

NUEVAS REIVINDICACIONES

1. Un método implementado por computador en una red informática, comprendiendo el método implementado por computador:

configurar un libro mayor electrónico distribuido en la memoria electrónica de una o más computadores en un sistema de cadenas de bloques, el libro mayor electrónico distribuido tiene una pluralidad de bloques interconectados retroconectados, dispuestos como una o más instancias de estructuras de datos de cadena de bloques lineales, arreglos de bloques no lineales, mallas n-dimensionales o estructuras de datos reticulares, o gráficos acíclicos dirigidos;

configurar cada uno de los bloques interconectados para incluir un conjunto ordenado de registros de datos individuales, de modo que al menos uno de los registros refleje una transformación de al menos una parte del estado global del libro mayor electrónico distribuido;

configurar el sistema de cadenas de bloques para que comprenda una red de nodos de computador entre homólogos, con una o más computadores configuradas como nodos de billetera, y con una o más computadores configuradas como nodos de construcción de bloques;

configurar uno o más nodos de billetera para transmitir uno o más de los registros de datos a uno o más nodos de construcción de bloques en la red entre homólogos; y

configurar el uno o más nodos de construcción de bloques para construir uno o más bloques interconectados en el libro mayor electrónico distribuido seleccionando y ordenando uno o más de los registros de datos para incluirlos en dicho uno o más nuevos bloques interconectados.

2. El método implementado por computador de la reivindicación 1, que incluye además la implementación en el sistema de cadenas de bloques, un proceso de propagación de datos de confiar, pero verificar, en el que al menos un nodo de construcción de bloques está configurado para crear al menos un nuevo bloque interconectado en el sistema de cadenas de bloques antes de verificar la corrección de uno o más bloques precedentes a los que se vincula dicho al menos un nuevo bloque interconectado.

3. El método implementado por computador de la reivindicación 2, en el que el proceso de propagación de datos de confiar, pero verificar incluye además propagar dicho al menos un nuevo bloque interconectado en el sistema de cadenas de bloques a través de un protocolo de chismes.

4. El método implementado por computador de la reivindicación 3, en el que el protocolo de chismes permite que dicho al menos un nuevo bloque interconectado se propague a través del sistema de cadenas de bloques, que incluye, además:

transmitir dicho al menos un bloque interconectado a través del protocolo de chismes como un encabezado de bloque, al mismo tiempo excluye la mayor parte de los datos pertenecientes a dicho al menos un bloque interconectado.

5. El método implementado por ordenador de la reivindicación 3, en el que el protocolo de chismes permite transmitir dicho al menos un nuevo bloque interconectado sin que uno o más registros de datos pertenezcan a dicho al menos un nuevo bloque interconectado, de tal manera que dichos uno o más registros de datos se transmiten separadamente de dicho al menos un nuevo bloque interconectado.

6. El método implementado por computador de la reivindicación 2, que además incluye:

al menos otro nodo de construcción de bloques crea al menos un siguiente bloque interconectado encima de dicho al menos un nuevo bloque interconectado después de que dicho al menos un nuevo bloque interconectado se distribuye al sistema de cadenas de bloques; y

el al menos otro nodo de construcción de bloques crea simultáneamente el al menos un siguiente bloque interconectado mientras que uno o más registros de datos pertenecientes a dicho al menos un nuevo bloque interconectado son descargados por el al menos otro nodo de construcción de bloques, o mientras dicho al menos se valida al menos un nuevo bloque interconectado.

7. El método implementado por computador de la reivindicación 2, en el que el proceso de propagación de datos de confiar, pero verificar incluye además hacer que al menos un nodo de construcción de bloques incluya un filtro Bloom en un encabezado de bloque de dicho al menos un nuevo bloque interconectado en el sistema de cadenas de bloques, de modo que el proceso de propagación de datos de confiar, pero verificar hace que al menos un nodo de construcción de bloques distribuya el filtro Bloom con al menos un nuevo bloque interconectado en el sistema de cadenas de bloques.

8. El método implementado por computador de la reivindicación 7, en el que el filtro Bloom está configurado para representar un conjunto de cuentas contables electrónicas distribuidas u otros datos afectados u operados durante uno de (i) la creación, (ii) la validación, o (iii) la ejecución de dicho al menos un nuevo bloque interconectado en el sistema de cadenas de bloques.

9. El método implementado por computador de la reivindicación 7, en el que el filtro Bloom de un bloque es una estructura de datos configurada al menos

con la propiedad de que cualquier cuenta u otros datos encontrados en el filtro Bloom es posible o probable que su estado sea modificado por la validación y ejecución del bloque, o que haya sido operado o afectado de otra manera por el bloque o por los registros de datos pertenecientes a el bloque, y

con la propiedad de que cualquier cuenta que no se encuentre en el filtro Bloom seguramente no cambiará en cuanto a su estado o no se verá afectada por el bloque o por los registros de datos que pertenecen al bloque.

