(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 009 744**

(51) Int. Cl.:

H04W 4/30 (2008.01)
H04L 9/40 (2012.01)
H04L 9/32 (2006.01)
H04L 67/104 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.12.2018 PCT/CN2018/121527**

(87) Fecha y número de publicación internacional: **25.06.2020 WO20124317**

(96) Fecha de presentación y número de la solicitud europea: **17.12.2018 E 18943668 (6)**

(97) Fecha y número de publicación de la concesión europea: **22.01.2025 EP 3900301**

(54) Título: **Nodo de computación de borde de acceso múltiple con libro mayor distribuido**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.03.2025

(73) Titular/es:

XENIRO (100.00%)
RM 1601, 238 Jiang Chang Third Road, Jingan District
Shanghai, CN

(72) Inventor/es:

HUANG, ENSHEN

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Nodo de computación de borde de acceso múltiple con libro mayor distribuido

Campo

La presente invención se relaciona con un nodo de computación de borde de acceso múltiple con un libro mayor distribuido.

Antecedentes

La tecnología de libro mayor descentralizado ha atraído mucho interés en los últimos años debido a su flexibilidad de aplicaciones: desde proporcionar una arquitectura para contraseñas de utilidad que se pueden usar para implementar contratos inteligentes integrados.

Sin embargo, las transacciones respaldadas por cadenas de bloques sufren varias limitaciones. Debido a la naturaleza en la cual se validan las transacciones, que requiere el consenso de múltiples máquinas, esto lleva a latencia cuando se procesan numerosas transacciones simultáneamente. La latencia causa dificultades al escalar la tecnología de cadena de bloques para soportar aplicaciones de internet de las cosas (IoT), por lo que se espera que el mercado de IoT crezca exponencialmente desde $157 mil millones a $457 mil millones de 2016 a 2020, de acuerdo con un artículo del 10 de diciembre de 2017 publicado por Forbes[1]. La naturaleza misma de la tecnología de cadena de bloques, que es un libro mayor descentralizado, tiene una falla de seguridad conocida como "ataque de 51%", por el cual si más de la mitad de las máquinas validan un libro mayor que contiene registros erróneos, es posible que las transacciones deshonestas se procesen erróneamente como transacciones válidas. La privacidad también es una preocupación, dado que se pueden obtener transacciones pasadas de las cuales se pueden obtener identidades.

Aunque hay enfoques existentes que intentan mejorar la latencia y mejorar la seguridad de la tecnología de cadena de bloques, muchos de estos enfoques abordan estos inconvenientes de manera unilateral, sin aprovechar plenamente la capacidad de la tecnología de cadena de bloques.

La presente invención busca abordar las deficiencias anteriores y suministrar un sistema que aprovecha la tecnología de cadena de bloques de manera más efectiva.

El documento US 2018/308134 A1 describe que un primer sistema de dispositivo de memoria accesible por procesador y un segundo sistema de dispositivo de memoria accesible por procesador de un sistema de transacciones autorregulado pueden almacenar cada uno una copia local respectiva de uno o más libros mayores de transacciones que registran transacciones. Un primer sistema de dispositivo de procesamiento de datos puede estar configurado para generar un bloque de información de transacciones asociado con un canal de mercado particular, almacenarlo en la copia local de un libro mayor de transacciones asociado con el canal de mercado particular almacenado en el primer sistema de dispositivo de memoria accesible por procesador y transmitirlo a un segundo sistema de dispositivo de procesamiento de datos a través de una red de comunicaciones para almacenamiento en la copia local del libro mayor de transacciones asociado con el canal de mercado particular almacenado en el segundo sistema de dispositivo de memoria accesible por procesador.

El documento US 2018/091524 A1 describe un libro mayor digital construido sobre una cadena de bloques con la capacidad de compartir de manera segura, precisa y verificable información de estado entre partes desconfiadas. El Libro Mayor Subcontratado Verificable está alojado en un entorno en red, accesible mediante múltiples partes, y mantiene una vista inmutable de las transacciones enviadas por las partes autorizadas y una vista continua de los estados compartidos entre las partes que las partes pueden replicar de manera independiente localmente para verificar la integridad del libro mayor.

El documento WO 2018/025028 A1 describe un sistema de protección de datos y se divulga un método. El sistema de protección de datos incluye un repositorio de datos, una interfaz de acceso a datos y un sistema de autentificación. El repositorio de datos almacena datos de usuario para un usuario. Los datos de usuario comprenden una pluralidad de componentes encriptados individualmente. La interfaz de acceso a datos está dispuesta para proporcionar acceso remoto a cada uno de los componentes encriptados individualmente en forma encriptada. El sistema de protección de datos está dispuesto para proporcionar acceso selectivo a cada componente individual en forma no encriptada cuando el sistema de autentificación autentifica al usuario para el componente respectivo.

El documento US 2018/117446 A1 describe un dispositivo de Internet de las Cosas (IoT) que incluye una cámara acoplada a un procesador; y un transceptor inalámbrico acoplado al procesador. Se pueden usar contratos inteligentes de cadena de bloques con el dispositivo para facilitar la operación segura.

Resumen de la invención

De acuerdo con un aspecto de la invención, se proporciona un nodo de computación de borde de acceso múltiple ubicado para utilizar la infraestructura de red de acceso por radio de una estación base de un operador de red móvil para comunicación celular que comprende bandas de frecuencia de 4G y 5G, comprendiendo el nodo de computación de borde de acceso múltiple al menos una memoria para almacenar un bloque de datos encadenado, donde cada bloque de datos está codificado con datos de una transacción pasada con respecto a un bien o servicio; y al menos un procesador configurado con funciones que: incluyen un nuevo bloque de datos, para registrar una transacción actual con respecto a un bien o servicio, en el bloque de datos encadenado en respuesta a una firma, generada a partir de procesar los datos de la transacción actual con los datos codificados de las transacciones pasadas almacenadas en el bloque de datos encadenado, que es validada por otros nodos de computación de borde de acceso múltiple, en donde el nodo de computación de borde de acceso múltiple y los otros nodos de computación de borde de acceso múltiple son de confianza, y se comunican a través de un canal común, en donde los datos con respecto a las transacciones se reciben a través de una conexión celular proporcionada por la estación base.

Las características opcionales se especifican en las reivindicaciones dependientes.

Breve descripción de los dibujos

Se describen en este documento realizaciones representativas de la presente invención, solo a modo de ejemplo, con referencia a los dibujos acompañantes, en donde:

La Figura 1 es un esquema de una porción de un sistema que comprende puntos de acceso, soportando cada uno un nodo de computación de borde de acceso múltiple respectivo.

La Figura 2 muestra un esquema de un protocolo usado para construir un bloque de datos encadenado en un libro mayor compartido por cada uno de los nodos de computación de borde de acceso múltiple de la Figura 1.

La Figura 3 muestra un caso de uso de contratos inteligentes que se relacionan con la gestión de cadena de suministro.

La Figura 4 muestra un caso de uso de un contrato inteligente que se relaciona con generar en flujo medios desde una fuente a un dispositivo receptor.

La Figura 5 muestra un esquema de nodos de computación de borde de acceso múltiple que se distribuyen a través del sistema para explicar cómo llegan a un consenso.

La Figura 6 proporciona un esquema de un protocolo híbrido que se usa por el libro mayor distribuido del sistema que se muestra en la Figura 1.

La Figura 7 proporciona un esquema de la interacción de protocolos usados en el libro mayor distribuido del sistema que se muestra en la Figura 1.

La Figura 8 proporciona un esquema de un grupo de nodos de computación de borde de acceso múltiple configurado para soportar la implementación de bloques de datos para permitir una carga de trabajo, orquestación y gobernanza diversas.

La Figura 9 proporciona un esquema de grupos de nodos de computación de borde de acceso múltiple, residiendo cada uno en diferentes regiones a través de la orquestación de contenedores federados.

La Figura 10 es un esquema de funciones que se ejecuta por un procesador estándar de cada uno de los nodos de computación de borde de acceso múltiple de la Figura 1 y un esquema de un procesador dedicado diseñado para compartir la carga computacional del procesador estándar de los nodos de computación de borde de acceso múltiple para ejecutar estas funciones.

La Figura 11 muestra una arquitectura del procesador dedicado de la Figura 10.

La Figura 12 proporciona un flujo que demuestra cómo un motor de políticas inteligentes 1210 que opera en un procesador estándar de un nodo de computación de borde de acceso múltiple funciona con el procesador dedicado de la Figura 11.

La Figura 13 es un esquema de un sistema que comprende un libro mayor distribuido que se implementa mediante un procesador de los nodos de computación de borde de acceso múltiple de la Figura 1 que comparte la carga computacional con el procesador dedicado de la Figura 11.

La Figura 14 es un esquema para explicar cómo se realiza la elección de nodos de computación de borde de acceso múltiple testigos.

Descripción detallada

En la siguiente descripción, se describen diversas realizaciones con referencia a los dibujos, donde caracteres de referencia similares generalmente se refieren a las mismas partes a lo largo de las diferentes vistas.

La presente solicitud, en una visión general amplia, se relaciona con un libro mayor que se distribuye a través de un sistema de nodos de computación de borde de acceso múltiple. El libro mayor es una base de datos que almacena registros de entradas de transacciones monitorizadas, distribuidas por cada uno de los nodos de computación de borde de acceso múltiple que alojan una réplica. En el contexto de las aplicaciones de IoT, una transacción puede ser iniciada automáticamente por los propios dispositivos de IoT (es decir de máquina a máquina o M2M), siempre que se cumplan ciertas condiciones; o puede requerir intervención humana, tal como un operador que trabaje con un dispositivo de IoT en un extremo (máquina a humano o M2H) o un operador que trabaje con un dispositivo de IoT en cada extremo (humano a humano. H2H).

El libro mayor distribuido también está sincronizado ya que cuando uno de los libros mayores alojados se actualiza para registrar datos de una nueva transacción en los datos de transacciones pasadas, su nodo de computación de borde de acceso múltiple de alojamiento verifica si el libro mayor actualizado está en consenso con los libros mayores alojados en otros nodos de computación de borde de acceso múltiple, actualizados con datos de la misma nueva transacción. La validación de máquina a máquina se logra cuando al menos una mayoría de los otros nodos de computación de borde de acceso múltiple están de acuerdo con el libro mayor actualizado. En una implementación, se usa el consenso de prueba de participación delegada (DPoS), donde se busca el acuerdo de un porcentaje (por ejemplo 66%) de un grupo seleccionado de nodos de computación de borde de acceso múltiple (llamados "testigos"). El grupo seleccionado de nodos de computación de borde de acceso múltiple son aquellos que producen resultados de confianza, es decir nodos de computación de borde de acceso múltiple que producen libros mayores actualizados que están en conformidad cuando cada uno de ellos registra un nuevo bloque de datos que contiene datos de la nueva transacción. El grupo de nodos de computación de borde de acceso múltiple del cual se busca el acuerdo es votado por los nodos de computación de borde de acceso múltiple de partes interesadas. Estas partes interesadas son nodos de computación de borde de acceso múltiple que poseen contraseñas de utilidad que proporcionan un porcentaje de propiedad de la plataforma creada por el sistema de nodos de computación de borde de acceso múltiple para alojar el libro mayor distribuido. Dado que solo los nodos de computación de borde de acceso múltiple de confianza validan un libro mayor actualizado, esto reduce la probabilidad de un "ataque de 51%" al hacer que los nodos de computación de borde de acceso múltiple adopten técnicas conocidas de "prueba de trabajo". Tener solo un número seleccionado de nodos de computación de borde de acceso múltiple valida el libro mayor actualizado también reduce la latencia, en comparación con el enfoque de "prueba de trabajo". En una implementación, solo el 66% de un grupo elegido de nodos de computación de borde de acceso múltiple realiza la actualización de libro mayor.

Cada nodo de computación de borde de acceso múltiple se ubica dentro de un área de cobertura celular soportada por una estación base de un operador de red móvil, tal como adyacente a la estación base. El nodo de computación de borde de acceso múltiple opera en bandas de frecuencia de 4G y 5G, de acuerdo con los estándares técnicos como se definen por el Instituto Europeo de Estándares de Telecomunicaciones (ETSI) y 3GPP (Proyecto de Asociación de 3ra Generación) con respecto a la computación de borde de acceso múltiple. Por consiguiente, el nodo de computación de borde de acceso múltiple se ubica en proximidad a la estación base para utilizar la infraestructura de red de acceso por radio de la estación base que proporciona comunicación celular en estas bandas de frecuencia de 4G y 5G, de tal manera que el nodo de computación de borde de acceso múltiple opere en condiciones de red de radiodifusión, en lugar de condiciones de red privada. Un espectro operativo de ejemplo yace entre 24 GHz y 86 GHz, para aprovechar una latencia más baja y un mayor rendimiento en comparación con operar en este espectro.

