(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 809 510**

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.08.2018 PCT/US2018/047975**

(87) Fecha y número de publicación internacional: **28.02.2019 WO19040886**

(96) Fecha de presentación y número de la solicitud europea: **24.08.2018 E 18769002 (9)**

(97) Fecha y número de publicación de la concesión europea: **22.07.2020 EP 3586474**

(54) Título: **Método y aparato de selección de nodos de consenso, y servidor**

(30) Prioridad:

24.08.2017 CN 201710736740

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.03.2021

(73) Titular/es:

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

(72) Inventor/es:

TANG, QIANG

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y aparato de selección de nodos de consenso, y servidor

REFERENCIA A SOLICITUDES RELACIONADAS

Esta solicitud reivindica la prioridad de la solicitud de patente china número 201710736740.5, presentada el 24 de agosto de 2017.

CAMPO TÉCNICO

La presente memoria descriptiva pertenece al sector de las tecnologías informáticas de procesamiento de datos y, en particular, a un método y un aparato de selección de nodos de consenso, y un servidor.

ESTADO DE LA TÉCNICA ANTERIOR

La tecnología de cadena de bloques es generalmente una tecnología de base de datos distribuida centralizada, con características tales como descentralización, transparencia, resistencia a manipulaciones, confianza, etc. Se puede utilizar para registrar información de datos en una red entre pares pública o privada. Para garantizar la consistencia de los datos de una cadena de bloques, los datos son generados y actualizados en la cadena de bloques utilizando un algoritmo de consenso. El algoritmo de tolerancia a fallos bizantinos práctica (PBFT, Practical Byzantine Fault Tolerance) es un algoritmo de consenso de consistencia distribuido, utilizado habitualmente en la industria.

PBFT es un algoritmo de replicación de máquina de estado. Normalmente, se seleccionan algunos nodos entre una serie de nodos en la cadena de bloques, como nodos de consenso para procesamiento de consenso. Normalmente, puede haber de 4 a 11 nodos de consenso participando en el consenso. Actualmente, en PBFT, los algoritmos para la selección de nodos de consenso pueden incluir selección aleatoria y selección fija. En la selección aleatoria de nodo de consenso, es difícil diseñar un algoritmo para hacer que todos los nodos aprueben un nodo de consenso recién seleccionado, y la propia selección de nodos es un proceso complicado de obtención de consenso. La selección fija de nodo de consenso es más simple que la selección aleatoria en términos de implementación, por ejemplo, solamente es necesario distribuir código fuente a todos los nodos. Sin embargo, este método se complica cuando se produce un fallo o cuando un nodo de consenso es actualizado por alguna razón.

Actualmente, existe una necesidad en la industria de una solución de selección de nodos de consenso PBFT que sea fácil de implementar y mantener, muy eficiente, y fiable. La publicación de internet "Neo: Election and Voting" (http://docs.neo.org/en-us/node/gui/vote.html) describe un método para determinar un nodo de consenso para cadena de bloques.

RESUMEN

Una o varias implementaciones de la presente memoria descriptiva están destinadas a proporcionar un método y un aparato de selección de nodos de consenso, y un servidor, para seleccionar un nodo de consenso de manera más fácil, eficiente y fiable en PBFT.

El método y el aparato de selección de nodos de consenso y el servidor dados a conocer en una o varias implementaciones de la presente memoria descriptiva se implementan utilizando los métodos siguientes:

Un método de selección de nodos de consenso incluye: obtener un resultado de la votación de participación accionarial de un nodo accionista para por lo menos un nodo esperado seleccionado, donde el nodo accionista incluye un nodo que posee por lo menos uno de los derechos accionariales totales predeterminados; determinar, en base al resultado de la votación de participación accionarial, el número de acciones que posee cada nodo accionista después de la votación de participación accionarial; y determinar un resultado de la selección de nodos de consenso en base al número de acciones que posee cada nodo accionista después de la votación de participación accionarial.

Un aparato de selección de nodos de consenso incluye: un módulo de adquisición del resultado de la votación, configurado para obtener un resultado de la votación de participación accionarial de un nodo accionista para por lo menos un nodo esperado seleccionado, donde dicho por lo menos un nodo accionista incluye un nodo que posee por lo menos una de las acciones totales predeterminadas; un módulo de determinación del resultado de la votación, configurado para determinar, en base al resultado de la votación de participación accionarial, el número de acciones que posee cada nodo accionista después de la votación de participación accionarial; y un módulo de determinación del nodo de consenso, configurado para determinar un resultado de la selección de nodos de consenso en base al número de acciones que posee cada nodo accionista después de la votación de participación accionarial.

Un aparato de selección de nodos de consenso incluye un procesador y una memoria configurada para almacenar una instrucción ejecutable por procesador. El procesador ejecuta la instrucción para: obtener un resultado de la votación de participación accionarial de un nodo accionista para por lo menos un nodo esperado, donde el nodo accionista incluye un nodo que posee por lo menos una de las acciones totales predeterminadas; determinar, en base al resultado de la votación de participación accionarial, el número de acciones que posee cada nodo accionista

después de la votación de participación accionarial; y determinar un resultado de la selección de nodos de consenso en base al número de acciones que posee cada nodo accionista después de la votación de participación accionarial.

Un servidor incluye por lo menos un procesador y una memoria configurados para almacenar una instrucción ejecutable por procesador. El procesador ejecuta la instrucción para: obtener un resultado de la votación de participación accionarial de un nodo accionista para por lo menos un nodo esperado, donde el nodo accionista incluye un nodo que posee por lo menos una de las acciones totales predeterminadas; determinar, en base al resultado de la votación de participación accionarial, el número de acciones que posee cada nodo accionista después de la votación de participación accionarial; y determinar un resultado de la selección de nodos de consenso en base al número de acciones que posee cada nodo accionista después de la votación de participación accionarial.

En el método y el aparato de selección de nodos de consenso, y en el servidor dados a conocer en una o varias implementaciones de la presente memoria descriptiva, un nodo accionista puede conducir una votación de participación accionarial, y seleccionar un nodo para participar en un consenso en base al número de acciones que poseen los nodos accionistas en un resultado de la votación. El método es fácil de implementar. El resultado de la selección es real y válido, y el resultado de la votación se da a conocer en toda la red y puede ser aprobado por otros nodos. Basándose en la solución de implementación en la presente memoria descriptiva, un nodo de consenso se puede seleccionar rápidamente en base a la proporción de acciones después de la votación de participación accionarial. De este modo, se reduce el consumo en un proceso de consenso, se simplifican las etapas de proceso de consenso, se mejora la eficiencia de la selección de nodos de consenso y el resultado de la selección es más fiable.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para describir más claramente las soluciones técnicas en la implementación de la presente memoria descriptiva o la tecnología existente, a continuación se describen brevemente los dibujos adjuntos para describir las implementaciones o la tecnología existente. Evidentemente, los dibujos adjuntos en las siguientes descripciones muestran tan sólo algunas implementaciones de la presente memoria descriptiva, y un experto en la materia puede no obstante obtener sin esfuerzos creativos otros dibujos a partir de estos dibujos adjuntos.

La figura 1 es un diagrama estructural esquemático que muestra la asignación de acciones totales predeterminadas a nodos y nodos de cadena de bloques servidos por un servidor de certificados, de acuerdo con una implementación de la presente memoria descriptiva.

La figura 2 es un diagrama esquemático que muestra un proceso de procesamiento de un método en un escenario de implementación, de acuerdo con la presente memoria descriptiva.

La figura 3 es un diagrama de flujo esquemático que muestra otra implementación del método, de acuerdo con la presente memoria descriptiva.

La figura 4 es un diagrama esquemático que muestra un escenario de selección de un nodo de consenso en una red de cadenas de bloques, de acuerdo con una implementación de la presente memoria descriptiva.

La figura 5 es un diagrama estructural esquemático que muestra módulos en un aparato de selección de nodos de consenso, de acuerdo con una implementación de la presente memoria descriptiva.

La figura 6 es un diagrama estructural esquemático que muestra módulos en un aparato de selección de nodos de consenso, de acuerdo con otra implementación de la presente memoria descriptiva.

La figura 7 es un diagrama estructural esquemático que muestra un servidor, de acuerdo con una implementación de la presente memoria descriptiva.

La figura 8 es un diagrama de flujo que muestra un ejemplo de un método implementado por ordenador, para seleccionar nodos de consenso en una cadena de bloques, de acuerdo con una implementación de la presente invención.

DESCRIPCIÓN DE IMPLEMENTACIONES

Para que un experto en la materia comprenda mejor las soluciones técnicas en la presente memoria descriptiva, a continuación, se describen de manera clara y exhaustiva las soluciones técnicas en las implementaciones de la presente memoria descriptiva, haciendo referencia a los dibujos adjuntos de las implementaciones de la presente memoria descriptiva. Evidentemente, las implementaciones descritas son tan sólo algunas, y no la totalidad de las implementaciones de la presente memoria descriptiva. Otras implementaciones obtenidas sin esfuerzos creativos por un experto en la materia basándose en las implementaciones de la presente memoria descriptiva, quedarán dentro del alcance de protección de la presente memoria descriptiva.

Aunque la presente memoria descriptiva da a conocer etapas operativas del método o una estructura de un aparato en las siguientes implementaciones o en los dibujos adjuntos, el método o el aparato pueden incluir, basándose en esfuerzos convencionales o no creativos, más etapas operativas o unidades de módulo, o menos etapas operativas o unidades de módulo después de la combinación de algunas etapas operativas o unidades de módulo. En las etapas

o estructuras sin necesaria causalidad lógica, la secuencia de ejecución de las etapas o la estructura de módulos del aparato no se limita a la secuencia de ejecución o a la estructura de módulos mostrada en las implementaciones o en los dibujos adjuntos en la presente memoria descriptiva. Cuando el método o la estructura de módulos se aplica a un aparato, servidor o producto terminal real, el método o la estructura de módulos se pueden ejecutar en una secuencia basada en el método o la estructura de módulos mostrada en las implementaciones o los dibujos adjuntos, o se puede ejecutar en paralelo (por ejemplo, en un entorno de procesamiento en paralelo, en un entorno de procesamiento multiproceso, e incluso en un entorno de procesamiento distribuido y un entorno de agrupación de servidores).

PBFT es un algoritmo de replicación de máquina de estado, es decir, un servicio utilizado como una máquina de estado para modelización. El servicio es normalmente un servicio de aplicación específica proporcionado por un servidor. Por ejemplo, para completar una transferencia, el servicio "transferir" se puede modelizar como una máquina de estado. La máquina de estado se replica en diferentes nodos en un sistema distribuido. Generalmente, cada copia de la máquina de estado almacena un estado de servicio, e implementa una operación de servicio. Cuando el número de nodos en una cadena de bloques supera un número determinado, los nodos que participan en el consenso pueden reducir la eficiencia del consenso. Por lo tanto, es necesario seleccionar algunos nodos a partir de los nodos en la cadena de bloques como nodos de consenso, utilizando un método, para que participen en el consenso. Por ejemplo, se generan copias por medio de modelización, y otros nodos están solamente sincronizados con un resultado del consenso (por ejemplo, son replicados) y no participan en el proceso de consenso.

En el algoritmo de consenso PBFT, normalmente, hay de 4 a 11 nodos participando en el consenso. Si hay menos de cuatro nodos participando en el consenso, el algoritmo PBFT deja de ser válido. Si hay más de 11 nodos participando en el consenso, el rendimiento del consenso disminuye con el incremento de los nodos. Para equilibrar la tolerancia a fallos bizantinos y el rendimiento del consenso, es necesario seleccionar algunos nodos como nodos de consenso a partir de un gran número de nodos, para que participen en el consenso. El consenso indica normalmente que los nodos distribuidos en una cadena de bloques pueden utilizar el mismo algoritmo y el mismo formato de datos (o el mismo protocolo de procesamiento) para generar y actualizar datos utilizando diferentes lenguajes. Las implementaciones de la presente memoria descriptiva proporcionan un método de selección de nodos de consenso PBFT eficaz basado en votación de participación accionarial. El método es fácil de implementar. Los nodos seleccionados son reales y válidos, y pueden ser aprobados por otros nodos. En una implementación específica, se puede introducir un servidor de certificados, y una clave pública del servidor de certificados se puede escribir en un bloque de creación en una cadena de bloques (un bloque de almacenamiento de datos en la cadena de bloques). Cada nodo en la cadena de bloques tiene que solicitar un certificado raíz a un servidor de certificados raíz. El certificado raíz puede ser utilizado para demostrar la validez de una identidad de nodo.

En la presente implementación, el número total de acciones puede ser predeterminado. Por ejemplo, el número total de acciones de todos los nodos en una cadena de bloques se puede ajustar a 100. En la presente implementación de la presente memoria descriptiva, las acciones pueden tener la misma fuerza (o ponderación), y las acciones se pueden transferir de un nodo a otro nodo en la cadena de bloques. Las acciones pueden ser consideradas un activo y se pueden negociar en la cadena de bloques. La validez de las acciones se puede demostrar en un proceso de confirmación de transacción basado en información registrada en un bloque de creación. El número total de acciones se puede determinar en base al número real de nodos, a un entorno de implementación, etc. Generalmente, el número total de acciones determinado es único y permanece invariable. Ciertamente, en otras implementaciones de la presente memoria descriptiva, el número total de acciones se puede incrementar o disminuir en base a un requisito de procesamiento de servicio, por ejemplo, un nodo importante al que se acaba de acceder posee 10 acciones. Las acciones totales se pueden asignar a los nodos correspondientes basándose en una regla de servicio. Una regla de asignación específica se puede determinar en base al tamaño del nodo, al volumen de tráfico, la importancia, etc. En una o varias implementaciones de la presente memoria descriptiva, un nodo asignado con una acción de las acciones totales predeterminadas se puede denominar un nodo accionista, o se puede considerar como un nodo que posee por lo menos una de las acciones totales predeterminadas. La figura 1 es un diagrama estructural esquemático que muestra la asignación de acciones totales predeterminadas a nodos y nodos de cadena de bloques servidos por un servidor de certificados, de acuerdo con la presente memoria descriptiva.

