(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 812 282**

(51) Int. CI.:

***G06F 21/64*** (2013.01)
***H04L 9/32*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.08.2018 E 18192002 (6)**

(97) Fecha y número de publicación de la concesión europea: **15.07.2020 EP 3617926**

(54) Título: **Equipo y procedimiento de formación de bloques, equipo de nodo y procedimiento de confirmación de bloques**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**16.03.2021**

(73) Titular/es:

**SIEMENS AKTIENGESELLSCHAFT (100.0%)**
**Werner-von-Siemens-Straße 1**
**80333 München, DE**

(72) Inventor/es:

**FALK, RAINER**

(74) Agente/Representante:

**LOZANO GANDIA, José**

## DESCRIPCIÓN

Equipo y procedimiento de formación de bloques, equipo de nodo y procedimiento de confirmación de bloques

La presente invención se refiere al campo de la técnica de automatización industrial y en especial a un equipo de formación de bloques, un procedimiento de formación de bloques, un equipo de nodo y un procedimiento de confirmación de bloques para un sistema de base de datos distribuida con cronometraje.

Las aplicaciones industriales, como sistemas de automatización industrial, formulan exigencias especiales a la técnica de información utilizada para el control y/o regulación en cuanto a seguridad funcional, disponibilidad y capacidad de tiempo real.

En un sistema de base de datos distribuida implementado con tecnología de cadena de bloques, pueden realizarse transacciones sin un puesto de compensación (clearing) o una relación especial de confianza entre las partes de la transacción en base a un consenso entre las partes de la transacción de forma protegida frente a la manipulación. Puede pensarse en memorizar en bloques de datos de transacción protegidos mediante tecnología de cadenas de bloques valores de medición / control, protegidos, por ejemplo como los llamados contratos inteligentes (Smart Contracts), órdenes de control para una instalación de automatización industrial. Sin embargo, la tecnología de cadenas de bloques conocida carece de la capacidad de tiempo real necesaria para los controles industriales. En particular, una cadena de bloques basada en Proof-of-Work (prueba de trabajo) sólo puede confirmar transacciones en promedio en ciertos intervalos, pero no se puede prescribir exactamente en qué instantes se debe confirmar una transacción o se debe ejecutar un contrato inteligente.

Elli Androulaki y colab., "Hyperledger Fabric: Un sistema operativo distribuido para cadenas de bloques con autorización", Actas de la Décimotercera Conferencia de Eurosys en Eurosys '18, 23-26 de abril de 2018, Porto, Portugal, da a conocer una estructura para operar sistemas de base de datos de cadena de bloques de acceso restringido.

La estructura funciona con una arquitectura Execute-Order-Validate (ejecutar-ordenar-validar), en la que la comprobación de transacciones, la ordenación de transacciones en bloques y la validación de los bloques están separadas entre sí. Sólo se cronometra la ordenación de las transacciones en bloques.

Partiendo de esta base, un objeto de la presente invención es mejorar un sistema de base de datos distribuida.

Según un primer aspecto, se propone un equipo de formación de bloques para un sistema de base de datos distribuida que incluye un conjunto de equipos de nodo. El equipo de formación de bloques incluye: una primera unidad para elegir un conjunto de transacciones a confirmar a partir de un conjunto de transacciones no confirmadas proporcionadas en el sistema de base de datos distribuida; una segunda unidad para formar un bloque no confirmado a partir del conjunto elegido de transacciones no confirmadas, comprobándose la validez de una respectiva transacción no confirmada elegida y rechazándose si no supera la prueba incluyéndose, de lo contrario en el bloque no confirmado y para proporcionar el bloque no confirmado en el sistema de base de datos distribuida; y una tercera unidad para recibir un cronometraje de un reloj y para determinar segmentos de tiempo de longitud predeterminada en base al cronometraje. La primera unidad y la segunda unidad están preparadas para realizar exactamente una vez la elección, la formación y la aportación dentro de un segmento de tiempo correspondiente.

El sistema de base de datos distribuida puede implementar un libro de transacciones a prueba de manipulaciones (en inglés "ledger"), que se representa mediante una cadena de bloques confirmados memorizada en cada uno de los equipos de nodo. La cadena puede estar formada mediante sumas de comprobación de encadenamiento. En particular, el sistema de base de datos distribuida puede ser una red de cadenas de bloques o una cadena de bloques.

El equipo de formación de bloques propuesto puede ser un equipo de minería (mining). El equipo de formación de bloques puede ser en particular un componente de un equipo de nodo del sistema de base de datos distribuida.

El equipo de formación de bloques propuesto puede formar ventajosamente el bloque respectivo no confirmado a partir de las transacciones no confirmadas proporcionadas en cada caso en el sistema de base de datos distribuida proporcionado con un titmo de cronometraje predeterminado. Esto permite una formación de bloques o extracción (mining) cronometrados y por lo tanto una confirmación cronometrada de transacciones no confirmadas. Por lo tanto, el equipo de formación de bloques propuesto puede hacer que el sistema de base de datos distribuida sea adecuado para utilizarlo para controlar una instalación de automatización industrial con exigencias de tiempo real.
"Un conjunto o una serie " significa un conjunto o una serie de uno o más.

Los equipos del sistema de base de datos distribuida, incluido el conjunto de equipos de nodo y en particular el equipo de formación de bloques propuesto, pueden ser capaces de comunicarse o estar conectados en red entre sí.

Se puede entender que "proporcionar o aportar en el sistema de base de datos distribuida" una transacción no confirmada o de un bloque no confirmado significa que la transacción no confirmada o el bloque no confirmado se transmite al menos a uno de los equipos del sistema de base de datos distribuida. La transacción no confirmada a proporcionar o el bloque no confirmado proporcionado se puede transmitir directamente, indirectamente o en el modo de igual a igual (peer-to-peer) al resto de los equipos del sistema de base de datos distribuida.

El sistema de base de datos distribuida puede estar configurado tal que el tiempo necesario para proporcionar o transmitir un bloque no confirmado o una transacción no confirmada a una mayoría o a todos los equipos del sistema de base de datos distribuida sea inferior a la longitud de uno de los segmentos de tiempo respectivos.

La primera unidad puede estar configurada para elegir el conjunto de transacciones a confirmar a partir del conjunto de transacciones no confirmadas proporcionadas en la secuencia en la que se proporcionan las transacciones individuales no confirmadas. Alternativamente, también es concebible que al elegir se realice una priorización en función de características de las respectivas transacciones no confirmadas.

La segunda unidad puede estar configurada para formar el bloque no confirmado a partir del conjunto elegido de transacciones no confirmadas de acuerdo con exigencias de una regla de consenso del sistema de base de datos distribuida.

En particular, la segunda unidad puede estar configurada para comprobar la validez de la correspondiente transacción no confirmada elegida en función de la regla de consenso, para rechazar la transacción no confirmada si no supera la prueba y caso contrario incluir la transacción no confirmada en el bloque no confirmado. En el marco de la comprobación, se puede ejecutar un contrato inteligente (Smart Contract) contenido en la transacción no confirmada y/o memorizado en un libro de transacciones del sistema de base de datos distribuida y referenciado por la transacción. De esta forma, se puede ejecutar el código del programa con instrucciones de control, que está archivado en los contratos inteligentes.

En particular, la segunda unidad puede estar configurada para asegurar frente a manipulaciones el bloque no confirmado y/o una de las transacciones no confirmadas incluidas en el bloque con una suma de comprobación, como por ejemplo un valor hash o una suma de comprobación raíz de un árbol hash, como un árbol de Merkle o de un árbol de Patricia.

En particular, la segunda unidad puede estar configurada para vincular el bloque no confirmado con el libro de transacciones del sistema de base de datos distribuida. Para ello puede incluir la misma en el bloque no confirmado, por ejemplo, una suma de comprobación de encadenamiento, como una suma de comprobación de un bloque inmediata o mediatamente precedente de la cadena de bloques confirmados. Tal concatenación puede ofrecer una mayor protección frente a la manipulación.

Al respecto se puede otorgar a la segunda unidad acceso a una copia local de una representación del libro de transacciones del sistema de base de datos distribuida. La copia local puede estar memorizada en un equipo de nodo del sistema de base de datos distribuida, por ejemplo un equipo de nodo del cual el equipo de formación de bloques es una parte, o un equipo de nodo con el que el equipo de formación de bloques puede comunicar.

En particular, la segunda unidad puede incluir un valor de comprobación en el bloque no confirmado a formar. El valor de comprobación puede entenderse como una prueba de un interés legítimo de la unidad de formación de bloques en un funcionamiento sin problemas del sistema de base de datos distribuida.

Puede pensarse por ejemplo en una prueba de participación (Proof-of-Stake), una firma digital que tenga una autorización especial o posición de confianza del equipo de formación de bloques (el llamado “permissioned ledger”, libro mayor autorizado), o una "Proof-of-Work” (prueba de trabajo) adaptada. que con seguridad se puede aportar dentro de un segmento de tiempo correspondiente, como por ejemplo una solución "relativa" de un puzzle criptográfico o “Best-Effort-Proof-of-Work” (la mejor prueba de trabajo que se pueda).

En particular, la segunda unidad puede incluir una transacción Coinbase en el bloque no confirmado a formar, que otorga al equipo de formación de bloques o a un equipo de nodo asignado al equipo de formación de bloques una recompensa por la formación del bloque.

Puesto que la regla de consenso de la base de datos distribuida por un lado prescribe la existencia de un valor de comprobación en un bloque a confirmar y por otro lado permite la existencia de una transacción Coinbase, por un lado se dificulta la formación y por lo tanto la manipulación de bloques y por otro lado se crea un incentivo para la formación de bloques conforme a las reglas. De esta manera, se puede

implementar ventajosamente un sistema de base de datos distribuida sin un puesto de compensación (clearing) central con una excelente posición en cuanto a confianza.

En respuesta a la aportación del bloque no confirmado así formado por parte de la segunda unidad, los equipos de nodo del sistema de base de datos distribuida pueden comprobar el bloque no confirmado proporcionado por ejemplo según la regla de consenso del sistema de base de datos distribuida e incluir el bloque no confirmado comprobado como bloque más recientemente confirmado en el libro de transacciones del sistema de base de datos distribuida. De esta manera, se pueden confirmar las transacciones no confirmadas contenidas en el bloque no confirmado. Puesto que el equipo de formación de bloques propuesto proporciona el bloque no confirmado cronometrado, puede confirmar de esta manera el sistema de base de datos distribuida, que incluye el equipo de formación de bloques propuesto, ventajosamente de manera cronometrada las transacciones no confirmadas e insertarlas en el sistema de base de datos distribuida.

El reloj puede ser un reloj local del equipo de formación de bloques y/o de un equipo de nodo, al que está asociado el equipo de formación de bloques, como por ejemplo un Chip Scale Atomic Clock (reloj atómico a escala de chip), un reloj distribuido del sistema de base de datos distribuida, como por ejemplo un protocolo de sincronización del tiempo del sistema de base de datos distribuida como NTP (Network Time Protocol, protocolo de tiempo de red) o PTP (Precision Time Protocol, protocolo de tiempo de precisión) o bien un reloj externo al equipo de formación de bloques y al sistema de base de datos distribuida y alejado de los mismos, como por ejemplo un temporizador de un sistema de navegación por satélite (GNSS, como por ejemplo GPS, Galileo, Beidou, Glonass), un transmisor de tiempo o un nodo maestro, que prescribe un cronometraje industrial (como por ejemplo IEEE Time Sensitive Networking, interoperación en red en tiempo real, Profinet isócrono o una retícula de tiempo del procesamiento de un programa de un sistema de control programable en memoria). Un cronometraje recibido del reloj puede ser un cronometraje absoluto o uno relativo. Bajo un cronometraje puede entenderse una secuencia de indicaciones de tiempo absolutas o relativas.

El cronometraje puede repetirse y/o recibirse cíclicamente.

Se puede proporcionar un conjunto o cada uno de los equipos del sistema de base de datos distribuida con el mismo cronometraje o bien un cronometraje síncrono en cada caso con el cronometraje del equipo de formación de bloques. Así el equipo de formación de bloques propuesto puede funcionar de manera sincronizada con otros equipos del sistema de base de datos distribuida según un cronometraje del sistema de base de datos distribuida

El ritmo de cronometraje puede ser un ritmo de cronometraje constante. Esto significa que los segmentos de tiempo respectivos pueden ser de la misma longitud.

La duración predefinida de un segmento de tiempo puede estar prescrita por el cronometraje. Por ejemplo, un segmento de tiempo puede corresponder al período de tiempo entre dos señales de reloj o a informaciones de tiempo transmitidas del cronometraje. La duración predeterminada también puede ser un múltiplo entero del período de tiempo entre dos señales de reloj o informaciones de tiempo transmitidas.

La tercera unidad puede estar configurada para fijar el ritmo del funcionamiento de la primera unidad y de la segunda unidad en función de los intervalos de tiempo determinados. Por ejemplo, la misma puede iniciar la operación de la primera unidad al comienzo de un segmento de tiempo respectivo, iniciar la operación de la segunda unidad después de que la primera unidad complete la elección y, en un momento predeterminado antes del final del segmento de tiempo, transmitir una señal a la segunda unidad que le solicite finalizar la formación del bloque no confirmado y proporcionar el bloque no confirmado formado hasta entonces de la mejor manera posible en el sistema de base de datos distribuida.

De esta manera, la primera unidad y la segunda unidad pueden estar configuradas para llevar a cabo la elección, formación y aportación exactamente una vez dentro del segmento de tiempo respectivo.

Tal cronometraje puede permitir ventajosamente la utilización del sistema de base de datos distribuida para memorizar valores de medición y control y para ejecutar un código de programa implementado como contratos inteligentes con instrucciones de control para controlar una instalación de automatización industrial con exigencias de tiempo real.

Cabe señalar que el concepto "realizar exactamente una vez" también puede entenderse que significa que la elección, formación y aportación no se realizan o se realizan exactamente una vez durante el segmento de tiempo correspondiente. En otras palabras, la elección, formación y aportación pueden completarse durante el segmento de tiempo correspondiente si se inicia. Tampoco se puede iniciar por ejemplo si el equipo de formación de bloques no está activado durante un segmento de tiempo determinado.

Según una forma de realización, la primera unidad está configurada para elegir, durante el segmento de tiempo correspondiente, todas las transacciones no confirmadas proporcionadas en el sistema de base de datos distribuida que corresponden a una condición predefinida como transacciones a confirmar.

El equipo de formación de bloques propuesto puede asegurar así de manera ventajosa que, en un segmento de tiempo respectivo, todas las transacciones no confirmadas proporcionadas que corresponden a la condición predeterminada son confirmadas por los equipos de nodo del sistema de base de datos distribuida.

La condición predeterminada puede ser que se incluyan todas las transacciones no confirmadas proporcionadas.

La condición predeterminada puede ser que se incluyan al menos aquellas de las transacciones no confirmadas proporcionadas que estén marcadas como críticas en el tiempo.

La condición predeterminada puede ser que se incluyan al menos aquellas de las transacciones no confirmadas proporcionadas que sean transacciones con valores de medición, valores de control y/o contratos inteligentes con órdenes de control para una instalación de automatización industrial.

La condición predeterminada puede ser que se confirmen al menos aquellas de las transacciones no confirmadas proporcionadas que para su confirmación otorguen como mínimo una recompensa predefinida al equipo de formación de bloques.

De esta manera puede garantizarse ventajosamente que en un segmento de tiempo correspondiente todas las transacciones proporcionadas, todas las transacciones críticas en el tiempo y/o todas las no confirmadas con una alta recompensa, se incluyen en el bloque formado.

Según una forma de realización, el equipo de formación de bloques propuesto tiene una cuarta unidad para recibir una señal de activación. La primera unidad y la segunda unidad están configuradas para llevar a cabo la elección, la formación y la aportación dentro del segmento de tiempo respectivo sólo exactamente una vez cuando la cuarta unidad recibe la señal de activación en el segmento de tiempo correspondiente.

La señal de activación puede ser transmitida por un equipo de planificación del tiempo del sistema de base de datos distribuida.

En consecuencia, es posible utilizar más de uno de los equipos de formación de bloques propuestos en un sistema de base de datos distribuida. Incluso si la formación de bloques en los equipos de formación de bloques propuestos se lleva a cabo en un cronometraje predeterminado, puede evitarse ventajosamente una situación competitiva insoluble activando el equipo de planificación del tiempo en cada segmento de tiempo sólo uno de los equipos de formación de bloques con la señal de activación. Aquí puede ser ventajoso utilizar varios equipos de formación de bloques en alternancia para lograr un equilibrio de confianza en un consenso mayoritario en el sistema de base de datos distribuida. Así por ejemplo, una recompensa otorgada por formar un bloque con éxito se puede otorgar alternativamente a diferentes equipos de formación de bloques y, por lo tanto, se puede conservar un equilibrio de créditos de tokens criptográficos en el sistema de base de datos distribuida. Esto puede ser ventajoso cuando la distribución de tokens criptográficos entre los equipos de nodo es importante para la seguridad frente a manipulación de la red, por ejemplo en el caso de la formación de bloques utilizando un Prof-of-Stake como valor de comprobación.