10. El método implementado por computador de la reivindicación 9, en el que la creación de dicho al menos un nuevo bloque interconectado incluye, además:

identificar cuentas afectadas u operadas cuando se ejecutan uno o más contratos inteligentes, o cuando se agregan uno o más registros de datos a dicho al menos un nuevo bloque interconectado;

verificar que cada cuenta identificada no esté contenida dentro de un filtro Bloom de al menos un bloque interconectado anterior que precede a dicho al menos un bloque interconectado nuevo; y

si una cuenta identificada está contenida dentro de un filtro Bloom del al menos un bloque interconectado anterior, detener la ejecución de dicho uno o más contratos inteligentes o detener la inclusión de dicho uno o más registros de datos, y descartar dicho uno o más contratos inteligentes o uno o más registros de datos de dicho al menos un nuevo bloque interconectado.

11. El método implementado por ordenador de la reivindicación 2, en el que el proceso de propagación de datos de confiar, pero verificar utiliza la estructura de datos de gráficos acíclicos dirigidos (DAG) para disponer dicho al menos un nuevo bloque interconectado.

12. El método implementado por computador de la reivindicación 11, en el que el proceso de propagación de datos de confiar, pero verificar permite que dicho al menos un nuevo bloque interconectado tenga referencias posteriores a uno o más bloques interconectados o subcadenas en el sistema de cadenas de bloques, provocando que al menos una parte del libro mayor electrónico distribuido constituya un gráfico acíclico dirigido (DAG).

13. El método implementado por computador de la reivindicación 12, en el que el proceso de propagación de datos de confiar, pero verificar asegura que los múltiples bloques o subcadenas interconectados que se construyen simultáneamente por dicho nuevo bloque interconectado incluyen registros asociados con conjuntos de cuentas u otros datos distintos y mutuamente excluyentes, de modo que los múltiples bloques interconectados o subcadenas que se construyen afectan conjuntos de cuentas u otros datos mutuamente excluyentes.

14. El método implementado por computador de la reivindicación 13, en el que el proceso de propagación de datos de confiar, pero verificar permite que los múltiples bloques o subcadenas interconectados se comparen rápidamente para determinar si alguno de los múltiples bloques o subcadenas interconectados opera con cuentas comunes u otros datos.

15. El método implementado por computador de la reivindicación 13, que además incluye la comparación de los filtros Bloom respectivos de los múltiples bloques o subcadenas interconectados para determinar con certeza que los bloques o subcadenas interconectados en el sistema de cadenas de bloques afectan u operan en conjuntos de cuentas u otros datos.

16. El método implementado por computador de la reivindicación 2, en el que el proceso de propagación de datos de confiar, pero verificar permite la creación simultánea de una pluralidad de nuevos bloques interconectados en el libro mayor electrónico distribuido, de modo que múltiples nodos en el sistema de cadenas de bloques están creando uno o más de la pluralidad de nuevos bloques interconectados en paralelo; y

en el que el proceso de propagación de datos de confiar, pero verificar garantiza que los registros de datos no se propaguen ampliamente a través del sistema de cadenas de bloques antes de la construcción de bloques interconectados, de modo que los registros de datos producidos por un nodo determinado solo se comparten con otros nodos determinados dentro del sistema de cadenas de bloques; y

en el que el proceso de propagación de datos de confiar, pero verificar garantiza que un nodo de construcción de bloques respectivo solo cree dicho al menos un nuevo bloque interconectado utilizando registros de datos propagados por ciertos nodos dentro del sistema de cadenas de bloques.

17. El método implementado por computador de la reivindicación 2, en el que, si un nodo de construcción de bloques descubre que dicho al menos un nuevo bloque interconectado no se puede validar, dicho al menos un nuevo bloque interconectado se descarta junto con cualquier bloque nuevo o subsiguiente que se construya sobre dicho al menos un nuevo bloque interconectado; y

en el que un bloque no se puede validar si ocurre uno de los siguientes: (i) una raíz de árbol de Merkle no se puede reproducir utilizando un conjunto de registros de datos que pertenecen a dicho bloque en el sistema de cadenas de bloques, (ii) un hash de bloque en dicho bloque se especifica incorrectamente, o (iii) un registro de datos perteneciente a dicho bloque no es válido o viola una regla en el sistema de cadenas de bloques.

18. El método implementado por computador de la reivindicación 2, en el que el proceso de propagación de datos de confiar, pero verificar aumenta el rendimiento de transacciones del sistema de cadenas de bloques en relación con el rendimiento de transacciones de un sistema de cadenas de bloques de prueba de trabajo de consenso de Nakamoto.

