo usuario, en una implementación, el aparato incluye además una cuarta unidad 506 de recepción configurada para, después de que la primera unidad 503 de envío envíe la primera clave al

segundo terminal y antes de que la tercera unidad 505 de envío envíe el segunda clave al primer terminal, recibir información de confirmación enviada por el segundo terminal para los primeros datos, la información de confirmación para los primeros datos indica que el segundo usuario determina que los primeros datos se ajustan a la descripción en el acuerdo.

En una implementación, el aparato incluye además una quinta unidad 507 de recepción configurada para, después de que la cuarta unidad 506 de recepción reciba la información de confirmación enviada por el segundo terminal para los primeros datos, recibir información de confirmación enviada por el primer terminal para los segundos datos, la información de confirmación para los segundos datos indica que el primer usuario determina que los segundos datos se ajustan a la descripción en el acuerdo.

En una implementación, el aparato incluye además una unidad 508 de escritura configurada para, después de que la quinta unidad 507 de recepción reciba la información de confirmación enviada por el primer terminal para los segundos datos, escribir en la cadena de bloques un registro de que el intercambio se realiza en un resultado del acuerdo de intercambio de datos, y almacenar el registro.

Para garantizar los intereses de ambas partes en el intercambio de datos, en una implementación, el aparato incluye además una segunda unidad 509 de recepción configurada para, antes de que la primera unidad 503 de envío envíe la primera clave al segundo terminal, recibir los terceros datos enviados por el segunda terminal; y una segunda unidad 510 de envío configurada para, después de que la primera unidad 503 de envío envíe la primera clave al segundo terminal, enviar los terceros datos al primer usuario cuando se determina que se cumple una condición preestablecida.

En una implementación, la determinación de que se cumple una condición preestablecida incluye específicamente: recibir, mediante la plataforma de intercambio de datos, una instrucción de envío de datos enviada por el segundo terminal, siendo la instrucción de envío de datos una instrucción para instruir a la plataforma de intercambio de datos que envíe los terceros datos a la primera terminal.

En una implementación, el acuerdo de intercambio de datos incluye información característica de los primeros datos.

La información característica de los primeros datos incluye al menos uno de los siguientes: un resumen de mensaje para verificar la integridad de los primeros datos; e información de referencia para resumir el contenido específico de los primeros datos.

Para evitar consumir más recursos humanos en el desarrollo de la interfaz, en una implementación, los primeros datos cifrados se transmiten al segundo terminal a través del primer terminal que implementa una interfaz de transmisión estándar. La interfaz de transmisión estándar es una interfaz universal definida por la plataforma de intercambio de datos y utilizada durante la transmisión de datos entre terminales.

En el aparato de envío de datos proporcionado en la Realización 3 de la presente solicitud, durante el intercambio de datos, una plataforma de intercambio de datos escribe en una cadena de bloques un acuerdo de intercambio de datos alcanzado entre un primer usuario y un segundo usuario que intercambian datos. La plataforma de intercambio de datos luego recibe una primera clave, enviada por un primer terminal correspondiente al primer usuario, para descifrar los primeros datos cifrados. El primer terminal envía los primeros datos cifrados a un segundo terminal correspondiente al segundo usuario. La plataforma de intercambio de datos envía la primera clave al segundo terminal, y el segundo terminal descifra los primeros datos cifrados recibidos en base a la primera clave para obtener los primeros datos. Es evidente que la plataforma de intercambio de datos se mantiene libre de los primeros datos intercambiados en el proceso de intercambio de datos, evitando así el riesgo de que los primeros datos puedan utilizarse por la plataforma de intercambio de datos para otros fines, mejorando la seguridad de los datos en el proceso de intercambio de datos, y en paralelo la plataforma de intercambio de datos.

En la década de 1990, una mejora en una tecnología puede distinguirse obviamente como una mejora en el hardware (por ejemplo, una mejora en una estructura de circuito tal como un diodo, un transistor y un interruptor) o una mejora en el software (una mejora en un procedimiento de método). Sin embargo, con el desarrollo de tecnologías, las mejoras de muchos procedimientos de método en la actualidad pueden considerarse como mejoras directas en las estructuras de circuitos de hardware. Casi todos los diseñadores programan los procedimientos del método mejorados en circuitos de hardware para obtener las correspondientes estructuras de circuito de hardware. Por lo tanto, es incorrecto suponer que la mejora de un procedimiento del método no puede implementarse utilizando un módulo de entidad de hardware. Por ejemplo, un dispositivo lógico programable (PLD) (por ejemplo, una matriz de compuertas programables en campo (FPGA)) es un circuito integrado cuyas funciones lógicas están determinadas por dispositivos programados por un usuario. Los diseñadores se programan solos para “integrar” un sistema digital en una pieza de PLD, sin la necesidad de pedirle a un fabricante de chips que diseñe y fabrique un chip de circuito integrado dedicado. Además, en la actualidad, la programación se implementa principalmente utilizando software compilador lógico, en lugar de fabricar manualmente un chip de circuito integrado. El software compilador lógico es similar a un compilador de software utilizado para desarrollar y escribir un programa, y el código original antes de la compilación también debe escribirse utilizando un lenguaje de programación específico, que se conoce como lenguaje de descripción de hardware (HDL). Hay muchos tipos de HDL, tal como el lenguaje de expresión booleana avanzada (ABEL), el lenguaje de descripción

de hardware Altera (AHDL), el lenguaje de programación de la Universidad de Cornell, Confluence, (CUPL), el lenguaje de descripción de hardware Java, HDCal, (JHDL), el lenguaje de descripción de hardware de Lava, Lola, MyHDL, PALASM y Ruby (RHDL), entre los cuales el Lenguaje de descripción de hardware de circuito integrado de muy alta velocidad (VHDL) y Verilog son los utilizados más comúnmente ahora. Los expertos en la técnica también deben saber que se puede obtener fácilmente un circuito de hardware para implementar el procedimiento del método lógico programando ligeramente de manera lógica el procedimiento del método utilizando los diversos lenguajes de descripción de hardware anteriores y programándolo en un circuito integrado.

Un controlador puede implementarse de cualquier manera adecuada. Por ejemplo, el controlador puede tener la forma de, por ejemplo, un microprocesador o un procesador y un medio legible por computadora que almacena el código de programa legible por computadora (por ejemplo, software o firmware) ejecutable por el (micro) procesador, una puerta lógica, un interruptor, un circuito integrado de aplicación específica (ASIC), un controlador lógico programable y un microcontrolador incorporado. Los ejemplos del controlador incluyen, entre otros, los siguientes microcontroladores: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20 y Silicone Labs C8051F320. Un controlador de memoria también puede implementarse como una parte de la lógica de control de una memoria. Los expertos en la técnica también saben que el controlador puede implementarse utilizando un código de programa legible por computadora puro, y además, los pasos del método pueden programarse lógicamente para permitir que el controlador implemente la misma función en forma de una puerta lógica, un interruptor, un circuito integrado aplicación específica, un controlador lógico programable, un microcontrolador incorporado y similares. Por lo tanto, este tipo de controlador puede considerarse como un componente de hardware, y los aparatos incluidos en el mismo para implementar diversas funciones también pueden considerarse como estructuras dentro del componente de hardware. O bien, los aparatos utilizados para implementar diversas funciones pueden incluso considerarse como módulos de software para implementar el método y las estructuras dentro del componente de hardware.

