(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 998 883**

(51) Int. Cl.:

H04L 9/40 (2012.01)
H04L 9/32 (2006.01)
H04L 9/00 (2012.01)
G06Q 20/02 (2012.01)
G06Q 20/40 (2012.01)
G06Q 20/38 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.07.2020 PCT/US2020/041427**

(87) Fecha y número de publicación internacional: **21.01.2021 WO21011308**

(96) Fecha de presentación y número de la solicitud europea: **09.07.2020 E 20750052 (1)**

(97) Fecha y número de publicación de la concesión europea: **06.11.2024 EP 4000236**

(54) Título: **Gestión segura de recursos para evitar el acceso fraudulento a recursos**

(30) Prioridad:

18.07.2019 US 201962875814 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.02.2025

(73) Titular/es:

EQUIFAX, INC. (100.00%)
1550 Peachtree Street, N. W.
Atlanta, GA 30309, US

(72) Inventor/es:

BONDUGULA, RAJKUMAR y
MCBURNETT, MICHAEL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Gestión segura de recursos para evitar el acceso fraudulento a recursos

Referencia cruzada a solicitudes relacionadas

Esta reivindica prioridad de la Solicitud Provisional de EE. UU. Nº 62/875,814, titulada et al. "Secure Resource Management to Prevent Fraudulent Resource Access" presentada el 18 de julio de 2019.

Campo técnico

Esta descripción se refiere, en general, al aumento de la seguridad de la gestión de recursos al evitar el acceso fraudulento a los recursos.

Antecedentes

La gestión de recursos, o más específicamente el control de acceso a los recursos, se vuelve cada vez más desafiante a medida que ahora pueden adquirirse, accederse y transferirse en línea cómodamente diversos recursos. Por ejemplo, un usuario puede adquirir un recurso de almacenamiento en línea para un término fijo a través de transacciones en línea con un proveedor de recursos del recurso de almacenamiento en línea, y acceder al recurso de almacenamiento en línea a través de Internet. Si el usuario decide más tarde que ya no necesita el recurso de almacenamiento en línea, el usuario puede transferir el término no utilizado del recurso de almacenamiento en línea a otro usuario o entidad, de nuevo a través de transacciones en línea con el otro usuario o entidad. De manera similar, para recursos monetarios, un acreedor puede adquirir el derecho al recurso, obtener el recurso, o transferir el derecho al recurso a través de transacciones en línea.

Esta naturaleza en línea del acceso y transferencia de recursos hace que los accesos fraudulentos de los recursos sean más fáciles que antes. Por ejemplo, un usuario que adquirió un recurso y más tarde transfirió el recurso podría tener todavía los medios, como credenciales o fichas, para acceder al recurso incluso después de la transferencia. Asimismo, el usuario podría transferir los derechos del mismo recurso a múltiples usuarios posteriores mediante fraude. Como resultado, el proveedor de recursos podría terminar proporcionando recursos a múltiples usuarios y un cesionario del recurso podría haber adquirido un recurso que ha sido agotado por otros cesionarios.

El problema podría resolverse, parcialmente, mejorando las medidas de seguridad en el proveedor de recursos revocando, oportunamente, el derecho de acceso de un usuario si el usuario ha transferido su acceso al recurso a otro usuario. Sin embargo, este enfoque requiere que el proveedor de recursos implemente sofisticados mecanismos de control de acceso a recursos. No todos los proveedores de recursos tienen las capacidades para hacerlo. El acceso fraudulento del recurso descrito anteriormente sigue siendo una gran amenaza para estos proveedores de recursos. La publicación de la solicitud de patente de EE. UU. Nº US 2019/0044700 A1 describe un sistema en el que se almacena un registro electrónico en un entorno distribuido con respecto a un elemento.

Compendio

Diversos aspectos de la presente descripción implican proporcionar un sistema centralizado de gestión segura de recursos para evitar el acceso fraudulento a recursos como se describe en las reivindicaciones adjuntas.

Este compendio no pretende identificar características clave o esenciales de la materia reivindicada, ni pretende utilizarse de manera aislada para determinar el alcance de la materia reivindicada. La materia debe entenderse con referencia a las partes apropiadas de toda la especificación, a cualquiera o a todos los dibujos, y a cada reivindicación.

Breve descripción de los dibujos

Lo anterior, junto con otras características y ejemplos, se hará más evidente al referirse a la siguiente especificación, reivindicaciones y dibujos adjuntos.

La FIGURA 1 es un diagrama de bloques que representa un ejemplo de un sistema de gestión segura de recursos para registrar y mantener, de forma segura, registros del recurso relacionados con recursos, según ciertos aspectos de la presente descripción.
Las FIGURAS 2A y 2B muestran varios diagramas de flujo que ilustran ejemplos de procesos para una gestión segura de recursos, según ciertos aspectos de la presente descripción.
La FIGURA 3 es un diagrama de flujo que muestra un ejemplo de un proveedor de recursos que distribuye recursos a través del servidor de gestión segura de recursos, según ciertos aspectos de la presente descripción.
La FIGURA 4 es un diagrama de flujo que muestra un ejemplo de un proveedor de recursos que distribuye recursos a través de un tercero de confianza, según ciertos aspectos de la presente descripción.
La FIGURA 5 es un diagrama de flujo que muestra otro ejemplo de un proveedor de recursos que distribuye recursos a través de un tercero de confianza, según ciertos aspectos de la presente descripción.

La FIGURA 6 es un diagrama de flujo que ilustra un ejemplo de un proceso para gestionar transacciones de recursos para evitar el acceso fraudulento a los recursos, según ciertos aspectos de la presente descripción.
La FIGURA 7 es un diagrama de bloques que representa un ejemplo de un sistema informático adecuado para implementar aspectos de las técnicas y tecnologías presentadas en la presente memoria.

Descripción detallada

Ciertos aspectos y características de la presente descripción implican proporcionar un sistema centralizado de gestión segura de recursos para evitar el acceso fraudulento a recursos. El sistema de gestión segura de recursos mantiene un repositorio de registros del recurso para almacenar registros del recurso de diversos recursos. Los registros del recurso contienen información de los proveedores de recursos de los recursos, información de los usuarios de recursos de los recursos, e historiales de transacciones de los recursos. Un usuario del recurso se refiere a un usuario autorizado a acceder a un recurso o que tiene derecho a obtener el recurso. El repositorio de registros del recurso se implementa en una cadena de bloques híbrida.

El sistema de gestión segura de recursos puede utilizar el repositorio de registros del recurso para atender solicitudes de verificación. Por ejemplo, si el sistema de gestión segura de recursos recibe una solicitud para verificar un usuario autorizado de un recurso, el sistema de gestión segura de recursos interroga al repositorio de registros del recurso para recuperar el registro del recurso e identifica al usuario autorizado actual del recurso. El sistema de gestión segura de recursos devuelve el resultado de verificación que identifica al usuario autorizado del recurso en respuesta a la solicitud. El proveedor de recursos puede proporcionar al usuario autorizado acceso al recurso según el resultado de verificación, por ejemplo, distribuyendo el recurso al usuario autorizado.

La solicitud puede ser enviada por un proveedor de recursos para confirmar que el usuario del recurso que solicita acceso al recurso es un usuario autorizado. La solicitud también puede ser enviada por un posterior usuario del recurso al que el actual usuario del recurso debe transferir el derecho al recurso. De esta manera, el proveedor de recursos (o el subsiguiente usuario del recurso) puede verificar la autenticidad del usuario del recurso y la cantidad del recurso antes de distribuir el recurso (o antes de adquirir el derecho al recurso del actual usuario del recurso). En algunos ejemplos, el posterior usuario del recurso también puede solicitar al sistema de gestión segura de recursos que determine el valor del recurso o la probabilidad de que el proveedor de recursos distribuya el recurso antes de aceptar la transferencia del recurso.

La distribución del recurso puede realizarse, directamente, desde el proveedor de recursos al usuario del recurso, o a través del sistema de gestión segura de recursos o de un tercero de confianza. En respuesta a cada distribución del recurso, el usuario del recurso, el proveedor de recursos, o el tercero de confianza pueden informar de la distribución del recurso al sistema de gestión segura de recursos de modo que el repositorio de registros del recurso pueda actualizarse para incluir la transacción de distribución. Asimismo, para cada transferencia de derecho del recurso, el actual usuario del recurso o el subsiguiente usuario del recurso puede informar de la transferencia al sistema de gestión segura de recursos de modo que el repositorio de registros del recurso pueda actualizarse para reflejar la transferencia y el actual usuario autorizado del recurso.

Como se describe en la presente memoria, ciertos aspectos proporcionan mejoras a la gestión de recursos al resolver los problemas de acceso fraudulento que son específicos para Internet. Como se ha discutido anteriormente, la naturaleza en línea del acceso y transferencia de recursos hace que el acceso fraudulento de los recursos sea más fácil de implementar y más difícil de detectar. El sistema centralizado de gestión segura de recursos en la presente descripción mantiene un seguimiento de cada transacción con respecto a un recurso y mantiene una copia segura de los registros en un repositorio seguro. Esto permite al proveedor de recursos, a posteriores usuarios del recurso, o a otras entidades verificar la autenticidad del recurso y el usuario autorizado antes de distribuir o adquirir el recurso. Al utilizar tecnologías informáticas seguras, como el cifrado de datos y las cadenas de bloques, esta solución de verificación segura reduce, significativamente, las posibilidades de acceso fraudulento a los recursos.

El sistema centralizado de gestión segura de recursos puede reducir la carga de implementar mecanismos seguros de control de acceso a recursos de proveedores de recursos individuales. Adicional o alternativamente, debido a que el sistema centralizado seguro de verificación de recursos puede implementarse con mecanismos de protección altamente complicados, la seguridad del proceso de control de acceso a recursos proporcionado por el sistema es más segura que el control de acceso implementado por proveedores de recursos individuales.

Estos ejemplos ilustrativos se dan para introducir al lector en la materia general discutida aquí y no pretenden limitar el alcance de los conceptos descritos. Las siguientes secciones describen diversas características y ejemplos adicionales con referencia a los dibujos en los que números similares indican elementos similares, pero no deben utilizarse para limitar la presente descripción.

Ejemplo de entorno operativo para un sistema de gestión segura de recursos

La FIGURA 1 es un diagrama de bloques que representa un ejemplo de un sistema 100 de gestión segura de recursos en el que los registros del recurso relativos a partes y transacciones relacionadas con los recursos se graban y

mantienen de forma segura. Estos registros del recurso pueden utilizarse para verificar un recurso y su usuario autorizado cuando sea necesario. El sistema 100 de gestión segura de recursos es un sistema informático especializado que puede utilizarse para procesar grandes cantidades de datos utilizando un gran número de ciclos de procesamiento informático.

El sistema 100 de gestión segura de recursos mostrado en la FIGURA 1 incluye un servidor 118 de gestión segura de recursos que está configurado para gestionar transacciones que involucran un recurso y para verificar al usuario autorizado del recurso. El sistema 100 de gestión segura de recursos incluye además un repositorio 124 de registros del recurso configurado para almacenar, de forma segura, registros 130 del recurso, cada uno de los cuales describe ciertos aspectos asociados a un recurso. Por ejemplo, el registro 130 del recurso para un recurso puede incluir información 134 del recurso que describe el tipo del recurso, el identificador del recurso, la cantidad del recurso, la fecha efectiva del recurso, la programación para la distribución del recurso, la cantidad no utilizada restante del recurso, etcétera. Por ejemplo, si el recurso es un recurso de almacenamiento en línea, la información 134 del recurso puede indicar que el recurso es un recurso de almacenamiento en línea. La información 134 del recurso para el recurso de almacenamiento en línea puede incluir además información como un número de serie asociado al recurso de almacenamiento en línea, la capacidad del recurso de almacenamiento en línea, el período de tiempo que puede utilizarse el recurso de almacenamiento, la dirección de red del recurso de almacenamiento, etcétera. Para un recurso monetario, la información 134 del recurso puede incluir el tipo o la naturaleza del recurso (p. ej., un fondo o el reembolso de un préstamo), la cantidad total del fondo o préstamo, la programación para la distribución del fondo o de los pagos del préstamo, el número de cuenta del fondo o préstamo, el saldo restante del préstamo, y otros.

El registro 130 del recurso para el recurso también puede incluir datos 132 del proveedor de recursos que contienen diversa información sobre el proveedor de recursos del recurso, como el nombre, la dirección, la identificación del proveedor de recursos. También puede incluirse otra información, como datos relacionados con la capacidad del proveedor de recursos que proporciona, oportunamente, el recurso. Si el proveedor de recursos es una compañía o una organización, como una compañía que proporciona un recurso de almacenamiento en línea, los datos 132 del proveedor de recursos pueden incluir el nombre de la compañía, la dirección de red o física de la compañía, la identificación (p. ej., el número de identificación fiscal (TIN)) de la compañía, los ingresos de la compañía, la capacidad total del recurso mantenido por la compañía, etcétera. Si el proveedor de recursos es un individuo o un grupo de individuos, como un prestatario del préstamo que proporciona los pagos del préstamo, los datos 132 del proveedor de recursos pueden incluir el nombre, la dirección, el número de la seguridad social (SSN) del prestatario del préstamo. Los datos 132 del proveedor de recursos también pueden incluir el ingreso del prestatario del préstamo que indica la capacidad del prestatario del préstamo para distribuir, oportunamente, el recurso monetario a un acreedor.

Asimismo, los registros 130 del recurso también incluyen datos 136 del usuario del recurso para registrar información sobre el usuario autorizado del recurso. Un usuario autorizado de un recurso puede ser una entidad o un individuo que tiene el derecho de acceder al recurso o de recibir la distribución del recurso del proveedor de recursos o de un tercero de confianza. Un usuario autorizado de un recurso también puede denominarse "un usuario del recurso" o un "usuario de recurso" por simplicidad. La distribución del recurso puede implicar proporcionar el recurso o una parte del recurso para acceder, utilizando exclusivamente, reivindicando la propiedad, o ejecutando de otro modo los derechos que tiene el usuario autorizado con respecto al recurso.

Debido a que el recurso (o el acceso al recurso) puede transferirse desde un usuario autorizado a otro usuario autorizado, los datos 136 de usuario del recurso incluyen la información sobre el usuario autorizado actual y los usuarios autorizados pasados del recurso. Para cada uno de los usuarios del recurso, los datos 136 de usuario del recurso pueden incluir información del usuario del recurso, como el nombre, la dirección, la identificación, etcétera.

