(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 809 161**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
G06Q 20/38 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.06.2017 PCT/US2017/036238**

(87) Fecha y número de publicación internacional: **11.01.2018 WO18009297**

(96) Fecha de presentación y número de la solicitud europea: **07.06.2017 E 17739731 (2)**

(97) Fecha y número de publicación de la concesión europea: **24.06.2020 EP 3482526**

(54) Título: **Método y sistema para la verificación de información de atributo de identidad**

(30) Prioridad:

08.07.2016 US 201615205410

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

(73) Titular/es:

MASTERCARD INTERNATIONAL INCORPORATED (100.0%)
2000 Purchase Street
Purchase, New York 10577, US

(72) Inventor/es:

DAVIS, STEVEN, CHARLES

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método y sistema para la verificación de información de atributo de identidad

Referencia cruzada a solicitud relacionada

Esta solicitud reivindica el beneficio y la prioridad de la solicitud de EE. UU. n° 15/205.410, presentada el 8 de julio de 2016. La divulgación completa de la solicitud anterior se incorpora en el presente documento como referencia.

Campo

La presente divulgación se refiere a la verificación de la información de atributo de identidad, específicamente el uso de técnicas de adición de sal y de cálculo de troceo específicamente configuradas para habilitar la verificación de la información de atributo de identidad al tiempo que se evita la capacidad de conjeturar la información de atributo de identidad.

Antecedentes

Con el fin de proteger información, datos confidenciales, tales como información de atributo de identificación relacionada con individuos, a menudo se almacenan de maneras que hacen difícil la recuperación o identificación de los datos. Por ejemplo, los datos pueden cifrarse de manera tal que solo entidades autorizadas que tienen acceso a la clave de cifrado apropiada puedan descifrar los datos. Sin embargo, el cifrado requiere generalmente que se comparta la clave de cifrado, lo que a veces puede ser difícil y proporciona la oportunidad de que la clave y, por extensión, los datos confidenciales, se vean comprometidos. Un método alternativo que se ha desarrollado para proteger los datos es el cálculo de troceo, donde se genera un valor de troceo a partir de datos que no pueden invertirse, de tal manera que ha de saberse que el valor de datos subyacente genera ese valor de troceo específico.

El cálculo de troceo puede ser muy efectivo para instancias donde los valores de datos subyacentes pueden tener una varianza grande en sus datos, tales como documentos donde cada carácter y espacio cambia el valor de troceo resultante. Si se usa un árbol de Merkle, el efecto se agrava debido a que no solo se han de conocer los valores de datos subyacentes, sino que también se ha de conocer la ordenación de los datos para la generación del árbol de Merkle. Sin embargo, si los valores de datos subyacentes son de un conjunto limitado, una entidad maliciosa puede, con acceso a un sistema informático suficiente, ser capaz de trocear cada valor de datos posible, así como las ordenaciones potenciales de un árbol de Merkle. Por ejemplo, si los valores de datos subyacentes son fechas de nacimiento de individuos, las posibilidades son muy limitadas, de tal manera que un sistema informático potente puede ser capaz de identificar cada valor de troceo y árbol de Merkle posible.

Por lo tanto, existe la necesidad de una solución técnica que habilite el cálculo de troceo y el almacenamiento de la información de atributo de identificación y otros valores de datos para la verificación que evite la capacidad de conjeturar los valores de datos subyacentes.

Sumario

La presente divulgación proporciona una descripción de sistemas y métodos para la verificación de valores de datos a través de una raíz de Merkle. Un número de ocasión se combina con el valor de datos para proteger la identificación del valor de datos a través de conjeturas del valor de datos y los valores posteriores en un árbol de Merkle. Por lo tanto, el valor de datos subyacente puede probarse a una entidad para la verificación de los mismos usando el valor de datos y el número de ocasión que se combinó antes del cálculo de troceo y el procesamiento del árbol de Merkle, habilitando una verificación y una prueba rápidas de los datos subyacentes, al tiempo que se protegen los datos frente a verse comprometidos incluso si los valores de datos subyacentes son de un conjunto limitado.

Un método para la verificación de un valor de datos a través de una raíz de Merkle incluye: almacenar, en una memoria de un servidor de procesamiento, una raíz de Merkle; recibir, por un dispositivo de recepción del servidor de procesamiento, al menos un valor de datos, un número de ocasión y una pluralidad de valores de ruta de troceo; generar, por un módulo de generación del servidor de procesamiento, un valor combinado al combinar el valor de datos y el número de ocasión; generar, por un módulo de cálculo de troceo del servidor de procesamiento, un primer valor de troceo a través de la aplicación de un algoritmo de cálculo de troceo al valor combinado; generar, por el módulo de cálculo de troceo del servidor de procesamiento, un valor de troceo posterior a través de la aplicación del algoritmo de cálculo de troceo a una combinación del primer valor de troceo y un primero de la pluralidad de valores de ruta de troceo; repetir, por el módulo de cálculo de troceo del servidor de procesamiento, la generación del valor de troceo posterior usando una combinación del siguiente valor de ruta de troceo de la pluralidad de valores de ruta de troceo y el valor de troceo posterior más reciente; y verificar, por un módulo de verificación del servidor de procesamiento, el valor de datos basándose en una comparación de la raíz de Merkle y el último valor de troceo posterior generado.

Un sistema para la verificación de un valor de datos a través de una raíz de Merkle incluye: una memoria de un servidor de procesamiento configurada para almacenar una raíz de Merkle; un dispositivo de recepción del servidor de procesamiento configurado para recibir al menos un valor de datos, un número de ocasión y una pluralidad de valores de ruta de troceo; un módulo de generación del servidor de procesamiento configurado para generar un valor combinado al combinar el valor de datos y el número de ocasión; un módulo de cálculo de troceo del servidor de procesamiento configurado para generar un primer valor de troceo a través de la aplicación de un algoritmo de cálculo de troceo al valor combinado, generar un valor de troceo posterior a través de la aplicación del algoritmo de cálculo de troceo a una combinación del primer valor de troceo y un primero de la pluralidad de valores de ruta de troceo y repetir la generación del valor de troceo posterior usando una combinación del siguiente valor de ruta de troceo de la pluralidad de valores de ruta de troceo y el valor de troceo posterior más reciente; y un módulo de verificación del servidor de procesamiento configurado para verificar el valor de datos basándose en una comparación de la raíz de Merkle y el último valor de troceo posterior generado.

Breve descripción de las figuras de los dibujos

El alcance de la presente divulgación se entiende mejor a partir de la siguiente descripción detallada de realizaciones ilustrativas cuando se leen en conjunción con los dibujos adjuntos. En los dibujos se incluyen las siguientes figuras:

La Figura 1 es un diagrama de bloques que ilustra una arquitectura de sistema de alto nivel para la verificación de valores de datos usando una raíz de Merkle de acuerdo con realizaciones ilustrativas.
La Figura 2 es un diagrama de bloques que ilustra el servidor de procesamiento de la Figura 1 para la verificación de valores de datos usando raíces de Merkle de acuerdo con realizaciones ilustrativas.
La Figura 3 es un diagrama de flujo que ilustra un proceso para la verificación de un valor de datos basándose en nodos en un árbol de Merkle usando el servidor de procesamiento de la Figura 2 de acuerdo con realizaciones ilustrativas.
La Figura 4 es un diagrama que ilustra un árbol de Merkle para su uso en la verificación de valores de datos usando el servidor de procesamiento de la Figura 2 de acuerdo con realizaciones ilustrativas.
La Figura 5 es un diagrama de flujo que ilustra un método ilustrativo para verificar un valor de datos a través de una raíz de Merkle de acuerdo con realizaciones ilustrativas.
La Figura 6 es un diagrama de bloques que ilustra una arquitectura de sistema informático de acuerdo con realizaciones ilustrativas.

Áreas de aplicabilidad adicionales de la presente divulgación serán evidentes a partir de la descripción detallada proporcionada en lo sucesivo. Debería entenderse que la descripción detallada de realizaciones ilustrativas se concibe para propósitos de ilustración únicamente y no se concibe, por lo tanto, para limitar necesariamente el alcance de la divulgación.

Descripción detallada

Glosario de términos

Cadena de bloques - un libro mayor público de todas las transacciones de una moneda basada en cadena de bloques. Uno o más dispositivos informáticos pueden comprender una red de cadena de bloques, que puede configurarse para procesar y registrar transacciones como parte de un bloque en la cadena de bloques. Una vez que se ha completado un bloque, el bloque se añade a la cadena de bloques y el registro de transacción se actualiza de ese modo. En muchos casos, la cadena de bloques puede ser un libro mayor de transacciones en orden cronológico, o puede presentarse en cualquier otro orden que pueda ser adecuado para su uso por la red de cadena de bloques. En algunas configuraciones, las transacciones registradas en la cadena de bloques pueden incluir una dirección de destino y una cantidad de moneda, de tal manera que la cadena de bloques registra qué cantidad de moneda es atribuible a una dirección específica. En algunos casos, las transacciones son financieras y otras no financieras, o podrían incluir información adicional o diferente, tal como una dirección de origen, una marca de tiempo, etc. En algunas realizaciones, una cadena de bloques puede incluir, también o como alternativa, casi cualquier tipo de datos como una forma de transacción que se coloca o es necesario colocar en una base de datos distribuida y sin permisos que mantiene una lista de registros de datos continuamente creciente, reforzada contra manipulaciones indebidas y revisiones, incluso por sus operadores, y puede ser confirmada y validada por la red de cadena de bloques a través de prueba de trabajo y/o cualquier otra técnica de verificación adecuada asociada a la misma. En algunos casos, los datos con respecto a una transacción dada pueden incluir adicionalmente datos adicionales que no son directamente parte de la transacción adjunta a los datos de transacción. En algunos casos, la inclusión de dichos datos en una cadena de bloques puede constituir una transacción. En tales casos, una cadena de bloques puede no estar directamente asociada con una moneda de tipo específico digital, virtual, fiduciario o de otro tipo. En algunos casos, la participación en una cadena de bloques (por ejemplo, como un nodo que envía y/o que confirma transacciones) puede ser sin permisos (por ejemplo, no moderada o restringida). En otros casos, una cadena de bloques puede ser una cadena de bloques con permiso donde solo dispositivos informáticos autorizados pueden operar como nodos, donde un nivel de participación puede basarse en sus permisos asociados.

