

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 809 205**

51 Int. Cl.:

G06F 21/31 (2013.01)

H04L 29/06 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **13.07.2018 PCT/US2018/042064**

87 Fecha y número de publicación internacional: **17.01.2019 WO19014577**

96 Fecha de presentación y número de la solicitud europea: **13.07.2018 E 18749946 (2)**

97 Fecha y número de publicación de la concesión europea: **17.06.2020 EP 3552132**

54 Título: **Método y dispositivo de procesamiento de información de inicio de sesión**

30 Prioridad:

14.07.2017 CN 201710574655

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, HAO

74 Agente/Representante:

LEHMANN NOVO, María Isabel

ES 2 809 205 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método y dispositivo de procesamiento de información de inicio de sesión

5 CAMPO TÉCNICO

La presente solicitud se refiere al campo de las tecnologías de cadena de bloques y, en particular, a un método y dispositivo de procesamiento de información de inicio de sesión.

10 ANTECEDENTES

15 Con el desarrollo de las tecnologías de Internet, diversos servicios de red se pueden proporcionar a los usuarios utilizando una plataforma de servicios de Internet. Antes de que un servidor correspondiente a la plataforma de servicios de Internet proporcione diversos servicios de red para un usuario, el usuario debe enviar información de inicio de sesión (por ejemplo, un nombre de usuario y contraseña registrados en el servidor), de modo que se pueda verificar la identidad de un usuario utilizando la información de inicio sesión enviada por el usuario. Como tal, cuando se verifica la identidad, el servidor puede proporcionar el servicio de red al usuario y, por lo tanto, se garantiza la seguridad del servicio de red proporcionado.

20 Sin embargo, con el rápido aumento del número de plataformas de servicios de Internet que pueden proporcionar un servicio de red para un usuario, para garantizar la seguridad de la información de inicio de sesión, la información de inicio de sesión de que un usuario puede registrar con diferentes plataformas de servicios de Internet puede ser la misma o diferente, provocando inconvenientes para que el usuario mantenga la información de inicio de sesión.

25 Actualmente, se proporciona un método de procesamiento de información de inicio de sesión. Para ser específicos, se almacena diferente información de inicio de sesión en un servidor de terceros que coopera con un servidor correspondiente a una plataforma de servidor de Internet. Cuando el usuario necesita utilizar la información de inicio de sesión, el usuario puede obtener la información de inicio de sesión necesaria desde el servidor de terceros.

30 Sin embargo, la industria necesita un método de procesamiento de información de inicio de sesión que pueda mejorar la seguridad de la información de inicio de sesión.

RESUMEN

35 Las implementaciones de la presente memoria descriptiva proporcionan un método y dispositivo de procesamiento de información de inicio de sesión, para mejorar la seguridad de la información de inicio de sesión.

40 La invención se define por las reivindicaciones independientes. Realizaciones adicionales están definidas por las reivindicaciones dependientes.

La al menos una solución técnica utilizada en las implementaciones de la presente memoria descriptiva puede lograr los siguientes efectos beneficiosos:

45 En las implementaciones de la presente memoria descriptiva, un contrato inteligente que incluye información de inicio de sesión de un cierto usuario puede crearse en base a una plantilla de contrato inteligente predeterminada, y el contrato inteligente se almacena en una red de cadena de bloques, de modo que la seguridad de almacenamiento de la información de inicio de sesión del usuario se mejora efectivamente. La al menos una solución técnica se implementa en base a la red de cadena de bloques, de modo que es menos probable que la información de inicio de sesión se pierda, robe o manipule, y se mejora la seguridad de almacenamiento de la información de inicio de sesión. Además, cuando el usuario necesita la información de inicio de sesión, el usuario puede obtener rápidamente la información de inicio de sesión necesaria desde la red de cadena de bloques a través de consulta, lo que hace que sea conveniente para el usuario mantener la información de inicio de sesión.

55 BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los dibujos adjuntos aquí se utilizan para proporcionar una mayor comprensión de la presente solicitud, y constituyen una parte de la presente solicitud. Las implementaciones de ejemplo de la presente aplicación y las descripciones de las implementaciones se utilizan para explicar la presente aplicación, y no constituyen una limitación inadecuada para la presente aplicación. En los dibujos adjuntos:

60 La FIG. 1 es un diagrama de flujo que ilustra un método de procesamiento de información de inicio de sesión, de acuerdo con una implementación de la presente memoria descriptiva.

la FIG. 2 es un diagrama de flujo que ilustra un método de procesamiento de información de inicio de sesión, de acuerdo con una implementación de la presente memoria descriptiva.

65 la FIG. 3 es un diagrama de flujo que ilustra un método de procesamiento de información de inicio de sesión, de acuerdo con una implementación de la presente memoria descriptiva.

La FIG. 4 es un diagrama estructural que ilustra un dispositivo de procesamiento de información de inicio de sesión, de acuerdo con una implementación de la presente memoria descriptiva.

La FIG. 5 es un diagrama estructural que ilustra un dispositivo de procesamiento de información de inicio de sesión, de acuerdo con una implementación de la presente memoria descriptiva.

5 La FIG. 6 es un diagrama de flujo que ilustra un ejemplo de un método implementado por computadora para procesar datos de información de inicio de sesión, de acuerdo con una implementación de la presente divulgación.

DESCRIPCIÓN DE IMPLEMENTACIONES

10 En base a las soluciones técnicas proporcionadas en la tecnología existente, la información de inicio de sesión se almacena en un servidor de terceros. Sin embargo, debido a que el servidor de terceros almacena la información de inicio de sesión de muchos usuarios, existe el riesgo de que la información de inicio de sesión almacenada en el servidor de terceros se filtre, lo que reduce la seguridad de la información de inicio de sesión de un usuario.

15 Para mejorar la seguridad de la información de inicio de sesión del usuario, las implementaciones de la presente memoria descriptiva proporcionan un método de procesamiento de información de inicio de sesión. El método de procesamiento de información de inicio de sesión puede realizarse por un dispositivo de procesamiento de información. El dispositivo de procesamiento de información puede almacenar información de inicio de sesión del usuario en una red de cadena de bloques, y la seguridad de la información de inicio de sesión del usuario puede mejorarse confiando
20 en la resistencia a la manipulación y la confiabilidad de la red de cadena de bloques.

La FIG. 1 es un diagrama de flujo que ilustra un método de procesamiento de información de inicio de sesión, de acuerdo con una implementación de la presente memoria descriptiva. El método de procesamiento de información de inicio de sesión incluye los siguientes pasos:

25 Paso 101: Un dispositivo de procesamiento de información recibe una solicitud de almacenamiento de información de inicio de sesión que se envía mediante un usuario y que incluye un identificador.

Paso 103: El dispositivo de procesamiento de información determina la información de inicio de sesión del usuario en base a la solicitud de almacenamiento de información de inicio de sesión.

30 Paso 105: Después de obtener la información de inicio de sesión del usuario, el dispositivo de procesamiento de información crea un contrato inteligente que incluye la información de inicio de sesión del usuario.

Paso 107: El dispositivo de procesamiento de información almacena el contrato inteligente en una red de cadena de bloques en base al identificador.

Paso 109: El dispositivo de procesamiento de información recibe una solicitud de consulta de información de inicio de sesión que se envía mediante el usuario y que incluye el identificador.

35 Paso 111: El dispositivo de procesamiento de información lee el contrato inteligente correspondiente al usuario desde la red de cadena de bloques en base al identificador.

Paso 113: El dispositivo de procesamiento de información ejecuta el contrato inteligente en la red de cadena de bloques para obtener la información de inicio de sesión correspondiente al usuario.

40 En base al método de procesamiento de información de inicio de sesión en la implementación de la presente memoria descriptiva, la información de inicio de sesión se almacena en la red de cadena de bloques, y la información de inicio de sesión se puede consultar y obtener desde la red de cadena de bloques. La red de cadena de bloques está construida en base a una tecnología de cadena de bloques. La tecnología de cadena de bloques, conocida como tecnología de libro de cuentas distribuido, es una tecnología de base de datos de Internet distribuida que se caracteriza
45 por la descentralización, la transparencia, la resistencia a la manipulación y la confiabilidad. Por lo tanto, es menos probable que la información de inicio de sesión se pierda, robe o manipule, y se mejora la seguridad de almacenamiento y consulta de la información de inicio de sesión.

50 Para clarificar los objetivos, las soluciones técnicas y las ventajas de la presente solicitud, lo siguiente describe clara y exhaustivamente las soluciones técnicas de la presente solicitud con referencia a implementaciones específicas y los correspondientes dibujos adjuntos en la presente solicitud. Aparentemente, las implementaciones descritas son simplemente algunas, pero no todas las implementaciones de la presente memoria descriptiva. Todas las demás implementaciones obtenidas sin esfuerzos creativos por un experto en la técnica en base a las implementaciones de la presente solicitud deberán caer dentro del alcance de protección de la presente solicitud.

55 Las soluciones técnicas proporcionadas en las implementaciones de la presente memoria descriptiva se describen en detalle a continuación con referencia a los dibujos adjuntos.

60 La FIG. 2 es un diagrama de flujo que ilustra un método de procesamiento de información de inicio de sesión, de acuerdo con una implementación de la presente memoria descriptiva. El método se muestra a continuación. La presente solución puede ejecutarse por un cliente de aplicación (que denomina cliente a continuación) que es capaz de procesar la información de inicio de sesión, o un complemento que se ejecuta en un navegador o un servidor. Una forma de implementación del cuerpo de ejecución no está limitada en la implementación de la presente memoria descriptiva.

65

El cliente es un cliente de aplicación que puede implementar la solución técnica registrada en la implementación de la presente memoria descriptiva, y puede ejecutarse en un dispositivo de terminal como un APP.

5 Paso 202: Recibir una solicitud de almacenamiento de información de inicio de sesión enviado por un usuario, donde la solicitud de almacenamiento de información de inicio de sesión incluye un identificador.

10 En la aplicación real, cuando el usuario necesita un servicio de red proporcionada por una determinada plataforma de servicios de Internet, el usuario normalmente necesita iniciar sesión en la plataforma de servicios de Internet. Cuando el usuario inicia sesión en la plataforma de servicio de Internet por primera vez, el usuario necesita registrarse en la plataforma de servicio de Internet, para generar la información de inicio de sesión utilizada por el usuario para iniciar sesión en la plataforma de servicio de Internet.

15 Para que sea más conveniente para el usuario para iniciar sesión en la plataforma de servicios de Internet, posteriormente, el usuario puede enviar la solicitud de almacenamiento de información de inicio de sesión a un dispositivo de procesamiento de información después de obtener la información de inicio de sesión, de modo que el dispositivo de procesamiento de datos procesa la información de inicio de sesión del usuario (el procesamiento aquí puede incluir almacenamiento, consulta, etc.). El dispositivo de procesamiento de información puede ser un dispositivo de procesamiento de información de inicio de sesión, o un dispositivo de procesamiento de información que tiene una capacidad de procesamiento de información de inicio de sesión y también otras capacidades.

20 El identificador registrado en la implementación de la presente memoria descriptiva puede entenderse como la información que es fácil de recordar por el usuario, también después de recibirse el identificador, la información de inicio de sesión de un usuario que proporciona el identificador puede identificarse. El identificador aquí puede ser una contraseña, una imagen, una cadena de caracteres, un código bidimensional, etc., los cual no está limitado. Si el
25 identificador es una contraseña, la contraseña puede consistir en uno o más de un número, un carácter chino, una letra o un símbolo.

30 Además, el identificador registrado en la implementación de la presente memoria descriptiva se puede establecer por el usuario, o se puede establecer por el dispositivo de procesamiento de información o de la plataforma de servicios de Internet para el usuario, lo cual no está limitado aquí.