El sistema, aparato, módulo o unidad ilustrados en las realizaciones anteriores puede implementarse específicamente utilizando un chip de computadora o una entidad, o un producto que tiene una determinada función. Un dispositivo de implementación típico es una computadora. Específicamente, la computadora puede ser, por ejemplo, una computadora personal, una computadora portátil, un teléfono móvil, 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 computadora tableta, un dispositivo portátil o una combinación de cualquiera de estos dispositivos.

Para facilitar la descripción, cuando se describe el aparato, se divide en diversas unidades en términos de funciones para la respectiva descripción. Definitivamente, cuando se implementa la presente solicitud, las funciones de las unidades pueden implementarse en la misma o múltiples piezas de software y/o hardware.

Los expertos en la técnica deben comprender que las realizaciones de la presente invención pueden proporcionarse como un método, un sistema o un producto de programa informático. Por lo tanto, la presente invención puede implementarse como una realización de hardware completa, una realización de software completa o una realización que combina software y hardware. Además, la presente invención puede ser un producto de programa informático implementado en uno o más medios de almacenamiento utilizables por computadora (que incluyen, entre otros, una memoria de disco magnético, un CD-ROM, una memoria óptica y similares) que incluye el código de programa utilizable por computadora.

La presente invención se describe con referencia a diagramas de flujo y/o diagramas de bloques del método, dispositivo (sistema) y producto de programa informático de acuerdo con las realizaciones de la presente invención. Debe entenderse que puede utilizarse una instrucción de programa informático para implementar cada uno de los procesos y/o bloques en los diagramas de flujo y/o diagramas de bloques y combinaciones de procesos y/o bloques en los diagramas de flujo y/o diagramas de bloques. Estas instrucciones de programa informático pueden proporcionarse para una computadora de propósito general, una computadora de propósito especial, un procesador incorporado o un procesador de cualquier otro dispositivo de procesamiento de datos programable para generar una máquina, de modo que las instrucciones ejecutadas por una computadora o un procesador de cualquier otro dispositivo de procesamiento de datos programable genera un aparato para implementar una función específica en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones de programa informático también pueden almacenarse en una memoria legible por computadora que puede instruir a la computadora o cualquier otro dispositivo de procesamiento de datos programable para que trabaje de una manera particular, de manera que las instrucciones almacenadas en la memoria legible por computadora generen un artefacto que incluya un aparato de instrucciones. El aparato de instrucción implementa una función especificada en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones del programa informático también pueden cargarse en una computadora u otro dispositivo de procesamiento de datos programable, de manera que se realicen una serie de pasos de operación en la computadora u otro dispositivo programable, generando así el procesamiento implementado por computadora. Por lo tanto, las instrucciones ejecutadas en la computadora u otro dispositivo programable proporcionan pasos para implementar una

función especificada en uno o más procesos 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 una o más unidades centrales de procesamiento (CPU), una interfaz de entrada/salida, una interfaz de red y una memoria.

La memoria puede incluir medios legibles por computadora tales como una memoria volátil, una memoria de acceso aleatorio (RAM) y/o memoria no volátil, por ejemplo, memoria de solo lectura (ROM) o RAM flash. La memoria es un ejemplo de un medio legible por computadora.

El medio legible por computadora incluye medios no volátiles y volátiles, así como medios móviles y no móviles, y puede implementar el almacenamiento de información por medio de cualquier método o tecnología. La información puede ser una instrucción legible por computadora, una estructura de datos y un módulo de un programa u otros datos. Un medio de almacenamiento de una computadora incluye, por ejemplo, pero no se limita a, una memoria de cambio de fase (PRAM), una memoria estática de acceso aleatorio (SRAM), una memoria dinámica de acceso aleatorio (DRAM), otros tipos de RAM, una ROM, una memoria de solo lectura programable y borrable eléctricamente (EEPROM), una memoria flash u otras tecnologías de memoria, una memoria de solo lectura de disco compacto (CD-ROM), un disco versátil digital (DVD) u otros almacenamientos ópticos, una cinta de casete, un almacenamiento de cinta magnética/disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio sin transmisión, y puede utilizarse para almacenar información a la que accede el dispositivo informático. De acuerdo con la definición de este texto, el medio legible por computadora no incluye medios transitorios, tales como una señal de datos modulada y una portadora.

Cabe señalar además que el término “incluye”, “comprende” u otras variaciones de los mismos están destinados a cubrir la inclusión no exclusiva, de modo que un proceso, método, producto o dispositivo que incluye una serie de elementos no solo incluye los elementos, sino que también también incluye otros elementos que no están claramente enumerados, o incluye elementos inherentes del proceso, método, producto o dispositivo. En un caso sin más limitaciones, un elemento definido por “incluyen un/una...” no excluye que el proceso, método, producto o dispositivo que incluye el elemento tenga además otros elementos idénticos.

La presente solicitud puede describirse en un contexto común de una instrucción ejecutable por computadora ejecutada por una computadora, por ejemplo, un módulo de programa. Generalmente, el módulo de programa incluye una rutina, un programa, un objeto, un ensamblaje, una estructura de datos y similares utilizados para ejecutar una tarea específica o implementar un tipo de datos abstracto específico. La presente solicitud también puede implementarse en entornos informáticos distribuidos y, en los entornos informáticos distribuidos, una tarea se ejecuta utilizando dispositivos de procesamiento remotos conectados a través de una red de comunicaciones. En el entorno informático distribuido, el módulo de programa puede ubicarse en medios de almacenamiento informáticos locales y remotos, incluido un dispositivo de almacenamiento.

Las realizaciones en la memoria descriptiva se describen progresivamente, se pueden obtener partes idénticas o similares de las realizaciones con referencia entre sí, y cada una de las realizaciones enfatiza una parte diferente de otras realizaciones. Especialmente, la realización del sistema es básicamente similar a la realización del método, por lo que se describe de manera simple y, para las partes relacionadas, se puede hacer referencia a la descripción de las partes en la realización del método.

La descripción anterior es meramente realizaciones de la presente solicitud, y no pretende limitar la presente solicitud. Para los expertos en la técnica, la presente solicitud puede tener diversas modificaciones y variaciones. Cualquier modificación, reemplazo equivalente, mejora o similar realizada sin apartarse del principio de la presente solicitud debería caer dentro del alcance de las reivindicaciones de la presente solicitud.

