(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 880 108**

(51) Int. CI.:

G06F 11/14 (2006.01)
H04L 9/32 (2006.01)
H04L 29/14 (2006.01)
G06F 11/20 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.03.2019 PCT/CN2019/078487**

(87) Fecha y número de publicación internacional: **31.05.2019 WO19101241**

(96) Fecha de presentación y número de la solicitud europea: **18.03.2019 E 19725895 (7)**

(97) Fecha y número de publicación de la concesión europea: **23.06.2021 EP 3593249**

(54) Título: **Sistema y método para finalizar el protocolo de cambio de vista**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.11.2021

(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:

YANG, DAYI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Sistema y método para finalizar el protocolo de cambio de vista

Campo técnico

Esta aplicación se refiere, en general, a métodos y dispositivos para realizar un cambio de vista, y, en particular, a métodos y dispositivos para finalizar el cambio de vista en un sistema de Tolerancia Práctica a Fallos Bizantinos (PBFT).

Antecedentes

La Tolerancia Práctica a Fallos Bizantinos (PBFT) es un tipo de mecanismo de consenso que puede implementarse en sistemas distribuidos tales como sistemas de cadena de bloques. El mecanismo de consenso de PBFT posibilita que un sistema distribuido alcance un consenso suficiente con seguridad y ejecución, a pesar de que pueden fallar ciertos nodos del sistema (por ejemplo, debido a conexión de red pobre o que se vuelvan defectuosos de otra manera) o se propague información incorrecta a otros clientes (por ejemplo, actuando de manera maliciosa). El objetivo de tal mecanismo es defenderse contra fallos de sistema catastróficos mitigando la influencia de los nodos que no funcionan en la función correcta del sistema y en el consenso alcanzado mediante nodos que funcionan (por ejemplo, nodos no defectuosos y honestos) en el sistema.

El mecanismo de consenso de PBFT se enfoca en proporcionar una replicación práctica de máquina de estado bizantino que tolera los fallos bizantinos (por ejemplo, nodos que no funcionan) a través de una suposición de que hay fallos de nodo independientes y mensajes manipulados propagados mediante nodos específicos e independientes. En este mecanismo de consenso de PBFT, por ejemplo, todos los nodos en un sistema de cadena de bloques están ordenados en una secuencia siendo un nodo el nodo primario (también conocido como el nodo líder o maestro) y denominados los otros como los nodos de respaldo (también conocidos como nodos seguidores). Todos los nodos en el sistema se comunican entre sí y el objetivo es para que todos los nodos honestos entren en un acuerdo/consenso en un estado del sistema.

Por ejemplo, para que funcione el mecanismo de consenso de PBFT, la suposición es que la cantidad de nodos que no funcionan en un sistema de cadena de bloques no pueden equivaler de manera simultánea o superar un tercio de los nodos globales en el sistema en una ventana de vulnerabilidad dada. El método proporciona eficazmente tanto la ejecución como la seguridad siempre que la mayoría de los nodos F sean nodos que no funcionan al mismo tiempo. En otras palabras, en algunas implementaciones, el número F de nodos que no funcionan que pueden tolerarse mediante el mecanismo de consenso de PBFT equivale a (N-1)/3, redondeado abajo hasta el número entero más cercano, en donde N designa el número total de nodos en el sistema. En algunas implementaciones, un sistema de cadena de bloques que implementa el mecanismo de consenso de PBFT puede manejar hasta F fallos bizantinos donde hay al menos 3F+1 nodos en total. Para realizar verificaciones de consenso, cada nodo ejecuta un protocolo de operación normal bajo el liderazgo del nodo primario. Cuando un nodo piensa que el nodo primario no está funcionando, el nodo puede entrar en un protocolo de cambio de vista para iniciar un cambio del nodo primario. Después de que un nuevo nodo primario sustituye al nodo primario que no funciona bajo un acuerdo por una mayoría de nodos, los nodos vuelven al protocolo de operación normal.

En las tecnologías actuales, un nodo sale del protocolo de cambio de vista de acuerdo con el procedimiento tradicional: esperando que una mayoría de los nodos también entren en el protocolo de cambio de vista y acuerden que el nodo primario no está funcionando. En el protocolo de cambio de vista tradicional, esta condición es que cuando al menos 2F+1 nodos entran en el protocolo de cambio de vista y multidifunden el mensaje de cambio de vista respectivamente, el nuevo nodo primario que obtiene al menos 2F+1 mensajes de cambio de vista multidifunde el nuevo mensaje de vista para ayudar a que los nodos vuelvan a la operación normal. Sin embargo, en algunos casos, la perturbación de la comunicación de red puede hacer que un nodo determine de manera errónea que el nodo primario no está funcionando y entre en el protocolo de cambio de vista mientras que los otros nodos aún están en operación normal. Como resultado, el nodo se atasca en el protocolo de cambio de vista y se excluye de manera eficaz del proceso de consenso. El retardo antes de llevar el nodo atascado de vuelta a la operación normal es impredecible, puesto que puede depender de cuándo ocurre un fallo o funcionamiento incorrecto del nodo primario real. Por lo tanto, se desperdicia la potencia informática del nodo atascado mientras se espera que otros nodos se unan al cambio de vista. Por lo tanto, es deseable proporcionar un mecanismo alternativo que pueda ayudar a los nodos a salir del protocolo de cambio de vista.

Atul Singh et al: "Zeno: Eventually Consistent Byzantine-Fault Tolerance", USENIX, The Advanced Computing Systems Association, 2 de abril de 2009 (02-04-2009), páginas 1-16 y Jiang Yanjun et al: "High Performance and Scalable Byzantine Fault Tolerance", 2019 IEEE 3RD Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), IEEE, 15 de marzo de 2019 (15-03-2019), páginas 1195-1202, ambos se refieren a redes Bizantinas tolerantes a fallos

Sumario

Diversas realizaciones de la memoria descriptiva incluyen, pero sin limitación, sistemas, métodos y medios legibles por ordenador no transitorios para realizar el cambio de vista.

De acuerdo con un aspecto de la presente invención, se proporciona un método implementado por ordenador para finalizar un cambio de vista en un mecanismo Tolerante a Fallos Bizantino Práctico, PBFT, para que se implemente en una cadena de bloques mantenida por un número (N) de nodos donde N es mayor de 1. El método se realiza por un primer nodo de los N nodos que se encuentra en un protocolo de cambio de vista. El método comprende: obtener, respectivamente desde al menos un quórum de Q segundos nodos de los N nodos, comprendiendo cada uno de los al menos Q primeros mensajes (a) una vista actual consistente conocida para el segundo nodo que indica un nodo primario designado entre los N nodos y (b) un número de secuencia actual consistente conocido para el segundo nodo, el número de secuencia actual asociado a un último bloque o una última transacción confirmada por el segundo nodo, en donde el número de secuencia actual es mayor que un primer número de secuencia conocido para el primer nodo, en donde el quórum Q es (N+F+1)/2 redondeado arriba hasta el número entero más cercano, y F es (N-1)/3 redondeado abajo hasta el número entero más cercano, y en respuesta a obtener los al menos Q primeros mensajes, sincronizar una primera copia de la cadena de bloques mantenida por el primer nodo con una segunda copia de la cadena de bloques mantenida por un segundo nodo, y salir del protocolo de cambio de vista para entrar en un protocolo de operación normal del PBFT usando la vista actual consistente para el primer nodo.

En algunas realizaciones, obtener los al menos Q primeros mensajes comprende: obtener, respectivamente desde los al menos Q segundos nodos, al menos Q mensajes de confirmación que indican que los al menos Q segundos nodos acuerdan un siguiente bloque para añadir a la cadena de bloques, comprendiendo los Q mensajes de confirmación respectivamente los Q primeros mensajes.

En otras realizaciones, obtener los al menos Q primeros mensajes comprende: obtener, respectivamente desde los al menos Q segundos nodos, al menos Q mensajes de confirmación que indican que los al menos Q segundos nodos acuerdan un siguiente bloque para añadir a la cadena de bloques, los Q primeros mensajes respectivamente anexados a los Q mensajes de confirmación.

En otras realizaciones más, el número de secuencia actual comprende una altura de una segunda copia de la cadena de bloques mantenida por el segundo nodo; y el primer número de secuencia comprende una altura de una primera copia de la cadena de bloques mantenida por el primer nodo.

En aún otras realizaciones, el número de secuencia actual comprende un número de secuencia de la última transacción confirmada por el segundo nodo; y el primer número de secuencia comprende un número de secuencia de una última transacción confirmada por el primer nodo.

En algunas realizaciones, el primer mensaje comprende una firma digital que certifica la vista actual y el número de secuencia actual ambos conocidos para el segundo nodo.

En otras realizaciones, el primer mensaje comprende adicionalmente un resumen del último bloque o la última transacción.

En otras realizaciones más, el resumen comprende un valor de función de troceo del último bloque o la última transacción.

En aún otras realizaciones, el resumen comprende una raíz de Merkle del último bloque conocido para el segundo nodo, pero desconocido para el primer nodo.

En otras realizaciones, el número de secuencia actual conocido para los al menos Q segundos nodos es (n+1); y el primer número de secuencia conocido para el primer nodo es n.

En otras realizaciones más, la vista actual para los al menos Q segundos nodos es v; y cuando está en el protocolo de cambio de vista, el primer nodo tiene una primera vista mayor que v.

En aún otras realizaciones, en la red de Tolerancia Práctica a Fallos Bizantinos (PBFT), uno de los N nodos actúa como el nodo primario y los otros (N-1) nodos actúan como nodos de respaldo.

En algunas realizaciones, un sistema de cambio de vista comprende: uno o más procesadores; y una o más memorias legibles por ordenador acopladas al uno o más procesadores y que tienen instrucciones almacenadas en las mismas que son ejecutables por el uno o más procesadores para realizar el método de cualquiera de las realizaciones anteriores.

En otras realizaciones, un aparato de cambio de vista comprende una pluralidad de módulos para realizar el método de cualquiera de las realizaciones anteriores.

De acuerdo con otra realización, un sistema de cambio de vista es para mantener una cadena de bloques, en donde un número (N) de nodos mantienen la cadena de bloques, actuando el sistema como un primer nodo de los N nodos que está en un protocolo de cambio de vista. El sistema comprende uno o más procesadores y una o más memorias legibles por ordenador no transitorias acopladas al uno o más procesadores y configuradas con instrucciones ejecutables por el uno o más procesadores para hacer que el sistema realice operaciones que comprenden: obtener, respectivamente desde al menos Q segundos nodos de los N nodos, al menos Q primeros mensajes que comprende cada uno (1) una vista actual consistente conocida para el segundo nodo que indica un nodo primario designado entre los N nodos y (2) un número de secuencia actual consistente conocido para el segundo nodo, el número de secuencia actual asociado a un último bloque o una última transacción confirmada por el segundo nodo, en donde el número de secuencia actual es mayor que un primer número de secuencia conocido para el primer nodo, Q (quórum) es (N+F+1)/2 redondeado arriba hasta el número entero más cercano, y F es (N-1)/3 redondeado abajo hasta el número entero más cercano; y en respuesta a obtener los al menos Q primeros mensajes, finalizar el protocolo de cambio de vista.

De acuerdo con otra realización más, un medio de almacenamiento legible por ordenador no transitorio es para mantener una cadena de bloques, en donde un número (N) de nodos mantiene la cadena de bloques, estando asociado el medio de almacenamiento con un primer nodo de los N nodos que está en un protocolo de cambio de vista. El medio de almacenamiento está configurado con instrucciones ejecutables por uno o más procesadores para hacer que el uno o más procesadores realicen operaciones que comprenden: obtener, respectivamente desde al menos Q segundos nodos de los N nodos, al menos Q primeros mensajes que cada uno comprende (1) una vista actual consistente conocida para el segundo nodo que indica un nodo primario designado entre los N nodos y (2) un número de secuencia actual consistente conocido para el segundo nodo, el número de secuencia actual asociado a un último bloque o una última transacción confirmada por el segundo nodo, en donde el número de secuencia actual es mayor que un primer número de secuencia conocido para el primer nodo, Q (quórum) es (N+F+1)/2 redondeado arriba hasta el número entero más cercano, y F es (N-1)/3 redondeado abajo hasta el número entero más cercano; y en respuesta a obtener los al menos Q primeros mensajes, finalizar el protocolo de cambio de vista.

De acuerdo con otra realización más, un aparato de cambio de vista es para mantener una cadena de bloques, en donde un número (N) de nodos mantienen la cadena de bloques, actuando el aparato como un primer nodo de los N nodos que está en un protocolo de cambio de vista. El aparato comprende un módulo de obtención para obtener, respectivamente desde al menos Q segundos nodos de los N nodos, al menos Q primeros mensajes que cada uno comprende (1) una vista actual consistente conocida para el segundo nodo que indica un nodo primario designado entre los N nodos y (2) un número de secuencia actual consistente conocido para el segundo nodo, el número de secuencia actual asociado a un último bloque o una última transacción confirmada por el segundo nodo, en donde el número de secuencia actual es mayor que un primer número de secuencia conocido para el primer nodo, Q (quórum) es (N+F+1)/2 redondeado arriba hasta el número entero más cercano, y F es (N-1)/3 redondeado abajo hasta el número entero más cercano; y un módulo de finalización para, en respuesta a obtener los al menos Q primeros mensajes, finalizar el protocolo de cambio de vista.

Las realizaciones desveladas en la memoria descriptiva tienen uno o más efectos técnicos. En algunas realizaciones, los métodos y sistemas pueden garantizar que un nodo (por ejemplo, un primer nodo) de un sistema de consenso de PBFT que haya entrado en un protocolo de cambio de vista pueda salir de manera eficaz del protocolo de cambio de vista y reanudar el protocolo de operación normal. En otras realizaciones, cuando un segundo nodo en el protocolo de operación normal multidifunde un mensaje de confirmación, puede añadir o anexar un primer mensaje al mensaje de confirmación, comprendiendo el primer mensaje una vista actual y un número de secuencia actual conocido para el segundo nodo. La vista actual indica la vista del segundo nodo del nodo primario, y el número de secuencia actual indica la última transacción o transacciones confirmadas del segundo nodo o una altura de la cadena de bloques (también conocida como altura de bloque) asociada con el último bloque o bloques de la cadena de bloques mantenida por el segundo nodo. En otras realizaciones más, el primer nodo atascado en el protocolo de cambio de vista puede obtener la vista actual y el número de secuencia actual desde el primer mensaje. Tras recibir un número de quórum Q de primeros mensajes consistentes, el primer nodo puede compararlos con su propia vista y número de secuencia para determinar si una mayoría de los nodos aún están en operación normal. Si la mayoría de otros nodos están aún en operación normal, el segundo nodo puede finalizar el protocolo de cambio de vista y reanudar el protocolo de operación normal. En aún otras realizaciones, como se indica por el número de secuencia en los primeros mensajes, la mayoría de nodos pueden haber acordado una siguiente transacción o un nuevo bloque en la secuencia de verificación de consenso, la siguiente transacción o el siguiente bloque no reconocidos aún por el primer nodo. Al darse cuenta de que la mayoría de nodos no entraron en el cambio de vista, el primer nodo puede finalizar sin problemas el protocolo de cambio de vista. En algunas realizaciones, el primer nodo puede finalizar el cambio de vista incluso si la mayoría de nodos tampoco entran en el cambio de vista y acuerdan una nueva vista para finalizar el protocolo de cambio de vista. El número de nodos en la operación normal y la contribución de su potencia informática puede optimizarse de esta manera.