En conjunto, los nodos de computación de borde de acceso múltiple proporcionan computación de borde de acceso múltiple, una arquitectura de red que soporta una mayor capacidad de computación y almacenamiento en un borde de red en comparación con las disponibles para los sistemas de ordenador interconectados dentro de la red, tal como un centro de datos central o una ubicación en la nube. Los libros mayores distribuidos tradicionales alojados en tales recursos de red experimentan latencia antes de que las transacciones puedan llegar a estos libros mayores distribuidos para ser procesadas y por lo tanto los procesos que buscan depender de plataformas que ejecutan tales libros mayores distribuidos no se pueden escalar de manera efectiva. Por el contrario, tener un libro mayor distribuido alojado en el borde de red aprovecha la latencia más baja y las mejores capacidades de rendimiento que se ofrecen por la computación de borde de acceso múltiple para permitir el procesamiento de tareas más cerca de los dispositivos de usuario final. Como tal, los nodos de borde de acceso múltiple y su libro mayor distribuido alojado, implementados de acuerdo con la presente invención, proporcionan una plataforma que facilita que las transacciones se realicen en dispositivos de Internet de las cosas (IoT), es decir cualquier dispositivo que esté integrado con componentes electrónicos que permitan que el dispositivo recolecte e intercambie datos que son con respecto a la transacción, siempre que el dispositivo pueda comunicarse con cualquiera de los nodos de computación de borde de acceso múltiple, por ejemplo a través de la conexión celular proporcionada por la estación base que soporta el nodo de computación de borde de acceso múltiple.

El operador de red móvil se refiere a cualquier compañía de telecomunicaciones que posee los derechos de radiodifusión dentro de un espectro de frecuencia asignado, proporcionando la estación base la infraestructura para crear una celda en una red celular. Por consiguiente, la estación base permite al operador de red móvil tener comunicación inalámbrica de datos a través del espectro de frecuencia asignado y también una puerta de acceso a la red central atendida por la estación base, siendo la red central parte de sistemas de ordenador interconectados, tal como el Internet,

Además de operar un protocolo que estipula cómo se logra el consenso en su libro mayor distribuido, cada uno de los nodos de computación de borde de acceso múltiple también opera un protocolo que hace que cada uno de los nodos de computación de borde de acceso múltiple se comunique a través de un canal común, como una trayectoria de comunicación que se usa para que una estación base se comunique con otra estación base. Esto restringe la comunicación a través de trayectorias de comunicación directas que se usan entre estaciones base y reduce la latencia, a diferencia de enrutar la comunicación a través de la red central. Esto está en contraste con los libros mayores distribuidos que se ejecutan en redes de acceso por radio.

La siguiente divulgación proporciona detalles de implementación del nodo de computación de borde de acceso múltiple que facilita la capacidad de libro mayor distribuido alojado por el nodo de computación de borde de acceso múltiple. En términos generales, el nodo de computación de borde de acceso múltiple tiene un procesador estándar (que es un procesador de servidor estándar), junto con un procesador dedicado (que es un procesador diseñado específicamente separado del procesador estándar), responsable de actualizar el libro mayor distribuido cuando se debe incluir un nuevo bloque de datos. Un motor de políticas es responsable de decidir un algoritmo para usar para validar transacciones registradas en el libro mayor distribuido y procesar la salida de protocolos de conocimiento cero que se usan cuando se deben registrar transacciones que contienen datos protegidos en el libro mayor distribuido. Este motor de políticas también puede configurarse además para determinar si las computaciones que se realizan para validar una actualización del libro mayor distribuido se realizan por el procesador estándar o el procesador dedicado.

La Figura 1 es un esquema de una porción de un sistema 100 que comprende las estaciones base 102, 104 y 106, soportando cada una un respectivo nodo de computación de borde de acceso múltiple 102M, 104M y 106M, de tal manera que cada uno de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M puede aprovechar la capacidad de transmisión y recepción de datos de la cobertura celular que proporcionan sus respectivas estaciones base 102, 104 y 106. En una implementación, esto se logra ubicando cada uno del nodo de computación de borde de acceso múltiple 102M, 104M y 106M dentro del área de cobertura celular de su respectiva estación base 102, 104 y 106. En otra implementación, esto se logra ubicando el nodo de computación de borde de acceso múltiple 102M, 104M y 106M en o al lado de su respectiva estación base 102, 104 y 106. En aras de la simplicidad, todos los otros nodos de computación de borde de acceso múltiple y su respectiva estación base asociada no se muestran en el esquema para el sistema 100.

En una implementación, cada una de las estaciones base 102, 104 y 106 pertenece al mismo operador de red móvil. La comunicación entre cada uno de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M para procesar una transacción es iniciada por los suscriptores de este operador de red móvil. En otra implementación, cada una de las estaciones base 102, 104 y 106 pertenece a un operador de red móvil diferente. La comunicación entre cada uno de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M para procesar una transacción es de acuerdo con las condiciones de una asociación de itinerancia de operador entre los diferentes operadores de red móvil, donde la transacción es iniciada por los suscriptores de cada uno de los respectivos operadores de red móvil.

En aún otra implementación las estaciones base 102, 104 y 106 pertenecen a un tercero, por lo que cada una de ellas es usada por diferentes operadores de redes móviles para facilitar la comunicación entre cada uno de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M para procesar una transacción iniciada por partes que se suscriben a diferentes operadores de redes móviles. Por ejemplo, la estación base 102 puede ser usada por los operadores de redes móviles A, B y C, de tal manera que el nodo de computación de borde de acceso múltiple 102M recibirá primero una notificación si una transacción se inicia por un suscriptor de cualquiera de los operadores de redes móviles A, B y C mientras está en el área de cobertura celular de la estación base 102.

La comunicación entre el nodo de computación de borde de acceso múltiple 102M con los otros nodos de computación de borde de acceso múltiple 104M y 106M para validar una transacción (por ejemplo que se produce en una estación de carga de vehículo eléctrico (EV) 114, donde las dos partes de transacción son un operador de estación de carga y un operador de EV) se producirá a través de la trayectoria de comunicación 108, 110 que las estaciones base 102, 104 y 106 usan para comunicar datos entre sí, en lugar de que se enruten a través de una red central de operador de red móvil 112. El establecimiento de un canal común a lo largo de la trayectoria de comunicación 108, 110 para aislar la comunicación entre los nodos de computación de borde de acceso múltiple 102M, 104M y 106M sirve para reducir el tiempo de latencia para el procesamiento de la transacción (por ejemplo entre el operador de estación de carga y el operador de EV). Incluso en los casos donde la validación, por ejemplo de una transacción transfronteriza, requiere comunicación con la red central de operador de red móvil 112 para extraer recursos (tal como para adquirir una tasa de intercambio de

moneda para la transacción transfronteriza, es decir cuando las contraseñas de utilidad propiedad de una parte de transacción en un extremo está en una jurisdicción diferente de una jurisdicción en la cual se ubica una parte de transacción del otro extremo), el canal común a lo largo de la trayectoria de comunicación 108, 110 aún es utilizado por los nodos de computación de borde de acceso múltiple 104M y 106M para validar la transacción transfronteriza. La trayectoria de comunicación 108. 110 puede realizarse usando medios cableados o inalámbricos.

Cada uno de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M tiene al menos una memoria para almacenar un bloque de datos encadenado. Un bloque de datos encadenado es esencialmente un registro de una transferencia de propiedad durante las transacciones desde la primera hasta la más reciente, de tal manera que el bloque de datos encadenado proporciona una función de libro mayor que es compartida por los nodos de computación de borde de acceso múltiple 102M, 104M y 106M. Su estructura de datos es un puntero de direccionamiento a bloques de transacciones vinculados hacia atrás. Cada bloque es identificable por un direccionamiento, generado por ejemplo usando el algoritmo de direccionamiento criptográfico SHA256, en el encabezado del bloque. El encabezado de cada bloque hace referencia a un bloque previo. Cada bloque contiene el direccionamiento de su progenitor dentro de su propio encabezado. Allí yace una cadena que va todo el camino de vuelta hasta el primer bloque creado, también conocido como el bloque génesis, vinculados juntos por una secuencia de direccionamientos.

Dado que el sistema 100 no tiene un organismo centralizado para autentificar ninguna de sus transacciones soportables, sino que usa validación de máquina a máquina, cada uno de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M se basa en la función de libro mayor del bloque de datos encadenado para determinar si hay suficientes activos para ejecutar una nueva transacción; los activos se refieren, por ejemplo, a si hay existencias para el bien o fondos en una billetera digital para pagar el bien.

La Figura 2 muestra un esquema de un protocolo 200 usado para construir un bloque de datos encadenado en cada uno de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M, estando la construcción basada en un principio de prueba de participación delegada como se explica con mayor detalle a continuación. Para simplificar la explicación de la construcción del bloque de datos encadenado, la Figura 2 supone que cada uno de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M es de confianza, es decir están entre los testigos de todos los nodos de computación de borde de acceso múltiple (es decir incluyendo aquellos que no se muestran en la Figura 1) a través de un voto mayoritario. Estos nodos de computación de borde de acceso múltiple testigos son responsables de garantizar la integridad del libro mayor compartido, es decir validan una transacción para registrarla en el libro mayor compartido. No se requiere el acuerdo de todos los nodos de computación de borde de acceso múltiple testigos, sino solo de una mayoría de ellos (por ejemplo 66%, aunque se puede establecer cualquier otro porcentaje predefinido) para validar la transacción. En una implementación, el número de contraseñas de utilidad que son nodos distribuidos es finita y es propiedad de las partes interesadas, donde las partes interesadas monitorizarán continuamente los nodos de computación de borde de acceso múltiple con mejor rendimiento y votarán para que sean de confianza como los nodos de computación de borde de acceso múltiple testigos. En una implementación, hay 101 nodos de computación de borde de acceso múltiple que actúan como testigos, con los cuales el consenso tiene que ser alcanzado por el 66 o 67 de ellos. Sin embargo, en otra implementación, un número diferente de nodos de computación de borde de acceso múltiple (es decir no necesariamente 101) actúan como testigos, mientras que se requiere otro porcentaje (es decir no necesariamente 66%) de los nodos de computación de borde de acceso múltiple testigos para llegar a un consenso. El número de nodos de computación de borde de acceso múltiple testigos 104M y 106M y su porcentaje para llegar al consenso es de acuerdo con las configuraciones de red, que pueden ser determinadas por partes llamadas "delegados", lo cual se describe más adelante con más detalle en la Figura 14. Asegurar que exista un consenso de libro mayor dentro de un porcentaje predeterminado de todos los nodos de computación de borde de acceso múltiple reduce el tiempo de procesamiento necesario para llegar a tal consenso.

Durante la inicialización, el libro mayor compartido no tiene contenido, de tal manera que la información de una primera transacción, "block0data", se convierte en contenido de un primer bloque de datos 202 (el bloque génesis) para inclusión en el libro mayor compartido de cualquiera del nodo de computación de borde de acceso múltiple 102M, 104M y 106M. La información proporcionada por "block0data" depende de la naturaleza de la transacción que está siendo registrada. Por ejemplo si la transacción se relaciona con la compra de un bien o servicio, la información puede incluir uno o más de punteros que pueden dar detalles sobre: el tipo de bien o servicio, su coste: detalles de una billetera digital usada para financiarlo y el saldo de la billetera digital a partir de entonces: un inventario del cual va a ser extraído el bien: y una identidad de las partes de la transacción (tal como vendedor y comprador, y el transportista del vendedor al comprador). Si la transacción se relaciona con la gestión de cadena de suministro, la información puede incluir uno o más de punteros que pueden dar detalle sobre: el tipo de bien o servicio que está siendo monitorizado, su respectivo precio de coste y precio de venta; un inventario de un almacén desde el cual se almacena un bien: un inventario de una ubicación a la cual se suministra el bien; una identidad del almacén donde se almacena el bien; una identidad de la ubicación a la cual se suministra el bien; una identidad de la parte que suministra el bien; y una identidad del proveedor del bien o servicio. Tal información existe como datos (es decir una cadena de bits de ordenador). Una combinación de "block0data", un valor de direccionamiento de un bloque de datos previo y un *nonce* aleatorio se convierte

en la entrada de una función de direccionamiento. Dado que no hay bloques de datos previos, el valor de direccionamiento previo es "0", de tal manera que el valor de direccionamiento del primer bloque de datos 202 es el valor de direccionamiento de "block0data". La función de direccionamiento es de tal manera que para cualquier entrada, su salida es una cadena de letras y números aleatorios, donde la misma entrada siempre daría la misma cadena de salida, pero cualquier cambio en la entrada haría que la salida cambiara aleatoriamente. La aplicación aquí es resolver un problema matemático donde la salida está en un formato de datos específico (tal como comenzar con una combinación predefinida de caracteres, por ejemplo siete ceros o una mezcla de letras y números), de tal manera que el *nonce* aleatorio se cambia repetidamente para producir tal salida. En el caso de la Figura 2, el valor de direccionamiento del primer bloque de datos 202 es "0xea34ad...55", que se convierte en la firma del primer bloque de datos 202, siendo "$#1" el *nonce* aleatorio encontrado para producir este valor de direccionamiento. Suponiendo, en aras de simplicidad, que la transacción de "block0data" es la primera de su tipo, el valor de direccionamiento "0xea34ad...55" está marcado en tiempo, fechado, serializado con un valor de índice "0" para crear con éxito el primer bloque de datos 202, para hacer referencia de vuelta a partir de bloques de datos encadenados posteriores. La creación exitosa del primer bloque de datos 202 se radiodifunde sobre la trayectoria de comunicación 108, 110 que las estaciones base 102, 104 y 106 usan para comunicarse datos entre sí, para que cada uno de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M conserve una copia del primer bloque de datos 202.

La información de una segunda transacción, "block1data" para inclusión como un segundo bloque de datos 204 en el libro mayor compartido es de la siguiente manera.