El registro 130 del recurso para un recurso mantiene además un historial 138 de transacciones del recurso que describe las transacciones que involucran el recurso. Por ejemplo, el historial 138 de transacciones del recurso puede incluir entradas para distribuciones y transferencias de recursos. Una entrada para la distribución del recurso en el historial 138 de transacciones del recurso puede contener el tiempo de la distribución, la cantidad del recurso que se distribuye, el destinatario de la distribución (es decir, el usuario autorizado posterior), la forma en que se distribuye el recurso (p. ej., proporcionando credenciales de inicio de sesión del usuario autorizado para acceder al recurso, o enviando las fichas del usuario autorizado u otros datos electrónicos que indican la distribución), y otra información.

En algunos ejemplos que no entran dentro del alcance de las reivindicaciones, el repositorio 124 de registros del recurso se implementa utilizando una base de datos segura implementando mecanismos seguros como cifrado de datos, control de acceso, control de integridad, copia de seguridad de datos, o cualquier combinación de los mismos. El repositorio 124 de registros del recurso se implementa a través de una cadena de bloques, donde la información contenida en los registros 130 del recurso se almacena, de forma segura, en la cadena de bloques. La cadena de bloques se actualiza a medida que se recibe nueva información en el repositorio 124 de registros del recurso, como cuando el recurso se transfiere de un usuario a otro usuario, cuando se está distribuyendo una parte del recurso, etcétera.

La cadena de bloques es una cadena de bloques híbrida que incluye una cadena de bloques privada que sólo es accesible por el sistema 100 de gestión segura de recursos y una cadena de bloques pública accesible por el público.

El repositorio 124 de registros del recurso puede almacenar la información detallada y sensible en los registros 130 de recursos en la cadena de bloques privada, como los datos 132 del proveedor de recursos, los datos 136 de usuario del recurso, información detallada en la información 134 del recurso y el historial 138 de transacciones del recurso. El repositorio 124 de registros del recurso puede almacenar una versión cifrada del historial 138 de transacciones del recurso en la cadena de bloques pública. La versión cifrada puede incluir el hash de cada una de las entradas en el historial 138 de transacciones del recurso.

En otros ejemplos que no entran dentro del alcance de las reivindicaciones, la cadena de bloques es una cadena de bloques pública. Los datos contenidos en el repositorio 124 de registros del recurso están cifrados y almacenados en la cadena de bloques pública. Aunque el repositorio 124 de registros del recurso está disponible públicamente, el contenido del repositorio 124 de registros del recurso no es accesible sin la clave de descifrado. Como tal, la información sensible contenida en el repositorio 124 de registros del recurso todavía está protegida en la cadena de bloques pública.

En función del repositorio 124 de registros del recurso, el servidor 118 de gestión segura de recursos puede utilizar un subsistema 120 de verificación de recursos para verificar la autenticidad de un recurso, incluyendo el tipo de recurso, la cantidad no utilizada restante del recurso, el usuario autorizado del recurso, las transacciones que involucran el recurso, etcétera. Por ejemplo, el subsistema 120 de verificación de recursos puede configurarse para recibir una solicitud para verificar la autenticidad de un recurso. En respuesta a dicha solicitud, el subsistema 120 de verificación de recursos se comunica con el repositorio 124 de registros del recurso y consulta los registros 130 del recurso para determinar el registro 130 del recurso para el recurso solicitado. Si la información contenida en la solicitud coincide con el registro 130 del recurso para el recurso solicitado, el subsistema 120 de verificación de recursos devuelve un mensaje al dispositivo informático solicitante que indica que la información sobre el recurso en la solicitud es auténtica. De lo contrario, el subsistema 120 de verificación de recursos devuelve un mensaje que muestra que la información sobre el recurso en la solicitud no es auténtica.

El subsistema 120 de verificación de recursos también puede configurarse para proporcionar información auténtica sobre un recurso. Por ejemplo, el subsistema 120 de verificación de recursos puede configurarse para procesar una solicitud de información como el usuario autorizado actual y la cantidad no utilizada del recurso. En respuesta, el subsistema 120 de verificación de recursos puede consultar y recuperar el registro 130 del recurso para el recurso del repositorio 124 de registros del recurso para identificar y devolver la información solicitada.

Si el repositorio 124 de registros del recurso se implementa utilizando una cadena de bloques híbrida, la cadena de bloques pública puede utilizarse para verificar la autenticidad de las transacciones que involucran un recurso, como una transferencia del recurso o distribución del recurso. Por ejemplo, una entidad que quiere verificar la autenticidad de una transacción que involucra un recurso puede enviar, utilizando un dispositivo informático, información asociada a la transacción al servidor 118 de gestión segura de recursos. El servidor 118 de gestión segura de recursos genera un hash para la transacción de consulta utilizando el mismo método de hash utilizado para generar el hash almacenado en la cadena de bloques pública. El servidor 118 de gestión segura de recursos puede enviar el hash generado a la cadena de bloques pública para su verificación. Adicionalmente, o alternativamente, el servidor 118 de gestión segura de recursos puede devolver el hash generado a la entidad solicitante de modo que la entidad solicitante pueda verificar la autenticidad de la propia transacción utilizando la cadena de bloques pública. Si la cadena de bloques pública devuelve una coincidencia al hash generado, puede determinarse que la transacción consultada es una transacción auténtica que efectivamente se produjo; de lo contrario, la transacción consultada no es una transacción auténtica.

El servidor 118 de gestión segura de recursos incluye además un subsistema 122 de predicción del valor del recurso. El subsistema 122 de predicción del valor del recurso puede configurarse para construir y utilizar un modelo para predecir un valor esperado de un recurso en función de los datos sobre el recurso almacenados en el repositorio 124 de registros del recurso. En algunos ejemplos, el modelo está configurado para predecir una probabilidad (p. ej., una probabilidad o una posibilidad) del recurso que se distribuye dentro de un cierto período de tiempo. El modelo está configurado además para predecir una cantidad o una cantidad asociada al recurso restante. En función de estas dos cantidades previstas, el subsistema 122 de predicción del valor del recurso puede calcular el valor esperado del recurso no transmitido restante. Como se discutirá más adelante, el valor esperado del recurso restante puede ser útil para un usuario posterior del recurso cuando se determina si aceptar la transferencia del recurso desde un usuario autorizado anterior. Detalles adicionales sobre la predicción del valor del recurso restante se proporcionan a continuación con respecto a la FIGURA 6.

El sistema 100 de gestión segura de recursos también incluye un subsistema 112 de cliente orientado al exterior que incluye uno o más dispositivos informáticos para proporcionar una subred física o lógica (a veces denominada "zona desmilitarizada" o "red perimetral"). El subsistema 112 de cliente orientado al exterior está configurado para exponer ciertas funciones en línea del sistema 100 de gestión segura de recursos a una red no confiable, como Internet u otra red 108 de datos pública. En algunos aspectos, el subsistema 112 de cliente orientado al exterior puede implementarse como nodos de borde, que proporcionan una interfaz entre la red 108 de datos pública y un sistema informático en clúster, como un clúster Hadoop utilizado por el sistema 100 de gestión segura de recursos.

El subsistema 112 de cliente orientado al exterior está acoplado, de forma comunicativa, a través de un dispositivo cortafuegos 116, a uno o más dispositivos informáticos que forman una red 114 de datos privada. El dispositivo cortafuegos 116, que puede incluir uno o más dispositivos, crea una parte segura del sistema 100 de gestión segura de recursos que incluye diversos dispositivos en comunicación a través de la red 114 de datos privada. En algunos aspectos, utilizando la red 114 de datos privada, el sistema 100 de gestión segura de recursos puede alojar el repositorio 124 de registros del recurso en una red aislada (es decir, la red 114 de datos privada) que no tiene accesibilidad directa a través de Internet o de otra red 108 de datos pública. Si el repositorio 124 de registros del recurso se implementa utilizando la cadena de bloques híbrida como se describió anteriormente, puede accederse, directamente, a la cadena de bloques pública a través de Internet o de otra red 108 de datos pública, pero no a la cadena de bloques privada.

Diversos sistemas informáticos pueden interactuar con el sistema 100 de gestión segura de recursos a través del subsistema 112 de cliente orientado al exterior, como un sistema informático 104 del proveedor de recursos, un sistema informático 106 del usuario del recurso, uno o más sistemas informáticos 110 del usuario posterior del recurso, o uno o más sistemas informáticos 102 de terceros de confianza.

Un sistema informático 104 del proveedor de recursos puede incluir cualquier dispositivo informático u otro dispositivo de comunicación operado por un individuo, como un consumidor, o una entidad, como una compañía, un instituto, una organización, u otros tipos de entidades. El sistema informático 104 del proveedor de recursos puede incluir instrucciones ejecutables almacenadas en uno o más medios legibles por ordenador no transitorios. El sistema informático 104 del proveedor de recursos también puede incluir uno o más dispositivos de procesamiento que son capaces de ejecutar el sistema informático 104 del proveedor de recursos para realizar las operaciones descritas en la presente memoria. En algunos aspectos, el sistema informático 104 del proveedor de recursos puede permitir a un usuario participar en el comercio móvil con un sistema informático 106 del usuario del recurso o un sistema informático 110 del usuario posterior del recurso.

Por ejemplo, el usuario u otra entidad que accede al sistema informático 104 del proveedor de recursos puede utilizar el sistema informático 104 del proveedor de recursos para participar en una transacción electrónica con un sistema informático 106 del usuario del recurso a través de un servicio en línea. Una transacción electrónica entre el sistema informático 104 del proveedor de recursos y el sistema informático 106 del usuario del recurso puede incluir, por ejemplo, el sistema informático 106 del usuario del recurso que se utiliza para solicitar una parte del recurso que se distribuye, o que es accedido por el sistema informático 106 del usuario del recurso a través de un servicio en línea, como un servicio de correo electrónico, un servicio VOIP, un servicio de mensajería, u otros servicios en línea que pueden entregar una solicitud del recurso al sistema informático 104 del proveedor de recursos. Por ejemplo, la transacción electrónica puede incluir que el sistema informático 106 del usuario del recurso envíe un correo electrónico a una cuenta de correo electrónico accesible a través del sistema informático 104 del proveedor de recursos para el reembolso del préstamo. Una transacción electrónica entre el sistema informático 104 del proveedor de recursos y el sistema informático 106 del usuario del recurso también puede incluir el sistema informático 104 del proveedor de recursos que se utiliza para distribuir o proporcionar acceso al sistema informático 106 del usuario del recurso a través de un servicio en línea, como una plataforma de distribución de recursos implementada por un sistema de terceros o por el sistema informático 106 del usuario del recurso. Por ejemplo, la transacción electrónica puede incluir que el proveedor de recursos paga una parte de un préstamo al sistema informático 106 del usuario del recurso a través de un servicio de banca en línea.

En respuesta a cada transacción de distribución del recurso, el sistema informático 106 del usuario del recurso está configurado para informar de la distribución del recurso al sistema 100 de gestión segura de recursos de modo que el servidor 118 de gestión segura de recursos pueda actualizar el repositorio 124 de registros del recurso en función de la transacción. La actualización puede incluir una actualización del historial 138 de transacciones del recurso para incluir la transacción de distribución del recurso y una actualización de la información 134 del recurso para actualizar la cantidad no utilizada restante del recurso.

El sistema informático 106 del usuario del recurso o cada sistema informático 110 del usuario posterior del recurso puede incluir uno o más dispositivos, como servidores individuales o grupos de servidores que operan de manera distribuida. Un sistema informático 106 del usuario del recurso o un sistema informático 110 del usuario posterior del recurso puede incluir cualquier dispositivo informático o grupo de dispositivos informáticos operados por un vendedor, prestador, u otro proveedor de productos o servicios. El sistema informático 106 del usuario del recurso o el sistema informático 110 del usuario posterior del recurso puede incluir uno o más dispositivos servidores que incluyen o acceden de otro modo a uno o más medios legibles por ordenador no transitorios. El sistema informático 106 del usuario del recurso o el sistema informático 110 del usuario posterior del recurso también puede ejecutar un servicio en línea. El servicio en línea puede incluir instrucciones ejecutables almacenadas en uno o más medios legibles por ordenador no transitorios. El sistema informático 106 del usuario del recurso o el sistema informático 110 del usuario posterior del recurso puede incluir además uno o más dispositivos de procesamiento que son capaces de ejecutar el servicio en línea para realizar las operaciones descritas en la presente memoria.

Un usuario u otra entidad que accede al sistema informático 106 del usuario del recurso puede utilizar el sistema informático 106 del usuario del recurso para participar en una transacción electrónica con un sistema informático 110

del usuario posterior del recurso a través de un servicio en línea. La transacción electrónica puede incluir transferir los derechos al recurso desde el usuario autorizado del recurso a un usuario posterior del recurso. Después de la transferencia, el usuario posterior del recurso se convierte en el usuario autorizado actual y el usuario autorizado anterior ya no está autorizado a acceder al recurso. Asimismo, el usuario posterior del recurso puede transferir cualquier derecho restante al recurso a otro usuario posterior del recurso.

Antes de una transferencia, un usuario posterior del recurso puede utilizar el sistema informático 110 del usuario posterior del recurso asociado para comunicarse con el sistema 100 de gestión segura de recursos, p. ej., a través del subsistema 112 de cliente orientado al exterior, para enviar una solicitud para verificar el recurso. La solicitud puede incluir verificar la autenticidad del recurso y del transmitente (es decir, si el recurso tiene una parte no utilizada restante como reivindica el transmitente) y si el transmitente es de hecho el usuario autorizado actual del recurso. El servidor 118 de gestión segura de recursos puede procesar la solicitud como se ha descrito anteriormente. Tras recibir los resultados de verificación, el sistema informático 110 del usuario posterior del recurso puede continuar la transacción de transferencia con el transmitente en consecuencia. Es decir, el sistema informático 110 del usuario posterior del recurso puede aceptar la transferencia si el transmitente es el usuario autorizado actual del recurso y el recurso tiene una parte no utilizada restante como reivindica el transmitente. El sistema informático 110 del usuario posterior del recurso puede denegar la transferencia si el transmitente no es el usuario autorizado actual del recurso o la parte no utilizada restante es diferente de lo que reivindica el transmitente.

En algunos ejemplos, el sistema informático 110 del usuario posterior del recurso también puede enviar una solicitud al sistema 100 de gestión segura de recursos para determinar el valor del recurso antes de aceptar la transferencia del recurso. El sistema 100 de gestión segura de recursos puede procesar dicha solicitud utilizando el subsistema 122 de predicción del valor del recurso como se ha discutido anteriormente y devolver el valor previsto del recurso al sistema informático 110 del usuario posterior del recurso. En función del valor previsto, el usuario posterior del recurso puede decidir si proceder o no con la transacción de transferencia.