Estas y otras características de los sistemas, métodos y medios no transitorios legibles por ordenador divulgados en este documento, así como los métodos de operación y funciones de los elementos de estructuras relacionados y la combinación de partes y economías de fabricación, se harán más evidentes tras la consideración de la siguiente descripción y las reivindicaciones adjuntas con referencia a los dibujos adjuntos, todos los cuales forman una parte de esta memoria descriptiva, en donde números de referencia similares designan partes correspondientes en las diversas

figuras. Debe entenderse expresamente, sin embargo, que los dibujos son para propósitos de ilustración y descripción únicamente y no pretenden ser limitantes.

Breve descripción de los dibujos

La Figura 1 ilustra una red, de acuerdo con diversas realizaciones.

La Figura 2A ilustra un protocolo de operación normal de PBFT.

La Figura 2B ilustra un protocolo de operación normal de PBFT con una réplica que no funciona.

La Figura 2C ilustra un protocolo de operación normal y un protocolo de cambio de vista de PBFT.

La Figura 3A ilustra un diagrama de flujo de rutas de conmutación entre el protocolo de operación normal y el protocolo de cambio de vista.

La Figura 3B ilustra un diagrama de flujo de rutas de conmutación entre el protocolo de operación normal y el protocolo de cambio de vista, de acuerdo con diversas realizaciones.

La Figura 4 ilustra un diagrama de flujo de las etapas de salida de cambio de vista, de acuerdo con diversas realizaciones.

La Figura 5A ilustra un diagrama de flujo de un método de cambio de vista, de acuerdo con diversas realizaciones.

La Figura 5B ilustra un diagrama de flujo de un método de cambio de vista, de acuerdo con diversas realizaciones.

La Figura 6 ilustra un diagrama de bloques de un sistema de cambio de vista, de acuerdo con diversas realizaciones.

La Figura 7 ilustra un diagrama de bloques de un sistema informático en el que puede implementarse cualquiera de las realizaciones descritas en el presente documento.

Descripción detallada

Las realizaciones desveladas en el presente documento incluyen, pero sin limitación, sistemas de cambio de vista, métodos y medios legibles por ordenador no transitorios que pueden implementarse en sistemas de PBFT. En diversas realizaciones, se proporciona una ruta para salir del protocolo de cambio de vista y reanudar el protocolo de operación normal. Un nodo que ha entrado en el cambio de vista puede llevarse de vuelta a la operación normal sin pasar a través del protocolo de cambio de vista tradicional, lo que requiere al menos Q nodos para entrar en el cambio de vista. Q (quórum) es (N+F+1)/2 redondeado arriba hasta el número entero más cercano, N representa el número total de nodos y es un número entero no menor que cuatro, y F es (N-1)/3 redondeado abajo hasta el número entero más cercano. Similar a PBFT, los sistemas, métodos, y el medio legible por ordenador no transitorio desvelados pueden aplicarse a otros protocolos de consenso tales como SecureRing, Byzantine Paxos, Q/U, HQ, Zyzzvyva, ABsTRACTs, RBFT, Adapt, Tangaroa, CheapBFT, MinBFT, FastBFT, etc. Puede hacerse referencia para diversos aspectos de PBFT a M. Castro, B. Liskov, "Practical Byzantine Fault Tolerance", Proceedings of the Third Symposium on Operating Systems Design and Implementation, (Feb 1999), que se incorpora por referencia en el presente documento en su totalidad.

La Figura 1 muestra una red 120, de acuerdo con diversas realizaciones. Los componentes presentados a continuación se pretende que sean ilustrativos. Como se muestra, la red 120 puede comprender un sistema de red 112. El sistema de red 112 puede comprender uno o más nodos (por ejemplo, el nodo 0, el nodo 1, el nodo 2, el nodo 3, el nodo 4, el nodo i, etc.) implementados en uno o más dispositivos informáticos tales como servidores, ordenadores, teléfonos móviles, etc. El sistema de red 112 puede instalarse con software apropiado (por ejemplo, programa de consenso) y/o hardware (por ejemplo, alambres, conexiones inalámbricas) para acceder a otros dispositivos de la red 120 o sistemas adicionales. El nodo puede incluir uno o más procesadores y una o más memorias acopladas al uno o más procesadores. Las memorias pueden ser no transitorias y legibles por ordenador y pueden configurarse con instrucciones ejecutables por uno o más procesadores para hacer que el uno o más procesadores realicen las operaciones descritas en el presente documento. Aunque se muestran los nodos como únicos componentes en esta figura, se apreciará que estos nodos pueden implementarse como dispositivos únicos o múltiples dispositivos acoplados juntos. En general, los nodos pueden comunicarse entre sí y con otros dispositivos fuera del sistema de red 112. Por ejemplo, pueden comunicarse datos a través de una o más redes alámbricas o inalámbricas (por ejemplo, Internet).

En diversas realizaciones, el sistema de red 112 puede implementarse como un sistema de red de cadena de bloques que comprende diversos nodos de cadena de bloques. Como se muestra, el sistema de red de cadena de bloques puede comprender una pluralidad de nodos de cadena de bloques (por ejemplo, el nodo 0, el nodo 1, el nodo 2, el

nodo 3, el nodo 4, el nodo i, etc.). Los nodos de cadena de bloques pueden formar una red (por ejemplo, red entre pares) con un nodo de cadena de bloques que se comunica con otro. El orden y el número de los nodos de cadena de bloques como se muestran son simplemente ejemplos y por simplicidad de ilustración. Los nodos de cadena de bloques pueden implementarse en servidores, ordenadores, etc. Cada nodo de cadena de bloques puede corresponder a uno o más dispositivos de hardware físico o dispositivos virtuales acoplados juntos mediante diversos tipos de métodos de comunicación tales como TCP/IP. Dependiendo de las clasificaciones, los nodos de cadena de bloques pueden comprender nodos totales, nodos Geth, nodos de consenso, etc.

En diversas realizaciones, el sistema de red de cadena de bloques puede interactuar con otros sistemas y dispositivos tales como el nodo A y el nodo B (por ejemplo, nodos ligeros). Las interacciones pueden implicar la transmisión y recepción de datos para el propósito de, por ejemplo, recibir una solicitud y devolver un resultado de ejecución de la solicitud. En un ejemplo, el usuario A puede desear realizar transacciones con el usuario B a través de la red de cadena de bloques. La transacción puede implicar transferir algún activo en la cuenta del usuario A a la cuenta del usuario B. El usuario A y el usuario B pueden usar respectivos nodo A y nodo B de los dispositivos instalados con un software de cadena de bloques apropiado (por ejemplo, monedero de criptomoneda) para la transacción. El nodo A puede acceder a la cadena de bloques a través de la comunicación con el nodo 0, y el nodo B puede acceder a la cadena de bloques a través de la comunicación con el nodo 1. Por ejemplo, el nodo A puede enviar una solicitud de transacción a la cadena de bloques a través del nodo 0, y el nodo B puede enviar una solicitud de ejecución de contrato inteligente a la cadena de bloques a través del nodo 1. Fuera de la cadena de bloques, el nodo A y el nodo B pueden tener otros canales de comunicación (por ejemplo, comunicación de internet convencional sin pasar a través de los nodos 0 y 1).

Los nodos de cadena de bloques pueden cada uno comprender o acoplarse a una memoria. En algunas realizaciones, la memoria puede almacenar una base de datos de agrupación. La base de datos de agrupación puede ser accesible para la pluralidad de nodos de cadena de bloques de una manera distribuida. Por ejemplo, la base de datos de agrupación puede almacenarse respectivamente en las memorias de los nodos de cadena de bloques. La base de datos de agrupación puede almacenar una pluralidad de transacciones enviadas mediante el uno o más dispositivos de usuario tales como los nodos A y B operados por los usuarios.

Los nodos de cadena de bloques forman una red (por ejemplo, una red P2P) que, a través de consenso, registra transacciones en un libro mayor distribuido conocido como cadena de bloques. Los participantes de una red P2P pueden denominarse como nodos, que mantienen la cadena de bloques. En una red P2P de cadena de bloques, cada nodo participa en las verificaciones de consenso y almacena una copia de libro mayor completa de la cadena de bloques. Cada nodo confirma lotes de transacciones por un método de consenso de cadena de bloques para garantizar que todos los nodos tienen resultados de confirmación consistentes y, por lo tanto, copias de la cadena de bloques consistentes.

Uno de los métodos de consenso de cadena de bloques es la Tolerancia Práctica a Fallos Bizantinos (PBFT). La tolerancia a fallos bizantinos se origina a partir del problema general bizantino. Para un sistema de red P2P, siempre que el número de tales nodos que no funcionen se encuentre dentro de un cierto límite, el sistema puede continuar funcionando de manera apropiada. Tal sistema se denomina sistema tolerante a fallos bizantinos. PBFT es un ejemplo de una optimización de la capacidad de red de tolerancia a fallos bizantinos. PBFT proporciona a la red con una máquina de estado bizantina, que copia servidores y que sincroniza interacciones de cliente con copias de servidor.

En el centro de la operación PBFT está el mantenimiento de la vista global consistente de la información registrada en la cadena de bloques, que forma la red troncal para posibilitar que los usuarios interactúen entre sí de una manera descentralizada. La seguridad del modelo de consenso de PBFT es crítica para una plataforma de cadena de bloques. Las dos propiedades clave de un modelo de consenso son: 1) seguridad o consistencia: todos los nodos honestos producen la misma salida válida; y 2) ejecución: todos los nodos honestos en consenso producen eventualmente un valor sin quedarse estancados en una etapa intermedia. Un protocolo de consenso de PBFT seguro y robusto necesita tolerar una amplia diversidad de comportamientos bizantinos, que incluyen fallos de nodos de red, partición de la red, retardo de mensaje, entrega de mensaje fuera de orden, corrupción de mensaje y similares y alcanzar el consenso en nodos siempre que esté limitado el número de nodos que no funcionan en el sistema. Para este fin, el modelo PBFT funciona bajo cualquiera de uno de dos protocolos mutuamente exclusivos: protocolo de operación normal/consistencia y protocolo de cambio de vista que se describen adicionalmente a continuación. En esta memoria descriptiva, que no funciona significa defectuoso y/o malicioso, y que funciona significa no defectuoso y honesto. Los posibles actos fallidos o maliciosos pueden incluir: fallo para entregar el mensaje, retardo de entrega de mensaje, entrega de mensaje fuera de orden, fallos bizantinos (entregar mensajes arbitrarios a diferentes nodos, infracción del protocolo), etc.

En algunas realizaciones, un sistema de Tolerancia Práctica a Fallos Bizantinos (PBFT) puede comprender N nodos, actuando uno de los N nodos como un nodo primario y actuando los otros de los N nodos como nodos de respaldo. La designación de nodo primario puede no estar fijada a un nodo particular, ya que puede elegirse otro nodo para que se vuelva un nuevo nodo primario a través del protocolo de cambio de vista. Por ejemplo, puede elegirse el nodo primario a través de una operación módulo, en la que un nodo que funciona con el número de serie más bajo (número de vista de modulo) se vuelve el nuevo nodo primario. La vista actual y el número total de nodos N puede determinar el id de nodo primario = (vista+1) mod N. En PBFT, la vista se cambia cada vez que se elige un nuevo nodo primario.

Por ejemplo, con cada cambio de vista, la vista aumenta de manera monotónica desde cero. Es decir, la vista puede cambiar con un cambio en el nodo primario.

En algunas realizaciones, el nodo primario está funcionando en la vista v, y se ejecuta el protocolo de operación normal. Para la operación normal, el nodo primario y/o los nodos de respaldo pueden recibir solicitudes asociadas con transacciones no verificadas desde uno o más clientes. Por ejemplo, el nodo A como un cliente puede enviar una solicitud al nodo primario y/o a los nodos de respaldo. Las solicitudes pueden incluir las transacciones no verificadas (por ejemplo, transacciones que han de añadirse a un nuevo bloque en la cadena de bloques). Las transacciones no verificadas pueden incluir, por ejemplo, transacciones financieras basadas en cadena de bloques, transacciones de implementación o ejecución de contratos inteligentes, etc. Los nodos primario y de respaldo pueden realizar o no alguna verificación preliminar de las transacciones. Los nodos de respaldo que reciben las solicitudes pueden reenviar las solicitudes recibidas al nodo primario. Una vez que las transacciones en el nodo primario alcanzan un cierto nivel o se cumple de otra manera una condición de activación, el nodo primario puede iniciar una ronda de verificación de consenso y proponer un resultado de verificación para las transacciones no verificadas. Los nodos de respaldo pueden responder al consenso y confirmar la propuesta para alcanzar un consenso. Los requisitos para los nodos son que son deterministas y empiezan en el mismo estado. El resultado final es que todos los nodos honestos entran en un consenso en el orden del registro y pueden aceptarlo o rechazarlo. Una vez verificadas por consenso, las transacciones pueden empaquetarse en un nuevo bloque de la cadena de bloques y añadirse a las copias de la cadena de bloques locales mantenidas mediante los nodos. También, son notificados los clientes (por ejemplo, el nodo A) que enviaron originalmente las solicitudes.

Para conservar la seguridad, el método de PBFT principal comprende tres fases para el protocolo de operación normal: preparación previa, preparación y confirmación. Haciendo referencia a la Figura 2A a la Figura 2C, un ejemplo de un sistema de PBFT comprende cuatro réplicas (siendo la réplica otro término para nodo): réplica 0, réplica 1, réplica 2 y réplica 3. Los números 0 a 3 son números de serie de réplica que pueden usarse para determinar un nuevo nodo primario. La réplica 0 puede corresponder al nodo primario 0, y las réplicas 1, 2 y 3 pueden corresponder a nodos de respaldo 1, 2 y 3. Las réplicas pueden implementarse, por ejemplo, en diversos nodos de cadena de bloques del sistema de red 112 anteriormente descrito. Se muestra un protocolo de operación normal en la Figura 2A con ningún nodo que no funcione presente, y se muestra otro protocolo de operación normal en la Figura 2B siendo la réplica 3 un nodo que no funciona. Para ambas situaciones, el protocolo de operación normal puede dividirse en una fase de solicitud, una fase de preparación previa, una fase de preparación, una fase de confirmación y una fase de respuesta.

Haciendo referencia a la Figura 2A y a la Figura 2B, la operación normal comienza en la fase de solicitud cuando un cliente envía una solicitud (mensaje) al nodo primario (réplica 0), que es responsable de apoyar la solicitud. La solicitud puede comprender información del cliente, una operación de solicitud (por ejemplo, una solicitud de transacción para verificación de consenso) y una indicación de tiempo de solicitud. El cliente (también denominado como un nodo cliente) puede implementarse, por ejemplo, en el nodo A anteriormente descrito. El nodo A puede ser un nodo ligero (por ejemplo, implementado en un teléfono móvil). Adicionalmente o como alternativa, el cliente puede enviar la solicitud a un nodo de respaldo, que reenvía la solicitud al nodo primario antes de la fase de preparación previa. Independientemente de si el nodo primario o de respaldo recibe la solicitud, el correspondiente nodo puede multidifundir la solicitud recibida a los otros nodos en la red. Por lo tanto, el nodo primario puede finalizar obteniendo las solicitudes pendientes enviadas por los clientes a la red de consenso de una manera o la otra.