Paso 204: Determinar la información de inicio de sesión correspondiente al usuario.

35 En la implementación de la presente memoria descriptiva, la información de inicio de sesión correspondiente al usuario puede establecerse por el usuario, o puede generarse automáticamente por el dispositivo de procesamiento de información para el usuario, lo cual no está limitado aquí.

40 Si la información de inicio de sesión correspondiente al usuario se establece por el usuario, determinar la información de inicio de sesión correspondiente al usuario incluye: determinar, como la información de inicio de sesión correspondiente al usuario, información de inicio de sesión incluida en la solicitud de almacenamiento de información de inicio de sesión.

45 Si la solicitud de almacenamiento de información de inicio de sesión no incluye la información de inicio de sesión, después de que el dispositivo de procesamiento de información recibe la solicitud de almacenamiento de información de inicio de sesión enviada por el usuario, la determinación de la información de inicio de sesión correspondiente al usuario incluye: generar información de inicio de sesión para el usuario; y determinar la información de inicio de sesión generada como la información de inicio de sesión correspondiente al usuario.

50 El dispositivo de procesamiento de información genera de forma aleatoria e irregular información de inicio de sesión para diferentes usuarios, de modo que la información de inicio de sesión no se puede descifrar fácilmente, y tiene alta seguridad.

55 La información de inicio de sesión registrada en la implementación de la presente memoria descriptiva puede incluir un nombre de usuario y una contraseña de inicio de sesión que se establecen por el usuario o el dispositivo de procesamiento de información, o puede incluir sólo una contraseña de inicio de sesión que se establece por el usuario o el dispositivo de procesamiento de información. Si la información de inicio de sesión incluye solo la contraseña de inicio de sesión, el usuario generalmente establece un nombre de usuario.

60 Paso 206: Crear, en base a una plantilla de contrato inteligente predeterminado utilizada para el procesamiento de información de inicio de sesión, un contrato inteligente que incluye la información de inicio de sesión.

65 En la implementación de la presente memoria descriptiva, el dispositivo de procesamiento de información genera previamente la plantilla de contrato inteligente utilizada para el procesamiento de información de inicio de sesión. La lógica de procesamiento utilizada para el procesamiento de información de inicio de sesión se registra en la plantilla de contrato inteligente. Para ser específicos, la información de inicio de sesión puede procesarse ejecutando la lógica de procesamiento.

Por ejemplo, la lógica para procesar la información de inicio de sesión puede incluir lógica para almacenar la información de inicio de sesión. La información de inicio de sesión se puede almacenar en una red de cadena de bloques en base a la lógica de almacenamiento.

5 Para dar otro ejemplo, la lógica para procesar la información de inicio de sesión puede incluir lógica para consultar la información de inicio de sesión. La información de inicio de sesión se puede consultar desde una red de cadena de bloques en base a la lógica de consulta.

10 Para dar otro ejemplo más, la lógica para procesar la información de inicio de sesión puede incluir lógica para actualizar o eliminar la información de inicio de sesión. La información de inicio de sesión almacenada se puede actualizar en base a la lógica de actualización, y la información de inicio de sesión almacenada se puede eliminar en base a la lógica de eliminación.

15 En particular, la actualización y eliminación aquí pueden entenderse como generar datos de servicios relacionados para actualizar en la red de cadena de bloques (para ser específicos, en la red de cadena de bloques se almacenan tanta información de inicio de sesión a ser actualizada e información de inicio de sesión actualizada) y generar datos de servicio relacionados con la eliminación.

20 En la implementación de la presente memoria descriptiva, la plantilla de contrato inteligente predeterminada utilizada para el procesamiento de información de inicio de sesión se puede almacenar en el dispositivo de procesamiento de información, o se pueden almacenar en la red de cadena de bloques, lo cual no está limitado aquí.

25 Si la plantilla de contrato inteligente se almacena en el dispositivo de procesamiento de información, después de determinar la información de inicio de sesión correspondiente al usuario, el dispositivo de procesamiento de información invoca la plantilla de contrato inteligente, y crea el contrato inteligente que incluye la información de inicio de sesión correspondiente al usuario. Si la plantilla de contrato inteligente se almacena en la red de cadena de bloques (para ser específicos, el dispositivo de procesamiento de información crea la plantilla de contrato inteligente en la red de cadena de bloques negociando con la red de cadena de bloques. En otras palabras, la red de cadena de bloques
30 asigna una dirección de almacenamiento fija a la plantilla de contrato inteligente, y almacena la plantilla de contrato inteligente en la red de cadena de bloques en base a la dirección de almacenamiento fija, y el dispositivo de procesamiento de información puede obtener la plantilla de contrato inteligente en base a la dirección de almacenamiento fija), después de determinar la información de inicio de sesión correspondiente al usuario, el dispositivo de procesamiento de información invoca la plantilla de contrato inteligente desde la red de cadena de bloques y crea el contrato inteligente que incluye la información de inicio de sesión correspondiente al usuario.
35

Para mejorar la seguridad de la información de inicio de sesión, el contrato inteligente puede crearse en base a la información de inicio de sesión cifrada. En la implementación de la presente memoria descriptiva, la creación de un contrato inteligente que incluye la información de inicio de sesión puede incluir: procesar el identificador para obtener un par de claves públicas-privadas; cifrar la información de inicio de sesión utilizando una clave pública en el par de claves públicas-privadas; y crear, en base a la plantilla de contrato inteligente predeterminada utilizada para el procesamiento de información de inicio de sesión, un contrato inteligente que incluye la información de inicio de sesión cifrada.
40

45 El procesamiento del identificador para obtener un par de claves privadas-públicas puede incluir: convertir el identificador en un código de bytes en base a una regla de conversión, por ejemplo, seleccionar un código binario como el código de bytes; y generar el par de claves públicas-privadas utilizando el código de bytes en base a la lógica de cálculo, donde el par de claves públicas-privadas está formado por una clave pública y una clave privada, la clave pública se utiliza para cifrar la información de inicio de sesión, y la clave privada se puede utilizar para descifrar la información de inicio de sesión cifrada.
50

Cuando se crea el contrato inteligente para la información de inicio de sesión, si la solicitud de almacenamiento de información de inicio de sesión incluye información de identificación, se crea un contrato inteligente que incluye la información de identificación y la información de inicio de sesión.
55

La información de identificación aquí puede entenderse como la información de identificación de la plataforma de servicios de Internet.

60 Paso 208: Almacenar el contrato inteligente creado en una red de cadena de bloques en base al identificador.

En la implementación de la presente memoria descriptiva, el almacenamiento del contrato inteligente creado en una red de cadena de bloques en base al identificador puede incluir: determinar una dirección de almacenamiento del contrato inteligente en la red de cadena de bloques en base al identificador; y almacenar el contrato inteligente en la red de cadena de bloques en base a la dirección de almacenamiento.
65

5 En la implementación de la presente memoria descriptiva, la determinación de una dirección de almacenamiento del contrato inteligente en la red de cadena de bloques en base al identificador incluye: procesar el identificador para obtener un par de claves públicas-privadas; obtener una primera dirección a través del cálculo en base a una clave pública incluida en el par de claves públicas-privadas; obtener una segunda dirección en base a la primera dirección, donde la segunda dirección se determina en la red de cadena de bloques en base a un evento de transacción especificado iniciado en la primera dirección; y determinar la segunda dirección como la dirección de almacenamiento del contrato inteligente en la red de cadena de bloques.

10 El evento de transacción especificado registrado en la implementación de la presente memoria descriptiva se puede entender como una transacción. Por ejemplo, en la red Ethereum, para obtener la dirección de almacenamiento del contrato inteligente, se debe pagar una cantidad particular de Ether a la red Ethereum. Para ser específicos, cuando se genera una transacción en la red Ethereum, una dirección de origen de la transacción puede ser la primera dirección, y una dirección de destino de la transacción puede denominarse la segunda dirección (la segunda dirección aquí puede asignarse en la red Ethereum). Una vez que se completa la transacción entre la primera dirección y la segunda dirección, el espacio de almacenamiento correspondiente a la segunda dirección se puede utilizar para almacenar el contrato inteligente creado para el usuario. En esta situación, la segunda dirección también puede denominarse la dirección de almacenamiento del contrato inteligente.

20 Consultar el procesamiento del identificador para obtener un par de claves públicas-privadas en el paso 206. Los detalles no se describen aquí. La obtención de una primera dirección a través del cálculo en base a una clave pública incluida en el par de claves públicas-privadas incluye: calcular, en base a un algoritmo especificado, la clave pública incluida en el par de claves públicas-privadas, para obtener la primera dirección, que incluye: calcular la clave pública en base a un algoritmo hash, para obtener un valor hash de una longitud fija, donde el valor hash es la primera dirección.

25 En base al método de procesamiento de información de inicio de sesión proporcionado en la implementación de la presente memoria descriptiva, se puede crear un contrato inteligente que incluye información de inicio de sesión de un determinado usuario, y el contrato inteligente se almacena en una red de cadena de bloques, de modo que la seguridad de almacenamiento de la información de inicio de sesión del usuario se mejora efectivamente. Esto se implementa en base a la red de cadena de bloques, de modo que es menos probable que la información de inicio de sesión se pierda, robe o manipule, y se mejora la seguridad de almacenamiento de la información de inicio de sesión.

30 La FIG. 3 es un diagrama de flujo que ilustra un método de procesamiento de información de inicio de sesión, de acuerdo con una implementación de la presente memoria descriptiva. El método se muestra a continuación. La presente solución puede ejecutarse por un cliente de aplicación (que se denomina cliente a continuación) con una capacidad de procesamiento de información de inicio de sesión, o un complemento que se ejecuta en un navegador o un servidor. Una forma de implementación del cuerpo de ejecución no está limitada en la implementación de la presente memoria descriptiva.

40 Paso 301: Recibir una solicitud de consulta de información de inicio de sesión que se envía por un usuario y que incluye un identificador.

45 En la implementación de la presente memoria descriptiva, al iniciar sesión en una plataforma de servicios de Internet, el usuario puede enviar la solicitud de consulta información de inicio de sesión a un dispositivo de procesamiento de información, para obtener la información de inicio de sesión necesaria. Cuando el usuario necesita la información de inicio de sesión, el usuario puede enviar la solicitud de consulta de información de inicio de sesión a un dispositivo de procesamiento de información, para obtener la información de inicio de sesión necesaria. El escenario de uso para enviar la solicitud de consulta de información de inicio de sesión mediante el usuario no está limitado aquí.

50 Para el contenido del identificador, consultar el contenido asociado registrado en la implementación descrita. Los detalles no se describen aquí.

Paso 303: Leer, desde una red de cadena de bloques en base al identificador, un contrato inteligente utilizado para el procesamiento de información de inicio de sesión.

55 En la implementación de la presente memoria descriptiva, una dirección de almacenamiento del contrato inteligente utilizada para el procesamiento de información de inicio de sesión primero se determina en base al identificador.

60 El identificador se procesa para obtener un par de claves privadas-públicas. Se obtiene una primera dirección a través del cálculo en base a una clave pública incluida en el par de claves públicas-privadas. Al menos una segunda dirección que realiza una transacción con la primera dirección se determina en base a la primera dirección. La dirección de almacenamiento del contrato inteligente se identifica a partir de la segunda dirección.

65 En la implementación de la presente memoria descriptiva, para el procesamiento el identificador para obtener un par de claves privadas-públicas, consultar el contenido en el paso 208. Los detalles no se describen aquí.

La obtención de una primera dirección a través del cálculo en base a una clave pública incluida en el par de claves públicas-privadas incluye: calcular, en base a un algoritmo especificado, la clave pública incluida en el par de claves públicas-privadas, para obtener la primera dirección.