Sistema para la verificación de valores de datos a través de una raíz de Merkle

La Figura 1 ilustra un sistema 100 para la verificación de un valor de datos a través del uso de una raíz de Merkle, donde el valor de datos se combina con un número de ocasión antes de su inclusión en el árbol de Merkle para la protección del mismo.

El sistema 100 puede incluir un servidor de procesamiento 102. El servidor de procesamiento 102, analizado con más detalle a continuación, puede configurarse para verificar valores de datos a través del uso de un árbol de Merkle. El sistema 100 también puede incluir un proveedor de datos 104. El proveedor de datos 104 puede configurarse para proporcionar un valor de datos al servidor de procesamiento 102 para la verificación del mismo. En algunos casos, el valor de datos puede comprender información de atributo de identidad, tal como una fecha de nacimiento, nombre, dirección, número de teléfono, número de seguridad social, número de identificación fiscal, etc. En algunos casos, el valor de datos puede ser de un conjunto limitado de valores de datos, tales como los incluidos en un conjunto acotado de números enteros u otros valores similares.

El valor de datos a verificar por el servidor de procesamiento 102 puede haberse usado en la generación de un árbol de Merkle que incluye el valor de datos como uno de una pluralidad de valores de datos usados en la generación del árbol de Merkle. Métodos para generar un árbol de Merkle serán evidentes para los expertos en la materia relevante. Puede generarse un árbol de Merkle al ordenar cada uno de los valores de datos, trocear cada uno de los valores de datos usando uno o más algoritmos de cálculo de troceo predeterminados, trocear pares de los valores resultantes y continuar troceando los pares resultantes hasta que se obtiene un único valor de troceo, denominado raíz del árbol de Merkle o "raíz de Merkle". El uso de algoritmos de cálculo de troceo puede garantizar que la raíz de Merkle para la pluralidad de valores de datos sea diferente si se cambia un único valor de datos. Como resultado, la verificación de un valor de datos puede realizarse al asegurar que una raíz de Merkle generada usando el valor de datos coincida con una raíz de Merkle previamente identificada que se hubiera generado usando el valor.

En el sistema 100, antes de la generación del árbol de Merkle, cada uno de los valores de datos puede combinarse con un número de ocasión. El número de ocasión puede ser un número aleatorio o pseudoaleatorio u otro valor, tal como una cadena de caracteres alfanuméricos, que puede combinarse con el valor de datos antes de la generación del árbol de Merkle. Por ejemplo, en una realización, el número de ocasión puede ser un número entero aleatorio de 256 bits. El número de ocasión puede añadirse a (por ejemplo, a través de adición aritmética) o combinarse de otro modo con (por ejemplo, adjuntado al final del valor de datos) el valor de datos. El valor combinado puede trocearse entonces como parte de la generación del árbol de Merkle. El uso del número de ocasión puede garantizar que cualquier entidad maliciosa que intente conjeturar cada uno de los valores de datos y nodos posteriores en el árbol de Merkle sea incapaz de identificar los valores de datos, debido a que los valores de troceo serían incorrectos a menos que el valor de datos se combinase con el mismo número de ocasión usado en la generación del árbol de Merkle. Como resultado, los valores de los datos solo pueden identificarse a través de conjeturas si tiene éxito la conjetura del número de ocasión para cada valor de datos. En tales casos, el uso de números aleatorios para los números de ocasión, así como el uso de un número de ocasión más largo (por ejemplo, 256 bits) puede hacer que el número de combinaciones potenciales sea demasiado grande para ser resuelto por cualquier sistema o sistemas informáticos existentes. Como resultado, los números de ocasión pueden proteger los valores de datos frente a ser identificados a través de conjeturas.

Para verificar un valor de datos, el servidor de procesamiento 102 puede recibir el valor de datos y su número de ocasión a partir del proveedor de datos 104. Por ejemplo, el valor de datos puede ser un contrato que el proveedor de datos 104 puede querer probar (por ejemplo, para la autenticación del lenguaje incluido en el mismo, firmas digitales, etc.), donde el proveedor de datos 104 puede dotar al servidor de procesamiento 102 del contrato y el número de ocasión añadido al mismo cuando se generó un árbol de Merkle que incluye el contrato. El servidor de procesamiento 102 puede añadir el número de ocasión al contrato y generar un árbol de Merkle. Si la raíz de Merkle resultante coincide con la raíz de Merkle para el árbol de Merkle original, entonces el contrato proporcionado por el proveedor de datos 104 puede verificarse como el mismo contrato usado cuando se generó el árbol de Merkle.

Tales procesos de verificación pueden ser beneficiosos en casos en los que el servidor de procesamiento 102 y otras entidades y sistemas informáticos pueden acceder públicamente al árbol de Merkle, o al menos la raíz de Merkle de un árbol de Merkle, para una pluralidad de valores de datos. En una realización de este tipo, la raíz de Merkle puede ser parte de una red de cadena de bloques 106. La red de cadena de bloques 106 puede incluir una pluralidad de nodos informáticos que pueden configurarse para generar y verificar bloques que se añaden a una cadena de bloques, donde cada bloque está compuesto por al menos un encabezamiento de bloque. El encabezamiento para un bloque puede incluir una raíz de Merkle que se genera usando todos los valores de transacción representados por ese bloque. En algunos casos, el bloque puede incluir los valores de transacción, o puede incluir versiones cifradas, troceadas o, por lo demás, ocultas o modificadas de los valores de transacción. El servidor de procesamiento 102 puede usar los métodos analizados en el presente documento para verificar un valor de transacción al hacer coincidir una raíz de Merkle posteriormente generada con la raíz de Merkle incluida en el encabezamiento de bloque. En tales casos, el valor de transacción puede, por lo tanto, autenticar un documento, verificar un saldo de cuenta, probar que tuvo lugar una transacción, etc.

En algunas realizaciones, el servidor de procesamiento 102 puede tener acceso a un árbol de Merkle completo. En tales realizaciones, el proveedor de datos 104 puede dotar al servidor de procesamiento 102 de solo el valor de datos y el número de ocasión correspondiente. El servidor de procesamiento 102 puede combinar el valor de datos y el número de ocasión y trocear el resultado, y comparar entonces el resultado con el nodo correspondiente en el árbol de Merkle. En algunos casos, el servidor de procesamiento 102 también puede generar la raíz de Merkle y comparar la raíz de Merkle con la raíz del árbol de Merkle al que se ha accedido.

En otras realizaciones, el servidor de procesamiento 102 solo puede tener acceso a la raíz de Merkle, tal como en casos en los que el servidor de procesamiento 102 obtiene la raíz de Merkle a partir de una red de cadena de bloques 106. En tales realizaciones, el proveedor de datos 104 puede dotar al servidor de procesamiento 102 de cada uno de los valores en la ruta de troceo del árbol de Merkle. La ruta de troceo puede referirse a cada uno de los valores de troceo que comprenden nodos en el árbol de Merkle que, cuando se dotan del valor de datos y su número de ocasión, habilitan la generación de la raíz de Merkle sin acceso a los otros valores de datos. En algunos casos, la ruta de troceo puede incluir la cantidad mínima de valores de troceo requeridos, que puede ser la n-ésima raíz del número de valores de datos usados en la generación de la raíz de Merkle. A continuación se proporciona información adicional con respecto a una ruta de troceo con respecto al árbol de Merkle ilustrado en la Figura 4.

El servidor de procesamiento 102 puede combinar el valor de datos y el número de ocasión y trocear el valor combinado para obtener un primer valor de troceo. El servidor de procesamiento 102 puede combinar entonces ese primer valor de troceo con el primer valor de ruta de troceo proporcionado por el proveedor de datos 104, y trocear entonces el valor combinado. El servidor de procesamiento 102 puede combinar entonces ese valor posterior con el siguiente valor de ruta de troceo y trocear el resultado, y puede continuar haciendo esto hasta que se obtiene un único valor. Este único valor corresponde a la raíz de Merkle del árbol de Merkle que incluye el valor de datos proporcionado. El servidor de procesamiento 102 puede determinar entonces si esa raíz de Merkle coincide con la raíz de Merkle identificada (por ejemplo, a partir de la cadena de bloques) para verificar si el valor de datos proporcionado es el mismo valor de datos usado en la generación de la raíz de Merkle original.

Los métodos y sistemas analizados en el presente documento habilitan que el servidor de procesamiento 102 verifique un valor de datos dado el valor de datos, su número de ocasión correspondiente y la ruta de troceo usada para generar una raíz de Merkle. El uso del número de ocasión puede garantizar que los valores de datos usados en la generación de la raíz de Merkle no sean aptos para conjeturarse incluso con una gran cantidad de potencia informática, al tiempo que se sigue habilitando una verificación rápida y conveniente de los datos. El uso de una ruta de troceo también puede garantizar que los datos pueden verificarse dado acceso solo a la raíz de Merkle, sin que el servidor de procesamiento 102 tenga que obtener ningún otro valor de datos o troceo asociado con el mismo, lo que puede prever verificaciones que mantengan un nivel más alto de seguridad de datos. Como resultado, la seguridad de datos puede aumentar en gran medida sin sacrificar la velocidad o la eficiencia en la verificación de datos.

Servidor de procesamiento

La Figura 2 ilustra una realización de un servidor de procesamiento 102 en el sistema 100. Será evidente para los expertos en la materia relevante que la realización del servidor de procesamiento 102 ilustrada en la Figura 2 se proporciona solo como ilustración y puede no ser exhaustiva para todas las configuraciones posibles del sistema de procesamiento 102 adecuadas para realizar las funciones como se analiza en el presente documento. Por ejemplo, el sistema informático 600 ilustrado en la Figura 6 y analizado con más detalle a continuación puede ser una configuración adecuada del servidor de procesamiento 102.