Según otra forma de realización, la segunda unidad está configurada para incluir en el bloque formado la mejor prueba criptográfica de trabajo que pueda determinar la misma dentro del segmento de tiempo respectivo.

En otras palabras, se propone una Proof-of-Work (prueba de trabajo) modificada basada en el Best-Effort (el mejor esfuerzo). Por ejemplo, un puzzle criptográfico no se puede resolver por completo, sino sólo de la mejor manera posible. Por ejemplo, la segunda unidad puede incluir un valor o nonce (número arbitrario de un solo uso) de libre elección en el bloque formado y determinar el nonce de tal manera que una suma de comprobación de todo el bloque formado, incluido el nonce, sea lo más extrema posible, por ejemplo lo más baja posible. Si se trata de una suma de comprobación criptográfica, como un valor hash, dicha determinación sólo es posible probando. Puede comenzarse a probar tan pronto como esté formado el bloque que se va a formar a excepción del nonce a determinar y la prueba puede terminar en un momento predeterminado dentro del segmento de tiempo respectivo. De esta manera, se puede proporcionar con seguridad la mejor prueba de trabajo posible dentro del tiempo disponible y dentro del segmento de tiempo correspondiente.

En consecuencia, es ventajosamente posible utilizar más de uno de los equipos de formación de bloques propuestos simultáneamente en un sistema de base de datos distribuida. Incluso si la formación de bloques en los equipos de formación de bloques propuestos tiene lugar en un cronometraje

predeterminado, puede resolverse ventajosamente una situación competitiva resultante de ello, por ejemplo, previendo la regla de consenso del sistema de base de datos distribuida que los equipos de nodo del sistema de base de datos distribuida confirmen aquél de un conjunto de bloques no confirmados que contiene la mejor prueba de trabajo.

Por lo tanto, las ventajas del mining o minería (formación de bloques por medio de la prueba de trabajo) también se pueden lograr si la formación de los bloques se lleva a cabo de manera cronometrada, de acuerdo con los equipos de formación de bloques propuestos.

Según otra forma de realización, la segunda unidad está configurada para incluir en el bloque formado una marca de tiempo que identifica el correspondiente segmento de tiempo.

En consecuencia, la regla de consenso del sistema de base de datos distribuida puede prever que solo se confirmen aquellos bloques no confirmados que contienen una marca de tiempo adecuada para un segmento de tiempo actual cuando se confirma. De esta manera pueden descartarse ventajosamente bloques tardíos o bloques prematuros (posiblemente manipulados).

Según un segundo aspecto, se propone un equipo de nodo para un sistema de base de datos distribuida que incluye un conjunto de equipos de nodo. El equipo de nodo incluye: una quinta unidad para memorizar una cadena de bloques confirmados, que representan al menos una sección de un libro de transacciones del sistema de base de datos distribuida; una sexta unidad para confirmar exactamente uno de un conjunto de bloques no confirmados proporcionados en el sistema de base de datos distribuida en el segmento de tiempo correspondiente, de modo que el bloque confirmado esté unido a la cadena de bloques confirmados, incluyendo la confirmación de exactamente uno del conjunto de bloques no confirmados una comprobación de uno, varios o todos los bloques no confirmados, una elección de uno de los bloques no confirmados comprobados con éxito y una agregación del bloque elegido como el bloque confirmado a la cadena de bloques confirmados; y una tercera unidad para recibir un cronometraje de un reloj y determinar segmentos de tiempo de longitud predeterminada en base al cronometraje. La sexta unidad está configurada para llevar a cabo la confirmación exactamente una vez dentro de un segmento de tiempo correspondiente.

Las características, definiciones y ventajas descritas en la descripción del equipo de formación de bloques propuesto son válidas, si corresponde, para el equipo de nodo propuesto de la forma correspondiente.
.
Se puede decir que el equipo de nodo propuesto forma una contraparte complementaria al equipo de formación de bloques propuesto.

El equipo de nodo propuesto puede confirmar ventajosamente bloques no confirmados en un cronometraje predeterminado. Por ejemplo, el equipo de nodo propuesto puede confirmar los bloques no confirmados cronometrados formados por el equipo de formación de bloques propuesto al mismo ritmo. Esto permite una confirmación cronometrada de transacciones no confirmadas. Por lo tanto, el equipo de nodo propuesto puede proporcionar al sistema de base de datos distribuida, que incluye el equipo de nodo propuesto, idoneidad para su utilización para controlar una instalación de automatización industrial con exigencias de tiempo real.

La cadena de bloques confirmados memorizada/s en la quinta unidad puede interpretarse como copia local de una versión del libro de transacciones, sobre la cual existe consenso entre el conjunto de equipos de nodo o se forma con el tiempo. El consenso se puede lograr entonces comportándose la sexta unidad, al elegir y confirmar exactamente un bloque a confirmar, de acuerdo con una regla de consenso definida del sistema de base de datos distribuida. Igualmente puede comportarse un equipo de formación de bloques, como el equipo de formación de bloques propuesto, del sistema de base de datos distribuida, al formar bloques no confirmados, preferiblemente según la misma regla de consenso establecida. La regla de consenso puede estar establecida tal que se recompense un comportamiento conforme a las reglas y no se recompense un comportamiento no conforme a las reglas o bien se impida automáticamente al equipo de nodo que no se comporta conforme a las reglas participar en lo sucesivo en la búsqueda de consenso. De esta manera se puede garantizar que se forme un consenso de tal manera que en una mayoría y con preferencia en todos los equipos de nodo del sistema de base de datos distribuida estén memorizadas representaciones idénticas del libro de transacciones y se dificulten o impidan manipulaciones no autorizadas.

La sexta unidad puede estar configurada para verificar un conjunto de los bloques no confirmados proporcionados en el sistema de base de datos distribuida durante el correspondiente segmento de tiempo de acuerdo con la regla de consenso, descartar bloques no confirmados que no cumplan con la regla de consenso y elegir un bloque a confirmar entre los bloques restantes no confirmados según la regla de consenso y agregar el bloque elegido a la cadena de bloques confirmados y confirmarlo así.

Por lo tanto, bajo "confirmar uno de un conjunto de bloques no confirmados" puede entenderse verificar uno, varios o todos los bloques no confirmados, elegir uno de los bloques no confirmados verificados con éxito y agregar el bloque elegido a la cadena de bloques confirmados.

Bajo “agregar" puede entenderse tanto agregar un anexo a un último bloque confirmado de la cadena de bloques confirmados como también crear una copia o una bifurcación de la cadena de bloques confirmados agregándolo en otra posición, es decir, a un bloque anterior al último confirmado de la cadena de bloques confirmados. En particular, el bloque a agregar se puede agregar según la regla de consenso a aquellos de la cadena de bloques confirmados cuya suma de comprobación corresponda a una suma de comprobación de encadenamiento contenida en el bloque a agregar.

La regla de consenso puede prescribir cuál de las copias o bifurcaciones de la cadena de bloques confirmados se considera como representación válida del libro de transacciones de la base de datos distribuida. Por ejemplo, la cadena más larga puede considerarse como representación válida.

El equipo de formación de bloques propuesto puede incluir una transacción no confirmada proporcionada en el sistema de base de datos distribuida en un bloque no confirmado que se proporciona en el sistema de base de datos distribuida. El bloque no confirmado proporcionado en el sistema de base de datos distribuida puede ser verificado por uno de los equipos de nodo correspondiente, tal como se ha descrito, y confirmado agregándolo al libro de transacciones (la copia local respectiva del libro de transacciones) de la base de datos distribuida. Esto permite confirmar las transacciones contenidas en el bloque correspondiente. Según la solución propuesta, tanto la formación del bloque no confirmado como también la confirmación del bloque no confirmado y por lo tanto la confirmación de la transacción no confirmada, pueden realizarse sincronizados en el tiempo según un cronometraje predeterminado, preferiblemente cíclico.

En particular, la sexta unidad puede estar configurada para esperar en el segmento de tiempo correspondiente hasta que se haya completado la formación y aportación de bloques mediante uno o varios equipos de formación de bloques del sistema de base de datos distribuida y a continuación elegir y confirmar uno de los bloques formados aportados no confirmados.

En el cronometraje propuesto, puede estar dividido un segmento de tiempo correspondiente en una sección de tiempo para proporcionar transacciones no confirmadas, una sección para formar bloques no confirmados, una sección para proporcionar los bloques no confirmados y una sección para confirmar los bloques no confirmados proporcionados. Como alternativa a ello, se pueden formar y proporcionar bloques alternadamente en cada caso en un segmento de tiempo y elegirse y confirmarse bloques en un segmento de tiempo posterior.

Según otra forma de realización, la sexta unidad está configurada para elegir exactamente un bloque para confirmación en base a al menos un criterio.

Si están previstos varios equipos de formación de bloques en la red, es concebible que se proporcione más de un bloque no confirmado durante un segmento de tiempo correspondiente. En una tal situación competitiva, la regla de consenso puede prescribir uno o más criterios según los cuales han de confirmarse los bloques no confirmados proporcionados.

En una variante, el criterio es "número y clase de transacciones incluidas en el bloque".

Por ejemplo, se puede elegir de los distintos bloques no confirmados aquél que tenga más transacciones no confirmadas. Así se puede generar ventajosamente un gran volumen de transacciones del sistema de base de datos distribuida.

Por ejemplo, se puede elegir de entre los varios bloques no confirmados aquél con la mayoría de las transacciones de una determinada clase. Así pueden priorizarse ventajosamente determinadas transacciones, como por ejemplo transacciones críticas en el tiempo.

En una variante, el criterio es "calidad de una prueba de trabajo criptográfica incluida en el bloque".

Por ejemplo se puede preferir un bloque de los varios bloques no confirmados que resuelva un puzzle criptográfico con la mayor calidad, por ejemplo el bloque con el menor valor nonce como prueba de trabajo. La calidad de una prueba de trabajo criptográfica puede no ser esencialmente predecible o casual. Así se puede asegurar ventajosamente que en distintos segmentos de tiempo se da preferencia a bloques que proceden de distintos equipos de nodo y/o equipos de formación de bloques. Si está prevista una recompensa para el equipo de nodo que formó el bloque cuando se confirma un bloque, se puede garantizar de esta manera un equilibrio de créditos de token criptográficos en el sistema de base de datos distribuida.

En una variante, el criterio es "calidad y/o complejidad de cálculo de una transacción respectiva incluida en el bloque".
La complejidad de cálculo de una transacción correspondiente puede referirse en particular a la carga de cálculo que ha aportado el equipo de formación de bloques que ha formado el bloque para verificar la validez de la transacción. Si una transacción contiene o hace referencia a un contrato inteligente, puede ser considerable esta carga de cálculo. En consecuencia, a un equipo de formación de bloques que

verifica dicha transacción puede quedarle menos capacidad de cálculo para determinar la mejor prueba de trabajo posible dentro del segmento de tiempo respectivo. Por lo tanto, si sólo se utilizase el criterio "calidad de una prueba de trabajo", sería poco probable que los equipos de nodo elijan el bloque en cuestión para su confirmación. Sin embargo, si también se utiliza el criterio "calidad de una transacción correspondiente", puede compensarse ese efecto y evitarse ventajosamente que se vean en desventaja bloques no confirmados con transacciones complejas al realizar la elección para confirmar.

Otros ejemplos de la calidad de una transacción son por ejemplo una cantidad o un total de tokens criptográficos (cuanto mayor sea el total, mayor es la calidad de la transacción), una clase de transacción (cuanto más crítica en el tiempo sea la transacción, mayor es su calidad), una cantidad de datos contenida en la transacción, etc.

En una variante, el criterio es “coincidencia de una marca de tiempo incluida en el bloque con el segmento de tiempo respectivo".

Mediante este criterio puede establecerse ventajosamente una correspondencia entre una secuencia de las transacciones confirmadas en el libro de transacciones del sistema de base de datos distribuida y la secuencia de la aportación de las transacciones no confirmadas. Es decir, se puede evitar que un bloque retrasado se aloje tarde o que un bloque con una marca de tiempo futura, como por ejemplo un bloque manipulado, se confirme prematuramente. Por lo tanto, se pueden mejorar así la fiabilidad y la capacidad de tiempo real del sistema de base de datos distribuida.

Cabe señalar que bajo "coincidencia", además del caso en el que la marca de tiempo incluida en el bloque designe el segmento de tiempo respectivo, también puede entenderse el caso en el que la marca de tiempo incluida en el bloque, designa un segmento de tiempo que precede directa o indirectamente al segmento de tiempo correspondiente.

En una variante, el criterio es "si un equipo de formación de bloques que ha proporcionado el bloque es un equipo de formación de bloques para el cual está destinada una señal de activación transmitida durante el segmento de tiempo correspondiente en el sistema de base de datos distribuida".

Según este criterio, puede evitarse ventajosamente que equipos de formación de bloques no activados explícitamente (y que por lo tanto posiblemente actúan maliciosamente) introduzcan bloques en el sistema de base de datos distribuida.

Según otra forma de realización, la sexta unidad está configurada para elegir exactamente un bloque para confirmarlo en base a un criterio de si el bloque incluye todas las transacciones no confirmadas proporcionadas en el sistema de base de datos distribuida durante el segmento de tiempo respectivo que corresponden a una condición predefinida.

Lo anteriormente descrito para formas de realización del equipo de formación de bloques en relación con la "condición predefinida", es válido correspondientemente.

Si un tal criterio es parte de la regla de consenso del sistema de base de datos distribuida, cada equipo de formación de bloques del sistema de base de datos distribuida tiene interés en incluir todas las transacciones no confirmadas proporcionadas en un respectivo segmento de tiempo en el sistema de base de datos distribuida que correspondan a la condición predefinida en el bloque no confirmado que ha creado, ya que de lo contrario esto no se confirmaría y el equipo de formación de bloques en consecuencia no recibiría ninguna recompensa.

Por lo tanto, el presente criterio puede garantizar ventajosamente que en cada segmento de tiempo se incluyan todas las transacciones no confirmadas proporcionadas en el segmento de tiempo correspondiente que correspondan a la condición predefinida, en un bloque no confirmado por un equipo de formación de bloques del sistema de base de datos distribuida durante el mismo segmento de tiempo y durante el mismo segmento de tiempo o el siguiente se confirme confirmando al confirmar el bloque no confirmado por parte de los equipos de nodo del sistema de base de datos distribuida.

Los criterios para elegir el bloque para la confirmación según las variantes y formas de realización anteriores, se pueden combinar según se desee.

Según otra forma de realización, presenta el equipo de nodo propuesto el equipo de formación de bloques propuesto.

En otras palabras, tanto la funcionalidad de formación de bloques cronometrada realizada por el equipo de formación de bloques propuesto como también la funcionalidad de confirmación cronometrada realizada por el equipo de nodo propuesto antes descrito, pueden estar reunidas en un equipo de nodo propuesto. Se entiende que entonces la tercera unidad del equipo de nodo y la tercera unidad del equipo de formación de bloques integrado pueden ser idénticas para el equipo de nodo que incluye el equipo de formación de bloques. En otras palabras, puede estar prevista sólo una tercera unidad.

Por lo tanto, con preferencia puede uno, con especial preferencia cada uno de los equipos de nodo de un sistema de base de datos distribuida, tanto formar bloques no confirmados cronometrados como también confirmar bloques temporizados no confirmados cronometrados proporcionados con cronometraje por otros equipos de nodo.

Según otra forma de realización, se propone un sistema de base de datos distribuida que incluye un conjunto de equipos de nodo de los propuestos. Los equipos de nodo propuestos están configurados para gestionar conjuntamente el libro de transacciones del sistema de base de datos distribuida. Al menos uno de los equipos de nodo incluye un equipo de formación de bloques propuesto. Los equipos de nodo pueden funcionar sincronizados en el tiempo según un cronometraje del sistema de base de datos distribuida.

Debido a que los equipos de nodo del sistema de base de datos distribuida propuesto se pueden operar sincronizados en el tiempo, se puede asegurar con especial fiabilidad que pueden confirmarse transacciones no confirmadas dentro de un segmento de tiempo derivado del cronometraje.

El conjunto de equipos de nodo se puede operar de manera sincronizada en el tiempo, al ser síncronos los cronometrajes a recibir del correspondiente equipo de red y el cronometraje del sistema de base de datos distribuida. Como alternativa a ello, puede estar configurado un equipo de nodo correspondiente para recibir el mismo cronometraje del sistema de base de datos distribuida.

Así están sincronizados en particular el o los cronometraje/s a recibir del correspondiente equipo de nodo y el cronometraje del sistema de base de datos distribuida.