Por lo tanto, cuando un nodo de consenso tiene que ser seleccionado en PBFT, un nodo que posee una acción puede elegir votar por un nodo esperado, y el resultado de la votación se puede difundir a toda la red de cadenas de bloques. Después de la votación, cada nodo puede recibir el mismo resultado de la votación de participación accionarial, y determinar a continuación un resultado de la selección de nodos de consenso en base al número de acciones que posee cada nodo. Se muestra una implementación específica en la figura 2. La presente memoria descriptiva proporciona una implementación de un método de selección de nodos de consenso. El método puede incluir las etapas siguientes:

S2. Obtener un resultado de la votación de participación accionarial de un nodo accionista para por lo menos un nodo esperado, donde el nodo accionista incluye un nodo que posee por lo menos una de las acciones totales predeterminadas.

Un nodo al que vota el nodo accionista se puede denominar el nodo esperado. El nodo esperado puede incluir un nodo accionista que posee una acción, o puede incluir un nodo que no posee ninguna acción antes de la votación. En una implementación, un nodo que posee una acción puede elegir independientemente votar a cualquier nodo. La base

para seleccionar el nodo esperado puede incluir, de forma no limitativa, la estabilidad de rendimiento del servicio del nodo, la capacidad de servicio del nodo, la política de selección determinada por un operador, etc. En una implementación de la presente memoria descriptiva, el nodo esperado seleccionado puede incluir: por lo menos un nodo seleccionado por el nodo accionista en base a una condición de selección de nodos de consenso predeterminada para votar con una acción al mismo.

La condición de selección de nodos de consenso predeterminada puede incluir por lo menos una de la estabilidad de rendimiento de servicio del nodo, la capacidad de servicio del nodo, la política de detección determinada por un operador, etc. El nodo accionista puede votar por sí mismo, o puede votar por otro nodo.

En la presente implementación de la presente memoria descriptiva, un nodo que posee una acción (nodo accionista) puede votar, y un nodo común sin acciones no puede votar.

En una implementación, el número total de votos de un nodo accionista no es mayor que el número de acciones de votación que posee el nodo accionista. Las acciones de votación no incluyen acciones para las que votan otros nodos accionistas durante la selección de nodos de consenso. Por lo tanto, en otra implementación del método dado a conocer en la presente memoria descriptiva, el número de veces que la acción es transferida de manera válida entre nodos en una cadena de bloques por medio de votación se ajusta a 1 en un único proceso de selección de nodos de consenso.

En la presente implementación, un nodo accionista puede votar por sí mismo, o puede votar por otro nodo. El nodo accionista no puede transferir votos obtenidos de otros nodos accionistas. En un proceso de votación único para selección de nodos de consenso, cada acción puede ser utilizada por el nodo accionista para votar solamente una vez.

En un ejemplo específico, el nodo 1 tiene 10 acciones, y las 10 acciones son acciones de votación. El nodo 1 vota seis acciones para el nodo 2, y el nodo 3 vota tres acciones para el nodo 1. Aunque el nodo 1 tiene siete acciones en este momento, dado que tres de estas son votadas por otro nodo para el nodo 1 y no son acciones de votación, el nodo 1 tiene cuatro acciones que pueden ser utilizadas para votación de participación accionarial. El nodo 1 puede votar por sí mismo, o puede votar por otro nodo esperado.

En otra implementación de la presente memoria descriptiva, una firma digital se puede poner en un resultado de votación de la votación de participación accionarial del nodo accionista. Así, se puede impedir que otro nodo fuerce el resultado de la votación del nodo accionista. La firma digital se puede utilizar asimismo como datos de verificación del resultado de la votación para impedir que el nodo accionista deniegue el resultado de votación propio. De este modo, se mejora sensiblemente la fiabilidad y seguridad del resultado de la votación de participación accionarial. En una implementación dada a conocer en la presente memoria descriptiva, el resultado de la votación de participación accionarial puede ser generado por un nodo accionista utilizando su clave privada para firmar digitalmente un resultado de la votación de participación accionarial de los nodos esperados.

Correspondientemente, después de obtener un resultado de la votación de participación accionarial, el método incluye además:

S20. Verificar el resultado de la votación de participación accionarial utilizando una correspondiente clave pública del nodo accionista.

La figura 3 es un diagrama de flujo esquemático que muestra otra implementación del método, de acuerdo con la presente memoria descriptiva. En la presente implementación, se puede utilizar una clave privada en cifrado asimétrico para estampar una firma en el resultado de la votación, y se puede difundir a otros nodos una clave pública correspondiente. Por consiguiente, el resultado con la firma firmada utilizando la clave privada puede ser verificado utilizando la clave pública del nodo correspondiente, para confirmar si el resultado de la votación de participación accionarial y un emisor del resultado de la votación de participación accionarial son válidos (legales). Si el resultado de la votación de participación accionarial no es válido, se puede llevar a cabo el envío de una alarma u otra operación de procesamiento predeterminada.

S4. Determinar, en base al resultado de la votación de participación accionarial, el número de acciones que posee cada nodo accionista después de la votación de participación accionarial.

Después de que el nodo accionista vote, el resultado de la votación de participación accionarial del nodo accionista se puede difundir a todos los nodos en la cadena de bloques. De este modo, cada nodo en la cadena de bloques puede recibir el resultado de la votación de participación accionarial del nodo accionista, y los nodos pueden recibir el mismo resultado de la votación de participación accionarial. En la presente implementación, después de que todos los nodos accionistas voten, el resultado de asignación de acciones en los nodos cambia normalmente. Por ejemplo, si un nodo que posee originalmente acciones ha votado en todas las acciones por otro nodo, no habiendo recibido votos de otros nodos, dicho nodo no tiene ahora acciones. Es decir, antes de la votación de participación accionarial, el nodo era un nodo accionista. Pero después de la votación de participación accionarial, el nodo ha pasado a ser un nodo común sin acciones. Si un nodo común sin acciones antes de la votación de participación accionarial, posee una acción después de la votación de participación accionarial, se convierte en un nuevo nodo accionista.

Por lo tanto, después de la votación de participación accionarial, un nodo accionista o un nodo común puede determinar, en base al resultado de la votación de participación accionarial recibido o a un resultado de la votación de participación accionarial propio, el número de acciones que posee cada nodo accionista. En el escenario de implementación de la presente implementación, después de la votación de participación accionarial, la suma de acciones de todos los nodos accionistas permanece sin cambios antes y después de la votación de participación accionarial.

En un ejemplo específico, antes de la votación de participación accionarial, el nodo accionista 10 posee 20 acciones, el nodo accionista 11 posee 25 acciones, el nodo accionista 15 posee 30 acciones, el nodo accionista 8 posee 10 acciones y el nodo accionista 6 posee 15 acciones. Después de la votación de participación accionarial, todos los nodos reciben el mismo resultado de la votación de participación accionarial. Un resultado de la votación de participación accionarial recibido por el nodo accionista 10 puede ser como sigue: el nodo accionista 10 posee 9 acciones, el nodo accionista 11 posee 20 acciones, el nodo accionista 15 posee 35 acciones, el nodo accionista 8 posee 3 acciones, el nodo accionista 6 posee 20 acciones y el nodo accionista 7 posee 13 acciones. Después de la votación de participación accionarial, no sólo han cambiado los números de acciones que poseen los nodos accionistas originales, sino que asimismo aparece un nuevo nodo accionista 7 y posee 13 acciones.

S6. Determinar el resultado de la selección de nodos de consenso en base al número de acciones que posee cada nodo accionista después de la votación de participación accionarial.

Después de que se obtenga al resultado de la votación de participación accionarial, el resultado de la selección de nodos de consenso se puede determinar en base al número de acciones que posee cada nodo accionista actual. El número específico de nodos de consenso seleccionados y un método de selección se pueden ajustar en base un escenario de aplicación real, o a un requisito de procesamiento. Por ejemplo, los cinco nodos accionistas que poseen la mayor parte de las acciones se seleccionan como nodos de consenso.

En otro escenario de implementación del método dado a conocer en la presente memoria descriptiva, puede haber nodos que poseen el mismo número de acciones después de una votación de participación accionarial. Por ejemplo, el nodo 10 y el nodo 11 poseen cada uno 20 acciones. Sin embargo, debido a limitaciones sobre el número de nodos de consenso (por ejemplo, hay que seleccionar cinco nodos de consenso, se han determinado cuatro nodos de consenso, y cada nodo de consenso determinado posee más de 20 acciones), es necesario seleccionar uno del nodo 10 y el nodo 11 como un nodo de consenso. En una implementación dada a conocer en la presente memoria descriptiva, cuando existen nodos que poseen el mismo número de acciones, los nodos de consenso se pueden seleccionar en base a una secuencia temporal de generación de certificados raíz de nodo. En otra implementación, la determinación de un resultado de la selección de nodos de consenso en base al número de acciones que posee cada nodo accionista después de la votación de participación accionarial puede incluir la etapa siguiente.

S601. Si el nodo accionista incluye nodos que poseen el mismo número de acciones después de una votación de participación accionarial, seleccionar un nodo de consenso a partir de los nodos que poseen el mismo número de acciones en base a una secuencia de tiempo de generación de certificados raíz de nodo, donde el certificado raíz de nodo incluye información de datos utilizada para demostrar una identidad de nodo y aplicada a un servidor de certificados específico por un nodo en una cadena de bloques.

Tal como se ha descrito anteriormente, en un método de implementación, antes de que se añada a la cadena de bloques, un nodo de la cadena de bloques tiene que solicitar al servidor de certificados designado un certificado raíz que se utiliza para demostrar que el nodo es válido. Cuanto antes se añada un nodo a la cadena de bloques, antes se genera un certificado raíz del nodo. Generalmente, cuanto antes se añada un nodo a la cadena de bloques, más estables, óptimos y fiables son sus parámetros de ejecución, rendimiento de servidor, política de procesamiento de datos, etc. Por lo tanto, en la presente implementación, cuando existen nodos que poseen el mismo número de acciones, un nodo con un certificado raíz generado anteriormente se puede seleccionar de manera preferente como un nodo de consenso. En un ejemplo específico, cuando los certificados raíz están numerados utilizando información que incluye el tiempo de generación de los certificados raíz, los nodos de consenso se pueden seleccionar en orden ascendente de números de los certificados raíz.

La figura 4 es un diagrama esquemático que muestra un escenario de selección de un nodo de consenso en una red de cadena de bloques, de acuerdo con una implementación de la presente memoria descriptiva. Una o varias implementaciones de la presente memoria descriptiva dan a conocer un método de selección de nodos de consenso. Un nodo accionista puede conducir una votación de participación accionarial, y seleccionar un nodo para participar en el consenso en base al número de acciones que poseen los nodos accionistas en un resultado de la votación. El método es fácil de implementar. El resultado de la selección es real y válido, y el resultado de la votación se da a conocer en toda la red y puede ser aprobado por otros nodos. Basándose en la solución de implementación en la presente memoria descriptiva, un nodo de consenso se puede seleccionar rápidamente en base a la proporción de acciones después de la votación de participación accionarial. De este modo, se reduce el consumo en un proceso de consenso, se simplifican las etapas de proceso de consenso, se mejora la eficiencia de la selección de nodos de consenso y el resultado de la selección es más fiable.

Basándose en el método de selección de nodos de consenso anterior, la presente memoria descriptiva da a conocer además un aparato de selección de nodos de consenso. El aparato puede incluir un aparato que utiliza un sistema

(incluyendo un sistema distribuido), software (aplicación), un módulo, un componente, un servidor, un cliente, un ordenador cuántico, etc., en el método en una o varias implementaciones de la presente memoria descriptiva, e incluye hardware de implementación necesario. Basándose en el mismo concepto inventivo, un aparato dado a conocer en dichas una o varias implementaciones de la presente memoria descriptiva se describe en las siguientes implementaciones. Una solución de implementación del aparato para resolver un problema es similar a la solución de implementación del método. Por lo tanto, para una o varias implementaciones específicas del aparato en la presente memoria descriptiva, se hace referencia a la implementación del método anterior. No se vuelven a describir detalles en este caso. En lo que sigue, el término "unidad" o "módulo" puede implementar una combinación de software y/o hardware de una función predeterminada. Aunque el aparato descrito en las siguientes implementaciones se implementa preferentemente utilizando software, el aparato se puede implementar asimismo utilizando hardware o una combinación de software y hardware.