El servidor de procesamiento 102 puede incluir un dispositivo de recepción 202. El dispositivo de recepción 202 puede configurarse para recibir datos a través de una o más redes a través de uno o más protocolos de red. El dispositivo de recepción 202 puede configurarse para recibir datos desde dispositivos informáticos 104 y otros dispositivos y sistemas a través de redes de comunicación adecuadas y protocolos de red correspondientes. En algunas realizaciones, el dispositivo de recepción 202 puede estar compuesto por múltiples dispositivos, tales como diferentes dispositivos de recepción para recibir datos a través de diferentes redes, tales como un primer dispositivo de recepción para recibir datos a través de una red de área local y un segundo dispositivo de recepción para recibir datos a través de una red de cadena de bloques. El dispositivo de recepción 202 puede recibir señales de datos transmitidas electrónicamente, donde los datos pueden superponerse o codificarse de otro modo en la señal de datos y descodificarse, analizarse, leerse u obtenerse de otro modo a través de la recepción de la señal de datos por el dispositivo de recepción 202. En algunos casos, el dispositivo de recepción 202 puede incluir un módulo de análisis para analizar la señal de datos recibida para obtener los datos superpuestos sobre la misma. Por ejemplo, el dispositivo de recepción 202 puede incluir un programa de análisis configurado para recibir y transformar la señal de datos recibida en una entrada utilizable para las funciones realizadas por el dispositivo de procesamiento para realizar los métodos y sistemas descritos en el presente documento.

El dispositivo de recepción 202 puede configurarse para recibir señales de datos transmitidas electrónicamente por los proveedores de datos 104, que pueden superponerse o codificarse de otro modo con al menos un valor de datos y un número de ocasión correspondiente. En algunos casos, las señales de datos también pueden superponerse o codificarse con una pluralidad de valores de ruta de troceo. El dispositivo de recepción 202 también puede

configurarse para recibir señales de datos transmitidas electrónicamente por las redes de cadena de bloques 106 o nodos asociados con las mismas, que pueden superponerse o codificarse de otro modo con una cadena de bloques o datos incluidos en la misma, que pueden incluir raíces de Merkle y, en algunos casos, pueden incluir valores de datos adicionales incluidos en un árbol de Merkle.

El servidor de procesamiento 102 también puede incluir un módulo de comunicación 204. El módulo de comunicación 204 puede configurarse para transmitir datos entre módulos, motores, bases de datos, memorias y otros componentes del servidor de procesamiento 102 para su uso en la realización de las funciones analizadas en el presente documento. El módulo de comunicación 204 puede estar compuesto por uno o más tipos de comunicación y utilizar diversos métodos de comunicación para las comunicaciones dentro de un dispositivo informático. Por ejemplo, el módulo de comunicación 204 puede estar compuesto por un bus, conectores de patilla de contacto, hilos, etc. En algunas realizaciones, el módulo de comunicación 204 también puede configurarse para comunicarse entre componentes internos del servidor de procesamiento 102 y componentes externos del servidor de procesamiento 102, tales como bases de datos conectadas externamente, dispositivos de visualización, dispositivos de entrada, etc. El servidor de procesamiento 102 también puede incluir un dispositivo de procesamiento. El dispositivo de procesamiento puede configurarse para realizar las funciones del servidor de procesamiento 102 analizado en el presente documento, como será evidente para los expertos en la materia relevante. En algunas realizaciones, el dispositivo de procesamiento puede incluir y/o estar compuesto por una pluralidad de motores y/o módulos especialmente configurados para realizar una o más funciones del dispositivo de procesamiento, tales como un módulo de consulta 210, un módulo de generación 212, un módulo de cálculo de troceo 214, un módulo de verificación 218, etc. Como se usa en el presente documento, el término "módulo" puede ser software o hardware particularmente programado para recibir una entrada, realizar uno o más procesos usando la entrada y proporcionar una salida. La entrada, la salida y los procesos realizados por diversos módulos serán evidentes para un experto en la materia basándose en la presente divulgación.

El servidor de procesamiento 102 puede incluir un módulo de consulta 210. El módulo de consulta 210 puede configurarse para ejecutar consultas en bases de datos para identificar información. El módulo de consulta 210 puede recibir uno o más valores de datos o cadenas de consulta, y puede ejecutar una cadena de consulta basándose en los mismos en una base de datos indicada para identificar información almacenada en la misma. El módulo de consulta 210 puede emitir entonces la información identificada a un motor o módulo apropiado del servidor de procesamiento 102 según sea necesario. El módulo de consulta 210 puede, por ejemplo, ejecutar una consulta en una memoria 220 del servidor de procesamiento 102 para identificar una raíz de Merkle incluida en una cadena de bloques para su uso en la verificación de un valor de datos.

El servidor de procesamiento 102 también puede incluir un módulo de generación 212. El módulo de generación 212 puede configurarse para generar datos para su uso en la realización de las funciones del servidor de procesamiento 102 como se analiza en el presente documento. El módulo de generación 212 puede recibir una solicitud, puede generar datos basándose en esa solicitud y puede emitir los datos generados a otro módulo o motor del servidor de procesamiento 102. Por ejemplo, el módulo de generación 212 puede configurarse para combinar valores de datos y números de ocasión o para combinar valores de troceo con otros valores de troceo para su uso en la generación de árboles de Merkle para realizar las funciones del servidor de procesamiento 102 analizado en el presente documento.

El servidor de procesamiento 102 también puede incluir un módulo de cálculo de troceo 214. El módulo de cálculo de troceo 214 puede configurarse para generar valores de troceo a través de la aplicación de uno o más algoritmos de cálculo de troceo a datos suministrados al módulo de cálculo de troceo 214. El módulo de cálculo de troceo 214 puede recibir datos a trocear como entrada, puede aplicar uno o más algoritmos de cálculo de troceo a los datos y puede emitir el valor de troceo generado a otro módulo o motor del servidor de procesamiento 102. En algunos casos, el módulo de cálculo de troceo 214 puede ser dotado del algoritmo o algoritmos de cálculo de troceo a usar en la generación de un valor de troceo. En otros casos, el módulo de cálculo de troceo 214 puede identificar los algoritmos de cálculo de troceo a usar, tal como a través de la generación de consultas para su ejecución por el módulo de consulta 210 en la memoria 220. El módulo de cálculo de troceo 214 puede configurarse, por ejemplo, para generar valores de troceo para su uso en la generación de árboles de Merkle, tal como al trocear valores de datos y números de ocasión combinados o valores de troceo combinados, tales como una combinación de dos valores de troceo previamente generados por el módulo de cálculo de troceo 214 como parte de la generación de un árbol de Merkle.

El servidor de procesamiento 102 también puede incluir un módulo de verificación 218. El módulo de verificación 218 puede configurarse para verificar datos como parte de las funciones del servidor de procesamiento 102. El módulo de verificación 218 puede recibir datos como entrada, puede intentar verificar los datos y puede emitir un resultado de la verificación a otro módulo o motor del servidor de procesamiento 102. Por ejemplo, el módulo de verificación 218 puede configurarse para verificar si una raíz de Merkle generada coincide con una raíz de Merkle identificada (por ejemplo, a partir de una cadena de bloques) como verificación de un valor de datos proporcionado. El módulo de verificación 218 puede emitir entonces el resultado de la verificación a otro módulo o motor del servidor de procesamiento 102, tal como a un dispositivo de transmisión 216 para la notificación al proveedor de datos 104.

El servidor de procesamiento 102 también puede incluir el dispositivo de transmisión 216. El dispositivo de transmisión 216 puede configurarse para transmitir datos a través de una o más redes a través de uno o más protocolos de red. El dispositivo de transmisión 216 puede configurarse para transmitir datos a los dispositivos informáticos 106 y otras entidades a través de redes de comunicación adecuadas y protocolos de red correspondientes. En algunas realizaciones, el dispositivo de transmisión 216 puede estar compuesto por múltiples dispositivos, tales como diferentes dispositivos de transmisión para transmitir datos a través de diferentes redes, tales como un primer dispositivo de transmisión para transmitir datos a través de una red de área local y un segundo dispositivo de transmisión para transmitir datos a través de una red de cadena de bloques. El dispositivo de transmisión 216 puede transmitir electrónicamente señales de datos que tienen datos superpuestos que pueden ser analizados por un dispositivo informático de recepción. En algunos casos, el dispositivo de transmisión 216 puede incluir uno o más módulos para superponer, codificar o dar de otro modo formato a datos en/a/para dar señales de datos adecuadas para la transmisión.

El dispositivo de transmisión 216 puede configurarse para transmitir electrónicamente señales de datos a proveedores de datos 104, tal como puede superponerse o codificarse de otro modo con resultados de verificación, tal como pueden ser generados por el módulo de verificación 218 como resultado de procesos de verificación analizados en el presente documento. El dispositivo de transmisión 216 también puede configurarse para transmitir electrónicamente señales de datos a proveedores de datos 104 que pueden superponerse o codificarse de otro modo con solicitudes de datos, tal como para solicitar datos que verificar o solicitar valores de ruta de troceo para su uso en la generación de una raíz de Merkle. En algunos casos, el dispositivo de transmisión 216 también puede configurarse para transmitir electrónicamente señales de datos a entidades adicionales, tales como nodos en la red de cadena de bloques 106, que pueden superponerse o codificarse de otro modo con una solicitud de una raíz de Merkle, tal como puede usarse para verificar datos proporcionados por el proveedor de datos 104.

El servidor de procesamiento 102 también puede incluir una memoria 220. La memoria 220 puede configurarse para almacenar datos para su uso por el servidor de procesamiento 102 en la realización de las funciones analizadas en el presente documento, tales como una clave privada, par de claves, reglas de formato, una cadena de bloques, etc. La memoria 220 puede configurarse para almacenar datos usando esquemas y métodos de formato de datos adecuados y puede ser cualquier tipo adecuado de memoria, tal como memoria de solo lectura, memoria de acceso aleatorio, etc. La memoria 220 puede incluir, por ejemplo, claves y algoritmos de cifrado, protocolos y normas de comunicación, normas y protocolos de formato de datos, código de programa para módulos y programas de aplicación del dispositivo de procesamiento, y otros datos que pueden ser adecuados para su uso por el servidor de procesamiento 102 en la realización de las funciones divulgadas en el presente documento, como será evidente para los expertos en la materia relevante. En algunas realizaciones, la memoria 220 puede estar compuesta por o puede incluir por lo demás una base de datos relacional que utiliza lenguaje de consulta estructurado para el almacenamiento, identificación, modificación, actualización, acceso, etc., de conjuntos de datos estructurados almacenados en la misma.