Bajo funcionamiento síncrono de los equipos de nodo del sistema de base de datos distribuida puede entenderse en particular lo siguiente:

Un cronometraje o los segmentos de tiempo respectivos de una funcionalidad de formación de bloques cronometrada (de la primera a la tercera unidad) y una funcionalidad de confirmación cronometrada (de la quinta, sexta y tercera unidad) de los equipos de nodo del sistema de base de datos distribuida, están preferiblemente sincronizados. Esto puede entenderse que significa que se usa el mismo cronometraje o que coinciden los segmentos de tiempo respectivos, o que el cronometraje de la funcionalidad de formación de bloques cronometrada y el cronometraje de la funcionalidad de confirmación cronometrada y/o los segmentos de tiempo respectivos, están desplazados en un decalaje de tiempo fijo. Pero también es posible que el cronometraje de la funcionalidad de formación de bloques cronometrada se realice cronometrado independientemente del cronometraje de la funcionalidad de confirmación cronometrada. Pueden concebirse otras variantes del cronometraje. Por ejemplo puede formarse el cronometraje de la funcionalidad de confirmación cronometrada compartiendo el cronometraje de la funcionalidad de formación de bloques cronometrada. Por ejemplo puede formarse un bloque correspondiente mediante la funcionalidad de confirmación cronometrada en cada caso después de una pluralidad, por ejemplo dos o cuatro ciclos de tiempo de la funcionalidad de formación de bloques cronometrada. Además, es concebible que el cronometraje no sea fijo, sino que se adapte de manera adaptativa, en función del número y/o clase de transacciones no confirmadas proporcionadas.

En particular, puede incluir un equipo de formación de bloques correspondiente más de uno de los equipos de nodo, tal como se propone. El sistema de base de datos distribuida puede tener un equipo de planificación del tiempo, que está configurado para transmitir una señal de activación en el segmento de tiempo respectivo a uno de los equipos de formación de bloques en cada caso.

Aquí el equipo de planificación puede estar configurado para decidir a cuál de los equipos de nodo (equipos de formación de bloques) se transmite la señal de activación en el segmento de tiempo correspondiente, según una secuencia predeterminada, aleatoriamente o en función de características de un equipo de nodo respectivo, como por ejemplo una cantidad de tokens criptográficos mantenidos por el equipo del nodo respectivo.

Según otra forma de realización, incluye el sistema de base de datos distribuida un reloj central, siendo el reloj desde el cual recibe la tercera unidad del equipo de nodo respectivo el cronometraje, el reloj central.

El reloj central puede ser un transmisor de tiempo DCF77, un temporizador GNSS, un servidor NTP/PTP o un nodo maestro que prescriba un cronometraje industrial o similares.

Al utilizar un reloj central, puede simplificarse la estructura de un equipo de nodo correspondiente, ya que sólo es necesario que el cronometraje se reciba y no se requiere un temporizador local en los equipos de nodo.

Según otra forma de realización, se propone un sistema de automatización industrial que incluye el sistema de base de datos distribuida propuesto y un conjunto de componentes de automatización que pueden funcionar según un cronometraje. El sistema de base de datos distribuida se puede operar para regular y/o controlar el conjunto de componentes de automatización. El cronometraje del sistema de base

de datos distribuida es sincrónico con el cronometraje del conjunto de componentes de automatización o un múltiplo entero del ritmo de cronometraje del conjunto de componentes de automatización.

Ejemplos de componentes de automatización son sensores, que están configurados para medir un estado físico en una instalación industrial, actuadores, que están configurados para influir en un estado físico en una instalación industrial, unidades de control, que implementan una lógica de control para determinar valores de control para los actuadores basados en valores medidos por los sensores y similares.

El sistema de base de datos distribuida puede por ejemplo funcionar para controlar el conjunto de componentes de automatización al estar archivadas secciones de la lógica de control del sistema de automatización en forma de contratos inteligentes confirmados en el libro de transacciones del sistema de base de datos distribuida. Igualmente pueden confirmarse los valores medidos suministrados por el conjunto de componentes de automatización y/o valores de control a transmitir al conjunto de componentes de automatización en forma de transacciones en el libro de transacciones del sistema de base de datos distribuida. De esta manera, se puede lograr ventajosamente transparencia, protección frente a manipulaciones y trazabilidad del funcionamiento del sistema de automatización. Mediante el funcionamiento cronometrado del sistema de base de datos propuesto, que en particular puede hacer posible una confirmación cronometrada de transacciones no confirmadas y con ello una ejecución cronometrada de contratos inteligentes, pueden lograrse éstas y otras ventajas del sistema de base de datos distribuida basado en cadenas de bloques incluso cuando se formulen elevadas exigencias de tiempo real a la lógica de control del sistema de automatización. En particular mediante la sincronización del cronometraje del sistema de base de datos distribuida con el cronometraje del sistema de automatización, pueden realizarse de forma trazable etapas individuales de control del sistema de automatización mediante el sistema de base de datos distribuida y documentarse de manera protegida frente a manipulación.

En una variante del sistema de automatización industrial propuesto y/o del sistema de base de datos distribuida propuesto, es concebible que el sistema de base de datos distribuida memorice varios libros de transacciones, representándose cada libro de transacciones mediante una cadena de bloques confirmados, representando una cadena del conjunto de cadenas un libro mayor de transacciones y representando el resto del conjunto de cadenas libros de transacciones laterales respectivos del sistema de base de datos distribuida.

Las cadenas que representan los libros de transacciones laterales ("cadenas laterales") se pueden operar con segmentos de tiempo que son más cortos en un factor entero que los segmentos de tiempo con los que se opera la cadena que representa el libro mayor de transacciones ("cadena principal").

La cadena principal y las cadenas laterales se pueden operar según distintas reglas de consenso. Así puede estar implementado en una cadena lateral un nivel de protección criptográfica más bajo, pero el funcionamiento de la cadena lateral se puede implementar utilizando menos recursos. Por el contrario, puede estar implementado un alto nivel de protección criptográfica en una cadena principal.

Bajo "operar una cadena" se puede entender aquí el funcionamiento de aquéllos de los equipos de nodo que memorizan la cadena respectiva en su quinta unidad.

De esta manera se puede realizar ventajosamente una distribución de carga entre las cadenas, confirmándose transacciones de menor importancia en las cadenas laterales y transacciones de mayor importancia en la cadena principal.

Un correspondiente libro de transacciones lateral puede estar vinculado con el libro de transacciones principal a intervalos de bloque regulares mediante valores hash o similares de bloques elegidos del libro de transacciones lateral archivados en el libro de transacciones principal. Así se puede extender un alto nivel de protección ofrecido por la cadena principal, al menos parcialmente, también a las cadenas laterales.

La unidad correspondiente, por ejemplo una correspondiente unidad de la primera a la sexta unidad, puede estar implementada en técnica de hardware y/o también en técnica de software. En una implementación en técnica de hardware, puede estar constituida la unidad respectiva como equipo o como parte de un equipo, por ejemplo como computadora o como microprocesador o como computadora de control de un vehículo. En una implementación en técnica de software, la unidad respectiva puede estar diseñada como producto de programa de computadora, como una función, como una rutina, como parte de un código de programa o como objeto ejecutable.

Según un tercer aspecto, se propone un procedimiento de formación de bloques para un sistema de base de datos distribuida que incluye una serie de equipos de nodo. El procedimiento de formación de bloques incluye: Elección de un conjunto de transacciones a confirmar a partir de un conjunto de transacciones no confirmadas proporcionadas en el sistema de base de datos distribuida; formación de un bloque no confirmado a partir del conjunto elegido de transacciones no confirmadas, verificándose la validez de una transacción correspondiente no confirmada elegida y descartándose si la comprobación no tiene éxito,

incluyéndose de lo contrario en el bloque no confirmado y aportación del bloque no confirmado en el sistema de base de datos distribuida; y recepción de un cronometraje desde un reloj y determinación de segmentos de tiempo de longitud predeterminada en base al cronometraje. La elección, la formación y la aportación se realizan entonces exactamente una vez dentro de un segmento de tiempo correspondiente.

Las formas de realización y características descritas para el equipo de formación de bloques propuesto según el primer aspecto, se aplican correspondientemente al procedimiento de formación de bloques propuesto según el tercer aspecto.

Según un cuarto aspecto, se propone un procedimiento de confirmación de bloques para un sistema de base de datos distribuida que incluye un conjunto de equipos de nodo. El procedimiento de confirmación de bloques incluye: Memorización de una cadena de bloques confirmados que representan un libro mayor de un base de datos distribuida; confirmación de exactamente uno de un conjunto de bloques no confirmados proporcionados en el sistema de base de datos distribuida en el segmento de tiempo respectivo, agregando el bloque confirmado a la cadena de bloques confirmados, incluyendo la confirmación de exactamente uno del conjunto de bloques no confirmados una comprobación de uno, varios o todos los bloques no confirmados, una elección de uno de los bloques no confirmados verificados con éxito y una agregación del bloque elegido como el bloque confirmado a la cadena de bloques confirmados; y recepción de un cronometraje desde un reloj y determinación de segmentos de tiempo de una longitud predeterminada en base al cronometraje. La confirmación se realiza entonces exactamente una vez dentro de un segmento de tiempo correspondiente.

Las formas de realización y características descritas para el equipo de nodo propuesto según el segundo aspecto, se aplican para el procedimiento de confirmación de bloques propuesto según el cuarto aspecto.

Además, se propone un producto de programa de computadora que provoca la ejecución de uno de los procedimientos explicados anteriormente en un equipo controlado por programa.

Un producto de programa de computadora, como por ejemplo un medio de programa de computadora puede proporcionarse o suministrarse por ejemplo como medio de almacenamiento, como por ejemplo tarjeta de memoria, pendrive USB, CD-ROM, DVD o también en forma de un archivo descargable desde un servidor en una red. Esto puede realizarse, por ejemplo, en una red de comunicación inalámbrica transmitiendo un fichero correspondiente con el producto de programa de computadora o el medio de programa de computadora.

A continuación se explican más detalles y otras variantes de sistemas de bases de datos distribuidas basados en tecnología de cadena de bloques, a los que pueden aplicarse el equipo de formación de bloques propuesto, el equipo de nodo propuesto y los procedimientos propuestos.

A menos que se indique lo contrario en la siguiente descripción, los términos "realizar", "calcular", "asistido por computadora", "computar", "determinar", "generar", "configurar", "reconstruir" y similares se refieren preferiblemente a operaciones y/o procesos y/o etapas de procesamiento que modifican y/o generan datos y/o convierten datos en otros datos, pudiendo representarse o existir los datos en particular como magnitudes físicas, por ejemplo, como impulsos eléctricos. En particular, el término "computadora" debe interpretarse de la manera más amplia posible, en particular para cubrir todos los aparatos electrónicos con características de procesamiento de datos. Las computadoras pueden ser por ejemplo ordenadores personales, servidores, controles programables en memoria (PLC), sistemas de computadora de mano, equipos de PC de bolsillo, aparatos de telefonía móvil y otros aparatos de comunicación que pueden procesar datos asistidos por computadora, procesadores y otros aparatos electrónicos para procesar datos.

Bajo "asistido por computadora", se puede entender en el contexto de la invención por ejemplo una implementación del procedimiento en el que, en particular, un procesador ejecuta al menos una etapa del procedimiento.

Bajo un procesador se puede entender en el contexto de la invención por ejemplo una máquina o un circuito electrónico. Un procesador puede ser en particular un procesador principal (en inglés Central Processing Unit, CPU), un microprocesador o un microcontrolador, por ejemplo un circuito integrado específico de la aplicación o un procesador de señales digitales, posiblemente en combinación con una unidad de memoria para memorizar instrucciones de programa, etc. Un procesador también puede ser por ejemplo un IC (circuito integrado, en inglés Integrated Circuit) en particular una FPGA (matriz de compuertas lógicas programable, en inglés Field Programmable Gate Array) o un ASIC (circuito integrado específico de la aplicación, en inglés Application-Specific Integrated Circuit) o un DSP (procesador de señales digitales, en inglés Digital Signal Processor) o un procesador gráfico GPU (Graphic Processing Unit). También se puede entender que un procesador significa un procesador virtualizado, una máquina virtual o una Soft-CPU. Por ejemplo también puede tratarse de un procesador programable que está equipado con etapas de configuración para ejecutar el procedimiento mencionado correspondiente a la invención o está configurado con etapas de configuración de modo que el procesador programable realice

las características correspondientes a la invención del procedimiento, del componente, de los módulos o de otros aspectos y/o aspectos parciales de la invención.

Bajo una "unidad de memoria", un "módulo de memoria" y similares, se puede entender en el contexto de la invención, por ejemplo una memoria volátil en forma de memoria de trabajo (memoria de acceso aleatorio, en inglés Random Access Memory, RAM) o una memoria permanente como un disco duro o un soporte de datos.

Bajo un "módulo" se puede entender en el contexto de la invención por ejemplo un procesador y/o una unidad de memoria para memorizar instrucciones de programa. Por ejemplo, el procesador está configurado especialmente para ejecutar las instrucciones del programa para que el procesador ejecute funciones para implementar o realizar el procedimiento correspondiente a la invención o una etapa del procedimiento correspondiente a la invención. Un módulo puede ser por ejemplo también un nodo del sistema de base de datos distribuida, que por ejemplo realiza las funciones/características específicas de un módulo correspondiente. Los correspondientes módulos pueden por ejemplo también estar configurados como módulos separados y/o autónomos. Para ello, los módulos correspondientes pueden incluir por ejemplo elementos adicionales. Estos elementos son, por ejemplo, una o varias interfaces (por ejemplo interfaces de base de datos, interfaces de comunicación, por ejemplo interfaz de red, interfaz WLAN) y/o una unidad de evaluación (por ejemplo un procesador) y/o una unidad de memoria. Mediante las interfaces se pueden intercambiar por ejemplo datos (por ejemplo recibir, transmitir, enviar o proporcionar). Mediante la unidad de evaluación pueden compararse, verificarse, procesarse, asociarse o calcularse datos, por ejemplo de manera asistida por computadora y/o automatizada. Mediante la unidad de memoria se pueden memorizar, descargar o proporcionar datos de manera asistida por computadora y/o automatizada.

Bajo "incluir", en particular con respecto a datos y/o informaciones, puede entenderse en el contexto de la invención por ejemplo una memorización (asistida por computadora) de una información correspondiente o de una fecha correspondiente en una estructura de datos/registro de datos (que por ejemplo a su vez está memorizada/o en una unidad de memoria).

Bajo "asignar", en particular con respecto a datos y/o informaciones, puede entenderse en relación con la invención por ejemplo una asignación de datos y/o informaciones asistida por computadora. Por ejemplo a una primera fecha se le asigna una segunda fecha utilizando una dirección de memoria o un identificador inequívoco (en inglés unique identifier, UID), memorizándose por ejemplo la primera fecha junto con la dirección de memoria o el identificador inequívoco de la segunda fecha junto con un registro de datos.

Bajo “aportar o proporcionar”, en particular con respecto a datos y/o informaciones, puede entenderse en el contexto de la invención por ejemplo una aportación asistida por computadora. La aportación tiene lugar por ejemplo a través de una interfaz (por ejemplo una interfaz de base de datos, una interfaz de red, una interfaz hacia una unidad de memoria). A través de esta interfaz pueden por ejemplo transmitirse y/o enviarse y o descargarse y/o recibirse los datos y/o informaciones correspondientes al aportarlos.

Bajo “aportar o proporcionar" también puede entenderse en el contexto de la invención por ejemplo, cargar o memorizar por ejemplo una transacción con los datos correspondientes. Esto se puede realizar, por ejemplo en o desde un módulo de memoria. También se puede entender que "aportar o proporcionar" significa por ejemplo una transmisión (o un envío o una transferencia) de datos correspondientes de un nodo a otro nodo de la cadena de bloques o del sistema de base de datos distribuida (o de su infraestructura).

Bajo "proceso de contrato inteligente" en relación con la invención puede entenderse en particular una ejecución de un código de programa (por ejemplo de las órdenes de control) en un proceso mediante el sistema de base de datos distribuida y/o su infraestructura.

Bajo una "suma de comprobación", por ejemplo una suma de comprobación de bloques de datos, una suma de comprobación de datos, una suma de comprobación de nodo, una suma de comprobación de transacción, una suma de comprobación de encadenamiento o similares, puede entenderse en relación con la invención por ejemplo una suma de comprobación criptográfica o hash criptográfico o bien valor hash, que en particular se forman o calculan mediante una función hash criptográfica por medio de un registro de datos y/o datos y/o una o más de las transacciones y/o una zona parcial de un bloque de datos (por ejemplo el encabezamiento del bloque de un bloque de una cadena de bloques o encabezamiento de bloque de datos de un bloque de datos del sistema de base de datos distribuida o sólo una parte de las transacciones de un bloque de datos). Bajo una suma de comprobación puede entenderse en particular una suma o sumas de comprobación o valor/es hash de un árbol de hash (por ejemplo, árbol de Merkle, árbol de Patricia). Además, puede entenderse bajo ello en particular también una firma digital o un código criptográfico de autentificación de mensajes. Mediante las sumas de comprobación puede por ejemplo realizarse a distintos niveles del sistema de base de datos una protección criptográfica/protección frente a manipulación para las transacciones y los (registros de) datos allí memorizados. Si por ejemplo se requiere un alto nivel de seguridad, se generan y comprueban por ejemplo las sumas de comprobación a nivel de transacción. Si se requiere menos seguridad, se generan y comprueban las sumas de

comprobación a nivel de bloque (por ejemplo sobre todo el bloque de datos o sólo sobre una parte del bloque de datos y/o una parte de las transacciones).