La FIG. 5 es un diagrama de flujo que ilustra otro ejemplo de un método 500 implementado por computadora para transacciones de datos seguras, de acuerdo con una realización de la presente solicitud. Para mayor claridad de presentación, la descripción que sigue describe en general el método 500 en el contexto de las otras figuras en esta descripción. Sin embargo, se entenderá que el método 500 puede realizarse, por ejemplo, por cualquier sistema, entorno, software y hardware, o una combinación de sistemas, entornos, software y hardware, según corresponda. En algunas implementaciones, se pueden ejecutar diversos pasos del método 500 en paralelo, en combinación, en bucles o en cualquier orden. En algunas implementaciones, el método 500 puede incluir pasos adicionales o diferentes (o una combinación de ambos) que no se muestran en el diagrama de flujo. En algunas implementaciones, también pueden omitirse pasos del método 500.

En 510, una plataforma de intercambio de datos escribe en una cadena de bloques un acuerdo de intercambio de datos entre un primer usuario y un segundo usuario. El acuerdo de intercambio de datos está asociado con los primeros datos. Por ejemplo, los primeros datos son los datos a ser transferidos del primer usuario al segundo usuario de acuerdo con el acuerdo de intercambio de datos. En algunas implementaciones, la plataforma de intercambio de datos almacena el acuerdo de intercambio de datos. El acuerdo de intercambio de datos incluye una o más información de identidad del primer y segundo usuario, información característica de los datos intercambiados, especificaciones de

uso de datos cumplidas por el primer y segundo usuario, y penalizaciones, cumplidas por el primer y segundo usuario, por violar el acuerdo y otra información asociada con los datos intercambiados.

En algunas implementaciones, antes de escribir en la cadena de bloques el acuerdo de intercambio de datos, se recibe la información de datos asociada con los primeros datos, mediante la plataforma de intercambio de datos y desde un primer dispositivo asociado con el primer usuario, para su publicación en la plataforma de intercambio de datos. La información de datos asociada con los primeros datos luego se publica mediante la plataforma de intercambio de datos. La plataforma de intercambio de datos recibe una orden asociada con los primeros datos y desde un segundo dispositivo asociado con el segundo usuario. La orden asociada con los primeros datos se transmite mediante la plataforma de intercambio de datos al primer dispositivo. La plataforma de intercambio de datos y el primer dispositivo reciben la información de confirmación de la orden asociada con los primeros datos. Tanto la orden como la información de confirmación están asociados con el acuerdo de intercambio de datos. En algunas implementaciones, se puede llegar al acuerdo de intercambio de datos utilizando otros métodos apropiados. De 510, el método 500 procede a 520.

En 520, la plataforma de intercambio de datos recibe una primera clave y desde un primer dispositivo asociado con el primer usuario. La primera clave se utiliza para descifrar los primeros datos cifrados. Por ejemplo, el primer dispositivo cifra los primeros datos para obtener los primeros datos cifrados. De 520, el método 500 procede a 530.

En 530, la primera clave recibida se transmite mediante la plataforma de intercambio de datos a un segundo dispositivo asociado con el segundo usuario. En algunas implementaciones, antes de transmitir la primera clave recibida, la plataforma de intercambio de datos recibe una segunda clave y desde el segundo dispositivo asociado con el segundo usuario. La segunda clave se utiliza para descifrar los segundos datos cifrados, y los segundos datos están asociados con el acuerdo de intercambio de datos. Por ejemplo, los segundos datos son los datos a ser transferidos del segundo usuario al primer usuario de acuerdo con el acuerdo de intercambio de datos. Después de transmitir la primera clave recibida, la segunda clave recibida ser transmite mediante la plataforma de intercambio de datos al primer dispositivo asociado con el primer usuario. El primer dispositivo descifra los segundos datos cifrados, recibidos desde el segundo dispositivo, en base a la segunda clave para obtener los segundos datos. De 530, el método 500 procede a 540.

En 540, el primer dispositivo transmite los primeros datos cifrados al segundo dispositivo, sin pasar a través de la plataforma de intercambio de datos. En algunas implementaciones, los primeros datos cifrados en lugar de pasar a través de la plataforma de intercambio de datos, el primer dispositivo transmite los primeros datos cifrados directamente al segundo dispositivo para evitar que la plataforma de intercambio de datos utilice los primeros datos cifrados para otros fines (por ejemplo, acciones no definidas en el acuerdo de intercambio de datos entre el primer usuario y el segundo usuario), o haciendo cambios no autorizados a los primeros datos cifrados antes de transmitirlos al segundo dispositivo. En algunas implementaciones, los primeros datos cifrados se transmiten al segundo dispositivo a través de una interfaz de transmisión estándar del primer dispositivo. La interfaz de transmisión estándar es una interfaz universal definida por la plataforma de intercambio de datos y utilizada para transmitir datos entre diferentes dispositivos. De 540, el método 500 procede a 550.

En 550, el primer dispositivo descifra los primeros datos cifrados, en base a la primera clave para obtener los primeros datos. En algunas implementaciones, después de transmitir la primera clave recibida y antes de transmitir la segunda clave recibida, la plataforma de intercambio de datos recibe la información de confirmación de los primeros datos y desde el segundo dispositivo asociado con el segundo usuario . La información de confirmación para los primeros datos indica que el segundo usuario determina que los primeros datos obtenidos se ajustan al acuerdo de intercambio de datos.

En algunas implementaciones, después de recibir la información de confirmación para los primeros datos, la plataforma de intercambio de datos recibe la información de confirmación para los segundos datos y desde el primer dispositivo asociado con el primer usuario. La información de confirmación para los segundos datos indica que el primer usuario determina que los segundos datos obtenidos se ajustan al acuerdo de intercambio de datos. La plataforma de intercambio de datos escribe un registro en la cadena de bloques que indica que el intercambio de datos entre el primer usuario y el segundo usuario se realiza de acuerdo con el acuerdo de intercambio de datos. El registro se almacena por la plataforma de intercambio de datos.

En algunas implementaciones, antes de transmitir la primera clave recibida, la plataforma de intercambio de datos recibe los terceros datos y desde el segundo dispositivo asociado con el segundo usuario. Los terceros datos están asociados con el acuerdo de intercambio de datos. Por ejemplo, los terceros datos son datos que pueden intercambiarse a través de la plataforma de intercambio de datos. Después de transmitir la primera clave recibida, la plataforma de intercambio de datos transmite los terceros datos recibidos al primer dispositivo asociado con el primer usuario cuando se cumple una condición predeterminada. En algunas implementaciones, la condición predeterminada incluye que la plataforma de intercambio de datos recibe una instrucción desde el segundo dispositivo. La instrucción es una instrucción que instruye a la plataforma de intercambio de datos para que transmita los terceros datos recibidos al primer dispositivo.