La figura 5 es un diagrama estructural esquemático que muestra módulos en un aparato de selección de nodos de consenso, de acuerdo con una implementación de la presente memoria descriptiva. Tal como se muestra en la figura 5, el aparato puede incluir: un módulo de adquisición de resultados de la votación 101, configurado para obtener un resultado de la votación de participación accionarial de un nodo accionista para por lo menos un nodo esperado, donde el nodo accionista incluye un nodo que posee por lo menos una de las acciones totales predeterminadas; un módulo de determinación de resultados de la votación 102, configurado para determinar, en base al resultado de la votación de participación accionarial, el número de acciones que posee cada nodo accionista después de la votación de participación accionarial; y un módulo de determinación de nodos de consenso 103, configurado para determinar un resultado de la selección de nodos de consenso en base al número de acciones que posee cada nodo accionista después de la votación de participación accionarial.

El número total de acciones se puede determinar en base al número real de nodos, a un entorno de implementación, etc. Generalmente, el número total de acciones determinado es único y permanece invariable. Las acciones totales se pueden asignar a los nodos correspondientes basándose en una regla de servicio. Una regla de asignación específica se puede determinar en base al tamaño del nodo, al volumen del tráfico, a la importancia, etc.

Cuando un nodo de consenso tiene que ser seleccionado en PBFT, un nodo que posee una acción puede elegir votar por un nodo esperado, y el resultado de la votación se puede difundir a toda la red de cadenas de bloques. Después de la votación, los nodos pueden recibir el mismo resultado de la votación de participación accionarial, y determinar a continuación un resultado de la selección de nodos de consenso en base al número de acciones que posee cada nodo. Basándose en la solución de implementación del aparato en la presente memoria descriptiva, el nodo de consenso se puede seleccionar rápidamente en base a la proporción de acciones después de una votación de participación accionarial. De este modo, se reduce el consumo en un proceso de consenso, se simplifican las etapas de proceso de consenso, se mejora la eficiencia de la selección de nodos de consenso y el resultado de la selección es más fiable.

En otra implementación del aparato dado a conocer en la presente memoria descriptiva, si el nodo accionista incluye nodos que poseen el mismo número de acciones después de una votación de participación accionarial, el módulo de determinación de nodos de consenso 103 selecciona un nodo de consenso a partir de los nodos que poseen el mismo número de acciones, en base a una secuencia de tiempo de generación de certificados raíz de nodo. El certificado raíz de nodo incluye información de datos utilizada para demostrar la identidad del nodo y solicitada por un nodo en una cadena de bloques a un servidor de certificados especificado.

La figura 6 es un diagrama estructural esquemático que muestra módulos en un aparato de selección de nodos de consenso, de acuerdo con otra implementación de la presente memoria descriptiva. Tal como se muestra en la figura 6, en una implementación del aparato dado a conocer por la presente memoria descriptiva, el resultado de la votación de participación accionarial puede incluir: un resultado de la votación de participación accionarial generado después de que el nodo accionista realice una firma en un resultado de la votación generado después de una votación de participación accionarial para el nodo esperado, utilizando una clave privada del nodo accionista.

En consecuencia, el aparato puede incluir además: un módulo de verificación 104, configurado para verificar el resultado de la votación de participación accionarial utilizando una correspondiente clave pública del nodo accionista después de que se obtenga el resultado de la votación de participación accionarial.

En una implementación, un nodo que posee una acción puede elegir independientemente votar a cualquier nodo. La base para seleccionar el nodo esperado puede incluir, de forma no limitativa, la estabilidad de rendimiento del servicio del nodo, la capacidad de servicio del nodo, la política de selección determinada por un operador, etc. En otra implementación del aparato dado a conocer en la presente memoria descriptiva, el nodo esperado seleccionado puede incluir: por lo menos un nodo seleccionado por el nodo accionista en base a una condición de selección de nodos de consenso predeterminada para votar con una acción al mismo.

En una implementación, el número total de votos de un nodo accionista se puede ajustar como no más que el número de acciones de votación que posee el nodo accionista. Las acciones de votación no incluyen acciones con las que otros nodos accionistas votan por el nodo accionista durante la selección de nodos de consenso. Por lo tanto, en otra implementación del aparato, el número de veces que una acción se transfiere de manera válida entre nodos en una cadena de bloques por medio de votación se ajusta a 1 en un proceso único de selección de nodos de consenso.

En esta implementación, en un único proceso de votación para selección de nodos de consenso, cada acción puede ser utilizada por el nodo accionista para votar solamente una vez, y el nodo accionista no puede transferir votos obtenidos de otros nodos accionistas.

El aparato en la implementación anterior se puede implementar en un único nodo, y puede incluir un nodo común o el nodo accionista. Dado que el resultado de la votación se difunde a todos los nodos en la red de cadena de bloques, y todos los nodos reciben el mismo resultado de la votación de participación accionarial, cada nodo puede confirmar el resultado de la selección de nodos de consenso en base al resultado de la votación de participación accionarial.

Importa señalar que las descripciones del aparato anterior en la presente memoria descriptiva pueden incluir además otra implementación basada en descripciones de implementación de métodos relacionados. Las implementaciones en la presente memoria descriptiva se describen todas de manera progresiva. Se puede hacer referencia mutua a partes iguales o similares en las implementaciones. Cada implementación se centra en una diferencia respecto de otras implementaciones. Una implementación de aparato de módulo es similar a una implementación de método, y por lo tanto se describe brevemente. Para partes relacionadas, se hace referencia a descripciones parciales en la implementación de método.

Se ha descrito anteriormente implementaciones específicas de la presente memoria descriptiva. Otras implementaciones caen dentro del alcance de las reivindicaciones adjuntas. En algunas situaciones, las acciones o las etapas registradas en las reivindicaciones se pueden llevar a cabo en un orden diferente al orden de las implementaciones y pueden no obstante conseguir un resultado deseado. Además, el proceso descrito en los dibujos adjuntos no requiere necesariamente el orden o secuencia mostrada para conseguir el resultado deseado. En algunas implementaciones, el procesamiento multitarea y el procesamiento en paralelo son asimismo factibles o posiblemente ventajosos.

La presente memoria descriptiva da a conocer un aparato de selección de nodos de consenso. Un nodo accionista puede conducir una votación de participación accionarial, y seleccionar un nodo para participar en el consenso en base al número de acciones que poseen los nodos accionistas en un resultado de la votación. El método es fácil de implementar. El resultado de la selección es real y válido, y el resultado de la votación se da a conocer a toda la red y puede ser aprobado por otros nodos. Basándose en la solución de implementación en la presente memoria descriptiva, un nodo de consenso se puede seleccionar rápidamente en base a la proporción de acciones después de la votación de participación accionarial. De este modo, se reduce el consumo en un proceso de consenso, se simplifican las etapas de proceso de consenso, se mejora la eficiencia de la selección de nodos de consenso y un resultado de la selección es más fiable.

El método de selección de nodos de consenso dado a conocer en la presente memoria descriptiva puede ser implementado por un procesador que ejecuta una correspondiente instrucción de programa en un ordenador. Por ejemplo, se puede implementar en un extremo de PC utilizando el lenguaje C++ en un sistema operativo Windows, o implementar utilizando un correspondiente lenguaje de diseño de programas en otro sistema tal como Linux, Android, iOS, o implementar basándose en lógica de procesamiento de un ordenador cuántico. En una implementación del aparato para selección de nodos de consenso en la presente memoria descriptiva, el aparato puede incluir un procesador y una memoria configurada para almacenar una instrucción ejecutable por procesador. El procesador ejecuta la instrucción para: obtener un resultado de la votación de participación accionarial de un nodo accionista para por lo menos un nodo esperado, donde el nodo accionista incluye un nodo que posee por lo menos una de las acciones totales predeterminadas; determinar, en base al resultado de la votación de participación accionarial, el número de acciones que posee cada nodo accionista después de la votación de participación accionarial; y determinar un resultado de la selección de nodos de consenso en base al número de acciones que posee cada nodo accionista después de la votación de participación accionarial.

Importa señalar que las descripciones del aparato anterior en la presente memoria descriptiva pueden incluir además otra implementación basada en descripciones de implementaciones de método relacionadas. Las implementaciones en la presente memoria descriptiva se describen todas de manera progresiva. Se puede hacer referencia mutua a partes iguales o similares en las implementaciones. Cada implementación se centra en una diferencia respecto de otras implementaciones. Una implementación de hardware + programa es similar a una implementación de método, y por lo tanto se describe brevemente. Para partes relacionadas, se hace referencia a descripciones parciales en la implementación de método.

El aparato o método anterior se puede utilizar para un servidor de un sistema de servicio de cadenas de bloques, para seleccionar o confirmar un nodo de consenso en una red de cadenas de bloques. Un servidor de procesamiento para selección de nodos de consenso puede seleccionar rápidamente un nodo de consenso en base a una proporción de acciones después de una votación de participación accionarial. De este modo, se reduce el consumo en un proceso de consenso, se simplifican las etapas de proceso de consenso, se mejora la eficiencia de la selección de nodos de consenso y un resultado de la selección es más fiable. El servidor puede incluir un aparato terminal que utiliza un sistema (incluyendo un sistema distribuido), software (aplicación), un módulo, un componente, un servidor, un cliente, un ordenador cuántico, etc. en una o varias implementaciones de método o implementaciones de aparato en la presente memoria descriptiva e incluyendo hardware de implementación necesario.

La figura 7 es un diagrama estructural esquemático que muestra un servidor, de acuerdo con una implementación de la presente memoria descriptiva. El servidor puede incluir por lo menos un procesador y una memoria configurada para almacenar una instrucción ejecutable por procesador. El procesador ejecuta la instrucción para: obtener un resultado de la votación de participación accionarial de un nodo accionista para por lo menos un nodo esperado, donde el nodo accionista incluye un nodo que posee por lo menos una de las acciones totales predeterminadas; determinar, en base al resultado de la votación de participación accionarial, el número de acciones que posee cada nodo accionista después de la votación de participación accionarial; y determinar un resultado de la selección de nodos de consenso en base al número de acciones que posee cada nodo accionista después de la votación de participación accionarial.

Cabe señalar que el servidor o aparato de hardware + programa puede incluir además otra implementación basada en las descripciones de la implementación de método. Para una implementación específica, se puede hacer referencia a las descripciones correspondientes en la implementación de método. No se vuelven a describir detalles en este caso.

En el método y el aparato de selección de nodos de consenso, y en el servidor dados a conocer en una o varias implementaciones de la presente memoria descriptiva, un nodo accionista puede conducir una votación de participación accionarial, y seleccionar un nodo para participar en un consenso en base al número de acciones que poseen los nodos accionistas en un resultado de la votación. El método es fácil de implementar. El resultado de la selección es real y válido, y el resultado de la votación se da a conocer en toda la red y puede ser aprobado por otros nodos. Basándose en la solución de implementación en la presente memoria descriptiva, un nodo de consenso se puede seleccionar rápidamente en base a la proporción de acciones después de la votación de participación accionarial. De este modo, se reduce el consumo en un proceso de consenso, se simplifican las etapas de proceso de consenso, se mejora la eficiencia de la selección de nodos de consenso y un resultado de la selección es más fiable.

Aunque el contenido de la presente memoria descriptiva proporciona descripciones sobre configuración, adquisición, interacción, cálculo, determinación, etc., de datos para la base para seleccionar un nodo esperado mediante un nodo accionista, limitaciones sobre el número de veces que una acción se transfiere con validez durante una votación, utilización de una clave privada para cifrar y una clave pública para descifrar un resultado de la votación, determinación de un nodo de consenso en base al número de acciones que poseen los nodos después de la votación, etc., la presente memoria descriptiva no se limita necesariamente a casos conformes con un estándar de comunicaciones de la industria, almacenamiento de datos de cadenas de bloques estándar y reglas de procesamiento y almacenamiento informático, o a los casos descritos en una o varias implementaciones de la presente memoria descriptiva. Una solución de implementación obtenida después de una leve modificación basada en algunos estándares de la industria, o utilizando un método auto-definido, o basada en una implementación descrita en las implementaciones, puede conseguir asimismo un efecto de implementación que sea igual, equivalente o similar a las implementaciones anteriores, o que se pueda predecir después de la transformación. Una implementación que utilice un método de adquisición, almacenamiento, determinación y procesamiento de datos, obtenido después de dicha modificación o transformación, sigue estando dentro del alcance de una o varias soluciones de implementación óptimas de la presente memoria descriptiva.