Si se produjo la transacción de transferencia del recurso, el sistema informático 110 del usuario posterior del recurso está configurado además para informar de dicha transferencia al sistema 100 de gestión segura de recursos de modo que el servidor 118 de gestión segura de recursos pueda actualizar el repositorio 124 de registros del recurso en función de la transacción. La actualización puede incluir una actualización de los datos 136 del usuario del recurso añadiendo datos acerca del nuevo usuario posterior del recurso, una actualización del historial 138 de transacciones de recursos para incluir la transacción de transferencia y otros datos impactados por la transacción. Asimismo, para cada distribución posterior del recurso, el sistema informático 110 del usuario posterior del recurso está configurado además para informar de la distribución al sistema 100 de gestión segura de recursos de modo que el repositorio 124 de registros del recurso pueda actualizarse en consecuencia.

Además de distribuir el recurso al sistema informático 106 del usuario del recurso o al sistema informático 110 del usuario posterior del recurso, el sistema informático 104 del proveedor de recursos también puede configurarse para distribuir el recurso a una o más terceros de confianza a través de los respectivos sistemas informáticos 102 de terceros de confianza. Cada sistema informático 102 de terceros de confianza puede incluir uno o más dispositivos de terceros (p. ej., dispositivos informáticos o grupos de dispositivos informáticos), como servidores individuales o grupos de servidores que operan de manera distribuida. Un sistema informático 102 de terceros de confianza puede incluir cualquier dispositivo informático o grupo de dispositivos informáticos operados por un tercero de confianza como un distribuidor certificado de recursos en línea, una plataforma de recursos en línea, un instituto financiero en línea, etc. Los sistemas informáticos 102 de terceros de confianza pueden configurarse para reenviar el recurso distribuido al usuario autorizado actual del recurso y para almacenar, formatear, y transmitir datos con respecto a la transacción de distribución del recurso al sistema 100 de gestión segura de recursos. Detalles adicionales con respecto al sistema 100 de gestión segura de recursos y a las interacciones entre los diversos sistemas con el sistema 100 de gestión segura de recursos se proporcionan a continuación con respecto a las FIGURAS 2-7.

Las FIGURAS 2A y 2B muestran varios diagramas de flujo que ilustran varios procesos 200A, 200B, 200C y 200D para una gestión segura de recursos. Con fines ilustrativos, los procesos 200A, 200B, 200C y 200D se describen con referencia a las implementaciones descritas anteriormente con respecto a uno o más ejemplos descritos en la presente memoria. Sin embargo, son posibles otras implementaciones. En particular, el proceso 200A ilustra aspectos del sistema informático 104 del proveedor de recursos, el proceso 200B ilustra aspectos del sistema informático 106 del usuario del recurso, el proceso 200C ilustra aspectos de un sistema informático 110 del usuario posterior del recurso, y el proceso 200D ilustra aspectos del servidor 118 de gestión segura de recursos. Los procesos 200A, 200B, 200C y 200D se describirán juntos a continuación.

En algunos aspectos, los pasos en las FIGURAS 2A y 2B pueden implementarse en código de programa que es ejecutado por los respectivos dispositivos informáticos como el sistema informático 104 del proveedor de recursos, el sistema informático 106 del usuario del recurso, los sistemas informáticos 110 de los usuarios posteriores del recurso y el servidor 118 de gestión segura de recursos representados en la FIGURA 1. En algunos aspectos de la presente descripción, una o más operaciones mostradas en las FIGURAS 2A y 2B pueden omitirse o realizarse en un orden diferente. De manera similar, pueden realizarse operaciones adicionales no mostradas en las FIGURAS 2A y 2B.

En el bloque 202, el proceso 200A implica que el sistema informático 104 del proveedor de recursos envíe un mensaje que conceda derechos de uso o propiedad de un recurso a un usuario del recurso. El mensaje también puede incluir información sobre el proveedor de recursos y el recurso. En un ejemplo de un recurso de almacenamiento en línea, el mensaje incluye un acuerdo de que la compañía proveedora de recursos proporcionará el recurso según términos acordados por ambas partes. En un ejemplo donde el recurso es un recurso monetario, el mensaje puede incluir un acuerdo del prestatario del préstamo (es decir, el proveedor de recursos) para devolver el importe del préstamo. El sistema informático 104 del proveedor de recursos envía el mensaje al sistema informático 106 del usuario del recurso.

En el bloque 222, tras recibir el mensaje, el sistema informático 106 del usuario del recurso genera además un mensaje de notificación que describe el evento de recepción de los derechos sobre el recurso y la información asociada al recurso, al proveedor de recursos y al usuario del recurso, o cualquier otra información necesaria para crear un registro 130 del recurso. En algunos ejemplos, el sistema informático 106 del usuario del recurso genera el mensaje de notificación en un formato especificado por el sistema 100 de gestión segura de recursos. El sistema informático 106 del usuario del recurso envía además el mensaje de notificación al servidor 118 de gestión segura de recursos. En el bloque 252, el servidor 118 de gestión segura de recursos crea o instruye al repositorio 124 de registros del recurso para crear un registro 130 del recurso para este recurso en función del mensaje de notificación. La información en el registro 130 del recurso, como los datos 132 del proveedor de recursos, la información 134 del recurso, los datos 136 del usuario del recurso y el historial 138 de transacciones del recurso, puede obtenerse del mensaje de notificación.

En el bloque 204, el sistema informático 104 del proveedor de recursos determina o recibe instrucciones de que una parte del recurso está disponible para su distribución. Por ejemplo, si el recurso es un recurso de almacenamiento en línea, el sistema informático 104 del proveedor de recursos puede determinar que una parte del recurso está disponible determinando que alguna parte de los espacios de almacenamiento en línea es liberada por los usuarios existentes y se vuelve disponible para su uso por otros usuarios, o se añaden nuevos espacios de almacenamiento en línea y los usuarios pueden ponerlos a su disposición. Si el recurso es un recurso monetario, el sistema informático 104 del proveedor de recursos puede detectar o recibir instrucciones de que se añaden fondos adicionales a la cuenta del proveedor de recursos, y una determinada parte de los fondos puede distribuirse al usuario del recurso.

En el bloque 206, el sistema informático 104 del proveedor de recursos distribuye la parte del recurso al sistema informático 106 del usuario del recurso. La parte del recurso puede distribuirse proporcionando un mecanismo al sistema informático 106 del usuario del recurso para acceder al recurso, como enviando una ficha o credenciales de inicio de sesión que pueden utilizarse para acceder a un sistema donde puede recuperarse o utilizarse la parte del recurso. En el bloque 224, el sistema informático 106 del usuario del recurso recibe la parte distribuida del recurso desde el sistema informático 104 del proveedor de recursos o desde el sistema donde puede recuperarse la parte del recurso. El sistema informático 106 del usuario del recurso informa además de la distribución del recurso por parte del sistema informático 104 del proveedor de recursos al servidor 118 de gestión segura de recursos. De manera similar al bloque 222, en algunos ejemplos, el sistema informático 106 del usuario del recurso genera el mensaje de notificación en el formato especificado por el sistema 100 de gestión segura de recursos.

En el bloque 254, el servidor 118 de gestión segura de recursos actualiza el registro 130 del recurso en función del mensaje de notificación. Por ejemplo, el servidor 118 de gestión segura de recursos añade la transacción de distribución del recurso al historial 138 de transacciones del recurso y actualiza la cantidad no utilizada restante del recurso en la información 134 del recurso en función de la cantidad que está siendo distribuida en la transacción de distribución. Los bloques 206, 224 y 254 pueden repetirse cada vez que el sistema informático 104 del proveedor de recursos distribuye una parte del recurso al sistema informático 106 del usuario del recurso.

En algún punto, el usuario del recurso puede decidir transferir el recurso no utilizado a un usuario posterior, porque, por ejemplo, el usuario del recurso ya no tiene la necesidad de utilizar el recurso o el usuario del recurso no espera recibir todo el recurso en una cierta fecha. En ese caso, el proceso 200B avanza al bloque 226 donde el sistema informático 106 del usuario del recurso solicita transferir los derechos del recurso al usuario posterior. En el bloque 232, el sistema informático 110 del usuario posterior del recurso asociado al usuario posterior recibe la solicitud de la transferencia. Antes de aceptar la solicitud, el sistema informático 110 del usuario posterior del recurso puede enviar una solicitud al servidor 118 de gestión segura de recursos para verificar el recurso, incluyendo la naturaleza del recurso, la cantidad no utilizada restante del recurso, el usuario autorizado actual del recurso, etcétera. Por ejemplo, un comprador de deuda puede solicitar al servidor 118 de gestión segura de recursos que verifique el préstamo, la cantidad restante en el préstamo, el acreedor actual del préstamo, etc. Tras recibir la solicitud de verificación, el servidor 118 de gestión segura de recursos realiza la verificación sobre el recurso y el transmitente en función del repositorio 124 de registros del recurso como se describió anteriormente con respecto a la FIGURA 1.

En función de los resultados de verificación, el usuario posterior del recurso puede aceptar la transferencia del recurso en el bloque 236. En otro ejemplo, el sistema informático 110 del usuario posterior del recurso también puede solicitar al servidor 118 de gestión segura de recursos que prediga el valor del recurso no utilizado restante. La decisión de aceptar la transferencia del recurso también puede realizarse en función del valor previsto del recurso. Después de que los derechos sobre el recurso se transfieran desde el usuario del recurso al usuario posterior del recurso, el usuario posterior del recurso puede utilizar el sistema informático 110 del usuario posterior del recurso para informar de la transferencia al servidor 118 de gestión segura de recursos. De nuevo, el mensaje de notificación puede generarse

en un formato especificado por el sistema 100 de gestión segura de recursos. El mensaje de notificación contiene la información requerida para actualizar el registro 130 del recurso en el repositorio 124 de registros del recurso, como la información sobre el usuario posterior del recurso, la cantidad del recurso que se transfiere desde el usuario del recurso al usuario posterior del recurso, etcétera. En el bloque 258, el servidor 118 de gestión segura de recursos actualiza el registro 130 del recurso en función del mensaje de notificación.

En el bloque 240, el sistema informático 110 del usuario posterior del recurso envía una solicitud al sistema informático 104 del proveedor de recursos para solicitar el recurso a distribuir. Debido a que el proveedor de recursos podría no conocer la transferencia del recurso entre el usuario del recurso al usuario del recurso posterior, el proveedor de recursos podría querer validar la autenticidad del usuario posterior del recurso. Como tal, tras recibir la solicitud de distribución del recurso en el bloque 208, el proveedor de recursos puede utilizar el sistema informático 104 del proveedor de recursos para enviar una solicitud al servidor 118 de gestión segura de recursos en el bloque 210 para verificar el usuario posterior del recurso. En el bloque 260, el servidor 118 de gestión segura de recursos determina si el usuario posterior del recurso es el usuario autorizado actual en función del registro 130 del recurso y devuelve los resultados de verificación al sistema informático 104 del proveedor de recursos.

Si el usuario posterior del recurso es de hecho el usuario autorizado actual, el proveedor de recursos podría distribuir el recurso o una parte del mismo que esté disponible al usuario posterior del recurso. En el bloque 242, el sistema informático 110 del usuario posterior del recurso recibe el recurso distribuido o la ficha para acceder al recurso distribuido. En el bloque 244, el sistema informático 110 del usuario posterior del recurso informa además de la distribución del recurso al sistema 100 de gestión segura de recursos, como a través de un mensaje de notificación como se describió anteriormente. En función del informe, el servidor 118 de gestión segura de recursos actualiza el registro 130 del recurso para reflejar la distribución del recurso.

El sistema informático 110 del usuario posterior del recurso puede seguir recibiendo la distribución del recurso desde el sistema informático 104 del proveedor de recursos o puede transferir el recurso no utilizado restante a otro usuario posterior del recurso. Para cada transacción, el servidor 118 de gestión segura de recursos recibe un informe para actualizar el registro 130 del recurso. Los procesos descritos anteriormente pueden continuar hasta que no haya más recursos no utilizados o el usuario autorizado actual determine que el valor del recurso se vuelve despreciable.

Aunque las FIGURAS 2A y 2B describen que el servidor 118 de gestión segura de recursos crea el registro 130 del recurso para un recurso cuando el proveedor de recursos concede los derechos del recurso al usuario del recurso, también pueden utilizarse otras implementaciones. Por ejemplo, el registro 130 del recurso para un recurso puede crearse cuando el recurso se transfiere desde el usuario autorizado inicial a un usuario posterior y actualizarse para cada transacción producida posteriormente. Esto se debe a que las solicitudes fraudulentas de recursos se producen, principalmente, después de que se transfiera el recurso, lo que lleva a confusión al proveedor de recursos en cuanto a qué usuario es el usuario autorizado.

Además, para algunos recursos, como los recursos monetarios como préstamos, reglamentos y normas (como Metro II) establecen requisitos y un marco de notificación para la información sobre el origen y el reembolso de préstamos cuando se notifica a una agencia de información crediticia. En dicho ejemplo, la información con respecto al recurso y al usuario autorizado ya se ha grabado y no es necesario duplicarla en el registro 130 del recurso. En este ejemplo, el registro 130 del recurso puede crearse después de que se transfiera el recurso desde el acreedor inicial (el usuario del recurso) a un comprador de deuda o a un cobrador de deudas (el usuario posterior del recurso) y en función del mensaje de notificación con respecto a la transferencia. Desde allí, el comprador de deuda o cobrador de deudas puede configurar su sistema informático 110 del usuario posterior del recurso para informar de cada pago realizado por el prestatario del préstamo (proveedor de recursos) al servidor 118 de gestión segura de recursos. De manera similar, si el préstamo se transfiere además a otro comprador de deuda o cobrador de deudas (otro usuario posterior del recurso), el comprador de deuda o cobrador de deudas posterior puede informar de la transferencia y de cualquier pago del préstamo al servidor 118 de gestión segura de recursos.

Antes de adquirir el préstamo (es decir, aceptar la transferencia), un comprador de deuda o cobrador de deudas puede solicitar al servidor 118 de gestión segura de recursos que verifique el préstamo, la cantidad restante en el préstamo y el acreedor del préstamo. Además, como parte de su decisión de adquirir el préstamo, el comprador de deuda o cobrador de deudas puede solicitar al servidor 118 de gestión segura de recursos que prediga el valor del préstamo. Un proceso similar puede aplicarse a otros tipos de recursos.