En algunas implementaciones, el acuerdo de intercambio de datos incluye información característica de los primeros datos. La información característica de los primeros datos se adquiere por el segundo dispositivo. La información característica de los primeros datos incluye al menos uno de un resumen de mensaje para verificar la integridad de los primeros datos y la información de referencia para resumir el contenido específico de los primeros datos. El segundo dispositivo realiza una determinación de si los primeros datos obtenidos se ajustan al acuerdo de intercambio de datos en base a la información característica adquirida de los primeros datos. Si se determina que los primeros datos obtenidos se ajustan al acuerdo de intercambio de datos en base a la información característica adquirida de los primeros datos, el segundo dispositivo transmite información de confirmación para los primeros datos a la plataforma de intercambio de datos. Si se determina que los primeros datos obtenidos no se ajustan al acuerdo de intercambio de datos en base a la información característica adquirida de los primeros datos, el segundo dispositivo no transmitirá la información de confirmación de los primeros datos a la plataforma de intercambio de datos. Después de 550, el método 500 se detiene.

Las implementaciones de la materia objeto y las operaciones funcionales descritas en esta memoria descriptiva pueden implementarse en circuitos electrónicos digitales, en software o firmware de computadora incorporado de forma tangible, en hardware de computadora, incluidas las estructuras dadas a conocer en esta memoria descriptiva y sus equivalentes estructurales, o en combinaciones de uno o más de ellos. Las implementaciones de software de la materia objeto descrita se pueden implementar como uno o más programas informáticos, es decir, uno o más módulos de instrucciones de programas informáticos codificados en un medio tangible, no transitorio, legible por computadora para su ejecución por, o para controlar la operación de, una computadora o sistema implementado por computadora. Alternativa, o adicionalmente, las instrucciones del programa pueden codificarse en/sobre una señal propagada generada artificialmente, por ejemplo, una señal eléctrica, óptica o electromagnética generada por máquina que se genera para codificar información para la transmisión a un aparato receptor para la ejecución por una computadora o sistema implementado por computadora. El medio de almacenamiento de computadora puede ser un dispositivo de almacenamiento legible por máquina, un sustrato de almacenamiento legible por máquina, un dispositivo de memoria de acceso aleatorio o en serie, o una combinación de medios de almacenamiento de computadora. Configurar una o más computadoras significa que la una o más computadoras tienen instalado hardware, firmware o software (o combinaciones de hardware, firmware y software) de modo que cuando el software se ejecuta por la una o más computadoras, se realizan operaciones de computación particulares.

El término “tiempo-real”, “tiempo real”, “tiempo real (rápido) (RFT)”, “casi tiempo real (NRT)”, “cuasi tiempo real” o términos similares (tal como lo entiende un experto en la técnica), significa que una acción y una respuesta son temporalmente próximas, de modo que un individuo percibe que la acción y la respuesta se producen de manera sustancialmente simultánea. Por ejemplo, la diferencia de tiempo para que se muestre una respuesta (o para iniciar una visualización) de datos después de la acción del individuo para acceder a los datos puede ser inferior a 1 milisegundo (ms), inferior a 1 segundo (s) o inferior de 5 s. Si bien los datos solicitados no necesitan visualizarse (o iniciarse para su visualización) instantáneamente, se visualizan (o inician para su visualización) sin retraso intencional alguno, teniendo en cuenta las limitaciones de procesamiento de un sistema informático descrito y el tiempo requerido para, por ejemplo, recopilar, medir, analizar, procesar, almacenar o transmitir los datos con precisión.

Los términos “aparato de procesamiento de datos”, “computadora” o “dispositivo informático electrónico” (o un término equivalente como lo entiende un experto en la técnica) se refieren al hardware de procesamiento de datos y abarcan todo tipo de aparatos, dispositivos y máquinas para procesar datos, incluidos a modo de ejemplo, un procesador programable, una computadora o múltiples procesadores o computadoras. La computadora también puede ser, o incluir además, circuitos lógicos de propósito especial, por ejemplo, una unidad central de procesamiento (CPU), una matriz de compuertas programables en campo (FPGA) o un circuito integrado de aplicación específica (ASIC). En algunas implementaciones, la computadora o el sistema implementado por computadora o la circuitería lógica de propósito especial (o una combinación de la computadora o sistema implementado por computadora y los circuitos lógicos de propósito especial) pueden estar basados en hardware o software (o una combinación de ambos basados en hardware y en software). La computadora puede incluir opcionalmente código que crea un entorno de ejecución para programas informáticos, por ejemplo, código que constituye el firmware del procesador, una pila de protocolos, un sistema de gestión de bases de datos, un sistema operativo o una combinación de entornos de ejecución. La presente divulgación contempla el uso de una computadora o sistema implementado por computadora con un sistema operativo de algún tipo, por ejemplo LINUX, UNIX, WINDOWS, MAC OS, ANDROID, IOS, otro sistema operativo o una combinación de sistemas operativos.

Un programa informático, que también puede referirse o describirse como un programa, software, una aplicación de software, una unidad, un módulo, un módulo de software, un script, código u otro componente, puede escribirse en cualquier forma de lenguaje de programación, incluidos los lenguajes compilados o interpretados, o los lenguajes declarativos o procedimentales, y puede desplegarse en cualquier forma, incluidos, por ejemplo, como un programa independiente, módulo, componente o subrutina, para su uso en un entorno informático. Un programa informático puede, pero no necesariamente, corresponder a un archivo en un sistema de archivos. Un programa puede almacenarse en una porción de un archivo que contiene otros programas o datos, por ejemplo, uno o más scripts almacenados en un documento de lenguaje de marcado, en un solo archivo dedicado al programa en cuestión, o en múltiples archivos coordinados, por ejemplo, archivos que almacenan uno o más módulos, subprogramas o porciones de código. Un programa informático puede desplegarse para ejecutarse en una computadora o en múltiples

computadoras que se encuentran en un sitio o distribuidas en múltiples sitios e interconectadas por una red de comunicaciones.

Si bien porciones de los programas ilustrados en las diversas figuras se pueden ilustrar como componentes individuales, tales como unidades o módulos, que implementan características y funcionalidades descritas utilizando diversos objetos, métodos u otros procesos, los programas pueden incluir una serie de subunidades, submódulos, servicios de terceros, componentes, librerías y otros componentes, según corresponda. Por el contrario, las características y la funcionalidad de diversos componentes se pueden combinar en componentes individuales, según corresponda. Los umbrales utilizados para hacer determinaciones computacionales pueden determinarse estática, dinámicamente o tanto estática como dinámicamente.

Los métodos, procesos o flujos lógicos descritos representan uno o más ejemplos de funcionalidad coherentes con la presente divulgación y no pretenden limitar la divulgación a las implementaciones descritas o ilustradas, sino para ser acordes con el alcance más amplio coherente con los principios y características descritos. Los métodos, procesos o flujos lógicos descritos pueden realizarse por una o más computadoras programables que ejecutan uno o más programas informáticos para realizar funciones operando sobre datos de entrada y generando datos de salida. Los métodos, procesos o flujos lógicos también pueden realizarse por, y las computadoras también pueden implementarse como, circuitería lógica de propósito especial, por ejemplo, una CPU, una FPGA o un ASIC.