Por consiguiente, el nodo primario actúa como un líder y conduce a los nodos de respaldo para verificar las transacciones asociadas con las solicitudes. El nodo primario es responsable de ordenar la ejecución de solicitudes dentro de su vista. En la fase de preparación previa, el nodo primario puede validar las solicitudes obtenidas y proponer un número de secuencia para cada una de las solicitudes. Por lo tanto, a cada una de las solicitudes puede asignarse un número de secuencia creciente y por lo tanto ponerse en orden. Adicionalmente, el mensaje de preparación previa puede comprender una altura de bloque. La altura de bloque puede estar basada en una altura actual de la cadena de bloques. Por ejemplo, si la cadena de bloques tiene actualmente 1000 bloques, la altura de bloque puede ser 1000 que indica que ya existen 1000 bloques en la cadena de bloques, o puede ser 1001 que indica que las transacciones asociadas con las solicitudes se proponen en el bloque de orden 1001 de la cadena de bloques, que ya va a verificarse por otros nodos. El nodo primario puede reenviar las solicitudes junto con el número de secuencias y/o la altura de bloque. Por ejemplo, después de obtener las solicitudes, el nodo primario puede disponer las solicitudes en un orden para ejecutar las correspondientes transacciones asignando los números de secuencia y almacenándolos en una lista. El nodo primario puede enviar un mensaje de preparación previa a cada nodo de respaldo (de la réplica 1 a la réplica 3) en el sistema de red de PBFT. Como se muestra en la Figura 2A, el nodo primario puede multidifundir la lista en o junto con el mensaje de preparación previa a los nodos de respaldo. Como se muestra en la Figura 2B, incluso si un nodo de respaldo (réplica 3) no está funcionando y el nodo primario no tiene conocimiento de eso, el nodo primario puede aún enviar el mensaje de preparación previa. Cada nodo de respaldo acepta el mensaje de preparación previa siempre que sea válido. El mensaje de preparación previa puede contener un número de vista, números de secuencia, firmas, un resumen (d), otros metadatos y similares, que permiten la determinación de la validez del mensaje.

En la fase de preparación, si un nodo de respaldo acepta el mensaje de preparación previa, puede continuar multidifundiendo un mensaje de preparación a otros nodos en el sistema de red de PBFT que incluyen el nodo primario. Multidifundir el mensaje de preparación indica que el nodo emisor acuerda el orden. Cada mensaje de preparación se

acepta por el nodo de recepción siempre que sea válido. La validez del mensaje de preparación puede determinarse de manera similar basándose en el número de vista, el número de secuencia, firmas, un resumen (d), otros metadatos y similares. Se prepara un nodo si ha recibido la solicitud original desde el nodo primario, ha preparado previamente (por ejemplo, multidifundiendo el mensaje de preparación previa), y ha obtenido al menos (Q-1) mensajes de preparación previa distintos, válidos y consistentes que coinciden con el mensaje de preparación previa. El mensaje de preparación (Q-1) puede incluir el mensaje de preparación de multidifusión. Q (quórum) es (N+F+1)/2 redondeado arriba hasta el número entero más cercano, N representa el número total de nodos y es un número entero no menor que cuatro, y F es (N-1)/3 redondeado abajo hasta el número entero más cercano. El sistema de red de PBFT de Q nodos puede tolerar hasta F fallos bizantinos. En algunas realizaciones, cuando N es al menos (3F+1), Q es (2F+1). En este punto, (Q-1) en lugar de que sean necesarios Q mensajes de preparación debido a que el mensaje de preparación previa puede tratarse como un equivalente de un mensaje de preparación del nodo primario (aunque el nodo primario puede no enviar el mensaje de preparación de por sí). Si se cuenta el mensaje de preparación previa como un mensaje de preparación más, entonces habría al menos Q mensajes de preparación distritos y válidos que indican que al menos Q de todos los nodos aceptaron el mensaje de preparación previa, de los cuales pueden tolerarse hasta F nodos que no funcionan. Por lo tanto, la fase de preparación previa a preparación garantiza que al menos (Q-F) nodos que funcionan (Q nodos preparados pero que contabilizan hasta F nodos que no funcionan) acuerdan que, si se ejecuta una solicitud en la vista v, se ejecutará con su número de secuencia. La fase de preparación asegura la ordenación consistente tolerante a fallos de cada solicitud dentro de las vistas.

En algunas realizaciones, después de recibir el mensaje de preparación previa y los (Q-1) mensajes de preparación, el nodo de respaldo puede verificar el orden y comparar el resultado de verificación con un resultado de verificación propuesto escrito por el nodo primario en el mensaje de preparación previa. Puede haber un número de maneras para verificar el orden. Por ejemplo, el resultado de verificación propuesto puede comprender una raíz de Merkle Patricia Trie escrita en el resumen (d). El nodo de respaldo puede disponer las transacciones asociadas con las solicitudes de acuerdo con el orden y calcular una raíz de Merkle Patricia Trie para comparar con la raíz de Merkle Patricia Trie propuesta. El cálculo puede requerir también cierta información existente tal como la función de troceo de nodo de los bloques existentes en la cadena de bloques. La comparación produce un resumen (D(m)) calculado mediante el nodo de respaldo. Si el resumen (D(m)) es consistente con el resumen (d), la verificación es satisfactoria. Una vez verificado, el nodo de respaldo puede estar de acuerdo con la ordenación de las solicitudes (por ejemplo, el orden para empaquetar las transacciones asociadas con las solicitudes en un nuevo bloque de la cadena de bloques). De manera similar, el nodo de respaldo puede verificar si los mensajes de confirmación (descritos a continuación con respecto a la fase de confirmación) que recibe comprenden el mismo resumen D(m) para determinar si otros nodos también están de acuerdo con la ordenación de las solicitudes. Si un nodo preparado ha obtenido Q mensajes de confirmación y se han ejecutado todas solicitudes con números de secuencia inferiores, el nodo puede ejecutar la solicitud.

En algunas realizaciones, el mensaje de preparación previa puede comprender un resumen (d) del nuevo bloque o información de otra manera relacionada con la ejecución de las solicitudes (por ejemplo, las transacciones asociadas con las solicitudes). El resumen (d) (por ejemplo, un valor de función de troceo) puede ser el resultado numérico de la aplicación de un algoritmo de función de troceo a los datos tales como las transacciones. El nodo de respaldo puede ejecutar las transacciones para confirmar el resumen (d). Para una pluralidad de solicitudes, el nodo de respaldo puede ejecutar las solicitudes de acuerdo con el orden (es decir, el número de secuencias de las solicitudes) para obtener un resumen D(m). Si D(m) y d son consistentes, el nodo de respaldo multidifunde un mensaje de confirmación (descrito a continuación con respecto a la fase de confirmación) que indica que el nodo de respaldo está de acuerdo con el resultado de validación del nodo primario. En algunas realizaciones, el mensaje de confirmación indica que el nodo de respaldo que multidifunde el mensaje de confirmación acuerda el mensaje de preparación previa y ha obtenido (Q-1) o más mensajes de preparación válidos y consistentes desde distintos nodos. Para una solicitud pendiente de un cierto número de secuencia, si un nodo preparado ha obtenido Q mensajes de confirmación y se han ejecutado todas las solicitudes con números de secuencia inferiores, el nodo puede ejecutar la solicitud.

En la fase de confirmación, si se prepara un nodo, puede multidifundir un mensaje de confirmación a otros nodos. El nodo puede recibir mensajes de confirmación de otros nodos. Cada nodo acepta el mensaje de confirmación siempre que sea válido. El mensaje de confirmación puede contener un número de vista, números de secuencia, firmas, un resumen, otros metadatos y similares, que permiten la determinación de la validez del mensaje. Si un nodo ha obtenido al menos Q mensajes distintos, válidos y consistentes, indica que se ha confirmado un número quórum de nodos (es decir, se preparan al menos (Q-F) nodos honestos) y se ha alcanzado consenso. Los al menos Q mensajes de confirmación válidos pueden incluir el mensaje de confirmación de multidifusión. Por lo tanto, la fase de preparación para confirmación asegura que al menos (Q-F) nodos que funcionan están de acuerdo (Q mensajes de confirmación pero que contabilizan hasta F nodos que no funcionan) con que se ejecutará eventualmente una solicitud en la vista v con su número de secuencia. Puesto que los nodos pueden confirmar en diferentes vistas (por ejemplo, cuando algunos nodos ya han entrado en una nueva vista y algunos otros nodos permanecen en la vista anterior), los mensajes de confirmación recibidos pueden corresponder a confirmaciones realizadas en diferentes vistas. La fase de confirmación asegura la ordenación consistente tolerante a fallos de cada solicitud a través de las vistas ya que los nodos que funcionan están de acuerdo con el número de secuencia de cada solicitud.

En algunas realizaciones, si un nodo ha obtenido al menos Q mensajes de confirmación distintos, válidos y consistentes, el nodo puede ejecutar la o las correspondientes solicitudes. Por ejemplo, una vez que se han obtenido

Q mensajes de confirmación, significa que el nuevo bloque está verificado en consenso. Por lo tanto, el nodo puede empaquetar el nuevo bloque en la copia de la cadena de bloques mantenida localmente. De otra manera, el nodo de respaldo puede activar directamente el protocolo de cambio de vista.

En la fase de respuesta, después de la ejecución de la solicitud o solicitudes, el nodo envía una respuesta directamente al cliente. Para una transacción empaquetada en la cadena de bloques, la respuesta puede comprender una dirección de la transacción en la cadena de bloques. Puesto que están permitidos hasta F fallos, el cliente espera las (Q-F) respuestas con firmas válidas desde diferentes nodos y con la misma indicación de tiempo de solicitud y el mismo resultado de ejecución antes de aceptar el resultado. Para el sistema de red de PBFT mostrado en la Figura 2A y en la Figura 2B, hay cuatro nodos totales, por lo que como máximo puede tolerarse un nodo que no funciona (N=4, Q=3 y F=1). Por lo tanto, incluso con réplica 3 que no funciona, puede aún alcanzarse el consenso en la Figura 2B.

Para conservar la ejecución, puede sustituirse el nodo primario en un protocolo de cambio de vista si ha pasado una cantidad de tiempo específica sin que el nodo primario multidifunda la solicitud. Por ejemplo, el nodo de respaldo puede mantener un temporizador. El nodo de respaldo inicia el temporizador cuando recibe una solicitud y el temporizador ya no está ejecutándose. El nodo de respaldo detiene el temporizador cuando ya no está esperando ejecutar la solicitud (es decir, se ejecuta la solicitud), pero reinicia el temporizador si está esperando ejecutar una o más otras solicitudes. Si se agota el temporizador, el nodo de respaldo puede determinar que el nodo primario no está funcionando. Por lo tanto, el nodo de respaldo puede multidifundir un mensaje de cambio de vista a otros nodos. Para otro ejemplo, el nodo de respaldo puede determinar que el nodo primario no está funcionando. Por lo tanto, el nodo de respaldo puede multidifundir un mensaje de cambio de vista. Para otro ejemplo, el cliente puede usar un temporizador para determinar si ha pasado demasiado tiempo después de que un cliente envía la solicitud al nodo primario sin recibir una respuesta. Cuando se agota este temporizador, el cliente envía su solicitud a todos los nodos. Si un nodo ya tiene conocimiento acerca de la solicitud, se ignora la re-difusión. Si el nodo no tiene conocimiento acerca de la solicitud, iniciará un temporizador. Cuando se agota el temporizador de nodo, el nodo inicia el proceso de cambio de vista multidifundiendo el mensaje de cambio de vista a otros nodos de respaldo basándose en la sospecha de que el nodo primario no está funcionando. El mensaje de cambio de vista incluye el estado del sistema (en forma de mensajes archivados que incluyen el mensaje de sí mismo durante la operación normal anterior), de modo que otros nodos tendrán conocimiento de que el nodo emisor no ha fallado.

Una súper mayoría de nodos honestos puede decidir si un nodo primario no está funcionando y eliminarlo con el siguiente nodo primario en línea con la sustitución. El cambio de vista tiene lugar cuando suficientes nodos creen que el nodo primario ha fallado. Una porción de la Figura 2C muestra el protocolo de cambio de vista. Haciendo referencia a la Figura 2C, bajo la fase de cambio de vista, si la vista actual es v, el nodo p = (v+1) mod N espera obtener Q mensajes de cambio de vista válidos para que se vuelvan el nuevo nodo primario, donde p es el número de serie de réplica/nodo, v es el número de vista, N es el número total de réplicas/nodos. Los Q mensajes de cambio de vista Q pueden incluir el mensaje de cambio de vista de multidifusión. Puesto que la vista anterior es v, los mensajes de cambio de vista puede cada uno comprender una nueva vista *v+1.* Una vez que el nuevo nodo primario p ha obtenido Q mensajes de cambio de vista, multidifunde un nuevo mensaje de vista. Este mensaje contiene todos los mensajes de cambio de vista válidos recibidos así como un conjunto de todas las solicitudes que pueden no haberse completado aún debido al fallo de nodo primario. El nuevo nodo primario puede decidir en el último punto de comprobación y garantizar, entre otras cosas, que se capturan los nodos que funcionan con los últimos estados, que puede implicar volver a confirmar solicitudes previas (por ejemplo, solicitudes preparadas, confirmadas, pero no ejecutadas) en la nueva vista. Aunque está teniendo lugar el cambio de vista, no se aceptan nuevas solicitudes. Después de que un nodo recibe un nuevo mensaje de vista válido que incluye los Q mensajes de cambio de vista, entra en la vista *v*+1 y procesa el conjunto de solicitudes no completadas. Posteriormente, el protocolo de operación normal continúa, y los nodos rehacen las solitudes entre el número de secuencia del último punto de comprobación estable y el número más alto en un mensaje de preparación, pero evitan la re-ejecución de solicitudes. Se ilustra la correspondiente conmutación de estado para un nodo entre el protocolo de operación normal y el protocolo de cambio de vista en la Figura 3A. Como se muestra en la Figura 3A, por ejemplo, un tiempo de espera para un nodo de respaldo puede activar una conmutación desde el protocolo de operación normal (por ejemplo, durante cualquier fase del protocolo de operación normal) al protocolo de cambio de vista (por ejemplo, iniciando la fase de cambio de vista). Después de ejecutar el protocolo de cambio de vista, una vez que se obtiene un nuevo mensaje de vista válido, el nodo de respaldo puede salir del protocolo de cambio de vista y reanudar el protocolo de operación normal para ejecutar las solicitudes pendientes. El nuevo mensaje válido puede incluir los Q mensajes de cambio de vista desde diferentes nodos.

Como se muestra en la Figura 3B, puede proporcionarse una ruta alternativa para que el nodo conmute el protocolo de cambio de vista al protocolo de operación normal, de acuerdo con diversas realizaciones. En algunas realizaciones, el nodo en el protocolo de cambio de vista puede obtener Q primeros mensajes para finalizar el protocolo de cambio de vista. El primer mensaje puede incluir una vista actual, un número de secuencia actual y/o un resumen. Basándose en los primeros mensajes, el nodo en el protocolo de cambio de vista puede determinar que la mayoría de otros nodos están en operación normal y, por lo tanto, salir del cambio de vista. Se describen más detalles a continuación con referencia a la Figura 4 a la Figura 6.