Bajo una "suma de comprobación de bloques de datos" puede entenderse en relación con la invención una suma de comprobación, que se calcula por ejemplo sobre una parte o la totalidad de las transacciones de un bloque de datos. Un nodo puede entonces por ejemplo comprobar/determinar la integridad/autenticidad de la parte correspondiente de un bloque de datos utilizando la suma de comprobación del bloque de datos. Adicional o alternativamente, puede haberse formado la suma de comprobación del bloque de datos en particular también mediante transacciones de un bloque de datos anterior/bloque de datos predecesor del bloque de datos. La suma de comprobación del bloque de datos también puede implementarse entonces en particular mediante un árbol hash, por ejemplo un árbol de Merkle [1] o un árbol de Patricia, siendo la suma de comprobación del bloque de datos en particular la suma de comprobación de raíz del árbol de Merkle o de un árbol de Patricia o de un árbol hash binario. En particular se aseguran transacciones mediante sumas de comprobación adicionales a partir del árbol de Merkle o árbol de Patricia (por ejemplo utilizando las sumas de comprobación de transacción), siendo en particular las sumas de comprobación adicionales hojas en el árbol de Merkle o árbol de Patricia. La suma de comprobación del bloque de datos puede así por ejemplo asegurar las transacciones, al formarse la suma de comprobación de raíz a partir de las sumas de comprobación adicionales. La suma de comprobación del bloque de datos se puede calcular en particular para transacciones de un bloque de datos determinado de los bloques de datos. En particular, dicha suma de comprobación de bloque de datos se puede incluir en un bloque de datos siguiente al bloque de datos determinado para encadenar este bloque de datos siguiente por ejemplo con sus bloques de datos precedentes y en particular para poder comprobar la integridad del sistema de base de datos distribuida. De esta manera la suma de comprobación del bloque de datos puede por ejemplo asumir la función de la suma de comprobación de encadenamiento o ser incluida en la suma de comprobación de encadenamiento. El encabezamiento de un bloque de datos (por ejemplo de un nuevo bloque de datos o del bloque de datos para el que se ha formado la suma de comprobación del bloque de datos) puede incluir por ejemplo la suma de comprobación del bloque de datos.

Bajo "suma de comprobación de la transacción" puede entenderse en relación con la invención una suma de comprobación que se forma en particular sobre una transacción de un bloque de datos. Adicionalmente por ejemplo se puede acelerar el cálculo de una suma de comprobación de bloque de datos para un bloque de datos correspondiente, ya que para ello pueden utilizarse por ejemplo sumas de comprobación de transacciones ya calculadas, directamente como hojas por ejemplo de un árbol de Merkle.

Bajo una "suma de comprobación de encadenamiento" puede entenderse en relación con la invención una suma de comprobación que en particular indica o referencia un bloque de datos correspondiente del sistema de base de datos distribuida al bloque de datos anterior del sistema de base de datos distribuida (denominado, en particular frecuentemente en la literatura especializada "previous block hash" (hash del bloque anterior) [1]. Para ello se forma una suma de comprobación de encadenamiento correspondiente, en particular para el bloque de datos anterior correspondiente. Como suma de comprobación de encadenamiento puede utilizarse por ejemplo una suma de comprobación de transacción o la suma de comprobación del bloque de datos de un bloque de datos (es decir, un bloque de datos existente del sistema de base de datos distribuida) para encadenar un nuevo bloque de datos con un bloque de datos (existente) del sistema de base de datos distribuida. Sin embargo, también es posible, por ejemplo, que una suma de comprobación se pueda formar mediante un encabezamiento (header) del bloque de datos precedente o mediante el bloque de datos precedente completo y se utilice como suma de comprobación de encadenamiento. Esto también se puede calcular por ejemplo para varios o todos los bloques de datos anteriores. También es posible, por ejemplo, que la suma de comprobación de encadenamiento se forme mediante el encabezamiento de un bloque de datos y la suma de comprobación del bloque de datos. Sin embargo, un bloque de datos correspondiente del sistema de base de datos distribuida incluye preferiblemente en cada caso una suma de comprobación de encadenamiento calculada para un bloque de datos anterior, en particular incluso más preferiblemente el bloque de datos directamente precedente, del bloque de datos respectivo o bien se relaciona con éste. También es posible, por ejemplo, formar una suma de comprobación de encadenamiento correspondiente sólo sobre una parte del bloque de datos correspondiente (por ejemplo, bloque de datos precedente). De esta manera, por ejemplo, se puede realizar un bloque de datos que incluye una parte de integridad protegida y una parte no protegida. Con ello se podría realizar por ejemplo un bloque de datos cuya parte de integridad protegida sea invariable y cuya parte no protegida pueda modificarse posteriormente. Bajo integridad protegida ha de entenderse aquí en particular que un cambio en los datos de integridad protegida puede detectarse mediante una suma de comprobación.

Los datos que se memorizan por ejemplo en una transacción de un bloque de datos, se pueden proporcionar en particular de diferentes maneras. En lugar de los datos, por ejemplo datos del usuario, como datos de medición, valores de medición, valores de control o datos/relaciones de propiedad con activos (assets), puede incluir por ejemplo una transacción de un bloque de datos solamente la suma de comprobación para estos datos. La suma de comprobación correspondiente se puede realizar entonces de diferentes maneras. Puede tratarse por ejemplo de una suma de comprobación del bloque de datos

correspondiente de un bloque de datos (con los datos correspondientes) de otro base de datos o del sistema de base de datos distribuida, una suma de comprobación de transacción de un bloque de datos con los datos correspondientes (del sistema de base de datos distribuida o de otro base de datos) o de una suma de comprobación de datos formada sobre los datos.

Además, la transacción correspondiente puede contener una referencia o una indicación hacia un lugar de memoria (por ejemplo una dirección de un servidor de archivos e indicaciones de dónde se pueden encontrar los datos correspondientes en el servidor de archivos (fileserver); o una dirección de otro base de datos distribuida que incluye los datos). Los datos correspondientes también podrían proporcionarse entonces por ejemplo en una transacción adicional de otro bloque de datos del sistema de base de datos distribuida (por ejemplo si los datos correspondientes y las sumas de comprobación asociadas están contenidos en diferentes bloques de datos). Pero también es concebible por ejemplo que estos datos se aporten a través de otro canal de comunicación (por ejemplo a través de otra base de datos y/o un canal de comunicación protegido criptográficamente).

Además de la suma de comprobación, también puede estar archivado por ejemplo un registro de datos adicionales (por ejemplo una referencia o una indicación relativa a un lugar de memoria) en la transacción correspondiente, que en particular indica un lugar de memoria de donde pueden descargarse los datos. Esto es en particular ventajoso para mantener un volumen de datos de la cadena de bloques o del sistema de base de datos distribuida lo más pequeño posible.

Bajo “seguridad protegida” puede entenderse en relación con la invención por ejemplo una protección que se realiza en particular mediante un procedimiento criptográfico. Por ejemplo, esto se puede realizar utilizando el sistema de base de datos distribuida para aportar o transmitir o enviar datos/transacciones correspondientes. Esto se logra preferiblemente mediante una combinación de las diversas sumas de comprobación (criptográficas), en particular interaccionando las mismas sinérgicamente, por ejemplo para mejorar la seguridad o la seguridad criptográfica para los datos de las transacciones. En otras palabras, bajo "seguridad protegida" en relación con la invención también puede entenderse en particular "protegido criptográficamente" y/o "protegido frente a manipulaciones". "Protegido frente a manipulaciones" también puede denominarse "de integridad protegida".

Bajo "encadenamiento de/de los bloques de datos de un sistema de base de datos distribuida" puede entenderse en relación con la invención, por ejemplo, que unos bloques de datos incluyen en cada caso una información (por ejemplo suma de comprobación de encadenamiento), que remite o referencia a otro bloque de datos u otros varios bloques de datos del sistema de base de datos distribuida, [1] [4] [5].

Bajo "insertar en el sistema de base de datos distribuida" y similares, puede entenderse en relación con la invención por ejemplo que en particular una transacción o las transacciones o un bloque de datos con sus transacciones se transmite a uno o varios nodos de un sistema de base de datos distribuida. Si por ejemplo estas transacciones se validan con éxito (por ejemplo por parte del/de los nodo/s), se encadenan estas transacciones en particular como nuevo bloque de datos con al menos un bloque de datos existente del sistema de base de datos distribuida [1] [4] [5]. Para ello las transacciones correspondientes se memorizan por ejemplo en un nuevo bloque de datos. En particular, esta validación y/o encadenamiento puede realizarse mediante un nodo confiable (por ejemplo un nodo de minería, un oráculo de cadenas de bloques o una plataforma de cadenas de bloques). En particular puede entenderse entonces bajo una plataforma de cadenas de bloques una cadena de bloques como servicio (Service), tal como proponen en particular Microsoft o IBM. En particular, un nodo confiable y/o un nodo pueden archivar en cada caso una suma de comprobación de nodo (por ejemplo una firma digital) en un bloque de datos (por ejemplo en el bloque de datos validado y generado por ellos, que a continuación se encadena), en particular para permitir que se pueda identificar el creador del bloque de datos y/o para que se pueda identificar el nodo. Entonces indica esta suma de comprobación de nodo qué nodo por ejemplo ha encadenado el bloque de datos correspondiente con al menos otro bloque de datos del sistema de base de datos distribuida.

Bajo "transacción" o "transacciones" se puede entender en relación con la invención por ejemplo un contrato inteligente [4] [5], una estructura de datos o un registro de datos de transacción, que en particular incluye en cada caso una de las transacciones o varias transacciones. Bajo "transacción" o “transacciones” pueden entenderse en relación con la invención por ejemplo también los datos de una transacción de un bloque de datos de una cadena de bloques (en inglés blockchain). Una transacción puede incluir en particular un código de programa que por ejemplo realiza un contrato inteligente. Por ejemplo, en relación con la invención, una transacción también puede entenderse como una transacción de control y/o una transacción de confirmación. Alternativamente, una transacción puede ser por ejemplo una estructura de datos que memoriza datos (por ejemplo las órdenes de control y/o datos contractuales y/u otros datos como datos de video, datos útiles, datos de medición, etc.).

En particular bajo "memorizar transacciones en bloques de datos", "memorizar transacciones" y similares ha de entenderse una memorización directa o memorización indirecta. Bajo una memorización directa puede entenderse aquí, por ejemplo, que el bloque de datos correspondiente (del sistema de base de datos distribuida o la transacción correspondiente del sistema de base de datos distribuida) incluye los

datos respectivos. Bajo una memorización indirecta puede entenderse aquí por ejemplo que el bloque de datos correspondiente o la transacción correspondiente incluye una suma de comprobación y opcionalmente un registro de datos adicional (por ejemplo una referencia o una indicación de un lugar de memoria) para los datos correspondientes y por lo tanto los datos correspondientes no están memorizados directamente en el bloque de datos (o en la transacción), (es decir, en lugar de ello sólo una suma de comprobación para estos datos). En particular, al memorizar transacciones en bloques de datos pueden por ejemplo validarse estas sumas de comprobación, tal como se ha explicado por ejemplo bajo “incluir en el sistema de base de datos distribuida”.

Bajo un "código de programa" (por ejemplo, un contrato inteligente) puede entenderse en relación con la invención, por ejemplo, una instrucción de programa o varias instrucciones de programa, que se memorizan en particular en una o varias transacciones. El código del programa puede ejecutarse en particular y se ejecuta por ejemplo mediante el sistema de base de datos distribuida. Esto se puede realizar por ejemplo utilizando un entorno de ejecución (por ejemplo, una máquina virtual), siendo con preferencia Turing completo el entorno de ejecución o el código del programa. El código del programa es ejecutado preferiblemente por la infraestructura del sistema de base de datos distribuida [4] [5]. Entonces por ejemplo una máquina virtual se realiza mediante la infraestructura del sistema de base de datos distribuida.

Bajo un "contrato inteligente" (Smart Contract) puede entenderse en relación con la invención por ejemplo un código de programa ejecutable [4] [5] (véase en particular la definición de "código de programa"). El contrato inteligente está memorizado preferiblemente en una transacción de un sistema de base de datos distribuida (por ejemplo una cadena de bloques), por ejemplo en un bloque de datos del sistema de base de datos distribuida. Por ejemplo el contrato inteligente puede ejecutarse de la misma manera que se ha explicado en la definición de "código de programa", en particular en relación con la invención.

Bajo "prueba de trabajo" o " comprobación de prueba de trabajo" puede entenderse en relación con la invención por ejemplo, una solución de una tarea intensiva en cálculo, que ha de resolverse en particular en función del contenido del bloque de datos/ contenido de una determinada transacción [1] [4] [5]. Una tal tarea intensiva en cálculo también se denomina por ejemplo puzzle criptográfico.

Bajo un "sistema de base de datos distribuida", que por ejemplo también puede denominarse base de datos distribuida, puede entenderse en relación con la invención por ejemplo un base de datos distribuida descentrizadamente, una cadena de bloques (en inglés blockchain), un libro mayor (ledger) distribuido, un sistema de memoria distribuido, un sistema (DLTS) basado en la tecnología de libro mayor distribuido (DLT), un sistema de base de datos a prueba de revisiones, una nube (cloud), un servicio en la nube, una cadena de bloques en una nube o un base de datos punto a punto (peer-to-peer). También se pueden utilizar por ejemplo diferentes implementaciones de una cadena de bloques o de un DLTS, como por ejemplo una cadena de bloques o un DLTS que utilizan un gráfico acíclico dirigido (Directed Acyclic Graph, DAG), un puzzle criptográfico, un gráfico hash o una combinación de las variantes de implementación mencionadas [6] [7]. También pueden implementarse por ejemplo distintas reglas de consenso o procedimientos de consenso (en inglés, consensus algorithms). Esto puede ser, por ejemplo, un procedimiento de consenso mediante un puzzle criptográfico, Gossip about Gossip (chismes sobre chismes), Virtual Voting (votación virtual) o una combinación de los citados procedimientos (por ejemplo Gossip about Gossip combinado con Virtual Voting) [6] [7]. Si por ejemplo se utiliza una cadena de bloques, esto se puede implementar en particular mediante una realización basada en Bitcoin o una realización basada en Ethereum [1] [4] [5]. Bajo un "sistema de base de datos distribuida" puede entenderse por ejemplo también un sistema de base de datos distribuida, del cual al menos una parte de sus nodos y/o aparatos y/o infraestructura están realizados mediante una nube (cloud). Por ejemplo están realizados los componentes correspondientes como nodos/aparatos en la nube (por ejemplo como nodo virtual en una máquina virtual). Esto se puede realizar por ejemplo mediante productos VM, Amazon Web Services o Microsoft Azure. Debido a la gran flexibilidad de las variantes de implementación explicadas, se pueden combinar entre sí en particular también aspectos parciales de las variantes de implementación citadas, utilizándose por ejemplo un gráfico hash como cadena de bloques, pudiendo también por ejemplo carecer de bloques la propia cadena de bloques.

Si por ejemplo se utiliza un Directed Acyclic Graph (DAG), por ejemplo IOTA o Tangle, entonces están conectadas en particular transacciones o bloques o nodos del gráfico entre sí a través de bordes dirigidos. Esto significa en particular que (todos) los bordes (siempre) tienen la misma dirección, similarmente por ejemplo a como sucede en el tiempo. En otras palabras, en particular no es posible iniciar o saltar a las transacciones o los bloques o los nodos del gráfico hacia atrás (es decir, en contra de la misma dirección común). Acíclico significa aquí en particular que no existe ningún bucle cuando se ejecuta el gráfico.

El sistema de base de datos distribuida puede ser, por ejemplo, un sistema de base de datos distribuida público (por ejemplo, una cadena de bloques pública) o un sistema de base de datos distribuida cerrado (o privado) (por ejemplo, una cadena de bloques privada).

Si es por ejemplo un sistema de base de datos distribuida público, esto significa que al sistema de base de datos distribuida pueden acceder o bien puede aceptar el mismo nuevos nodos y/o aparatos sin acreditación o sin autentificación o sin anunciarse debidamente o sin credenciales. En tal caso, en particular, los operadores de los nodos y/o aparatos pueden permanecer en el anónimato. Si el sistema de base de datos distribuida es, por ejemplo, un sistema de base de datos distribuida cerrado, los nuevos nodos y/o aparatos requieren, por ejemplo, una acreditación válida y/o información de autentificación válida y/o credenciales válidas y/o anunciarse debidamente para poder acceder al sistema de base de datos distribuida y/o para ser aceptado por el mismo.

Un sistema de base de datos distribuida también puede ser, por ejemplo, un sistema de comunicación distribuido para el intercambio de datos. Ésto puede ser, por ejemplo, una red o una red peer-2-peer (punto a punto).