El contenido de "block1data" varía dependiendo de la naturaleza de la segunda transacción, de tal manera que los comentarios anteriores sobre "block0data" se aplican igualmente. Una combinación de "block1data", el valor de direccionamiento del primer bloque de datos 202 (es decir "0xea34ad...55") y un *nonce* aleatorio se convierte en la entrada de una función de direccionamiento. En el caso de la Figura 2, el valor de direccionamiento del segundo bloque de datos 204 es "0xf6e1da2...deb", que se convierte en la firma del segundo bloque de datos 204, siendo "@$%" el *nonce* aleatorio encontrado para producir este valor de direccionamiento.

Todos los nodos de computación de borde de acceso múltiple 102M, 104M y 106M recibirán una notificación de la segunda transacción que busca registrarse en el libro mayor compartido, donde cada uno buscará entonces resolver para obtener una firma del segundo bloque de datos 204. Suponiendo que el nodo de computación de borde de acceso múltiple 102M es el primero en obtener la firma del segundo bloque de datos 204, el nodo de computación de borde de acceso múltiple 102M radiodifunde la firma del segundo bloque de datos 204 al nodo de computación de borde de acceso múltiple 104M y al nodo de computación de borde de acceso múltiple 106M, que desde la perspectiva del nodo de computación de borde de acceso múltiple 102M son nodos de computación de borde de acceso múltiple externos que son de confianza. Cada uno de los nodos de computación de borde de acceso múltiple 104M y 106M valida la firma del segundo bloque de datos 204 haciendo referencia al bloque de datos validado previo, a saber el primer bloque de datos 202 ("block0data"), a través del valor de direccionamiento del primer bloque de datos. El direccionamiento del primer bloque de datos 202 y el *nonce* aleatorio se direccionan entonces para determinar si se produce una salida que tenga el formato de datos específico descrito anteriormente (es decir que comience con una combinación predefinida de caracteres, por ejemplo siete ceros o una mezcla de letras y números). Si es así, se valida la firma del segundo bloque de datos 204, es decir se llega a un consenso mediante los nodos de computación de borde de acceso múltiple 104M y 106M. Con el consenso determinado, el valor de direccionamiento "0xf6e1da2...deb" es marcado en tiempo, fechado, serializado con un valor de índice "1", dando como resultado la creación exitosa del segundo bloque de datos 202. Dado que la segunda transacción se produce después de la primera transacción, el segundo bloque de datos 204 tiene una marca de tiempo posterior de "17:17" en comparación con la marca de tiempo "17:15" del primer bloque de datos 202. La creación exitosa del segundo bloque de datos 204 se radiodifunde a través de la trayectoria de comunicación 108, 110 que las estaciones base 102, 104 y 106 usan para comunicarse datos entre sí, para que cada uno de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M conserve una copia del segundo bloque de datos 204.

La información de una tercera transacción, "block2data", para inclusión como tercer bloque de datos 206 en el libro mayor compartido sigue un procedimiento similar al de la inclusión de la segunda transacción, "block1data" como el segundo bloque de datos 204 en el libro mayor compartido.

El contenido de "block2data" varía dependiendo de la naturaleza de la tercera transacción, de tal manera que los comentarios anteriores sobre "block0data" se aplican igualmente. Una combinación de "block2data", el valor de direccionamiento del segundo bloque de datos 202 (es decir "0xf6e1da2...deb") y un *nonce* aleatorio se convierte en la entrada de una función de direccionamiento. En el caso de la Figura 2, el valor de direccionamiento del tercer bloque de datos 206 es "0x9327eb1b...36a21", que se convierte en la firma del tercer bloque de datos 206, siendo "#!!" el *nonce* aleatorio encontrado para producir este valor de direccionamiento.

Todos los nodos de computación de borde de acceso múltiple 102M, 104M y 106M recibirán una notificación de la tercera transacción que busca registrarse en el libro mayor compartido, donde cada uno buscará entonces resolver para obtener una firma del tercer bloque de datos 206. De nuevo asumiendo que el nodo de

computación de borde de acceso múltiple 102M es el primero en obtener la firma del tercer bloque de datos 206, el nodo de computación de borde de acceso múltiple 102M radiodifunde la firma del tercer bloque de datos 206 al nodo de computación de borde de acceso múltiple 104M y al nodo de computación de borde de acceso múltiple 106M, que desde la perspectiva del nodo de computación de borde de acceso múltiple 102M son nodos de computación de borde de acceso múltiple externos que son de confianza. Cada uno de los nodos de computación de borde de acceso múltiple 104M y 106M valida la firma del tercer bloque de datos 206 haciendo referencia al bloque de datos validado previo, a saber el segundo bloque de datos 204 ("block1data"), a través del valor de direccionamiento del segundo bloque de datos. El direccionamiento del segundo bloque de datos 204 y el *nonce* aleatorio se direccionan entonces para determinar si se produce una salida que tiene el formato de datos específico descrito anteriormente (es decir que comienza con una combinación predefinida de caracteres, por ejemplo siete ceros o una mezcla de letras y números). Si es así, se valida la firma del tercer bloque de datos 206, es decir se llega a un consenso mediante los nodos de computación de borde de acceso múltiple 104M y 106M. Con el consenso determinado, el valor de direccionamiento "0x9327eblb...36a21" es marcado en tiempo, fechado, serializado con un valor de índice "2", dando como resultado la creación exitosa del tercer bloque de datos 206. Dado que la tercera transacción se produce después de la segunda transacción, el tercer bloque de datos 206 tiene una marca de tiempo posterior de "17:19" en comparación con la marca de tiempo "17:17" del segundo bloque de datos 204. La creación exitosa del tercer bloque de datos 206 se radiodifunde a través de la trayectoria de comunicación 108, 110 que las estaciones base 102, 104 y 106 usan para comunicarse datos entre sí, para que cada uno de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M conserve una copia del tercer bloque de datos 206.

Retornando a la Figura 1, se muestra que el sistema 100 soporta un caso de uso de contratos inteligentes 122, 124 que se relacionan con la gestión del uso de potencia, que ve la provisión de potencia desde una planta de potencia 118 a una estación de carga de drones 116 y una estación de carga de vehículos eléctricos (EV) 114. Un contrato inteligente se refiere a un contrato digital, que es un contrato cuyos términos y condiciones están programados en código de ordenador, almacenados y replicados en un libro mayor distribuido. La implementación del contrato inteligente en el libro mayor distribuido se hace mediante la planta de potencia 118 comunicándose con el nodo de computación de borde de acceso múltiple 106M, por ser el más cercano. El contrato inteligente 122 para la carga de drones y el contrato inteligente 124 para la carga de EV pueden usar términos y condiciones diferentes, que pueden ser acomodados por el libro mayor distribuido de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M.

La Figura 1 muestra que la estación de carga de EV 114 está en proximidad del nodo de computación de borde de acceso múltiple 102M, de tal manera que si se inicia una transacción (tal como carga de un vehículo eléctrico) de acuerdo con el contrato inteligente 126, el acceso para que la transacción sea procesada por el libro mayor distribuido alojado por el sistema 100 sería a través del nodo de computación de borde de acceso múltiple 102M. De manera similar, la estación de carga de drones 116 está en proximidad del nodo de computación de borde de acceso múltiple 104M, de tal manera que si se inicia una transacción (tal como carga de un dron) de acuerdo con el contrato inteligente 128, el acceso para que la transacción sea procesada por el libro mayor distribuido alojado por el sistema 100 sería a través del nodo de computación de borde de acceso múltiple 104M. Con referencia a la Figura 2, la cadena de bloques en el libro mayor distribuido podría adaptarse para, por ejemplo, atender un acuerdo de consenso en cuanto a si una billetera digital tiene fondos suficientes para pagar una cantidad de potencia solicitada a partir de analizar una nueva transacción contra transacciones pasadas. Se apreciará que aunque solo se muestran una estación de carga de EV 114 y una estación de carga de drones 116, cualquier otra plataforma que adopte el libro mayor distribuido alojado por el sistema 100 también puede utilizar el libro mayor distribuido aprovechando el nodo de computación de borde de acceso múltiple más próximo. Cada uno de los nodos de computación de borde de acceso múltiple recibe notificaciones de una transacción que se busca registrar en el libro mayor distribuido a través de la conexión celular proporcionada por su estación base asociada.

Además de gestionar el uso de potencia, otros contratos inteligentes soportables mediante el libro mayor distribuido del sistema 100 incluyen contratos de compra y venta, acreditación y débito de una billetera digital, rastreo de recursos en una cadena de suministro, la generación de flujo de contenido multimedia y la monitorización de las condiciones de tráfico en carretera.

La Figura 3 muestra un caso de uso de los contratos inteligentes 328 y 330 que se relacionan con la gestión de cadena de suministro, siendo estos contratos inteligentes 328 y 330 escritos en los libros mayores de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M. Similar a la Figura 2, cada una de las partes (a saber un fabricante principal 302, un fabricante subcontratado 304 y una empresa de logística 306 que suministra los bienes terminados en nombre del fabricante subcontratado 304) comunica el estado de un bien al nodo de computación de borde de acceso múltiple más cercano 102M, 104M y 106M. El contrato inteligente 328 puede ayudar con la gestión de cadena de suministro de la siguiente manera.

El fabricante principal 302 subcontrata ciertas partes de fabricación al fabricante subcontratista 304. Ambos inician un contrato inteligente 328 basado en los términos y condiciones acordados. El fabricante subcontratista 304 implementa entonces un contrato inteligente 330 con la empresa de logística 306 para suministrar el producto final al fabricante principal 302. Todos los contratos inteligentes 328 y 330 se registran en el libro

mayor distribuido desde el cual el fabricante principal 302 puede rastrear en tiempo real los eventos anteriores a la llegada del bien final.

La Figura 4 muestra un caso de uso de un contrato inteligente 406 que se relaciona con la generación de flujo de multimedia desde una fuente 402 a un dispositivo receptor (por ejemplo un monitor, altavoz o ambos) provisto dentro de un vehículo 410. La estación base 102 que soporta el nodo de computación de borde de acceso múltiple 102M puede estar situada en una región diferente (por ejemplo los EE. UU.) de la de la estación base 104 que soporta el nodo de computación de borde de acceso múltiple 104M (por ejemplo en Asia), de tal manera que un operador de red móvil basado en los EE. UU. usa la estación base 102, mientras que un operador de red móvil basado en Asia usa la estación base 104. El contrato inteligente 406 está codificado para tener en cuenta los requisitos de regulación en la región diferente en la cual reside cada parte (la fuente 402 que está en Asia y el vehículo 410 que está en los EE. UU.), siendo las billeteras digitales 406 y 408 usadas para asegurar el pago de los medios que se generan en flujo desde la fuente 402 al dispositivo receptor dentro del vehículo 410. Similar a la Figura 1, el libro mayor distribuido alojado por los nodos de computación de borde de acceso múltiple 102M y 104M está adaptado para atender un acuerdo de consenso con respecto al estado de cada una de las billeteras digitales 406 y 408 al procesar el flujo de multimedia, a partir de analizar una nueva transacción contra transacciones pasadas.

El seccionamiento de red 414 se implementa mediante la red central de virtualización de funciones de red (NFV) de operadores de redes móviles. La fuente 402 y el monitor en el vehículo 410 se convierten en partes de la red virtual, donde la red virtual permite el nivel correcto de conectividad que permite que la fuente 402 se comunique con el dispositivo receptor dentro del vehículo 410. Esto es particularmente ventajoso dado que IoT puede ser elementos personalizables (por ejemplo una placa de circuito simple con la electrónica necesaria para realizar su propósito específico), en lugar de un terminal de computación completo. Dado que tales elementos pueden ejecutar su propia arquitectura, la necesidad de que ellos se comuniquen con alta tasa de datos, baja latencia y buena QoS (Calidad de Servicio) se vuelve importante, lo cual se facilita al ser parte de la red virtual. El libro mayor distribuido proporciona entonces la arquitectura troncal para garantizar que se puedan validar las transacciones de acuerdo con los contratos inteligentes que cada uno de estos elementos está diseñado para soportar.

El caso de uso de la Figura 4 se aplica en un escenario de seccionamiento de red federada que utiliza tecnología de 5G que ofrece servicios intercontinentales transfronterizos de la siguiente manera. Suponer que una empresa de taxis autónomos (basada en los EE. UU.) ha firmado con una empresa de publicidad multimedia (basada en Asia) para proporcionar servicios publicitarios dentro del sistema en coche. Ambas empresas están ubicadas en diferentes continentes. Hay una ranura abierta para una campaña publicitaria de cinco minutos. La empresa de publicidad multimedia iniciará un contrato inteligente a través de los nodos de computación de borde de acceso múltiple 102M con la empresa de taxis (consultar número de referencia 410), una vez que se valide el pago en el libro mayor distribuido. El servicio se generará en flujo a través de los nodos de computación de borde de acceso múltiple 102M con conectividad de 5G que se ejecuta, profundo dentro de la red central virtualizada de operadores asiáticos aplicando secciones de red federadas específicas con QoS garantizada. Este servicio también se suministrará a través de la red de 5G del operador de contraparte y la infraestructura de nodos de computación de borde de acceso múltiple 104M en el continente de los EE. UU. y directamente en los paneles de sistema de los vehículos autónomos. Esta sección de red estará disponible en ambas plataformas de operadores, preferiblemente con servidores alojados en sus respectivos centros de datos, específicamente para operadores de redes móviles que quieran mantener todos los servicios de red a través de diferentes huellas de operadores que requieran acuerdos interoperadores.