19. El método implementado por computador de la reivindicación 3, en el que el al menos un nodo de construcción de bloques es un nodo de construcción de bloques identificable configurado con una dirección de recompensa que se incluye con al menos un bloque interconectado sujeto que está siendo construido por dicho al menos un nodo de construcción de bloques identificable; y

en el que dicho al menos un bloque interconectado en cuestión es un bloque firmado criptográficamente por dicho al menos un nodo de construcción de bloques identificable que utiliza al menos una clave criptográfica asociada con dicha dirección de recompensa,

en el que el al menos un bloque firmado se propaga en la red de cadena de bloques a través del protocolo de chismes.

20. El método implementado por ordenador de la reivindicación 20, en el que al menos otro nodo de construcción de bloques implementa un proceso de evaluación de confianza, mediante el cual, dicho al menos otro nodo de construcción de bloques, al recibir dicho bloque firmado, determina si generar un nuevo subsiguiente bloque que se basa en dicho bloque firmado o encabezado de bloque antes de que dicho bloque firmado o encabezado de bloque sea validado;

en el que el proceso de evaluación de confianza incluye además evaluar si dicha dirección de recompensa ha firmado algún bloque anterior previamente propagado en la red de cadena de bloques, y en el que dichos bloques anteriores firmados por dicha dirección de recompensa son válidos o no válidos.

21. El método implementado por computador de la reivindicación 20, en el que configurar el proceso de propagación de datos de confiar, pero verificar incluye además al menos uno de:

(a) configurar el bloque firmado para especificar una tarifa de construcción como una cantidad de credenciales de libro mayor electrónico distribuidos, cuyo bloque firmado está configurado como un bloque incentivado, y al menos otro nodo de construcción de bloques genera un nuevo bloque posterior configurado con una referencia a dicho bloque incentivado;

en el que la tarifa de construcción de bloques incentivada se transfiere desde la dirección de recompensa a una dirección de libro mayor distribuida especificada por al menos otro nodo de construcción de bloques; o

(b) configurar el bloque firmado para especificar credenciales en riesgo como una cantidad de credenciales de libro mayor electrónico distribuidos, cuyo bloque firmado funciona como un bloque garantizado, y configurar al menos otro nodo en la red de cadena de bloques construye un registro de penalización que contiene o hace referencia al bloque garantizado,

cuyo registro de penalización, cuando se incorpora a un nuevo bloque posterior, hace que las credenciales en riesgo especificados se transfieran desde la dirección de recompensa a una dirección de libro mayor distribuida especificada por al menos otro nodo en la red de cadena de bloques, si el bloque garantizado es inválido.

22. El método implementado por computador de la reivindicación 1, en el que configurar el sistema de cadenas de bloques incluye además configurar al menos uno de los registros de datos como un registro de transacción dispuesto como una colección ordenada de registros constituyentes, con cada uno de los registros constituyentes configurados como un contrato inteligente o como un registro que no es un contrato inteligente; y

en el que al menos uno de los registros constituyentes representa una transformación de estado de al menos una parte del estado global del libro mayor electrónico distribuido.

23. El método implementado por computador de la reivindicación 22, en el que configurar el sistema de cadenas de bloques incluye además el registro de transacción que incorpora un registro de encabezado de transacción, una o más instancias adicionales de registros constituyentes respectivos y una o más firmas criptográficas.

24. El método implementado por ordenador de la reivindicación 23, en el que al menos una de una o más firmas criptográficas es una firma de primera parte, en el que la firma de primera parte incluye además al menos uno de:

firmar digitalmente una representación estandarizada de un registro de pie de página de transacción agregado a las instancias de los respectivos registros constituyentes, o

firmar digitalmente una representación estandarizada del registro de la transacción que encapsula los registros constituyentes.

25. El método implementado por ordenador de la reivindicación 24, en el que el registro del encabezado de la transacción está configurado para permitir la verificación del registro de la transacción; y

en el que la verificación del registro de transacciones incluye determinar que el registro de transacciones no es válido a menos que la firma de la primera parte se firme utilizando al menos una de las claves criptográficas de una o más direcciones de libros electrónicos distribuidos especificadas por el registro de encabezado de transacciones.

26. El método implementado por computador de la reivindicación 25, que además incluye:

configurar al menos un registro constitutivo del al menos un registro de transacciones para que esté asociado con al menos una referencia a uno o más registros precedentes que preceden a al menos un registro constitutivo en la colección ordenada de registros constitutivos;

en el que la al menos una referencia a uno o más registros anteriores se implementa como un hash de registro anterior generado de manera determinista de una representación estandarizada de los datos de uno o más registros anteriores; y

en el que la representación estandarizada de los datos de uno o más registros anteriores incluye al menos una referencia hecha a su vez a los registros constituyentes que aún preceden a esos registros anteriores, en forma de otro hash de registro anterior.