5 En la implementación de la presente memoria descriptiva, la dirección de almacenamiento del contrato inteligente se puede determinar utilizando un evento de transacción especificado. Después de producirse el evento de transacción, los datos de transacción correspondientes al evento de transacción se almacenan en la red de cadena de bloques. Como tal, la primera dirección puede utilizarse como una palabra clave de consulta, los datos de transacción, incluida la primera dirección, se consultan en la red de cadena de bloques, y la al menos una segunda dirección se lee de los
10 datos de transacción.

Para el mismo usuario, debido a que la primera dirección se determina en base al identificador proporcionado por el usuario, no puede haber uno o más datos de transacción que incluyen la primera dirección, y cada uno de los datos de transacción incluye la segunda dirección. Por lo tanto, la al menos una segunda dirección se puede determinar en
15 base a la primera dirección.

La identificación de la dirección de almacenamiento del contrato inteligente a partir de la segunda direcciones puede incluir: si se determina que hay una segunda dirección haciendo una transacción con la primera dirección, determinar la segunda dirección como la dirección de almacenamiento del contrato inteligente; o si se determina que hay más de
20 una segunda dirección haciendo una transacción con la primera dirección, buscar una segunda dirección en la que se almacena el contrato inteligente y determinar la segunda dirección identificada como la dirección de almacenamiento del contrato inteligente. En esta situación, puede haber una o más direcciones de almacenamiento del contrato inteligente.

25 El contenido inteligente se lee entonces, desde la red de cadena de bloques en base a la dirección de almacenamiento.

Si se lee un contrato inteligente desde la red de cadena de bloques, se determina que el contrato inteligente es un contrato inteligente correspondiente al usuario.

30 Si se lee más de un contrato inteligente desde la red de cadena de bloques, se selecciona un contrato inteligente que satisfaga una condición especificada de los contratos inteligentes leídos.

En la implementación de la presente memoria descriptiva, la selección, a partir de los contratos inteligentes leídos, de un contrato inteligente que satisface una condición especificada incluye: seleccionar, a partir de los contratos inteligentes leídos en base a la información de identificación incluida en contrato inteligente leído, un contrato inteligente con la misma información de identificación que la información de identificación incluida en la solicitud de consulta de información de inicio de sesión.

40 Paso 305: Ejecutar el contrato inteligente para obtener la información de inicio de sesión correspondiente al usuario.

En la implementación de la presente memoria descriptiva, el contrato inteligente se ejecuta para obtener al menos una información de inicio de sesión.

45 La al menos una información de inicio de sesión se envía al usuario, de modo que el usuario confirma la información de inicio de sesión que satisface una necesidad del usuario.

En la implementación de la presente memoria descriptiva, se puede almacenar una o más información de inicio de sesión en el contrato inteligente.

50 Si una información de inicio de sesión se obtiene ejecutando el contrato inteligente, se puede determinar que la información de inicio de sesión satisface la necesidad del usuario, y la información de inicio de sesión se envía directamente al usuario.

55 Si se obtiene más de una información de inicio de sesión ejecutando el contrato inteligente, la información de inicio de sesión se puede enviar al usuario para la confirmación.

Alternativamente, cuando la información de inicio de sesión incluye información de identificación, la información de identificación se analiza a partir de cada una de las informaciones de inicio de sesión, con el fin de seleccionar la información de inicio de sesión con la misma información de identificación que la información de identificación incluida en la solicitud de consulta de información de inicio de sesión, y determinar que la información de inicio de sesión seleccionada satisface las necesidades del usuario.

60 La información de inicio de sesión almacenada en el contrato inteligente puede estar descifrada o cifrada. Para la información de inicio de sesión cifrada, la ejecución de un contrato inteligente para obtener la información de inicio de sesión correspondiente al usuario incluye: ejecutar el contrato inteligente para obtener la información de inicio de
65 sesión correspondiente al usuario incluye: ejecutar el contrato inteligente para obtener la información de inicio de

sesión cifrada; y descifrar la información de inicio de sesión cifrada para obtener la información de inicio de sesión correspondiente al usuario.

5 El descifrado de la información de inicio de sesión cifrada incluye: procesar el identificador para obtener un par de claves privadas-públicas; y descifrar la información de inicio de sesión cifrada utilizando una clave privada en el par de claves privadas-públicas.

10 En base a una implementación en el paso 206, el par de claves públicas-privadas se genera utilizando el identificador, y la información de inicio de sesión se cifra usando una clave pública en el par de claves públicas-privadas. En el presente paso, la información de inicio de sesión cifrada utilizando la clave pública se puede descifrar utilizando la clave privada en el par de claves públicas-privadas.

15 El texto plano de la información de inicio de sesión obtenida se envía al usuario, y el usuario puede utilizar la información de inicio de sesión para completar el inicio de sesión.

20 En la implementación de la presente memoria descriptiva, el usuario puede enviar, además, una solicitud de procesamiento de información de inicio de sesión al dispositivo de procesamiento de información. En esta situación, después de obtener la información de inicio de sesión, el método de procesamiento de información de inicio de sesión incluye además: procesar la información de inicio de sesión en base a una solicitud de procesamiento recibida; y si la solicitud de procesamiento recibida es una solicitud de actualización, actualizar la información de inicio de sesión y almacenar la información de inicio de sesión actualizada en la red de cadena de bloques; o si la solicitud de procesamiento recibida es una solicitud de eliminación, eliminar la información de inicio de sesión de la red de cadena de bloques.

25 En base al método de procesamiento de información de inicio de sesión proporcionado en la implementación de la presente memoria descriptiva, cuando un usuario necesita la información de inicio de sesión, el usuario puede obtener rápidamente la información de inicio de sesión necesaria desde una red de cadena de bloques a través de consulta, haciendo que sea conveniente para el usuario mantener la información de inicio de sesión.

30 La FIG. 4 es un diagrama estructural que ilustra un dispositivo de procesamiento de información de inicio de sesión, de acuerdo con una implementación de la presente memoria descriptiva. El dispositivo de procesamiento de información de inicio de sesión incluye: un módulo 41 de recepción, configurado para recibir una solicitud de consulta de información de inicio de sesión que se envía por un usuario, donde la solicitud incluye un identificador; un módulo 42 de lectura, configurado para leer, de una red de cadena de bloques en base al identificador, un contrato inteligente utilizado para el procesamiento de información de inicio de sesión; y un módulo 43 de procesamiento, configurado para ejecutar el contrato inteligente para obtener información de inicio de sesión correspondiente al usuario.

35 Opcionalmente, el módulo 42 de lectura está configurado para: determinar, en base al identificador, una dirección de almacenamiento del contrato inteligente que se utiliza para el procesamiento de información de inicio de sesión; y leer el contrato inteligente desde la red de cadena de bloques en base a la dirección de almacenamiento.

45 Opcionalmente, el módulo 42 de lectura está configurado para: procesar el identificador para obtener un par de claves privadas-públicas; obtener una primera dirección a través del cálculo en base a una clave pública incluida en el par de claves públicas-privadas; determinar, en base a la primera dirección, al menos una segunda dirección haciendo una transacción con la primera dirección; e identificar la dirección de almacenamiento del contrato inteligente a partir de las segundas direcciones.

50 Opcionalmente, el módulo 42 de lectura está configurado para: calcular, en base a un algoritmo especificado, la clave pública incluida en el par de claves públicas-privadas, para obtener la primera dirección.

Opcionalmente, el módulo 42 de lectura está configurado para: si se lee más de un contrato inteligente desde la red de cadena de bloques, seleccionar, a partir de los contratos inteligentes leídos, un contrato inteligente que satisface una condición especificada.

55 Opcionalmente, el módulo 42 de lectura está configurado para: seleccionar, de la información de identificación incluida en los contratos inteligentes leídos, un contrato inteligente con la misma información de identificación que la información de identificación incluida en la solicitud de consulta de información de inicio de sesión.

60 Opcionalmente, el módulo 43 de procesamiento está configurado para: ejecutar el contrato inteligente para obtener al menos una información de inicio de sesión correspondiente a un usuario; y enviar la al menos una información de inicio de sesión al usuario, de modo que el usuario confirme que la información de inicio de sesión ha satisfecho una necesidad del usuario.

65 Opcionalmente, el módulo 43 de procesamiento está configurado para: ejecutar el contrato inteligente para obtener información de inicio de sesión cifrada correspondiente a un usuario; y descifrar la información de inicio de sesión cifrada para obtener la información de inicio de sesión correspondiente al usuario.

Opcionalmente, el módulo 43 de procesamiento está configurado para: procesar el identificador para obtener un par de claves privadas-públicas; y descifrar la información de inicio de sesión cifrada utilizando una clave privada en el par de claves privadas-públicas.

5 Opcionalmente, después de obtener la información de inicio de sesión, el módulo 43 de procesamiento procesa la información de inicio de sesión en base a una solicitud de procesamiento recibida.

10 Opcionalmente, el módulo 43 de procesamiento está configurado para: si la solicitud de procesamiento recibida es una solicitud de actualización, actualizar la información de inicio de sesión, y almacenar la información de inicio de sesión actualizada en la red de cadena de bloques.

15 Opcionalmente, el módulo 43 de procesamiento está configurado para: si la solicitud de procesamiento recibida es una solicitud de eliminación, eliminar la información de inicio de sesión de la red de cadena de bloques.

En particular, el dispositivo de procesamiento de información de inicio de sesión registrado en la implementación de la presente memoria descriptiva puede implementarse utilizando software o hardware, lo cual no está limitado aquí.

20 Como tal, el usuario puede consultar la información de inicio de sesión desde la red de cadena de bloques utilizando el dispositivo de procesamiento de información de inicio de sesión, y procesar además la información de inicio de sesión. El dispositivo de procesamiento de información de inicio de sesión (que puede denominarse dispositivo de procesamiento de información para abreviar) puede tener una única función de procesamiento de información de inicio de sesión, o puede tener otras funciones de procesamiento de información además de una función de procesamiento de información de inicio de sesión.

25 En base al mismo concepto de divulgación, una implementación de la presente memoria descriptiva proporciona además un dispositivo de procesamiento de información de inicio de sesión. El dispositivo de procesamiento de información de inicio de sesión incluye al menos un procesador y una memoria. La memoria almacena un programa y el al menos un procesador está configurado para realizar los siguientes pasos: recibir una solicitud de consulta de información de inicio de sesión que se envía por un usuario y que incluye un identificador; leer, desde una red de cadena de bloques en base al identificador, un contrato inteligente utilizado para el procesamiento de información de inicio de sesión; y ejecutar el contrato inteligente para obtener la información de inicio de sesión correspondiente al usuario.

30 Para otra función del procesador, consultar el contenido registrado en la implementación descrita anteriormente. Los detalles no se describen aquí.

35 En base al mismo concepto de divulgación, una implementación de la presente memoria descriptiva proporciona además un medio de almacenamiento legible por computadora. El medio de almacenamiento legible por computadora incluye un programa utilizado en combinación con un dispositivo electrónico y un procesador puede ejecutar el programa para realizar los siguientes pasos: recibir una solicitud de consulta de información de inicio de sesión que se envía por un usuario y que incluye un identificador; leer, desde una red de cadena de bloques en base al identificador, un contrato inteligente utilizado para el procesamiento de información de inicio de sesión; y ejecutar el contrato inteligente para obtener la información de inicio de sesión correspondiente al usuario.

40 Para otra función del procesador, consultar el contenido registrado en la implementación descrita anteriormente. Los detalles no se describen aquí.

45 Como tal, el medio de almacenamiento legible por computadora proporciona un portador de un método para consultar la información de inicio de sesión desde la red de cadena de bloques.