La Figura 5 muestra un esquema de los nodos de computación de borde de acceso múltiple 502M, 504M que se distribuyen a través del sistema 100 para explicar cómo llegan a un consenso. Con referencia a la Figura 1, las estaciones base respectivas de los nodos de computación de borde de acceso múltiple 502M, 504M no se muestran en aras de la simplicidad.

Los nodos de computación de borde de acceso múltiple 502M, 504M que se muestran en la Figura 5 son testigos a los que se les permite validar nuevos bloques que van a ser agregados al libro mayor distribuido. Como tal, el principio de prueba de participación delegada descrito en la Figura 2 no requiere que todos los nodos de computación de borde de acceso múltiple del sistema validen una transacción antes de que el libro mayor distribuido se actualice con la transacción, permitiendo de esa manera que se ejecute la transacción. Además, tampoco se requiere que todos los nodos de computación de borde de acceso múltiple testigos 502M, 504M validen una transacción. En cambio, sería suficiente que un grupo de estos nodos de computación de borde de acceso múltiple 502M, 504M validen la transacción. En el caso de la Figura 5, una transacción se valida si el 66% de los nodos llegan a un consenso sobre la transacción, es decir 4 de los 6 nodos de computación de borde de acceso múltiple 502M, 504M (a saber los nodos de computación de borde de acceso múltiple 504M, mientras que no es requerido que los nodos de computación de borde de acceso múltiple 502M validen la transacción).

La Figura 6 proporciona un esquema de un protocolo híbrido 600 que se usa por el libro mayor distribuido del sistema 100 que se muestra en la Figura 1.

El protocolo híbrido 600 tiene dos capas. El protocolo 200 usado por la primera capa fue descrito en la Figura 2 y proporciona una cadena principal 252 para registrar transacciones hechas con respecto a bienes o servicios, que están de acuerdo con los términos y condiciones de un contrato inteligente. Los casos de uso fueron descritos en las Figuras 1, 3 y 4.

El protocolo 650 es usado por la segunda capa para controlar una o más cadenas laterales 652 de bloques de datos que se vinculan a un bloque de datos designado de la cadena principal 252 controlada por el protocolo 200 usado por la primera capa. Las cadenas laterales 652 pueden usarse para registrar transacciones hechas con respecto a bienes o servicios que pertenecen a una categoría diferente de las registradas en la cadena principal 252. El protocolo 650 usa algoritmos que se basan en conceptos matemáticos de grafos acíclicos dirigidos.

El propósito de la una o más cadenas laterales 652 es descargar la computación de la cadena principal 252 sobre la una o más cadenas laterales 652 de bloques de datos. Aunque en este documento se describen como bloques de datos, se apreciará que pueden entenderse como grafos de datos, dado que se usan conceptos matemáticos de grafos acíclicos dirigidos. La una o más cadenas laterales 652 de bloques de datos descargan la computación debido a que cada una de ellas puede definirse mediante un conjunto de reglas personalizado, que está de acuerdo con los principios del protocolo 650 usado por la segunda capa. Esto permite que la una o más cadenas laterales 652 de bloques de datos se optimicen para aplicaciones que requieren altas velocidades o computación liviana, mientras se conserva la cadena principal 252 para aplicaciones que requieren computación de peso pesado. Las aplicaciones que requieren una computación liviana se refieren a transacciones sin contrato subyacente o que están reguladas por un contrato subyacente donde el cumplimiento de sus términos y condiciones es rápidamente validado por los nodos de computación de borde de acceso múltiple del sistema 100 que se muestran en la Figura 1. Las aplicaciones que requieren una computación de peso pesado se refieren a transacciones que están reguladas por un contrato subyacente donde la validación del cumplimiento de sus términos y condiciones toma comparativamente más potencia de procesamiento y tiempo.

Cada una de la una o más cadenas laterales 652 de bloques de datos se sincroniza 654 con la cadena principal 252 en un bloque de datos designado de la cadena lateral 652 (se denota usando el número de referencia 658) para conciliar registros almacenados en la cadena principal 252 actualizando la cadena principal 252 con transacciones que se registran en la cadena lateral 652. La creación de estas cadenas laterales 652 y su sincronización con la cadena principal 252 se describe con más detalle en la Figura 7.

La Figura 7 proporciona un esquema de la interacción del protocolo 200 usado por la primera capa y el protocolo 650 usado por la segunda capa en el libro mayor distribuido del sistema 100 mostrado en la Figura 1. Esta interacción se ilustra en el bloque encadenado de datos mostrado en la Figura 2 y se produce en el segundo bloque de datos 204, que en el ejemplo mostrado en la Figura 7 es el nodo raíz de la cadena lateral 652. La interacción usa un enfoque de clavija bidireccional que se describe con mayor detalle a continuación. En el momento cuando uno o más de los nodos de computación de borde de acceso múltiple 502M, 504M (refiérase a la Figura 5) están validando el segundo bloque de datos 204, uno de estos nodos recibe una solicitud para crear una cadena lateral 652 de bloques de datos que se extiende desde la cadena principal 252 de bloques de datos (se representa usando la flecha 702 en la Figura 7). Esto hace que los activos se muevan de la cadena principal 252 a la cadena lateral 652 debido a que las transacciones se deben registrar en la cadena lateral 652 y se requieren activos para efectuar las transacciones. Los activos no necesariamente se refieren a monedas digitales o contraseñas, sino que también incluyen inventario usado para efectuar transacciones de bienes o servicios, dependiendo de los datos registrados en la cadena principal 252 y la cadena lateral 652. Los activos movidos se marcan para que se bloqueen en la cadena principal 252 de bloques de datos, lo cual hace que tales activos bloqueados no sean utilizables para efectuar transacciones registradas en la cadena principal 252. Para sincronizar la cadena principal 252 y la cadena lateral 652, se definen dos períodos de espera: un período de confirmación y un período de concurso.

El período de confirmación de una transferencia a la cadena lateral 652 es una duración durante la cual un activo debe estar bloqueado en la cadena principal 252 antes de que pueda transferirse a la cadena lateral 652. El propósito de este período de confirmación es permitir la firma múltiple de los nodos de computación de borde de acceso múltiple 502M, 504M, es decir que los nodos de computación de borde de acceso múltiple testigos 502M validen el bloqueo de activos en el segundo bloque de datos 204. La obtención de las firmas múltiples de los nodos de computación de borde de acceso múltiple 502M, 504M hace que un ataque de denegación de servicio en el siguiente período de espera (es decir el período de concurso) sea más difícil. Después de esperar el período de confirmación, se puede crear una transacción en la cadena lateral 652 que haga referencia a la prueba de que ha sido validada a través del consenso de los nodos de computación de borde de acceso múltiple 502M, 504M en la cadena principal 252.

El período de concurso es una duración en la cual un activo recién transferido no puede gastarse en la cadena lateral 652. El propósito del período de concurso es evitar el doble gasto al transferir activos bloqueados previamente. Si en cualquier punto durante este retraso, se genera un bloque de datos "en conflicto" para inclusión en la cadena principal 252 antes de los nodos de computación de borde de acceso múltiple testigos

504M, que no incluye el bloque de datos en el cual están bloqueados los activos, la conversión se invalida retroactivamente.

Si hay carencia de recepción del bloque de datos "en conflicto", esto significa que hay consenso entre los nodos de computación de borde de acceso múltiple testigos 504M, lo cual verifica que el segundo bloque de datos 204 con los activos bloqueados esté incluido en la cadena principal 252 (se representa usando la flecha 702 en la Figura 7). Esto hace que la cadena principal 252 de bloques de datos tenga al menos un bloque de datos con un registro de activos bloqueados.

Mientras están bloqueados en la cadena principal 252, los activos pueden transferirse libremente dentro de la cadena lateral 652 sin interacción adicional con la cadena principal 252. Las transacciones, determinadas como basadas en los activos bloqueados, pueden registrarse en uno o más bloques de datos 706 de la cadena lateral 652, sin requerir que sean validadas por el protocolo descrito en la Figura 2 que es con respecto a la cadena principal 252. Las nuevas transacciones registradas en uno o más bloques de datos 706 de la cadena lateral 652 se validan cuando cada nueva transacción puede aprobar dos transacciones previas registradas en bloques de datos anteriores de la cadena lateral 652 haciendo referencia a estas dos transacciones anteriores. La validación en la cadena lateral 652 por lo tanto se somete a un procedimiento de validación más simple en comparación con las validadas en la cadena principal 252.

El activo bloqueado conserva su identidad como un activo de cadena principal 252 y solo puede transferirse de vuelta a la misma cadena principal 252 de la que procede. La cadena lateral 652 está vinculada al bloque de datos de la cadena principal 252 con los activos bloqueados, es decir el segundo bloque de datos 204 de la cadena principal 252 es el nodo raíz de la cadena lateral 652.

Cuando se deben transferir activos desde la cadena lateral 652 de vuelta a la cadena principal 252, se hace una transacción de clavija hacia afuera en la cadena lateral 652. Esta transacción es verificada por los nodos de computación de borde de acceso múltiple testigos 504M que firman un gasto de transacción desde una billetera de firma múltiple que controlan en la cadena principal 252. Un número umbral (por ejemplo 66%) de los nodos de computación de borde de acceso múltiple testigos 504M debe firmar antes de que la transacción de cadena principal 252 se vuelva válida. Los nodos de computación de borde de acceso múltiple testigos 504M luego firman transacciones en la cadena lateral 652 que destruyen un número correspondiente de activos en la cadena lateral 652, transfiriendo efectivamente los activos desde la cadena lateral 652 a la cadena principal 252 (se representa usando la flecha 704 en la Figura 7).

Se proporciona un escenario de caso de uso para la cadena lateral 652 de la siguiente manera.

En una implementación, cada cadena lateral 652 está definida por un "conjunto de reglas" personalizado y se puede usar para descargar computaciones de otra cadena. Las cadenas laterales individuales 652 pueden seguir diferentes conjuntos de reglas de la cadena principal 252, lo cual significa que se pueden optimizar para aplicaciones que requieren velocidades extremadamente altas. Las cadenas laterales 652 se pueden entender como un gráfico discreto que está vinculado a la cadena principal 252 aplicado a través de una clavija bidireccional. En este caso, un DAG actúa como una cadena lateral 652, donde una máquina que escribe transacciones en la cadena principal 252 tiene que enviar sus fondos a una dirección de salida. Una vez que las contraseñas están en la dirección de salida, quedan bloqueados. Esto significa que la máquina ya no es capaz de usar las contraseñas. Para garantizar una seguridad aumentada, la comunicación se envía a través de la cadena principal 252 y la cadena lateral 652 y se permite un período de espera después de que la contraseña de la máquina se mueve a la dirección de salida. Una vez que se termina el período de espera, la contraseña se libera a la cadena lateral 652. La máquina entonces es capaz de gastar las contraseñas en la cadena lateral 652. Al moverse desde la cadena lateral 652 a la cadena principal 252, la máquina envía las monedas desde la cadena lateral 652 a una dirección de salida donde están bloqueadas. Una vez que se termina el período de espera, se transfiere un número equivalente de contraseñas a la cadena principal 252. Esto actúa como una sincronización bidireccional entre los dos libros mayores distribuidos híbridos, siendo el primero realizado mediante la cadena principal 252 y siendo el segundo realizado mediante la cadena lateral 652. La cadena lateral 652 proporciona muchos beneficios: (1) La cadena lateral DAG 652 es independiente de la cadena principal 252 que está protegida por cortafuegos y es responsable de su propia seguridad sin un riesgo importante para la integridad de la cadena principal 252. (2) DAG es conocido por escalabilidad a través de transacciones paralelas en su propia naturaleza, siendo DAG un escalamiento de capa 2 que permite que las transacciones se realicen fuera de la cadena principal 252, esto se puede escalar además con IoT. De este modo, se quita presión a la cadena principal 252 y se permite que la cadena principal 252 acelere además las transacciones. (3) Soporta activos sujetados bidireccionales (las cadenas laterales 652 emiten un activo que está respaldado en una tasa de intercambio determinista para los activos de cadena principal 252) con interoperabilidad. (4) La opción de incluir una cadena lateral federada para agregar nodos en medio de la cadena principal 252 y la cadena lateral 652 a través del consenso.

La Figura 8 proporciona un esquema de un grupo de nodos de computación de borde de acceso múltiple 800 que comprende varios nodos de computación de borde de acceso múltiple 802M, donde cada uno está configurado para soportar la implementación de bloques de datos (tanto en la cadena principal 252 como en la

cadena lateral 652, consultar las Figuras 6 y 7) de acuerdo con la presente invención para permitir una diversa carga de trabajo, orquestación y gobernanza que están accionadas por políticas. Cada nodo de computación de borde de acceso múltiple 802M tiene un bloque de plataforma de automatización 820 que sirve como una interfaz operativa para comunicarse con el libro mayor distribuido, tal como para verificar su estado y ejecutar instrucciones. A continuación se proporciona una visión general de las funciones proporcionadas por la plataforma de automatización 820.

Los contratos inteligentes existen como una o más aplicaciones descentralizadas o aplicaciones de libro mayor distribuido que se ejecutan en una capa de aplicación 804. Estos contratos inteligentes están escritos en código que cumple con las reglas de una capa de interfaz de aplicación 806, de tal manera que los contratos inteligentes pueden funcionar con el libro mayor distribuido proporcionado por los bloques de datos implementados en troquel. Ejemplos de contratos inteligentes incluyen aplicaciones que permiten que los servicios de IoT aprovechen la cadena de bloques implementada por los nodos de computación de borde de acceso múltiple 802M, incluyendo estos servicios, pero no limitados a, realidad aumentada (AR), realidad virtual (VR) o reconocimiento facial.