Proceso para la verificación de un valor de datos a través de valores de ruta de troceo

La Figura 3 ilustra un proceso 300 para la verificación de un valor de datos basándose en una raíz de Merkle, usando valores de ruta de troceo proporcionados por el proveedor de datos 104.

En la etapa 302, el dispositivo de recepción 202 del servidor de procesamiento 102 puede recibir un valor de datos para la verificación a partir del proveedor de datos 104. El valor de datos puede estar acompañado por al menos un número de ocasión y una pluralidad de valores de ruta de troceo. En la etapa 304, el servidor de procesamiento 102 puede identificar la raíz de Merkle relacionada con los datos a verificar. En algunos casos, la identificación puede incluir la consulta (por ejemplo, por el módulo de consulta 210 del servidor de procesamiento 102) de la memoria 220 del servidor de procesamiento 102 para identificar la raíz de Merkle, tal como puede incluirse en una cadena de bloques. En otros casos, la identificación puede incluir la transmisión (por ejemplo, por el dispositivo de transmisión 216 del servidor de procesamiento 102) de una solicitud de datos a una entidad asociada, tal como la red de cadena de bloques 106, y la recepción (por ejemplo, por el dispositivo de recepción 202) de la raíz de Merkle.

En la etapa 306, el módulo de generación 212 del servidor de procesamiento 102 puede generar un valor combinado al combinar el valor de datos con el número de ocasión correspondiente proporcionado por el proveedor de datos 104. En algunos casos, la combinación del número de ocasión con el valor de datos puede incluir la adición matemática del número de ocasión al valor de datos. En la etapa 308, el módulo de cálculo de troceo 214 del servidor de procesamiento 102 puede trocear el siguiente valor a través de la aplicación de uno o más algoritmos de cálculo de troceo predeterminados al mismo. En la primera ejecución de la etapa 308, puede trocearse el valor de datos combinado.

En la etapa 310, el módulo de verificación 218 del servidor de procesamiento 102 puede determinar si el valor de troceo generado por el módulo de cálculo de troceo 214 coincide con el valor correspondiente en el árbol de Merkle. En algunos casos, la etapa 310 puede ser una etapa opcional, tal como en casos en los que el servidor de procesamiento 102 puede no tener acceso a los valores de árbol de Merkle (por ejemplo, donde solo puede accederse a la raíz de Merkle). Si el valor de troceo generado no coincide con el valor de árbol de Merkle, entonces

el proceso 300 puede completarse debido a que el valor de datos subyacente proporcionado por el proveedor de datos 104 puede, por lo tanto, ser incorrecto. En algunos casos, el dispositivo de transmisión 216 puede transmitir una señal de datos al proveedor de datos 104 que se superpone o se codifica de otro modo con una indicación de que la verificación no tuvo éxito.

Si el valor de troceo sí coincide con el valor de árbol de Merkle correspondiente, o si no puede realizarse una verificación de este tipo (por ejemplo, debido a la falta de disponibilidad de valores de árbol de Merkle), entonces, en la etapa 312, el servidor de procesamiento 102 puede determinar si hay valores de ruta de troceo adicionales restantes que usar en la generación de la raíz de Merkle. La determinación puede basarse en los datos proporcionados por el proveedor de datos 104, específicamente el número de valores de ruta de troceo proporcionados. Si no se han usado todos los valores de ruta de troceo, entonces el proceso 300 puede proceder a la etapa 314, donde el módulo de generación 212 puede combinar el valor de troceo con el siguiente valor de ruta de troceo. En algunos casos, los valores de ruta de troceo pueden ordenarse en un orden específico para su uso en la generación de los valores combinados. El proceso 300 puede volver entonces a la etapa 308, donde este valor recién combinado se trocea y se verifica, según sea aplicable.

El proceso 300 puede continuar ejecutándose hasta que, en la etapa 312, se determina que se ha usado cada valor de ruta de troceo, donde se determina que el valor de troceo resultante (por ejemplo, generado en la última ejecución de la etapa 308) es la raíz de Merkle. En tales casos, el resultado de la verificación realizada en la etapa 310 para la raíz de Merkle puede ser el resultado de verificación del valor de datos proporcionado. En algunas realizaciones, el método 300 también puede incluir la transmisión, por el dispositivo de transmisión 216, de una notificación al proveedor de datos 104 que indica el resultado del proceso 300, que puede indicar la verificación con éxito o sin éxito del valor de datos basándose en la verificación de la raíz de Merkle generada a partir del mismo.

Valores de ruta de troceo

La Figura 4 ilustra un árbol de Merkle y valores correspondientes incluidos en el mismo, que pueden usarse en la verificación de valores de datos usando los métodos y sistemas analizados en el presente documento. Será evidente para los expertos en la materia relevante que el árbol de Merkle ilustrado en la Figura 4 generado a partir de cuatro valores de datos subyacentes, los valores de datos V1, V2, V3 y V4, es solo ilustrativo, y que pueden generarse árboles de Merkle usando cualquier número adecuado de valores.

Como se ilustra en la Figura 4, el árbol de Merkle ilustrado en la misma puede generarse a partir de cuatro valores subyacentes, V1 - V4. Cada valor subyacente puede tener un número de ocasión N1 - N4 correspondiente. Los valores V1 - V4 pueden ser combinados con los números de ocasión N1 - N4 correspondientes, respectivamente, por el módulo de generación 212 del servidor de procesamiento 102. Después de combinarse, el módulo de cálculo de troceo 214 del servidor de procesamiento 102 puede trocear cada uno de los valores combinados a través de la aplicación de uno o más algoritmos de cálculo de troceo predeterminados al mismo. Los valores resultantes son valores de troceo H1 - H4, que pueden considerarse valores en el árbol de Merkle. El módulo de generación 212 puede combinar entonces pares de los valores, H1 con H2 y H3 con H4, y el módulo de cálculo de troceo 214 puede trocear los valores combinados para generar los valores de troceo H5 y H6, donde H5 es un troceo de la combinación de H1 y H2, y donde H6 es un troceo de la combinación de H3 y H4. El módulo de generación 212 puede combinar H5 y H6 y el módulo de cálculo de troceo 214 puede trocear el valor combinado para generar el valor de troceo H7.

El valor de troceo H7, que es un único valor de troceo en el árbol de Merkle sin ningún otro valor con el que combinarse, puede considerarse la raíz de Merkle para el árbol. En los métodos analizados en el presente documento, el servidor de procesamiento 102 puede comparar el valor de troceo H7 con una raíz de Merkle previamente identificada (por ejemplo, a partir de una cadena de bloques u otra fuente de datos de terceros) para verificar un valor de datos proporcionado por el proveedor de datos 104.

En algunas realizaciones, el servidor de procesamiento 102 puede configurarse para generar la raíz de Merkle H7 sin acceso a todos los valores de datos V1 - V4 subyacentes y los números de ocasión N1 - N4 correspondientes. En tales realizaciones, el proveedor de datos 104 puede dotar al servidor de procesamiento 102 de un valor de datos específico, tal como el valor de datos V3, y su número de ocasión correspondiente, N3 en un ejemplo de este tipo, así como cada uno de los valores de ruta de troceo necesarios para que el servidor de procesamiento 102 genere la raíz de Merkle H7. Los valores de ruta de troceo necesarios pueden ser los valores de troceo en el árbol de Merkle que se combinan con valores generados por el módulo de cálculo de troceo 214 del servidor de procesamiento 102 que son necesarios para generar la raíz de Merkle H7.

Por ejemplo, si el proveedor de datos 104 proporciona el valor V3 y su número de ocasión N3 correspondiente, entonces los valores de ruta de troceo serían valores de troceo H4 y H5. En un ejemplo de este tipo, el módulo de cálculo de troceo 214 puede generar H3 a partir de la combinación de V3 y N3, generar H6 a partir de H3 y el H4 proporcionado, y generar H7 a partir de H6 y el H5 proporcionado. Por lo tanto, H4 y H5 son valores de ruta de troceo si se va a verificar V3. En otro ejemplo, si se va a verificar V1, los valores de ruta de troceo serían H2 y H6. En tales casos, el servidor de procesamiento 102 puede ser capaz de generar la raíz de Merkle H7 sin acceso a

ninguno de los valores subyacentes adicionales, protegiendo de ese modo los valores al tiempo que se sigue habilitando que el servidor de procesamiento 102 verifique el valor de datos proporcionado.

Método ilustrativo para la verificación de un valor de datos a través de una raíz de Merkle

La Figura 5 ilustra un método 500 para la verificación de un valor de datos a través del uso de una raíz de Merkle y valores de ruta de troceo.

En la etapa 502, una raíz de Merkle puede almacenarse en una memoria (por ejemplo, la memoria 220) de un servidor de procesamiento (por ejemplo, el servidor de procesamiento 102). En la etapa 504, al menos un valor de datos, un número de ocasión y una pluralidad de valores de ruta de troceo pueden ser recibidos por un dispositivo de recepción (por ejemplo, el dispositivo de recepción 202) del servidor de procesamiento. En la etapa 506, un valor combinado puede ser generado por un módulo de generación (por ejemplo, el módulo de generación 212) del servidor de procesamiento al combinar el valor de datos y el número de ocasión. En la etapa 508, un primer valor de troceo puede ser generado por un módulo de cálculo de troceo (por ejemplo, el módulo de cálculo de troceo 214) del servidor de procesamiento a través de la aplicación de un algoritmo de cálculo de troceo al valor combinado.

En la etapa 510, un valor de troceo posterior puede ser generado por el módulo de cálculo de troceo del servidor de procesamiento a través de la aplicación del algoritmo de cálculo de troceo a una combinación del primer valor de troceo y un primero de la pluralidad de valores de ruta de troceo. En la etapa 512, la generación del valor de troceo posterior puede ser repetida por el módulo de cálculo de troceo del servidor de procesamiento usando una combinación del siguiente valor de ruta de troceo de la pluralidad de valores de ruta de troceo y un valor de troceo posterior más reciente. En la etapa 514, el valor de datos puede ser verificado por un módulo de verificación (por ejemplo, el módulo de verificación 218) del servidor de procesamiento basándose en una comparación de la raíz de Merkle y el último valor de troceo posterior generado.