50 La FIG. 5 es un diagrama estructural que ilustra un dispositivo de procesamiento de información de inicio de sesión, de acuerdo con una implementación de la presente memoria descriptiva. El dispositivo de procesamiento de información de inicio de sesión incluye: un módulo 51 de recepción, configurado para recibir una solicitud de almacenamiento de información de inicio de sesión enviada por un usuario, donde la solicitud de almacenamiento de información de inicio de sesión incluye un identificador; un módulo 52 de determinación, configurado para determinar la información de inicio de sesión correspondiente al usuario; un módulo 53 de creación, configurado para crear, en base a una plantilla de contrato inteligente predeterminada utilizada para el procesamiento de información de inicio de sesión, un contrato inteligente que incluye la información de inicio de sesión; y un módulo 54 de almacenamiento, configurado para almacenar el contrato inteligente creado en una red de cadena de bloques en base al identificador.

55 Opcionalmente, el módulo 52 de determinación está configurado para: generar información de inicio de sesión para el usuario; y determinar la información de inicio de sesión generada como la información de inicio de sesión correspondiente al usuario.

60

Opcionalmente, el módulo 52 de determinación está configurado para: determinar, como la información de inicio de sesión correspondiente al usuario, información de inicio de sesión incluida en la solicitud de almacenamiento de información de inicio de sesión.

5 Opcionalmente, el módulo 54 de almacenamiento está configurado para: determinar una dirección de almacenamiento del contrato inteligente en la red de cadena de bloques en base al identificador; y almacenar el contrato inteligente en la red de cadena de bloques en base a la dirección de almacenamiento.

10 Opcionalmente, el módulo 54 de almacenamiento está configurado para: procesar el identificador para obtener un par de claves públicas-privadas; obtener una primera dirección a través del cálculo en base a una clave pública incluida en el par de claves públicas-privadas; obtener una segunda dirección en base a la primera dirección, donde la segunda dirección se determina en la red de cadena de bloques en base a un evento de transacción especificado iniciado en la primera dirección; y determinar la segunda dirección como la dirección de almacenamiento del contrato inteligente en la red de cadena de bloques.

15 Opcionalmente, el módulo 54 de almacenamiento está configurado para: calcular, en base a un algoritmo especificado, la clave pública incluida en el par de claves públicas-privadas, para obtener la primera dirección.

20 Opcionalmente, el módulo 53 de creación está configurado para: procesar el identificador para obtener un par de claves públicas-privadas; cifrar la información de inicio de sesión utilizando una clave pública en el par de claves públicas-privadas; y crear, en base a la plantilla de contrato inteligente predeterminada utilizada para el procesamiento de información de inicio de sesión, un contrato inteligente que incluye la información de inicio de sesión cifrada.

25 En particular, el dispositivo de procesamiento de información de inicio de sesión registrado en la implementación de la presente memoria descriptiva puede implementarse utilizando software o hardware, lo cual no está limitado aquí.

30 Como tal, el usuario puede almacenar la información de inicio de sesión en la red de cadena de bloques utilizando el dispositivo de procesamiento de información de inicio de sesión. El dispositivo de procesamiento de información de inicio de sesión puede tener una única función de procesamiento de información de inicio de sesión, o puede tener otras funciones de procesamiento de información además de una función de procesamiento de información de inicio de sesión.

35 En base al mismo concepto de divulgación, una implementación de la presente memoria descriptiva proporciona además un dispositivo de procesamiento de información de inicio de sesión. El dispositivo de procesamiento de información de inicio de sesión incluye al menos un procesador y una memoria. La memoria almacena un programa, y el al menos un procesador está configurado para realizar los siguientes pasos: recibir una solicitud de almacenamiento de información de inicio de sesión enviada por un usuario, donde la solicitud de almacenamiento de información de inicio de sesión incluye un identificador; determinar la información de inicio de sesión correspondiente al usuario; crear, en base a una plantilla de contrato inteligente predeterminada utilizada para el procesamiento de información de inicio de sesión, un contrato inteligente que incluye la información de inicio de sesión; y almacenar el contrato inteligente creado en una red de cadena de bloques en base al identificador.

40 Para otra función del procesador, consultar el contenido registrado en la implementación descrita. Los detalles no se describen aquí.

45 En base al mismo concepto de divulgación, una implementación de la presente memoria descriptiva proporciona además un medio de almacenamiento legible por computadora. El medio de almacenamiento legible por computadora incluye un programa utilizado en combinación con un dispositivo electrónico, y un procesador puede ejecutar el programa para realizar los siguientes pasos: recibir una solicitud de almacenamiento de información de inicio de sesión enviada por un usuario, donde la solicitud de almacenamiento de información de inicio de sesión incluye un identificador; determinar la información de inicio de sesión correspondiente al usuario; crear, en base a una plantilla de contrato inteligente predeterminada utilizada para el procesamiento de información de inicio de sesión, un contrato inteligente que incluye la información de inicio de sesión; y almacenar el contrato inteligente creado en una red de cadena de bloques en base al identificador.

50 Para otra función del procesador, consultar el contenido registrado en la implementación descrita. Los detalles no se describen aquí.

55 Como tal, el usuario puede almacenar la información de inicio de sesión en la red de cadena de bloques a través de la interacción con el dispositivo de procesamiento de información de inicio de sesión o el medio de almacenamiento legible por computadora.

60 En la década de 1990, la mejora de una tecnología se puede distinguir claramente entre la mejora del hardware (por ejemplo, la mejora en una estructura de circuito tal como un diodo, un transistor o un interruptor) y la mejora del software (mejora en un procedimiento de método). Sin embargo, con el desarrollo de tecnologías, la mejora de muchos procesos de método puede considerarse como una mejora directa de una estructura de circuito de hardware. Casi

65

5 todos los diseñadores programan un procedimiento de método mejorado para un circuito de hardware, para obtener una correspondiente estructura de circuito de hardware. Por lo tanto, no se puede decir que una mejora de un procedimiento de método no se puede implementar 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
 10 circuito integrado de este tipo. Una función lógica del dispositivo lógico programable está determinada por la programación del componente ejecutado por un usuario. Los diseñadores realizan una programación voluntaria para "integrar" un sistema digital en un único PLD sin requerir que un fabricante de chips diseñe y produzca un chip de circuito integrado dedicado. Además, en lugar de producir manualmente un chip de circuito integrado, la programación se implementa principalmente mediante el software "compilador lógico", que es similar a un compilador de software
 15 utilizado durante el desarrollo del programa. El código original antes de la compilación también está escrito en un lenguaje de programación específico, que se conoce como lenguaje de descripción de hardware (HDL), y hay más de un tipo de HDL, tal como un ABEL (Advanced Boolean Expression Language), un AHDL (Lenguaje de descripción de hardware de Altera), Confluence, un CUPL (lenguaje de programación de la Universidad de Cornell), HDCal, JHDL (lenguaje de descripción de hardware Java), un Lava, un Lola, un MyHDL, un PALASM, un RHDL (lenguaje de descripción de hardware Ruby), etc. Actualmente, VHDL (lenguaje de descripción de hardware de circuito integrado de muy alta velocidad) y Verilog son los más utilizados. Un experto en la técnica también debe comprender que un procedimiento de método solo necesita programarse lógicamente y programarse en el circuito integrado utilizando los lenguajes de descripción de hardware anteriores, de modo que se pueda obtener fácilmente un circuito de hardware que implemente el proceso de método lógico.

20 Se puede implementar un controlador utilizando cualquier método apropiado. Por ejemplo, el controlador puede ser un microprocesador o un procesador, o un medio legible por computadora, una puerta lógica, un interruptor, un circuito integrado de aplicación específica (ASIC), un controlador lógico programable o un microprocesador integrado que almacena código de programa legible por computadora (tal como software o firmware) que puede ejecutarse por el
 25 microprocesador o el procesador. Los ejemplos del controlador incluyen, entre otros, los siguientes microprocesadores: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20 y Silicone Labs C8051F320. El controlador de memoria también se puede implementar como parte de la lógica de control de la memoria. Un experto en la técnica también sabe que un controlador puede implementarse de una manera de código de programa puro legible por computadora, y los pasos del método pueden programarse lógicamente para permitir que el controlador implemente además las mismas
 30 funciones en forma de una puerta lógica, un interruptor, un circuito integrado de aplicación específica, un controlador lógico programable, un microcontrolador incorporado, etc. Por lo tanto, el controlador puede considerarse como un componente de hardware y un aparato que está incluido en el controlador y que está configurado para implementar diversas funciones también se puede considerar como una estructura en el componente de hardware. Alternativamente, un aparato configurado para implementar diversas funciones puede considerarse tanto un módulo de software para implementar el método y una estructura en el componente de hardware.

35 El sistema, aparato, módulo o unidad descritos en las implementaciones descritas pueden implementarse mediante un chip de computadora o una entidad, o implementarse mediante un producto con una determinada función. Un dispositivo de implementación típico es una computadora. 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, o un dispositivo ponible, o una combinación de cualquiera de estos dispositivos.

45 Para facilitar la descripción, el aparato descrito se describe dividiendo las funciones en diversas unidades. Ciertamente, cuando se implementa la presente solicitud, las funciones de las unidades se pueden implementar en una o más piezas de software y/o hardware.

50 Un experto en la técnica debería comprender que las implementaciones de la presente divulgación se pueden proporcionar como un método, un sistema o un producto de programa informático. Por lo tanto, la presente divulgación puede utilizar una forma de implementaciones solo de hardware, implementaciones solo de software o implementaciones con una combinación de software y hardware. Además, la presente divulgación puede utilizar una forma de un producto de programa informático que se implementa en uno o más medios de almacenamiento utilizables por computadora (que incluyen, entre otros, una memoria de disco, un CD-ROM, una memoria óptica, etc.) que incluye
 55 código de programa utilizable por computadora.

60 La presente descripción se describe con referencia a los diagramas de flujo y/o diagramas de bloques del método, el dispositivo (sistema), y el producto de programa informático de acuerdo con las implementaciones de la presente divulgación. Debe entenderse que las instrucciones de programa informático pueden utilizarse para implementar cada uno de los procesos y/o cada uno de los bloques en los diagramas de flujo y/o los diagramas de bloques y una combinación de un proceso y/o un bloque en los diagramas de flujo y/o los diagramas de bloques. Estas instrucciones de programa de computadora se pueden proporcionar para una computadora de propósito general, una computadora dedicada, 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
 65 procesador de cualquier otro dispositivo de procesamiento de datos programable generan un aparato para

implementar una función específica en uno o más procesos en los diagramas de flujo o en uno o más bloques en los diagramas de bloques.

5 Estas instrucciones de programa informático 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 específica, de modo que las instrucciones almacenadas en la memoria legible por computadora generan un artefacto que incluye un aparato de instrucción. El aparato de instrucción implementa 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.

10 Estas instrucciones de programa informático pueden cargarse en una computadora u otro dispositivo de procesamiento de datos programable, de modo que se realicen una serie de operaciones y pasos en la computadora o el otro dispositivo programable, generando así el procesamiento implementado por computadora. Por lo tanto, las instrucciones ejecutadas en la computadora o el otro dispositivo programable proporcionan pasos para implementar una función específica en uno o más procesos en los diagramas de flujo o en uno o más bloques en los diagramas de bloques.

15 En la configuración típica, el dispositivo informático incluye una o más unidades centrales de procesamiento (CPU), una interfaz de entrada/salida, una interfaz de red y una memoria.

20 La memoria puede incluir una forma de una memoria volátil, una memoria de acceso aleatorio (RAM) y/o una memoria no volátil, etc. en un medio legible por computadora, tal como una memoria de solo lectura (ROM) o una memoria flash (RAM flash). La memoria es un ejemplo del medio legible por computadora.