La FIGURA 3 representa un ejemplo de un proveedor de recursos que distribuye recursos a través del servidor 118 de gestión segura de recursos según los aspectos presentados en la presente memoria. En el bloque 302, el proveedor de recursos determina, de manera similar al bloque 204, que una parte del recurso se vuelve disponible para su distribución. En el bloque 304, el sistema informático 104 del proveedor de recursos distribuye la parte del recurso de forma similar al bloque 206. A diferencia del bloque 206, el recurso se distribuye al servidor 118 de gestión segura de recursos en lugar de al usuario autorizado actual. Esto elimina la carga del usuario del recurso de informar de la transacción de distribución del recurso al servidor 118 de gestión segura de recursos.

En el bloque 322, el servidor 118 de gestión segura de recursos recibe la distribución del recurso de forma similar a un usuario del recurso que recibe la distribución del recurso como se describe con respecto a los bloques 224 y 242. En el bloque 324, el servidor 118 de gestión segura de recursos determina el usuario autorizado actual en función de los registros 130 del recurso almacenados en el repositorio 124 de registros del recurso. En el bloque 326, el servidor 118 de gestión segura de recursos redistribuye la parte del recurso al usuario autorizado actual a través del dispositivo informático del usuario del recurso asociado al usuario autorizado. El dispositivo informático del usuario del recurso recibe la distribución del recurso en el bloque 312. En el bloque 328, el servidor 118 de gestión segura de recursos actualiza el registro 130 del recurso en función de la distribución del recurso.

La FIGURA 4 representa un ejemplo de un proveedor de recursos que distribuye recursos a través de un tercero de confianza según los aspectos presentados en la presente memoria. En el bloque 402, el proveedor de recursos determina que una parte del recurso se vuelve disponible para su distribución de forma similar a los bloques 204 y 302. En el bloque 404, el proveedor de recursos identifica un distribuidor de recursos de terceros de confianza. Un tercero de confianza puede ser un distribuidor certificado de recursos en línea, una plataforma de recursos en línea, un instituto financiero en línea, etc. El proveedor de recursos puede identificar al tercero de confianza consultando al sistema 100 de gestión segura de recursos que puede mantener una lista de distribuidores de recursos de terceros de confianza. Alternativamente, o adicionalmente, el proveedor de recursos puede seleccionar un distribuidor de recursos en que el proveedor de recursos confía en función de, por ejemplo, la reputación del tercero o de la experiencia pasada del proveedor de recursos con el tercero.

En el bloque 406, el sistema informático 104 del proveedor de recursos distribuye la parte del recurso al sistema informático 102 de terceros de confianza. En el bloque 412, los dispositivos informáticos 102 de terceros de confianza reciben la parte del recurso y en el bloque 414, los dispositivos informáticos 102 de terceros de confianza determinan el usuario autorizado actual del recurso consultando al servidor 118 de gestión segura de recursos. En respuesta a la recepción de la consulta, el servidor 118 de gestión segura de recursos recupera la información sobre el usuario actual del recurso en función del registro 130 del recurso almacenado en el repositorio 124 de registros del recurso. En función de dicha información, los dispositivos informáticos 102 de terceros de confianza distribuyen la parte del recurso al usuario autorizado en el bloque 416 a través del correspondiente sistema informático 106 del usuario del recurso o sistema informático 110 del usuario posterior del recurso. El sistema informático 106 asociado al usuario autorizado actual recibe el recurso distribuido en el bloque 422.

Los dispositivos informáticos 102 de terceros de confianza informan, además, en el bloque 418, de la distribución del recurso al servidor 118 de gestión segura de recursos, p. ej., enviando un mensaje de notificación en un formato especificado por el sistema 100 de gestión segura de recursos. El servidor 118 de gestión segura de recursos, en el bloque 434, recibe el mensaje de notificación y actualiza el registro 130 del recurso en consecuencia. Enviar el recurso a un tercero de confianza elimina la carga del usuario del recurso de informar de la distribución del recurso y la carga del servidor 118 de gestión segura de recursos de recibir y redistribuir el recurso.

La FIGURA 5 representa otro ejemplo de un proveedor de recursos que distribuye recursos a través de un tercero de confianza según los aspectos presentados en la presente memoria. En el bloque 502, el proveedor de recursos determina que una parte del recurso se vuelve disponible para su distribución de forma similar a los bloques 204, 302 y 402. En el bloque 504, el sistema informático 104 del proveedor de recursos se comunica con el servidor 118 de gestión segura de recursos para solicitar el usuario autorizado actual del recurso. En el bloque 532, el servidor 118 de gestión segura de recursos identifica al usuario autorizado actual del recurso en función del registro 130 del recurso en el repositorio 124 de registros del recurso.

En el bloque 506, el sistema informático 104 del proveedor de recursos se comunica con un dispositivo informático 102 de terceros de confianza para distribuir el recurso al tercero de confianza. El sistema informático 104 del proveedor de recursos también transmite la información sobre el usuario autorizado actual del recurso a los dispositivos informáticos 102 de terceros de confianza. En el bloque 512, el dispositivo informático 102 de terceros de confianza recibe la parte distribuida del recurso y la información del usuario autorizado actual. En el bloque 514, el dispositivo informático 102 de terceros de confianza distribuye la parte del recurso al usuario autorizado actual a través del sistema informático asociado al usuario autorizado. El sistema informático del usuario del recurso recibe la parte distribuida del recurso en el bloque 522. En el bloque 516, el dispositivo informático 102 de terceros de confianza informa de la distribución del recurso al servidor 118 de gestión segura de recursos, en función de la cual, el servidor 118 de gestión segura de recursos actualiza el registro 130 del recurso para el recurso en el repositorio 124 de registros del recurso en el bloque 534.

Un proveedor de recursos puede utilizar cualquiera de los mecanismos de distribución de recursos descritos anteriormente con respecto a las FIGURAS 3-5. El proveedor de recursos también puede distribuir el recurso mediante otras formas siempre que la distribución del recurso se informe al servidor 118 de gestión segura de recursos.

La FIGURA 6 es un diagrama de flujo que ilustra un ejemplo de un proceso 600 para gestionar transacciones de recursos para evitar el acceso fraudulento a los recursos según ciertos aspectos de la presente descripción. Con fines ilustrativos, el proceso 600 se describe con referencia a las implementaciones descritas anteriormente con respecto a uno o más ejemplos descritos en la presente memoria. Sin embargo, son posibles otras implementaciones. En algunos

aspectos, los pasos en la FIGURA 6 pueden implementarse en código de programa que es ejecutado por uno o más dispositivos informáticos, como el servidor 118 de gestión segura de recursos representado en la FIGURA 1. En algunos aspectos de la presente descripción, una o más operaciones mostradas en la FIGURA 6 pueden omitirse o realizarse en un orden diferente. De manera similar, pueden realizarse operaciones adicionales no mostradas en la FIGURA 6.

En el bloque 602, el proceso 600 implica recibir un mensaje de notificación de transacción del recurso. Como se ha descrito anteriormente con respecto a las FIGURAS 1-5, el mensaje de notificación puede generarse en respuesta a que el proveedor de recursos concede los derechos del recurso al usuario del recurso, distribuyéndose una parte del recurso al usuario del recurso con o sin un tercero de confianza, o transfiriéndose el recurso de un usuario a otro usuario.

En el bloque 604, el servidor 118 de gestión segura de recursos crea o actualiza un registro 130 del recurso para el recurso dependiendo del tipo del mensaje de notificación. Si el mensaje de notificación es para el proveedor de recursos que concede los derechos del recurso al usuario del recurso, el servidor 118 de gestión segura de recursos crea un registro 130 del recurso para el recurso en el repositorio 124 de registros del recurso. Si el mensaje de notificación es para distribución o transferencia del recurso, el servidor 118 de gestión segura de recursos actualiza el registro 130 del recurso en función de la transacción descrita en el mensaje de notificación. El proceso 600 puede repetir los bloques 602 y 604 a medida que se reciben nuevos mensajes de notificación en el servidor 118 de gestión segura de recursos.

En el bloque 606, el proceso 600 implica recibir una solicitud para verificar un recurso y el usuario autorizado del recurso. La solicitud puede pedir al servidor 118 de gestión segura de recursos que verifique la autenticidad de un recurso dado y que determine si la cantidad no utilizada restante del recurso y su usuario autorizado actual coinciden con los almacenados en el registro 130 del recurso. La solicitud puede pedir, alternativamente, información detallada acerca de un recurso dado, incluyendo la identificación del recurso, la cantidad no utilizada restante, y el usuario autorizado actual. En respuesta a la solicitud, en el bloque 608, el servidor 118 de gestión segura de recursos busca el repositorio 124 de registros del recurso para recuperar el registro 130 del recurso correspondiente al recurso para su verificación.

En el bloque 610, el servidor 118 de gestión segura de recursos determina si la solicitud pide además una predicción del valor esperado del recurso. En algunos escenarios, como cuando un usuario posterior del recurso decide si aceptar la transferencia del recurso, el usuario posterior del recurso puede solicitar al servidor 118 de gestión segura de recursos que proporcione una estimación o una predicción sobre el valor esperado del recurso para evaluar si vale la pena aceptar la transferencia. Por ejemplo, un comprador de deuda puede querer conocer el valor esperado del préstamo restante antes de adquirir el préstamo del acreedor actual. Si se recibe una solicitud para predecir el valor esperado del recurso, el proceso 600 implica, en el bloque 612, entrenar y utilizar un modelo de predicción para predecir el valor esperado del recurso en el momento de la solicitud.

En un ejemplo, el subsistema 122 de predicción del valor del recurso puede utilizarse para construir un modelo estadístico para predecir el valor esperado del recurso. El modelo estadístico requiere dos elementos: una definición de rendimiento que estipula el marco temporal y el comportamiento necesario para identificar lo que se va a predecir (Y), y predictores que se utilizan para generar estimaciones de parámetros asociadas a un conjunto de variables o atributos utilizados para predecir Y. El subsistema 122 de predicción del valor del recurso predice el valor esperado del recurso prediciendo la probabilidad (p. ej., la probabilidad o posibilidad) del recurso que se distribuye, como la probabilidad de que un consumidor reembolse el préstamo. El subsistema 122 de predicción del valor del recurso determina además una cantidad o un importe asociado al recurso no utilizado restante.

Para predecir la probabilidad de la distribución del recurso, la definición de rendimiento puede definirse a lo largo de un intervalo de tiempo limitado, como un mes, dos meses, seis meses, u otro intervalo relativamente corto correspondiente al lapso de tiempo que un usuario del recurso puede intentar obtener el recurso antes de transferirlo a otro usuario. Un comportamiento de distribución del recurso positivo se define como uno (1), y un fallo o comportamiento de distribución negativo se define como cero (0). El resultado previsto es una variable dependiente binaria.

El conjunto de atributos del predictor puede extraerse de los registros 130 del recurso para el proveedor de recursos, o datos alternativos distintos de los registros 130 del recurso. Puede incluirse conocimientos, como el tiempo que el recurso ha estado distribuido de forma incompleta, como atributos para predecir la probabilidad de distribución del recurso. Por ejemplo, el subsistema 122 de predicción del valor del recurso puede determinar el número de veces que un recurso particular ha sido transferido a un usuario posterior del recurso y cuánto de la cantidad original del recurso permanece en la transferencia. Estos atributos podrían utilizarse para predecir la probabilidad de distribución del recurso por parte del proveedor de recursos.

En un ejemplo, el modelo para predecir la probabilidad de distribución del recurso es

$$P(Y = 1) = f(\boldsymbol{XB}), \qquad (1)$$

donde *Y* toma el valor 1 si el proveedor de recursos ha distribuido el recurso, y 0 en caso contrario. La matriz *X* contiene los atributos del predictor candidato seleccionado del registro 130 del recurso o datos alternativos y el vector *B* contiene estimaciones de parámetros que determinan la relación entre los predictores e *Y*. Diversas formas funcionales *f* pueden utilizarse para estimar los parámetros en este modelo, como un modelo de regresión logística o un modelo probit. Los modelos de aprendizaje automático, como redes neuronales, también pueden utilizarse para estimar los parámetros del modelo. En función del modelo seleccionado, puede calcularse la probabilidad de distribución del recurso, que se encuentra en [0,1] y define la probabilidad de distribución de todo el recurso.

El modelo puede modificarse para acomodar una distribución parcial del recurso, que puede ser más útil para el usuario posterior del recurso, como posteriores compradores de deuda de préstamos. En este ejemplo, estos compradores de deuda pueden no estar interesados en intentar recuperar la cantidad completa del préstamo (aunque podría desear) ya que el esfuerzo de recuperación final para los últimos recursos restantes puede tener un coste superior al rendimiento del esfuerzo.

Como se mencionó anteriormente, el subsistema 122 de predicción del valor del recurso está configurado además para predecir una cantidad o un importe asociado al recurso no utilizado restante. En un ejemplo, la cantidad puede predecirse como la cantidad de recurso que no se ha distribuido a los usuarios. En este ejemplo, el modelo para calcular la cantidad de recursos que un usuario posterior del recurso recibirá viene dado por

$$E(\text{ recurso recibido }) = P(Y = 1) \times (\text{cantidad del recurso no distribuido}). \qquad (2)$$

En palabras, el valor esperado o la cantidad esperada que un usuario del recurso puede recibir de la distribución del proveedor de recursos se determina por las características del proveedor de recursos definidas en la Ecuación (1) anterior, que genera la probabilidad de distribución del recurso. Esta probabilidad multiplicada por la cantidad de los recursos no distribuidos conducirá a la cantidad de recursos que puede recibir un usuario del recurso. Este modelo, sin embargo, puede ser simplista ya que no hace suposiciones sobre las características del proveedor de recursos en términos de la capacidad del proveedor para distribuir el recurso.

Por ejemplo, considere dos proveedores de recursos, cada uno de los cuales concedió, originalmente, recursos monetarios, como préstamos no garantizados de $100.000. Uno de los proveedores de recursos ha perdido su trabajo y no ha encontrado empleo desde entonces, mientras que el otro proveedor de recursos sigue empleado. Supongamos de otro modo que estos dos proveedores de recursos son, demográficamente, idénticos, y que sus otros datos como datos de crédito son idénticos. Es probable que la probabilidad de reembolso para estos dos individuos sea idéntica, lo que induce a error a los usuarios posteriores, como un cobrador de deudas, a aplicar el mismo esfuerzo de recuperación a ambas cuentas. Para proporcionar una mejor predicción, la cantidad de recursos que se estima recuperable puede ajustarse haciendo uso del dato adicional (alternativo) de que un proveedor de recursos está desempleado.