En una realización, la pluralidad de valores de ruta de troceo pueden tener un orden especificado. En una realización adicional, el siguiente valor de ruta de troceo de la pluralidad de valores de ruta de troceo puede identificarse basándose en el orden especificado. En algunas realizaciones, el número de ocasión puede ser un número aleatorio o pseudoaleatorio de 256 bits. En una realización, el valor de datos y el número de ocasión pueden ser números enteros, y el valor combinado puede generarse al añadir el número de ocasión al valor de datos.

En algunas realizaciones, el método 500 puede incluir adicionalmente recibir, por el dispositivo de recepción del servidor de procesamiento, una cadena de bloques, en donde la cadena de bloques está compuesta por una pluralidad de bloques, estando compuesto cada bloque por un encabezamiento de bloque y uno o más valores de datos, en donde la raíz de Merkle se incluye en el encabezamiento de bloque de uno de la pluralidad de bloques. En una realización adicional, el método 500 puede incluir adicionalmente incluso ejecutar, por un módulo de consulta (por ejemplo, el módulo de consulta 210) del servidor de procesamiento, una consulta en la cadena de bloques para identificar el uno de la pluralidad de bloques. En aún otra realización más, recibir el valor de datos, el número de ocasión y la pluralidad de valores de ruta de troceo puede incluir adicionalmente recibir un identificador de bloque, y el identificador de bloque puede incluirse en el encabezamiento de bloque del uno de la pluralidad de bloques.

Arquitectura de sistema informático

La Figura 6 ilustra un sistema informático 600 en el que pueden implementarse realizaciones de la presente divulgación, o porciones de las mismas, como código legible por ordenador. Por ejemplo, el servidor de procesamiento 102 de la Figura 1 puede implementarse en el sistema informático 600 usando hardware, software, firmware, medios legibles por ordenador no transitorios que tienen instrucciones almacenadas en los mismos, o una combinación de los mismos, y puede implementarse en uno o más sistemas informáticos u otros sistemas de procesamiento. Hardware, software o cualquier combinación de los mismos pueden materializar módulos y componentes usados para implementar los métodos de las Figuras 3 y 4.

Si se usa lógica programable, tal lógica puede ejecutarse en una plataforma de procesamiento comercialmente disponible configurada por código de software ejecutable para volverse un ordenador de propósito específico o un dispositivo de propósito especial (por ejemplo, matriz lógica programable, circuito integrado de aplicación específica, etc.). Un experto en la materia puede apreciar que realizaciones de la materia objeto divulgada pueden practicarse con diversas configuraciones de sistema informático, incluyendo sistemas multiprocesador y multinúcleo, miniordenadores, ordenadores centrales, ordenadores enlazados o agrupados con funciones distribuidas, así como ordenadores ubicuos o en miniatura que pueden embeberse en prácticamente cualquier dispositivo. Por ejemplo, pueden usarse al menos un dispositivo de procesador y una memoria para implementar las realizaciones anteriormente descritas.

Una unidad o dispositivo de procesador como se analiza en este documento puede ser un único procesador, una pluralidad de procesadores o combinaciones de los mismos. Dispositivos de procesador pueden tener uno o más "núcleos" de procesador. Las expresiones "medio de programa informático", "medio legible por ordenador no transitorio" y "medio utilizable por ordenador" como se analizan en este documento se usan para referirse

generalmente a medios tangibles tal como una unidad de almacenamiento extraíble 618, una unidad de almacenamiento extraíble 622 y un disco duro instalado en una unidad de disco duro 612.

Diversas realizaciones de la presente divulgación se describen en términos de este sistema informático 600 de ejemplo. Después de leer esta descripción, será evidente para un experto en la materia relevante cómo implementar la presente divulgación usando otros sistemas informáticos y/o arquitecturas informáticas. Aunque operaciones pueden describirse como un proceso secuencial, algunas de las operaciones pueden de hecho realizarse en paralelo, simultáneamente y/o en un entorno distribuido, y con código de programa almacenado local o remotamente para acceso por máquinas de un único o múltiples procesadores. Además, en algunas realizaciones, el orden de las operaciones puede reorganizarse sin apartarse del espíritu de la materia objeto divulgada.

El dispositivo de procesador 604 puede ser un dispositivo de procesador de propósito especial o de propósito general configurado específicamente para realizar las funciones analizadas en el presente documento. El dispositivo de procesador 604 puede conectarse a una infraestructura de comunicación 606, tal como un bus, cola de mensajes, red, esquema de traspaso de mensajes multinúcleo, etc. La red puede ser cualquier red adecuada para realizar las funciones como se divulgan en este documento y puede incluir una red de área local (LAN), una red de área extensa (WAN), una red inalámbrica (por ejemplo, WiFi), una red de comunicación móvil, una red por satélite, Internet, fibra óptica, cable coaxial, infrarrojos, radiofrecuencia (RF) o cualquier combinación de las mismas. Otros tipos y configuraciones de red adecuados serán evidentes para los expertos en la materia relevante. El sistema informático 600 también puede incluir una memoria principal 608 (por ejemplo, memoria de acceso aleatorio, memoria de sólo lectura, etc.), y también puede incluir una memoria secundaria 610. La memoria secundaria 610 puede incluir la unidad de disco duro 612 y una unidad de disco de almacenamiento extraíble 614, tal como una unidad de disco flexible, una unidad de cinta magnética, una unidad de disco óptico, una memoria flash, etc.

La unidad de disco de almacenamiento extraíble 614 puede leer de y/o escribir en la unidad de almacenamiento extraíble 618 de una manera bien conocida. La unidad de almacenamiento extraíble 618 puede incluir un medio de almacenamiento extraíble que puede leerse por y escribirse por la unidad de disco de almacenamiento extraíble 614. Por ejemplo, si la unidad de almacenamiento extraíble 614 es una unidad de disco flexible o un puerto de bus serie universal, la unidad de almacenamiento extraíble 618 puede ser un disco flexible o una unidad flash portátil, respectivamente. En una realización, la unidad de almacenamiento extraíble 618 puede ser medio de grabación legible por ordenador no transitorio.

En algunas realizaciones, la memoria secundaria 610 puede incluir medios alternativos para permitir que programas informáticos u otras instrucciones se carguen en el sistema informático 600, por ejemplo, la unidad de almacenamiento extraíble 622 y una interfaz 620. Ejemplos de tales medios pueden incluir un cartucho de programa e interfaz de cartucho (por ejemplo, como se encuentran en sistemas de videojuegos), un chip de memoria extraíble (por ejemplo, EEPROM, PROM, etc.) y zócalo asociado, y otras unidades de almacenamiento extraíbles 622 e interfaces 620 como será evidente para los expertos en la materia relevante.

Datos almacenados en el sistema informático 600 (por ejemplo, en la memoria principal 608 y/o la memoria secundaria 610) pueden almacenarse en cualquier tipo de medio legible por ordenador adecuado, tal como almacenamiento óptico (por ejemplo, un disco compacto, disco versátil digital, disco Blu-ray, etc.) o almacenamiento de cinta magnética (por ejemplo, una unidad de disco duro). Los datos pueden configurarse en cualquier tipo de configuración de base de datos adecuada, tal como una base de datos relacional, una base de datos de lenguaje de consulta estructurada (SQL), una base de datos distribuida, una base de datos de objetos, etc. Configuraciones y tipos de almacenamiento adecuados serán evidentes para un experto en la materia relevante.

El sistema informático 600 también puede incluir una interfaz de comunicaciones 624. La interfaz de comunicaciones 624 puede configurarse para permitir que software y datos se transfieran entre el sistema informático 600 y dispositivos externos. Interfaces de comunicaciones 624 ilustrativas pueden incluir un módem, una interfaz de red (por ejemplo, una tarjeta de Ethernet), un puerto de comunicaciones, una ranura y tarjeta PCMCIA, etc. Software y datos transferidos a través de la interfaz de comunicaciones 624 pueden ser en forma de señales, que pueden ser electrónicas, electromagnéticas, ópticas u otras señales como será evidente para expertos en la materia relevante. Las señales pueden viajar a través de una trayectoria de comunicación 626, que puede configurarse para transportar las señales y puede implementarse usando hilo, cable, fibra óptica, una línea telefónica, un enlace de teléfono celular, un enlace de radiofrecuencia, etc.

El sistema informático 600 puede incluir adicionalmente una interfaz de visualizador 602. La interfaz de visualizador 602 puede configurarse para permitir que los datos se transfieran entre el sistema informático 600 y el visualizador externo 630. Las interfaces de visualizador 602 ilustrativas pueden incluir una interfaz multimedios de alta definición (HDMI), una interfaz visual digital (DVI), una matriz de gráficos de vídeo (VGA), etc. El visualizador 630 puede ser cualquier tipo de visualizador adecuado para mostrar datos transmitidos a través de la interfaz de visualización 602 del sistema informático 600, incluyendo un visualizador de tubo de rayos catódicos (CRT), visualizador de cristal líquido (LCD), visualizador de diodos emisores de luz (LED), visualizador táctil capacitivo, visualizador de transistores de película delgada (TFT), etc.

Medio de programa informático y medio utilizable por ordenador pueden referirse a memorias, tal como la memoria principal 608 y memoria secundaria 610, que pueden ser semiconductores de memoria (por ejemplo, DRAM, etc.). Estos productos de programa informático pueden ser medios para proporcionar software al sistema informático 600. Programas informáticos (por ejemplo, lógica de control informático) pueden almacenarse en la memoria principal 608 y/o la memoria secundaria 610. También pueden recibirse programas informáticos a través de la interfaz de comunicaciones 624. Tales programas informáticos, cuando se ejecutan, pueden habilitar que el sistema informático 600 implemente los presentes métodos como se analiza en este documento. En particular, los programas informáticos, cuando se ejecutan, pueden habilitar que el dispositivo de procesador 604 implemente los métodos ilustrados por las Figuras 3 y 4, como se analiza en este documento. En consecuencia, tales programas informáticos pueden representar controladores del sistema informático 600. Donde la presente divulgación se implementa usando software, el software puede almacenarse en un producto de programa informático y cargarse en el sistema informático 600 usando la unidad de disco de almacenamiento extraíble 614, interfaz 620 y unidad de disco duro 612 o interfaz de comunicaciones 624.