25 El medio legible por computadora incluye medios volátiles y no volátiles, extraíbles y no extraíbles, y puede almacenar información utilizando cualquier método o tecnología. La información puede ser una instrucción legible por computadora, una estructura de datos, un módulo de programa u otros datos. Un medio de almacenamiento de computadora incluye, entre otros, una memoria de acceso aleatorio de parámetros (PRAM), una memoria estática de acceso aleatorio (SRAM), una memoria dinámica de acceso aleatorio (DRAM), una memoria de acceso aleatorio (RAM) de otro tipo, una memoria de solo lectura (ROM), una memoria de solo lectura programable y borrable eléctricamente (EEPROM), una memoria flash u otra tecnología de memoria, una memoria de solo lectura de disco compacto (CD-ROM), un disco versátil digital (DVD) u otro óptico almacenamiento, una cinta magnética, un almacenamiento en disco magnético, otro dispositivo de almacenamiento magnético o cualquier otro medio sin transmisión que pueda utilizarse para almacenar información a la que pueda acceder el dispositivo informático. Como se define en la presente memoria descriptiva, el medio legible por computadora no incluye medios transitorios, por ejemplo, una señal de datos modulada y una portadora.

35 En particular, los términos “incluye”, “contiene”, o sus otras variantes están destinados a cubrir la inclusión no exclusiva, de modo que un proceso, un método, un artículo o un dispositivo que incluye una serie de elementos no solo incluye estos elementos, sino que también incluye otros elementos que no están expresamente listados, o incluye elementos inherentes a dicho proceso, método, artículo o dispositivo. Cuando no hay más restricciones, también es posible que haya otro elemento igual o equivalente en el proceso, el método, un producto o un dispositivo que incluye el elemento.

40 La presente solicitud se puede describir en el contexto general de instrucciones ejecutables por computadora ejecutadas por un computador, tal como un módulo de programa. Generalmente, el módulo de programa incluye una rutina, un programa, un objeto, un componente, una estructura de datos, etc. para ejecutar una tarea específica o implementar un tipo de datos abstracto específico. La presente solicitud también se puede practicar en entornos informáticos distribuidos en los que las tareas se realizan por dispositivos de procesamiento remotos que están conectados utilizando una red de comunicaciones. En un entorno informático distribuido, el módulo de programa puede ubicarse en medios de almacenamiento de computadora locales y remotos que incluyen dispositivos de almacenamiento.

45 Las implementaciones en la presente memoria descriptiva se describen todas de manera progresiva, para las mismas partes o partes similares en las implementaciones, se refieren entre sí, y cada una de las implementaciones se enfoca en una diferencia de otras implementaciones. Particularmente, dado que la implementación de un sistema es similar a la implementación de un método y, por lo tanto, se describe brevemente; y para las partes relevantes, se puede hacer referencia a descripciones parciales de la implementación del método.

50 Las descripciones anteriores son meramente implementaciones de la presente solicitud y no pretenden limitar la presente solicitud. Para un experto en la técnica, la presente solicitud puede tener diversas modificaciones y cambios. Cualquier modificación, reemplazo equivalente, mejora, etc. realizada dentro del espíritu y principio de la presente solicitud caerá dentro del alcance de las reivindicaciones de la presente solicitud.

55 La FIG. 6 es un diagrama de flujo que ilustra un ejemplo de un método 600 implementado por computadora para el procesamiento de datos de información de inicio de sesión, de acuerdo con una implementación de la presente divulgación. Para mayor claridad de presentación, la descripción que sigue describe generalmente el método 600 en el contexto de las otras figuras en esta descripción. Sin embargo, se entenderá que el método 600 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 600 en paralelo, en combinación, en bucles o en cualquier orden.

5 En 602, se crea un contrato inteligente mediante un dispositivo de procesamiento de información en base a una plantilla de contrato inteligente predeterminada. El contrato inteligente creado incluye información de inicio de sesión correspondiente a un usuario. La información de inicio de sesión se determina en base a una solicitud de almacenamiento de información de inicio de sesión enviada por el usuario, y la solicitud de almacenamiento de información de inicio de sesión incluye un identificador. En algunas implementaciones, el dispositivo de procesamiento de información puede ser un cliente de aplicación capaz de procesar información de inicio de sesión. El cliente de aplicación puede implementar la solución técnica registrada en la implementación de la presente memoria descriptiva y puede ejecutarse en un dispositivo terminal como una APP. En algunas implementaciones, el dispositivo de procesamiento de información también puede ser un complemento que se ejecuta un navegador o un servidor.

15 Cuando un usuario necesita un servicio de red proporcionado por una determinada plataforma de servicio de Internet, el usuario generalmente necesita iniciar sesión en la plataforma de servicio de Internet. Cuando el usuario inicia sesión en la plataforma de servicio de Internet por primera vez, el usuario necesita registrarse en la plataforma de servicio de Internet, para generar la información de inicio de sesión utilizada por el usuario para iniciar sesión en la plataforma de servicio de Internet. Para que sea conveniente para que el usuario inicie sesión en la plataforma de servicios de Internet, el usuario puede enviar una solicitud de almacenamiento de información de inicio de sesión a un dispositivo de procesamiento de información después de obtener la información de inicio de sesión, de modo que el dispositivo de procesamiento de información procesa la información de inicio de sesión (por ejemplo, almacenamiento o consulta). El dispositivo de procesamiento de información puede ser un dispositivo de procesamiento de información de inicio de sesión o un dispositivo de procesamiento de información que tiene una capacidad de procesamiento de información de inicio de sesión y otras capacidades consistentes con esta divulgación.

20 En algunas implementaciones, la información de inicio de sesión correspondiente a un usuario se puede establecer por el usuario, o puede generarse automáticamente por el dispositivo de procesamiento de información para el usuario. El dispositivo de procesamiento de información puede, de forma aleatoria, generar información de inicio de sesión para diferentes usuarios, de modo que la información de inicio de sesión es segura y no puede determinarse fácilmente.

25 Un identificador registrado es información que un usuario puede recordar fácilmente. Después de recibir el identificador, se puede identificar la información de inicio de sesión de un usuario que proporciona el identificador. En algunas implementaciones, el identificador puede ser, entre otros, una contraseña, una imagen, una cadena de caracteres o un código bidimensional. Si el identificador es una contraseña, la contraseña puede incluir uno o más de un número, un carácter chino, una letra o un símbolo. Además, el identificador registrado puede establecerse para el usuario mediante el usuario, el dispositivo de procesamiento de información o la plataforma de servicio de Internet para el usuario.

35 En algunas implementaciones, el dispositivo de procesamiento de información puede generar previamente la plantilla de contrato inteligente utilizada para el procesamiento de información de inicio de sesión. La lógica de procesamiento utilizada para el procesamiento de información de inicio de sesión se registra en la plantilla de contrato inteligente. Específicamente, la información de inicio de sesión puede procesarse ejecutando la lógica de procesamiento. Por ejemplo, la lógica para procesar la información de inicio de sesión puede incluir lógica para almacenar la información de inicio de sesión. La información de inicio de sesión se puede almacenar en una red de cadena de bloques en base a la lógica de almacenamiento. En otro ejemplo, la lógica para procesar la información de inicio de sesión puede incluir lógica para consultar la información de inicio de sesión. La información de inicio de sesión se puede consultar desde una red de cadena de bloques en base a la lógica de consulta. En otro ejemplo más, la lógica para procesar la información de inicio de sesión puede incluir lógica para actualizar o eliminar la información de inicio de sesión. La información de inicio de sesión almacenada se puede eliminar en base a la lógica de actualización, y la información de inicio de sesión almacenada se puede eliminar en base a la lógica de eliminación. Se puede entender que la actualización y eliminación generan datos de servicio relacionados con la actualización en la red de cadena de bloques (por ejemplo, en la red de cadena de bloques se almacenan información de inicio de sesión a ser actualizada e información de inicio de sesión actualizada) y generan datos de servicio relacionados con la eliminación.

40 En algunas implementaciones, la plantilla de contrato inteligente predeterminada utilizada para el procesamiento de información de inicio de sesión se puede almacenar en el dispositivo de procesamiento de información. En algunas implementaciones, la plantilla de contrato inteligente predeterminada puede ser o puede almacenarse en, la red de cadena de bloques. El dispositivo de procesamiento de información crea la plantilla de contrato inteligente en la red de cadena de bloques al negociar con la red de cadena de bloques. La red de cadena de bloques asigna una dirección de almacenamiento fija a la plantilla de contrato inteligente y almacena la plantilla de contrato inteligente en la red de cadena de bloques en base a la dirección de almacenamiento fija. El dispositivo de procesamiento de información puede obtener la plantilla de contrato inteligente en base a la dirección de almacenamiento fija.

50 En algunas implementaciones, para mejorar la seguridad de la información de inicio de sesión, el contrato inteligente se puede crear en base a información de inicio de sesión cifrada. Por ejemplo, crear un contrato inteligente que incluye

la información de inicio de sesión puede incluir: procesar el identificador para obtener un par de claves públicas-privadas; cifrar la información de inicio de sesión utilizando una clave pública en el par de claves públicas-privadas; y crear, en base a la plantilla de contrato inteligente predeterminada utilizada para el procesamiento de información de inicio de sesión, un contrato inteligente que incluye la información de inicio de sesión cifrada. En algunas implementaciones, procesar el identificador para obtener un par de claves públicas-privadas puede incluir: convertir el identificador en un código de bytes en base a una regla de conversión, por ejemplo, seleccionar un código binario como código de bytes; y generar el par de claves públicas-privadas utilizando el código de bytes en base a la lógica de cálculo, donde el par de claves públicas-privadas está formado por una clave pública y una clave privada, la clave pública se utiliza para cifrar la información de inicio de sesión y la clave privada se puede utilizar para descifrar la información de inicio de sesión cifrada.

En algunas implementaciones, si la solicitud de almacenamiento de información de inicio de sesión incluye información de identificación (por ejemplo, la información de identificación de la plataforma de servicio de Internet), el contrato inteligente creado también incluye esa información de identificación. Desde 602, el método 600 pasa a 604.

En 604, el contrato inteligente creado se almacena en una dirección de almacenamiento en una red de cadena de bloques en base al identificador asociado con la solicitud de almacenamiento de información de inicio de sesión. En algunas implementaciones, para almacenar el contrato inteligente, primero se determina una dirección de almacenamiento, y luego el contrato inteligente se almacena en la dirección de almacenamiento determinada.

En algunas implementaciones, para determinar la dirección de almacenamiento de cada uno de los contratos inteligentes, el identificador se procesa primero para obtener un par de claves públicas-privadas; obtener una primera dirección en base a una clave pública en el par de claves públicas-privadas, y la primera dirección se obtiene calculando la clave pública en base a un algoritmo. Por ejemplo, la clave pública se puede calcular en base a un algoritmo hash, para obtener un valor hash de una longitud fija, donde el valor hash es la primera dirección. Luego, también se puede determinar una segunda dirección en base a la primera dirección, y la red de cadena de bloques determina la segunda dirección en base a un evento de transacción específico iniciado en la primera dirección. Finalmente, la segunda dirección se determina como la dirección de almacenamiento del contrato inteligente en la red de cadena de bloques. En algunas implementaciones, el evento de transacción especificado puede entenderse como una transacción. Por ejemplo, en la red Ethereum, para obtener la dirección de almacenamiento del contrato inteligente, se debe pagar una cantidad particular de Ether a la red Ethereum. Específicamente, cuando se genera una transacción en la red Ethereum, una dirección de origen de la transacción puede ser la primera dirección, y una dirección de destino de la transacción puede denominarse la segunda dirección (la segunda dirección se puede asignar en la red Ethereum). Una vez que se completa la transacción entre la primera dirección y la segunda dirección, el espacio de almacenamiento correspondiente a la segunda dirección se puede utilizar para almacenar el contrato inteligente creado para el usuario. Aquí, la segunda dirección también puede denominarse la dirección de almacenamiento del contrato inteligente. Desde 604, el método 600 pasa a 606.