En los años 90, la mejora de una tecnología se puede distinguir claramente entre mejora de hardware (por ejemplo, mejora de estructuras de circuito, tales como un diodo, un transistor y un conmutador) y mejora de software (mejora de un procedimiento de método). Sin embargo, con el desarrollo de las tecnologías, la mejora de muchos procedimientos de método se puede considerar como una mejora directa de una estructura de circuitos de hardware. Los diseñadores casi siempre programan un procedimiento de método mejorado para un circuito de hardware, para obtener una correspondiente estructura de circuito de hardware. Por lo tanto, no se puede decir que una mejora de un procedimiento de método no pueda ser implementada utilizando un módulo de entidad de hardware. Por ejemplo, un dispositivo lógico programable (PLD, programmable logic device) (por ejemplo, una matriz de puertas programables in situ (FPGA, field programmable gate array)) es un tipo de circuito integrado. Una función lógica del dispositivo lógico programable se determina mediante programación de componentes ejecutada por un usuario. Los diseñadores realizan programación para "integrar" un sistema digital en un único PLD sin requerir que un fabricante de chips diseñe y fabrique un chip de circuito integrado dedicado. Además, en lugar de fabricar manualmente un chip de circuito integrado, la programación es fundamentalmente implementada mediante software de "compilador lógico", que es similar a un compilador de software utilizado durante el desarrollo del programa. El código original anterior a la compilación se describe asimismo en un lenguaje de programación especificado, que se denomina lenguaje de descripción de hardware (HDL, hardware description language). Hay más de un tipo de HDL, tal como un lenguaje avanzado de expresión booleana (ABEL, Advanced Boolean Expression Language), un lenguaje de descripción de hardware Altera (AHDL, Altera Hardware Description Language), Confluence, un lenguaje de programación de la universidad de Cornwell (CUPL, Cornell University Programming Language), un HDCal, un lenguaje de descripción de hardware Java (JHDL, Java Hardware Description Language), Lava, Lola, MyHDL, PALASM y un lenguaje de descripción de hardware Ruby (RHDL, Ruby Hardware Description Language). Actualmente, el lenguaje de descripción de hardware de circuitos integrados de muy alta velocidad (VHDL, very-high-speed Integrated Circuit Hardware Description Language) y Verilog son los más utilizados. Un experto en la materia debe comprender asimismo que un procedimiento de método necesita solamente ser programado lógicamente, y programado en el circuito integrado utilizando lenguajes de descripción de hardware anteriores, de manera que se puede obtener fácilmente un circuito de hardware que implemente el procedimiento de método lógico.

El controlador se puede implementar de cualquier manera adecuada. Por ejemplo, el controlador puede ser un microprocesador, un procesador, un medio legible por ordenador, una puerta lógica, un conmutador, un circuito integrado de aplicación específica (ASIC, application-specific integrated circuit), un controlador lógico programable, o un microprocesador incorporado que almacena código de programa legible por ordenador (tal como software o software inalterable) que puede ser ejecutado por el microprocesador o el procesador. Ejemplos del controlador incluyen, de forma no limitativa, los siguientes microcontroladores: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20 y Silicone Labs C8051F320. El controlador de memoria se puede implementar asimismo como una parte de la lógica de control de la memoria. Un experto en la materia sabe asimismo que un controlador se puede implementar en un modo de solamente código de programa legible por ordenador, y las etapas en el método se pueden programar lógicamente para permitir que el controlador implemente además funciones iguales en forma de una puerta lógica, un conmutador, un circuito integrado de aplicación específica, un controlador lógico programable, un microcontrolador incorporado, etc. Por lo tanto, el controlador se puede considerar como un componente de hardware, y un aparato incluido en el controlador y configurado para implementar varias funciones se puede considerar asimismo como una estructura en el componente de hardware. Alternativamente, un aparato configurado para implementar varias funciones se puede considerar como un módulo de software para implementar el método y como una estructura en un componente de hardware.

El sistema, el aparato, el módulo o la unidad descritos en las implementaciones anteriores se puede implementar mediante un chip informático o una entidad, o implementar mediante un producto con una función específica. Un dispositivo de implementación típico es un ordenador. El ordenador puede ser, por ejemplo, un ordenador personal, un ordenador portátil, un dispositivo de interacción humano-máquina en un vehículo, un teléfono móvil, un teléfono con cámara, un teléfono inteligente, un asistente digital personal, un reproductor multimedia, un dispositivo de navegación, un dispositivo de correo electrónico, una consola de juegos, un ordenador de tableta, un dispositivo portable o una combinación de cualesquiera de estos dispositivos.

Aunque la presente memoria descriptiva da a conocer las etapas operativas del método en una implementación o un diagrama de flujo, se pueden incluir más o menos etapas operativas en base a medios convencionales o no creativos. La secuencia de etapas enumerada en las implementaciones es tan sólo una de una serie de secuencias de ejecución de etapas, y no representa una secuencia de ejecución única. En la práctica, cuando un aparato o un producto terminal ejecuta etapas, la ejecución se puede llevar a cabo en una secuencia mostrada en una implementación o en un método mostrado en el dibujo adjunto, o llevar a cabo en paralelo (por ejemplo, en un entorno de procesamiento en paralelo, en un entorno de procesamiento de múltiples procesos, e incluso en un entorno de procesamiento de datos distribuido). Los términos "comprende", "incluye" o cualesquiera de sus variantes están destinados a abarcar una inclusión no exclusiva, de tal modo que un proceso, un método, un artículo o un dispositivo que incluye una lista de elementos no solamente incluye dichos elementos, sino que incluye asimismo otros elementos que no se enumeran expresamente, o elementos adicionales inherentes a dicho proceso, método, artículo o dispositivo. Cuando no existen más restricciones, es posible asimismo que exista otro elemento igual o equivalente en el proceso, el método, un producto o un dispositivo que incluye el elemento.

Para facilitar la descripción, el aparato anterior se describe dividiendo las funciones en varios módulos. Ciertamente, cuando se implementa la presente memoria descriptiva, una función de cada módulo se puede implementar en uno o varios elementos de software y/o de hardware, o un módulo que implementa la misma función se puede implementar como una combinación de una serie de submódulos o subunidades. La implementación de aparato descrita es tan sólo un ejemplo. Por ejemplo, la división de unidades es meramente una división de funciones lógicas y puede ser otra división en una implementación real. Por ejemplo, una serie de unidades o componentes se pueden combinar o integrar en otro sistema, o algunas características se pueden ignorar o no realizar. Además, los acoplamientos mutuos o acoplamientos directos o conexiones de comunicación mostradas o explicadas se pueden implementar utilizando algunas interfaces. Los acoplamientos indirectos o conexiones de comunicación entre los aparatos o unidades se pueden implementar de forma electrónica, mecánica u otras.

Un experto en la materia sabe asimismo que un controlador se puede implementar en un modo de solamente código de programa legible por ordenador, y las etapas en el método se pueden programar lógicamente para permitir que el controlador implemente además funciones iguales en forma de una puerta lógica, un conmutador, un circuito integrado de aplicación específica, un controlador lógico programable, un microcontrolador incorporado, etc. Por lo tanto, el controlador se puede considerar como un componente de hardware, y un aparato incluido en el controlador y configurado para implementar varias funciones se puede considerar asimismo como una estructura en el componente de hardware. Alternativamente, un aparato configurado para implementar varias funciones se puede considerar como un módulo de software para implementar el método y como una estructura en un componente de hardware.

La presente invención se describe haciendo referencia a los diagramas de flujo y/o diagramas de bloques del método, el dispositivo (sistema) y el producto de programa informático según las implementaciones de la presente invención. Se debe entender que las instrucciones de programa informático se pueden utilizar para implementar cada proceso y/o cada bloque en los diagramas de flujo y/o en los diagramas de bloques, y una combinación de un proceso y/o de un bloque en los diagramas de flujo y/o los diagramas de bloques. Estas instrucciones de programa informático pueden ser proporcionadas por un ordenador de propósito general, un ordenador dedicado, un procesador incorporado o un procesador de cualquier otro dispositivo programable de procesamiento de datos para generar una máquina, de tal modo que las instrucciones ejecutadas por un ordenador o un procesador de cualquier otro dispositivo programable

de procesamiento de datos generen un aparato para implementar una función específica en uno o varios procedimientos en los diagramas de flujo y/o en uno o varios bloques en los diagramas de bloques.

Estas instrucciones de programa informático se pueden almacenar en una memoria legible por ordenador que puede instruir al ordenador o a cualesquiera otros dispositivos programables de procesamiento de datos para que funcionen de una manera específica, de tal modo que las instrucciones almacenadas en la memoria legible por ordenador pueden generar un artefacto que incluye un aparato de instrucciones. El aparato de instrucciones implementa una función específica en uno o varios procedimientos en los diagramas de flujo y/o en uno o varios bloques en los diagramas de bloques.

Estas instrucciones de programa informático se pueden cargar en un ordenador u otro dispositivo programable de procesamiento de datos, de tal modo que se lleven a cabo una serie de operaciones y etapas en el ordenador u otro dispositivo programable, generándose de ese modo un proceso implementado por ordenador. Por lo tanto, las instrucciones ejecutadas en el ordenador u otro dispositivo programable proporcionan etapas para implementar una función específica en uno o varios procedimientos en los diagramas de flujo y/o en uno o varios bloques en los diagramas de bloques.

En una típica configuración, el dispositivo informático incluye uno o varios procesadores (CPU), una interfaz de entrada/salida, una interfaz de red y una memoria.

La memoria puede incluir una memoria no persistente, una memoria de acceso aleatorio (RAM, random access memory), una memoria no volátil y/o de otra clase, que están en un medio legible por ordenador, por ejemplo, una memoria de sólo lectura (ROM, read-only memory) o una memoria flash (memoria flash). La memoria es un ejemplo de un medio legible por ordenador.

El medio legible por ordenador incluye medios persistentes, no persistentes, móviles e inmóviles que implementan almacenamiento de información utilizando cualquier método o tecnología. La información puede ser una instrucción legible por ordenador, una estructura de datos, un módulo de programa u otros datos. Un ejemplo de un medio de almacenamiento informático incluye, de forma no limitativa, una memoria de cambio de fase (PRAM, phase change memory), una memoria de acceso aleatorio estática (SRAM, static random access memory), una memoria de acceso aleatorio dinámica (DRAM, dynamic random access memory), otro tipo de memoria de acceso aleatorio (RAM), una memoria de sólo lectura (ROM), una memoria de sólo lectura programable borrable eléctricamente (EEPROM, electrically erasable programmable read-only memory), una memoria flash u otra tecnología de memoria, una memoria de sólo lectura de disco compacto (CD-ROM, compact disc read-only memory), un disco versátil digital (DVD, digital versatile disc) u otro almacenamiento óptico, una cinta magnética de casete, un almacenamiento de cinta y de disco u otro dispositivo de almacenamiento magnético o cualquier otro medio no de transmisión que se pueda configurar para almacenar información a la que accede un dispositivo informático. Tal como se define en la presente memoria descriptiva, el medio legible por ordenador no incluye medios transitorios legibles por ordenador (medios transitorios), tales como una señal de datos modulada y una portadora.

Un experto en la materia deberá comprender que las implementaciones de la presente memoria descriptiva se pueden proporcionar como un método, un sistema o un producto de programa informático. Por lo tanto, la presente memoria descriptiva puede utilizar una forma de implementaciones solamente de hardware, implementaciones solamente de software o implementaciones con una combinación de software y hardware. Además, la presente memoria descriptiva puede utilizar una clase de producto de programa informático implementado en uno o varios medios de almacenamiento utilizables por ordenador (incluyendo, de forma no limitativa, una memoria de disco, un CD-ROM, una memoria óptica, etc.) incluyendo código de programa utilizable por ordenador.

La presente memoria descriptiva se puede describir en el contexto general de instrucciones ejecutables por ordenador, ejecutadas por un ordenador, tal como una unidad de programa. Generalmente, el módulo de programa incluye una rutina, un programa, un objeto, un componente, una estructura de datos, etc. para ejecutar una tarea particular o implementar un tipo particular de datos abstractos. La presente memoria descriptiva se puede poner en práctica asimismo en entornos informáticos distribuidos, en los que se ejecutan tareas mediante dispositivos remotos de procesamiento conectados utilizando una red de comunicaciones. En los entornos informáticos distribuidos, los módulos de programa pueden estar ubicados en medios de almacenamiento informático tanto locales como remotos, incluyendo dispositivos de almacenamiento.

Las implementaciones en la presente memoria descriptiva se describen todas de manera progresiva. Se puede hacer referencia mutua a partes iguales o similares en las implementaciones. Cada implementación se centra en una diferencia respecto de otras implementaciones. Una implementación de sistema es similar a una implementación de método, y por lo tanto se describe brevemente; y para las partes relevantes se puede hacer referencia a descripciones parciales de la implementación de método. En las descripciones de la presente memoria descriptiva, los términos de referencia tales como "una implementación", "algunas implementaciones", "ejemplo", "ejemplo específico", y "algunos ejemplos" significan que los aspectos, estructuras, materiales o características específicas descritas haciendo referencia a las implementaciones o ejemplos están incluidas en, por lo menos, una implementación o ejemplo en la presente memoria descriptiva. En la presente memoria descriptiva, los términos anteriores se describen no necesariamente para la misma implementación o ejemplo. Además, los aspectos, estructuras, materiales o características específicas descritas se pueden combinar de manera adecuada en cualesquiera una o varias

implementaciones o ejemplos. Además, un experto en la materia puede combinar diferentes realizaciones o ejemplos descritos en la presente memoria descriptiva, y características de diferentes implementaciones o ejemplos sin contradicción mutua.

Las descripciones anteriores son tan sólo una o varias implementaciones de la presente memoria descriptiva, y no están destinadas a limitar la presente memoria descriptiva. Para un experto en la materia, la presente memoria descriptiva puede tener varios cambios y variaciones.

La figura 8 es un diagrama de flujo que muestra un ejemplo de un método 800 implementado por ordenador, para seleccionar nodos de consenso en una cadena de bloques, de acuerdo con una implementación de la presente invención. Para hacer más clara la presentación, la descripción que sigue describe en general el método 800 en el contexto de otras figuras de esta descripción. Sin embargo, se comprenderá que el método 800 puede ser realizado, por ejemplo, por cualquier sistema, entorno, software y hardware, o una combinación de sistemas, entornos, software y hardware, según convenga. En algunas implementaciones, varias etapas del método 800 pueden discurrir en paralelo, en combinación, en bucles o en cualquier orden.