El dispositivo de procesador 604 puede comprender uno o más módulos o motores configurados para realizar las funciones del sistema informático 600. Cada uno de los módulos o motores puede implementarse usando hardware y, en algunos casos, también puede utilizar software, tal como uno correspondiente a código de programa y/o programas almacenados en la memoria principal 608 o la memoria secundaria 610. En tales casos, el código de programa puede ser compilado por el dispositivo de procesador 604 (por ejemplo, por un módulo o motor de compilación) antes de la ejecución por el hardware del sistema informático 600. Por ejemplo, el código de programa puede ser código fuente escrito en un lenguaje de programación que se traduce a un lenguaje de nivel inferior, tal como lenguaje ensamblador o código máquina, para su ejecución por el dispositivo de procesador 604 y/o cualquier componente de hardware adicional del sistema informático 600. El proceso de compilación puede incluir el uso de análisis léxico, preprocesamiento, análisis, análisis semántico, traducción dirigida por sintaxis, generación de código, optimización de código y cualquier otra técnica que pueda ser adecuada para la traducción del código de programa a un lenguaje de nivel inferior adecuado para controlar el sistema informático 600 para realizar las funciones divulgadas en el presente documento. Será evidente para los expertos en la materia relevante que tales procesos dan como resultado que el sistema informático 600 sea un sistema informático especialmente configurado 600 programado de manera singular para realizar las funciones analizadas anteriormente.

Técnicas consistentes con la presente divulgación proporcionan, entre otras características, sistemas y métodos para la verificación de valores de datos a través de una raíz de Merkle. Aunque se han descrito anteriormente diversas realizaciones ilustrativas del sistema y método divulgados debería entenderse que se han presentado para propósitos de ejemplo únicamente, no limitaciones. No es exhaustivo y no limita la divulgación a la forma precisa divulgada. Son posibles modificaciones y variaciones a la luz de las enseñanzas anteriores o pueden obtenerse a partir de la puesta en práctica de la divulgación. El alcance de la invención se define por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para la verificación de un valor de datos a través de una raíz de Merkle, que comprende:

almacenar, en una memoria de un servidor de procesamiento, una raíz de Merkle;
recibir, por un dispositivo de recepción del servidor de procesamiento, al menos un valor de datos, un número de ocasión y una pluralidad de valores de ruta de troceo;
generar, por un módulo de generación del servidor de procesamiento, un valor combinado al combinar el valor de datos y el número de ocasión;
generar, por un módulo de cálculo de troceo del servidor de procesamiento, un primer valor de troceo a través de la aplicación de un algoritmo de cálculo de troceo al valor combinado;
generar, por el módulo de cálculo de troceo del servidor de procesamiento, un valor de troceo posterior a través de la aplicación del algoritmo de cálculo de troceo a una combinación del primer valor de troceo y un primero de la pluralidad de valores de ruta de troceo;
repetir, por el módulo de cálculo de troceo del servidor de procesamiento, la generación del valor de troceo posterior usando una combinación del siguiente valor de ruta de troceo de la pluralidad de valores de ruta de troceo y el valor de troceo posterior más reciente; y
verificar, por un módulo de verificación del servidor de procesamiento, el valor de datos basándose en una comparación de la raíz de Merkle y el último valor de troceo posterior generado.

2. El método de la reivindicación 1, en donde la pluralidad de valores de ruta de troceo tienen un orden especificado.

3. El método de la reivindicación 2, en donde el siguiente valor de ruta de troceo de la pluralidad de valores de ruta de troceo se identifica basándose en el orden especificado.

4. El método de la reivindicación 1, en donde el número de ocasión es un número aleatorio o pseudoaleatorio de 256 bits.

5. El método de la reivindicación 1, en donde
el valor de datos y el número de ocasión son números enteros, y
el valor combinado se genera al añadir el número de ocasión al valor de datos.

6. El método de la reivindicación 1, que comprende adicionalmente:

recibir, por el dispositivo de recepción del servidor de procesamiento, una cadena de bloques, en donde la cadena de bloques está compuesta por una pluralidad de bloques, estando compuesto cada bloque por un encabezamiento de bloque y uno o más valores de datos, en donde
la raíz de Merkle se incluye en el encabezamiento de bloque de uno de la pluralidad de bloques.

7. El método de la reivindicación 6, que comprende adicionalmente:
ejecutar, por un módulo de consulta del servidor de procesamiento, una consulta en la cadena de bloques para identificar el uno de la pluralidad de bloques.

8. El método de la reivindicación 7, en donde
recibir el valor de datos, el número de ocasión y la pluralidad de valores de ruta de troceo incluye adicionalmente recibir un identificador de bloque, y
el identificador de bloque se incluye en el encabezamiento de bloque del uno de la pluralidad de bloques.

9. Un sistema para la verificación de un valor de datos a través de una raíz de Merkle, que comprende:

una memoria de un servidor de procesamiento configurada para almacenar una raíz de Merkle;
un dispositivo de recepción del servidor de procesamiento configurado para recibir al menos un valor de datos, un número de ocasión y una pluralidad de valores de ruta de troceo;
un módulo de generación del servidor de procesamiento configurado para generar un valor combinado al combinar el valor de datos y el número de ocasión;
un módulo de cálculo de troceo del servidor de procesamiento configurado para

generar un primer valor de troceo a través de la aplicación de un algoritmo de cálculo de troceo al valor combinado,
generar un valor de troceo posterior a través de la aplicación del algoritmo de cálculo de troceo a una combinación del primer valor de troceo y un primero de la pluralidad de valores de ruta de troceo, y
repetir la generación del valor de troceo posterior usando una combinación del siguiente valor de ruta de troceo de la pluralidad de valores de ruta de troceo y el valor de troceo posterior más reciente; y

un módulo de verificación del servidor de procesamiento configurado para verificar el valor de datos basándose en una comparación de la raíz de Merkle y el último valor de troceo posterior generado.

10. El sistema de la reivindicación 9, en donde la pluralidad de valores de ruta de troceo tienen un orden especificado.

11. El sistema de la reivindicación 10, en donde el siguiente valor de ruta de troceo de la pluralidad de valores de ruta de troceo se identifica basándose en el orden especificado.

12. El sistema de la reivindicación 9, en donde el número de ocasión es un número aleatorio o pseudoaleatorio de 256 bits.

13. El sistema de la reivindicación 9, en donde
el valor de datos y el número de ocasión son números enteros, y
el valor combinado se genera al añadir el número de ocasión al valor de datos.

14. El sistema de la reivindicación 9, en donde
el dispositivo de recepción del servidor de procesamiento está configurado adicionalmente para recibir una cadena de bloques, en donde la cadena de bloques está compuesta por una pluralidad de bloques, estando compuesto cada bloque por un encabezamiento de bloque y uno o más valores de datos, y
la raíz de Merkle se incluye en el encabezamiento de bloque de uno de la pluralidad de bloques.

15. El sistema de la reivindicación 14, que comprende adicionalmente:
un módulo de consulta del servidor de procesamiento configurado para ejecutar una consulta en la cadena de bloques para identificar el uno de la pluralidad de bloques.

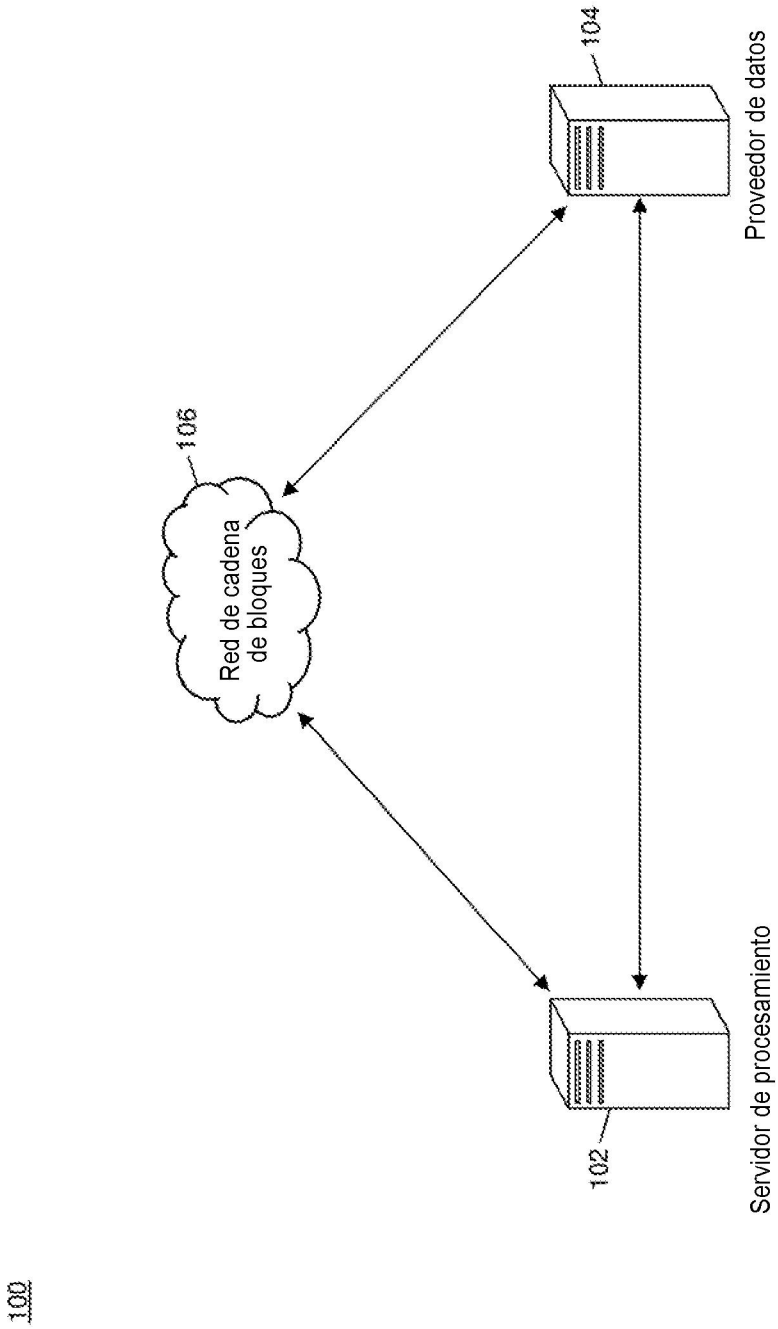
100
102
Servidor de procesamiento
104
Proveedor de datos
106
Red de cadena de bloques