Puede utilizarse un nuevo modelo para la cantidad de recursos que pueden recibirse para proporcionar una estimación más precisa de la parte del recurso restante que podría recuperarse. Por ejemplo, la cantidad del recurso no distribuido utilizada en la Ecuación (2) puede ajustarse considerando el historial de distribución del recurso del proveedor de recursos. Con este ajuste, el modelo en la Ecuación (2) se convierte:

$$E(\text{ recurso recibido }) \qquad (3)$$

$$= P(Y = 1) \times (\text{ cantidad ajustada del recurso a recibir en el intervalo t }).$$

Factores como la falta de empleo afectarán a la cantidad de recursos que pueden ser recibidos por el usuario del recurso. El valor esperado de las cantidades de recursos a recibir de los proveedores de recursos puede tener un ordenamiento de rango diferente al de la Ecuación (2). Esto proporciona a los usuarios del recurso unas expectativas más realistas sobre qué proveedores de recursos es probable que proporcionen la totalidad de recursos. Esto facilita a un usuario posterior del recurso en su decisión de si adquirir el recurso no distribuido del usuario autorizado actual y cuánto pagar por dichos recursos no distribuidos.

El proceso anterior de predecir la cantidad de recursos a recibir puede realizarse automáticamente. Los datos utilizados para estimar cada elemento de los modelos anteriores se almacenan en datos estructurados en el repositorio 124 de registros del recurso, que es una cadena híbrida de la cadena de bloques de custodia. El servidor 118 de gestión segura de recursos puede extraer y convertir la información del repositorio 124 de registros del recurso en atributos que describen cantidades del recurso no distribuido, cantidades distribuidas a lo largo del tiempo, y otros elementos utilizados para predecir la probabilidad de distribución o para ajustar la cantidad que se espera distribuir.

A medida que los usuarios del recurso reciben la distribución del recurso y actualizan el repositorio 124 de registros del recurso, la información actualizada puede utilizarse para automatizar la estimación o actualizar estimaciones de *E*

(recurso recibido). Los modelos que pueden utilizarse para estimar la probabilidad de distribución del recurso incluyen, pero no se limitan a, modelos de regresión logística, modelos probit, o modelos de aprendizaje automático. Estos modelos de aprendizaje automático podrían incluir redes neuronales, modelos basados en árboles, o modelos de aprendizaje profundo que pueden incorporar tiempo en su estimación, como redes neuronales convolucionales. La regresión logarítmica-lineal, las redes neuronales, o los modelos de aprendizaje profundo también pueden utilizarse para estimar la cantidad de recursos que se espera distribuir. El servidor 118 de gestión segura de recursos puede ejecutar estos modelos para predecir la cantidad de recursos a recibir bajo demanda (es decir, tras recibir una solicitud) o en una programación para refinar, continuamente, el modelo y actualizar E(recurso recibido). Las salidas del modelo refinado reflejan las últimas actualizaciones en los registros 130 del recurso de los usuarios del recurso y del proveedor de recursos.

En el bloque 614, el proceso 600 implica que el servidor 118 de gestión segura de recursos transmita la información solicitada, incluyendo la información de recursos, el usuario autorizado y el valor previsto del recurso, a la entidad solicitante. El proceso 600 puede repetirse hasta que el recurso esté completamente distribuido (p. ej., la capacidad de almacenamiento completa se ha utilizado para el término completo, o se paga el préstamo), o el usuario autorizado actual decide no seguir la distribución del recurso (p. ej., el usuario actual del recurso ya no necesita el recurso y decide no transferirlo a un usuario posterior o el acreedor decide que el coste del cobro de la deuda supera el valor de la deuda).

Aunque la descripción anterior se centra en predecir el valor esperado del recurso, el servidor 118 de gestión segura de recursos también puede utilizar el subsistema 122 de predicción del valor del recurso u otros subsistemas para predecir la pérdida esperada del recurso. La pérdida esperada del recurso mide la expectativa sobre la cantidad del recurso por la que un usuario del recurso o un usuario posterior del recurso no recibirá la distribución. De manera similar al valor esperado del recurso, la pérdida esperada del recurso también puede ser utilizada por usuarios posteriores del recurso para evaluar si vale la pena aceptar la transferencia del recurso.

Para determinar la pérdida esperada del recurso, el servidor 118 de gestión segura de recursos puede construir y utilizar un modelo estadístico o un modelo de aprendizaje automático para predecir la probabilidad de que el recurso no se distribuya dentro de un cierto período de tiempo. Estos modelos pueden construirse de forma similar a los modelos utilizados para predecir la probabilidad de que el recurso se distribuya como se ha discutido anteriormente. Esta probabilidad prevista de que el recurso no se distribuya puede combinarse con la cantidad prevista o la cantidad ajustada asociada al recurso no utilizado restante, como se ha discutido anteriormente para determinar la pérdida esperada del recurso. Por ejemplo, la pérdida esperada del recurso puede determinarse reemplazando P(Y=1) en las Ecuaciones (1) o (2) con la probabilidad prevista de que el recurso no se distribuya dentro del periodo de tiempo.

Ejemplo de entorno informático para una gestión segura de recursos

Cualquier sistema informático o grupo de sistemas informáticos adecuado puede utilizarse para realizar las operaciones para las operaciones de aprendizaje automático descritas en la presente memoria. Por ejemplo, la FIGURA 7 es un diagrama de bloques que representa un ejemplo de un dispositivo informático 700, que puede utilizarse para implementar el servidor 118 de gestión segura de recursos, el sistema informático 104 del proveedor de recursos, el sistema 106 informático del usuario del recurso, el sistema informático 110 del usuario posterior del recurso o el dispositivo informático 102 de terceros de confianza. El dispositivo informático 700 puede incluir diversos dispositivos para comunicarse con otros dispositivos en el sistema 100 de gestión segura de recursos, como se describe con respecto a la FIGURA 1. El dispositivo informático 700 puede incluir diversos dispositivos para realizar una o más operaciones de gestión segura de recursos descritas anteriormente con respecto a las FIGURAS 1-8.

El dispositivo informático 700 puede incluir un procesador 702 que está acoplado, de forma comunicativa, a una memoria 704. El procesador 702 ejecuta un código de programa ejecutable por ordenador almacenado en la memoria 704, accede a la información almacenada en la memoria 704, o ambos. El código de programa puede incluir instrucciones ejecutables por máquina que pueden representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de software, una clase, o cualquier combinación de instrucciones, estructuras de datos, o declaraciones del programa. Un segmento de código puede acoplarse a otro segmento de código o un circuito de hardware pasando o recibiendo información, datos, argumentos, parámetros, o contenidos de memoria. La información, argumentos, parámetros, datos, etc. puede pasarse, enviarse, o transmitirse a través de cualquier medio adecuado incluyendo compartición de memoria, paso de mensajes, paso de fichas, transmisión de red, entre otros.

Los ejemplos de un procesador 702 incluyen un microprocesador, un circuito integrado de aplicación específica, una matriz de puertas programable in situ, o cualquier otro dispositivo de procesamiento adecuado. El procesador 702 puede incluir cualquier número de dispositivos de procesamiento, incluyendo uno. El procesador 702 puede incluir o comunicarse con una memoria 704. La memoria 704 almacena código de programa que, cuando es ejecutado por el procesador 702, hace que el procesador realice las operaciones descritas en esta descripción.

La memoria 704 puede incluir cualquier medio legible por ordenador no transitorio adecuado. El medio legible por ordenador puede incluir cualquier dispositivo de almacenamiento electrónico, óptico, magnético u otro capaz de

proporcionar un procesador con código de programa legible por ordenador u otro código de programa. Ejemplos no limitantes de un medio legible por ordenador incluyen un disco magnético, un chip de memoria, un almacenamiento óptico, una memoria flash, una memoria de clase de almacenamiento, una ROM, una RAM, un ASIC, un almacenamiento magnético, o cualquier otro medio desde el cual un procesador informático pueda leer y ejecutar código de programa. El código de programa puede incluir código de programa específico del procesador generado por un compilador o un intérprete a partir de código escrito en cualquier lenguaje de programación informática adecuado. Ejemplos de lenguajes de programación adecuados incluyen Hadoop, C, C++, C#, Visual Basic, Java, Scala, Python, Perl, JavaScript, ActionScript, etc.

El dispositivo informático 700 también puede incluir varios dispositivos externos o internos como dispositivos de entrada o de salida. Por ejemplo, el dispositivo informático 700 se muestra con una interfaz 708 de entrada/salida que puede recibir una entrada de los dispositivos de entrada o proporcionar una salida a los dispositivos de salida. También puede incluirse un bus 706 en el dispositivo informático 700. El bus 706 puede acoplar, de forma comunicativa, uno o más componentes del dispositivo informático 700.

El dispositivo informático 700 puede ejecutar un código 714 del programa como el subsistema 120 de verificación de recursos o el subsistema 122 de predicción del valor del recurso. El código 714 del programa puede residir en cualquier medio legible por ordenador adecuado y puede ejecutarse en cualquier dispositivo de procesamiento adecuado. Por ejemplo, como se representa en la FIGURA 7, el código 714 del programa puede residir en la memoria 704 en el dispositivo informático 700 junto con los datos 716 del programa asociados al código 714 del programa, como el mensaje de notificación, el modelo de predicción del valor del recurso, o el valor previsto. La ejecución del código 714 del programa puede configurar el procesador 702 para realizar las operaciones descritas en la presente memoria.

En algunos aspectos, el dispositivo informático 700 puede incluir uno o más dispositivos de salida. Un ejemplo de un dispositivo de salida es el dispositivo 710 de interfaz de red representado en la FIGURA 7. Un dispositivo 710 de interfaz de red puede incluir cualquier dispositivo o grupo de dispositivos adecuado para establecer una conexión de datos por cable o inalámbrica a una o más redes de datos descritas en la presente memoria. Los ejemplos no limitantes del dispositivo 710 de interfaz de red incluyen un adaptador de red Ethernet, un módem, etc.

Otro ejemplo de un dispositivo de salida es el dispositivo 712 de presentación representado en la FIGURA 7. Un dispositivo 712 de presentación puede incluir cualquier dispositivo o grupo de dispositivos adecuado para proporcionar una salida visual, auditiva, u otra salida sensorial adecuada. Los ejemplos no limitantes del dispositivo 712 de presentación incluyen una pantalla táctil, un monitor, un altavoz, un dispositivo informático móvil separado, etc. En algunos aspectos, el dispositivo 712 de presentación puede incluir un dispositivo informático de cliente remoto que se comunica con el dispositivo informático 700 utilizando una o más redes de datos descritas en la presente memoria. En otros aspectos, el dispositivo 712 de presentación puede omitirse.

Consideraciones generales

En la presente memoria se exponen numerosos detalles específicos para proporcionar una comprensión exhaustiva de la materia reivindicada. Sin embargo, los expertos en la técnica entenderán que la materia reivindicada puede ponerse en práctica sin estos detalles específicos. En otros casos, los métodos, aparatos, o sistemas que serían conocidos por una persona de conocimiento ordinario no se han descrito en detalle para no oscurecer la materia reivindicada.

A menos que se indique específicamente lo contrario, se aprecia que a lo largo de esta especificación términos como "procesamiento", "computación", "determinación" e "identificación", o similares, se refieren a acciones o procesos de un dispositivo informático, como uno o más ordenadores o un dispositivo o dispositivos informáticos electrónicos similares, que manipulan o transforman datos representados como cantidades físicas electrónicas o magnéticas dentro de memorias, registros, u otros dispositivos de almacenamiento de información, dispositivos de transmisión, o dispositivos de visualización de la plataforma informática.

El sistema o sistemas discutidos en la presente memoria no se limitan a ninguna arquitectura o configuración de hardware particular. Un dispositivo informático puede incluir cualquier disposición adecuada de componentes que proporcione un resultado condicionado a una o más entradas. Los dispositivos informáticos adecuados incluyen sistemas informáticos basados en microprocesadores multipropósito que acceden a software almacenado que programa o configura el sistema informático desde un aparato informático de propósito general a un aparato informático especializado que implementa uno o más aspectos de la presente materia. Puede utilizarse cualquier lenguaje de programación, de secuencia de comandos u otro tipo de lenguaje o combinaciones de lenguajes adecuados para implementar las enseñanzas contenidas en la presente memoria en un software que se utilizará para programar o configurar un dispositivo informático.

Aspectos de los métodos descritos en la presente memoria pueden realizarse en el funcionamiento de dichos dispositivos informáticos. El orden de los bloques presentados en los ejemplos anteriores puede variarse - por ejemplo, los bloques pueden reordenarse, combinarse, o dividirse en sub bloques. Ciertos bloques o procesos pueden realizarse en paralelo.

El uso de "adaptado a" o "configurado para" en la presente memoria se entiende como un lenguaje abierto e inclusivo que no excluye dispositivos adaptados o configurados para realizar tareas o pasos adicionales. Adicionalmente, el uso de " en función de" pretende ser abierto e inclusivo, en que un proceso, paso, cálculo, u otra acción "en función de" una o más condiciones o valores enumerados puede, en la práctica, basarse en condiciones o valores adicionales más allá de los enumerados. Los títulos, listas y numeración incluidos en la presente memoria son sólo para facilitar la explicación y no pretenden ser limitantes.

Aunque la presente materia se ha descrito en detalle con respecto a aspectos específicos de la misma, se apreciará que los expertos en la técnica, tras lograr una comprensión de lo anterior, pueden producir, fácilmente, alteraciones, variaciones y equivalentes a dichos aspectos. Cualquier aspecto o ejemplo puede combinarse con cualquier otro aspecto o ejemplo. En consecuencia, debe entenderse que la presente descripción se ha presentado con fines de ejemplo en lugar de limitación, y no excluye la inclusión de dichas modificaciones, variaciones, o adiciones a la presente materia como sería fácilmente evidente para una persona de conocimiento ordinario en la técnica.