La Figura 4 ilustra un diagrama de flujo de las etapas de salida de cambio de vista 410, de acuerdo con diversas realizaciones de esta memoria descriptiva. Las etapas 410 pueden implementarse por uno o más componentes del

sistema 100 de la Figura 1 (por ejemplo, el nodo 0, el nodo 1, el nodo 2... , o el nodo i, anteriormente descritos o un dispositivo similar, o una combinación de cualquiera de los nodos y uno o más dispositivos adicionales tales como el nodo A). Las etapas 410 pueden implementarse por uno o más nodos de cadena de bloques (por ejemplo, el nodo primario, el nodo de respaldo). El nodo primario y el nodo de respaldo pueden ser aquellos definidos en el modelo de PBFT. Las etapas 410 pueden implementarse por un sistema o dispositivo de cambio de vista (por ejemplo, ordenador, servidor) que comprende diversa máquina de hardware y/o software. Por ejemplo, el sistema o dispositivo de salida de cambio de vista puede comprender uno o más procesadores y uno o más medios de almacenamiento legibles por ordenador no transitorios (por ejemplo, una o más memorias) acoplados al uno o más procesadores y configurados con instrucciones ejecutables por el uno o más procesadores para hacer que el sistema o dispositivo (por ejemplo, el procesador) realice las etapas 410. Se pretende que las operaciones que se presentan a continuación sean ilustrativas. Dependiendo de la implementación, las operaciones pueden incluir etapas adicionales, menos o alternativas realizadas en diversos órdenes o en paralelo.

En la etapa 411, un primer nodo (por ejemplo, un nodo de respaldo) puede entrar en un protocolo de cambio de vista. En la etapa 412, el primer nodo puede multidifundir un mensaje de cambio de vista. Para entrar en el cambio de vista, el primer nodo finaliza el protocolo de operación normal y entra en la fase de cambio de vista del protocolo de cambio de vista anteriormente descrito. En una realización, el primer nodo puede entrar en el protocolo de cambio de vista multidifundiendo el mensaje de cambio de vista. Por ejemplo, el primer nodo puede multidifundir el mensaje de cambio de vista al nodo primario y a otros nodos de respaldo. El primer nodo puede determinar que el nodo primario es defectuoso o que no funciona de otra manera y empezar a multidifundir el mensaje de cambio de vista de acuerdo con el protocolo de cambio de vista.

El nodo primario y los (N-1) nodos de respaldo pueden formar un sistema de consenso de PBFT. En este punto, el nodo primario verdaderamente puede o no estar no funcionando. Si el nodo primario verdaderamente no está funcionando, una mayoría de los nodos de respaldo (por ejemplo, Q nodos de respaldo) puede cada uno entrar en el protocolo de cambio de vista y cada uno multidifundir un mensaje de cambio de vista. Cuando el primer nodo obtiene Q mensajes de cambio de vista, puede determinar que la mayoría de nodos ha alcanzado un consenso de que el nodo primario no está funcionando y es necesario que se elija un nuevo nodo primario. El resto del protocolo de cambio de vista puede continuar. Sin embargo, si el nodo primario aún está funcionando, el primer nodo puede finalizar el protocolo de cambio de vista de acuerdo con las siguientes etapas. Para tales casos, el primer nodo puede haber entrado en cambio de vista debido a un error, conexión inestable y/u otras razones, que provocan un retardo al enviar y/o recibir el mensaje de preparación previa, el mensaje o mensajes de preparación, o el mensaje o mensajes de confirmación anteriormente descritos.

En la etapa 413, el segundo nodo o nodos puede cada uno multidifundir un primer mensaje. En algunas realizaciones, el segundo nodo o nodos pueden estar aún en el protocolo de operación normal y ejecutar los procedimientos anteriormente descritos (por ejemplo, recibir un mensaje de preparación previa, multidifundir un mensaje de preparación, recibir mensajes de preparación, multidifundir un mensaje de conformación, recibir mensajes de confirmación, etc.). En el protocolo de operación normal, el segundo nodo o nodos puede cada uno enviar un primer mensaje al primer nodo o multidifundir el primer mensaje de modo que el primer nodo puede obtener el primer mensaje. En algunas realizaciones, el primer mensaje puede estar incluido en el mensaje de confirmación multidifundido en la fase de confirmación. En otras realizaciones, el primer mensaje puede anexarse al mensaje de confirmación multidifundido en la fase de confirmación. En otras realizaciones más, puede enviarse o multidifundirse el primer mensaje independientemente, por ejemplo, después de que se multidifunde el mensaje de confirmación.

En una realización, el primer mensaje puede incluir una vista actual y un número de secuencia actual conocidos ambos para el segundo nodo. La vista actual puede indicar cuál de los nodos es conocido para el segundo nodo como el nodo primario. El número de secuencia actual puede indicar (1) un número de secuencia de la última solicitud (por ejemplo, solicitud de transacción) confirmada por el segundo nodo en la fase de confirmación, o (2) una altura de bloque que indica el último bloque confirmado por el segundo nodo en la fase de confirmación. La altura de bloque puede estar basada en el número de bloques en la cadena de bloques. Por ejemplo, la altura de un bloque puede ser el número de bloques en la cadena entre este y el bloque génesis). El primer bloque en la cadena de bloques puede tener una altura de bloque de 0, el siguiente bloque puede tener una altura de bloque de 1 y así sucesivamente. Este ejemplo no se pretende para limitar la manera de representación de la altura de bloque, que puede tener otros tipos de representación siempre que indiquen un número de serie del bloque en la cadena de bloques. Opcionalmente, el primer mensaje puede comprender también un resumen de la última solicitud o del último bloque.

En la etapa 414, el primer nodo puede obtener los primeros mensajes respectivamente desde los segundos nodos. En respuesta a obtener Q o más primeros mensajes consistentes, el primer nodo puede finalizar el protocolo de cambio de vista para entrar en el protocolo de operación normal. Los Q o más primeros mensajes significan que al menos Q nodos acuerdan una "vista" y "número de secuencia" consistentes. La "vista" y "número de secuencia" consistentes indican que la mayoría de los nodos están funcionando normalmente en sus protocolos de operación normal ya que han verificado por consenso satisfactoriamente una o más transacciones para la solicitud o bloque. Si el primer nodo no obtiene Q primeros mensajes con vistas y números de secuencia consistentes, el primer nodo puede seguir en el protocolo de cambio de vista.

En algunas realizaciones, el número de secuencia actual conocido para los Q o más segundos nodos es mayor que el primer número de secuencia conocido para el primer nodo (por ejemplo, mayor en uno). Esto indica que la mayoría de los nodos han completado una ronda de verificación de consenso de una solicitud o un bloque, que se perdió por el primer nodo. Por lo tanto, el primer nodo que recibe los al menos Q primeros mensajes puede conocer a través de los primeros mensajes consistentes que la mayoría de los nodos están aún en operación normal.

En algunas realizaciones, el primer nodo puede entrar en operación normal basándose en al menos la vista actual. Por ejemplo, tras la salida del cambio de vista, el primer nodo puede entrar en el protocolo de operación normal usando la vista actual como su propia vista. El primer nodo puede también sincronizar su copia de cadena de bloques con la última copia de la cadena de bloques incorporando la información (por ejemplo, el resumen) del último bloque. Por lo tanto, el primer nodo puede reanudar el protocolo de operación normal con la vista correcta y la copia actualizada de la cadena de bloques. Además, puede predecirse el tiempo que transcurre para que el primer nodo reanude la operación normal a partir de la entrada en el cambio de vista. Debido a que la altura de la cadena de bloques aumenta añadiéndose un nuevo bloque, el primer nodo puede descubrir su error por el tiempo que se añade un nuevo bloque a la cadena de bloques desde que el primer nodo entró en el cambio de vista y perdió la verificación de consenso del nuevo bloque. Por lo tanto, el tiempo que lleva reanudar la operación normal puede ser menor que el tiempo para completar una ronda de verificación de consenso.

Como tal, un nodo que entró en el cambio de vista puede finalizar de manera eficaz el protocolo de cambio de vista a través de una ruta alternativa y reunirse a otros nodos que funcionan de manera normal. Esta ruta puede ser útil para nodos que entraron en el cambio de vista, por ejemplo, debido a error, conexión inestable y/u otras razones. Esta ruta evita el protocolo de cambio de vista tradicional, que requiere Q nodos para acordar el cambio de vista para cambiar el nodo primario y reanudar la operación normal. Por lo tanto, pueden utilizarse de manera más eficaz los recursos globales de la red garantizando un número máximo de nodos en operación normal.

La Figura 5A ilustra un diagrama de flujo de un método de cambio de vista 510, de acuerdo con diversas realizaciones de esta memoria descriptiva. El método 510 pueden implementarse por uno o más componentes del sistema 100 de la Figura 1 (por ejemplo, el nodo 0, el nodo 1, el nodo 2... , o el nodo i, anteriormente descritos o un dispositivo similar, o una combinación de cualquiera de los nodos y uno o más dispositivos adicionales tales como el nodo A). El método 510 puede implementarse por uno o más nodos de cadena de bloques (por ejemplo, un nodo de respaldo en un sistema de PBFT). El nodo primario y el nodo de respaldo pueden ser aquellos definidos en el modelo de PBFT. El método 510 puede implementarse por un sistema o dispositivo de cambio de vista (por ejemplo, ordenador, servidor) que comprende diversa máquina de hardware y/o software. Por ejemplo, el sistema o dispositivo de cambio de vista puede comprender uno o más procesadores y uno o más medios de almacenamiento legibles por ordenador no transitorios (por ejemplo, una o más memorias) acoplados al uno o más procesadores y configurados con instrucciones ejecutables por el uno o más procesadores para hacer que el sistema o dispositivo (por ejemplo, el procesador) realice el método 510. Se pretende que las operaciones del método 510 que se presentan a continuación sean ilustrativas. Dependiendo de la implementación, el método 510 puede incluir etapas adicionales, menos etapas o etapas alternativas realizadas en diversos órdenes o en paralelo. Puede hacerse referencia a detalles adicionales del método 510 en la Figura 1 a la Figura 4 y en las descripciones relacionadas anteriores. El método 510 puede realizarse por un primer nodo.

En diversas realizaciones, el método 510 puede ser un método de cambio de vista implementado por ordenador para implementarse en una cadena de bloques mantenida por un número (N) de nodos (por ejemplo, nodos de un sistema de consenso de PBFT). En una realización, los N nodos forman una red de Tolerancia Práctica a Fallos Bizantinos (PBFT), en la que uno de los N nodos actúa como el nodo primario y los otros (N-1) nodos actúan como nodos de respaldo. El método 510 puede realizarse por un primer nodo (por ejemplo, el nodo de respaldo) de los N nodos que está en un protocolo de cambio de vista.

En algunas realizaciones, antes del bloque 511, el primer nodo puede haber entrado en cambio de vista. A medida que se entra en el cambio de vista, el primer nodo puede multidifundir un mensaje de cambio de vista a los otros nodos. Por ejemplo, el primer nodo puede ser un nodo de respaldo y puede multidifundir el mensaje de cambio de vista al nodo primario y a otros nodos de respaldo. El nodo primario y los nodos de respaldo pueden formar un sistema de consenso de PBFT. El mensaje de cambio de vista indica que el primer nodo ha salido de su protocolo de operación normal y ha entrado en un protocolo de cambio de vista. Si el primer nodo no recibe (Q-1) mensajes de cambio de vista similares desde otros nodos (obteniendo así un total de Q mensajes de cambio de vista consistentes que incluyen su propio mensaje de cambio de vista), no se cumplirá el umbral para el protocolo de cambio de vista tradicional. Independientemente, las siguientes etapas pueden permitir que el primer nodo finalice el protocolo de cambio de vista y entre en el protocolo de operación normal.

El bloque 511 incluye obtener, respectivamente desde al menos Q segundos nodos de los N nodos, al menos Q primeros mensajes que cada uno comprende (1) una vista actual consistente conocida para el segundo nodo que indica un nodo primario designado entre los N nodos y (2) un número de secuencia actual consistente conocido para el segundo nodo, el número de secuencia actual asociado a un último bloque o una última transacción confirmada por el segundo nodo, en donde el número de secuencia actual es mayor que un primer número de secuencia conocido para el primer nodo (por ejemplo, mayor en uno), Q (quórum) es (N+F+1)/2 redondeado arriba hasta el número entero

más cercano, y F es (N-1)/3 redondeado abajo hasta el número entero más cercano. N puede ser cualquier número entero no menor que cuatro. En algunas realizaciones, cuando N es al menos (3F+1), Q es (2F+1). El número de secuencia actual asociado a la última transacción puede comprender, por ejemplo, un número de secuencia de una o más últimas transacciones confirmadas por el correspondiente segundo nodo. El número de secuencia actual asociado al último bloque puede comprender, por ejemplo, una altura de una copia de la cadena de bloques mantenida por el correspondiente segundo nodo. Como se ha descrito anteriormente, la altura de la cadena de bloques puede depender del número de bloques en la cadena de bloques y aumentarse con una adición del último bloque. En una realización, para que el primer nodo finalice el cambio de vista, los al menos Q primeros mensajes pueden incluir vistas actuales consistentes y números de secuencia actuales consistentes. El bloque 512 incluye, en respuesta a obtener los al menos Q primeros mensajes, finalizar el protocolo de cambio de vista.

En algunas realizaciones, el término "transacción" puede implementarse mediante un sistema de cadena de bloques y registrarse en la cadena de bloques. La transacción puede incluir, por ejemplo, una transacción financiera, una transacción de contrato de cadena de bloques para implementar o invocar un contrato de cadena de bloques, una transacción que actualiza un estado (por ejemplo, estado mundial) de la cadena de bloques, etc. La transacción no tiene que implicar un intercambio financiero.

En algunas realizaciones, obtener los al menos Q primeros mensajes comprende: obtener, respectivamente desde los al menos Q segundos nodos, al menos Q mensajes de confirmación que indican que los al menos Q segundos nodos acuerdan un siguiente bloque para añadir a la cadena de bloques, comprendiendo los Q mensajes de confirmación respectivamente los Q primeros mensajes. Por ejemplo, el mensaje de confirmación puede comprender la vista actual y el número de secuencia actual.

En otras realizaciones, obtener los al menos Q primeros mensajes comprende: obtener, respectivamente desde los al menos Q segundos nodos, al menos Q mensajes de confirmación que indican que los al menos Q segundos nodos acuerdan un siguiente bloque para añadir a la cadena de bloques, los Q primeros mensajes respectivamente anexados a los Q mensajes de confirmación. Por ejemplo, el primer mensaje puede enviarse o multidifundirse con el mensaje de confirmación por el segundo nodo.

En diversas realizaciones, la vista actual para los al menos Q segundos nodos es v; y cuando en el protocolo de cambio de vista, el primer nodo tiene una primera vista mayor que v. Por ejemplo, el primer y segundo nodos pueden todos tener la vista v antes de que el primer nodo entrara en el cambio de vista, pero luego el primer nodo sospecha que el primer nodo no funcionaba y ha entrado en el cambio de vista con la vista v+1, mientras que los segundos nodos todavía están en la vista v.