En 606, se recibe una solicitud de consulta de información de inicio de sesión desde un usuario y en el dispositivo de procesamiento de información. La solicitud de consulta de información de inicio de sesión comprende un identificador.

En algunas implementaciones, al iniciar sesión en una plataforma de servicio de Internet, el usuario puede enviar la solicitud de consulta de información de inicio de sesión a un dispositivo de procesamiento de información, para obtener la información de inicio de sesión necesaria. Cuando el usuario necesita información de inicio de sesión, el usuario puede enviar la solicitud de consulta de información de inicio de sesión a un dispositivo de procesamiento de información, para obtener la información de inicio de sesión necesaria. Un escenario de uso para enviar la solicitud de consulta de información de inicio de sesión mediante el usuario no es limitante. Desde 606, el método 600 pasa a 608.

En 608, en base al identificador asociado con la solicitud de consulta de información de inicio de sesión, se recupera al menos un contrato inteligente desde la red de cadena de bloques. El contrato inteligente correspondiente al usuario se determina a partir del al menos un contrato inteligente recuperado.

En algunas implementaciones, para recuperar el contrato inteligente desde la dirección de almacenamiento en la red de cadena de bloques, primero se determina en base al identificador una dirección de almacenamiento del contrato inteligente utilizada para el procesamiento de información de inicio de sesión. Por ejemplo, el identificador asociado con la solicitud de consulta de información de inicio de sesión se procesa primero para obtener un par de claves públicas-privadas. Se puede obtener una primera dirección en base a una clave pública en el par de claves públicas-privadas. La primera dirección se puede obtener calculando la clave pública en base a un algoritmo. En base a la primera dirección, se puede obtener al menos una segunda dirección y cada una de las segundas direcciones realiza una transacción con la primera dirección. Específicamente, después de que se produce un evento de transacción especificado, los datos de transacción correspondientes al evento de transacción se almacenan en la red de cadena de bloques. La primera dirección se puede utilizar como una palabra clave de consulta, los datos de transacción, incluida la primera dirección, se pueden consultar en la red de cadena de bloques, y la al menos una segunda dirección se puede leer de los datos de transacción. Para el mismo usuario, dado que la primera dirección se determina en base al identificador proporcionado por el usuario, los datos de transacción pueden incluir la primera dirección y la segunda dirección. En consecuencia, la al menos una segunda dirección puede determinarse en base a la primera dirección, y

una dirección de almacenamiento del contrato inteligente puede identificarse a partir de la determinada al menos una segunda dirección. Finalmente, se puede recuperar al menos un contrato inteligente desde la dirección de almacenamiento.

5 En algunas implementaciones, si se determina que hay una segunda dirección que realiza una transacción con la primera dirección, determinar la segunda dirección como la dirección de almacenamiento del contrato inteligente; o si se determina que hay más de una segunda dirección realizando una transacción con la primera dirección, buscar una segunda dirección en la que se almacena el contrato inteligente y determinar la segunda dirección identificada como la dirección de almacenamiento del contrato inteligente. En esta situación, puede haber una o más direcciones de
10 almacenamiento del contrato inteligente, y uno o más contratos inteligentes se pueden recuperar en consecuencia.

En algunas implementaciones, si se lee un contrato inteligente desde la red de cadena de bloques, se determina que el contrato inteligente es un contrato inteligente correspondiente al usuario. En algunas implementaciones, si se recupera más de un contrato inteligente desde la red de cadena de bloques, se puede seleccionar un contrato
15 inteligente que satisfaga una condición especificada de los contratos inteligentes recuperados. Por ejemplo, un contrato inteligente con la misma información de identificación que la información de identificación incluida en la solicitud de consulta de información de inicio de sesión se puede seleccionar de los contratos inteligentes recuperados. Desde 608, el método 600 pasa a 610.

20 En 610, el contrato inteligente recuperado se ejecuta para obtener la información de inicio de sesión correspondiente al usuario. La información de inicio de sesión obtenida se puede enviar de vuelta al usuario. La información de inicio de sesión obtenida, por ejemplo, en forma de texto plano, se puede enviar al usuario, de modo que el usuario puede utilizar la información de inicio de sesión para completar un inicio de sesión.

25 En algunas implementaciones, si la información de inicio de sesión se obtiene ejecutando el contrato inteligente, se puede determinar que la información de inicio de sesión satisface las necesidades del usuario, y la información de inicio de sesión se puede proporcionar al usuario. En algunas implementaciones, si se obtienen múltiples datos de información de inicio de sesión ejecutando el contrato inteligente, la información de inicio de sesión se puede proporcionar al usuario para la confirmación.
30

Alternativamente, en algunas implementaciones, cuando la información de inicio de sesión incluye información de identificación, la información de identificación se puede analizar a partir de la información de inicio de sesión, con el fin de seleccionar información de inicio de sesión particular con la misma información de identificación que la información de identificación incluida en la solicitud de consulta de información de inicio de sesión y determinar que la
35 información de inicio de sesión seleccionada satisface las necesidades del usuario.

En algunas implementaciones, donde la información de inicio de sesión almacenada en el contrato inteligente está cifrada, para ejecutar el contrato inteligente y obtener la información de inicio de sesión correspondiente al usuario, el contrato inteligente se ejecuta primero para obtener información de inicio de sesión cifrada. El identificador asociado
40 con la solicitud de consulta de información de inicio de sesión se puede procesar para obtener un par de claves públicas-privadas. La información de inicio de sesión cifrada se puede descifrar además utilizando una clave privada en el par de claves privadas-públicas para obtener información de inicio de sesión descifrada. La información de inicio de sesión descifrada obtenida se puede proporcionar al usuario, y el usuario puede confirmar la información de inicio de sesión recibida.
45

En algunas implementaciones, el usuario puede enviar una solicitud de procesamiento de información de inicio de sesión a un dispositivo de procesamiento de información. Aquí, la información de inicio de sesión obtenida puede procesarse adicionalmente en base a la solicitud de procesamiento recibida. En algunas implementaciones, si la solicitud de procesamiento recibida es una solicitud de actualización, la información de inicio de sesión se puede
50 actualizar y la información de inicio de sesión actualizada se puede almacenar en la red de cadena de bloques. En algunas implementaciones, si la solicitud de procesamiento recibida es una solicitud de eliminación, la información de inicio de sesión se puede eliminar de la red de cadena de bloques. Después de 610, el método 600 se detiene.

Las implementaciones de la presente solicitud pueden resolver problemas técnicos en el procesamiento de información de inicio de sesión. En la tecnología existente, la información de inicio de sesión se almacena en un servidor de terceros. Sin embargo, debido a que el servidor de terceros almacena información de inicio de sesión para muchos usuarios, existe el riesgo de que la información de inicio de sesión almacenada se pueda divulgar o acceder de forma incorrecta, lo que reduce la seguridad de la información de inicio de sesión para un usuario. La metodología descrita
55 permite evitar este problema para mejorar la seguridad de los datos de información de inicio de sesión.

Las implementaciones de la presente memoria descriptiva describen un método de procesamiento de información de inicio de sesión. El método de procesamiento de información de inicio de sesión puede realizarse por un dispositivo de procesamiento de información. En base al método de procesamiento de información de inicio de sesión proporcionado en la implementación de la presente memoria descriptiva, se puede crear un contrato inteligente que
60 incluye información de inicio de sesión de un determinado usuario, y el contrato inteligente se almacena en una red de cadena de bloques. La información de inicio de sesión puede consultarse y obtenerse desde la red de cadena de

bloques. La red de cadena de bloques está construida en base a una tecnología de cadena de bloques. La tecnología de cadena de bloques, conocida como tecnología de libro de cuentas distribuido, es una tecnología de base de datos de Internet distribuida que se caracteriza por la descentralización, la transparencia, la resistencia a la manipulación y la confiabilidad. La solución divulgada en esta divulgación se implementa en base a la red de cadena de bloques, de modo que es menos probable que la información de inicio de sesión se pierda, robe o manipule, y la seguridad de almacenamiento de la información de inicio de sesión se mejora efectivamente. Además, en base al método de procesamiento de información de inicio de sesión proporcionado en la implementación de la presente memoria descriptiva, cuando un usuario necesita la información de inicio de sesión, el usuario puede obtener rápidamente la información de inicio de sesión necesaria desde una red de cadena de bloques a través de consulta, haciendo que sea conveniente para el usuario mantener la información de inicio de sesión.

Las realizaciones y las operaciones descritas en esta memoria descriptiva pueden implementarse en circuitos electrónicos digitales, o en software de computadora, firmware o hardware, incluyendo las estructuras divulgadas en esta memoria descriptiva o en combinaciones de uno o más de ellos. Las operaciones pueden implementarse como operaciones realizadas por un aparato de procesamiento de datos sobre datos almacenados en uno o más dispositivos de almacenamiento legibles por computadora o recibidos de otras fuentes. Un aparato de procesamiento de datos, computadora o dispositivo informático puede abarcar aparatos, dispositivos y máquinas para procesar datos, incluyendo a modo de ejemplo un procesador programable, una computadora, un sistema en un chip, o múltiples, o combinaciones, de los anteriores. El aparato puede incluir 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). El aparato también puede incluir código que crea un entorno de ejecución para el programa informático en cuestión, por ejemplo, código que constituye el firmware del procesador, una pila de protocolos, un sistema de gestión de base de datos, un sistema operativo (por ejemplo, un sistema operativo o una combinación de sistemas operativos), un entorno de tiempo de ejecución multiplataforma, una máquina virtual o una combinación de uno o más de ellos. El aparato y el entorno de ejecución pueden realizar diversas infraestructuras de modelos informáticos diferentes, tales como servicios web, computación distribuida e infraestructuras de computación en malla.

Un programa informático (también conocido, por ejemplo, como un programa, software, aplicación de software, módulo de software, unidad de software, script o código) puede escribirse en cualquier forma de lenguaje de programación, incluyendo lenguajes compilados o interpretados, declarativos o lenguajes procedimentales, y puede implementarse en cualquier forma, incluso como un programa independiente o como un módulo, componente, subrutina, objeto u otra unidad adecuada para el uso en un entorno informático. 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 único 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 se puede ejecutar en una computadora o en múltiples computadoras que están ubicadas en un sitio o distribuidas en múltiples sitios e interconectadas por una red de comunicaciones.

Los procesadores para la ejecución de un programa informático incluyen, a modo de ejemplo, microprocesadores de uso general y especial, y uno o más procesadores de cualquier tipo de computadora digital. En general, un procesador recibirá instrucciones y datos desde una memoria de solo lectura o una memoria de acceso aleatorio o ambas. Los elementos esenciales de una computadora son un procesador para realizar acciones de acuerdo con las instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. Generalmente, una computadora también incluirá, o estará operativamente acoplada para recibir datos desde o transferir datos a, o ambos, uno o más dispositivos de almacenamiento masivo para almacenar datos. Una computadora puede integrarse en otro dispositivo, por ejemplo, un dispositivo móvil, un asistente digital personal (PDA), una consola de juegos, un receptor del sistema de posicionamiento global (GPS) o un dispositivo de almacenamiento portátil. Los dispositivos adecuados para almacenar instrucciones y datos de programa informático incluyen memoria no volátil, medios y dispositivos de memoria, que incluyen, a modo de ejemplo, dispositivos de memoria semiconductores, discos magnéticos y discos magnetoópticos. El procesador y la memoria pueden complementarse o incorporarse en un circuito lógico de propósito especial.