REIVINDICACIONES

1. Un método (600) que incluye uno o más dispositivos (702) de procesamiento de un sistema (100) de gestión segura de recursos que realiza operaciones que comprenden:

recibir (606) una solicitud para verificar un usuario autorizado de un recurso;
en respuesta a la recepción de la solicitud, consultar (608) un repositorio (124) de registros del recurso;
determinar, a partir de una cadena de bloques privada, un usuario del recurso que, actualmente, tiene derecho a obtener el recurso como el usuario autorizado del recurso;
transmitir (614), en respuesta a la solicitud, un resultado de verificación a un dispositivo informático (104, 110) remoto, identificando el resultado de verificación al usuario autorizado del recurso, en donde el resultado de verificación puede utilizarse para conceder acceso al recurso al usuario autorizado;
caracterizado por que el repositorio de registros del recurso se implementa en una cadena de bloques híbrida, comprendiendo la cadena de bloques híbrida (a) la cadena de bloques privada que almacena un registro (130) del recurso que comprende información de un proveedor de recursos del recurso (132), información de los usuarios del recurso que tienen derecho a obtener el recurso (136), y un historial (138) de transacciones del recurso y (b) una cadena de bloques pública que almacena una versión cifrada del historial de transacciones del recurso contenido en el registro del recurso, de manera que la cadena de bloques pública pueda utilizarse para verificar la autenticidad de una transacción que involucre el recurso, y en donde la cadena de bloques pública es accesible, directamente, a través de una red (108) de datos pública y la cadena de bloques privada sólo es accesible por el sistema de gestión segura de recursos.

2. El método (600) de la reivindicación 1, que comprende, además:

recibir (602) un mensaje de notificación de transacción del recurso; y
actualizar (604) el repositorio (124) de registros del recurso en función del mensaje de notificación de transacción del recurso.

3. El método (600) de la reivindicación 2, en donde el mensaje de notificación de transacción del recurso comprende datos que describen una distribución del recurso o una transferencia del recurso.

4. El método (600) de la reivindicación 1, que comprende, además:

entrenar y utilizar un modelo para predecir la probabilidad de que el recurso esté disponible dentro de un período de tiempo dado;
determinar la cantidad del recurso disponible dentro del periodo de tiempo dado; y
generar una predicción de un valor del recurso combinando la probabilidad de que el recurso esté disponible dentro del periodo de tiempo dado y la cantidad del recurso disponible dentro del periodo de tiempo dado.

5. El método (600) de la reivindicación 4, que comprende, además:

en respuesta a determinar que se recibe una solicitud para la predicción del valor del recurso, generar la predicción del valor del recurso; y
transmitir la predicción del valor del recurso a un dispositivo informático remoto.

6. El método (600) de la reivindicación 1, que comprende, además:

entrenar y utilizar un modelo para predecir la probabilidad de que el recurso no esté disponible dentro de un período de tiempo dado;
determinar la cantidad del recurso asociada al periodo de tiempo dado; y
generar una predicción de una pérdida del recurso combinando la probabilidad de que el recurso no esté disponible dentro del periodo de tiempo dado y la cantidad del recurso asociada al periodo de tiempo dado.

7. Un sistema (100) de gestión segura de recursos, que comprende:

un repositorio (124) de registros del recurso configurado para almacenar un registro (130) del recurso para un recurso; y
un subsistema (120) de verificación de recursos configurado para realizar el método de cualquiera de las reivindicaciones 1-3

caracterizado por que el repositorio de registros del recurso se implementa en una cadena de bloques híbrida, comprendiendo la cadena de bloques híbrida (a) una cadena de bloques privada que almacena el registro (130) del recurso que comprende información de un proveedor de recursos del recurso (132), información de los usuarios del recurso que tienen un derecho a obtener el recurso (136), y un historial (138) de transacciones del recurso y (b) una cadena de bloques pública que almacena una versión cifrada del historial de transacciones del recurso contenido en el registro del recurso, de manera que la

cadena de bloques pública pueda utilizarse para verificar la autenticidad de una transacción que involucre el recurso, y en donde la cadena de bloques pública es accesible, directamente, a través de una red (108) de datos pública y la cadena de bloques privada sólo es accesible por el sistema de gestión segura de recursos.

8. El sistema (100) de gestión segura de recursos de la reivindicación 5, que comprende además un subsistema (122) de predicción del valor del recurso configurado para realizar acciones que comprenden los pasos del método de las reivindicaciones 4-6.

9. Un soporte (704) de almacenamiento legible por ordenador no transitorio que tiene un código (714) del programa que es ejecutable por un dispositivo procesador (704) para hacer que un dispositivo informático (700) realice operaciones, comprendiendo las operaciones el método de cualquiera de las reivindicaciones 1-6.

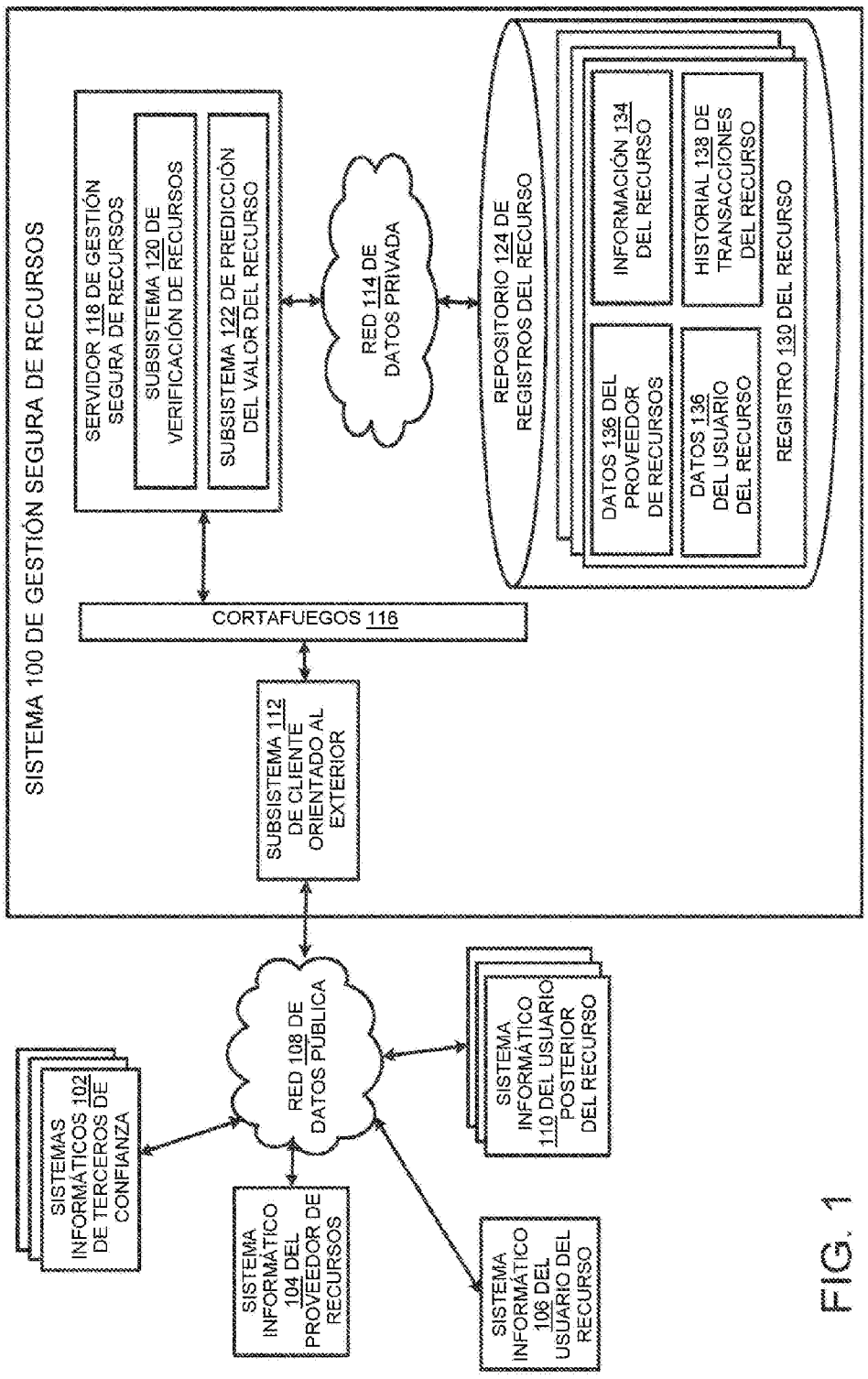
SISTEMA 100 DE GESTIÓN SEGURA DE RECURSOS
SERVIDOR 118 DE GESTIÓN SEGURA DE RECURSOS
SUBSISTEMA 120 DE VERIFICACIÓN DE RECURSOS
SUBSISTEMA 122 DE PREDICCIÓN DEL VALOR DEL RECURSO
RED 114 DE DATOS PRIVADA
REPOSITORIO 124 DE REGISTROS DEL RECURSO
INFORMACIÓN 134 DEL RECURSO
HISTORIAL 138 DE TRANSACCIONES DEL RECURSO
DATOS 136 DEL PROVEEDOR DE RECURSOS
DATOS 136 DEL USUARIO DEL RECURSO
REGISTRO 130 DEL RECURSO
CORTAFUEGOS 116
SUBSISTEMA 112 DE CLIENTE ORIENTADO AL EXTERIOR
SISTEMAS INFORMÁTICOS 102 DE TERCEROS DE CONFIANZA
RED 108 DE DATOS PÚBLICA
SISTEMA INFORMÁTICO 110 DEL USUARIO POSTERIOR DEL RECURSO
SISTEMA INFORMÁTICO 104 DEL PROVEEDOR DE RECURSOS
SISTEMA INFORMÁTICO 106 DEL USUARIO DEL RECURSO

FIG. 1

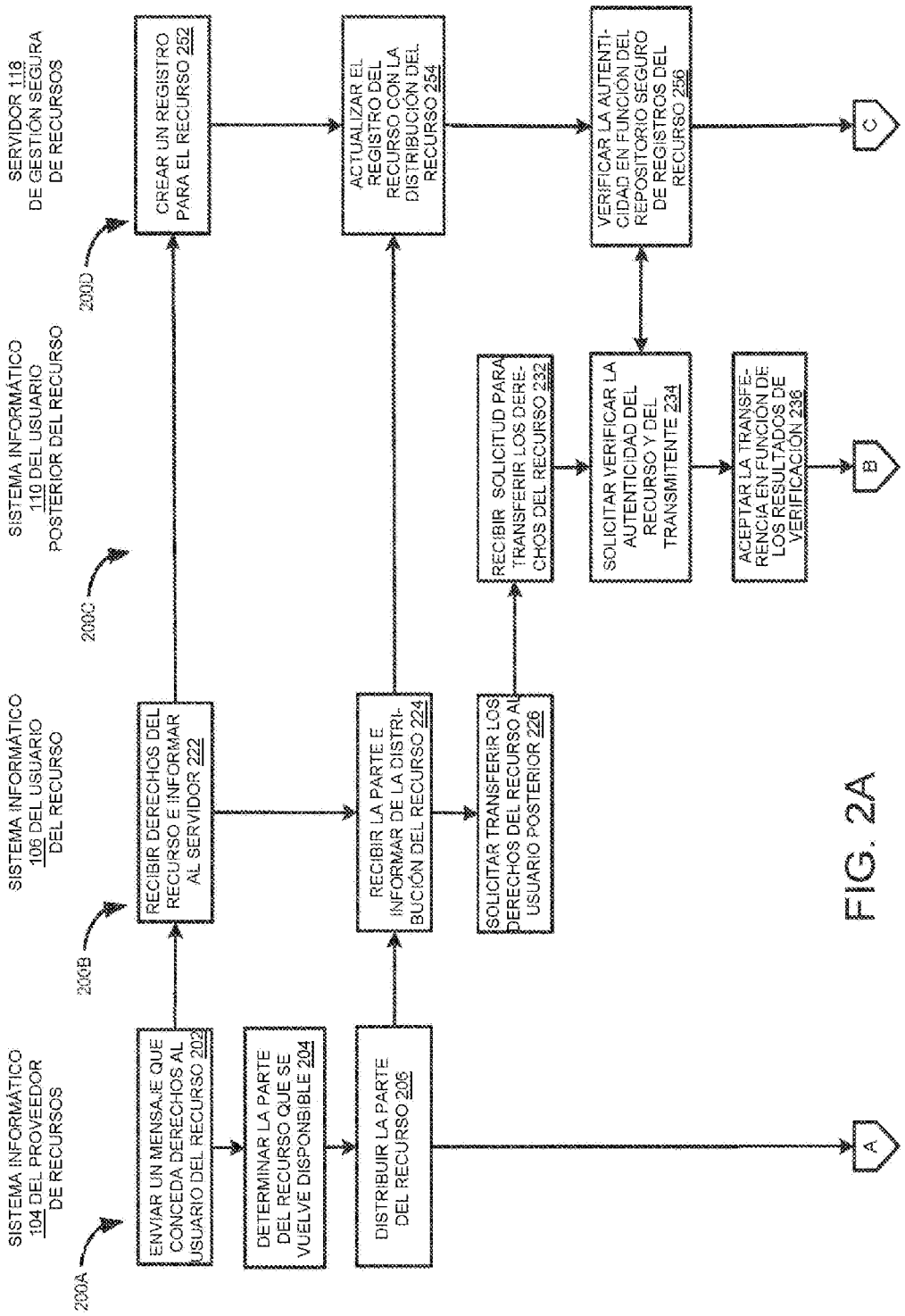
SISTEMA INFORMÁTICO 104 DEL PROVEEDOR DE RECURSOS
SISTEMA INFORMÁTICO 106 DEL USUARIO DEL RECURSO
SISTEMA INFORMÁTICO 110 DEL USUARIO POSTERIOR DEL RECURSO
SERVIDOR 118 DE GESTIÓN SEGURA DE RECURSOS
200A
200B
200C
200D
ENVIAR UN MENSAJE QUE CONCEDA DERECHOS AL USUARIO DEL RECURSO 202
DETERMINAR LA PARTE DEL RECURSO QUE SE VUELVE DISPONIBLE 204
DISTRIBUIR LA PARTE DEL RECURSO 206
RECIBIR DERECHOS DEL RECURSO E INFORMAR AL SERVIDOR 222
RECIBIR LA PARTE E INFORMAR DE LA DISTRIBUCIÓN DEL RECURSO 224
SOLICITAR TRANSFERIR LOS DERECHOS DEL RECURSO AL USUARIO POSTERIOR 226
CREAR UN REGISTRO PARA EL RECURSO 252
ACTUALIZAR EL REGISTRO DEL RECURSO CON LA DISTRIBUCIÓN DEL RECURSO 254
RECIBIR SOLICITUD PARA TRANSFERIR LOS DERECHOS DEL RECURSO 232
SOLICITAR VERIFICAR LA AUTENTICIDAD DEL RECURSO Y DEL TRANSMITENTE 234
ACEPTAR LA TRANSFERENCIA EN FUNCIÓN DE LOS RESULTADOS DE VERIFICACIÓN 236
VERIFICAR LA AUTENTICIDAD EN FUNCIÓN DEL REPOSITORIO SEGURO DE REGISTROS DEL RECURSO 256
A
B
C