En 802, un proceso de votación es realizado por una serie de nodos accionistas para generar un resultado de la votación para cada nodo accionista. El proceso de votación incluye la votación de nodos accionistas para una serie de nodos esperados seleccionados. Los nodos esperados y los nodos accionistas pertenecen a un grupo de nodos asociados con una cadena de bloques. Un nodo accionista es un nodo que posee por lo menos una acción. En algunas implementaciones, un nodo asignado con una acción de las acciones totales predeterminadas se puede denominar un nodo accionista. Un nodo al que vota el nodo accionista se puede denominar un nodo esperado. El nodo esperado puede ser un nodo accionista que posee una acción antes de la votación, o puede ser un nodo que no posee ninguna acción antes de la votación. En algunas implementaciones, un nodo accionista puede elegir independientemente a que nodo esperado vota. En algunas implementaciones, la base para seleccionar el nodo esperado puede incluir, de forma no limitativa, la estabilidad del rendimiento de servicio del nodo, la capacidad de servicio del nodo o una política de selección determinada por un operador.

En algunas implementaciones, solamente los nodos accionistas pueden votar, y los nodos comunes que no poseen acciones no pueden votar. Los nodos accionistas pueden votar por sí mismos, o por otros nodos. Sin embargo, los nodos accionistas no pueden transferir acciones que reciben de otro nodo. Es decir, durante cada proceso de votación, una acción puede ser utilizada solamente para votar una vez. Por ejemplo, antes del proceso de votación, el nodo accionista 1 tiene diez acciones, y el nodo 1 vota con seis de las diez acciones al nodo 2, mientras que otro nodo accionista 3 vota con tres acciones al nodo 1. Aunque el nodo uno tiene ahora siete acciones (10-6+3=4), puede utilizar solamente cuatro acciones para votar debido a que las otras tres acciones fueron transferidas desde otro nodo. De 802, el método 800 avanza a 804.

En 804, se verifica un resultado de la votación (por ejemplo, un resultado de la votación de participación accionarial) para cada nodo accionista. En algunas implementaciones, el resultado de la votación para cada nodo accionista puede ser verificado por una firma digital, impidiendo que se falsifique el resultado de la votación e impidiendo que los nodos accionistas denieguen sus resultados de la votación. En algunas implementaciones, un nodo accionista puede firmar digitalmente su resultado de la votación para los nodos esperados utilizando una clave privada asociada con el nodo accionista. En algunas implementaciones, se puede utilizar una clave privada que utilice cifrado asimétrico, para estampar una firma en el resultado de la votación. Una correspondiente clave pública se puede difundir a los nodos en la cadena de bloques.

El resultado de la votación con la firma puede ser verificado por otro nodo en la cadena de bloques utilizando la clave pública difundida. La verificación se puede utilizar para confirmar si el resultado de la votación y un emisor del resultado de la votación son válidos (legales). Si el resultado de la votación de participación accionarial no es válido, se puede llevar a cabo el envío de una alarma u otra operación de procesamiento predeterminada. De 804, el método 800 avanza a 806.

En 806, se determina en base al resultado de la votación el número de acciones que posee cada nodo (es decir, la participación accionarial) del grupo de nodos después del proceso de votación. En algunas implementaciones, después de que el nodo accionista vote, el resultado de la votación del nodo accionista se puede difundir a todos los nodos en la cadena de bloques. Así, cada nodo en la cadena de bloques puede recibir el resultado de la votación del nodo accionista.

En algunas implementaciones, después del proceso de votación, un nodo accionista o un nodo común puede determinar, en base al resultado de la votación difundido recibido, o en base al resultado de la votación de su propio nodo, el número de acciones que posee cada nodo accionista. Después del proceso de votación, ha cambiado el número de acciones que posee no sólo el nodo accionista original, sino asimismo un nuevo nodo accionista. De 806, el método 800 avanza a 808.

En 808, se seleccionan una serie de nodos de consenso de entre los nodos accionistas en base al número de acciones que posee cada uno de los nodos accionistas. Los nodos accionistas son nodos que poseen por lo menos una acción después del proceso de votación. En algunas implementaciones, cuando el número de nodos en una cadena de bloques supera un determinado umbral, los nodos que participan en el consenso pueden reducir la eficiencia del

consenso. Por lo tanto, es necesario seleccionar algunos nodos a partir de los nodos en la cadena de bloques como nodos de consenso, utilizando un método, para que participen en el consenso. Por ejemplo, en el algoritmo de consenso PBFT, normalmente, para equilibrar la tolerancia a fallos bizantinos y el rendimiento del consenso, es necesario que se seleccionen algunos nodos como nodos de consenso a partir de un gran número de nodos, para participar en el consenso. El consenso indica normalmente que los nodos distribuidos en una cadena de bloques pueden utilizar el mismo algoritmo y el mismo formato de datos (o el mismo protocolo de procesamiento) para generar y actualizar datos, y este proceso se puede implementar utilizando diferentes lenguajes.

En la presente implementación, después de que todos los nodos accionistas voten, el resultado de la asignación de acciones en los nodos cambia normalmente. Por ejemplo, si un nodo que posee originalmente acciones ha votado con todas las acciones por otro nodo, no habiendo recibido votos de otros nodos, dicho nodo no tiene ahora acciones. Es decir, antes de la votación de participación accionarial, el nodo era un nodo accionista. Pero después de la votación de participación accionarial, el nodo ha pasado a ser un nodo común sin acciones. Si un nodo común sin acciones antes de la votación posee una acción después de una votación de participación accionarial, se convierte en un nuevo nodo accionista.

Después de que se obtenga al resultado de la votación de participación accionarial, el resultado de la selección de nodos de consenso se puede determinar en base al número de acciones que posee cada nodo accionista actual. El número específico de nodos de consenso seleccionados y un método de selección se pueden ajustar en base a un escenario de aplicación real, o a un requisito de procesamiento. Por ejemplo, los cinco nodos accionistas que poseen la mayor parte de las acciones se seleccionan como nodos de consenso.

En algunas implementaciones, antes de ser añadido a la cadena de bloques, un nodo en la cadena de bloques (tanto nodos accionistas como comunes) tiene que solicitar a un servidor de certificados designado un certificado raíz que se utiliza para demostrar que el nodo es válido. Cuanto antes se añada un nodo a la cadena de bloques, antes se genera un certificado raíz del nodo.

En algunas implementaciones, si los nodos accionistas incluyen nodos que poseen el mismo número de acciones después del proceso de votación y existe una limitación sobre el número de nodos de consenso, la selección de nodos de consenso a partir de los nodos accionistas que poseen el mismo número de acciones se puede basar en la secuencia temporal de generación de certificados raíz de nodo. Cuanto antes se añade un nodo a la cadena de bloques más estables, óptimos y fiables se consideran los parámetros de ejecución del nodo, el rendimiento del servidor o la política de procesamiento de datos. Por lo tanto, en la presente implementación, cuando existen nodos que muestran el mismo número de acciones, un nodo con un certificado raíz generado anteriormente se puede seleccionar preferentemente como un nodo de consenso. En un ejemplo específico, cuando los certificados raíz están numerados utilizando información que incluye el tiempo de generación de los certificados raíz, los nodos de consenso se pueden seleccionar en orden ascendente de números de los certificados raíz. Después de 808, el método 800 se detiene.

Las implementaciones de la presente solicitud pueden resolver problemas técnicos en selección de nodos de consenso de cadenas de bloques. La tecnología de cadenas de bloques es generalmente una tecnología de bases de datos distribuida descentralizada, con características tales como descentralización, transparencia, resistencia a manipulaciones, y confianza. Se puede utilizar para registrar información de datos en una red entre pares pública o privada. Para garantizar la consistencia de los datos de una cadena de bloques, los datos son generados y actualizados en la cadena de bloques utilizando un algoritmo de consenso. El algoritmo PBFT es un algoritmo de consenso de consistencia distribuido utilizado normalmente en la industria. En PBFT, los algoritmos convencionales para selección de nodos de consenso incluyen principalmente selección aleatoria y selección fija. Sin embargo, en enfoques convencionales, es difícil diseñar un algoritmo para hacer que todos los nodos aprueben un nodo de consenso recién seleccionado después de un proceso complicado de selección de nodos de consenso. Además, aunque la selección fija de nodos de consenso es más simple que una selección aleatoria en términos de implementación, el método se complica cuando se produce un fallo o cuando un nodo de consenso es actualizado por alguna razón. Lo que se necesita es una técnica para soslayar estos problemas en los métodos convencionales, y proporcionar una solución de selección de nodos de consenso PBFT que sea fácil de implementar y mantener, muy eficiente, y fiable.

Las implementaciones de la presente solicitud describen métodos y aparatos para mejorar la selección de nodos de consenso en una cadena de bloques. Durante el proceso de selección de nodos de consenso, los nodos accionistas pueden votar a nodos esperados para generar resultados de la votación. Los resultados de la votación pueden ser verificados por los nodos accionistas firmando digitalmente los resultados utilizando una clave privada, y la correspondiente clave pública se puede difundir a todos los nodos en la cadena de bloques. De este modo, todos los nodos pueden recibir los resultados de la votación y aprobar el resultado simultáneamente, lo que tiene como resultado una manera más simple y rápida de que los nodos dentro de la cadena de bloques aprueben a un nodo de consenso recién seleccionado. Además, debido a una firma digital firmada, los resultados de la votación no pueden ser falsificados o denegados por nodos accionistas, mejorando la seguridad de los datos. Los nodos de consenso se pueden seleccionar en base al número de acciones que posee cada nodo, y cuando existen nodos que tienen el mismo número de acciones, la selección se puede basar en una secuencia de tiempo. Generalmente, cuanto antes se añade un nodo a la cadena de bloques, esto indica que más estables, óptimos y fiables son los parámetros de ejecución de un nodo, el rendimiento del servidor o la política de procesamiento de datos. Por lo tanto, seleccionar nodos de

consenso situados en una secuencia de tiempo anterior dentro de la cadena de bloques puede tener como resultado nodos más estables y fiables participando en los procesos de adopción de decisiones de cadenas de bloques.

El método es asimismo fácil de implementar. El resultado de la votación se da a conocer a toda la red y puede ser aprobado por otros nodos. Basándose en la solución descrita, un nodo de consenso se puede seleccionar rápidamente en base a la proporción de acciones después de la votación. De este modo se reduce el consumo en un proceso de consenso, se simplifican las etapas de proceso de consenso, se mejora la eficiencia de la selección de nodos de consenso y es más fiable un resultado de la selección.

Las realizaciones y operaciones descritas en esta memoria descriptiva se pueden implementar en circuitos de electrónica digital, o en software informático, software inalterable o hardware, incluyendo las estructuras dadas a conocer en esta memoria descriptiva o en combinaciones de una o varias de las mismas. Las operaciones se pueden implementar como operaciones llevadas a cabo por un aparato de procesamiento de datos sobre datos almacenados en uno o varios dispositivos de almacenamiento legibles por ordenador o recibidos desde otras fuentes. Un aparato de procesamiento de datos, ordenador o dispositivo informático puede abarcar aparatos, dispositivos y máquinas para procesar datos, incluyendo a modo de ejemplo un procesador programable, un ordenador, un sistema en chip, o múltiples de los mismos, o combinaciones de los anteriores. El aparato puede incluir circuitos lógicos de propósito especial, por ejemplo, una unidad central de procesamiento (CPU), una matriz de puertas programables in situ (FPGA) o un circuito integrado de aplicación específica (ASIC). El aparato puede incluir asimismo código que crea un entorno de ejecución para el programa informático en cuestión, por ejemplo, código que constituye software inalterable de procesador, una pila de protocolos, un sistema de gestión de bases de datos, un sistema operativo (por ejemplo, un sistema operativo o una combinación de sistemas operativos), un entorno de tiempo de ejecución multiplataforma, una máquina virtual o una combinación de uno o varios de los anteriores. El aparato y el entorno de ejecución pueden realizar varias infraestructuras de modelos informáticos diferentes, tales como infraestructuras de servicios web, computación distribuida y computación en malla.

Un programa informático (conocido asimismo, por ejemplo, como un programa, software, aplicación de software, módulo de software, unidad de software, guión o código) se puede escribir en cualquier clase de lenguaje de programación, incluyendo lenguajes compilados o interpretados, lenguajes declarativos o procedimentales, y se puede desplegar en cualquier forma, incluyendo como un programa independiente o como un módulo, componente, subrutina, objeto u otra unidad adecuada para utilizar en un entorno de programación. Un programa se puede almacenar en una parte de un archivo que contiene otros programas o datos (por ejemplo, uno o varios guiones almacenados en un documento de lenguaje de marcado), en un único archivo dedicado al programa en cuestión, o en múltiples archivos coordinados (por ejemplo, archivos que almacenan uno o varios módulos, subprogramas, o partes de código). Un programa informático se puede ejecutar en un ordenador o en múltiples ordenadores que están situados en un sitio o distribuidos a través de múltiples sitios e interconectados por una red de comunicación.