Las computadoras para la ejecución de un programa informático pueden basarse en microprocesadores de propósito general o especial, ambos u otro tipo de CPU. En general, una CPU recibirá instrucciones y datos de, y escribirá en, una memoria. Los elementos esenciales de una computadora son una CPU, para realizar o ejecutar instrucciones, y uno o más dispositivos de memoria para almacenar instrucciones y datos. En general, una computadora también incluirá, o estará operativamente acoplada, para recibir datos de o transferir datos a, o ambos, uno o más dispositivos de almacenamiento masivo para almacenar datos, por ejemplo, discos magnéticos, magnetoópticos o discos ópticos. Sin embargo, una computadora no necesita tener tales dispositivos. Además, una computadora puede integrarse en otro dispositivo, por ejemplo, un teléfono móvil, un asistente digital personal (PDA), un reproductor de audio o video móvil, una consola de juegos, un receptor de sistema de posicionamiento global (GPS) o un dispositivo de almacenamiento de memoria portátil.

Los medios legibles por computadora no transitorios para almacenar instrucciones y datos de programas informáticos pueden incluir todas las formas de memoria, medios y dispositivos de memoria permanentes/no permanentes o volátiles/no volátiles, incluidos a modo de ejemplo dispositivos de memoria semiconductores, por ejemplo, memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria de cambio de fase (PRAM), memoria estática de acceso aleatorio (SRAM), memoria dinámica de acceso aleatorio (DRAM), memoria de solo lectura programable borrable (EPROM), memoria de solo lectura programable borrable eléctricamente (EEPROM) y dispositivos de memoria flash; dispositivos magnéticos, por ejemplo, cintas, cartuchos, casetes, discos internos/extraíbles; discos magnetoópticos; y dispositivos de memoria óptica, por ejemplo, disco versátil/video digital (DVD), disco compacto (CD)-ROM, DVD+/-R, DVD-RAM, DVD-ROM, (HD)-DVD de alta definición/densidad, y DISCO BLU-RAY/BLU-RAY (BD) y otras tecnologías de memoria óptica. La memoria puede almacenar diversos objetos o datos, incluidos cachés, clases, marcos, aplicaciones, módulos, datos de respaldo, trabajos, páginas web, plantillas de páginas web, estructuras de datos, tablas de bases de datos, repositorios que almacenan información dinámica u otra información apropiada, incluidos los parámetros, variables, algoritmos, instrucciones, reglas, restricciones o referencias. Además, la memoria puede incluir otros datos apropiados, tales como registros, políticas, datos de seguridad o de acceso o archivos de informes. El procesador y la memoria pueden complementarse o incorporarse en circuitería lógica de propósito especial.

Para proporcionar interacción con un usuario, las implementaciones de la materia objeto descrita en esta memoria descriptiva se pueden implementar en una computadora que tenga un dispositivo de visualización, por ejemplo, un tubo de rayos catódicos (CRT), pantalla de cristal líquido (LCD), diodo emisor de luz (LED), o monitor de plasma, para visualizar información al usuario y un teclado y un dispositivo señalador, por ejemplo, un ratón, bola de seguimiento o panel táctil mediante el cual el usuario puede proporcionar entrada a la computadora. La entrada también se puede proporcionar a la computadora utilizando una pantalla táctil, tal como una superficie de tableta con sensibilidad a la presión, una pantalla multitáctil utilizando detección capacitiva o eléctrica, u otro tipo de pantalla táctil. Se pueden utilizar otros tipos de dispositivos para interactuar con el usuario. Por ejemplo, la retroalimentación proporcionada al usuario puede ser cualquier forma de retroalimentación sensorial (tal como visual, auditiva, táctil o una combinación de tipos de retroalimentación). La entrada del usuario se puede recibir en cualquier forma, incluida entrada acústica, de voz o táctil. Además, una computadora puede interactuar con el usuario enviando documentos y recibiendo documentos de un dispositivo informático cliente que utiliza el usuario (por ejemplo, enviando páginas web a un navegador web en el dispositivo informático móvil de un usuario en respuesta a solicitudes recibidas del navegador web).

El término “interfaz gráfica de usuario” o “GUI” puede utilizarse en singular o en plural para describir una o más interfaces gráficas de usuario y cada una de las pantallas de una interfaz gráfica de usuario particular. Por lo tanto, una GUI puede representar cualquier interfaz gráfica de usuario, incluidas, entre otros, un navegador web, una pantalla táctil o una interfaz de línea de comando (CLI) que procesa información y presenta de manera eficiente los resultados

de la información al usuario. En general, una GUI puede incluir una serie de elementos de la interfaz de usuario (UI), algunos o todos asociados con un navegador web, como campos interactivos, listas desplegables y botones. Estos y otros elementos de la IU pueden estar relacionados o representar las funciones del navegador web.

Las implementaciones de la materia objeto descrita en esta memoria descriptiva se pueden implementar en un sistema informático que incluye un componente servidor, por ejemplo, como un servidor de datos, o que incluye un componente middleware, por ejemplo, un servidor de aplicaciones, o que incluye un componente frontal, por ejemplo, una computadora cliente que tiene una interfaz gráfica de usuario o un navegador web a través del cual un usuario puede interactuar con una implementación de la materia objeto descrita en esta memoria descriptiva, o cualquier combinación de uno o más de estos componentes servidores, middleware o frontales. Los componentes del sistema pueden interconectarse mediante cualquier forma o medio de comunicación de datos digitales por cable o inalámbrica (o una combinación de comunicación de datos), por ejemplo, una red de comunicaciones. Los ejemplos de redes de comunicaciones incluyen una red de área local (LAN), una red de acceso de radio (RAN), una red de área metropolitana (MAN), una red de área amplia (WAN), interoperabilidad mundial para acceso por microondas (WIMAX), una red de área local inalámbrica (WLAN) que utiliza, por ejemplo, 802.11 a/b/g/n u 802.20 (o una combinación de 802.11x y 802.20 u otros protocolos compatibles con la presente divulgación), todo o una parte del Internet, otra red de comunicaciones o un combinación de redes de comunicaciones. La red de comunicaciones puede comunicarse con, por ejemplo, paquetes de Protocolo de Internet (IP), tramas de retransmisión de tramas, celdas de modo de transferencia asincrónica (ATM), voz, video, datos u otra información entre nodos de red.

El sistema informático puede incluir clientes y servidores. Un cliente y un servidor generalmente están alejados entre sí y generalmente interactúan a través de una red de comunicaciones. La relación del cliente y el servidor surge en virtud de los programas informáticos que se ejecutan en las respectivas computadoras y que tienen una relación cliente-servidor entre sí.