FIG. 2A

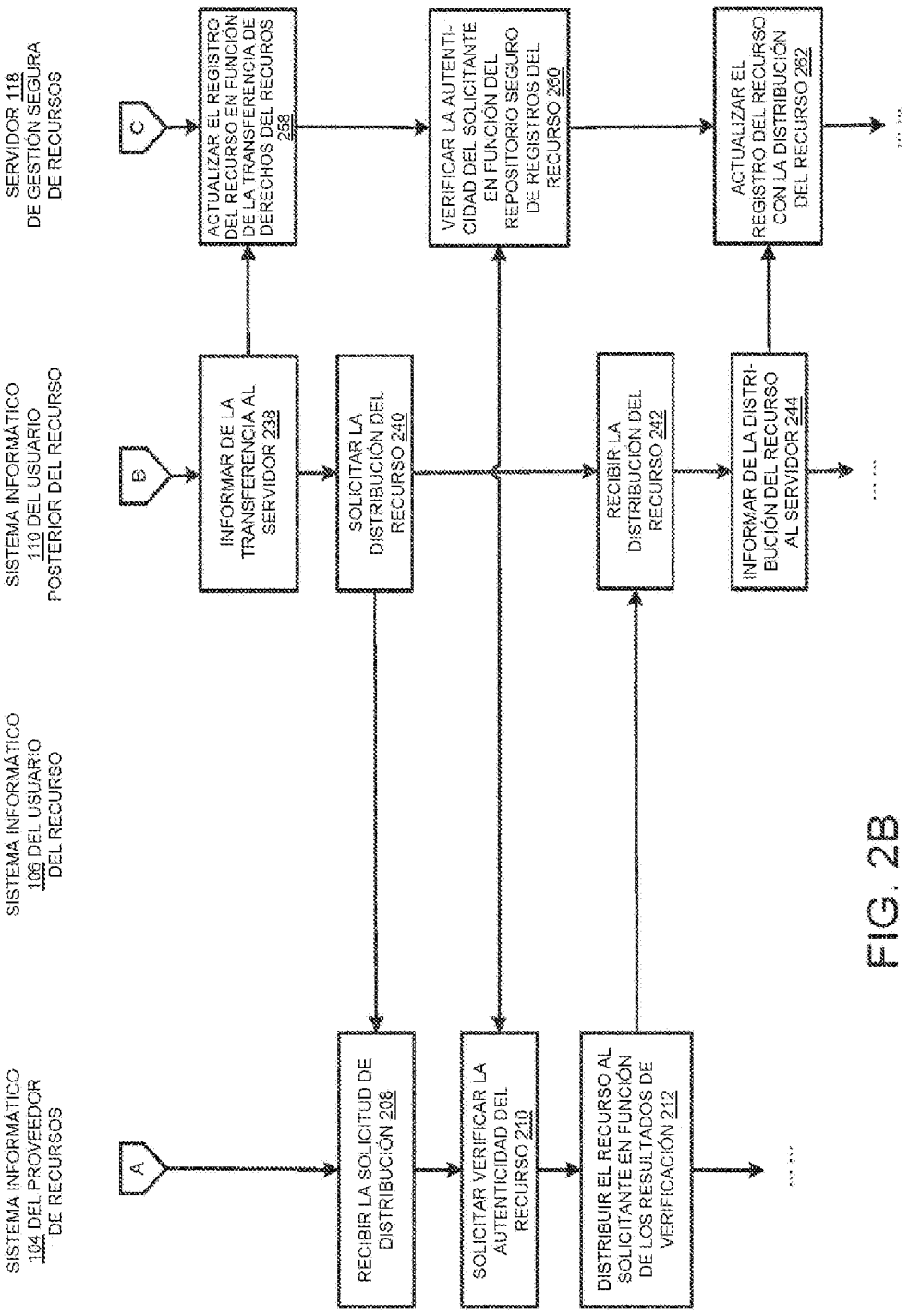
SISTEMA INFORMÁTICO 104 DEL PROVEEDOR DE RECURSOS
SISTEMA INFORMÁTICO 106 DEL USUARIO DEL RECURSO
SISTEMA INFORMÁTICO 110 DEL USUARIO POSTERIOR DEL RECURSO
SERVIDOR 118 DE GESTIÓN SEGURA DE RECURSOS
A
B
C
RECIBIR LA SOLICITUD DE DISTRIBUCIÓN 208
SOLICITAR VERIFICAR LA AUTENTICIDAD DEL RECURSO 210
DISTRIBUIR EL RECURSO AL SOLICITANTE EN FUNCIÓN DE LOS RESULTADOS DE VERIFICACIÓN 212
INFORMAR DE LA TRANSFERENCIA AL SERVIDOR 238
SOLICITAR LA DISTRIBUCIÓN DEL RECURSO 240
RECIBIR LA DISTRIBUCIÓN DEL RECURSO 242
INFORMAR DE LA DISTRIBUCIÓN DEL RECURSO AL SERVIDOR 244
ACTUALIZAR EL REGISTRO DEL RECURSO EN FUNCIÓN DE LA TRANSFERENCIA DE DERECHOS DEL RECUROS 258
VERIFICAR LA AUTENTICIDAD DEL SOLICITANTE EN FUNCIÓN DEL REPOSITORIO SEGURO DE REGISTROS DEL RECURSO 260
ACTUALIZAR EL REGISTRO DEL RECURSO CON LA DISTRIBUCIÓN DEL RECURSO 262

FIG. 2B

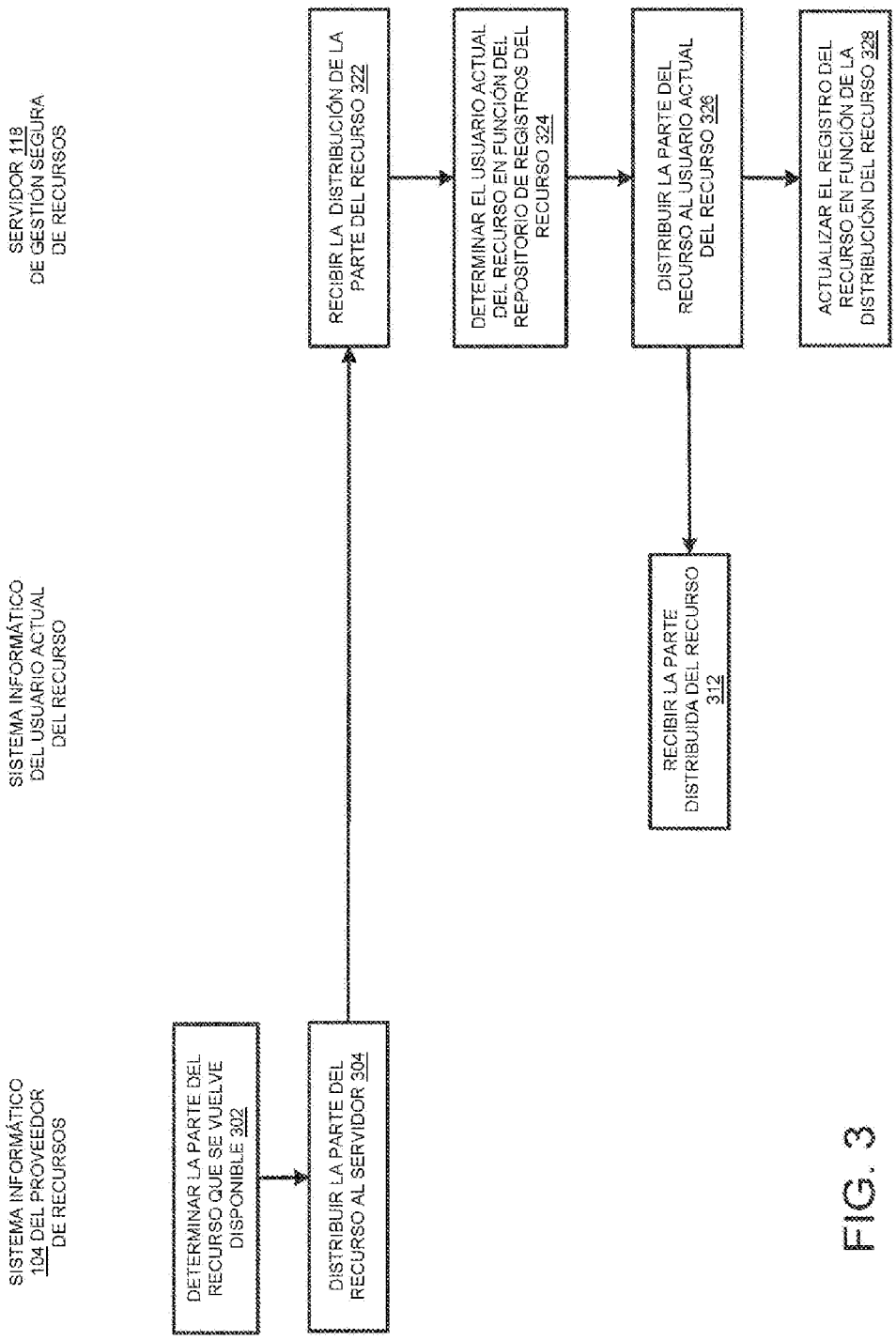
SISTEMA INFORMÁTICO 104 DEL PROVEEDOR DE RECURSOS
SISTEMA INFORMÁTICO DEL USUARIO ACTUAL DEL RECURSO
SERVIDOR 118 DE GESTIÓN SEGURA DE RECURSOS
DETERMINAR LA PARTE DEL RECURSO QUE SE VUELVE DISPONIBLE 302
DISTRIBUIR LA PARTE DEL RECURSO AL SERVIDOR 304
RECIBIR LA DISTRIBUCIÓN DE LA PARTE DEL RECURSO 322
DETERMINAR EL USUARIO ACTUAL DEL RECURSO EN FUNCIÓN DEL REPOSITORIO DE REGISTROS DEL RECURSO 324
DISTRIBUIR LA PARTE DEL RECURSO AL USUARIO ACTUAL DEL RECURSO 326
ACTUALIZAR EL REGISTRO DEL RECURSO EN FUNCIÓN DE LA DISTRIBUCIÓN DEL RECURSO 328
RECIBIR LA PARTE DISTRIBUIDA DEL RECURSO 312

FIG. 3

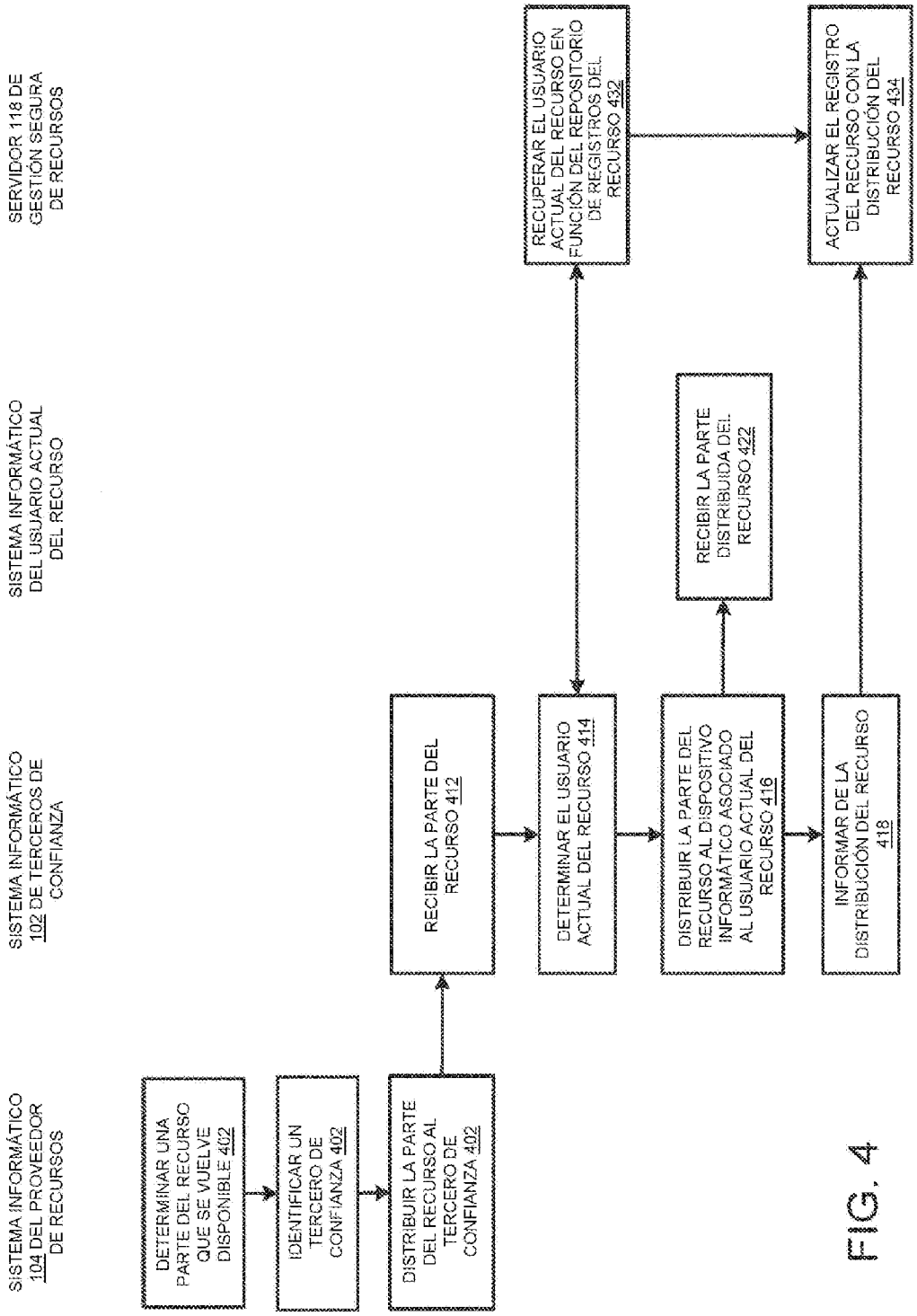
SISTEMA INFORMÁTICO 104 DEL PROVEEDOR DE RECURSOS
SISTEMA INFORMÁTICO 102 DE TERCEROS DE CONFIANZA
SISTEMA INFORMÁTICO DEL USUARIO ACTUAL DEL RECURSO
SERVIDOR 118 DE GESTIÓN SEGURA DE RECURSOS
DETERMINAR UNA PARTE DEL RECURSO QUE SE VUELVE DISPONIBLE 402
IDENTIFICAR UN TERCERO DE CONFIANZA 402
DISTRIBUIR LA PARTE DEL RECURSO AL TERCERO DE CONFIANZA 402
RECIBIR LA PARTE DEL RECURSO 412
DETERMINAR EL USUARIO ACTUAL DEL RECURSO 414
DISTRIBUIR LA PARTE DEL RECURSO AL DISPOSITIVO INFORMÁTICO ASOCIADO AL USUARIO ACTUAL DEL RECURSO 416
INFORMAR DE LA DISTRIBUCIÓN DEL RECURSO 418
RECUPERAR EL USUARIO ACTUAL DEL RECURSO EN FUNCIÓN DEL REPOSITORIO DE REGISTROS DEL RECURSO 432
RECIBIR LA PARTE DISTRIBUIDA DEL RECURSO 422
ACTUALIZAR EL REGISTRO DEL RECURSO CON LA DISTRIBUCIÓN DEL RECURSO 434