Los dispositivos móviles pueden incluir teléfonos, equipos de usuario (UE), teléfonos móviles (por ejemplo, teléfonos inteligentes), tabletas, dispositivos ponibles (por ejemplo, relojes inteligentes y gafas inteligentes), dispositivos implantados dentro del cuerpo humano (por ejemplo, biosensores, implantes cocleares) u otros tipos de dispositivos móviles. Los dispositivos móviles pueden comunicarse de forma inalámbrica (por ejemplo, utilizando señales de radiofrecuencia (RF)) a diversas redes de comunicaciones (descritas a continuación). Los dispositivos móviles pueden incluir sensores para determinar las características del entorno actual del dispositivo móvil. Los sensores pueden incluir cámaras, micrófonos, sensores de proximidad, sensores GPS, sensores de movimiento, acelerómetros, sensores de luz ambiente, sensores de humedad, giroscopios, brújulas, barómetros, sensores de huella digital, sistemas de reconocimiento facial, sensores de RF (por ejemplo, radios Wi-Fi y móviles), sensores térmicos u otros tipos de sensores. Por ejemplo, las cámaras pueden incluir una cámara hacia adelante o hacia atrás con lentes móviles o fijas, un flash, un sensor de imagen y un procesador de imagen. La cámara puede ser una cámara de megapíxeles capaz de capturar detalles para reconocimiento facial y/o de iris. La cámara junto con un procesador de datos y la información de autenticación almacenada en memoria o accedida de forma remota puede formar un sistema de reconocimiento

facial. El sistema de reconocimiento facial o uno o más sensores, por ejemplo, micrófonos, sensores de movimiento, acelerómetros, sensores GPS o sensores RF, se pueden utilizar para la autenticación del usuario.

5 Para proporcionar interacción con un usuario, las realizaciones se pueden implementar en una computadora que tiene un dispositivo de visualización y un dispositivo de entrada, por ejemplo, una pantalla de cristal líquido (LCD) o una
10 pantalla de diodo orgánico emisor de luz (OLED)/realidad virtual (VR)/realidad aumentada (AR) para visualizar información al usuario y una pantalla táctil, teclado y un dispositivo señalador mediante el cual el usuario puede proporcionar entrada a la computadora. También se pueden utilizar otros tipos de dispositivos para proporcionar interacción con un usuario; por ejemplo, la retroalimentación proporcionada al usuario puede ser cualquier forma de
15 retroalimentación sensorial, por ejemplo, retroalimentación visual, retroalimentación auditiva o retroalimentación táctil; y la entrada del usuario puede recibirse en cualquier forma, incluida la entrada acústica, de voz o táctil. Además, una computadora puede interactuar con un usuario enviando y recibiendo documentos de un dispositivo que utiliza el usuario; por ejemplo, enviando páginas web a un navegador web en el dispositivo cliente de un usuario en respuesta a las solicitudes recibidas del navegador web.

15 Las realizaciones pueden implementarse utilizando dispositivos informáticos interconectados por cualquier forma o medio de comunicaciones de datos digitales cableado o inalámbrico (o combinación de los mismos), por ejemplo, una red de comunicaciones. Ejemplos de dispositivos interconectados son un cliente y un servidor generalmente remotos
20 entre sí que típicamente interactúan a través de una red de comunicaciones. Un cliente, por ejemplo, un dispositivo móvil, puede realizar transacciones por sí mismo, con un servidor, o a través de un servidor, por ejemplo, realizando transacciones de compra, venta, pago, entrega, envío o préstamo, o autorizando las mismas. Las transacciones de este tipo pueden ser en tiempo real de tal manera que una acción y una respuesta son temporalmente próximas; por ejemplo, un individuo percibe que la acción y la respuesta se producen de manera sustancialmente simultánea, la
25 diferencia de tiempo para una respuesta después de la acción del individuo es inferior a 1 milisegundo (ms) o inferior a 1 segundo (s), o la respuesta es sin demora intencional teniendo en cuenta las limitaciones de procesamiento del sistema.

30 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) y una red de área amplia (WAN). La red de comunicaciones puede incluir todo o una porción del Internet, otra red de comunicaciones o una combinación de redes de comunicaciones. La información se puede transmitir en la red de comunicaciones de acuerdo con diversos protocolos y estándares, incluidos evolución a largo plazo(LTE), 5G IEEE 802, Protocolo de Internet (IP) u otros protocolos o combinaciones de protocolos. La red de comunicaciones puede transmitir datos de voz, video, biométricos o de autenticación u otra información entre los
35 dispositivos informáticos conectados.

REIVINDICACIONES

1. Un método para procesar una información de inicio de sesión, el método comprende:
 5 recibir una solicitud de almacenamiento de información de inicio de sesión enviada por un usuario, en donde la solicitud de almacenamiento de información de inicio de sesión comprende un identificador (101);
 determinar información de inicio de sesión correspondiente al usuario (103);
 crear, en base a una plantilla de contrato inteligente predeterminada utilizada para el procesamiento de información de inicio de sesión, un contrato inteligente que comprende la información de inicio de sesión, en donde la lógica de procesamiento utilizada para el procesamiento de información de inicio de sesión se registra en la plantilla de contrato
 10 inteligente predeterminada (105);
 almacenar el contrato inteligente creado en una red de cadena de bloques en base al identificador (107);
 recibir una solicitud de consulta de información de inicio de sesión que se envía por un usuario y que comprende un identificador (109, 202);
 leer, desde una red de cadena de bloques en base al identificador, al menos un contrato inteligente utilizado para el
 15 procesamiento de información de inicio de sesión (111, 608);
 determinar el contrato inteligente correspondiente al usuario que realiza la solicitud de consulta de información del al menos un contrato inteligente (608);
 ejecutar el contrato inteligente para obtener información de inicio de sesión correspondiente al usuario que realiza la solicitud de consulta de información (113); y
 20 enviar la información de inicio de sesión obtenida al usuario que realiza la solicitud de consulta de información (610).
2. El método de acuerdo con la reivindicación 1, en donde la lectura, desde una red de cadena de bloques en base al identificador, de al menos un contrato inteligente utilizado para el procesamiento de información de inicio de sesión comprende:
 25 determinar, en base al identificador, una dirección de almacenamiento del contrato inteligente utilizado para el procesamiento de información de inicio de sesión (604); y
 leer el contrato inteligente de la red de cadena de bloques en base a la dirección de almacenamiento (608).
3. El método de acuerdo con la reivindicación 2, en donde determinar, en base al identificador, una dirección de almacenamiento del contrato inteligente utilizado para el procesamiento de información de inicio de sesión comprende:
 30 procesar el identificador para obtener un par de claves públicas-privadas;
 obtener una primera dirección a través del cálculo en base a una clave pública comprendida en el par de claves públicas-privadas;
 determinar, en base a la primera dirección, al menos una segunda dirección que realiza una transacción con la primera
 35 dirección; e
 identificar la dirección de almacenamiento del contrato inteligente a partir de las segundas direcciones.
4. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en donde la información de inicio de sesión es para el usuario que inicia sesión en una plataforma de servicio de Internet, la solicitud de almacenamiento comprende información de identificación que es información de identificación de la plataforma de servicio de Internet, y crear un contrato inteligente comprende crear un contrato inteligente que comprende la información de identificación.
 40
5. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en donde determinar el contrato inteligente correspondiente al usuario que realiza la solicitud de consulta de información comprende:
 45 si se lee un contrato inteligente desde la red de cadena de bloques, ese contrato inteligente se determina como el contrato inteligente correspondiente al usuario que realiza la solicitud de consulta de información; y
 si se lee más de un contrato inteligente desde la red de cadena de bloques, seleccionar, de los contratos inteligentes leídos, un contrato inteligente que cumple una condición especificada.
6. El método de acuerdo con la reivindicación 5, en donde seleccionar, de los contratos inteligentes leídos, un contrato inteligente que satisface una condición especificada comprende:
 50 seleccionar, de la información de identificación comprendida en los contratos inteligentes leídos, un contrato inteligente con la misma información de identificación que la información de identificación incluida en la solicitud de consulta de información de inicio de sesión.
 55
7. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 6, en donde ejecutar el contrato inteligente para obtener información de inicio de sesión correspondiente al usuario comprende:
 60 ejecutar el contrato inteligente para obtener al menos una información de inicio de sesión (113, 305, 610); y
 enviar la al menos una información de inicio de sesión al usuario (610), de modo que el usuario confirme la información de inicio de sesión correspondiente.
 60
8. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en donde ejecutar el contrato inteligente para obtener información de inicio de sesión correspondiente al usuario comprende:
 65 ejecutar el contrato inteligente para obtener información de inicio de sesión cifrada; y
 descifrar la información de inicio de sesión cifrada para obtener la información de inicio de sesión correspondiente al usuario.

9. El método de acuerdo con la reivindicación 8, en donde el descifrado de la información de inicio de sesión cifrada comprende:
procesar el identificador para obtener un par de claves públicas-privadas; y
descifrar la información de inicio de sesión cifrada utilizando una clave privada en el par de claves públicas-privadas.
- 5
10. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 9, en donde después de obtenerse la información de inicio de sesión, el método comprende, además:
procesar la información de inicio de sesión en base a una solicitud de procesamiento recibida.
- 10
11. El método de acuerdo con la reivindicación 10, en donde el procesamiento de información de inicio de sesión en base a una solicitud de procesamiento recibida comprende:
si la solicitud de procesamiento recibida es una solicitud de actualización, actualizar la información de inicio de sesión y almacenar la información de inicio de sesión actualizada en la red de cadena de bloques.
- 15
12. El método de acuerdo con la reivindicación 10, en donde el procesamiento de información de inicio de sesión en base a una solicitud de procesamiento recibida comprende:
si la solicitud de procesamiento recibida es una solicitud de eliminación, eliminar la información de inicio de sesión de la red de cadena de bloques.
- 20
13. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 12, en donde almacenar el contrato inteligente comprende:
determinar una dirección de almacenamiento para el contrato inteligente, en donde determinar la dirección de almacenamiento comprende:
procesar el identificador para obtener un par de claves públicas-privadas;
- 25
- obtener una primera dirección en base a una clave pública en el par de claves públicas-privadas, en donde la primera dirección se obtiene calculando la clave pública en base a un algoritmo;
obtener una segunda dirección en base a la primera dirección, en donde la segunda dirección se determina mediante la red de cadena de bloques en base a un evento de transacción especificado iniciado en la primera dirección; y
determinar que una segunda dirección es la dirección de almacenamiento del contrato inteligente en la red de cadena
- 30
- de bloques; y
almacenar el contrato inteligente en la dirección de almacenamiento determinada en la red de cadena de bloques; y
en donde leer el contrato inteligente desde la red de cadena de bloques comprende:
procesar, el identificador para obtener un par de claves públicas-privadas;
- 35
- obtener una primera dirección en base a una clave pública en el par de claves públicas-privadas, en donde la primera dirección se obtiene calculando la clave pública en base a un algoritmo;
determinar, en base a la primera dirección, al menos una segunda dirección, en donde cada una de las al menos una segunda dirección realiza una transacción con la primera dirección;
- 40
- identificar, una dirección de almacenamiento del contrato inteligente de la al menos una segunda dirección; y
leer, al menos un contrato inteligente de la dirección de almacenamiento identificada.
14. Un dispositivo para procesar una información de inicio de sesión, el dispositivo que comprende una pluralidad de módulos configurados para realizar el método de acuerdo con una cualquiera de las reivindicaciones 1 a 13.