Un bloque de gestión 808 comprende un bloque de motor de políticas inteligentes 810, un bloque de contratos inteligentes 812 y un bloque de máquina virtual (VM) 814. Con referencia a las Figuras 6 y 7, el bloque de motor de políticas inteligentes de troquel 810 determina cuál del protocolo 200 de la primera capa y el protocolo 650 de la segunda capa se usa para procesar contratos inteligentes. Cuando los contratos inteligentes emplean encriptación para proteger datos confidenciales (como datos personales de las partes que ejecutan los contratos inteligentes y las billeteras digitales usadas para financiarlos), el bloque de motor de políticas inteligentes 810 también procesa la salida de protocolos de conocimiento cero que son soportados mediante cada uno de los nodos de computación de borde de acceso múltiple 802M, siendo estos protocolos descritos con mayor detalle en la Figura 10. El bloque de motor de políticas inteligentes 810 ayuda de este modo a gestionar bloques de datos que se generan a partir de transacciones efectuadas por contratos inteligentes escritos en los bloques de datos encadenados. En una implementación, donde está disponible el acceso a un procesador dedicado (descrito más adelante en la Figura 10), el bloque de motor de políticas inteligentes 810 también asigna carga computacional entre el procesador dedicado y un procesador estándar del nodo de computación de borde de acceso múltiple 802M. El bloque de máquina virtual 814 se usa para proporcionar un entorno de tiempo de ejecución para proporcionar un sistema de reglas manipuladas con datos que necesitan seguirse para crear un contrato inteligente compatible.

Un bloque de almacenamiento 816 gestiona el registro de transacciones de contratos inteligentes en bloques de datos en el libro mayor distribuido (ya sea el de la cadena principal 252 o el de la cadena lateral 652). El bloque de almacenamiento 816 también gestiona datos periféricos asociados con la transacción de contrato inteligente, tal como pero no se limita a una identidad de los dispositivos de IoT que son partes de la transacción de contrato inteligente y datos generados por las aplicaciones descentralizadas que se ejecutan en la capa de aplicación 804. Los bloques de datos se almacenan de acuerdo con cualquier estándar de sistema de archivos distribuido de pares, tal como el Sistema de Archivos Interplanetario (IPFS) y "Ceph" de Redhat®. Tal estándar soporta el protocolo híbrido descrito en las Figuras 6 y 7.

Un bloque de mensajería 818 se usa para la comunicación de datos o para ingresar instrucciones.

La Figura 9 proporciona un esquema de los grupos de nodos de computación de borde de acceso múltiple 902, 904 y 906, residiendo cada uno en diferentes regiones A, B y C. El DLT de libro mayor distribuido 908 que aloja los grupos 902, 904 y 906, de acuerdo con la presente invención, se muestra esquemáticamente.

La Figura 9 muestra un ecosistema de grupos de nodos de computación de borde de acceso múltiple interconectados 902, 904 y 906 en una red federada que usa la orquestación de contenedores 910. En más detalle, cada nodo de los grupos 902, 904 y 906 ejecuta una imagen de contenedor que es un paquete de software liviano, independiente, ejecutable que incluye todo lo necesario para ejecutar el libro mayor distribuido: código, tiempo de ejecución, herramientas de sistema, bibliotecas de sistema y configuraciones. La orquestación de contenedores 910 aprovisiona, programa y gestiona contenedores a escala para aplicaciones descentralizadas/aplicaciones de libro mayor distribuido (DApps) que residen en tales contenedores.

Los servicios de DApps se orquestan en los grupos de nodos de computación de borde de acceso múltiple 902, 904 y 906. Un contenedor federado es donde estos contenedores se gestionan en grupos, de tal manera que la orquestación de contenedores federados 912 está presente dado que estos grupos de nodos de computación de borde de acceso múltiple 902, 904 y 906 pueden pertenecer a diferentes redes de operadores. La orquestación de contenedores federados 912 se puede realizar mediante virtualización a nivel de sistema operativo de código abierto.

La orquestación de contenedores federados 912 permite una implementación consistente de DApps en cada nodo de computación de borde de acceso múltiple de los grupos 902, 904 y 906, permitiendo por lo tanto que las DApps funcionen de manera eficiente y fiable. La extrapolación, orquestación de contenedores federados 912 facilita la implementación de un paquete de aplicaciones de libro mayor distribuido en los grupos de nodos

de computación de borde de acceso múltiple 902, 904 y 906, en donde cada una de las aplicaciones está configurada para interconectarse con el DLT de libro mayor distribuido 908. Es decir el paquete de aplicaciones de libro mayor distribuido ya está codificado para funcionar en el DLT de libro mayor distribuido 908 y emitir datos en un formato compatible para inclusión en el bloque de datos encadenado compartido por el DLT de libro mayor distribuido 908. Como se explicó anteriormente, las aplicaciones de libro mayor distribuido son programas codificados para soportar contratos inteligentes escritos en el DLT de libro mayor distribuido 908. Bajo la orquestación de contenedores federados 912, el paquete de aplicaciones de libro mayor distribuido se codifica para cumplir con las regulaciones impuestas en una jurisdicción a la cual pertenece cada uno de los grupos de nodos de computación de borde de acceso múltiple 902, 904 y 906. Es decir si se ejecuta un contrato entre una parte en la región A y una parte en la región B, se cumplen automáticamente los requisitos reglamentarios en ambas regiones A y B, dado que una aplicación de libro mayor distribuido que soporta la ejecución del contrato en la región A cumple con los requisitos reglamentarios de la región A, mientras que una aplicación de libro mayor distribuido que soporta la ejecución del contrato en la región B cumple con los requisitos reglamentarios de la región B. De esa manera se implementa una solución para implementar transacciones transfronterizas. Adicionalmente, cada grupo 902, 904 y 906 comparte el descubrimiento de servicios, de tal manera que un recurso de ordenador principal es accesible desde cualquier otro grupo. Si un contenedor falla, se creará otro automáticamente.

Se apreciará que las diversas funciones descritas hasta ahora (por ejemplo generación de bloques de datos, ejecución de contratos inteligentes y gestión de motores de políticas inteligentes) se controlan a través de una unidad de procesamiento central (CPU) del nodo de computación de borde de acceso múltiple. La CPU está formada por uno o más procesadores centrales que tienen tal funcionalidad después de la instalación de software que escribe instrucciones que realizan las operaciones aritméticas y lógicas necesarias para ejecutar las funciones en el registro del sistema operativo del nodo de computación de borde de acceso múltiple. El término "procesador estándar" se refiere a tal CPU, que es parte de las especificaciones técnicas estándar del nodo de computación de borde de acceso múltiple.

La Figura 10 muestra un esquema no exhaustivo de las funciones 1004 que se ejecutan por el procesador estándar de cada uno de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M de la Figura 1 cuando se implementa un DLT de libro mayor distribuido 1008. También se muestra un esquema de un procesador dedicado 1040 diseñado para compartir la carga computacional del procesador estándar de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M para ejecutar estas funciones. El procesador dedicado 1040, a diferencia del procesador estándar, es un procesador que está diseñado específicamente para compartir la carga de trabajo computacionalmente pesada del procesador estándar que se encuentra durante la implementación de bloques de datos. Como tal, la arquitectura del procesador dedicado 1040 está equipada con particiones lógicas que son atendidas para tal implementación de bloques de datos.

Las funciones 1004 incluyen la determinación de un mecanismo de consenso 1006, protección de transacciones 1008. gestión de nodos 1010 y un generador de claves cuánticas 1012.

Con referencia a las Figuras 6 y 7, el mecanismo de consenso 1006 se refiere a descargar la carga de trabajo de computación (encriptación/desencriptación) que se produce cuando se ejecuta el mecanismo de consenso descrito en las Figuras 2, 6 y 7.

La protección de transacciones 1008 se refiere a abordar las preocupaciones de privacidad y seguridad en el DLT de libro mayor distribuido 1008, a través del uso de protocolos de conocimiento cero. ZKP permite a las entidades almacenar solo la prueba de la transacción en un nodo. Mantienen los datos confidenciales para sí mismos, mientras que aún mantienen la confianza en un registro conectado de procedencia.

Un protocolo de conocimiento cero es un método mediante el cual una parte (el probador) puede probar a otra parte (el verificador) que algo es verdadero, sin revelar ninguna información aparte del hecho de que esa declaración específica es verdadera. Las pruebas de conocimiento cero (ZKP) validan la verdad de algo sin revelar cómo se conoce la verdad ni compartir el contenido de esta verdad con el verificador. Este principio se basa en un algoritmo que toma algunos datos como entrada y retorna 'verdadero' o 'falso'. Las ZKP deben satisfacer tres criterios:

1. Completitud: si la declaración es verdadera, el verificador honesto (es decir, aquel que sigue el protocolo correctamente) estará convencido de este hecho por un probador honesto.

2. Solidez: si la declaración es falsa, ningún probador tramposo puede convencer al verificador honesto de que es verdadera, excepto con alguna pequeña probabilidad.

3. Conocimiento cero: si la declaración es válida, ningún verificador aprende nada más que el hecho de que la declaración es verdadera. En otras palabras, solo conocer la declaración (no el secreto) es suficiente para imaginar un escenario que muestre que el probador conoce el secreto. Esto se formaliza mostrando que cada verificador tiene algún simulador que, dada solamente la declaración que va a ser probada (y sin acceso al

probador), puede producir una transcripción que "parece" una interacción entre el probador honesto y el verificador en cuestión.

Los dos primeros de estos son propiedades de sistemas de prueba interactivos más generales. El tercero es lo que hace que la prueba sea de conocimiento cero.

Un protocolo de conocimiento cero, en línea con los principios anteriores, se aplica mediante la función de protección de transacciones 1008 cuando los nodos de computación de borde de acceso múltiple 102M, 104M y 106M detectan que una transacción actual para registro como un nuevo bloque de datos en el DLT de libro mayor distribuido 1008 contiene datos protegidos (por ejemplo una identidad de las partes de una transacción de contrato inteligente; detalles de una billetera digital usada para financiar la transacción de contrato inteligente: mensajes o conjunto de instrucciones entre ambas o múltiples partes en el libro mayor distribuido) para autentificar los datos protegidos. La autentificación de los datos protegidos se reduce a operaciones aritméticas donde una salida de nivel lógico "1" o "0" determina si se conoce el contenido de los datos protegidos. La salida del protocolo de conocimiento cero determina si la transacción actual es capaz de proceder con la validación (es decir puede registrarse como un nuevo bloque de datos en la cadena de bloques).

Cuando cualquiera o ambos del procesador estándar y el procesador dedicado 1040 de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M detectan que están presentes datos protegidos, estos procesadores identifican la existencia, dentro de la transacción actual, de declaraciones diseñadas para probar una verdad sobre si se conoce el contenido de los datos protegidos, estando los datos protegidos enmascarados o encriptados. Tales declaraciones sirven como medio para evidenciar que una transacción es sólida debido a que los datos protegidos están enmascarados y no se pueden analizar para tomar tal decisión. Las declaraciones identificadas se pueden formular dependiendo de los principios de la prueba de conocimiento cero en los cuales se basan los algoritmos. Los algoritmos aceptan datos específicos como entrada y retornan si las declaraciones identificadas son ya sea 'verdaderas' o 'falsas'. Los procesadores evalúan una verdad de las declaraciones identificadas y si se determina que es verdad que se conoce el contenido de los datos protegidos, autentifican la transacción protegida actual. Aunque no se garantiza una certeza absoluta, las declaraciones se formulan de tal manera que los resultados afirmativos reflejan un alto grado de probabilidad de que la transacción actual sea sólida, lo cual luego permite que la transacción actual se registre como un nuevo bloque de datos, como se establece en las Figuras 2, 6 y 7.

Al evaluar la verdad de las declaraciones identificadas, los procesadores de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M están configurados además para determinar que las declaraciones identificadas sean evaluadas como verdaderas por cada uno de un grupo de nodos de computación de borde de acceso múltiple externos. Es decir, tomando la perspectiva del nodo de computación de borde de acceso múltiple 102M como ejemplo, se llega a un consenso por cada uno de los nodos de computación de borde de acceso múltiple 104M y 106M que también están evaluando la verdad de la una o más declaraciones identificadas. El consenso puede seguir el enfoque como se describe en la Figura 2.

Un primer enfoque basa las declaraciones usadas para establecer la validez de la transacción actual en un ARgumento de Conocimiento Sucinto No Interactivo de conocimiento cero (zk-SNARK). Esto es un protocolo que crea un marco en el cual la transacción actual - enviada para validación por un nodo de computación de borde de acceso múltiple (por ejemplo 102M, véase Figura 1) llamado probador - puede convencer rápidamente a otros nodos de computación de borde de acceso múltiple (por ejemplo 104M y 106M, véase Figura 2) - llamados verificadores - de que el probador conoce un secreto sin revelar nada del secreto.

El protocolo realiza circuitos con entradas de 0 o 1 y una salida de 0 o 1. El probador conoce una cadena (0, 1, ..., 1) que dará como resultado una salida de 0. El secreto del probador es esta cadena, que en una implementación se basa en los detalles de los datos que están siendo protegidos y en otra implementación puede generarse arbitrariamente. Con el fin de convencer al verificador de que el probador conoce una cadena que tiene una salida de 0, el probador da una prueba π al verificador. El verificador verifica esta prueba. Si la prueba es correcta, el verificador puede estar seguro de que el probador conoce una cadena correcta.