Bajo "bloque de datos", que también puede denominarse "miembro" o "bloque", en particular según el contexto y la realización, puede entenderse en relación con la invención por ejemplo un bloque de datos de un sistema de base de datos distribuida (por ejemplo una cadena de bloques o un base de datos punto a punto), que está realizado en particular como estructura de datos y que preferiblemente incluye una de las transacciones o varias de las transacciones. En una implementación, la base de datos (o el sistema de base de datos) puede ser por ejemplo un sistema basado en DLT (DLTS) o una cadena de bloques y un bloque de datos puede ser un bloque de la cadena de bloques o del DLTS. Un bloque de datos puede incluir por ejemplo información sobre el tamaño (tamaño de datos en bytes) del bloque de datos, un encabezamiento de bloque de datos (en inglés block-header), un contador de transacciones y una o varias transacciones [1]. El encabezamiento del bloque de datos puede incluir por ejemplo una versión, una suma de comprobación de encadenamiento, una suma de comprobación de bloque de datos, una marca de tiempo, una acreditación de Proof-of-Work y un nonce (valor para una sola vez, valor aleatorio o contador, que se utiliza para la acreditación de Proof-of-Work) [1] [4] [5]. Un bloque de datos también puede ser, por ejemplo, solo una determinada zona de memoria o una zona de direcciones del conjunto de datos que están memorizados en el sistema de base de datos distribuida. Con ello pueden realizarse por ejemplo sistemas de base de datos distribuidas sin bloques (en inglés blockless), como por ejemplo la cadena de IoT (ITC), IOTA y Byteball. Entonces se combinan entre sí en particular las funcionalidades de los bloques de una cadena de bloques y de las transacciones de tal manera que, por ejemplo las transacciones mismas aseguran la secuencia o cadena de transacciones (del sistema de base de datos distribuida), memorizándose en particular con seguridad protegida. Para ello pueden por ejemplo encadenarse las propias transacciones entre sí por ejemplo con una suma de comprobación de encadenamiento, en el sentido de que con preferencia una suma de comprobación separada o la suma de comprobación de la transacción de una o varias transacciones sirve como suma de comprobación de encadenamiento, que al memorizar una nueva transacción en el sistema de base de datos distribuida se memoriza a la vez en la correspondiente nueva transacción. En una tal forma de realización, un bloque de datos también puede incluir por ejemplo una o varias transacciones, por ejemplo, en el caso más simple, un bloque de datos correspondiente a una transacción.

Bajo "nonce" puede entenderse en relación con la invención por ejemplo un nonce criptográfico (abreviatura de: "used only once" o usado sólo una vez [2] o "number used once", número usado una vez) [3]). En particular un nonce designa una combinación individual de números o una combinación de letras, que se utiliza preferiblemente sólo una vez en el contexto correspondiente (por ejemplo transacción, transmisión de datos).

Bajo "bloques de datos anteriores a un (determinado) bloque de datos del sistema de base de datos distribuida" puede entenderse en relación con la invención, por ejemplo, el bloque de datos del sistema de base de datos distribuida que en particular precede directamente a un (determinado) bloque de datos. Alternativamente, bajo "bloques de datos anteriores a un (determinado) bloque de datos del sistema de base de datos distribuida" también pueden entenderse, en particular, todos los bloques de datos del sistema de base de datos distribuida que preceden al bloque de datos determinado. De esta manera puede formarse por ejemplo la suma de comprobación de encadenamiento o la suma de comprobación de la transacción en particular sólo sobre el bloque de datos (o sus transacciones) que precede directamente al bloque de datos determinado o sobre todos los bloques de datos (o sus transacciones) que preceden al primer bloque de datos.

Bajo un "nodo de cadena de bloques", "nodo", "nodo de un sistema de base de datos distribuida", "equipo de nodo" y similares, pueden entenderse en relación con la invención por ejemplo aparatos (por ejemplo, aparatos de campo, teléfonos móviles), computadoras, teléfonos inteligentes, clientes o participantes, que realizan operaciones (con) el sistema de base de datos distribuida (por ejemplo una cadena de bloques) [1] [4] [5]. Tales nodos pueden, por ejemplo, ejecutar transacciones de un sistema de base de datos distribuida o de sus bloques de datos o insertar o encadenar nuevos bloques de datos con nuevas transacciones en el sistema de base de datos distribuida mediante nuevos bloques de datos. En particular, esta validación y/o encadenamiento puede realizarse mediante un nodo confiable (por ejemplo un Mining Node o nodo de minería) o exclusivamente mediante nodos confiables. Un nodo confiable es por ejemplo un nodo que dispone de medidas de seguridad adicionales (por ejemplo firewalls, limitaciones de acceso al nodo o similares), para impedir una manipulación del nodo. Alternativa o adicionalmente, un

nodo confiable puede por ejemplo, cuando se encadena un nuevo bloque de datos con el sistema de base de datos distribuida, memorizar una suma de comprobación de nodo (por ejemplo una firma digital o un certificado) en el nuevo bloque de datos. Con ello puede aportarse en particular una acreditación que indica que el bloque de datos correspondiente ha sido insertado por un nodo determinado o indica su origen. Los aparatos (por ejemplo el aparato correspondiente) son por ejemplo aparatos de un sistema técnico y/o instalación industrial y/o de una red de automatización y/o de una instalación fabril, que son en particular también un nodo del sistema de base de datos distribuida. Entonces pueden ser los aparatos por ejemplo aparatos de campo o aparatos en Internet de las Cosas, que en particular también son un nodo del sistema de base de datos distribuida. Los nodos también pueden incluir al menos un procesador para por ejemplo realizar su funcionalidad implementada en computadora.

Bajo un "oráculo de cadena de bloques" y similares se pueden entender en relación con la invención por ejemplo nodos, aparatos o computadoras, que por ejemplo tienen un módulo de seguridad, que por ejemplo está implementado mediante mecanismos de protección de software (por ejemplo procedimientos criptográficos), equipos de protección mecánicos (por ejemplo una carcasa que puede cerrarse) o equipos de protección eléctricos (por ejemplo protección tamper o antimanipulación o un sistema de protección que elimina los datos del módulo de seguridad en caso de utilización/tratamiento inadmisible del oráculo de cadena de bloques). El módulo de seguridad puede incluir entonces, por ejemplo, claves criptográficas que se necesitan para calcular las sumas de comprobación (por ejemplo sumas de comprobación de transacciones o sumas de comprobación de nodo).

Bajo una "computadora" o un "aparato" se puede entender en relación con la invención por ejemplo, una computadora (sistema de computadora), un cliente, un teléfono inteligente, un aparato o un servidor, cada uno de los cuales está dispuesto fuera de la cadena de bloques o bien que no es ningún participante del sistema de base de datos distribuida (por ejemplo de la cadena de bloques) (es decir, no realizan ninguna operación con el sistema de base de datos distribuida o sólo lo consultan, pero sin realizar transacciones, insertar bloques de datos o calcular acreditaciones de prueba de trabajo). Alternativamente puede entenderse en particular también bajo una computadora un nodo del sistema de base de datos distribuida. En otras palabras, bajo un aparato puede entenderse en particular un nodo del sistema de base de datos distribuida o también un aparato de fuera de la cadena de bloques o del sistema de base de datos distribuida. Un aparato de fuera del sistema de base de datos distribuida puede por ejemplo acceder a los datos (por ejemplo transacciones o transacciones de control) del sistema de base de datos distribuida y/o ser controlado por nodos (por ejemplo mediante contratos inteligentes y/u oráculos de cadena de bloques). Si por ejemplo se realiza un manejo y/o control de un aparato (por ejemplo un aparato diseñado como nodo o un aparato de fuera del sistema de base de datos distribuida) mediante un nodo, esto puede realizarse por ejemplo mediante un contrato inteligente, que está memorizado en particular en una transacción del sistema de base de datos distribuida.

Otras posibles implementaciones de la invención también incluyen combinaciones no citadas explícitamente de características o formas de realización descritas anteriormente o a continuación con referencia a los ejemplos de realización. El experto en la materia también añadirá aspectos individuales como mejoras o adiciones a la correspondiente forma básica de la invención.

Otras mejoras y aspectos ventajosos de la invención son objeto de las reivindicaciones secundarias, así como de los ejemplos de realizaciones de la invención que se describen a continuación. La invención se explica con más detalle a continuación en base a formas de realización preferidas con referencia a las figuras adjuntas.

Figura 1 muestra esquemáticamente un equipo de formación de bloques según un primer ejemplo de realización;
figura 2 muestra un diagrama de flujo de un procedimiento de formación de bloques según el primer ejemplo de realización;
figura 3 muestra esquemáticamente un equipo de nodo según un segundo ejemplo de realización;
figura 4 muestra un diagrama de flujo de un procedimiento de confirmación de bloque según el segundo ejemplo de realización;
figura 5 muestra esquemáticamente un equipo de nodo según un perfeccionamiento del primer y segundo ejemplos de realización;
figura 6 muestra un sistema de base de datos distribuida según un tercer ejemplo de realización;
figura 7 muestra un cronometraje del sistema de base de datos distribuida según una variante del tercer ejemplo de realización;
figura 8 muestra esquemáticamente un bloque no confirmado según ejemplos de realización;
figura 9 muestra un libro de transacciones del sistema de base de datos distribuida según una variante del tercer ejemplo de realización y
figura 10 muestra un sistema de base de datos distribuida según un cuarto ejemplo de realización.

En las figuras se han dotado los elementos que son iguales o tienen la misma función de las mismas referencias, salvo que se indique lo contrario.

La figura 1 muestra esquemáticamente un equipo de formación de bloques 10 y la figura 2 muestra un diagrama de flujo de un procedimiento de formación de bloques según el primer ejemplo de realización. El equipo de formación de bloques 10 y el procedimiento de formación de bloques según el primer ejemplo de realización se describirán ahora con referencia a las figuras 1 y 2.

El equipo de formación de bloques 10 tiene una primera unidad 1, una segunda unidad 2 y una tercera unidad 3. En un sistema de base de datos distribuida (no mostrado), al que pertenece el equipo de formación de bloques 10, se proporciona un conjunto de transacciones no confirmadas 41, 42, 43. Así se proporciona el conjunto de transacciones no confirmadas 41, 42 43 también al equipo de formación de bloques 10.

El equipo de formación de bloques 10 está configurado para formar un bloque 61 no confirmado correspondiente cronometrado a partir de transacciones elegidas de entre las transacciones 41, 42, 43 no confirmadas, que se puede confirmar mediante equipos de nodo (no mostrados) del sistema de base de datos distribuida (no mostrado) incluyéndolo en un libro de transacciones del sistema de base de datos distribuida según una regla de consenso del sistema de base de datos distribuida.

En especial, la tercera unidad 3 es un receptor de tiempo. En la etapa S30, la tercera unidad 3 recibe repetida o cíclicamente impulsos de reloj desde un reloj (no mostrado).
El reloj puede ser un reloj interno del equipo de formación de bloques 1 o un reloj externo. Los impulsos de reloj pueden ser una secuencia de impulsos de tiempo o una secuencia de indicaciones de tiempo. En función de los impulsos de reloj recibidos, la tercera unidad 3 determina segmentos de tiempo de una longitud predeterminada.

Durante cada uno de los segmentos de tiempo, la primera unidad 1 y la segunda unidad 2 del equipo de formación de bloques 10 llevan a cabo las siguientes etapas, exactamente una vez:

En la etapa S10, la primera unidad 1 elige un conjunto de transacciones a confirmar a partir de las transacciones no confirmadas 41, 42, 43 proporcionadas.

En la etapa S20, la segunda unidad 2 forma un bloque no confirmado 61 a partir de las transacciones elegidas a confirmar.

En particular, la segunda unidad 2 puede verificar la validez de las transacciones elegidas 41, 42, 43 a confirmar y rechazar las transacciones inválidas. En particular, la segunda unidad 2 puede formar el bloque no confirmado 61 según una regla de consenso acordada en el sistema de base de datos distribuida. En particular, la segunda unidad 2 puede insertar un valor de verificación requerido por la regla de consenso, tal como una prueba de trabajo, en el bloque no confirmado 61 a formar.

La segunda unidad 2 finaliza con garantía la formación del bloque no confirmado 61 dentro del segmento de tiempo correspondiente y proporciona el bloque no confirmado 61 formado en el sistema de base de datos distribuida (no mostrado). Por ejemplo, la segunda unidad 2 puede transmitir el bloque no confirmado 61 formado al menos a otro equipo de nodo (no mostrado) del sistema de base de datos distribuida.

El equipo de formación de bloques 10 permite ventajosamente que se forme exactamente un bloque no confirmado dentro de cada segmento de tiempo.

Según un perfeccionamiento preferido, la primera unidad 1 elige en el segmento de tiempo correspondiente todas las transacciones no confirmadas 41-43 proporcionadas en el sistema de base de datos distribuida. En consecuencia, se puede asegurar que todas las transacciones no confirmadas proporcionadas se incluyen exactamente en un bloque no confirmado dentro de cada segmento de tiempo.

Según otro perfeccionamiento preferido, la primera unidad 1 elige en el segmento de tiempo correspondiente todas las transacciones no confirmadas 41 - 43 proporcionadas en el sistema de base de datos distribuida que responden a una condición predeterminada. En consecuencia, se puede asegurar que dentro de cada segmento de tiempo se incluyen al menos todas aquellas transacciones no confirmadas proporcionadas que corresponden a la condición predeterminada exactamente en un bloque no confirmado. Por ejemplo, se eligen todas las transacciones no confirmadas que están marcadas como de tiempo crítico, que están marcadas como transacción de valor de sensor o transacción de valor medido o contrato inteligente de orden de control, o similares.
La figura 3 muestra esquemáticamente un equipo de nodo 20 y la figura 4 muestra un diagrama de flujo de un procedimiento de confirmación de bloques según un segundo ejemplo de realización. Remitimos a las figuras 3 y 4.

El equipo de nodo 20 tiene una tercera unidad 3, una quinta unidad 5 y una sexta unidad 6. En la quinta unidad está memorizada una cadena de bloques previamente confirmados 71, 72, que representa un libro de transacciones de un sistema de base de datos distribuida (no mostrado). En el sistema de base de

datos distribuida (no mostrado) que pertenece al equipo de nodo 20, se proporciona un conjunto de bloques no confirmados 61, 62. La aportación la ha realizado por ejemplo un conjunto de equipos de formación de bloques 10 en la figura 1.

El equipo de nodo 20 está configurado para elegir cronometrado un bloque a confirmar de entre los bloques no confirmados 61, 62 proporcionados en el sistema de base de datos distribuida y para confirmar el bloque elegido a confirmar, con lo que el bloque confirmado 73 queda añadido a la cadena de bloques confirmados 71, 72, 73.

En especial, la tercera unidad 3 es un receptor de tiempo. En la etapa S30, la tercera unidad 3 recibe repetida o cíclicamente impulsos de reloj desde un reloj (no mostrado). En función de los impulsos de reloj recibidos, la tercera unidad 3 determina segmentos de tiempo de una longitud predeterminada.

Durante cada uno de los segmentos de tiempo, la sexta unidad 6 realiza la siguiente etapa exactamente una vez:

En la etapa S60, la sexta unidad 6 elige exactamente uno de los bloques no confirmados 61, 62 y confirma el bloque elegido. Entonces el bloque elegido se agrega como bloque confirmado 73 a la cadena de bloques previamente confirmados 71, 72, con lo que el bloque confirmado 73 queda agregado a la cadena de bloques confirmados 71, 72, 73.

En particular, la sexta unidad 6 puede elegir el bloque a confirmar de entre los bloques no confirmados 61, 62 proporcionados en el segmento de tiempo respectivo, según una regla de consenso de la base de datos distribuida.

Entonces, la sexta unidad 6 puede verificar en particular cada uno de los bloques no confirmados 61, 62 proporcionados en el segmento de tiempo respectivo, que se puede agregar a la cadena de bloques previamente confirmados 71, 72, según la regla de consenso. Si se verifica con éxito más de uno de los bloques no confirmados 61, 62, la regla de consenso puede prescribir entonces criterios para elegir uno de los bloques no confirmados comprobados 61, 62.

La sexta unidad 6 agrega a la cadena de bloques previamente confirmados 71, 72 aquél de los bloques no confirmados 61, 62 que se ha de confirmar y así se convierte en otro bloque confirmado 73 de la cadena de bloques confirmados 71, 72, 73. De esta manera, se convierten en particular las transacciones no confirmadas del bloque a confirmar en transacciones del bloque confirmado 73 confirmadas en el libro de transacciones.

La sexta unidad 6 completa la etapa S60 dentro del segmento de tiempo respectivo con garantía.

El equipo de nodo 20 permite ventajosamente agregar exactamente un bloque confirmado a la cadena de bloques confirmados dentro de cada segmento de tiempo.

La figura 5 muestra esquemáticamente un equipo de nodo 30 según un perfeccionamiento del primer y segundo ejemplos de realización.

El equipo de nodo 30 incluye un equipo de formación de bloques 10 en la figura 1 según el primer ejemplo de realización y los elementos del equipo de nodo (20 en la figura 3) según el segundo ejemplo de realización. La tercera unidad 3 está prevista entonces sólo una vez y realiza cronometradamente, según el presente perfeccionamiento actual, tanto el funcionamiento de la primera unidad 1 y de la segunda unidad 2 del equipo de formación de bloques 10, como también el funcionamiento de la sexta unidad 6 del equipo de nodo 30. En otras palabras, el equipo de nodo 30 dispone en particular tanto de funcionalidad para formar bloques no confirmados (por ejemplo, funcionalidad de mining o minería) como también de funcionalidad para confirmar bloques no confirmados, que proporcionan equipos de formación de bloques distintos del equipo de formación de bloques 10 del mismo sistema de base de datos distribuida.