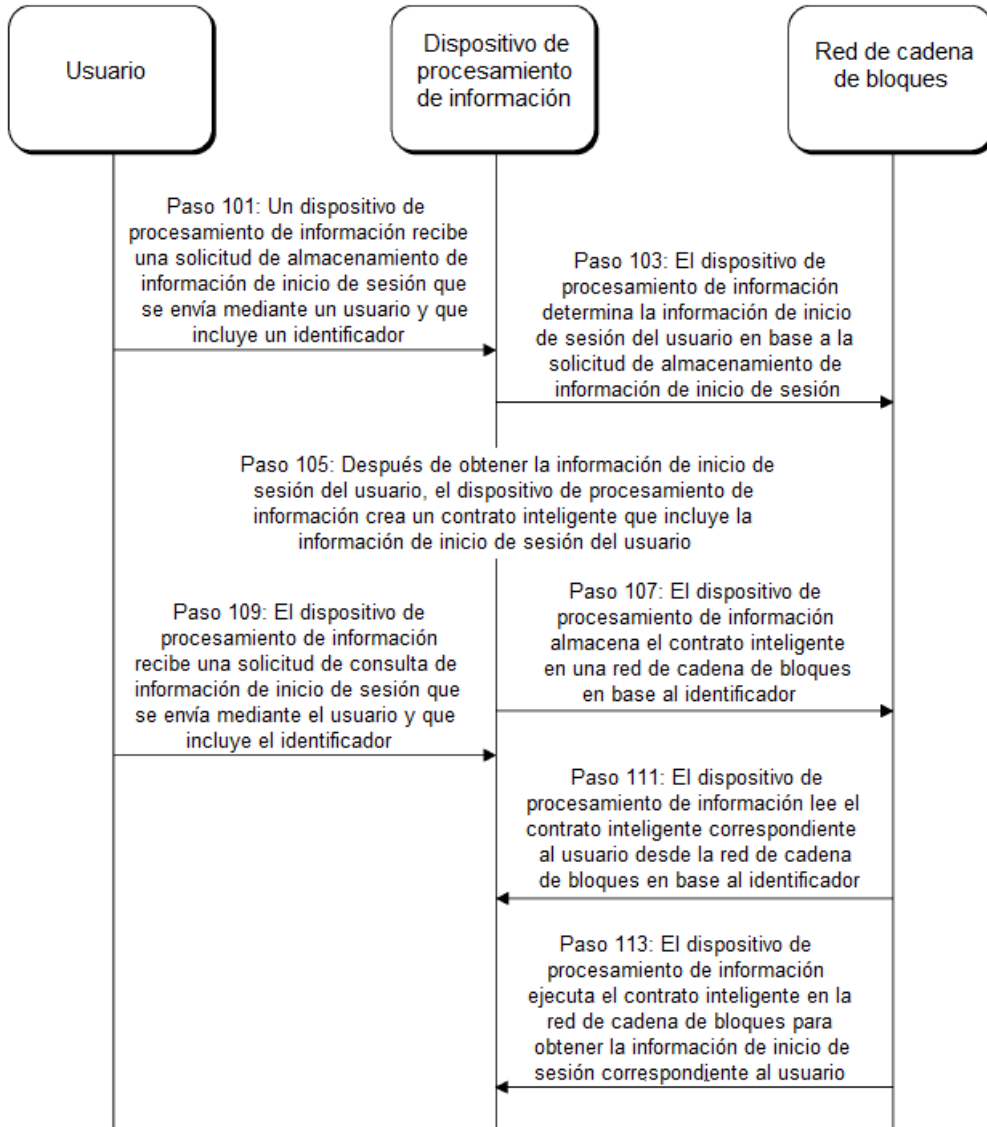


FIG. 1

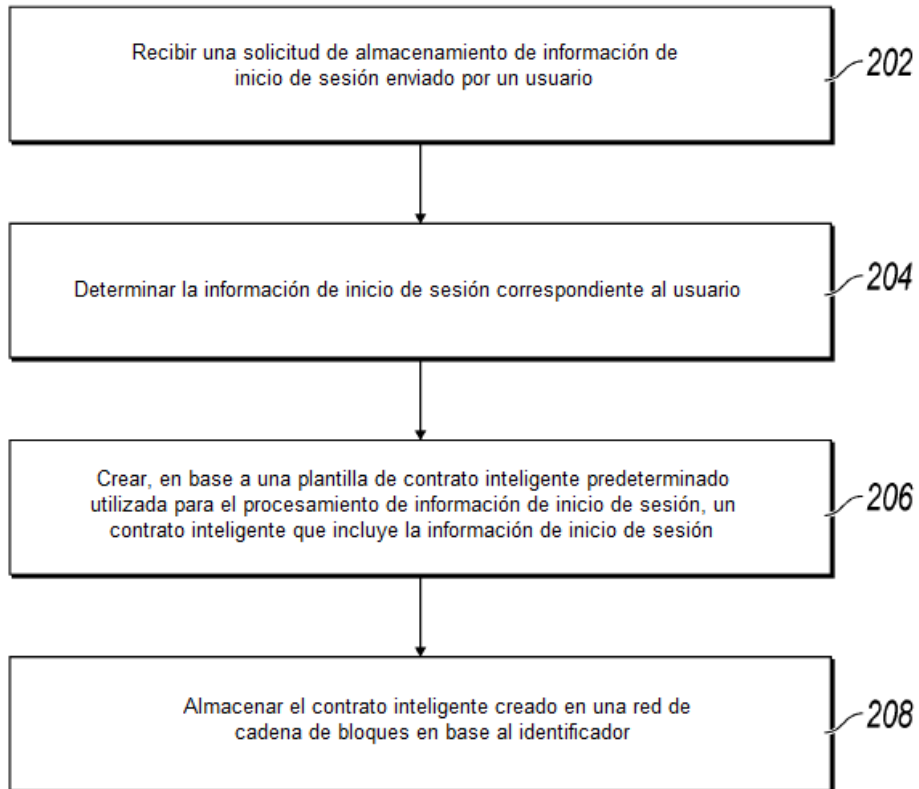


FIG. 2

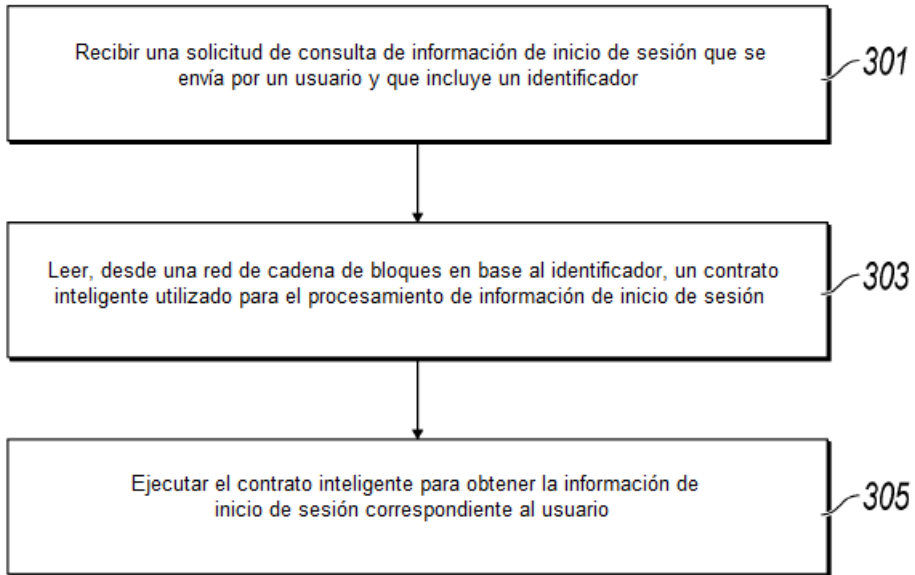


FIG. 3

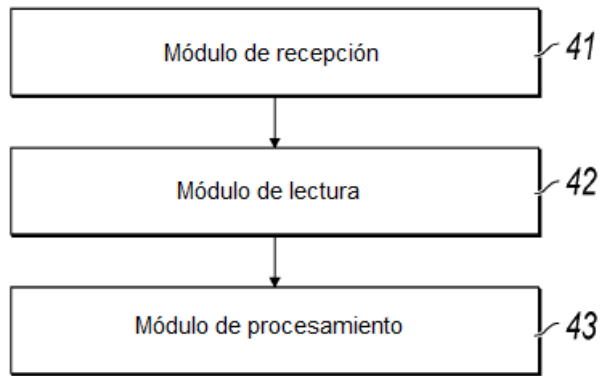


FIG. 4

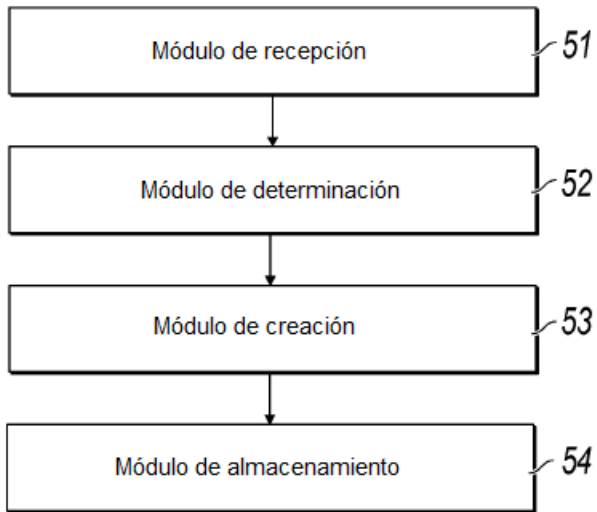


FIG. 5

600
⚡

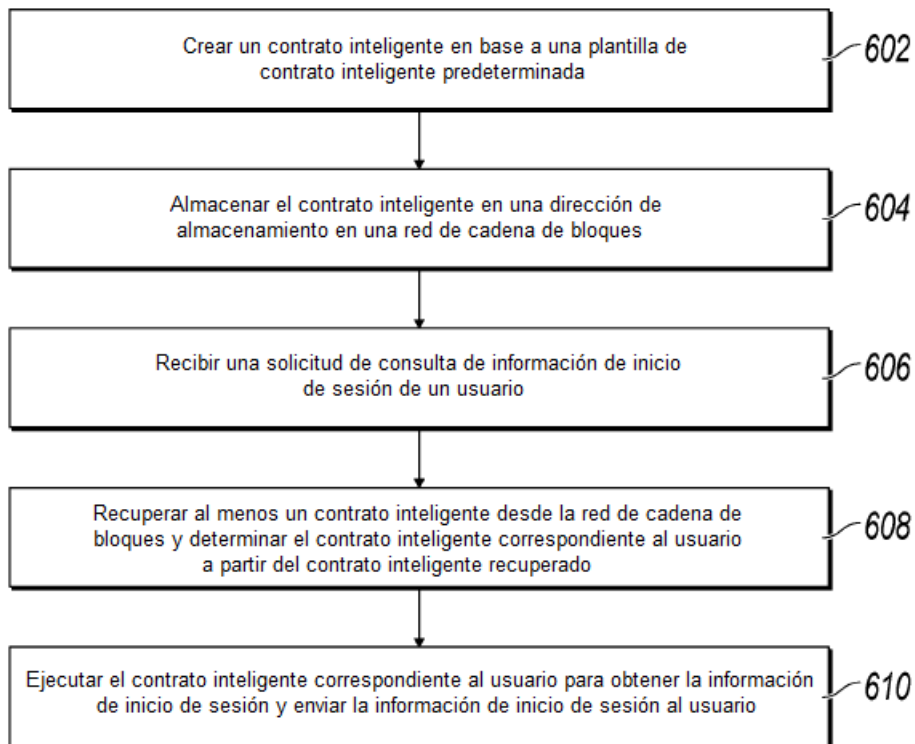


FIG. 6