Los procesadores para la ejecución de un programa informático incluyen, a modo de ejemplo, procesadores tanto de propósito general como de propósito especial, y cualesquiera uno o varios procesadores de cualquier clase de ordenador digital. Generalmente, un procesador recibirá instrucciones y datos de una memoria de sólo lectura o una memoria de acceso aleatorio, o ambas. Los elementos esenciales del ordenador son un procesador para llevar a cabo acciones de acuerdo con instrucciones, y uno o varios dispositivos de memoria para almacenar instrucciones y datos. Generalmente, un ordenador incluirá asimismo, o estará acoplado operativamente para recibir datos desde, o transferir datos hacia, o ambas cosas, uno o varios dispositivos de almacenamiento masivo para almacenar datos. Un ordenador puede estar incorporado en otro dispositivo, por ejemplo, un dispositivo móvil, un asistente digital personal (PDA, personal digital assistant), una consola de juegos, un receptor del sistema de posicionamiento global (GPS, Global Positioning System) o un dispositivo de almacenamiento portátil. Los dispositivos adecuados para almacenar instrucciones de programa informático y datos incluyen memoria no volátil, dispositivos multimedia y de memoria, incluyendo, a modo de ejemplo, dispositivos de memoria de semiconductor, discos magnéticos y discos magnetoópticos. El procesador y la memoria pueden complementarse mediante, o incorporarse en circuitos lógicos de propósito especial.

Los dispositivos móviles pueden incluir microteléfonos, un equipo de usuario (UE, user equipment), teléfonos móviles (por ejemplo, teléfonos inteligentes), tabletas, dispositivos integrables (por ejemplo, relojes inteligentes y gafas inteligentes), dispositivos implantados dentro del cuerpo humano (por ejemplo, biosensores, implantes de cóclea) u otros tipos de dispositivos móviles. Los dispositivos móviles pueden comunicar de forma inalámbrica (por ejemplo, utilizando señales de radiofrecuencia (RF)) con varias redes de comunicación (descritas a continuación). Los dispositivos móviles pueden incluir sensores para determinar características del entorno actual del dispositivo móvil. Los sensores pueden incluir cámaras, micrófonos, sensores de proximidad, sensores GPS, sensores de movimiento, acelerómetros, sensores de luz ambiental, sensores de humedad, giróscopos, brújulas, barómetros, sensores de huella digital, sensores de reconocimiento facial, sensores de RF (por ejemplo, radios WiFi y celulares), sensores térmicos u otros tipos de sensores. Por ejemplo, las cámaras pueden incluir una cámara frontal o una cámara posterior con lentes desplazables o fijas, un flash, un sensor de imagen y un procesador de imágenes. La cámara puede ser una cámara de megapíxeles que puede capturar detalles para reconocimiento facial y/o del iris. La cámara junto con un procesador de datos e información de autenticación almacenada en la memoria o accedida remotamente, puede formar un sistema de reconocimiento facial. El sistema de reconocimiento facial o uno o varios sensores, por ejemplo,

micrófonos, sensores de movimiento, acelerómetros, sensores GPS o sensores de RF, se puede utilizar para autenticación de usuarios.

Para proporcionar interacción con un usuario, se pueden implementar realizaciones en un ordenador que tenga un dispositivo de visualización y un dispositivo de entrada, por ejemplo, una pantalla de cristal líquido (LCD, liquid crystal display) o una pantalla de diodo orgánico emisor de luz (OLED, organic light-emitting diode)/realidad virtual (VR, virtual-reality)/realidad aumentada (AR, augmented-reality) para mostrar información al usuario y una pantalla táctil, un teclado y un dispositivo de puntero mediante los que el usuario puede proporcionar entradas al ordenador. Se pueden utilizar también otras clases de dispositivos para proporcionar interacción con un usuario; por ejemplo, la retroalimentación proporcionada al usuario puede ser cualquier clase de retroalimentación sensorial, por ejemplo por retroalimentación visual, retroalimentación auditiva o retroalimentación táctil; y una entrada del usuario se puede recibir en cualquier forma, incluyendo una entrada acústica, de voz o táctil. Además, un ordenador puede interaccionar con un usuario enviando documentos, y recibiendo documentos de un dispositivo utilizado por el usuario; por ejemplo, enviando páginas web a un navegador web en un dispositivo cliente de un usuario, en respuesta a solicitudes recibidas desde el navegador web.

Las realizaciones se pueden implementar utilizando dispositivos informáticos interconectados mediante cualquier clase o medio cableado o inalámbrico de comunicación de datos digitales (o una combinación de los mismos), por ejemplo, una red de comunicación. Ejemplos de dispositivos interconectados son un cliente y un servidor, generalmente remotos entre sí, que interactúan habitualmente por medio de una red de comunicación. Un cliente, por ejemplo, un dispositivo móvil, puede llevar a cabo otras acciones por sí mismo, con un servidor o a través de un servidor, por ejemplo, realizando transacciones de compra, venta, pago, donación, envío o préstamo, o autorizándolas. Dichas transacciones pueden ser en tiempo real, de tal modo que una acción y una respuesta sean próximas temporalmente; por ejemplo, un individuo percibe que la acción y la respuesta se producen de manera sustancialmente simultánea, la diferencia de tiempo para una respuesta que sigue a la acción del individuo es menor de 1 milisegundo (ms) o menor que 1 segundo (s), o la respuesta es sin retardo intencionado teniendo en cuenta las limitaciones de procesamiento del sistema.

Ejemplos de redes de comunicación incluyen una red de área local (LAN, local area network), una red de acceso radio (RAN, radio access network), una red de área metropolitana (MAN, metropolitan area network) y una red extensa (WAN, wide area network). La red de comunicación puede incluir la totalidad o parte de internet, otra red de comunicación o una combinación de redes de comunicación. La información se puede transmitir sobre la red de comunicación según diversos protocolos y estándares, incluyendo evolución a largo plazo (LTE, Long Term Evolution), 5G IEEE 802, protocolo de internet (IP, Internet Protocol) u otros protocolos o combinaciones de protocolos. La red de comunicación puede transmitir datos de voz, video, biométricos o de autenticación, u otra información entre los dispositivos informáticos conectados.

Las características descritas como implementaciones independientes se pueden implementar, en combinación, en una única implementación, mientras que las características descritas como una única implementación se pueden implementar en múltiples implementaciones, por separado o en cualquier combinación secundaria adecuada. No se deberá entender que las operaciones descritas y reivindicadas en un orden particular requieren que dicho orden particular, ni las operaciones mostradas, se tengan que producir (algunas operaciones pueden ser opcionales). Según convenga, se puede llevar a cabo procesamiento multitarea o en paralelo (o una combinación de procesamiento multitarea y en paralelo).

REIVINDICACIONES

1. Un método para seleccionar un nodo de consenso a partir de múltiples nodos en una cadena de bloques, comprendiendo el método:

obtener un resultado de la votación de participación accionarial de un nodo accionista para por lo menos un nodo esperado, donde el nodo accionista comprende un nodo que posee por lo menos una de las acciones totales predeterminadas y donde un nodo esperado comprende un nodo por el que vota el nodo accionista (S2);

determinar, en base al resultado de la votación de participación accionarial, un número de acciones que posee cada nodo accionista después de la votación de participación accionarial (S4); y

determinar un resultado de la selección de nodos de consenso en base al número de acciones que posee cada nodo accionista después de la votación de participación accionarial (S6), estando el método caracterizado por que comprende, además, si el nodo accionista comprende múltiples nodos que poseen el mismo número de acciones después de una votación de participación accionarial:

seleccionar un nodo de consenso a partir de los múltiples nodos que poseen el mismo número de acciones en base a una secuencia de tiempo de los certificados raíz generados para los múltiples nodos que poseen el mismo número de acciones después de una votación de participación accionarial, donde un certificado raíz para un nodo comprende:

información de datos utilizada para demostrar que el nodo es válido, e

información que representa el tiempo en el que se generó el certificado raíz.

2. El método según la reivindicación 1, en el que el certificado raíz para un nodo se genera en respuesta a que un nodo solicite un certificado raíz a un servidor de certificados específico.

3. El método según cualquiera de las reivindicaciones 1 a 2, en el que el resultado de la votación de participación accionarial comprende:

un resultado de la votación de participación accionarial generado después de que el nodo accionista estampa, utilizando una clave privada de nodo accionista, una firma en un resultado de la votación generado después de una votación de participación accionarial para el nodo esperado; y

correspondientemente, después de obtener un resultado de la votación de participación accionarial, el método comprende además:

verificar el resultado de la votación de participación accionarial utilizando una correspondiente clave pública del nodo accionista (S20).

4. El método según cualquiera de las reivindicaciones 1 a 3, en el que el nodo esperado seleccionado comprende:

por lo menos un nodo seleccionado por el nodo accionista en base a una condición de selección de nodos de consenso predeterminada para votar con una acción al mismo

5. Método según la reivindicación 4, en el que la condición de selección de nodos de consenso predeterminada comprende por lo menos una de una estabilidad del rendimiento de servicio del nodo, una capacidad de servicio del nodo y una política de selección.

6. El método según cualquiera de las reivindicaciones 1 a 5, en el que:

el número de veces que la acción es transferida de forma válida entre nodos en una cadena de bloques por medio de votación se ajusta a 1 en un único proceso de selección de nodos de consenso.

7. El método según la reivindicación 1, en el que seleccionar un nodo de consenso a partir de los múltiples nodos que poseen el mismo número de acciones, en base a una secuencia de tiempo de los certificados raíz generados para los múltiples nodos que poseen el mismo número de acciones después de la votación de participación accionarial comprende: seleccionar el nodo con el certificado raíz generado primero en el tiempo, como el nodo de consenso.

8. Un aparato de selección de un nodo de consenso, comprendiendo el aparato una serie de módulos configurados para realizar el método según cualquiera de las reivindicaciones 1 a 7.

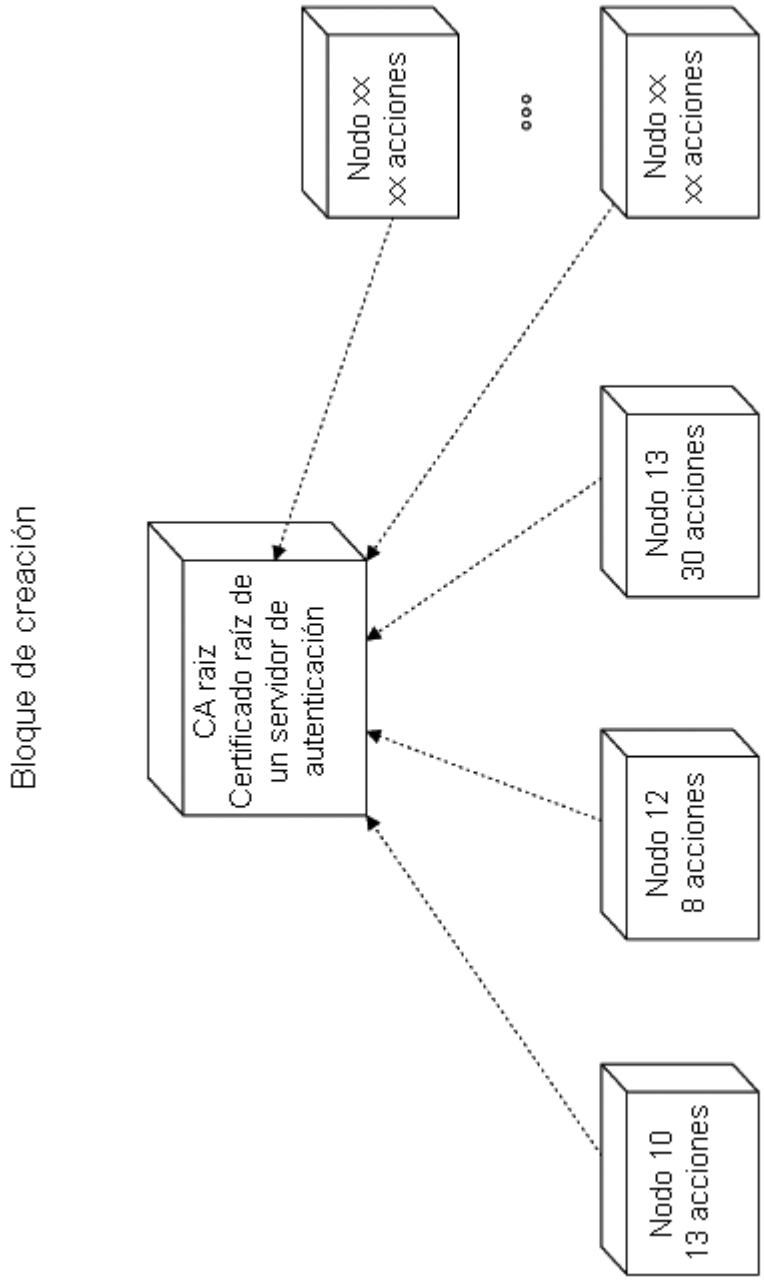
Bloque de creación
CA raiz
Certificado raíz de un servidor de autenticación
Nodo 10
13 acciones
Nodo 12
8 acciones
Nodo 13
30 acciones
Nodo xx
xx acciones
Nodo xx
xx acciones