Un Programa Aritmético Cuadrático (QAP) proporciona al probador herramientas para construir la prueba π para la reivindicación de que el probador conoce una asignación válida $(a, \ldots, a_N) \in F^N$ para un circuito C. Un QAP $Q(C) := (\vec{A}, \vec{B}, \vec{C}, Z)$ para un circuito aritmético dado C proporciona tres conjuntos de polinomios

$$\vec{A} = (A_i(z))_{i=0}^{m}, \quad \vec{B} = (B_i(z))_{i=0}^{m}, \quad \vec{C} = (C_i(z))_{i=0}^{m} \qquad (m \geq N)$$

con coeficientes en F, y un polinomio objetivo $Z(z) \in F(z)$ de tal manera que: El polinomio Z(z) divide al polinomio

$$P(z) := \underbrace{\left(A_0(z) + \sum_{i=1}^{m} a_i A_i(z)\right)}_{:=A(z)} \underbrace{\left(B_0(z) + \sum_{i=1}^{m} a_i B_i(z)\right)}_{:=B(z)} - \underbrace{\left(C_0(z) + \sum_{i=1}^{m} a_i C_i(z)\right)}_{:=C(z)}$$

si y solo si (a_1, . . . , a_N) es una asignación válida para el circuito C. El probador construye P(z) para su prueba π, y el verificador puede verificar la propiedad de divisibilidad de P(z) por Z(z).

Otro enfoque usa una configuración de confianza de una vez para generar un par de claves privada/pública que se usa para generar declaraciones que se usan para establecer la validez de la transacción actual. La parte privada se destruye y a partir de la parte pública se genera otro par de claves, produciendo una clave de prueba y una clave de verificación. La clave de prueba y la clave de verificación se distribuyen para proporcionar una referencia común compartida entre el probador y el verificador. Una transacción actual que va a ser registrada en el libro mayor distribuido de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M contiene una computación creada a partir de la clave de probador distribuida, por ejemplo usando una entrada pública dada y la clave de probador para generar una prueba. Los procesadores de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M, al realizar su función como el "verificador", están configurados para obtener la clave de verificación distribuida que corresponde a la clave de probador distribuida. Los procesadores evalúan la computación usando la clave de verificación distribuida y permiten que la validación proceda (es decir que se registre un nuevo bloque de datos) en respuesta a la evaluación de la computación que produce una salida correcta.

Un segundo enfoque para evaluar la verdad de las declaraciones usadas para establecer la validez de la transacción actual usa un enfoque interactivo.

Un sistema de prueba interactivo <P, V> para un algoritmo L es de conocimiento cero si para cualquier verificador V* existe un simulador esperado S de tal manera que

$$\forall\, x \in L, z \in \{0,1\}^*, \text{Vista}_{V^*}[P(x) \leftrightarrow V^*(x,z)] = S(x,z)$$

La definición establece que un sistema de prueba interactivo <P, V> es de conocimiento cero si para cualquier verificador V* existe un simulador eficiente S que esencialmente puede producir una transcripción de la conversación que habría tenido lugar entre P y V* en cualquier entrada dada. Por lo tanto, tener una conversación con P no puede enseñar a V* a computar algo que no podría haber computado antes. La cadena z en la definición desempeña la función de "conocimiento previo" (incluyendo las monedas aleatorias de V*); V* no puede usar ninguna cadena de conocimiento previo z para extraer información de su conversación con P debido a que el requisito es que si a S también se le da este conocimiento previo entonces puede reproducir la conversación entre V* y P tal como antes.

En el enfoque interactivo, los procesadores de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M están configurados para iterar las declaraciones identificadas a través de al menos una prueba: y concluir que las declaraciones son verdaderas cuando la mayoría de las iteraciones producen un resultado consistente.

Volviendo a la gestión de nodos 1010, esto se refiere a monitorizar la operación del chip dedicado 1040, tal como su registro 1018A, RAM 1018B y registro de QKD (Distribución de Claves Cuánticas) 1018C. El registro 1018A contiene una ID única del chip dedicado 1040. Este ID se escribe en el registro 1018A durante la fabricación. La misma ID se protege y se almacena en la DLT 1008. Existe la posibilidad de añadir más de un registro 1018A al chip dedicado 1040.

La RAM 1018B proporciona caché para el chip dedicado 1040. El registro de QKD 1018C almacena claves criptográficas usadas por el chip dedicado 1040, el procesador estándar o ambos.

La generación de clave cuántica 1012 es responsable de seleccionar un protocolo de conocimiento cero del registro de QKD 1018C para uso al analizar transacciones con datos protegidos.

Cuando se debe registrar una transacción en el DLT de libro mayor distribuido 1008, la computación requerida se puede extraer tanto del procesador de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M como del procesador dedicado 1040. El procesador dedicado 1040 está diseñado para compartir la carga computacional del procesador estándar de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M al estar dividido en bloques lógicos 1014, 1016 y 1018. Cada bloque tiene componentes electrónicos diseñados para compartir la ejecución de una respectiva de las funciones del procesador a través de una combinación de puertas lógicas conectadas adecuadamente. En una implementación de ASIC (circuito integrado de aplicación específica) 1020, se fabrica un sustrato semiconductor con puertas lógicas a partir de una biblioteca de componentes de acuerdo con un esquema de circuitería que es atendido específicamente para soportar el DLT de libro mayor distribuido 1008.

Un bloque acelerador de encriptación/desencriptación 1014 comparte la carga computacional con el mecanismo de consenso 1006. Un bloque acelerador de ZKP (protocolo de conocimiento cero) 1016 comparte la carga computacional con la protección de transacciones 1008. Un bloque de Registro de OID/RAM Segura/Registro de QKD proporciona almacenamiento para datos asociados con la gestión de nodos 1010 y el generador de QKD 1012. La comunicación entre el procesador dedicado 1040 y el procesador de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M es a través de un bus de alta velocidad 1022. El bus de alta velocidad 1022 puede ejecutarse en uno cualquiera o más de los siguientes protocolos de conexión: USB2.0. 3.X. PCIe, SATA. NVMe.

La Figura 11 muestra un diseño del procesador dedicado 1040 de la Figura 10. El procesador dedicado 1040 es para instalación en un nodo de computación de borde de acceso múltiple ubicado dentro de un área de cobertura celular soportada por una estación base de un operador de red móvil, tal como uno cualquiera de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M y sus estaciones base asociadas 102, 104 y 106 descritas en la Figura 1. El procesador dedicado 1040 puede proporcionarse como una llave inteligente removible, montado en una placa de circuito impreso o integrado a una placa madre o placa de circuito electrónico en la cual está montado el procesador estándar de los nodos de computación de borde de acceso múltiple 102M, 104M y 106M, a través del bus de alta velocidad 1022 mencionado en la Figura 10.

Dentro de una placa 1106 en la cual está montado el procesador dedicado 1040, el procesador dedicado 1040 tiene componentes electrónicos divididos en particiones lógicas distribuidas en un área segura 1102 y un área no segura 1104 de un límite de chip 1105. Esta electrónica incluye numerosas puertas lógicas elementales de configuración AND, OR, XOR, NOT. NAND. NOR y XNOR que están conectadas adecuadamente para realizar la función requerida de cada partición lógica.

La placa 1106 tiene dispositivos de nivel de placa 1108, una fuente de alimentación 1110 para alimentar los componentes del procesador dedicado 1040 y un reloj externo 1112.

El área no segura 1104 tiene su propio segmento de potencia 1116, una interfaz genérica 1114, un reloj 1118 y un servicio de sistema 1120. La comunicación entre el área no segura 1104 y el área segura 1104 se produce a través de un APB (bus periférico avanzado) 1122.

Los componentes del área segura 1102 son de la siguiente manera: un núcleo de procesador 1124, una RAM en chip 1126, un almacenamiento en chip 1128, módulos de acceso directo a memoria (DMA) 1134 y 1136, memoria de código de corrección de errores 1132 (para corregir corrupción de datos internos), ROM de arranque segura 1138, un generador de números aleatorios verdaderos (TRNG) 1140, una sección programable una vez (OTP) 1142 que proporciona una o más áreas donde cada una puede usarse para almacenar datos como el número de serie del chip dedicado con fusibles de interconexión que subsecuentemente se funden, y módulos de encriptación: SHA-2 1144, SHA-3 1146, ZKP 1148; RSA 1150 y AES 1152.

El núcleo de procesador 1124 se comunica con los módulos de encriptación a través de un bus avanzado de alto rendimiento (AHB) 1130. Los módulos SHA-2 1144 y SHA-3 1146 proporcionan los algoritmos de direccionamiento seguros usados para direccionar bloques de datos en la cadena de bloques descrita en las Figuras 2, 6 y 7. El módulo de ZKP 1148 proporciona los protocolos de conocimiento cero para procesar transacciones que tienen datos protegidos, como se describe en la Figura 10. El módulo RSA 1150 proporciona algoritmos compatibles con Rivest-Shamir-Adleman, mientras que el módulo AES 1152 proporciona algoritmos estándar de encriptación avanzados que se pueden usar durante el procesamiento de una transacción para registro en la cadena de bloques. El núcleo de procesador 1124 también usa el AHB 1130 para comunicarse con componentes externos (tal como el procesador estándar de un nodo de computación de borde de acceso múltiple) a través de una interfaz de alta velocidad 1154 o con el área no segura 1104 a través de un puente 1156.

Con referencia a la Figura 10, se recurre a uno o más componentes del área segura 1102 para facilitar la computación requerida que se emprende por el procesador estándar para realizar las funciones 1004. Por ejemplo, uno o más componentes del área segura 1102 se activan para proporcionar una partición de gestión de libro mayor que está configurada para compartir la carga computacional del procesador estándar del nodo de computación de borde de acceso múltiple para incluir un nuevo bloque de datos, para registrar una transacción actual con respecto a un bien o servicio, en un bloque de datos encadenado almacenado en al menos una memoria del nodo de computación de borde de acceso múltiple en el cual está instalado el procesador dedicado 1040. El nuevo bloque de datos se registra en respuesta a una firma, generada a partir de procesar los datos de la transacción actual con datos codificados de transacciones pasadas almacenadas en el bloque de datos encadenado, que es validada por un grupo de nodos de computación de borde de acceso múltiple externos que son de confianza. La partición de gestión de libro mayor puede incluir el núcleo de procesador 1124 que envía instrucciones a los módulos SHA-2 1144, SHA-3 1146, RSA 1150, AES 1152 y ECC 1132 para realizar el direccionamiento requerido para registrar un nuevo bloque de datos como se describe en la Figura 2.

Las Figuras 6 y 7 describen que el libro mayor distribuido puede registrar un nuevo bloque de datos en una cadena principal 252 o una cadena lateral 652, dependiendo de la potencia de procesamiento requerida para registrar el nuevo bloque de datos. Para permitir la implementación de la cadena lateral 652, la partición de gestión de libro mayor puede configurarse además para compartir la carga computacional del procesador estándar del nodo de computación de borde de acceso múltiple para: bloquear activos en al menos un bloque de datos de la cadena principal 252. El procesador dedicado 1040 registra entonces transacciones, determinadas como basadas en los activos bloqueados, en uno o más bloques de datos de la cadena lateral 652; y ayuda a vincular la cadena lateral 652 al bloque de datos de la cadena principal 252 con los activos bloqueados.

Uno o más componentes del área segura 1102 se activan para proporcionar una partición de validación de transacciones protegida que está configurada para compartir la carga computacional del procesador estándar del nodo de computación de borde de acceso múltiple para procesar transacciones con datos protegidos, que son datos que se pretende que se mantengan confidenciales y no se compartan.

En el caso donde la partición de validación de transacciones protegidas detecte transacciones con tales datos protegidos, la partición de validación de transacciones protegidas usa una prueba de conocimiento cero que busca autentificar los datos protegidos a través de la aplicación de operaciones aritméticas que se reducen a una salida de nivel lógico "1" o "0" para determinar si se conoce el contenido de los datos protegidos. La salida del protocolo de conocimiento cero determina si la transacción actual es capaz de proceder con la validación (es decir puede registrarse como un nuevo bloque de datos en la cadena de bloques). La partición de validación de transacciones protegidas busca ubicar declaraciones diseñadas para probar una verdad sobre si se conoce el contenido de los datos protegidos, con las operaciones aritméticas que se aplican a tales declaraciones, estando los datos protegidos enmascarados o encriptados. Las declaraciones identificadas pueden formularse dependiendo de los principios de la prueba de conocimiento cero. Si la evaluación de las declaraciones identificadas indica que es verdadero que se conoce el contenido de los datos protegidos, esto autentifica los datos protegidos y permite que la transacción actual se registre como un nuevo bloque de datos, como se establece en las Figuras 2, 6 y 7.

Al evaluar la verdad de las declaraciones identificadas, la partición de validación de transacciones protegidas puede configurarse además para determinar que las declaraciones identificadas sean evaluadas como verdaderas por cada uno de un grupo de nodos de computación de borde de acceso múltiple externos. Es decir, se llega a un consenso por cada uno de los nodos de computación de borde de acceso múltiple que también están evaluando la verdad de la una o más declaraciones identificadas.