La figura 6 muestra un sistema de base de datos distribuida 100 según un tercer ejemplo de realización.

El sistema de base de datos distribuida 100 incluye varios equipos de nodo 20, 30, 31, 32, que están conectados en red mediante una red 101.El equipo de nodo 20 es un equipo de nodo 20 según el segundo ejemplo de realización, que sólo tiene funcionalidad para confirmar bloques no confirmados. Los equipos de nodo 30, 31 y 32 son equipos de nodo según el perfeccionamiento, que incluyen adicionalmente un equipo de formación de bloques respectivo 3010, 3110, 3210 (instancias del equipo de formación de bloques 10 de la figura 1).

Cada uno de los equipos de nodo 20, 30, 31, 32 tiene una respectiva tercera unidad 203, 303, 313, 323. Las otras unidades de los equipos de nodo 20, 30, 31, 32 corresponden a las del primer o segundo ejemplo de realización, pero no se muestran para simplificar.

Cada uno de los equipos de nodo 20, 30, 31, 32 recibe impulsos de reloj con su respectiva tercera unidad 203, 303, 313, 323. Los respectivos impulsos de reloj recibidos son síncronos.

Así funciona el sistema de base de datos distribuida 100 ventajosamente de manera sincronizada en el tiempo según un ritmo de tiempos común del sistema de base de datos distribuida 100; las respectivas unidades primera, segunda y sexta de los respectivos equipos de nodo 20, 30, 31, 32 realizan las etapas S20, S30, S60 que tienen asignadas sincrónicamente durante el mismo segmento de tiempo en cada caso.

La figura 7 muestra un cronometraje del sistema de base de datos distribuida 100 según una variante del tercer ejemplo de realización. La figura 7 se describirá con referencia a las figuras 1, 3 y 6.

En un instante T0 comienza un segmento de tiempo de uno de los equipos de nodo 20, 30, 31, 32 correspondientes.

Una primera sección de tiempo del segmento de tiempo comienza en el instante T0. Durante la primera sección de tiempo, cada uno de los equipos de nodo 20, 30, 31, 32 puede proporcionar transacciones no confirmadas 41, 42, 43 en el sistema de base de datos distribuida 100.

Por ejemplo, el equipo de nodo 20 puede estar conectado con un componente de automatización de un sistema de automatización industrial y crear una transacción no confirmada, que representa un valor de sensor determinado al comienzo del segmento de tiempo. El equipo de nodo 32 puede tener una interfaz de usuario y puede, por ejemplo, proporcionar una transacción no confirmada, que incluye un contrato inteligente programado por el usuario con órdenes de control para el sistema de automatización industrial.

El sistema de base de datos distribuida 100 está diseñado tal que queda asegurado que cada transacción no confirmada proporcionada haya llegado a todos los equipos de nodo 20, 30, 31, 32 a tiempo antes del instante t1 del segmento de tiempo.

Cada uno de los equipos de formación de bloques 3010, 3110, 3210 recibe las transacciones no confirmadas 41, 42, 43 proporcionadas y elige un conjunto de transacciones a confirmar. Por ejemplo se pueden elegir al menos todas las transacciones no confirmadas de tiempo crítico. Las transacciones no confirmadas no elegidas 41, 42, 43 se pueden memorizar y mantener disponibles para un segmento de tiempo posterior o se pueden desechar.

La primera sección de tiempo, durante la cual se proporcionan y eligen transacciones no confirmadas 41, 42, 43, finaliza en el instante t1.

En el instante t1 comienza una segunda sección de tiempo del segmento de tiempo. El equipo de nodo 20 permanece inactivo durante la segunda sección de tiempo. Los equipos de nodo 30, 31, 32 forman durante la segunda sección de tiempo cada uno un bloque no confirmado 60, 61 a partir de las transacciones no confirmadas 41, 42, 43 elegidas, tal como se ha descrito antes en base al primer ejemplo de realización. Aunque la formación de un bloque en un base de datos distribuida, que por ejemplo se opera según la tecnología de cadenas de bloques, puede ser un proceso lento, la regla de consenso y los equipos de nodo 20, 30, 31, 32 del base de datos distribuida 100 están configurados tal que se garantiza que la formación de los bloques no confirmados 60, 61 se complete hasta el instante t2, en el que finaliza la segunda sección de tiempo.

En el instante t2 comienza una tercera sección de tiempo del segmento de tiempo. Durante la tercera sección de tiempo, proporcionan los equipos de formación de bloques 3010, 3110, 3210 el bloque no confirmado 61, 62, que cada uno ha formado, en el sistema de base de datos distribuida 100 y los otros equipos de nodo 20, 30, 31, 32 reciben los bloques no confirmados 61, 62 proporcionados. La aportación y recepción de los bloques no confirmados proporcionados finaliza en el instante t3. La tercera sección de tiempo termina en el instante t3.

En el instante t3 comienza una cuarta sección de tiempo del segmento de tiempo. Durante la cuarta sección, los equipos de nodo 20, 30, 31, 32 confirman cada uno exactamente uno de los bloques no confirmados 60, 62 proporcionados en la tercera sección de tiempo, añadiendo los mismos el bloque confirmado 73 a la cadena de bloques confirmados memorizada en la quinta unidad 6 del correspondiente equipo de nodo 20, 30, 31, tal como se ha descrito antes para el segundo ejemplo de realización. La cuarta sección de tiempo termina en el instante T0 + ΔT y por lo tanto también termina el segmento de tiempo.
De esta manera funciona el sistema de base de datos distribuida 100 con impulsos de reloj y de manera sincronizada, con lo que puede garantizarse que dentro de un período de tiempo predeterminado ΔT (longitud de un segmento de tiempo) una transacción no confirmada 41, 42, 43 proporcionada se incluye como transacción confirmada en las representaciones del libro de transacciones del sistema de base de datos distribuida 100 de los respectivos equipos de nodo 20, 30, 31, 32.

La figura 8 muestra esquemáticamente la estructura de un bloque no confirmado 61 según ejemplos de realización. Señalemos que la estructura mostrada de un bloque no confirmado 61 también es válida correspondientemente para un respectivo bloque confirmado 71, 72, 73 (figura 3) y por lo tanto este último no se describe de nuevo. La descripción se realiza en base a la figura 8 y con referencia a las figuras 1, 3 y 6.

El bloque no confirmado 61 es, por ejemplo, un bloque no confirmado 61 que ha sido formado por el equipo de formación de bloques 10 (figura 1) y está constituido como sigue:

El bloque no confirmado 61 incluye un conjunto de transacciones no confirmadas 41, 42, 43, así como un valor hash 611, que por ejemplo es una raíz de Merkle (valor raíz de un árbol de hash criptográfico) y protege las transacciones no confirmadas 41, 42, 43 frente a manipulaciones posteriores.

Además, el bloque no confirmado 61 puede incluir una transacción 40 de coinbase no confirmada, siempre que la regla de consenso del sistema de base de datos distribuida 100 lo prevea. La transacción coinbase 40 es generada por el propio equipo de formación de bloques 10 y puede otorgar al equipo de formación de bloques 10 o bien a un equipo de nodo 30 que lo incluye (figura 5), una remuneración predeterminada por formar el bloque.

El bloque no confirmado 61 incluye opcionalmente además una marca de tiempo 612, que identifica el segmento de tiempo en el que se formó el bloque no confirmado 61.

El bloque 61 no confirmado incluye un valor hash de encadenamiento 613, que puede ser un valor hash criptográfico del último bloque confirmado de una representación del libro de transacciones del sistema de base de datos distribuida 100 conocida por el equipo de formación de bloques 10.

El bloque no confirmado 61 también incluye un valor de comprobación 614, que según un ejemplo es un valor nonce, que representa la llamada Best-Effort-Proof-of-Work (prueba de trabajo de mejor esfuerzo). En particular, el equipo de formación de bloques 10, después de haber formado el bloque no confirmado 61, puede utilizar el tiempo restante hasta el final de la segunda sección de tiempo en el tiempo t2 (figura 7) para determinar el valor nonce probando de tal forma que un valor hash de todo el bloque no confirmado 61 sea lo más extremo posible, por ejemplo lo más pequeño posible.

De esta manera, el equipo de formación de bloques 10 puede documentar de forma trazable su interés legítimo en incluir el bloque en el libro de transacciones del sistema de base de datos distribuida 100. Esta prueba de trabajo, también llamada prueba de trabajo de mejor esfuerzo, se puede proporcionar con seguridad dentro de la segunda sección de tiempo t2.

En base al bloque no confirmado 61 se describirá ahora más en detalle una regla de consenso del sistema de base de datos distribuida 100. Los criterios de la regla de consenso descritos a continuación pueden combinarse de manera adecuada. Los criterios descritos a continuación pueden utilizarse por un equipo de nodo 20, 30, 31, 32 correspondiente del sistema de base de datos distribuida 100 para comprobar durante la cuarta sección de tiempo desde t3 hasta T0 + ΔT (figura 7) del correspondiente segmento de tiempo un bloque respectivo no confirmado 61, 62 y elegir entre todos los bloques no confirmados 61, 62 comprobados con éxito exactamente un bloque a confirmar. La regla de consenso se describe a modo de ejemplo en base al equipo de nodo 20 de la figura 3 y el bloque no confirmado 61 en la figura 8. Se entiende que los otros equipos de nodo 30, 31, 32 funcionan según la misma regla de consenso.

En particular, un criterio de la regla de consenso es que la raíz de Merkle 611 debe corresponder a un valor de raíz de un árbol de Merkle construido a partir de las transacciones no confirmadas 41, 42, 43 del bloque no confirmado. De esta manera se puede asegurar que el bloque no confirmado 61 no se modificó sin autorización al aportarlo.

En particular, un criterio de la regla de consenso es que el valor de hash de encadenamiento 611 debe ser un valor de hash válido del último o de uno precedente de la cadena de bloques confirmados 71, 72, 73 memorizada en la quinta unidad 5 del equipo de nodo 20. De esta manera se puede determinar si y en qué posición se puede agregar el bloque no confirmado 61 a la cadena de bloques confirmados 71, 72, 73 o si se debe descartar.

En particular, un criterio de la regla de consenso es que cada una de las transacciones no confirmadas 41, 42, 43 debe ser una transacción válida. Se puede entender bajo una transacción válida que la transacción en cuestión cambia de un estado actual, mediante la secuencia de transacciones confirmadas de la representación memorizada del libro de transacciones del sistema de base de datos distribuida 100 en la quinta unidad 5, a un nuevo estado válido. Por ejemplo, una de las transacciones no confirmadas 41, 42, 43 puede tratarse como transacción válida 41, 42, 43 cuando un contrato inteligente incluido en la transacción o referenciado por la transacción se ejecuta sin errores.

En particular, un criterio de la regla de consenso puede ser que la marca de tiempo 612 del bloque no confirmado 61 designa un segmento de tiempo que coincide con el segmento de tiempo actual. De esta manera, se puede controlar si el cronometraje del sistema de base de datos distribuida 100 funciona correctamente.

En particular, un criterio de la regla de consenso puede ser que el bloque no confirmado 61 debe incluir todas las transacciones no confirmadas 41, 42, 43 que se proporcionaron durante la primera sección de tiempo entre T0 y t1 (figura 7) y que corresponden a una condición predeterminada. En otras palabras, el equipo de nodo 20 también puede recibir y mantener disponibles las transacciones no confirmadas 41, 42, 43 proporcionadas en la red distribuida 100 durante el segmento de tiempo respectivo, para poder verificar posteriormente durante el mismo segmento de tiempo si todas las transacciones indeterminadas que responden a la condición se han incluido correctamente en el bloque no confirmado 61. La condición predeterminada puede ser por ejemplo que han de incluirse todas las transacciones no confirmadas 40, 41, 42 que están marcadas como de tiempo crítico y/o relacionadas con órdenes de control, valores medidos o valores de control de un sistema de automatización industrial. Así se puede garantizar la capacidad de tiempo real del sistema de base de datos distribuida 100.

Los criterios antes mencionados pueden ser utilizados por el respectivo equipo de nodo 20, 30, 31, 32 para rechazar como no válidos bloques no confirmados 61 que no cumplan al menos uno de los criterios mencionados. Pueden utilizarse otros criterios que se mencionan a continuación para elegir el bloque que se confirmará entre varios bloques no confirmados 61, 62 válidos y verificados.

En particular, un criterio de la regla de consenso puede ser que se elija aquel bloque no confirmado 61, 62 que incluya el mayor número posible de transacciones no confirmadas 41, 42, 43 o transacciones no confirmadas 41, 42, 43 de una clase determinada. De esta manera, se puede lograr un incentivo para mejorar el volumen de transacciones y/o la capacidad de tiempo real del base de datos distribuida 100.

En particular, un criterio de la regla de consenso puede ser que se elija aquel bloque no confirmado 61, 62 con el mejor valor de verificación 614. Así puede por ejemplo elegirse aquel bloque no confirmado 61, 62 cuyo valor hash, en el que también se incorpora el valor de verificación 614, es especialmente extremo, por ejemplo es el más bajo, el más alto o presenta una cantidad lo mayor posible de ceros binarios iniciales o de unos binarios iniciales. De esta manera puede resolverse ventajosamente una situación competitiva entre varios bloques no confirmados 61, 62 y se puede lograr un incentivo para los equipos de formación de bloques 10 de la red distribuida 100 para proporcionar la mejor prueba de trabajo posible (Best-Effort-Proof-of-Work).

El criterio antes descrito puede modificarse en particular tal que, además de la calidad del valor de verificación 614, también se tenga en cuenta una calidad y/o complejidad de cálculo de las transacciones no confirmadas 41, 42, 43 comprendidas en el bloque no confirmado 61, 62. Así puede por ejemplo darse preferencia a un bloque no confirmado 61 frente a otro bloque no confirmado 62 incluso si el bloque no confirmado 61 contiene un valor de verificación 614 de menor calidad que el otro bloque 62 no confirmado (si el valor hash del bloque 61 no confirmado es menos extremo que el valor hash del otro bloque 62 no confirmado) y sin embargo el bloque 61 no confirmado incluye un número correspondientemente mayor de transacciones no confirmadas 41, 42, 43 de cálculo complejo. Bajo una transacción no confirmada 41, 42, 43 de cálculo complejo puede entenderse una transacción cuya comprobación genera en el marco de la formación del bloque no confirmado 61 una alta carga de cálculo en el equipo de formación de bloques 10 en cuestión u ocupa mucho tiempo de cálculo del equipo de formación de bloques 10 en cuestión. De esta manera, puede evitarse ventajosamente que se vea afectado negativamente un equipo de formación de bloques 10 que asume muchas transacciones 41, 42, 43 de cálculo complejo en un bloque no confirmado 61 y que, debido a ello, dentro de la segunda sección de tiempo entre t1 y t2 (figura 7) sólo quede poco tiempo de cálculo para determinar el valor de verificación 614 antes del final de la segunda sección de tiempo.

La figura 9 muestra un libro de transacciones del sistema de base de datos distribuida 100 según una variante preferida del tercer ejemplo de realización.

La figura 9 muestra una cadena de bloques confirmados 71, 72, 73 tal como puede estar memorizada en la quinta unidad (figura 3) de un equipo de nodo 20, 30, 31, 32 correspondiente (figura 6) de la red de base de datos distribuida 100 (figura 6). La cadena de bloques confirmados 71, 72, 73 representa aquí un libro de transacciones de la red de base de datos distribuida 100 (figura 6). A continuación nos referiremos a la figura 9 y a la figura 6.

Cada uno de los bloques confirmados 71, 72, 73 incluye un valor de verificación 714, 724, 734, un valor hash de encadenamiento 713, 723, 733, una marca de tiempo 712, 722, 732, una raíz de Merkle 711, 721, 731 y las correspondientes transacciones no confirmadas 50-53, 54-56, 57-59. Los elementos mencionados corresponden a los elementos correspondientes del bloque no confirmado 61, que se han descrito en base a la figura 8.

Como se muestra en la figura 9, los bloques 71, 72, 73 están encadenados mediante los valores de hash de encadenamiento 713, 723, 733 de tal manera que en cada caso un bloque siguiente 72, 73 tiene un valor de hash de encadenamiento 713, 723, 733 del respectivo bloque precedente 71, 72. Así puede protegerse la cadena de bloques frente a manipulaciones.

La figura 9 muestra además un eje de tiempos que designa los instantes de inicio T0, T0 + ΔT, T0 + 2ΔT de los respectivos segmentos de tiempo. El bloque 71 confirmado se formó y confirmó en el segmento de tiempo asociado al instante T0. El bloque 72 confirmado se formó en el segmento de tiempo desde T0 + ΔT. El bloque 73 confirmado se formó en el segmento de tiempo desde T0 + 2ΔT. En consecuencia, la marca de tiempo 712 del bloque confirmado 71 contiene el valor "T0", la marca de tiempo 722 contiene el valor "T0 + ΔT" y la marca de tiempo 732 contiene el valor "T0 + 2ΔT".

Como se puede ver en la figura 9, en la red de base de datos distribuida 100 se agrega exactamente un bloque confirmado al libro de transacciones a intervalos de tiempo ΔT predeterminados.