En algunas realizaciones, el número de secuencia actual comprende una altura de una segunda copia de la cadena de bloques (también conocida como altura de bloque) mantenida por el segundo nodo; y el primer número de secuencia comprende una altura de una primera copia de la cadena de bloques mantenida por el primer nodo. En una realización, el número de secuencia actual conocido para los al menos Q segundos nodos es (n+1); y el primer número de secuencia conocido para primer nodo es n. Por ejemplo, antes de que el primer nodo entrara en el cambio de vista, el primer y segundo nodos pueden todos haber empezado con una cadena de bloques de altura de bloque de 99 (es decir, 100 bloques en la cadena de bloques) en la vista v. Después de que el primer nodo haya entrado en el protocolo de cambio de vista antes de entrar en la fase de confirmación (por ejemplo, multidifundiendo un mensaje de confirmación) y, por lo tanto, se saliera de la verificación de consenso, los segundos nodos han alcanzado un consenso en el bloque de orden 101 y de esta manera, han aumentado la altura de bloque a 100. El bloque de orden 101 desconocido para el primer nodo atascado en el protocolo de cambio de vista puede causar la diferencia entre el número de secuencia actual (100) y el primer número de secuencia (99).

En otras realizaciones, el número de secuencia actual comprende un número de secuencia de la última transacción confirmada por el segundo nodo; y el primer número de secuencia comprende un número de secuencia de una última transacción confirmada por el primer nodo. En una realización, el número de secuencia actual conocido para los al menos Q segundos nodos es (n+1); y el primer número de secuencia conocido para el primer nodo es n. Por ejemplo, antes de que el primer nodo entre en el cambio de vista, el primer y segundo nodos pueden todos haber empezado con 80 solicitudes (por ejemplo, solicitudes de transacción) para verificación de consenso. Las solicitudes pueden tener asignados números de secuencia crecientes. En la vista v, el primer y segundo nodos pueden tener 50 solicitudes verificadas por consenso. Después de que el primer nodo haya entrado en el protocolo de cambio de vista antes de entrar en la fase de confirmación (por ejemplo, multidifundiendo un mensaje de confirmación) y, por lo tanto, salió de la verificación de consenso, los segundos nodos han alcanzado un consenso en la solicitud de orden 51 y, de esta manera, aumentaron el número de secuencia de una siguiente solicitud pendiente a 52. La solicitud de orden 51 que se ha verificado como consenso es desconocida para el primer nodo atascado en el protocolo de cambio de vista y puede causar la diferencia entre el número de secuencia actual (51) y el primer número de secuencia (50).

En algunas realizaciones, el primer mensaje comprende adicionalmente un resumen del último bloque o la última transacción. El resumen (por ejemplo, un valor de función de troceo) puede ser el resultado numérico de la aplicación de un algoritmo de función de troceo a los datos, tales como las transacciones. En una realización, el resumen comprende un valor de función de troceo del último bloque o la última transacción. En un ejemplo, el resumen

comprende una función de troceo de transacción de la última transacción confirmada por el segundo nodo, pero no confirmada por el primer nodo. En otro ejemplo, el resumen comprende funciones de troceo de transacción de las últimas transacciones confirmadas por el segundo nodo, pero no confirmadas por el primer nodo. En otro ejemplo, el resumen comprende una raíz de Merkle del último bloque conocido para el segundo nodo, pero desconocido para el primer nodo. En otro ejemplo, el resumen comprende raíces de Merkle de los últimos bloques conocidos para el segundo nodo, pero desconocidos para el primer nodo.

En algunas realizaciones, la "vista", "número de secuencia" y/o "resumen" pueden incluirse en el primer mensaje como una o más firmas digitales (o firmas por brevedad). El primer mensaje comprende una firma digital que certifica la vista actual y el número de secuencia actual ambos conocidos para el segundo nodo. La "firma" muestra el endoso de la entidad que envió el correspondiente mensaje. El término "firma" puede ser cualquier forma de indicación de aprobación. En una realización, la "vista", "número de secuencia" y/o "resumen" pueden introducirse en primer lugar en una función de troceo unidireccional, el valor de función de troceo de salida el cual está encriptado con la correspondiente clave privada del nodo para obtener la firma digital. La encriptación puede conseguirse a través de diversas maneras, tales como Encriptación de Clave Pública-Privada (también conocida como criptografía asimétrica), Algoritmo de Firma Digital (DSA) tal como Algoritmo de Firma Digital de Curva Elíptica (ECDSA), etc. Por ejemplo, usando un algoritmo de clave pública, tal como RSA, pueden generarse dos claves que estén vinculadas matemáticamente: una privada y una pública. Las firmas digitales funcionan puesto que la criptografía de clave pública depende de dos claves criptográficas que se autentican mutuamente. El nodo que crea la firma digital puede usar su propia clave privada para encriptar la "vista", el "número de secuencia" y/o el "resumen"; la única manera para desencriptar esos datos es con la clave pública del nodo firmante. Por lo tanto, la firma digital puede representar la "vista", el "número de secuencia" y/o el "resumen" conocidos para el correspondiente nodo.

En algunas realizaciones, finalizar el protocolo de cambio de vista comprende: sincronizar una primera copia de la cadena de bloques mantenida por el primer nodo con una segunda copia de la cadena de bloques mantenida por el segundo nodo; y salir del protocolo de cambio de vista para entrar en un protocolo de operación normal usando la vista actual consistente para el primer nodo. Por lo tanto, si los segundos nodos están en la vista v y el primer nodo se atascó en la vista (v+1), el primer nodo puede finalizar el protocolo de cambio de vista y entrar en el protocolo de operación normal en la vista v.

La Figura 5B ilustra un diagrama de flujo de un método de cambio de vista 520, de acuerdo con diversas realizaciones de esta memoria descriptiva. El método 520 pueden implementarse por uno o más componentes del sistema 100 de la Figura 1 (por ejemplo, el nodo 0, el nodo 1, el nodo 2... , o el nodo i, anteriormente descritos o un dispositivo similar, o una combinación de cualquiera de los nodos y uno o más dispositivos adicionales tales como el nodo A). El método 520 puede implementarse por uno o más nodos de cadena de bloques (por ejemplo, un nodo primario o un nodo de respaldo en un sistema de PBFT). El nodo primario y el nodo de respaldo pueden ser aquellos definidos en el modelo de PBFT. El método 520 puede implementarse por un sistema o dispositivo de cambio de vista (por ejemplo, ordenador, servidor) que comprende diversa máquina de hardware y/o software. Por ejemplo, el sistema o dispositivo de cambio de vista puede comprender uno o más procesadores y uno o más medios de almacenamiento legibles por ordenador no transitorios (por ejemplo, una o más memorias) acoplados al uno o más procesadores y configurados con instrucciones ejecutables por el uno o más procesadores para hacer que el sistema o dispositivo (por ejemplo, el procesador) realice el método 520. Se pretende que las operaciones del método 520 que se presentan a continuación sean ilustrativas. Dependiendo de la implementación, el método 520 puede incluir etapas adicionales, menos etapas o etapas alternativas realizadas en diversos órdenes o en paralelo. Puede hacerse referencia a detalles adicionales del método 520 en la Figura 1 a la Figura 4 y en las descripciones relacionadas anteriores. El método 520 puede realizarse por un segundo nodo. Si el segundo nodo es un nodo primario, el segundo nodo puede realizar las etapas 521a, 522a, 523, 524, 525 y 526. Si el segundo nodo es un nodo de respaldo, el segundo nodo puede realizar las etapas 521b, 522b, 523, 524, 525 y 526.

El bloque 521a incluye obtener, por un segundo nodo (por ejemplo, un nodo primario), una o más solicitudes (por ejemplo, solicitudes de transacción). La solicitud puede implicar una transacción de cadena de bloques (con o sin un contrato inteligente) para la verificación de consenso. En un ejemplo, las solicitudes pueden corresponder a transacciones para que se verifiquen por consenso y se añadan a la cadena de bloques. La verificación de consenso puede realizarse durante la ejecución de una ronda del protocolo de operación normal. Como alternativa, las solicitudes pueden corresponder a otras operaciones. En algunas realizaciones, un nodo primario puede obtener la solicitud desde un cliente (por ejemplo, un nodo ligero) o desde un nodo de respaldo que obtiene la solicitud desde el cliente y reenvió la solicitud al nodo primario.

El bloque 522a incluye multidifundir un mensaje de preparación previa y las solicitudes a los nodos de respaldo. En algunas realizaciones, después de obtener múltiples solicitudes, el segundo nodo puede multidifundir el mensaje de preparación previa y las solicitudes a cada uno de los nodos de respaldo. El mensaje de preparación previa puede incluir un orden para las solicitudes (por ejemplo, un orden para transacciones asociadas con las solicitudes). El orden puede comprender el número de secuencia para cada solicitud y/o el número de secuencia para que se añada el siguiente bloque a la cadena de bloques.

El bloque 521b incluye obtener, por el segundo nodo (por ejemplo, un nodo de respaldo), un mensaje de preparación

previa y la una o más solicitudes. Por ejemplo, el mensaje de preparación previa y las solicitudes pueden obtenerse por un nodo de respaldo desde un nodo primario. De manera similar, el nodo de respaldo puede obtener el mensaje de preparación previa y las solicitudes con el orden para ejecutar las solicitudes.

El bloque 522b incluye multidifundir un mensaje de preparación si el segundo nodo acepta el mensaje de preparación previa. Multidifundir puede significar difundir. Por ejemplo, el mensaje de preparación puede multidifundirse por un nodo de respaldo al nodo primario y a otros nodos de respaldo.

El bloque 523 incluye obtener (Q-1) o más mensajes de preparación. En algunas realizaciones, Q (quórum) es (N+F+1)/2 redondeado arriba hasta el número entero más cercano, y F es (N-1)/3 redondeado abajo hasta el número entero más cercano, que representa un número máximo de nodos que no funcionan permitidos entre los N nodos para mantener un sistema de consenso de los N nodos que funcionan. Obtener (Q-1) o más mensajes de preparación puede ser una condición para que se cumpla antes de entrar en la fase de confirmación. El (Q-1) o más mensajes de preparación pueden incluir el correspondiente mensaje de preparación de multidifusión del propio nodo.

El bloque 524 incluye multidifundir a otros nodos un mensaje de confirmación que comprende (1) una vista actual que indica un nodo primario conocido para el segundo nodo y (2) un número de secuencia actual conocido para el segundo nodo. En algunas realizaciones, el mensaje de confirmación de multidifusión comprende una o más firmas digitales que encriptan la vista actual y el número de secuencia actual.

En algunas realizaciones, el mensaje de confirmación comprende adicionalmente un resumen de una o más transacciones asociadas con la solicitud. Por ejemplo, el resumen puede comprender una función de troceo de transacción de una última transacción confirmada o una raíz de Merkle Trie de un último bloque de la cadena de bloques.

En algunas realizaciones, el segundo nodo no ha entrado en el cambio de vista; y el número de secuencia actual conocido para el segundo nodo es mayor que un primer número de secuencia conocido para un primer nodo que ha entrado en el cambio de vista (por ejemplo, en uno).

En algunas realizaciones, pueden no estar funcionando hasta F nodos. A pesar de eso, el método descrito y la verificación de consenso pueden llevarse a cabo de manera apropiada, ya que el sistema de PBFT tolera hasta F nodos que no funcionan.

El bloque 525 incluye obtener al menos Q mensajes de confirmación. Los Q mensajes de confirmación pueden incluir el correspondiente mensaje de confirmación de multidifusión del propio nodo.

El bloque 526 incluye ejecutar la una o más solicitudes. Por ejemplo, la una o más solicitudes pueden verificarse en consenso y añadirse en correspondencia a las copias locales de la cadena de bloques. Como resultado, si suficientes nodos (por ejemplo, Q nodos) han verificado la correspondiente transacción, la transacción se empaqueta en la cadena de bloques.

La Figura 6 ilustra un diagrama de bloques de un sistema de cambio de vista 610, de acuerdo con diversas realizaciones. El sistema de cambio de vista 610 (por ejemplo, un sistema informático) puede ser un ejemplo de una implementación del nodo 0, el nodo 1, el nodo 2... , o el nodo i anteriormente descritos o un dispositivo similar, o una combinación de cualquiera de los nodos y un dispositivo adicional (por ejemplo, el nodo A). El método 510 puede implementarse por el sistema de cambio de vista 610. El sistema de cambio de vista 610 puede comprender uno o más procesadores y uno o más medios de almacenamiento legibles por ordenador no transitorios (por ejemplo, una o más memorias) acoplados al uno o más procesadores y configurados con instrucciones ejecutables por el uno o más procesadores para hacer que el sistema o dispositivo (por ejemplo, el procesador) realice el método 510. El sistema de cambio de vista 610 puede comprender diversas unidades/módulos que corresponden a las instrucciones (por ejemplo, instrucciones de software).

En algunas realizaciones, el sistema de cambio de vista 610 puede denominarse como un aparato de cambio de vista. El aparato de cambio de vista puede ser para mantener una cadena de bloques, en donde un número (N) de nodos mantiene la cadena de bloques con uno de los N nodos actuando como un nodo primario y actuando los otros (N-1) como nodos de respaldo, actuando el aparato de consenso como un primer nodo de los N nodos que está en un protocolo de cambio de vista. El aparato de consenso puede comprender uno o más procesadores y una o más memorias legibles por ordenador no transitorias acopladas al uno o más procesadores y configuradas con instrucciones ejecutables por el uno o más procesadores para hacer que el aparato realice las operaciones. El sistema de consenso puede comprender diversas unidades/módulos que corresponden a las instrucciones (por ejemplo, instrucciones de software). El aparato de consenso puede comprender un módulo de obtención 611 para obtener, respectivamente desde al menos Q segundos nodos de los N nodos, al menos Q primeros mensajes que comprende cada uno (1) una vista actual consistente conocida para el segundo nodo que indica un nodo primario designado entre los N nodos y (2) un número de secuencia actual consistente conocido para el segundo nodo, el número de secuencia actual asociado a un último bloque o una última transacción confirmada por el segundo nodo, en donde el número de secuencia actual es mayor que un primer número de secuencia conocido para el primer nodo, Q (quórum) es (N+F+1)/2

redondeado arriba hasta el número entero más cercano, y F es (N-1)/3 redondeado abajo hasta el número entero más cercano; y un módulo de finalización 612 para, en respuesta a obtener los al menos Q primeros mensajes, finalizar el protocolo de cambio de vista.