Un enfoque basa las declaraciones usadas para autentificar los datos ocultos que se basan en un ARgumento de Conocimiento Sucinto No Interactivo de Conocimiento Cero (zk-SNARK). Por ejemplo, se usa una configuración de confianza de una vez para generar un par de claves privada/pública para generar declaraciones usadas para establecer la validez de la transacción actual. La parte privada se destruye y a partir de la parte pública se genera otro par de claves, produciendo una clave de prueba y una clave de verificación. La clave de prueba y la clave de verificación se distribuyen para proporcionar una referencia común compartida. Una transacción actual que va a ser registrada en el libro mayor distribuido contiene una computación creada a partir de la clave de probador distribuida, por ejemplo usando una entrada pública dada y la clave de probador para generar una prueba. La partición de validación de transacciones protegidas está configurada para obtener la clave de verificación distribuida que corresponde a la clave de probador distribuida. La partición de validación de transacciones protegidas evalúa la computación usando la clave de verificación distribuida y permite que la validación (es decir que se registre un nuevo bloque de datos) proceda en respuesta a la evaluación de la computación que produce una salida correcta.

Otro enfoque evalúa la verdad de las declaraciones usadas para autentificar los datos protegidos a través de un enfoque interactivo. La partición de validación de transacciones protegidas puede configurarse además para iterar las declaraciones identificadas a través de al menos una prueba; y concluir que las declaraciones son verdaderas cuando la mayoría de las iteraciones producen un resultado consistente.

En el caso donde la partición de validación de transacciones protegidas detecte que una transacción actual contiene datos que requieren protección, la partición de validación de transacciones protegidas procede a proteger tales datos. La partición de validación de transacciones protegidas formula entonces declaraciones diseñadas para probar una verdad sobre si se conoce el contenido de los datos protegidos, estando los datos protegidos enmascarados.

La Figura 12 proporciona un flujo que demuestra cómo un motor de políticas inteligentes 1210 (también consultar número de referencia 810 de la Figura 8) que opera en un procesador estándar de un nodo de computación de borde de acceso múltiple trabaja con el procesador dedicado 1040 de la Figura 11 para implementar los libros mayores distribuidos descritos en las Figuras 2, 6 y 7.

En la etapa 0, tiene lugar una transacción, que puede ser una simple nano transacción (Tx) que va a ser registrada en una cadena lateral (consultar las Figuras 6 y 7) o una transacción con contrato inteligente (SC)

que va a ser registrado en una cadena principal. Las transacciones pueden o pueden no requerir protección de datos y su protocolo de conocimiento cero asociado.

En la etapa 1, el motor de políticas inteligentes 1210 actúa como un puente de comunicación entre el libro mayor distribuido 1212 y el procesador dedicado 1040. El motor de políticas inteligentes 1210 recolectará las tareas requeridas y la cantidad de prueba de conocimiento cero (ZKP) para procesar desde el libro mayor distribuido 1212.

En la etapa 2, el motor de políticas inteligentes 1210 organiza las tareas en un grupo y asigna prioridades de transacción de ZKP. El motor de políticas inteligentes 1210 puede dividir los grupos en "Grupo grande", "Grupo mediano" o "Grupo pequeño".

En la etapa 3, se completa la configuración de priorización y los conjuntos de instrucciones se envían al procesador dedicado 1040 uno a la vez, dependiendo de la política definida por el motor de políticas inteligentes 1210.

En la etapa 4, el procesador dedicado 1040 incluye un mezclador de tareas interno que es responsable de emitir trabajos a múltiples aceleradores integrados (acc_1, acc_2_n) dentro del procesador dedicado 1040. La computación se completa dentro de una ventana predefinida. Un combinador combinará colectivamente todos los resultados de computación en un lote.

En la etapa 5, el procesador dedicado 1040 envía los resultados de vuelta al motor de políticas inteligentes 1210.

En la etapa 6, el motor de políticas inteligentes 1210 completará un paquete enmascarado de ZKP que se suministra al libro mayor distribuido 1212 para validación.

La Figura 13 es un esquema de un sistema que comprende un libro mayor distribuido 1008 que se implementa mediante un procesador de los nodos de computación de borde de acceso múltiple 102M y 104M de la Figura 1 que comparte carga computacional con el procesador dedicado 1040 de la Figura 11.

Con el procesador dedicado 1040 que está conectado al procesador estándar de los nodos de computación de borde de acceso múltiple 102M y 104M, se impulsan todas las funciones. Los protocolos 200 y 650 que registran transacciones de los casos de uso 1324 y 1326 en el libro mayor distribuido 1008 se ejecutan más rápido. El caso de uso 1324 demuestra una transacción de contrato inteligente de peso pesado a través de la capa 1 (consultar número de referencia 200) y el caso de uso 1326 es una nano transacción de peso ligero a través de la capa 2 (consultar número de referencia 650) que acelera el rendimiento y el consenso en el libro mayor distribuido 1008 soportado mediante el procesador dedicado 1040.

La incorporación del procesador dedicado 1040 da como resultado una latencia global más baja, impulsa el rendimiento y soporta la encriptación de privacidad.

La Figura 14 es un esquema para explicar cómo se realiza la elección de los nodos de computación de borde de acceso múltiple testigos 1406.

En una red 1400 que comprende nodos de computación de borde de acceso múltiple que utilizan un libro mayor distribuido, las partes interesadas 1402 hacen referencia a las máquinas que contienen contraseñas de utilidad. Estas partes interesadas 1402 monitorizan continuamente los nodos de computación de borde de acceso múltiple con mejor rendimiento y los votan para que sean de confianza. Los nodos de computación de borde de acceso múltiple de confianza se convierten en testigos 1404 a los que se les permite actualizar el libro mayor distribuido con datos de nuevas transacciones. El consenso tiene que ser alcanzado por un porcentaje de los testigos 1404 (por ejemplo 66 o 67 de ellos). Los delegados 1406 están formados por un consorcio de operadores de redes móviles, que tienen el poder de proponer cambios a la red 1400 a través de la votación de partes interesadas 1402.

En la solicitud, a menos que se especifique otra cosa, los términos "que comprende", "comprende" y variantes gramaticales de los mismos, previstos para representar un lenguaje "abierto" o "inclusivo" de tal manera que incluyan elementos citados pero también permitan la inclusión de elementos adicionales, no citados explícitamente. También se apreciará que los términos "información" y "datos" se usan de manera intercambiable, especialmente cuando se hace referencia al registro de transacciones en un libro mayor distribuido.

Aunque está invención se ha descrito con referencia a realizaciones de ejemplo, se entenderá por los expertos en la técnica que se pueden hacer diversos cambios y se pueden sustituir equivalentes por elementos de la misma, sin apartarse del alcance de la invención. Además, se puede hacer modificación para adaptar las enseñanzas de la invención a situaciones y materiales particulares, sin apartarse del alcance esencial de la invención. De este modo, la invención no se limita a los ejemplos particulares que se divulgan en esta

especificación, sino que abarca todas las realizaciones que caen dentro del alcance de las reivindicaciones anexas.

REIVINDICACIONES

1. Un nodo de computación de borde de acceso múltiple (102M) ubicado para utilizar la infraestructura de red de acceso por radio de una estación base (102) de un operador de red móvil (A) para comunicación celular que comprende bandas de frecuencia de 4G y 5G, comprendiendo el nodo de computación de borde de acceso múltiple

al menos una memoria para almacenar un bloque de datos encadenado, donde cada bloque de datos está codificado con datos de una transacción pasada con respecto a un bien o servicio; y

al menos un procesador configurado con funciones que:

incluyen un nuevo bloque de datos, para registrar una transacción actual con respecto a un bien o servicio, en el bloque de datos encadenado en respuesta a una firma, generada a partir de procesar los datos de la transacción actual con los datos codificados de las transacciones pasadas almacenadas en el bloque de datos encadenado, que es validada por otros nodos de computación de borde de acceso múltiple, en donde el nodo de computación de borde de acceso múltiple y los otros nodos de computación de borde de acceso múltiple son de confianza, y se comunican a través de un canal común,

en donde los datos con respecto a transacciones se reciben a través de conexión celular proporcionada por la estación base.

2. El nodo de computación de borde de acceso múltiple (102M) de la reivindicación 1, en donde los bloques de datos pertenecen a una cadena principal y en donde el procesador está configurado con funciones adicionales que:

bloquean activos en al menos un bloque de datos de la cadena principal;

registran transacciones, determinadas como basadas en los activos bloqueados, en uno o más bloques de datos de una cadena lateral; y

vinculan la cadena lateral al bloque de datos de la cadena principal con los activos bloqueados.

3. El nodo de computación de borde de acceso múltiple (102M) de la reivindicación 2, en donde el procesador está configurado con funciones adicionales que:

escriben las transacciones registradas en los bloques de datos de la cadena lateral en uno o más bloques de datos de la cadena principal al actualizar la cadena principal del gasto de los activos bloqueados que resultan de las transacciones registradas en la cadena lateral.

4. El nodo de computación de borde de acceso múltiple (102M) de la reivindicación 2 o 3, en donde el procesador está configurado con funciones adicionales que proporcionan un motor de políticas que:

evalúa la transacción actual para registro en la cadena principal o en la cadena lateral, en una instancia cuando se realiza la transacción actual; y

registra la transacción actual ya sea en la cadena principal o en la cadena lateral en respuesta a la evaluación.

5. El nodo de computación de borde de acceso múltiple (102M) de una cualquiera de las reivindicaciones precedentes, en donde el procesador está configurado con funciones adicionales que tras la determinación de que la transacción actual contiene datos protegidos:

analizan la transacción actual usando un protocolo de conocimiento cero configurado para autentificar los datos protegidos; y

procesan una salida del protocolo de conocimiento cero, en donde la salida determina si la transacción actual es capaz de proceder con la validación.

6. El nodo de computación de borde de acceso múltiple (102M) de la reivindicación 5, en donde el protocolo de conocimiento cero tiene el procesador que está configurado además con funciones adicionales que:

identifican la existencia, dentro de la transacción actual, de declaraciones diseñadas para probar una verdad sobre si se conoce el contenido de los datos protegidos, estando los datos protegidos enmascarados;

evalúan las declaraciones identificadas; y

permiten que la validación proceda en respuesta a la evaluación que prueba que se conocen los datos protegidos.

7. El nodo de computación de borde de acceso múltiple (102M) de la reivindicación 6, en donde el procesador está configurado además con funciones adicionales que:

determinan que una misma evaluación de las declaraciones identificadas se alcanza por cada uno de los otros nodos de computación de borde de acceso múltiple.

8. El nodo de computación de borde de acceso múltiple (102M) de la reivindicación 6 o 7, en donde las declaraciones se basan en una computación creada a partir de una clave de prueba distribuida, en donde el procesador está configurado además con funciones adicionales que:

obtienen una clave de verificación distribuida que corresponde a la clave de probador distribuida;

evalúan la computación usando la clave de verificación distribuida; y

permiten que la validación proceda en respuesta a la evaluación de la computación que produce una salida correcta.

9. El nodo de computación de borde de acceso múltiple (102M) de la reivindicación 6 o 7, en donde para evaluar la verdad de las declaraciones identificadas, el procesador está configurado además con funciones adicionales que:

iteran las declaraciones identificadas a través de al menos una prueba; y

concluyen que las declaraciones son verdaderas cuando una mayoría de las iteraciones producen un resultado consistente.

10. El nodo de computación de borde de acceso múltiple (102M) de la reivindicación 5, en donde el procesador está configurado con funciones adicionales que proporcionan un motor de políticas que está configurado para decidir si registrar la transacción actual ya sea en la cadena principal o en la cadena lateral y procesar la salida del protocolo de conocimiento cero.

11. El nodo de computación de borde de acceso múltiple (102M) de una cualquiera de las reivindicaciones precedentes, en donde el canal común yace a lo largo de una trayectoria usada por la estación base (102) que soporta el nodo de computación de borde de acceso múltiple para comunicarse con una estación base que tiene un área de cobertura celular dentro de la cual se ubica el otro nodo de computación de borde de acceso múltiple.

12. El nodo de computación de borde de acceso múltiple (102M) de una cualquiera de las reivindicaciones precedentes, en donde el procesador está configurado con funciones adicionales que

copian el bloque de datos encadenado en la al menos una memoria desde los otros nodos de computación de borde de acceso múltiple en respuesta a la recepción de un certificado de seguridad acompañante que autentifica los bloques de datos encadenados.

13. El nodo de computación de borde de acceso múltiple (102M) de una cualquiera de las reivindicaciones precedentes, en donde cada uno de los bloques de datos en el bloque de datos encadenado comprende un direccionamiento de los datos en un bloque de datos precedente.

14. El nodo de computación de borde de acceso múltiple (102M) de una cualquiera de las reivindicaciones precedentes, en donde las transacciones almacenadas en el bloque de datos encadenado comprenden datos relacionados con la ejecución de contratos inteligentes.

15. El nodo de computación de borde de acceso múltiple (102M) de la reivindicación 14, en donde los datos relacionados con la ejecución de contratos inteligentes comprenden uno cualquiera o más de los términos en un contrato de compra y venta; acreditación y débito de una billetera digital; rastreo de recursos en una cadena de suministro; generación de flujo de contenido multimedia; gestión de uso de potencia; y monitorización de condiciones de tráfico en carretera.

16. El nodo de computación de borde de acceso múltiple (102M) de una cualquiera de las reivindicaciones precedentes, que comprende además un procesador dedicado (1040), en donde el procesador dedicado está configurado para compartir la carga computacional del procesador.

17. El nodo de computación de borde de acceso múltiple (102M) de la reivindicación 16, en donde el procesador dedicado (1040) está dividido en particiones lógicas, teniendo cada partición componentes electrónicos diseñados para compartir la ejecución de una respectiva de las funciones del procesador.