La figura 10 muestra un sistema de base de datos distribuida 100 según un cuarto ejemplo de realización. La descripción de la figura 10 se realiza con referencia a las figuras 1, 3 y 6. El sistema de base de datos distribuida 100 correspondiente al cuarto ejemplo de realización mostrado en la figura 10 corresponde al sistema de base de datos distribuida 100 mostrado en la figura 6 correspondiente al tercer ejemplo de realización y los mismos elementos no se describen de nuevo. A continuación y con referencia a la figura 10, figura 6, figura 3 y figura 1 sólo incidiremos en diferencias del cuarto ejemplo de realización.

El sistema de base de datos distribuida 100 según el cuarto ejemplo de realización tiene un reloj central 7 proporcionado en la red 101. La respectiva tercera unidad 203, 303, 313, 323 está configurada para recibir los impulsos de reloj desde el reloj central 7. El reloj 7 puede ser un transmisor de tiempo DCF77, un servidor NTP o PTP o un generador de impulsos de reloj de un sistema de automatización industrial. De esta manera, puede mantenerse sincrónicamente con especial facilidad el correspondiente cronometraje de los equipos de nodo 20, 30, 31, 32.

El sistema de base de datos distribuida 100 correspondiente al cuarto ejemplo de realización también tiene un equipo de planificación del tiempo 8 aportado en la red 101. El equipo de planificación del tiempo 8 recibe los impulsos de tiempo desde el reloj central 7 de la misma manera que las terceras unidades 303, 313, 323 y determina los segmentos de tiempo respectivos de la longitud predeterminada basándose en el cronometraje.

El correspondiente equipo de formación de bloques 3010, 3110, 3210 tiene, además de la respectiva primera unidad 1 y la respectiva segunda unidad 2, también una cuarta unidad 304, 314, 324.

Al comienzo de un segmento de tiempo respectivo, el equipo de planificación del tiempo 8 envía una señal de planificación del tiempo a exactamente una cuarta unidad 304, 314, 324 de exactamente uno de los equipos de formación de bloques 3010, 3110, 3210. El equipo de planificación del tiempo 8 puede elegir exactamente un equipo de formación de bloques 3010, 3110, 3210 por turno, aleatoriamente o según otra planificación.

Los equipos de formación de bloques 3010, 3110, 3210 según el cuarto ejemplo de realización están configurados de tal manera que su correspondiente primera unidad 1 y la segunda unidad 2 en el segmento de tiempo respectivo sólo ejecutan las etapas S10 y S20 (figura 2) descritas en base al primer ejemplo de realización cuando la cuarta unidad 304, 314, 324 del equipo de formación de bloques 3010, 3110, 3210 correspondiente recibe la señal de activación del equipo de planificación del tiempo 8. De lo contrario, la primera 1 y la segunda unidad 2 permanecen inactivas en el segmento de tiempo respectivo en el que no se recibió ninguna señal de activación.

Por consiguiente, sólo se forma ventajosamente exactamente un bloque no confirmado 61 por cada segmento de tiempo y al confirmar los bloques no confirmados 61, 62 mediante los respectivos equipos de nodo 20, 30, 31, 32, se puede evitar una situación competitiva entre varios bloques no confirmados 61, 62 y puede renunciarse a una Best-Effort-Proof-of-Work. En lugar de ello, puede utilizarse una Proof-of-Stake como valor de verificación o utilizarse un Permissioned Ledger.

En este caso, para aumentar la seguridad, el equipo de nodo respectivo 20, 30, 31, 32 puede aplicar el criterio adicional de la regla de consenso de que un bloque 61 no confirmado solo puede verificarse con éxito y confirmarse si el bloque 61 no confirmado ha sido proporcionado por el equipo de formación de bloques 3010, 3110, 3210 activado en el correspondiente segmento de tiempo.

Aunque la presente invención se ha descrito en base a ejemplos de realizaciones, puede modificarse de muchas maneras.

En aras de la simplicidad, sólo se ha descrito el principio básico de un sistema de base de datos distribuida basado en cadenas de bloques con un libro de transacciones y bloques encadenados, cada uno de los cuales incluye varias transacciones. Sin embargo, la enseñanza divulgada ahora sobre la

formación cronometrada y la confirmación de bloques también es aplicable a otros sistemas de bases de datos distribuidas y perfeccionamientos de sistemas de bases de datos basados en cadenas de bloques, como por ejemplo en sistemas de bases de datos distribuidas con varios libros de transacciones, como un libro mayor y un libro de páginas, en otras clases de encadenamiento, como por ejemplo gráficos dirigidos o cadenas de transacciones sin bloques y similares.

En la red de base de datos distribuida 100 del tercer ejemplo de realización puede estar previsto un reloj central 7. En la red de base de datos distribuida 100 de la cuarta forma de realización, también puede no estar previsto ningún reloj central 7.

Las técnicas para encontrar consenso, tales como Best-Effort-Proof-of-Work, Proof-of-Stake, Permissioned Ledger y similares, se pueden combinar a voluntad siempre que el equipo de formación de bloques 10 pueda generar con garantía el valor de verificación 614 dentro de la sección de tiempo prevista para ello en el segmento de tiempo respectivo.

En base a la figura 6 se describió una raíz de Merkle, pero puede pensarse también en una raíz de Patricia y otras clases de valores hash, árboles hash y otras clases de aseguramiento criptográfico de un bloque y/o transacciones individuales frente a manipulaciones.

En base a la figura 7 se describió una subdivisión concebible de un segmento de tiempo y se describió que todos los equipos de nodo 20, 30, 31, 32 están sincronizados con impulsos de cronometraje de tal manera que comience un segmento de tiempo correspondiente en todos los equipos de nodo 20, 30, 31, 32 al mismo tiempo. Sin embargo, también son concebibles formas de realización en las que el ritmo de tiempos respectivo de los equipos de nodo 20, 30, 31, 32 está sincronizado en el tiempo de otra manera y/o el segmento de tiempo respectivo está dividido de manera diferente. Por ejemplo, los ritmos de tiempo de distintos equipos de nodo podrían estar decalados entre sí en una fracción de la longitud predeterminada $\Delta T$; de esta manera se podría lograr por ejemplo un mayor grado de paralelización sin la fase de inactividad de equipos de nodo individuales 20.

La solución propuesta puede entenderse como un equipo de formación de bloques y un equipo de nodo para un sistema de base de datos distribuida, cada uno con una unidad para recibir un cronometraje desde un reloj y determinar segmentos de tiempo de longitud predeterminada en base al cronometraje, eligiendo el equipo de formación de bloques dentro de un segmento de tiempo respectivo exactamente una vez transacciones a confirmar a partir de transacciones no confirmadas proporcionadas en el sistema de base de datos, formando un bloque no confirmado a partir de las transacciones no confirmadas elegidas y proporcionando el bloque no confirmado en el sistema de bases de datos y memorizando el equipo de nodo una cadena de bloques confirmados que representan un libro de transacciones del sistema de base de datos y confirmando dentro de un segmento de tiempo correspondiente exactamente una vez exactamente uno de los bloques no confirmados proporcionados en el sistema de base de datos en el segmento de tiempo y anexándolo a la cadena de bloques confirmados.

La solución propuesta se puede aplicar de manera particularmente ventajosa a un sistema de automatización industrial que incluye un conjunto de componentes de automatización que pueden funcionar cronometrados. Un sistema de base de datos distribuida propuesto, como por ejemplo el sistema de base de datos distribuida 100 según uno de los ejemplos de realización, puede estar diseñado mediante contratos inteligentes que implementan la lógica de control y equipos de interfaz que forman una interfaz entre los equipos de nodo del sistema de base de datos distribuido y los componentes de automatización del sistema de automatización y similares, para controlar y/o regular el conjunto de componentes de automatización. Un equipo de interfaz correspondiente puede estar configurado para hacer que un valor de medición de un componente de automatización respectivo se proporcione al sistema de base de datos 100 como transacción no confirmada, o para hacer que se proporcione un valor de control de una transacción del componente de automatización respectivo confirmada en el sistema de base de datos 100.En este caso se puede utilizar un generador de impulsos de reloj del sistema de automatización como reloj central (7 en la figura 10) del sistema de base de datos distribuida. Así se puede realizar un cronometraje del sistema de base de datos distribuida que es sincrónico con el cronometraje del conjunto de componentes de automatización o un múltiplo entero del mismo. Así pueden confirmarse ventajosamente valores de medida y/o valores de control en sincronismo en el sistema de base de datos distribuida en forma de registros de datos de transacciones, al ser suministrados los mismos por los componentes de automatización o deben enviarse a ellos. Así puede realizarse un control en tiempo real del sistema de automatización industrial con ayuda de un base de datos distribuida basada en tecnología de cadenas de bloques.

**Referencias**

[1] Andreas M. Antonopoulos "Mastering Bitcoin: Unlocking Digital Cryptocurrencies", O'Reilly Media, Diciembre 2014

[2] Roger M. Needham, Michael D. Schroeder "Using encryption for authentication in large networks of computers" ACM: Communications of the ACM. volumen 21, núm.12 diciembre 1978,

[3] Ross Anderson "Security Engineering. A Guide to Building Dependable Distributed Systems" Wiley, 2001

[4] Henning Diedrich "Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations", CreateSpace Independent Publishing Platform, 2016

[5] "The Ethereum Book Project/Mastering Ethereum" https://github.com/ethereumbook/ethereumbook, a fecha 5.10.2017

[6] Leemon Baird"The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance",Swirlds Tech Report SWIRLDS-TR-2016-01, 31.5.2016

[7] Leemon Baird"Overview of Swirlds Hashgraph", 31.5.2016

[8] Blockchain Oracles https://blockchainhub.net/blockchain-oracles/

**REIVINDICACIONES**

1. Equipo de formación de bloques (10) para un sistema de base de datos distribuida (100) que incluye un conjunto de equipos de nodo (20, 30 - 32) con:
una primera unidad (1) para elegir un conjunto de transacciones a confirmar a partir de un conjunto de transacciones no confirmadas (41 - 43) proporcionadas en el sistema de base de datos distribuida;
una segunda unidad (2) para formar un bloque no confirmado (61, 62) a partir del conjunto elegido de transacciones no confirmadas (41 - 43), comprobándose la validez de una respectiva transacción no confirmada (41 - 43) elegida y rechazándose si no supera la prueba, incluyéndose de lo contrario en el bloque no confirmado (61, 62) y para proporcionar el bloque no confirmado (61, 62) en el sistema de base de datos distribuida (100); y
una tercera unidad (3) para recibir un cronometraje de un reloj (7) y para determinar segmentos de tiempo de longitud predeterminada (ΔT) en base al cronometraje;
estando preparadas la primera unidad (1) y la segunda unidad (2) para realizar exactamente una vez la elección, la formación y la aportación dentro de un segmento de tiempo correspondiente.

2. Equipo de formación de bloques según la reivindicación 1,
**caracterizado porque** la primera unidad (1) está configurada para elegir, durante el segmento de tiempo correspondiente, todas las transacciones no confirmadas (41 - 43) proporcionadas en el sistema de base de datos distribuida (100) que corresponden a una condición predefinida como transacciones a confirmar.

3. Equipo de formación de bloques según la reivindicación 1 ó 2,
**caracterizado por** una cuarta unidad (304, 314, 324) para recibir una señal de activación,
estando configuradas la primera unidad (1) y la segunda unidad (2) para llevar a cabo la elección, la formación y la aportación dentro del segmento de tiempo respectivo sólo exactamente una vez cuando la cuarta unidad (304, 314, 324) recibe la señal de activación en el segmento de tiempo correspondiente.

4. Equipo de formación de bloques según una de las reivindicaciones 1 a 3,
**caracterizado porque** la segunda unidad (2) está configurada para incluir en el bloque (61) formado una mejor prueba criptográfica de trabajo (614) que pueda determinar la misma dentro del segmento de tiempo respectivo.

5. Equipo de formación de bloques según una de las reivindicaciones 1 a 4,
**caracterizado porque** la segunda unidad (2) está configurada para incluir en el bloque (61) formado una marca de tiempo (612) que identifica el correspondiente segmento de tiempo.

6. Equipo de nodo (20, 30 - 32) para un sistema de base de datos distribuida (100) que incluye un conjunto de equipos de nodo (20, 30 - 32) con:
una quinta unidad (5) para memorizar una cadena de bloques confirmados (71 - 72), que representan al menos una sección de un libro de transacciones del sistema de base de datos distribuida (100);
una sexta unidad (6) para confirmar exactamente uno de un conjunto de bloques no confirmados (61, 62) proporcionados en el sistema de base de datos distribuida (100) en un segmento de tiempo correspondiente, de modo que el bloque confirmado (73) esté unido a la cadena de bloques confirmados (71 - 73), incluyendo la confirmación de exactamente uno del conjunto de bloques no confirmados una comprobación de uno, varios o todos los bloques no confirmados (61, 62), una elección de uno de los bloques no confirmados (61, 62) comprobados con éxito y una agregación del bloque elegido como el bloque confirmado (73) a la cadena de bloques confirmados (71 - 73); y una tercera unidad (3) para recibir un cronometraje de un reloj (7) y determinar segmentos de tiempo de longitud predeterminada en base al cronometraje;
estando configurada la sexta unidad (6) para llevar a cabo la confirmación y la agregación exactamente una vez dentro de un segmento de tiempo correspondiente.

7. Equipo de nodo según la reivindicación 6,
**caracterizado porque** la sexta unidad (6) está configurada para elegir exactamente un bloque para confirmarlo (61, 62) en base a al menos uno de los siguientes criterios:
   - número y clase de transacciones (41, 42, 43) incluidas en el bloque (61, 62);
   - calidad de una prueba de trabajo criptográfica (614) incluida en el bloque;
   - calidad y/o complejidad de cálculo de una transacción (41, 42. 43) respectiva incluida en el bloque (61, 62);
   - coincidencia de una marca de tiempo incluida en el bloque (61, 62) con el segmento de tiempo respectivo; y/o
   - si un equipo de formación de bloques (10) que ha proporcionado el bloque es un equipo de formación de bloques (10) para el cual está destinada una señal de activación transmitida durante el segmento de tiempo correspondiente en el sistema de base de datos distribuida (100).

8. Equipo de nodo según la reivindicación 6 ó 7,

**caracterizado porque** la sexta unidad está configurada para elegir exactamente un bloque (61, 62) para confirmarlo en base a un criterio de si el bloque (61, 62) incluye todas las transacciones no confirmadas (41, 42, 43) proporcionadas en el sistema de base de datos distribuida (100) durante el segmento de tiempo respectivo que corresponden a una condición predefinida.

9. Equipo de nodo según una de las reivindicaciones 6 a 8,
**caracterizado porque** el equipo de nodo (30, 31, 32) tiene un equipo de formación de bloques (10) según una de las reivindicaciones 1 a 5.

10. Sistema de base de datos distribuida (100) que incluye un conjunto de equipos de nodo (20, 30 - 32) según una de las reivindicaciones 6 a 9, que están configurados para gestionar conjuntamente el libro de transacciones del sistema de base de datos distribuida (100), en el que al menos uno de los equipos de nodo (30 - 32) incluye un equipo de formación de bloques (10) según una de las reivindicaciones 1 a 5 y el conjunto de equipos de nodo (20, 30 - 32) puede funcionar sincronizado en el tiempo según un cronometraje del sistema de base de datos distribuida.

11. Sistema de base de datos distribuida según la reivindicación 10,
**caracterizado porque** el sistema de base de datos distribuida (100) incluye además un reloj central (7), siendo el reloj (7) desde el cual recibe el cronometraje la tercera unidad (3, 203, 303, 313, 323) del equipo de nodo (20, 30 - 32) respectivo, el reloj central (7).

12. Sistema de automatización industrial, que incluye un sistema de base de datos distribuida (100) según la reivindicación 10 u 11 y un conjunto de componentes de automatización que pueden funcionar según un cronometraje,
pudiendo operar el sistema de base de datos distribuida (100) para regular y/o controlar el conjunto de componentes de automatización,
siendo el cronometraje del sistema de base de datos distribuida (100) sincrónico con el cronometraje del conjunto de componentes de automatización o un múltiplo entero del ritmo de cronometraje del conjunto de componentes de automatización.

13. Procedimiento de formación de bloques para un sistema de base de datos distribuida (100) que incluye un conjunto de equipos de nodo (20, 30 - 32) con:
elección (S10) de un conjunto de transacciones a confirmar a partir de un conjunto de transacciones no confirmadas (41 - 43) proporcionadas en el sistema de base de datos distribuida (100);
formación (S21) de un bloque no confirmado (61) a partir del conjunto elegido de transacciones no confirmadas (41, 42, 43), comprobándose la validez de una respectiva transacción no confirmada (41-43) elegida y rechazándose si no supera la prueba, incluyéndose de lo contrario en el bloque no confirmado (61) y aportación (S22) del bloque no confirmado (61) en el sistema de base de datos distribuida (100) y recepción (S30) de un cronometraje de un reloj (7) y determinación de segmentos de tiempo de longitud predeterminada (ΔT) en base al cronometraje;
realizándose la elección (S10), la formación (S21) y la aportación (S22) exactamente una vez dentro de un segmento de tiempo correspondiente.