FIG. 1

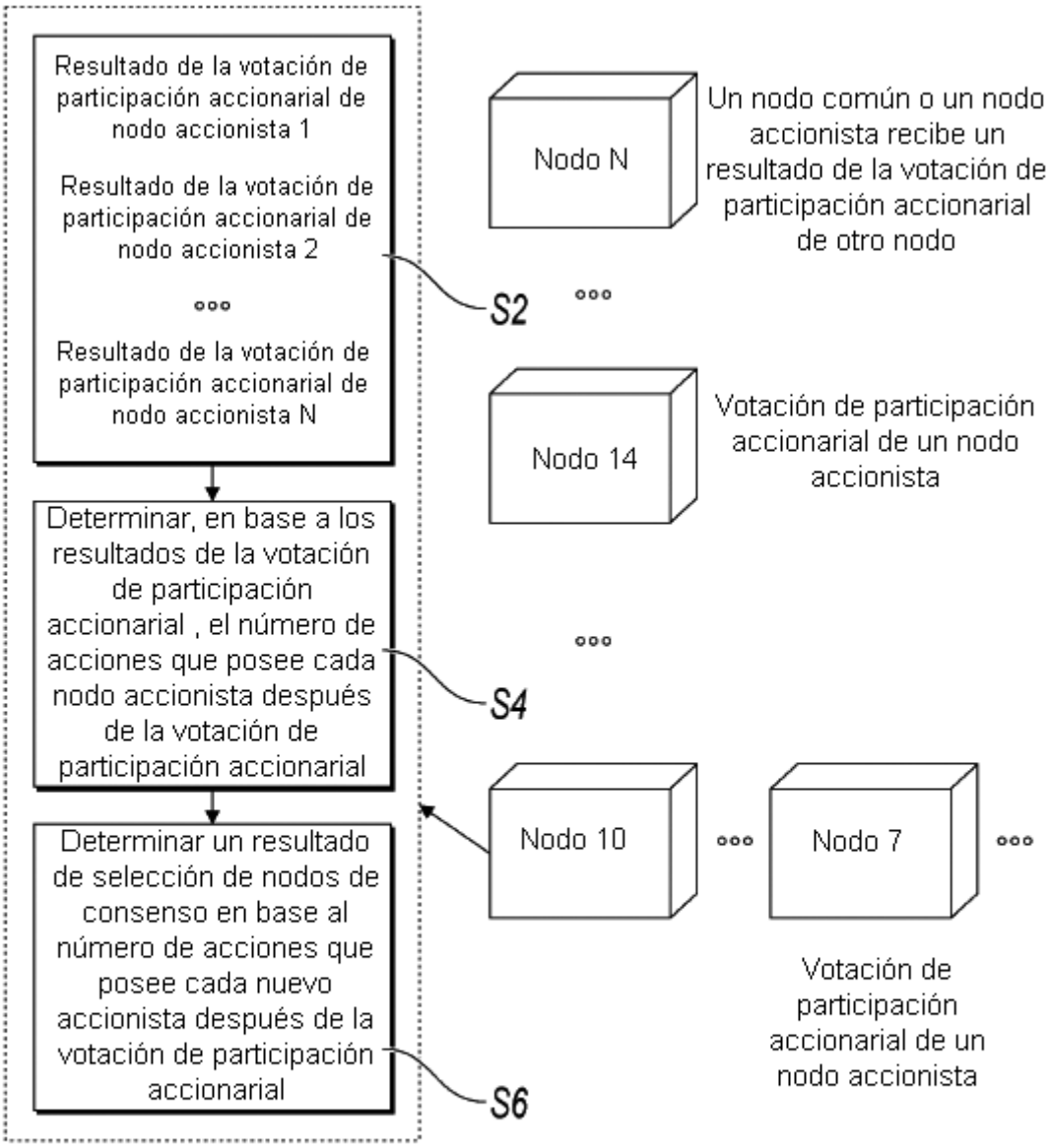
Resultado de la votación de participación accionarial de nodo accionista 1
Resultado de la votación de participación accionarial de nodo accionista 2
...
Resultado de la votación de participación accionarial de nodo accionista N
S2
Determinar, en base a los resultados de la votación de participación accionarial , el número de acciones que posee cada nodo accionista después de la votación de participación accionarial
S4
Determinar un resultado de selección de nodos de consenso en base al número de acciones que posee cada nuevo accionista después de la votación de participación accionarial
S6
Nodo N
Un nodo común o un nodo accionista recibe un resultado de la votación de participación accionarial de otro nodo
...
Nodo 14
Votación de participación accionarial de un nodo accionista
...
Nodo 10
...
Nodo 7
...
Votación de participación accionarial de un nodo accionista

FIG. 2

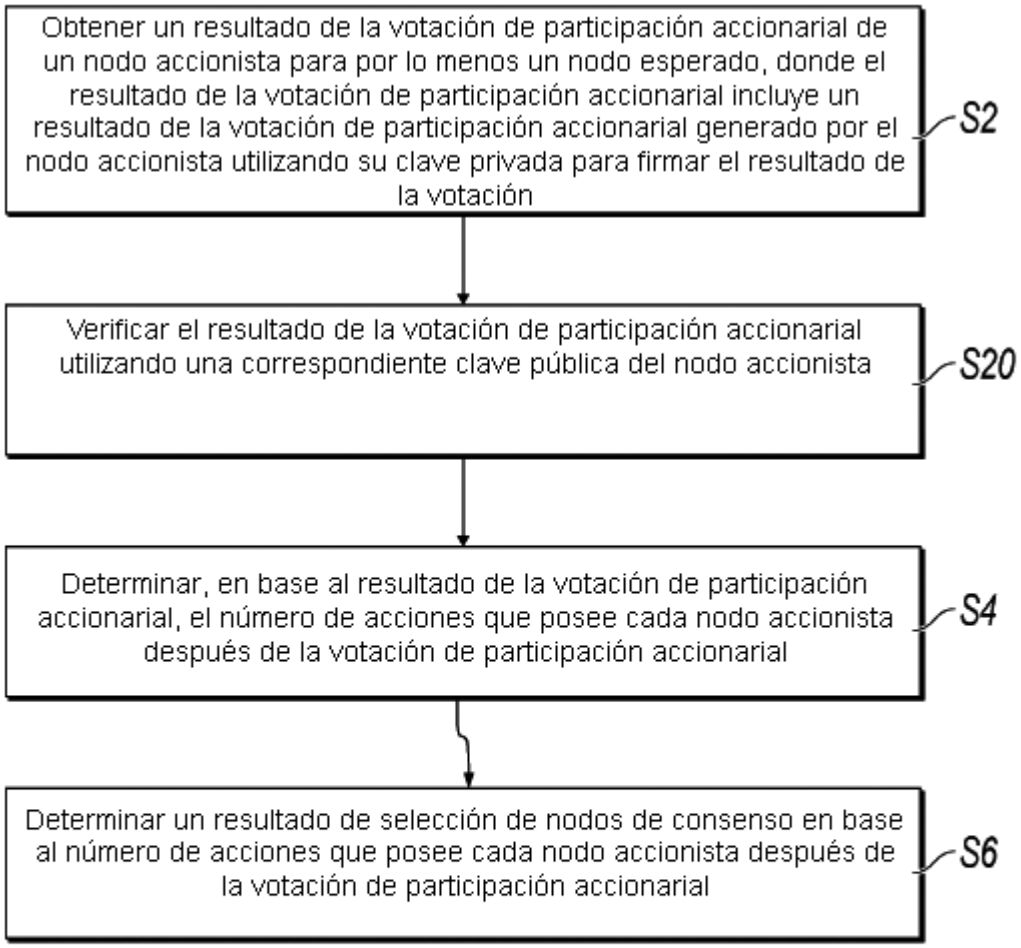
Obtener un resultado de la votación de participación accionarial de un nodo accionista para por lo menos un nodo esperado, donde el resultado de la votación de participación accionarial incluye un resultado de la votación de participación accionarial generado por el nodo accionista utilizando su clave privada para firmar el resultado de la votación
S2
Verificar el resultado de la votación de participación accionarial utilizando una correspondiente clave pública del nodo accionista
S20
Determinar, en base al resultado de la votación de participación accionarial, el número de acciones que posee cada nodo accionista después de la votación de participación accionarial
S4
Determinar un resultado de selección de nodos de consenso en base al número de acciones que posee cada nodo accionista después de la votación de participación accionarial
S6

FIG. 3

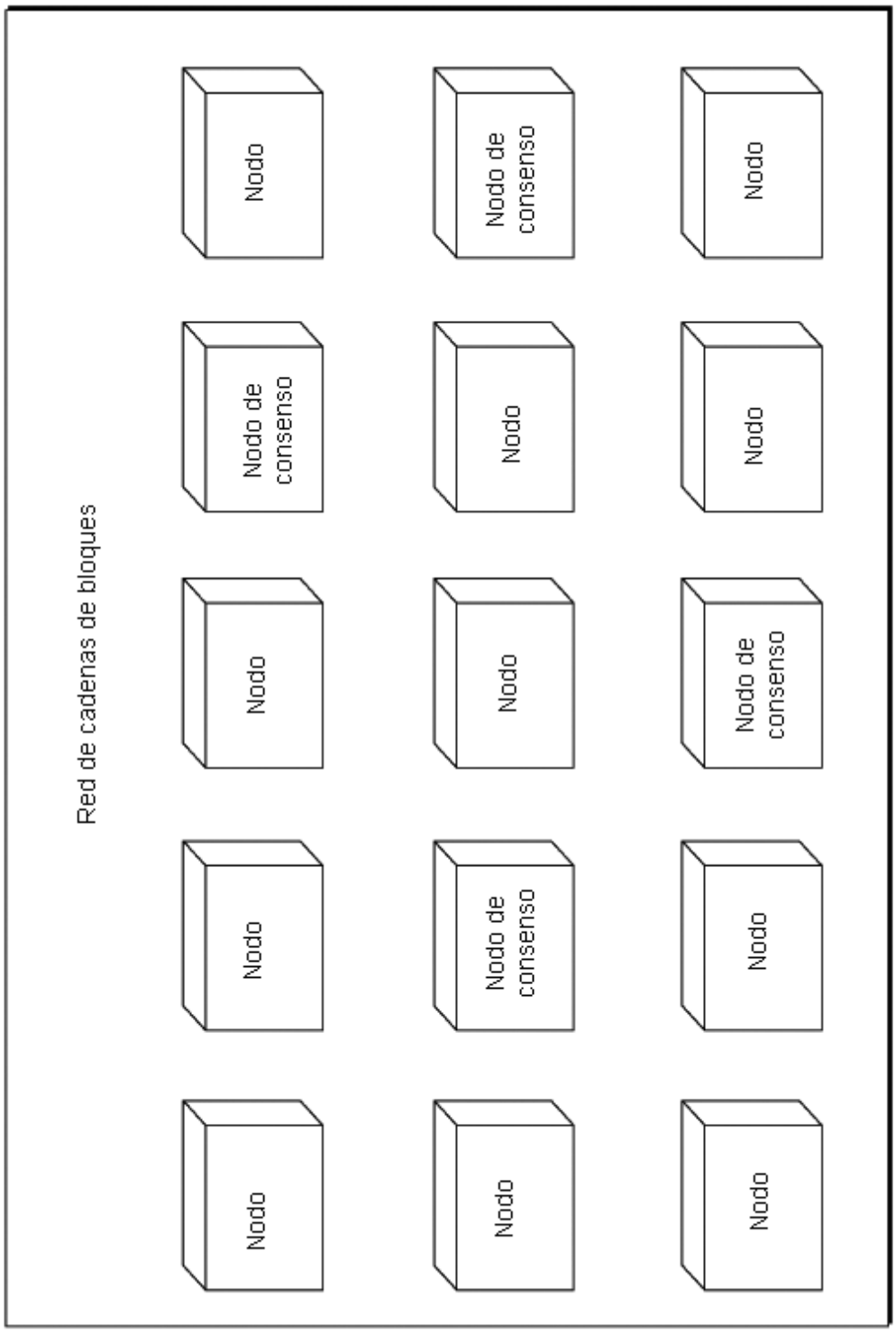
Red de cadenas de bloques
Nodo
Nodo de consenso
Nodo
Nodo de consenso
Nodo
Nodo
Nodo de consenso
Nodo
Nodo de consenso
Nodo
Nodo
Nodo de consenso
Nodo
Nodo de consenso
Nodo