FIG. 4

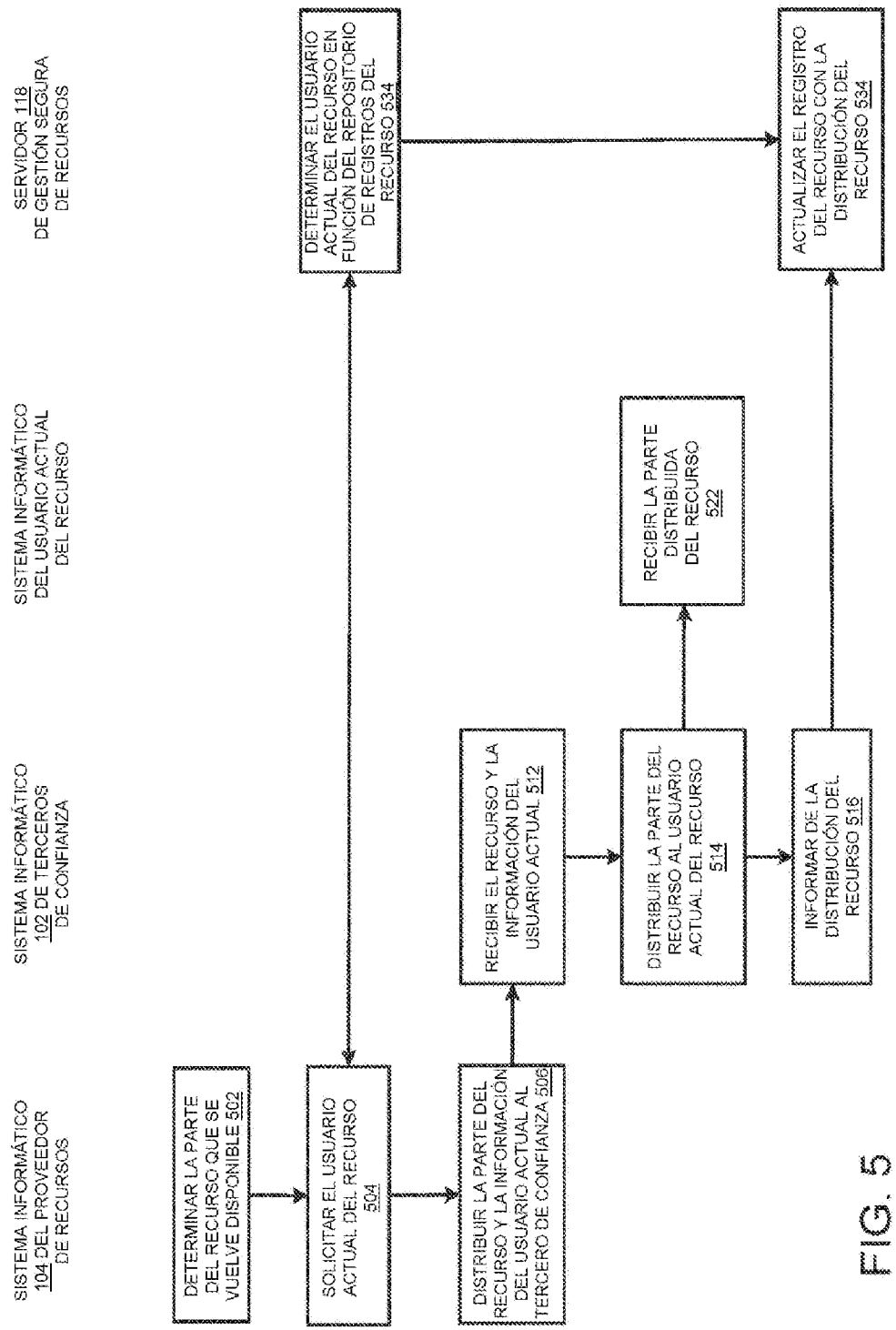
SISTEMA INFORMÁTICO 104 DEL PROVEEDOR DE RECURSOS
SISTEMA INFORMÁTICO 102 DE TERCEROS DE CONFIANZA
SISTEMA INFORMÁTICO DEL USUARIO ACTUAL DEL RECURSO
SERVIDOR 118 DE GESTIÓN SEGURA DE RECURSOS
DETERMINAR LA PARTE DEL RECURSO QUE SE VUELVE DISPONIBLE 502
SOLICITAR EL USUARIO ACTUAL DEL RECURSO 504
DISTRIBUIR LA PARTE DEL RECURSO Y LA INFORMACIÓN DEL USUARIO ACTUAL AL TERCERO DE CONFIANZA 506
RECIBIR EL RECURSO Y LA INFORMACIÓN DEL USUARIO ACTUAL 512
DISTRIBUIR LA PARTE DEL RECURSO AL USUARIO ACTUAL DEL RECURSO 514
INFORMAR DE LA DISTRIBUCIÓN DEL RECURSO 516
RECIBIR LA PARTE DISTRIBUIDA DEL RECURSO 522
DETERMINAR EL USUARIO ACTUAL DEL RECURSO EN FUNCIÓN DEL REPOSITORIO DE REGISTROS DEL RECURSO 534
ACTUALIZAR EL REGISTRO DEL RECURSO CON LA DISTRIBUCIÓN DEL RECURSO 534

FIG. 5

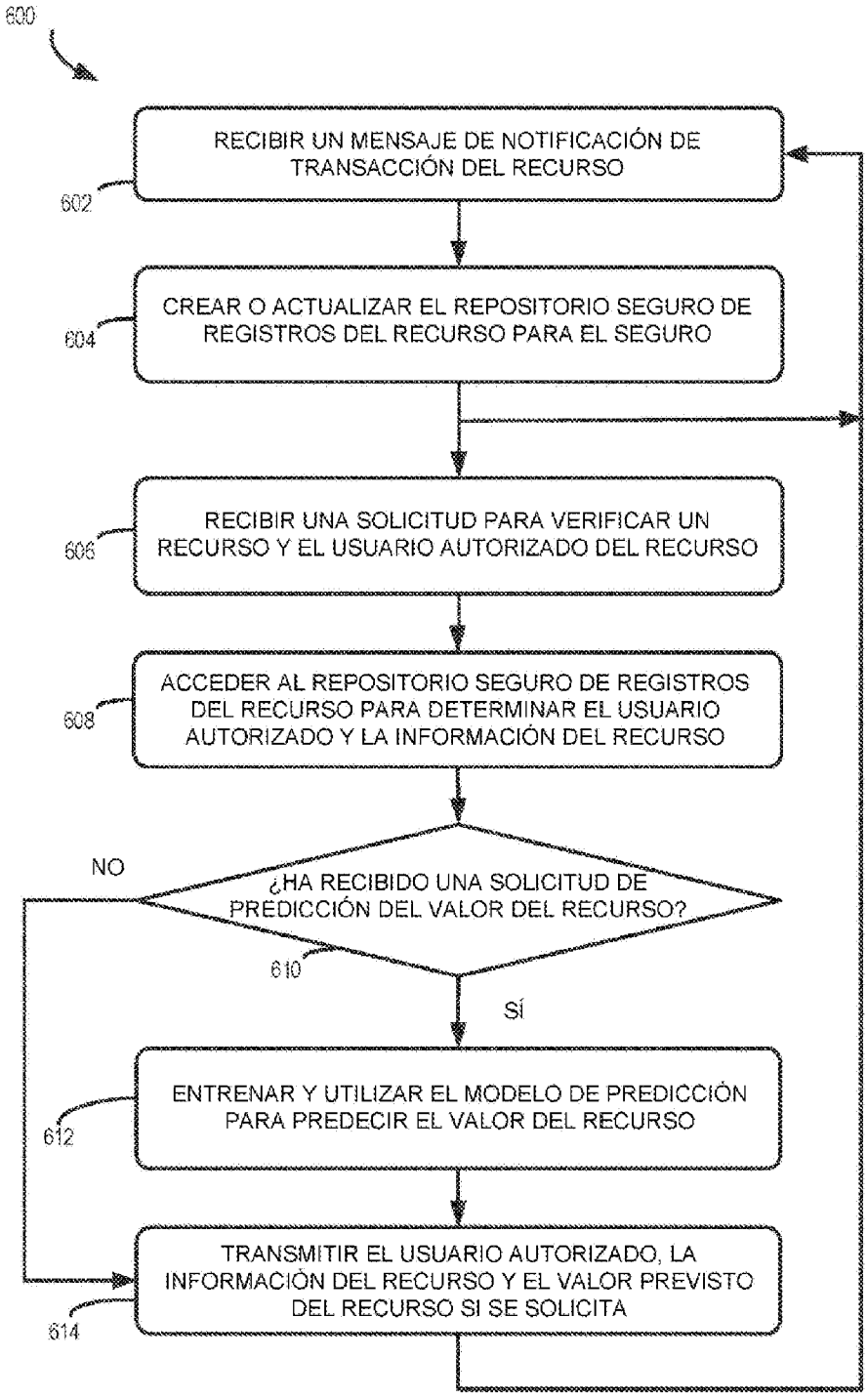
600
RECIBIR UN MENSAJE DE NOTIFICACIÓN DE TRANSACCIÓN DEL RECURSO
602
CREAR O ACTUALIZAR EL REPOSITORIO SEGURO DE REGISTROS DEL RECURSO PARA EL SEGURO
604
RECIBIR UNA SOLICITUD PARA VERIFICAR UN RECURSO Y EL USUARIO AUTORIZADO DEL RECURSO
606
ACCEDER AL REPOSITORIO SEGURO DE REGISTROS DEL RECURSO PARA DETERMINAR EL USUARIO AUTORIZADO Y LA INFORMACIÓN DEL RECURSO
608
¿HA RECIBIDO UNA SOLICITUD DE PREDICCIÓN DEL VALOR DEL RECURSO?
610
NO
SÍ
ENTRENAR Y UTILIZAR EL MODELO DE PREDICCIÓN PARA PREDECIR EL VALOR DEL RECURSO
612
TRANSMITIR EL USUARIO AUTORIZADO, LA INFORMACIÓN DEL RECURSO Y EL VALOR PREVISTO DEL RECURSO SI SE SOLICITA
614

FIG. 6

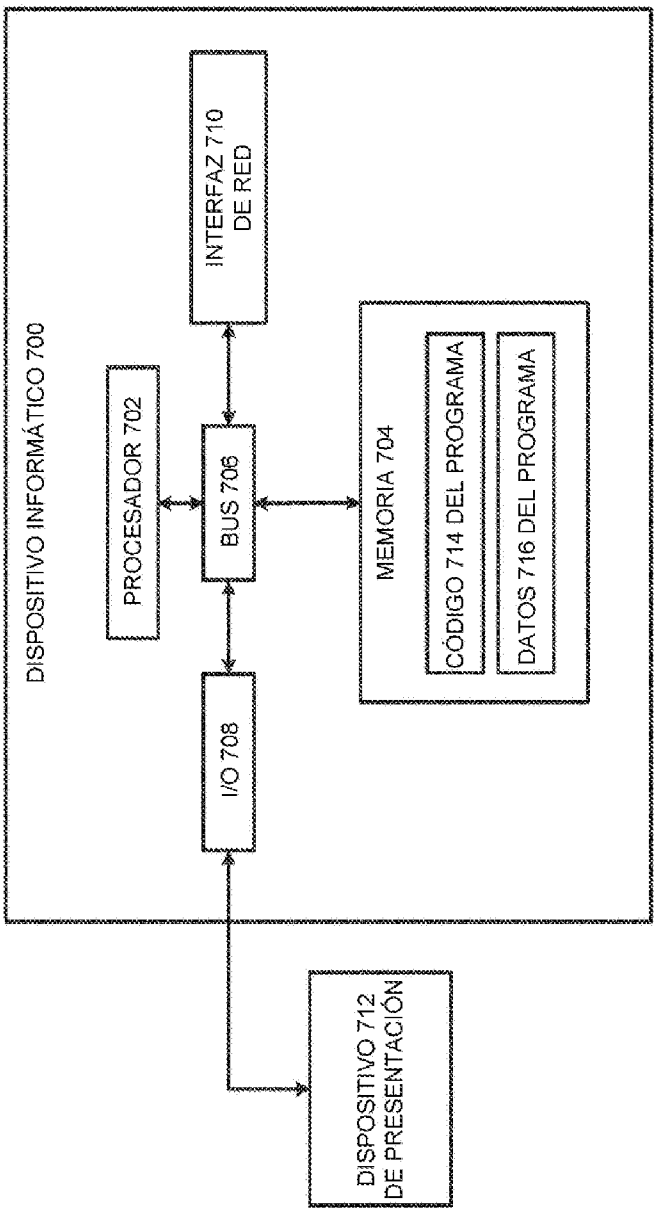
DISPOSITIVO INFORMÁTICO 700
PROCESADOR 702
BUS 706
INTERFAZ 710 DE RED
MEMORIA 704
CÓDIGO 714 DEL PROGRAMA
DATOS 716 DEL PROGRAMA
I/O 708
DISPOSITIVO 712 DE PRESENTACIÓN

FIG. 7