FIG. 1

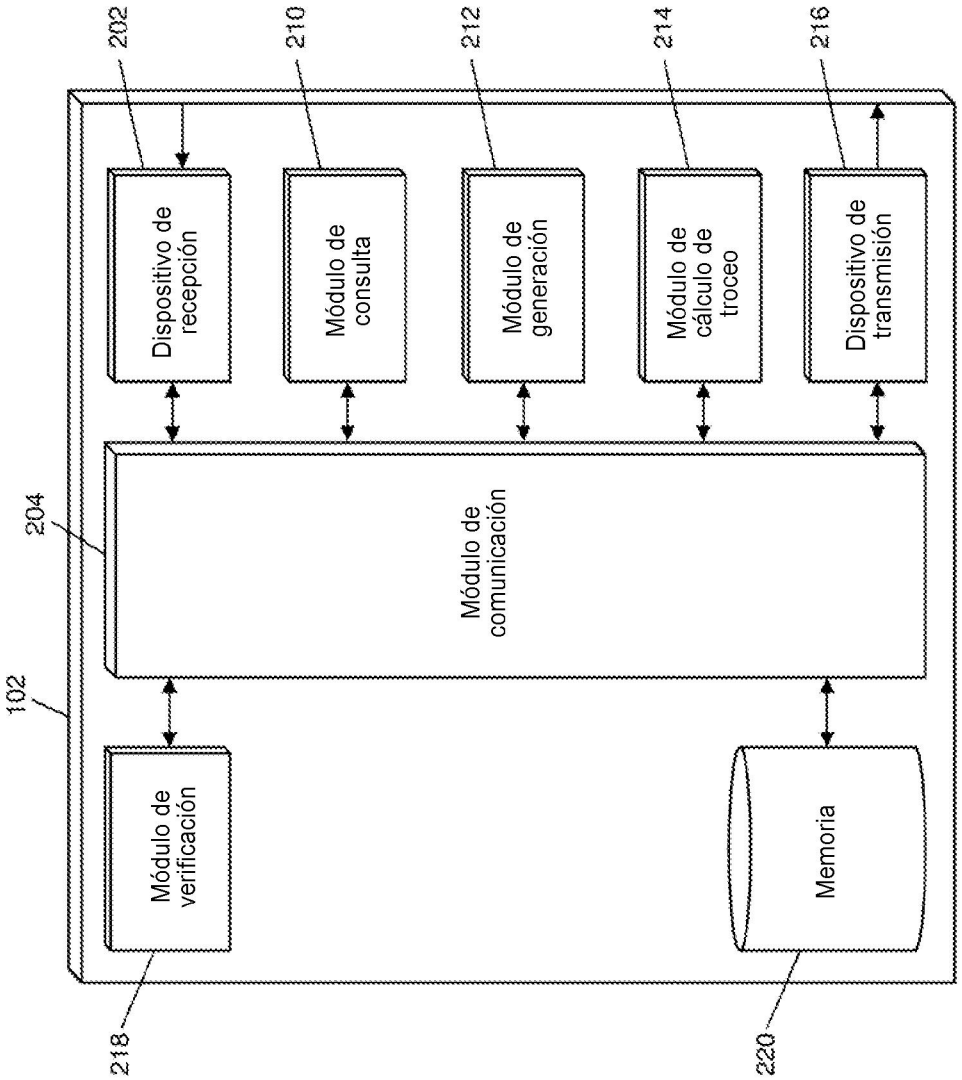
202
210
212
214
216
Dispositivo de recepción
Módulo de consulta
Módulo de generación
Módulo de cálculo de troceo
Dispositivo de transmisión
204
Módulo de comunicación
102
Módulo de verificación
Memoria
218
220

FIG. 2

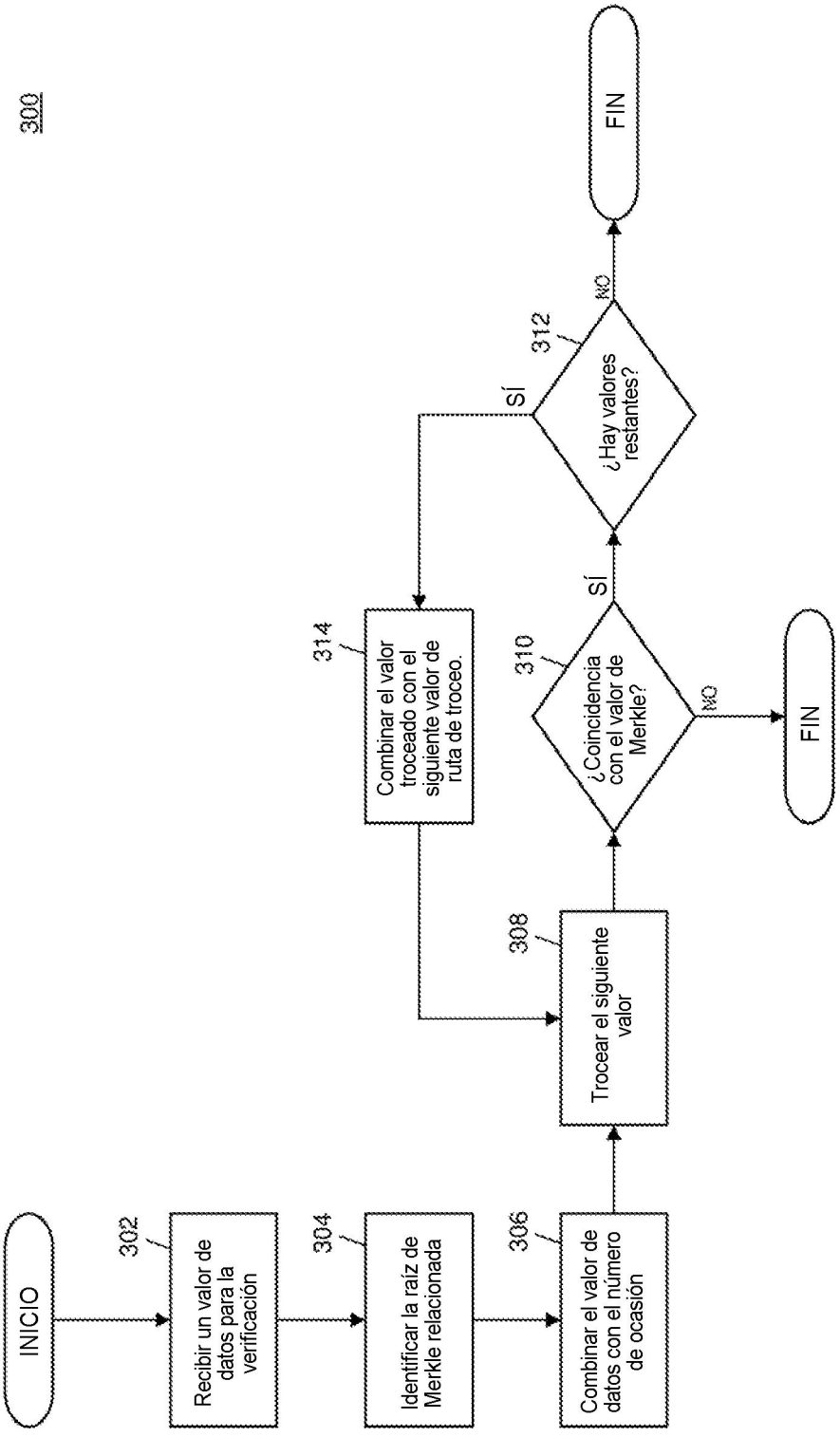
300
INICIO
302
Recibir un valor de datos para la verificación
304
Identificar la raíz de Merkle relacionada
306
Combinar el valor de datos con el número de ocasión
308
Trocear el siguiente valor
310
¿Coincidencia con el valor de Merkle?
NO
FIN
SÍ
312
¿Hay valores restantes?
SÍ
NO
FIN
314
Combinar el valor troceado con el siguiente valor de ruta de troceo.