Las técnicas descritas en este documento se implementan mediante uno o más dispositivos informáticos de uso especial. Los dispositivos informáticos de uso especial pueden ser sistemas informáticos de escritorio, sistemas informáticos servidores, sistemas informáticos portátiles, dispositivos portátiles, dispositivos de red o cualquier otro dispositivo o combinación de dispositivos que incorpora lógica por cable y/o de programa para implementar las técnicas. Los dispositivos informáticos de fin especial pueden implementarse como ordenadores personales, portátiles, teléfonos celulares, teléfonos de cámara, teléfonos inteligentes, asistentes digitales personales, reproductores de medios, dispositivos de navegación, dispositivos de correo electrónico, consolas de juegos, ordenadores de tableta, dispositivos llevables, o una combinación de los mismos. El o los dispositivos informáticos generalmente están controlados y coordinados por el software del sistema operativo. Los sistemas operativos convencionales controlan y programan procesos informáticos para su ejecución, realizan gestión de memoria, proporcionan sistema de archivos, interconexión en red, servicios de E/S y proporcionan una funcionalidad de interfaz de usuario, tal como una interfaz gráfica de usuario ("GUI"), entre otras cosas. Los diversos sistemas, aparatos, medios de almacenamiento, módulos, y unidades descritas en el presente documento pueden implementarse en los dispositivos informáticos de fin especial, o en uno o más chips informáticos del uno o más dispositivos informáticos de fin especial. En algunas realizaciones, las instrucciones descritas en el presente documento pueden implementarse en una máquina virtual en el dispositivo informático de fin especial. Cuando se ejecutan, las instrucciones pueden hacer que el dispositivo informático de fin especial realice diversos métodos descritos en el presente documento. La máquina virtual puede incluir un software, hardware o una combinación de los mismos. Por ejemplo, la máquina virtual puede incluir un software de Máquina Virtual de Ethereum (EVM) que proporciona el entorno de tiempo de ejecución para contratos inteligentes en Ethereum.

La Figura 7 es un diagrama de bloques que ilustra un sistema informático 700 en el que se puede implementar cualquiera de las realizaciones descritas en el presente documento. El sistema 700 puede realizar cualquiera de los métodos descritos en el presente documento (por ejemplo, el método de cambio de vista 510, el método de cambio de vista 520). El sistema 700 puede implementarse en cualquiera de los sistemas descritos en el presente documento (por ejemplo, el sistema de cambio de vista 610). El sistema 700 puede implementarse en cualquiera de los nodos descritos en el presente documento y configurarse para realizar correspondientes etapas para implementar el contrato de cadena de bloques. El sistema informático 700 incluye un bus 702 u otro mecanismo de comunicación para comunicar información, y uno o más procesador o procesadores de hardware 704 acoplados con el bus 702 para procesar información. El procesador o procesadores de hardware 704 pueden ser, por ejemplo, uno o más microprocesadores de fin general.

El sistema informático 700 también incluye una memoria principal 706, tal como una memoria de acceso aleatorio (RAM), caché y/u otros dispositivos de almacenamiento dinámico, acoplados al bus 702 para almacenar información e instrucciones ejecutables por el procesador o procesadores 704. La memoria principal 706 puede usarse también para almacenar variables temporales u otra información intermedia durante la ejecución de instrucciones ejecutables por el procesador o los procesadores 704. Tales instrucciones, cuando se almacenan en medios de almacenamiento accesibles al procesador o procesadores 704, representan el sistema informático 700 en una máquina de uso especial que se personaliza para realizar las operaciones especificadas en las instrucciones. El sistema informático 700 incluye adicionalmente una memoria de solo lectura (ROM) 708 u otro dispositivo de almacenamiento estático acoplado al bus 702 para almacenar información estática e instrucciones para el procesador o procesadores 704. Se proporciona un dispositivo de almacenamiento 710, tal como un disco magnético, un disco óptico o una unidad de memoria USB (unidad flash), etc., y se acopla al bus 702 para almacenar información e instrucciones.

El sistema informático 700 puede implementar las técnicas descritas en el presente documento usando lógica de cableado permanente personalizada, uno o más ASIC o FPGA, firmware y/o lógica de programa que, en combinación con el sistema informático, provoca o programa al sistema informático 700 para que sea una máquina de fin especial. De acuerdo con una realización, las operaciones, métodos y procesos descritos en el presente documento son realizados por el sistema informático 700 en respuesta a que el procesador o procesadores 704 ejecuten una o más secuencias de una o más instrucciones contenidas en la memoria principal 706. Tales instrucciones pueden leerse en la memoria principal 706 desde otro medio de almacenamiento, tal como el dispositivo de almacenamiento 710. La ejecución de las secuencias de instrucciones contenidas en la memoria principal 706 provoca que el procesador o procesadores 704 realicen las etapas del proceso descritas en el presente documento. En realizaciones alternativas, puede usarse circuitería de cableado permanente en lugar de o en combinación con instrucciones de software.

La memoria principal 706, la ROM 708, y/o el almacenamiento 710 pueden incluir medios de almacenamiento no transitorios. La expresión "medios no transitorios" y términos similares, como se usan en el presente documento, se refieren a medios que almacenan datos y/o instrucciones que hacen que una máquina funcione de una manera específica, los medios excluyen las señales transitorias. Tales medios no transitorios pueden comprender medios no volátiles y/o medios volátiles. Los medios no volátiles incluyen, por ejemplo, discos ópticos o magnéticos, tales como un dispositivo de almacenamiento 710. Los medios volátiles incluyen memoria dinámica, tal como la memoria principal 706. Las formas comunes de medios no transitorios incluyen, por ejemplo, un disco flexible, un disco flexible, un disco duro, disco de estado sólido, cinta magnética, o cualquier otro medio de almacenamiento de datos magnético, un CD-

ROM, cualquier otro medio de almacenamiento de datos óptico, cualquier medio físico con patrones de orificios, una RAM, una PROM y EPROM, una FLASH-EPROM, NVRAM, cualquier otro chip o cartucho de memoria y versiones en red de los mismos.

El sistema informático 700 también incluye una interfaz de comunicación 718 acoplada al bus 702. La interfaz de red 718 proporciona un acoplamiento de comunicación de datos bidireccional a uno o más enlaces de red que están conectados a una o más redes locales. Por ejemplo, la interfaz de red 718 puede ser una tarjeta de red digital de servicios integrados (ISDN), módem por cable, módem por satélite o un módem para proporcionar una conexión de comunicación de datos a un correspondiente tipo de línea telefónica. Como otro ejemplo, la interfaz de red 718 puede ser una tarjeta de red de área local (LAN) para proporcionar una conexión de comunicación de datos a una LAN compatible (o componente WAN para comunicarse con una WAN). También pueden implementarse enlaces inalámbricos. En cualquier implementación de este tipo, la interfaz de red 718 envía y recibe señales eléctricas, electromagnéticas u ópticas que transportan flujos de datos digitales que representan diversos tipos de información.

El sistema informático 700 puede enviar mensajes y recibir datos, incluyendo código de programa, a través de la red o redes, el enlace de red y la interfaz de comunicación 718. En el ejemplo de Internet, un servidor podría transmitir un código solicitado para un programa de aplicación a través de Internet, el ISP, la red local y la interfaz de red 718.

El código recibido puede ejecutarse mediante el procesador o procesadores 704 como se recibió, y/o almacenarse en el dispositivo de almacenamiento 710, u otro almacenamiento no volátil para su ejecución posterior.

Cada uno de los procesos, métodos y algoritmos descritos en las secciones anteriores puede estar incorporado y automatizado total o parcialmente por módulos de código ejecutados por uno o más sistemas informáticos o procesadores informáticos que comprenden hardware informático. Los procesos y algoritmos pueden implementarse parcial o totalmente en circuitería específica de la aplicación.

Las diversas características y procesos anteriormente descritos pueden usarse de manera independiente unos de otros, o pueden combinarse de diversas maneras. Se pretende que todas las posibles combinaciones y subcombinaciones entren dentro del alcance de la presente memoria descriptiva. Además, ciertos bloques de métodos o proceso pueden omitirse en algunas implementaciones. Los métodos y procesos descritos en el presente documento tampoco están limitados a ninguna secuencia particular y los bloques o estados relacionados con los mismos pueden realizarse en otras secuencias que sean apropiadas. Por ejemplo, los bloques o estados descritos pueden realizarse en un orden distinto del específicamente desvelado o múltiples bloques o estados pueden combinarse en un único bloque o estado. Los ejemplos de bloques o estados pueden realizarse en serie, en paralelo o en alguna otra manera. Los bloques o estados pueden añadirse a o retirarse de las realizaciones desveladas. Los ejemplos de sistemas y componentes descritos en el presente documento pueden configurarse de manera diferente a lo descrito. Por ejemplo, pueden añadirse elementos, eliminarse, o reorganizarse en comparación con las realizaciones de desveladas.

Las diversas operaciones de los métodos descritos en el presente documento pueden realizarse, al menos parcialmente, por uno o más procesadores que están configurados temporalmente (por ejemplo, por software) o configurados permanentemente para realizar las operaciones relevantes. Ya sea que estén configurados de forma temporal o permanente, dichos procesadores pueden constituir motores implementados por procesadores que operan para realizar una o más operaciones o funciones descritas en el presente documento.

De manera similar, los métodos descritos en el presente documento pueden implementarse al menos parcialmente con un procesador, siendo un procesador o procesadores particulares un ejemplo de hardware. Por ejemplo, al menos algunas de las operaciones de un método pueden realizarse por uno o más procesadores o motores implementados por procesador. Además, el uno o más procesadores también pueden operar para soportar la realización de las operaciones relevantes en un entorno de "informática en la nube" o como un "software como servicio" (SaaS). Por ejemplo, al menos algunas de las operaciones pueden realizarse por un grupo de ordenadores (como ejemplos de máquinas que incluyen procesadores), siendo estas operaciones accesibles a través de una red (por ejemplo, Internet) y a través de una o más interfaces apropiadas (por ejemplo, una Interfaz de Programa de Aplicación (API)).

El rendimiento de algunas de las operaciones puede distribuirse entre los procesadores, que no solo se encuentran dentro de una sola máquina, sino que están desplegados en varias máquinas. En algunas realizaciones, los procesadores o motores implementados por procesador pueden ubicarse en una única ubicación geográfica (por ejemplo, dentro de un entorno doméstico, un entorno de oficina o una granja de servidores). En otras realizaciones, los procesadores o motores implementados por procesador pueden distribuirse a través de varias ubicaciones geográficas.

A lo largo de la presente memoria descriptiva, varias instancias pueden implementar componentes, operaciones o estructuras descritas como una única instancia. Aunque las operaciones individuales de uno o más métodos se ilustran y describen como operaciones separadas, una o más de las operaciones individuales pueden realizarse simultáneamente y nada requiere que las operaciones se realicen en el orden ilustrado. Las estructuras y la funcionalidad presentadas como componentes separados en las configuraciones se pueden implementar como una estructura o componente combinado. De forma similar, las estructuras y la funcionalidad presentadas como un único

componente se pueden implementar como componentes separados. Estas y otras variaciones, modificaciones, adiciones y mejoras entran dentro del alcance de la materia objeto del presente documento. Adicionalmente, los términos relacionados (tales como "primero", "segundo", "tercero" etc.) usados en el presente documento no indican cualquier orden, altura, o importancia, sino que en su lugar se usan para distinguir un elemento de otro elemento. Adicionalmente, los términos "un" "una" y "pluralidad" no indican una limitación de cantidad en el presente documento, sino que en su lugar indican la presencia de al menos uno de los artículos mencionados.

Aunque se ha descrito una vista general de la materia objeto con referencia a realizaciones específicas, pueden realizarse diversas modificaciones y cambios a estas realizaciones sin alejarse del ámbito más amplio de las realizaciones de esta memoria descriptiva.

REIVINDICACIONES

1. Un método implementado por ordenador para finalizar un cambio de vista en un mecanismo de Tolerancia Práctica a Fallos Bizantinos, PBFT, en un primer nodo para implementarse en una cadena de bloques mantenida por un número (N) de nodos donde N es mayor de 1, el método realizado por el primer nodo de los N nodos que se encuentra en un protocolo de cambio de vista, comprendiendo el método:

obtener, respectivamente desde al menos un quórum de Q segundos nodos de los N nodos, al menos Q primeros mensajes que cada uno comprende (a) una vista actual consistente conocida para el segundo nodo que indica un nodo primario designado entre los N nodos y (b) un número de secuencia actual consistente conocido para el segundo nodo, el número de secuencia actual asociado a un último bloque o una última transacción confirmada por el segundo nodo, en donde el número de secuencia actual es mayor que un primer número de secuencia conocido para el primer nodo, en donde el quórum Q es (N+F+1)/2 redondeado arriba hasta el número entero más cercano, y F es (N-1)/3 redondeado abajo hasta el número entero más cercano;
en respuesta a obtener los al menos Q primeros mensajes, sincronizar una primera copia de la cadena de bloques mantenida por el primer nodo con una segunda copia de la cadena de bloques mantenida por un segundo nodo; y
salir del protocolo de cambio de vista para entrar en un protocolo de operación normal del PBFT usando la vista actual consistente para el primer nodo.

2. El método de la reivindicación 1, en donde la obtención de los al menos Q primeros mensajes comprende:
obtener, respectivamente desde los al menos Q segundos nodos, al menos Q mensajes de confirmación que indican que los al menos Q segundos nodos acuerdan un siguiente bloque para añadir a la cadena de bloques, comprendiendo los Q mensajes de confirmación respectivamente los Q primeros mensajes.

3. El método de la reivindicación 1, en donde la obtención de los al menos Q primeros mensajes comprende:
obtener, respectivamente desde los al menos Q segundos nodos, al menos Q mensajes de confirmación que indican que los al menos Q segundos nodos acuerdan un siguiente bloque para añadir a la cadena de bloques, los Q primeros mensajes respectivamente anexados a los Q mensajes de confirmación.

4. El método de cualquiera de las reivindicaciones 1-3, en donde:

el número de secuencia actual comprende una altura de una segunda copia de la cadena de bloques mantenida por el segundo nodo; y
el primer número de secuencia comprende una altura de una primera copia de la cadena de bloques mantenida por el primer nodo.

5. El método de cualquiera de las reivindicaciones 1-3, en donde:

el número de secuencia actual comprende un número de secuencia de la última transacción confirmada por el segundo nodo; y
el primer número de secuencia comprende un número de secuencia de una última transacción confirmada por el primer nodo.

6. El método de cualquier reivindicación anterior, en donde:
el primer mensaje comprende una firma digital que certifica la vista actual y el número de secuencia actual, ambos conocidos para el segundo nodo.

7. El método de cualquier reivindicación anterior, en donde:
el primer mensaje comprende adicionalmente un resumen del último bloque o de la última transacción.

8. El método de la reivindicación 7, en donde:
el resumen comprende un valor de función de troceo del último bloque o de la última transacción.

9. El método de cualquiera de las reivindicaciones 7 y 8, en donde:
el resumen comprende una raíz de Merkle del último bloque conocido para el segundo nodo, pero desconocido para el primer nodo.

10. El método de cualquier reivindicación anterior, en donde:

el número de secuencia actual conocido para los al menos Q segundos nodos es (n+1); y
el primer número de secuencia conocido para el primer nodo es n.

11. El método de cualquier reivindicación anterior, en donde:

la vista actual para los al menos Q segundos nodos es v; y
cuando está en el protocolo de cambio de vista, el primer nodo tiene una primera vista mayor que v.

12. El método de cualquier reivindicación anterior, en donde:
en la red de Tolerancia Práctica a Fallos Bizantinos (PBFT), uno de los N nodos actúa como el nodo primario y los otros (N-1) nodos actúan como nodos de respaldo.

13. Un sistema de cambio de vista, que comprende:

uno o más procesadores; y
una o más memorias legibles por ordenador acopladas a los uno o más procesadores y que tienen instrucciones almacenadas en las mismas que son ejecutables por los uno o más procesadores para realizar el método de cualquiera de las reivindicaciones 1 a 12.

14. Un aparato de cambio de vista, que comprende una pluralidad de módulos para realizar el método de cualquiera de las reivindicaciones 1 a 12.