Si bien esta memoria descriptiva contiene muchos detalles de implementación específicos, estos no deben interpretarse como limitaciones en el alcance de cualquier concepto inventivo o en el alcance de lo que se puede reivindicar, sino más bien como descripciones de características que pueden ser específicas para implementaciones particulares de conceptos inventivos particulares. Ciertas características que se describen en esta memoria descriptiva en el contexto de implementaciones separadas también se pueden implementar, en combinación, en una sola implementación. Por el contrario, diversas características que se describen en el contexto de una sola implementación también se pueden implementar en múltiples implementaciones, por separado o en cualquier subcombinación. Además, aunque las características descritas anteriormente pueden describirse como actuando en ciertas combinaciones e incluso reivindicarse inicialmente como tales, una o más características de una combinación reivindicada pueden, en algunos casos, eliminarse de la combinación, y la combinación reivindicada puede dirigirse a un subcombinación o variación de una subcombinación.

Se han descrito implementaciones particulares de la materia objeto. Otras implementaciones, alteraciones y permutaciones de las implementaciones descritas están dentro del alcance de las siguientes reivindicaciones, como será evidente para los expertos en la técnica. Si bien las operaciones se representan en los dibujos o reivindicaciones en un orden particular, esto no debe entenderse como que requiere que tales operaciones se realicen en el orden particular mostrado o en orden secuencial, o que se realicen todas las operaciones ilustradas (algunas operaciones pueden considerarse opcionales), para lograr resultados deseables. En ciertas circunstancias, el procesamiento multitarea o paralelo (o una combinación de procesamiento multitarea y paralelo) puede ser ventajoso y realizarse según se considere apropiado.

Además, la separación o integración de diversos módulos y componentes del sistema en las implementaciones descritas anteriormente no debe entenderse que requieren tal separación o integración en todas las implementaciones, y debe entenderse que los componentes y sistemas del programa descritos pueden generalmente integrarse juntos en un producto de software único o empaquetarse en múltiples productos de software.

Por consiguiente, las implementaciones de ejemplo descritas anteriormente no definen ni limitan la presente divulgación. Otros cambios, sustituciones y alteraciones también son posibles sin apartarse del alcance de la presente divulgación.

Además, cualquier implementación reivindicada se considera aplicable al menos a un método implementado por computadora; un medio no transitorio, legible por computadora que almacena instrucciones legibles por computadora para realizar el método implementado por computadora; y un sistema informático que comprende una memoria de computadora acoplada interoperablemente con un procesador de hardware configurado para realizar el método implementado por computadora o las instrucciones almacenadas en el medio no transitorio, legible por computadora.

REIVINDICACIONES

1. Un método para enviar primeros datos desde un primer terminal directamente a un segundo terminal, que comprende:

escribir y almacenar en una cadena de bloques, mediante una plataforma de intercambio de datos, un acuerdo de intercambio de datos logrado entre un primer usuario y un segundo usuario, en donde el acuerdo de intercambio de datos incluye información característica de los datos intercambiados, en donde los datos intercambiados incluyen los primeros datos del primer usuario y datos a ser intercambiados del segundo usuario (101, 510);

recibir, mediante la plataforma de intercambio de datos, una primera clave enviada por el primer terminal y utilizada para descifrar los primeros datos cifrados, siendo el primer terminal un terminal correspondiente al primer usuario, en donde el primer terminal cifra los primeros datos para obtener los primeros datos cifrados de acuerdo con una tecnología de cifrado simétrico, el primer terminal envía la primera clave a la plataforma de intercambio de datos, y el primer terminal envía directamente los primeros datos cifrados al segundo terminal (102, 520); y

cuando se verifica, mediante la plataforma de intercambio de datos, que los terceros datos recibidos por la plataforma de intercambio de datos desde el segundo terminal cumplen con el acuerdo de intercambio de datos, enviar, mediante la plataforma de intercambio de datos, la primera clave al segundo terminal, de manera que el segundo terminal, después de recibir los primeros datos cifrados enviados por el primer terminal, descifra los primeros datos cifrados recibidos en base a la primera clave para obtener los primeros datos, siendo el segundo terminal un terminal correspondiente al segundo usuario, en donde los terceros datos son los datos a ser intercambiados del segundo usuario para recibir los primeros datos del primer usuario (103, 530).

2. El método de la reivindicación 1, que comprende, además:

enviar, mediante la plataforma de intercambio de datos, los terceros datos al primer terminal cuando se recibe una instrucción de envío de datos enviada por el segundo terminal, en donde los terceros datos son los datos a ser intercambiados del segundo usuario referidos en el acuerdo de intercambio de datos, en donde los terceros datos se intercambian a través de la plataforma de intercambio de datos con el primer usuario.

3. El método de la reivindicación 1, que comprende, además:

descifrar, mediante el segundo terminal, los primeros datos cifrados recibidos utilizando la primera clave para obtener los primeros datos (550).

4. El método de la reivindicación 3, en donde antes del paso de escribir y almacenar en la cadena de bloques, mediante la plataforma de intercambio de datos, el acuerdo de intercambio de datos entre el primer usuario y el segundo usuario, el método comprende, además:

recibir, en la plataforma de intercambio de datos, información de datos emitida por el primer terminal y publicar la información de datos;

recibir, en la plataforma de intercambio de datos, una solicitud de puesta de orden para la información de datos publicada por el segundo terminal, y enviar la solicitud al primer terminal; y

recibir, mediante la plataforma de intercambio de datos, la información de confirmación enviada por el primer terminal para la solicitud de puesta de orden para lograr el acuerdo de intercambio de datos.

5. El método de la reivindicación 1, en donde antes del paso de enviar la primera clave al segundo terminal, el método comprende, además:

recibir, mediante la plataforma de intercambio de datos, una segunda clave enviada por el segundo terminal y utilizada para descifrar los segundos datos cifrados; y

después del paso de enviar, mediante la plataforma de intercambio de datos, la primera clave al segundo terminal, el método comprende, además enviar, mediante la plataforma de intercambio de datos, la segunda clave al primer terminal, de manera que el primer terminal, después de recibir los segundos datos cifrados enviados por el segundo terminal, descifra los segundos datos cifrados recibidos en base a la segunda clave para obtener los segundos datos.

6. El método de la reivindicación 5, en donde después del paso de enviar, mediante la plataforma de intercambio de datos, la primera clave al segundo terminal y antes del paso de enviar la segunda clave al primer terminal, el método comprende, además recibir, mediante el plataforma de intercambio de datos, información de confirmación para los primeros datos enviados por el segundo terminal, la información de confirmación para los primeros datos indica que el segundo usuario determina que los primeros datos se ajustan a la descripción en el acuerdo.