FIG. 3

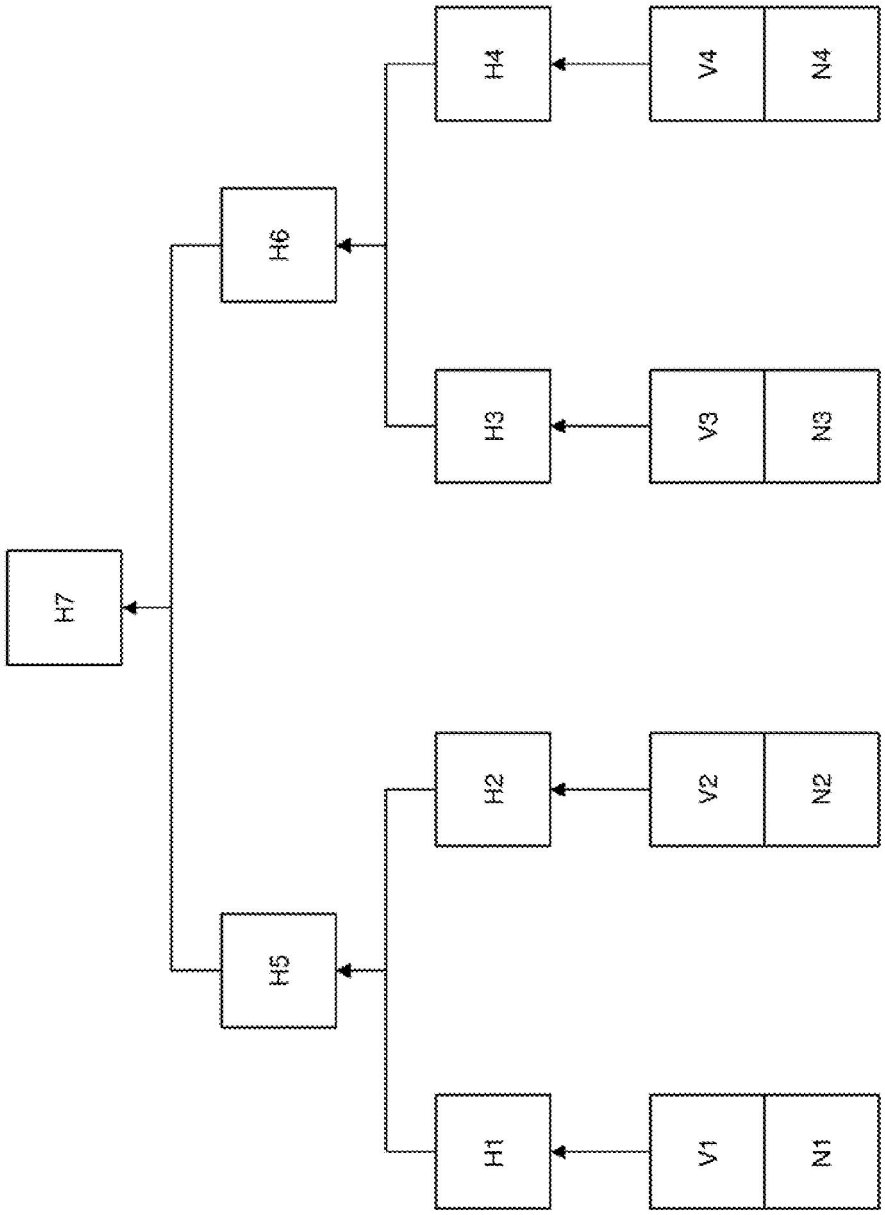

FIG. 4

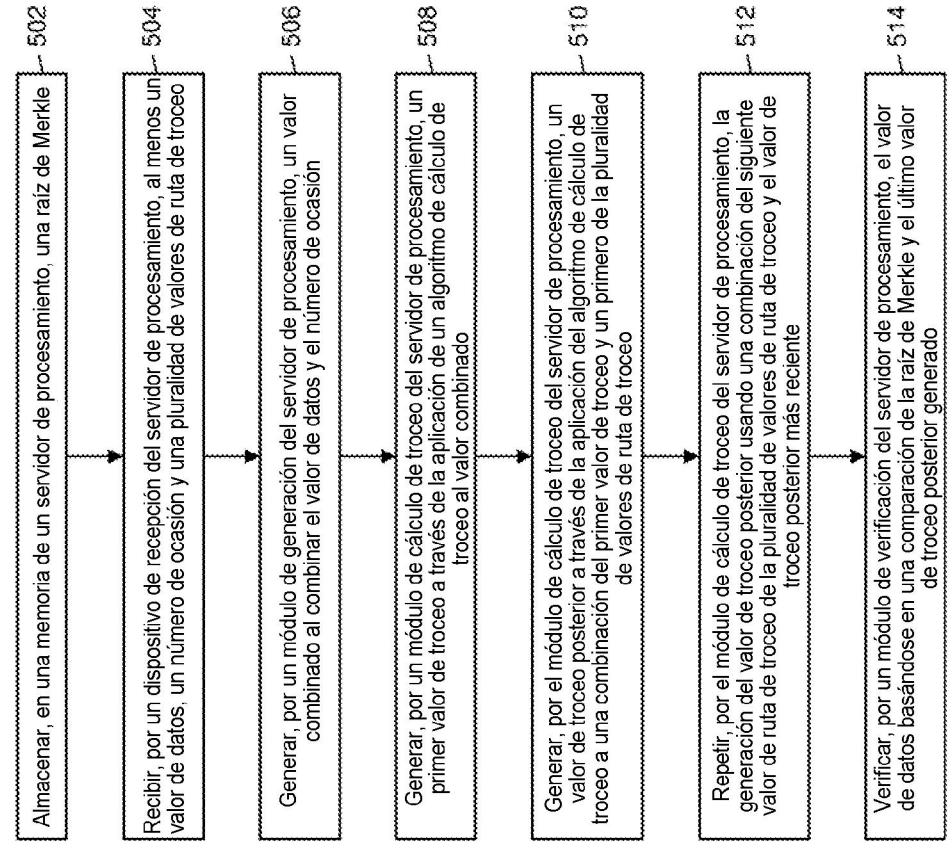
500
502
Almacenar, en una memoria de un servidor de procesamiento, una raíz de Merkle
504
Recibir, por un dispositivo de recepción del servidor de procesamiento, al menos un valor de datos, un número de ocasión y una pluralidad de valores de ruta de troceo
506
Generar, por un módulo de generación del servidor de procesamiento, un valor combinado al combinar el valor de datos y el número de ocasión
508
Generar, por un módulo de cálculo de troceo del servidor de procesamiento, un primer valor de troceo a través de la aplicación de un algoritmo de cálculo de troceo al valor combinado
510
Generar, por el módulo de cálculo de troceo del servidor de procesamiento, un valor de troceo posterior a través de la aplicación del algoritmo de cálculo de troceo a una combinación del primer valor de troceo y un primero de la pluralidad de valores de ruta de troceo
512
Repetir, por el módulo de cálculo de troceo del servidor de procesamiento, la generación del valor de troceo posterior usando una combinación del siguiente valor de ruta de troceo de la pluralidad de valores de ruta de troceo y el valor de troceo posterior más reciente
514
Verificar, por un módulo de verificación del servidor de procesamiento, el valor de datos basándose en una comparación de la raíz de Merkle y el último valor de troceo posterior generado

FIG. 5

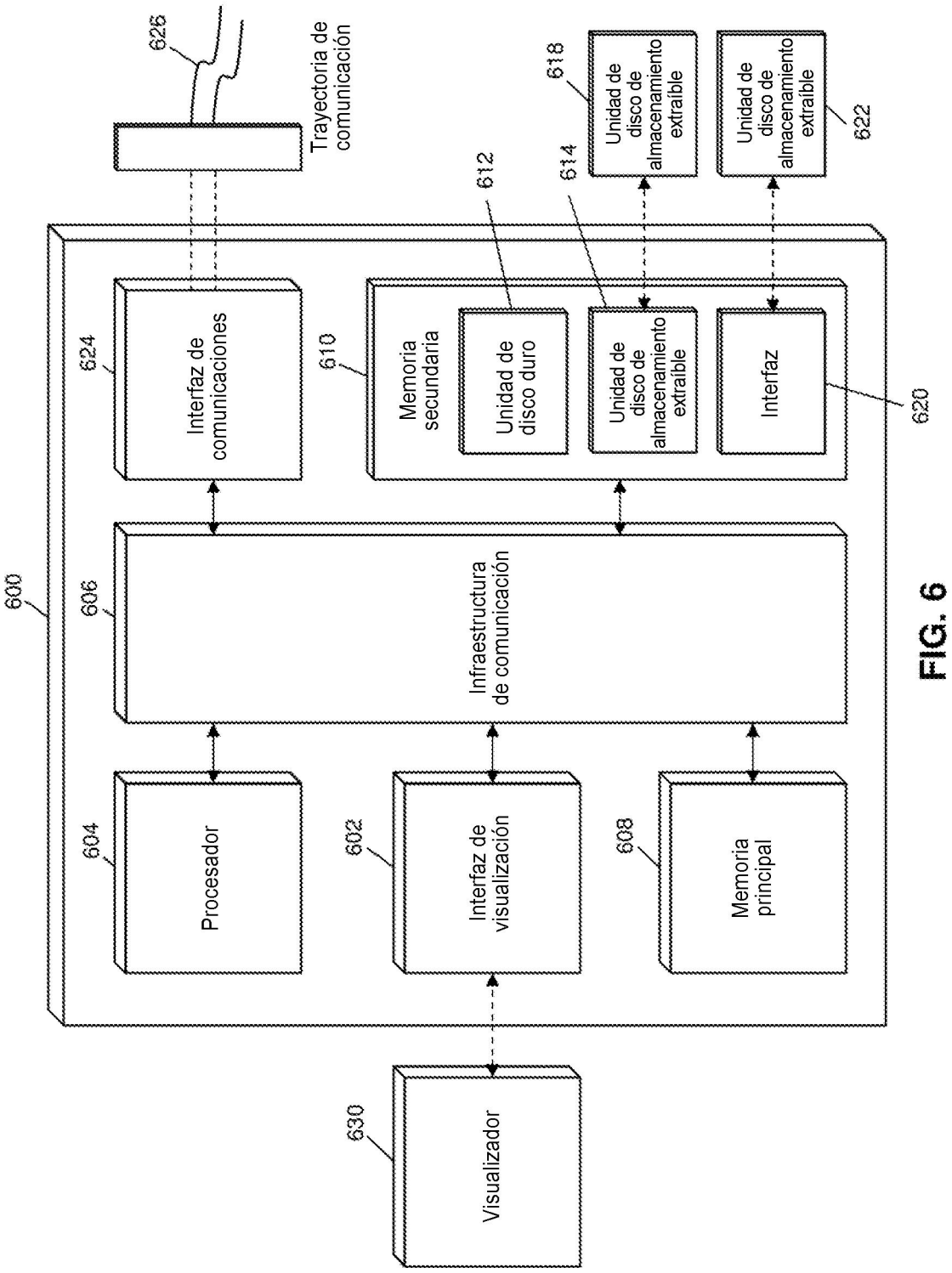
626
Trayectoria de comunicación
618
Unidad de disco de almacenamiento extraíble
622
Unidad de disco de almacenamiento extraíble
612
614
624
Interfaz de comunicaciones
610
Memoria secundaria
Unidad de disco duro
Unidad de disco de almacenamiento extraíble
Interfaz
620
600
606
Infraestructura de comunicación
604
Procesador
602
Interfaz de visualización
608
Memoria principal
630
Visualizador

FIG. 6