FIG. 4

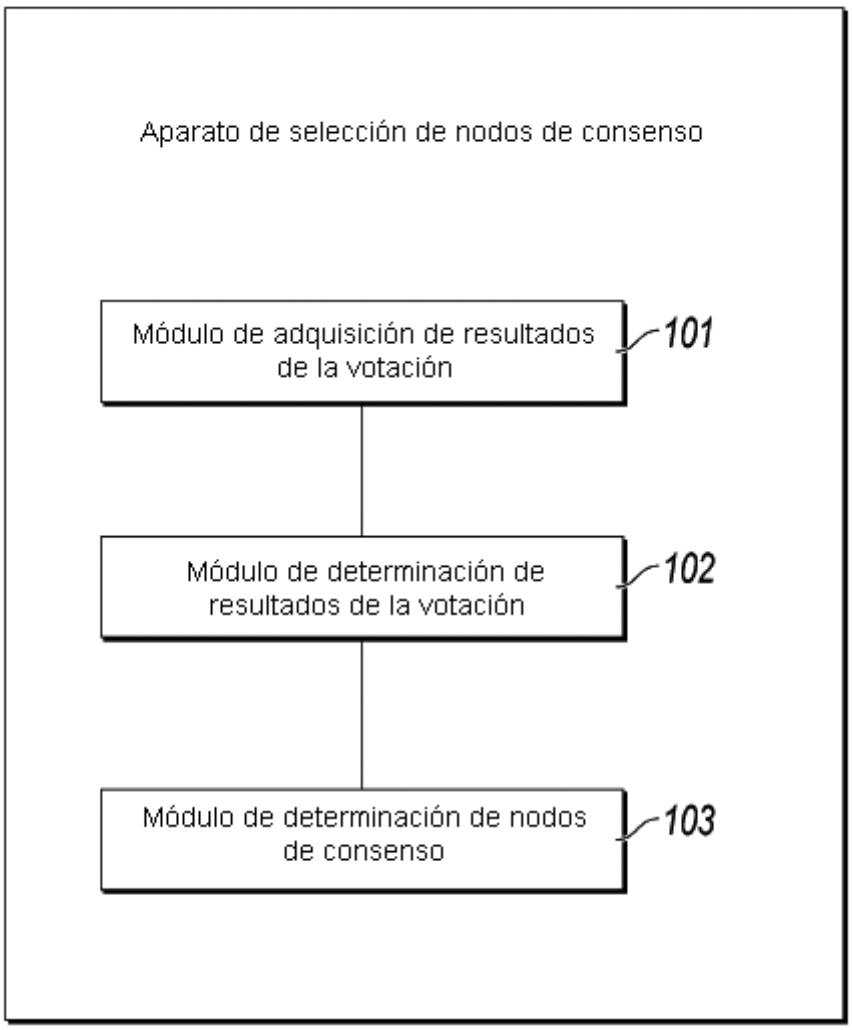
Aparato de selección de nodos de consenso
Módulo de adquisición de resultados de la votación
101
Módulo de determinación de resultados de la votación
102
Módulo de determinación de nodos de consenso
103

FIG. 5

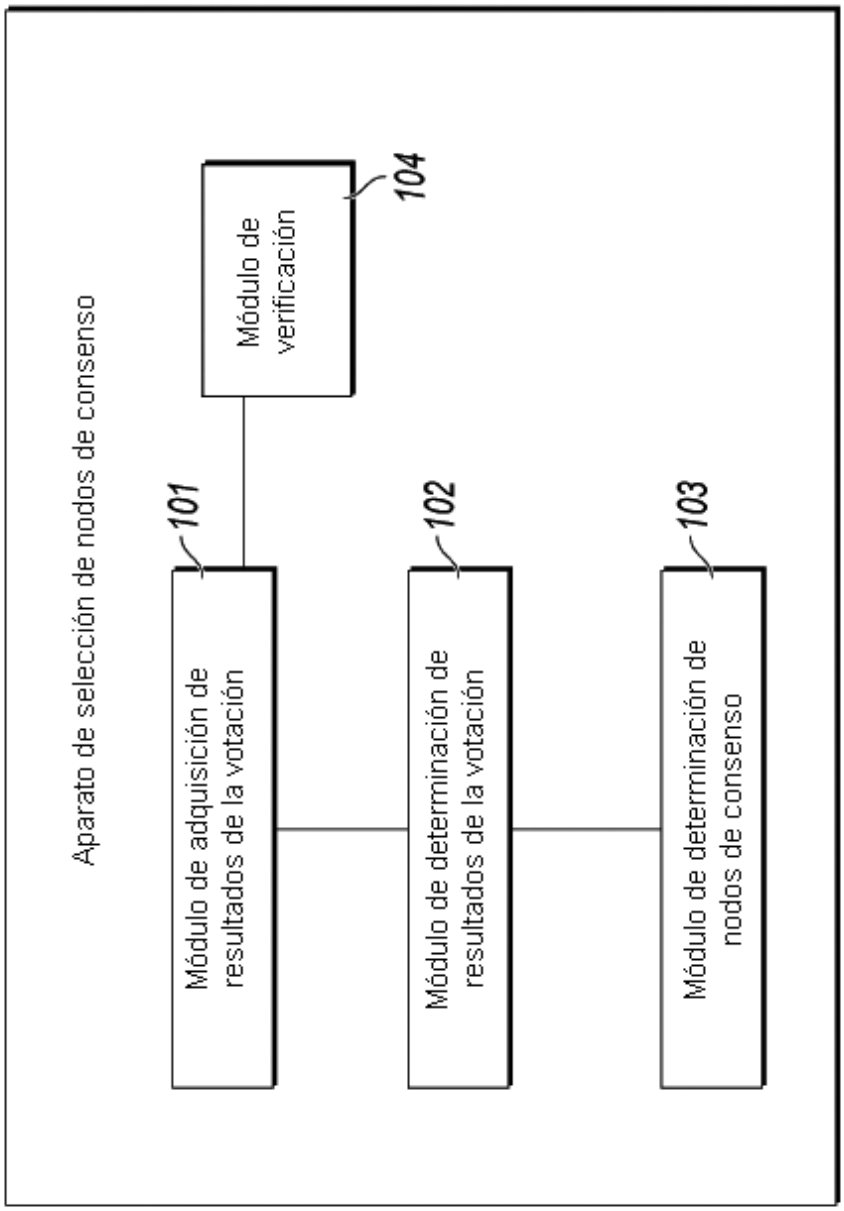
Aparato de selección de nodos de consenso
Módulo de verificación
104
101
102
103
Módulo de adquisición de resultados de la votación
Módulo de determinación de resultados de la votación
Módulo de determinación de nodos de consenso

FIG. 6

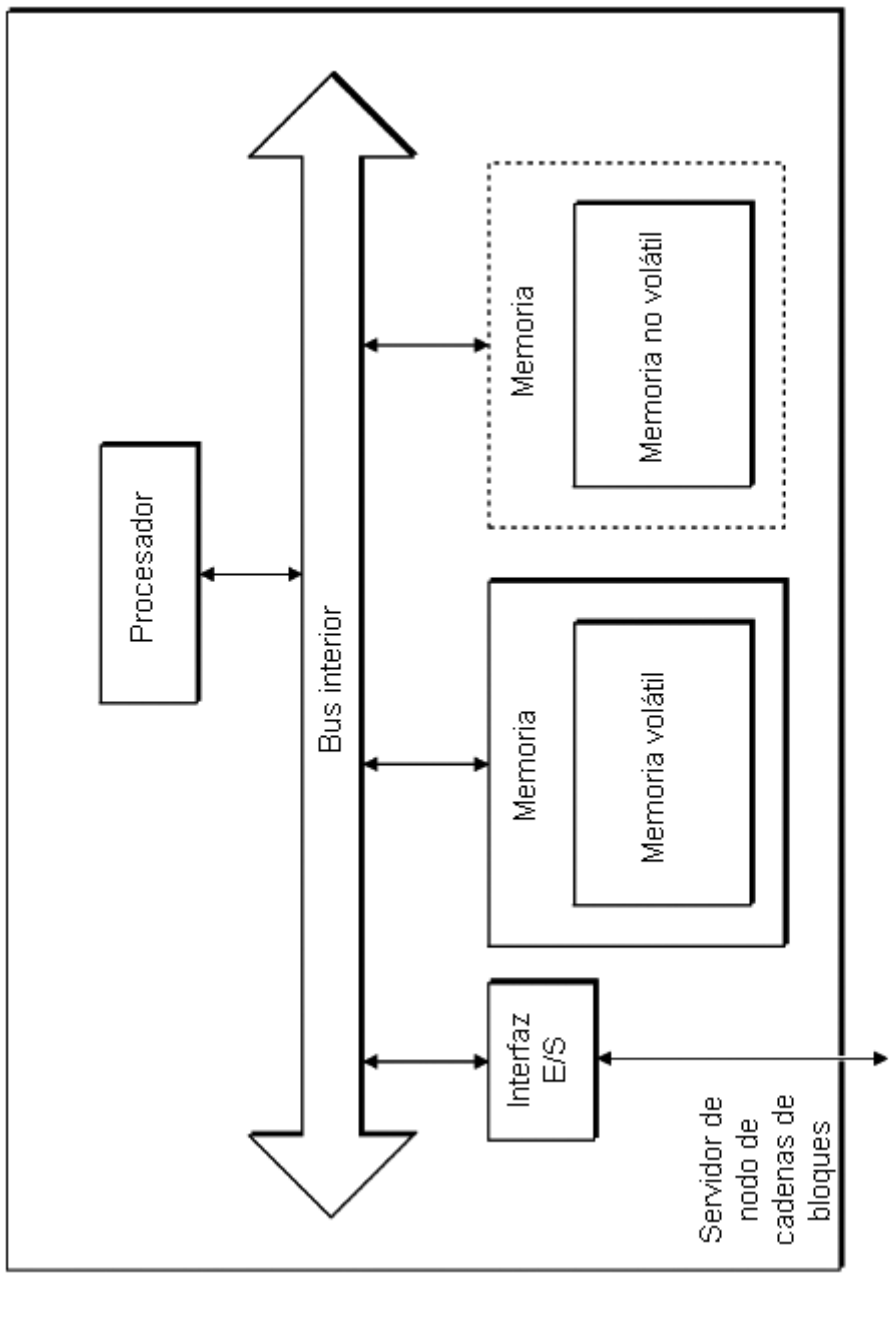
Procesador
Bus interior
Memoria
Memoria no volátil
Memoria
Memoria volátil
Interfaz E/S
Servidor de nodo de cadenas de bloques
Resultado de votación de participación accionarial de un nodo accionista

FIG. 7

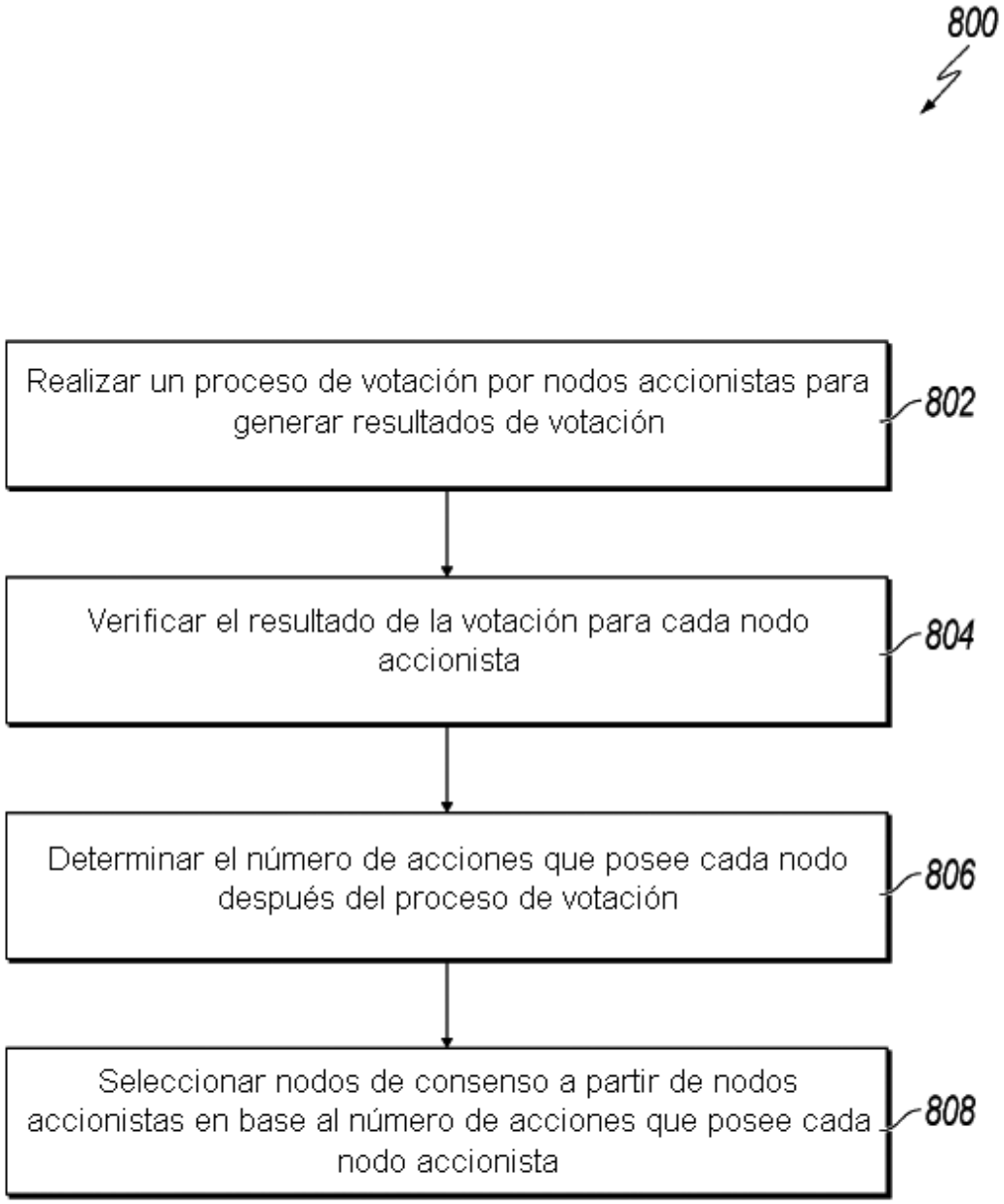
800
Realizar un proceso de votación por nodos accionistas para generar resultados de votación
802
Verificar el resultado de la votación para cada nodo accionista
804
Determinar el número de acciones que posee cada nodo después del proceso de votación
806
Seleccionar nodos de consenso a partir de nodos accionistas en base al número de acciones que posee cada nodo accionista
808

FIG. 8