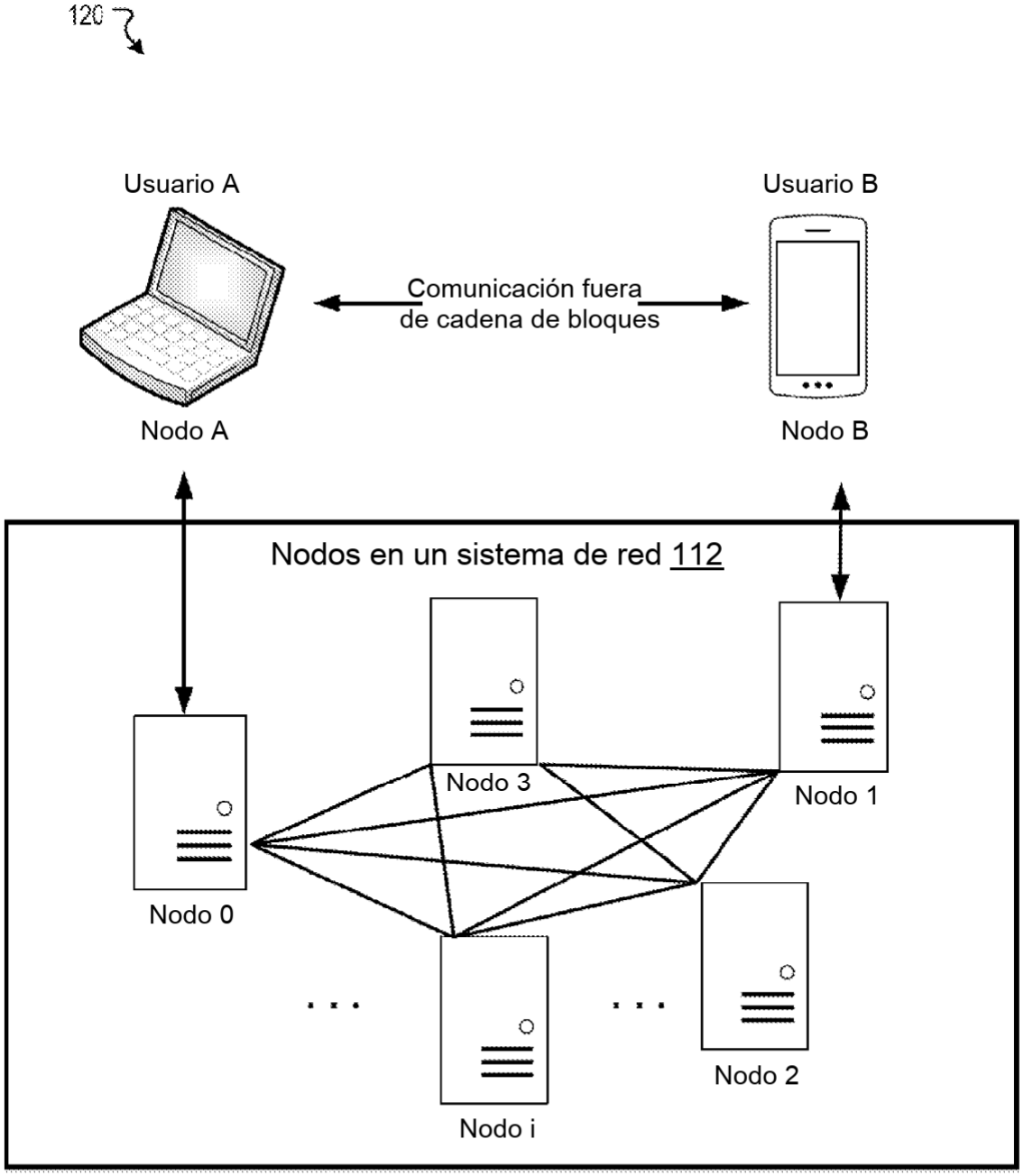

120
Usuario A
Usuario B
Comunicación fuera
de cadena de bloques
Nodo A
Nodo B
Nodos en un sistema de red 112
Nodo 3
Nodo 1
Nodo 0
Nodo 2
Nodo i

FIG. 1

Protocolo de operación normal

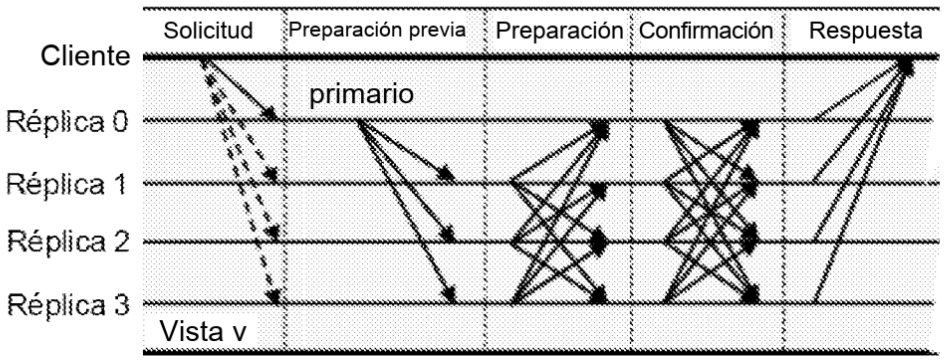


FIG. 2A

Protocolo de operación normal con un nodo de respaldo defectuoso

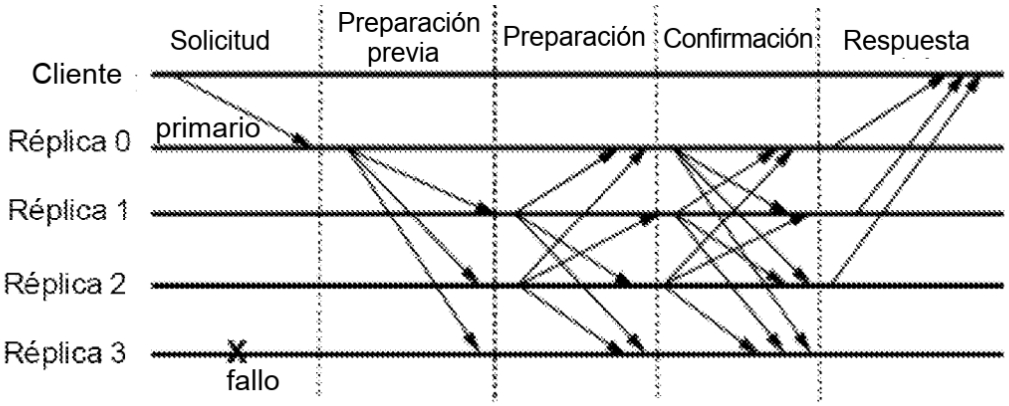


FIG. 2B

Protocolo de operación normal

Protocolo de cambio de vista

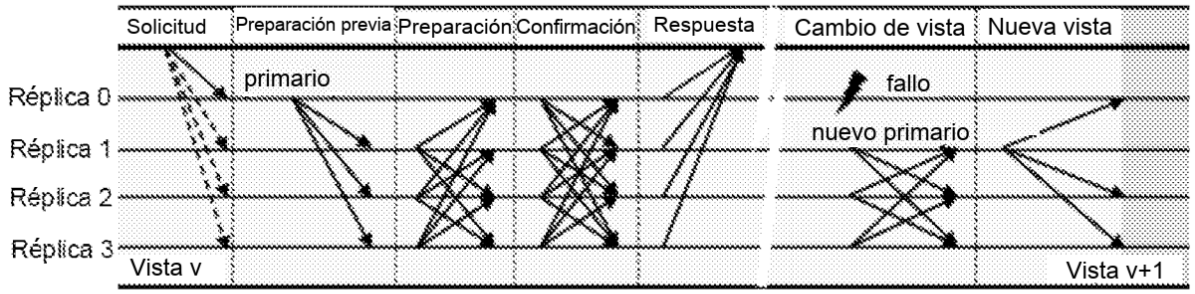


FIG. 2C

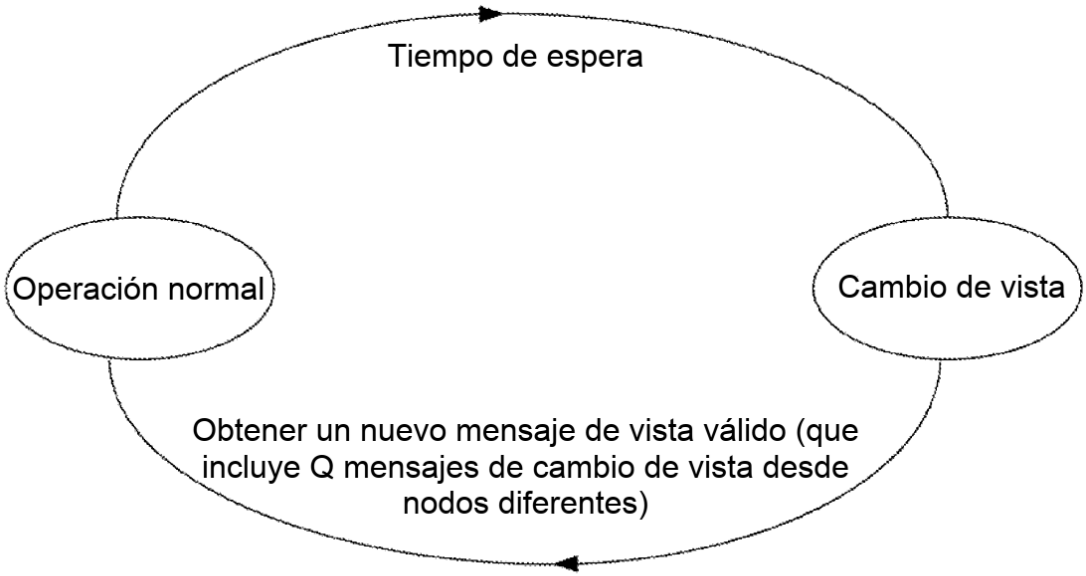
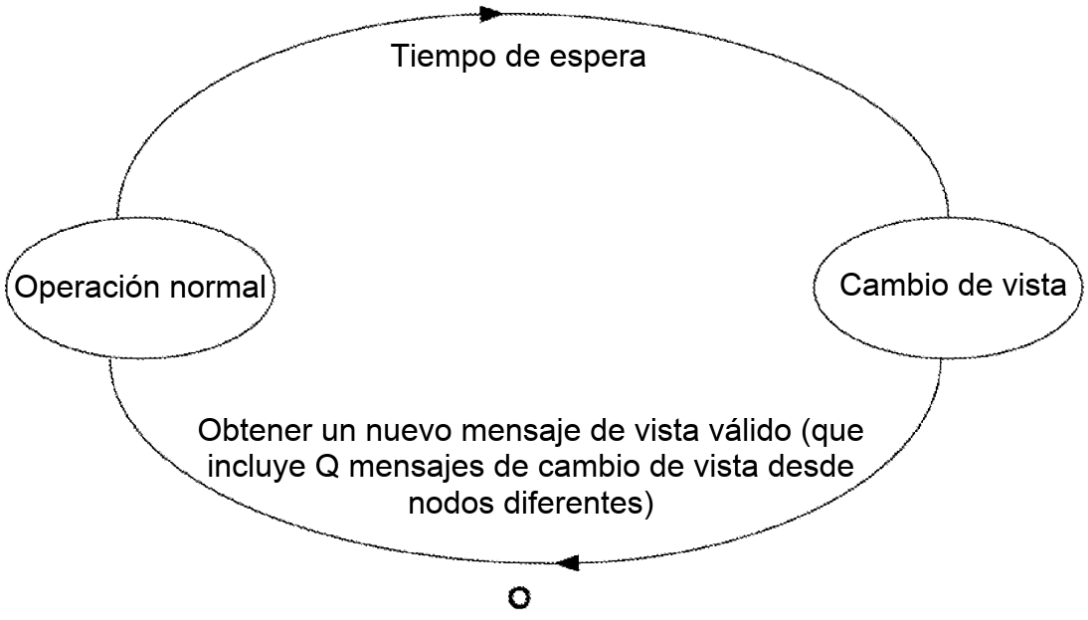


FIG. 3A



Obtener Q primeros mensajes que cada uno comprende una vista actual consistente y un número de secuencia actual consistente

FIG. 3B

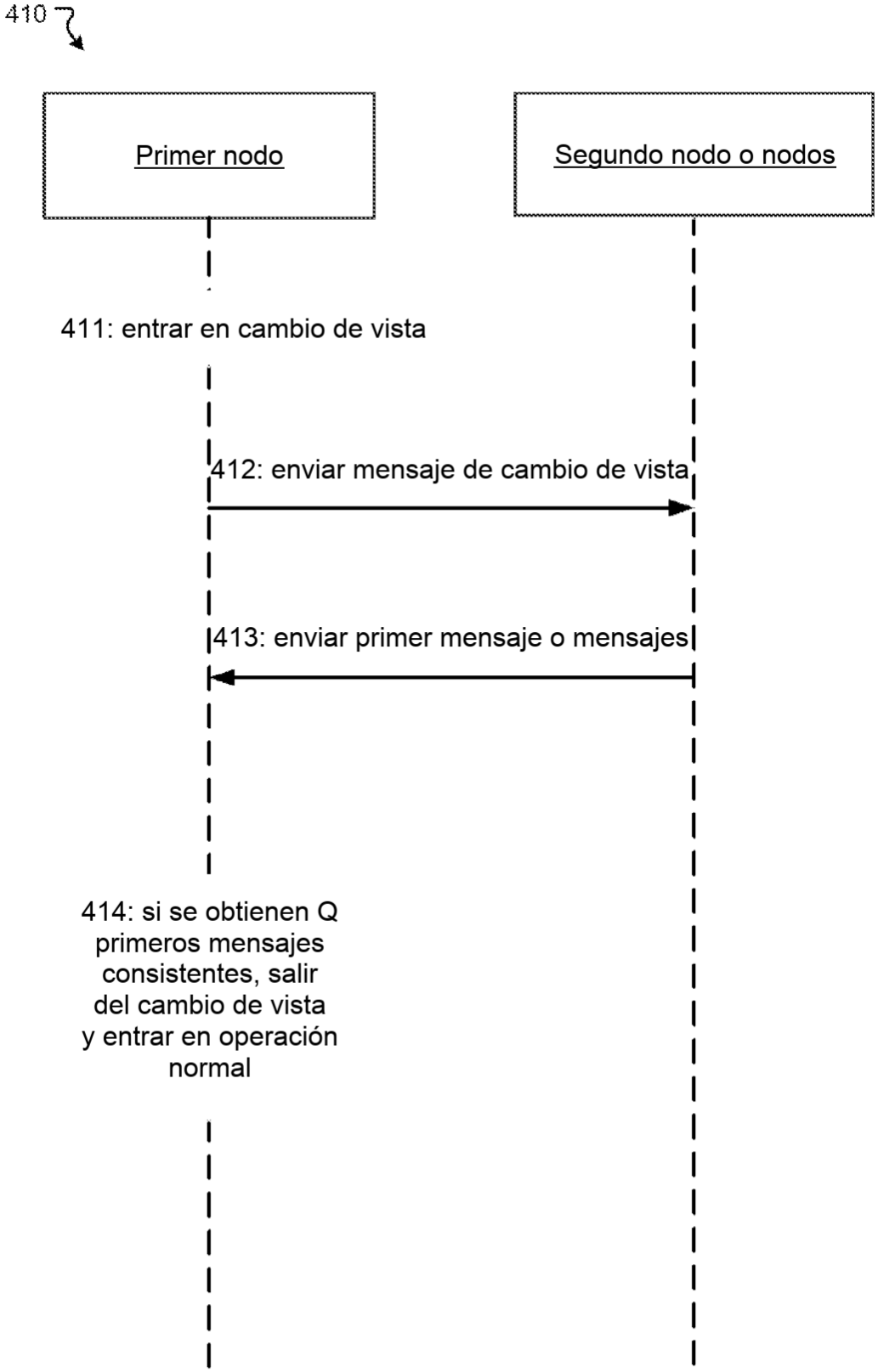

410
Primer nodo
Segundo nodo o nodos
411: entrar en cambio de vista
412: enviar mensaje de cambio de vista
413: enviar primer mensaje o mensajes
414: si se obtienen Q primeros mensajes consistentes, salir del cambio de vista y entrar en operación normal