7. El método de la reivindicación 6, en donde después del paso de recibir, mediante la plataforma de intercambio de datos, la información de confirmación enviada por el segundo terminal para los primeros datos, el método comprende, además recibir, mediante la plataforma de intercambio de datos, la información de confirmación enviada por el primer terminal para los segundos datos, la información de confirmación para los segundos datos indica que el primer usuario determina que los segundos datos se ajustan a la descripción en el acuerdo.

8. El método de la reivindicación 7, en donde después del paso de recibir, mediante la plataforma de intercambio de datos, la información de confirmación enviada por el primer terminal para los segundos datos, el método comprende, además escribir y almacenaren la cadena de bloques, mediante la plataforma de intercambio de datos, un registro que se realiza el intercambio en un resultado del acuerdo de intercambio de datos.

9. El método de la reivindicación 1, en donde después de enviar, mediante la plataforma de intercambio de datos, la primera clave al segundo terminal, el método comprende, además enviar, mediante la plataforma de intercambio de datos, los terceros datos al primer usuario cuando se determina que se cumple una condición predeterminada.

10. El método de la reivindicación 9, en donde determinar que la condición preestablecida se cumple comprende específicamente recibir, mediante la plataforma de intercambio de datos, una instrucción de envío de datos enviada por el segundo terminal, siendo la instrucción de envío de datos una instrucción para instruir a la plataforma de intercambio de datos para que envíe los terceros datos al primer terminal.

11. El método de una cualquiera de las reivindicaciones 2-10, en donde:
el acuerdo de intercambio de datos comprende información característica de los primeros datos;
el método comprende, además obtener, mediante el segundo terminal, la información característica y determinar, de acuerdo con la información característica, si los primeros datos adquiridos se ajustan al registro en el acuerdo; y
la información característica de los primeros datos comprende al menos uno de los siguientes:
un resumen de mensaje para verificar la integridad de los primeros datos; e
información de referencia para resumir contenido específico de los primeros datos.

12. El método de una cualquiera de las reivindicaciones 2-10, en donde los primeros datos cifrados se transmiten al segundo terminal mediante el primer terminal que implementa una interfaz de transmisión estándar, y la interfaz de transmisión estándar comprende una interfaz universal definida por la plataforma de intercambio de datos y utilizada para transmitir datos entre terminales.

13. El método de cualquiera de las reivindicaciones 1 a 11, en donde se determina que un estado de transmisión de los primeros datos cifrados incluye si los primeros datos cifrados se han transmitido o no al segundo terminal, en donde determinar el estado de transmisión del primer los datos cifrados incluye recibir el estado de transmisión de los primeros datos cifrados informados activamente mediante el primer terminal y el segundo terminal.

14. El método de las reivindicaciones 1 a 4, en donde los terceros datos son datos que representan dinero, y allí el primer usuario es un vendedor de datos y el segundo usuario es un comprador de datos.

15. Un sistema de envío de datos que comprende al menos un primer terminal, un segundo terminal y una plataforma de intercambio de datos configurada para realizar el método de una cualquiera de las reivindicaciones 1-14

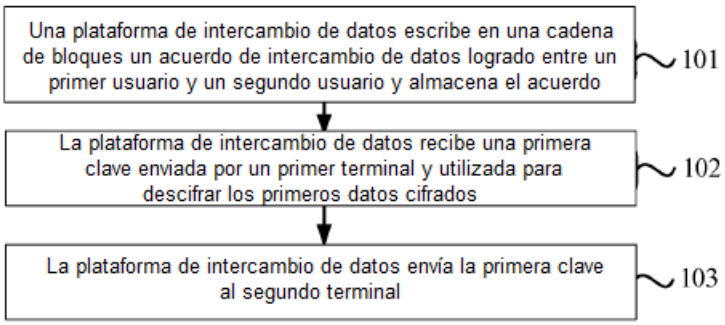
Una plataforma de intercambio de datos escribe en una cadena de bloques un acuerdo de intercambio de datos logrado entre un primer usuario y un segundo usuario y almacena el acuerdo
101
La plataforma de intercambio de datos recibe una primera clave enviada por un primer terminal y utilizada para descifrar los primeros datos cifrados
102
La plataforma de intercambio de datos envía la primera clave al segundo terminal
103

FIG. 1

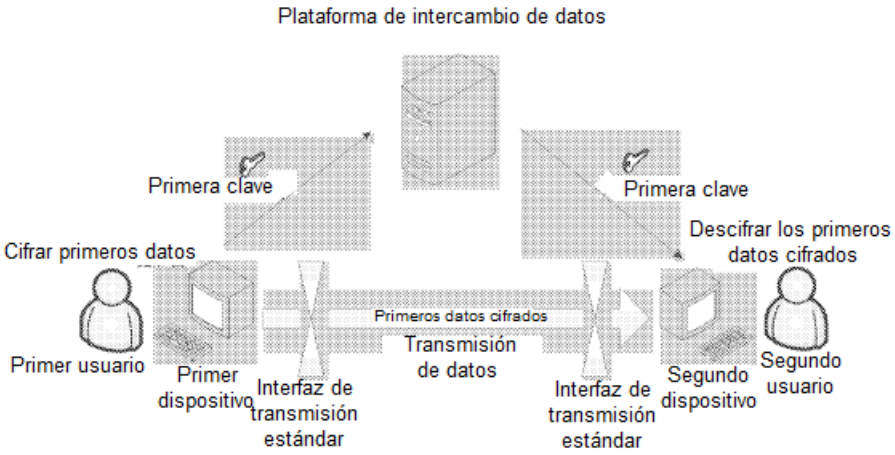
Plataforma de intercambio de datos
Primera clave
Primera clave
Cifrar primeros datos
Descifrar los primeros datos cifrados
Primeros datos cifrados
Transmisión de datos
Primer usuario
Primer dispositivo
Interfaz de transmisión estándar
Interfaz de transmisión estándar
Segundo dispositivo
Segundo usuario