14. Procedimiento de confirmación de bloques para un sistema de base de datos distribuida (100) que incluye un conjunto de equipos de nodo (20, 30 - 32) con:

memorización (S50) de una cadena de bloques confirmados (71 - 72) que representan un libro mayor de una base de datos distribuida (100);
confirmación (S60) de exactamente uno de un conjunto de bloques no confirmados (61, 62) proporcionados en el sistema de base de datos distribuida (100) en el segmento de tiempo respectivo, agregando el bloque confirmado (73) a la cadena de bloques confirmados (71 - 73), incluyendo la confirmación de exactamente uno del conjunto de bloques no confirmados una comprobación de uno, varios o todos los bloques no confirmados (61, 62), una elección de uno de los bloques no confirmados (61, 62) verificados con éxito y una agregación del bloque elegido como el bloque confirmado (73) a la cadena de bloques confirmados (71 - 73); y
recepción (330) de un cronometraje desde un reloj (7) y determinación de segmentos de tiempo de una longitud predeterminada en base al cronometraje,
realizándose la confirmación y la aportación (S60) exactamente una vez dentro de un segmento de tiempo correspondiente.

15. Producto de programa de computadora que provoca la realización de un procedimiento según la reivindicación 13 ó 14 sobre un equipo controlado por programa.

FIG 1

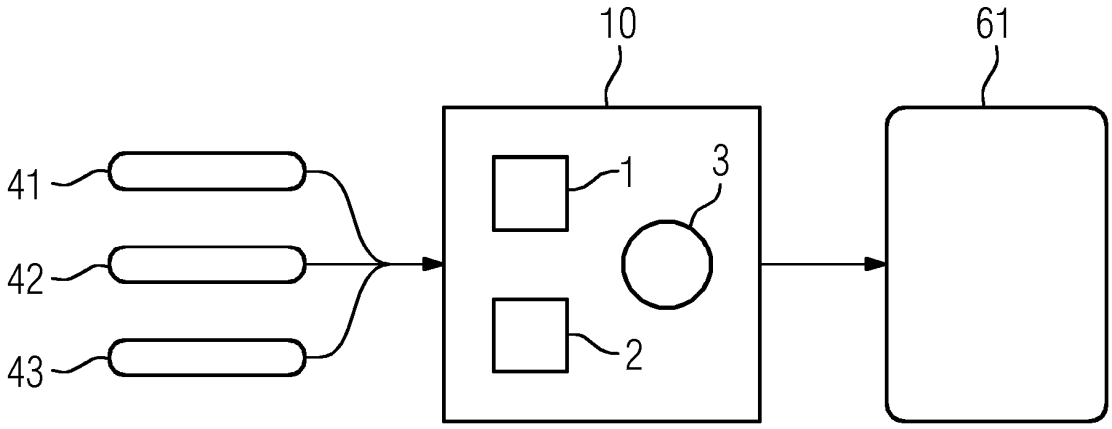


FIG 2

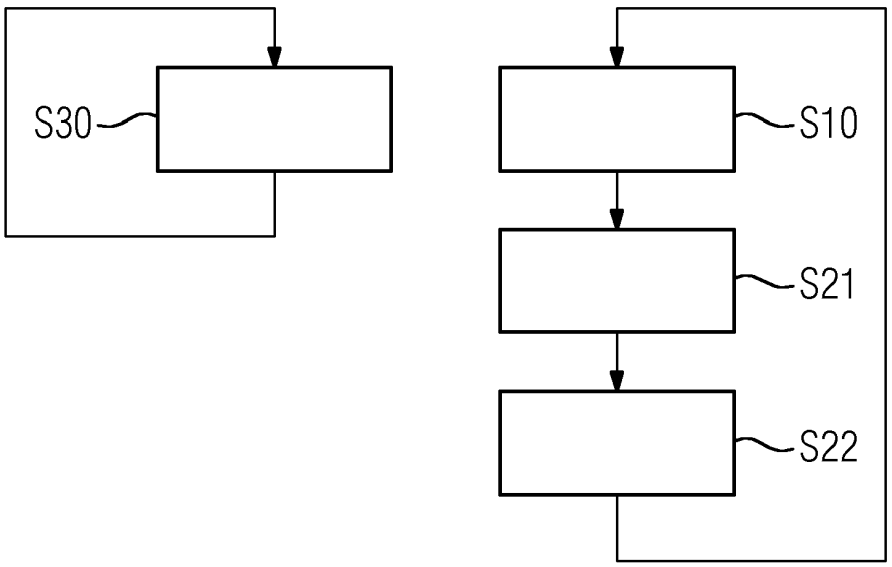

FIG 3

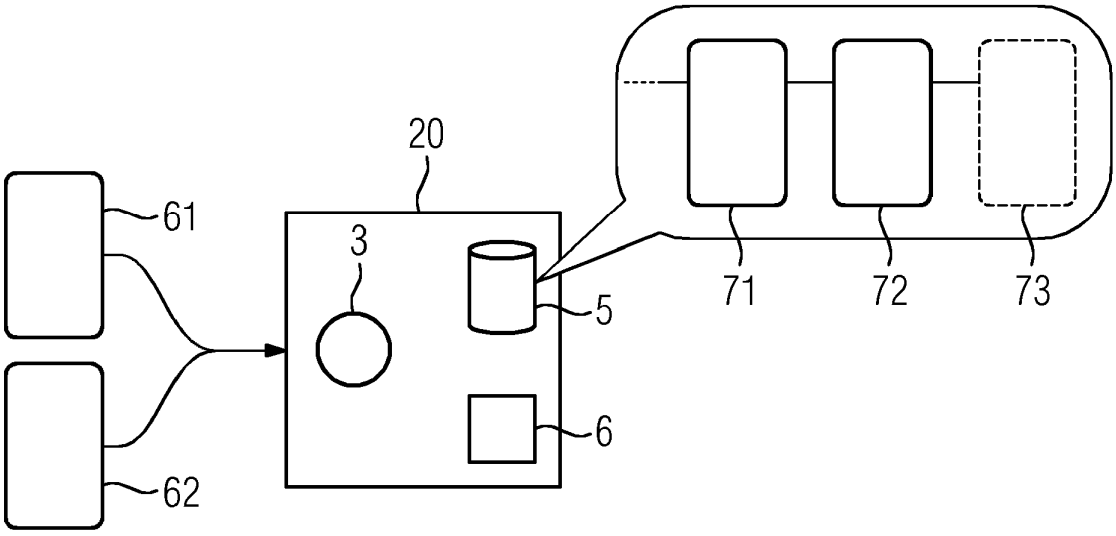


FIG 4

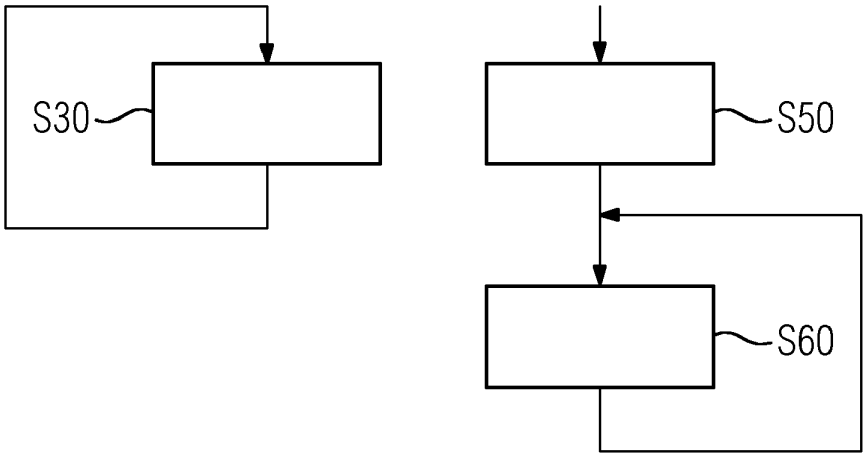

FIG 5

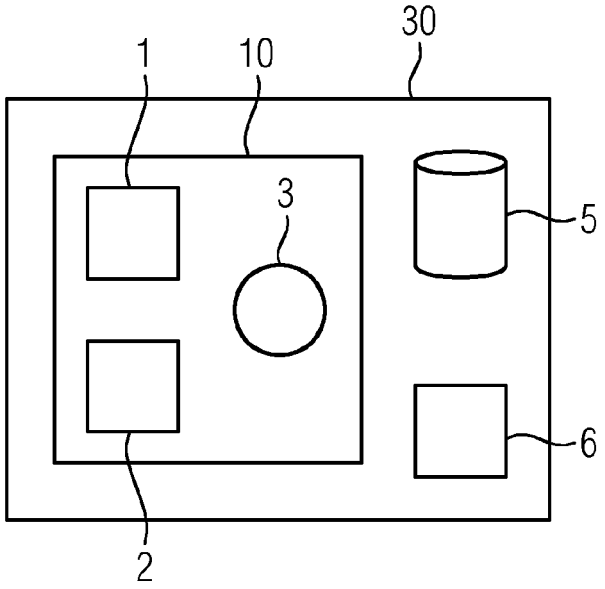


FIG 6

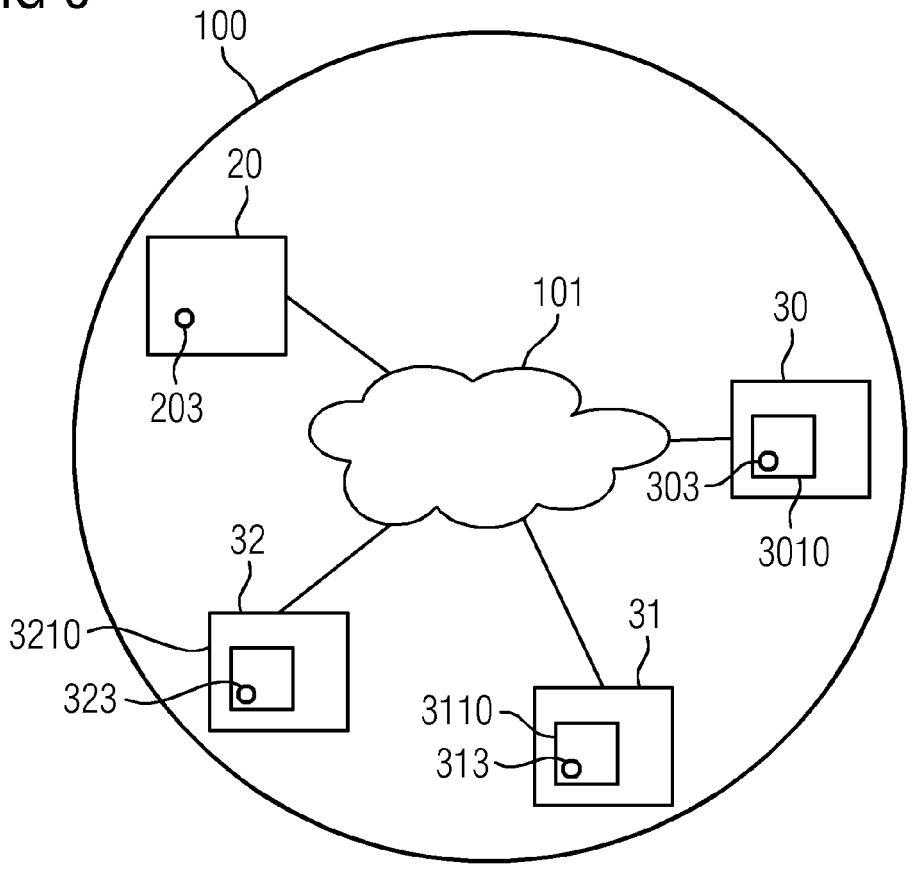

FIG 7

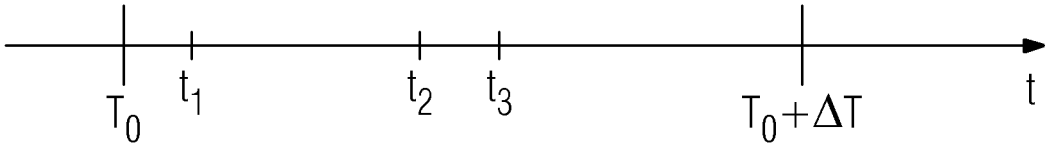


FIG 8

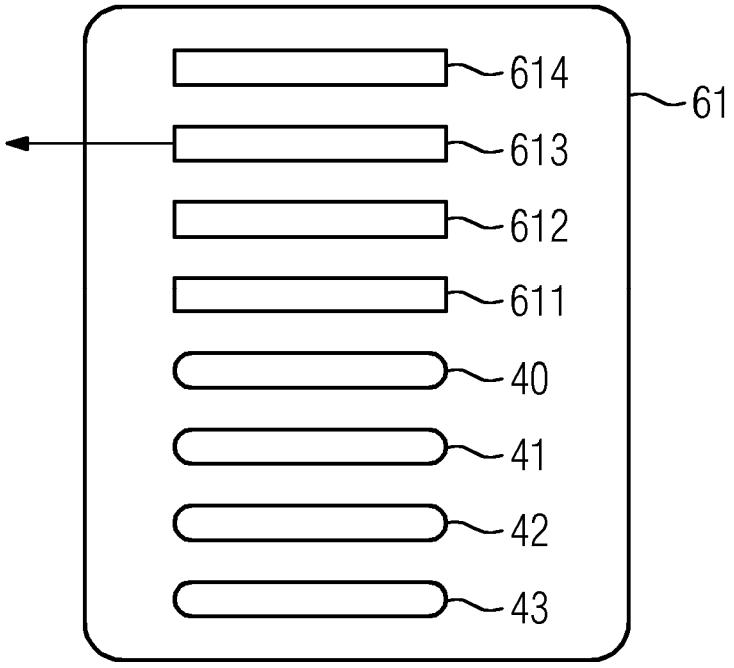

FIG 9

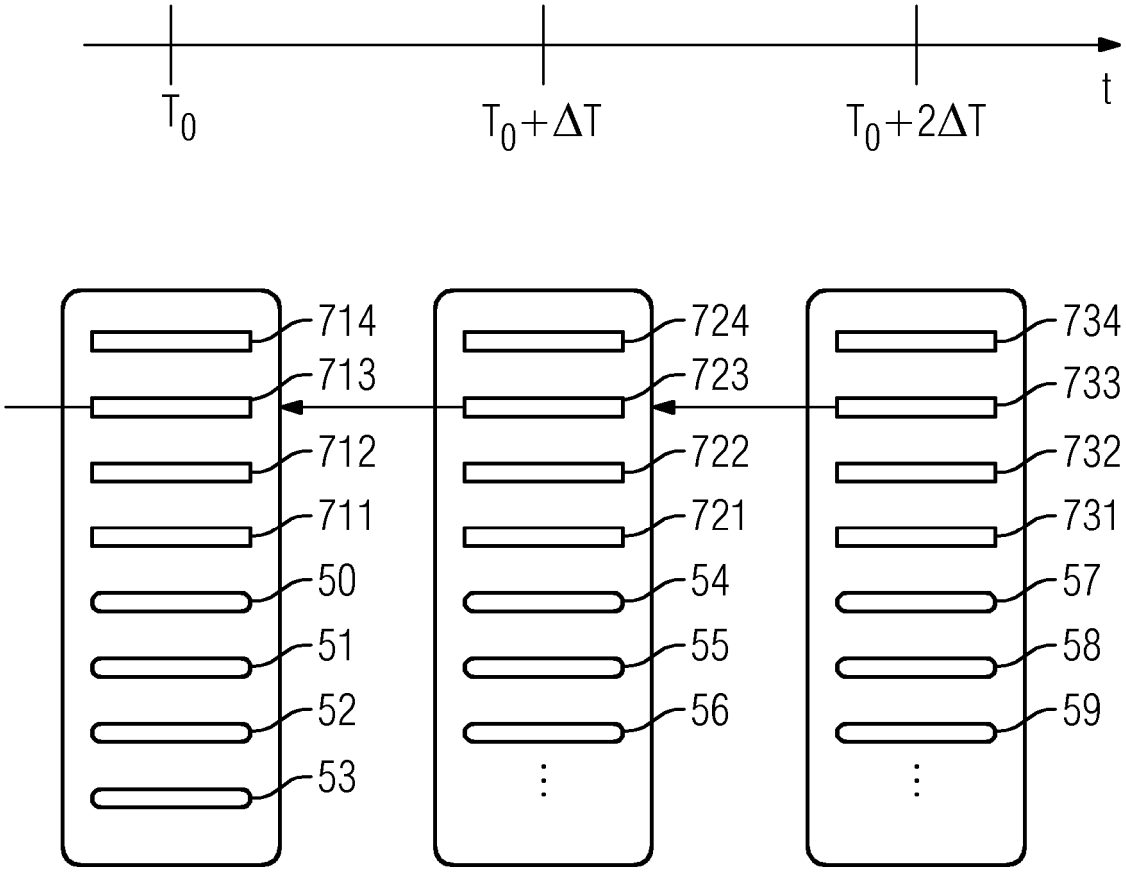
T0
T0+ΔT
T0+2ΔT
t
714
713
712
711
50
51
52
53
724
723
722
721
54
55
56
734
733
732
731
57
58
59

FIG 10