FIG. 4

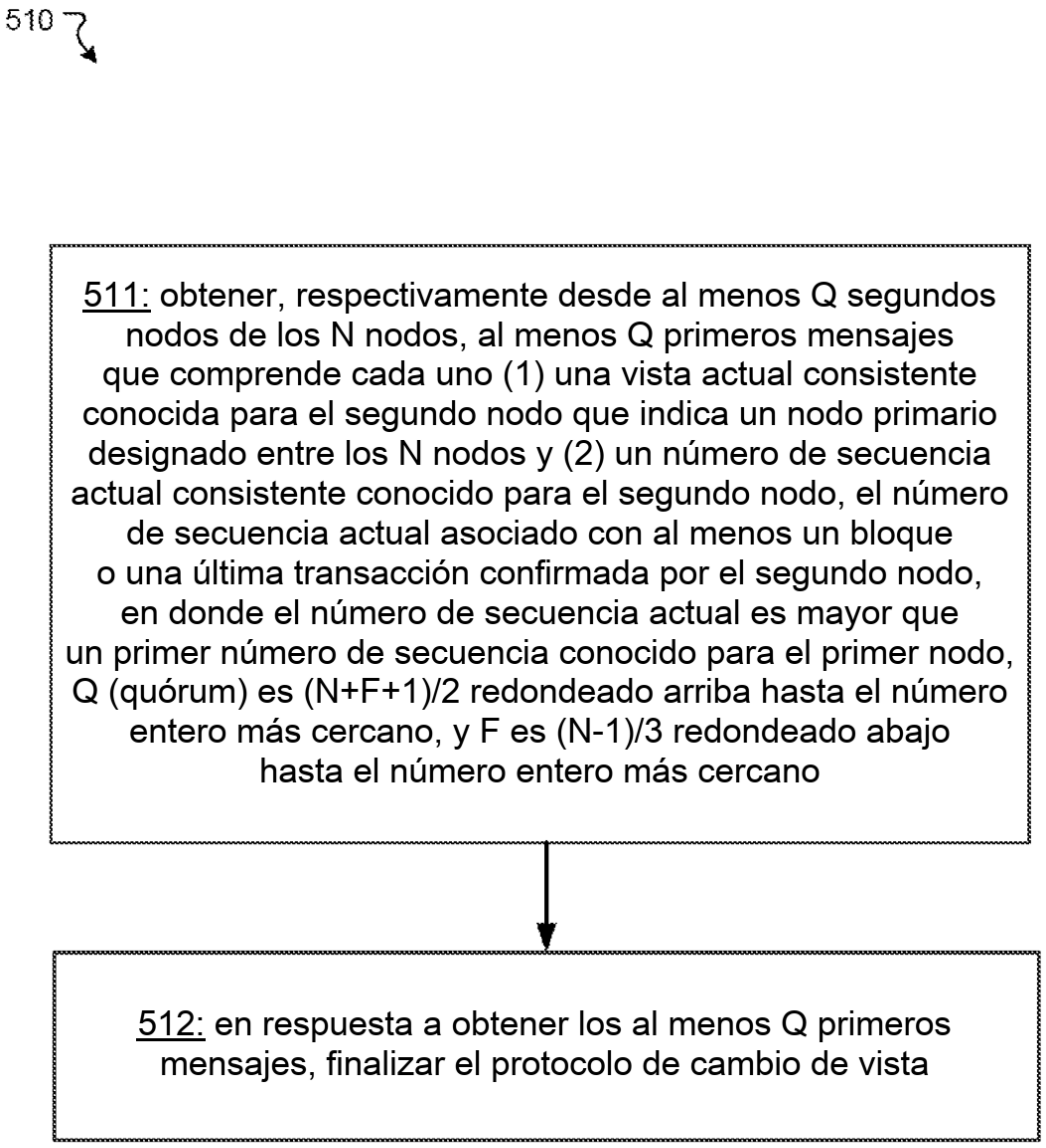

510
511: obtener, respectivamente desde al menos Q segundos nodos de los N nodos, al menos Q primeros mensajes que comprende cada uno (1) una vista actual consistente conocida para el segundo nodo que indica un nodo primario designado entre los N nodos y (2) un número de secuencia actual consistente conocido para el segundo nodo, el número de secuencia actual asociado con al menos un bloque o una última transacción confirmada por el segundo nodo, en donde el número de secuencia actual es mayor que un primer número de secuencia conocido para el primer nodo, Q (quórum) es (N+F+1)/2 redondeado arriba hasta el número entero más cercano, y F es (N-1)/3 redondeado abajo hasta el número entero más cercano
512: en respuesta a obtener los al menos Q primeros mensajes, finalizar el protocolo de cambio de vista

FIG. 5A

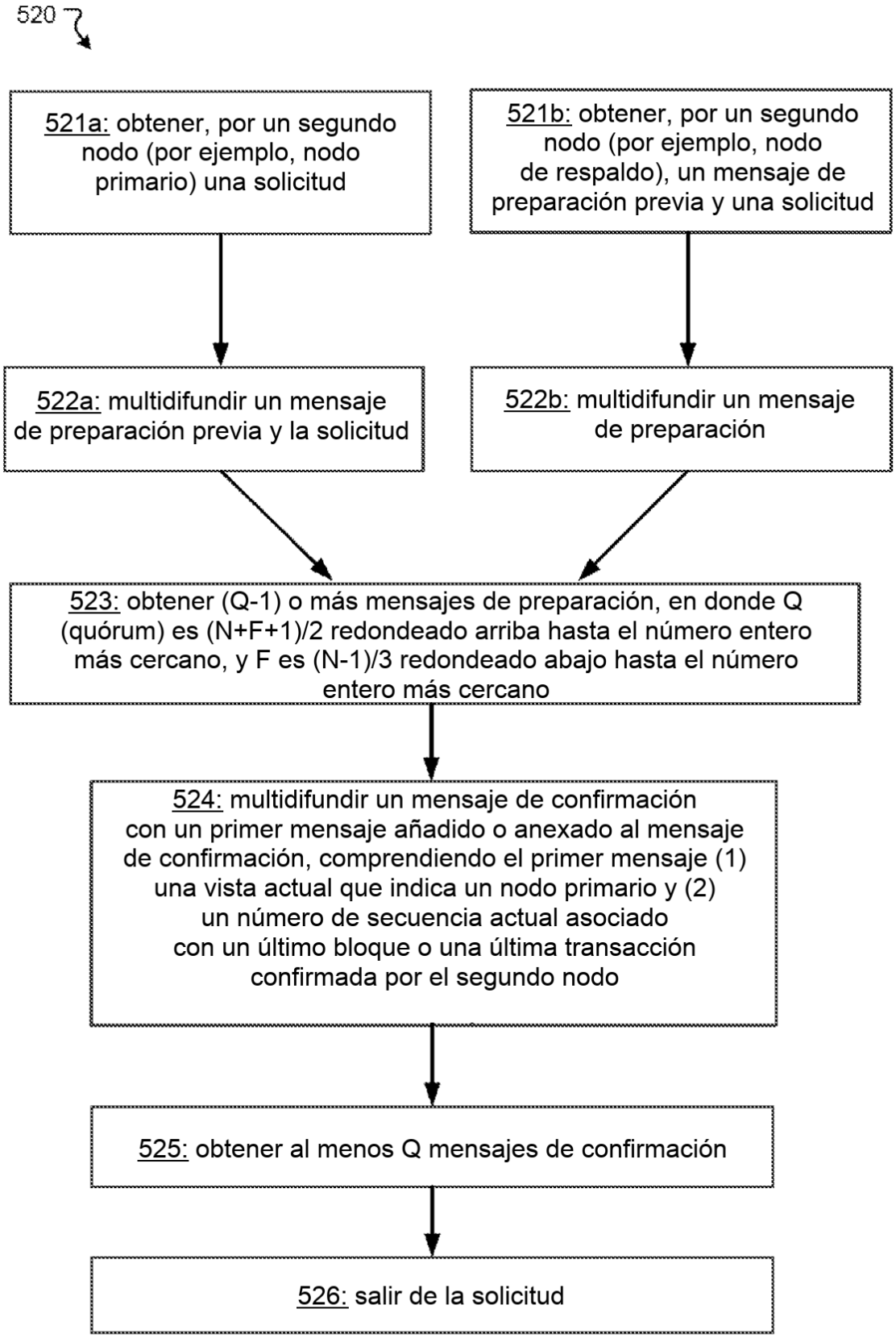

520
521a: obtener, por un segundo nodo (por ejemplo, nodo primario) una solicitud
521b: obtener, por un segundo nodo (por ejemplo, nodo de respaldo), un mensaje de preparación previa y una solicitud
522a: multidifundir un mensaje de preparación previa y la solicitud
522b: multidifundir un mensaje de preparación
523: obtener (Q-1) o más mensajes de preparación, en donde Q (quórum) es (N+F+1)/2 redondeado arriba hasta el número entero más cercano, y F es (N-1)/3 redondeado abajo hasta el número entero más cercano
524: multidifundir un mensaje de confirmación con un primer mensaje añadido o anexado al mensaje de confirmación, comprendiendo el primer mensaje (1) una vista actual que indica un nodo primario y (2) un número de secuencia actual asociado con un último bloque o una última transacción confirmada por el segundo nodo
525: obtener al menos Q mensajes de confirmación
526: salir de la solicitud

FIG. 5B

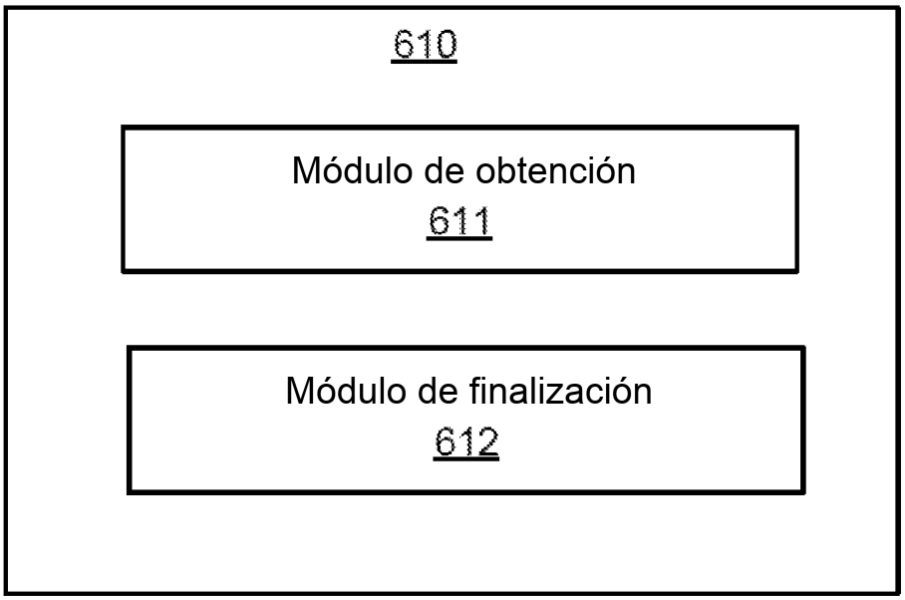


FIG. 6

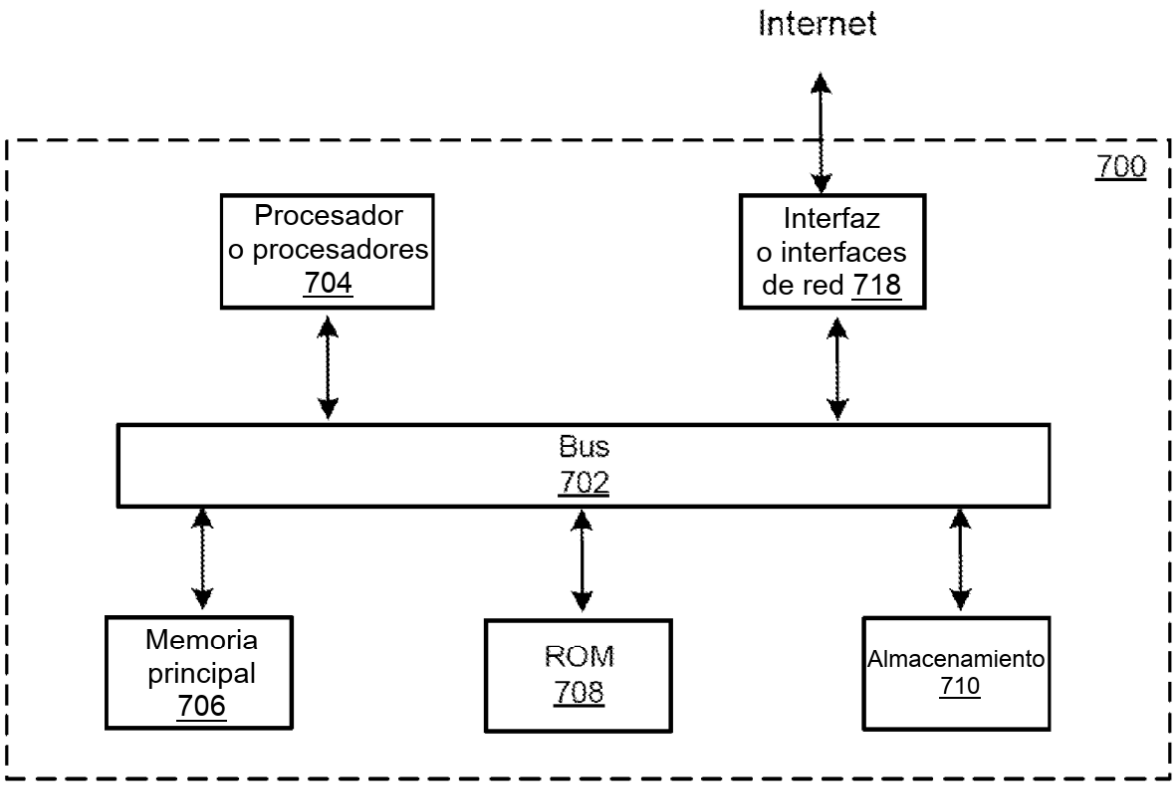

Internet
700
Procesador o procesadores 704
Interfaz o interfaces de red 718
Bus 702
Memoria principal 706
ROM 708
Almacenamiento 710

FIG. 7