FIG. 2

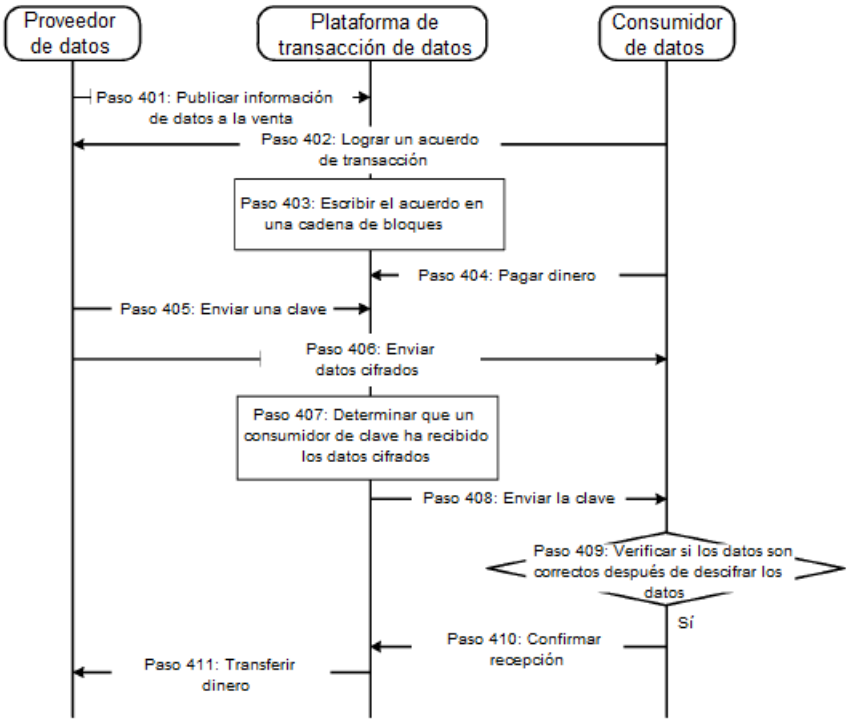
Proveedor de datos
Plataforma de transacción de datos
Consumidor de datos
Paso 401: Publicar información de datos a la venta
Paso 402: Lograr un acuerdo de transacción
Paso 403: Escribir el acuerdo en una cadena de bloques
Paso 404: Pagar dinero
Paso 405: Enviar una clave
Paso 406: Enviar datos cifrados
Paso 407: Determinar que un consumidor de clave ha recibido los datos cifrados
Paso 408: Enviar la clave
Paso 409: Verificar si los datos son correctos después de descifrar los datos
Sí
Paso 410: Confirmar recepción
Paso 411: Transferir dinero

FIG. 3

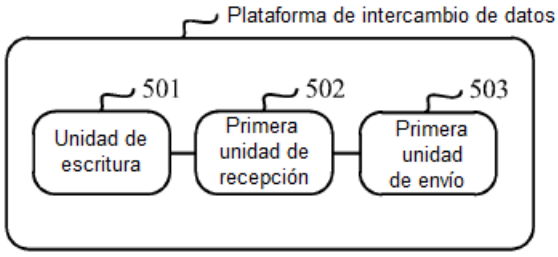
Plataforma de intercambio de datos
501
Unidad de escritura
502
Primera unidad de recepción
503
Primera unidad de envío

FIG. 4

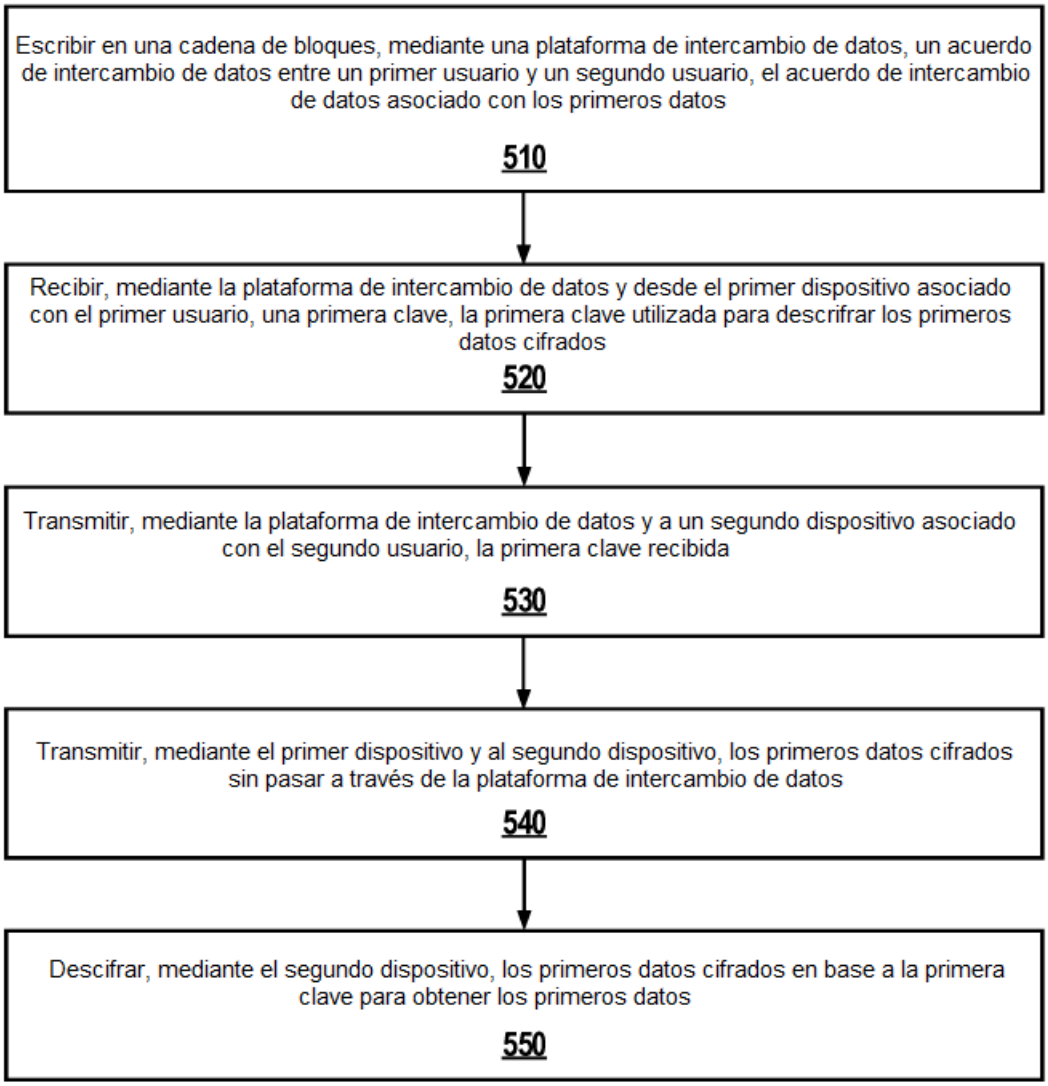
Escribir en una cadena de bloques, mediante una plataforma de intercambio de datos, un acuerdo de intercambio de datos entre un primer usuario y un segundo usuario, el acuerdo de intercambio de datos asociado con los primeros datos
510
Recibir, mediante la plataforma de intercambio de datos y desde el primer dispositivo asociado con el primer usuario, una primera clave, la primera clave utilizada para descrifrar los primeros datos cifrados
520
Transmitir, mediante la plataforma de intercambio de datos y a un segundo dispositivo asociado con el segundo usuario, la primera clave recibida
530
Transmitir, mediante el primer dispositivo y al segundo dispositivo, los primeros datos cifrados sin pasar a través de la plataforma de intercambio de datos
540
Descifrar, mediante el segundo dispositivo, los primeros datos cifrados en base a la primera clave para obtener los primeros datos
550

FIG. 5

500