27. El método implementado por computador de la reivindicación 26, que además incluye hacer coincidir al menos un registro constituyente con al menos una firma criptográfica, que comprende:

generar al menos una firma criptográfica firmando una representación estandarizada de los datos de al menos un registro constituyente, usando claves criptográficas de al menos una dirección de libro mayor electrónico distribuido que origina ese registro constituyente;

en el que la representación estandarizada incluye el hash del registro anterior correspondiente a dicho registro constituyente.

28. El método implementado por computador de la reivindicación 27, en el que configurar el sistema de cadenas de bloques incluye además un protocolo de transacción atómica de múltiples firmas que incluye:

generar, por al menos un nodo del sistema de cadenas de bloques, la colección ordenada de registros constituyentes, en cada caso incluyendo primero un registro de encabezado de transacción, seguido de una o más instancias de registros constituyentes, y bien transmitiendo dicha colección ordenada de registros constituyentes a al menos otro nodo del sistema de cadenas de bloques, o generar una instancia de registro de transacciones;

recibir, por al menos un nodo del sistema de cadenas de bloques, la colección ordenada de registros constituyentes de al menos otro nodo del sistema de cadenas de bloques, y en cada caso:

generar una instancia de registro de transacciones; o

actualizar primero dicha colección ordenada de registros constituyentes para incluir uno o más registros constituyentes adicionales y luego transmitir dicha colección ordenada de registros constituyentes a al menos otro nodo del sistema de cadenas de bloques, o generar una instancia de registro de transacciones;

la generación de una instancia de registro de transacción comprende encapsular la colección ordenada de registros constituyentes en un registro de transacción, combinado con una o más firmas criptográficas; y

al menos un nodo del sistema de cadenas de bloques que transmita uno o más registros de transacciones a la red de cadena de bloques, y al menos un nodo de construcción de bloques dentro de la red de cadena de bloques que verifique la validez de uno o más registros de transacciones y los registros constituyentes y firmas criptográficas del uno o más registros de transacciones.

29. El método implementado por computador de la reivindicación 28, en el que cada uno o más registros constituyentes agregados o incluidos en la colección ordenada de registros constituyentes después del registro de encabezado de transacción, incluye al menos una referencia a al menos un registro anterior que precede a ese registro constituyente en al menos un registro de transacción;

en el que al menos una referencia a al menos un registro anterior en la colección ordenada de registros constituyentes se implementa como un hash de registro anterior generado de forma determinista de una representación estandarizada de los datos del al menos un registro anterior; y

en el que la representación estandarizada de los datos del al menos un registro anterior en la colección ordenada de registros constituyentes incluye al menos una referencia hecha a su vez a al menos un registro perteneciente al registro de transacción que precede a al menos un registro anterior, a menos que el al menos un registro anterior es un registro de encabezado de transacción; y

en el que al menos una de las una o más firmas criptográficas se firma usando claves criptográficas de al menos una dirección de libro mayor electrónico distribuida que origina al menos uno de los uno o más registros constituyentes.

30. El método implementado por computador de la reivindicación 22, que incluye además la configuración del al menos un nodo de construcción de bloques para procesar en secuencia cada registro constituyente y contrato inteligente dentro de un registro de transacción, de modo que no se procese ningún otro registro intermedio o contrato inteligente hasta que cada constituyente registro y contrato inteligente dentro de la colección ordenada de registros constituyentes se evalúa en el orden especificado, a menos que el procesamiento de un registro intermedio o contrato inteligente sea obligatorio para ejecutar al menos uno de los registros constituyentes o contratos inteligentes de la colección ordenada de registros constituyentes.

31. El método implementado por computador de la reivindicación 23, que incluye además la configuración de al menos un nodo de construcción de bloques para procesar la colección ordenada de registros constituyentes y contratos inteligentes en al menos un registro de transacción en una base de todo o nada, de modo que ninguna transformación a cualquier parte del estado global del libro mayor electrónico distribuido codificado por cualquier registro constituyente o contrato inteligente que pertenezca a la colección ordenada de registros constituyentes procede si cualquier registro constituyente individual o contrato inteligente dentro de la colección no es válido o no logra efectuar al menos una transformación del registro de transacciones con éxito.

32. El método implementado por computador de la reivindicación 1, en el que el sistema de cadena de bloques impone un retraso de tiempo entre el al menos un nuevo bloque interconectado y al menos un bloque interconectado posterior al requerir un espacio de tiempo mínimo entre bloques.

33. El método implementado por computador de la reivindicación 22, en el que el espacio mínimo de tiempo entre bloques es un segmento de tiempo cuantificado por un número mínimo de unidades computacionales a ejecutar en secuencia.