18. El nodo de computación de borde de acceso múltiple (102M) de la reivindicación 16 o 17, en donde el procesador dedicado (1040) es: proporcionado como una llave inteligente removible, montando en una placa de circuito impreso o integrado en una placa de circuito en la cual está montado el procesador.

19. El nodo de computación de borde de acceso múltiple (102M) de una cualquiera de las reivindicaciones precedentes, en donde el nodo de computación de borde de acceso múltiple está ubicado adyacente a la estación base (102).

20. El nodo de computación de borde de acceso múltiple (102M) de una cualquiera de las reivindicaciones precedentes, en donde la comunicación de datos con respecto a la inclusión del nuevo bloque de datos se produce dentro de bandas de frecuencia de 4G o 5G.

21. El nodo de computación de borde de acceso múltiple (102M) de una cualquiera de las reivindicaciones precedentes, en donde el procesador está configurado además para implementar aplicaciones de libro mayor distribuido codificadas para soportar la ejecución de contratos inteligentes transfronterizos.

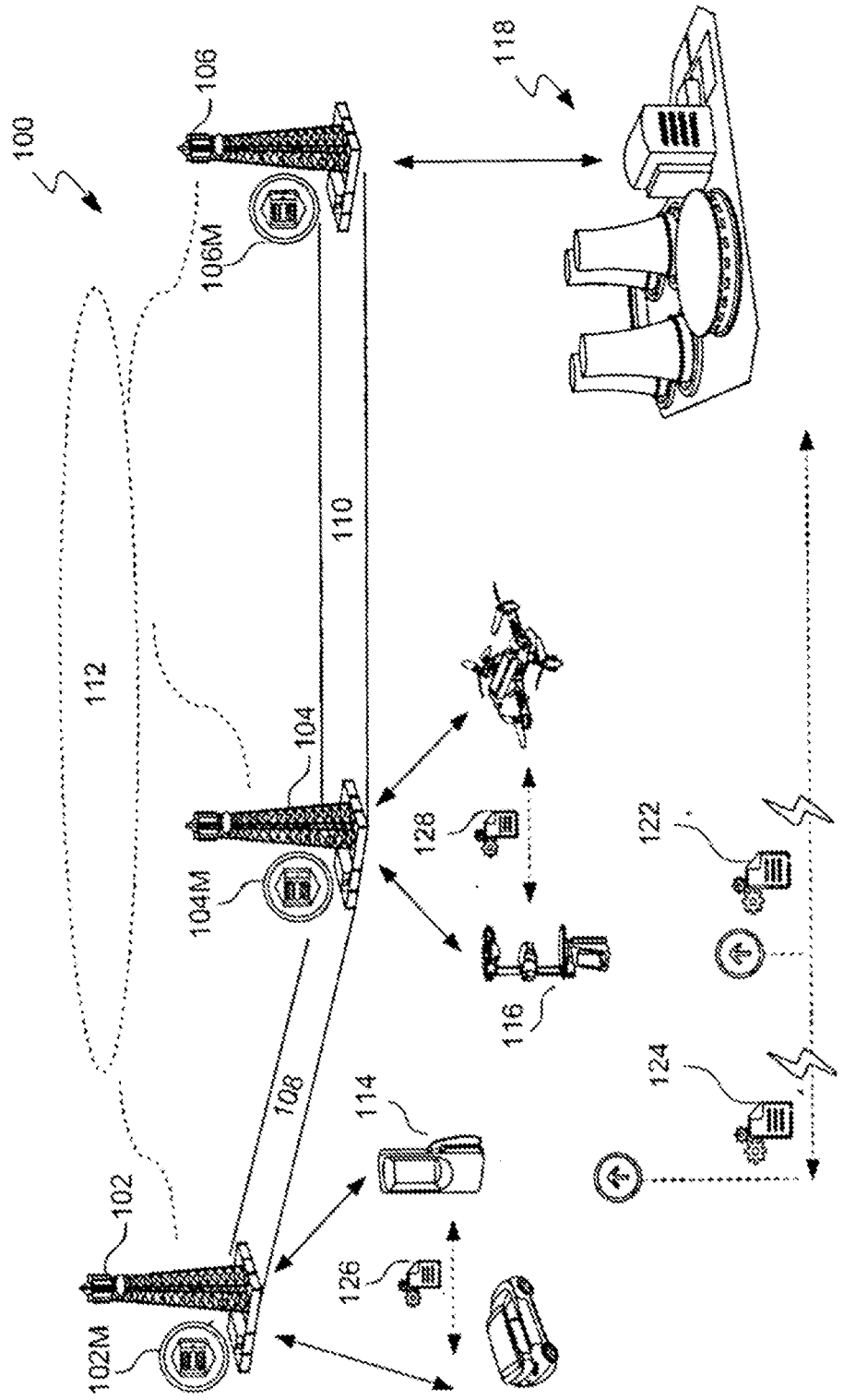
100
102
102M
104
104M
106
106M
108
110
112
114
116
118
122
124
126
128

Figura 1

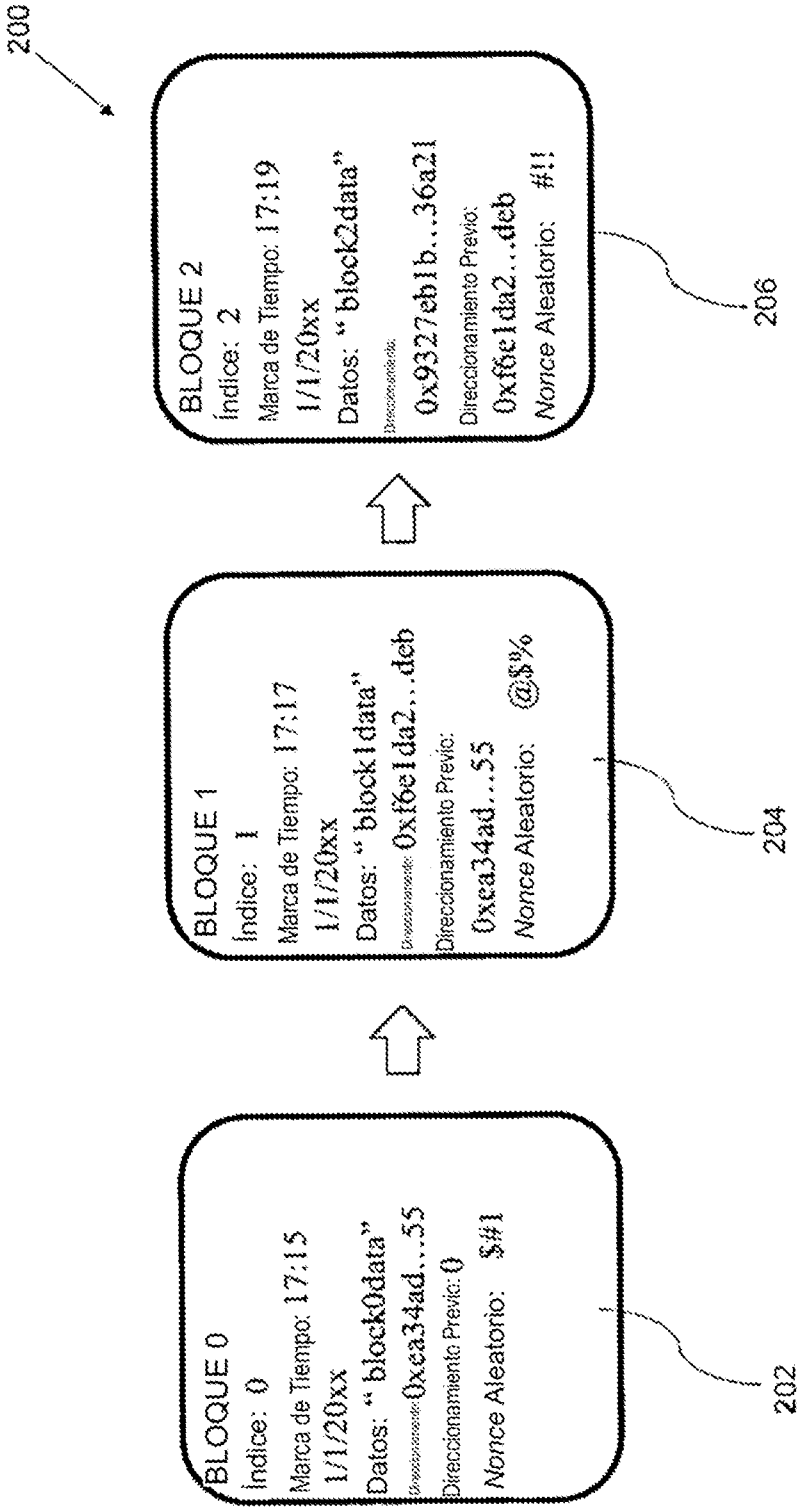
200
BLOQUE 0
Índice: 0
Marca de Tiempo: 17:15
1/1/20xx
Datos: " block0data"
0xea34ad...55
Direccionamiento Previo: 0
Nonce Aleatorio: $#1
202
BLOQUE 1
Índice: 1
Marca de Tiempo: 17:17
1/1/20xx
Datos: " block1data"
0xf6e1da2...deb
Direccionamiento Previo:
0xea34ad...55
Nonce Aleatorio: @$%
204
BLOQUE 2
Índice: 2
Marca de Tiempo: 17:19
1/1/20xx
Datos: " block2data"
0x9327eb1b...36a21
Direccionamiento Previo:
0xf6e1da2...deb
Nonce Aleatorio: #!!
206

Figura 2

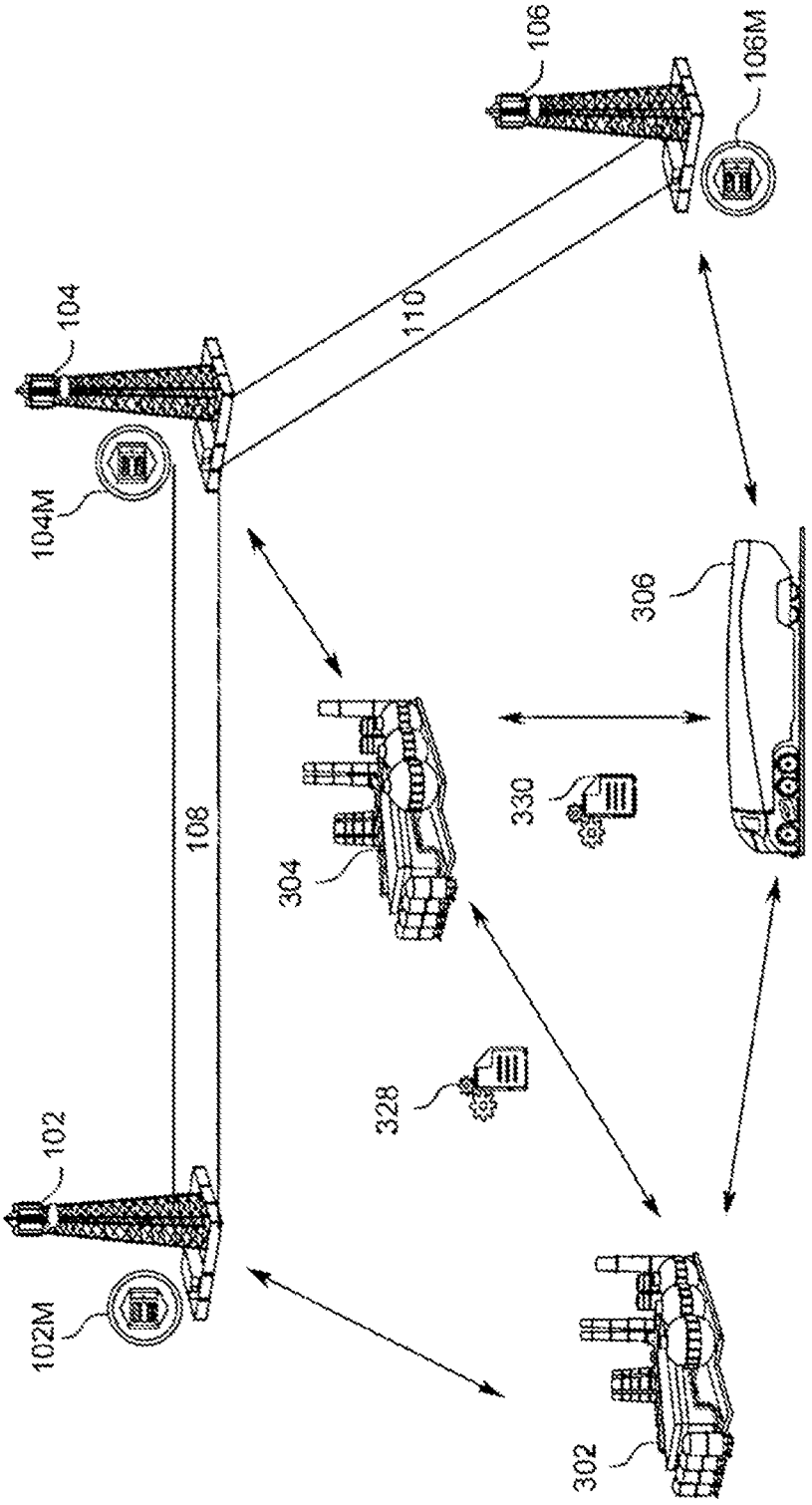

Figura 3

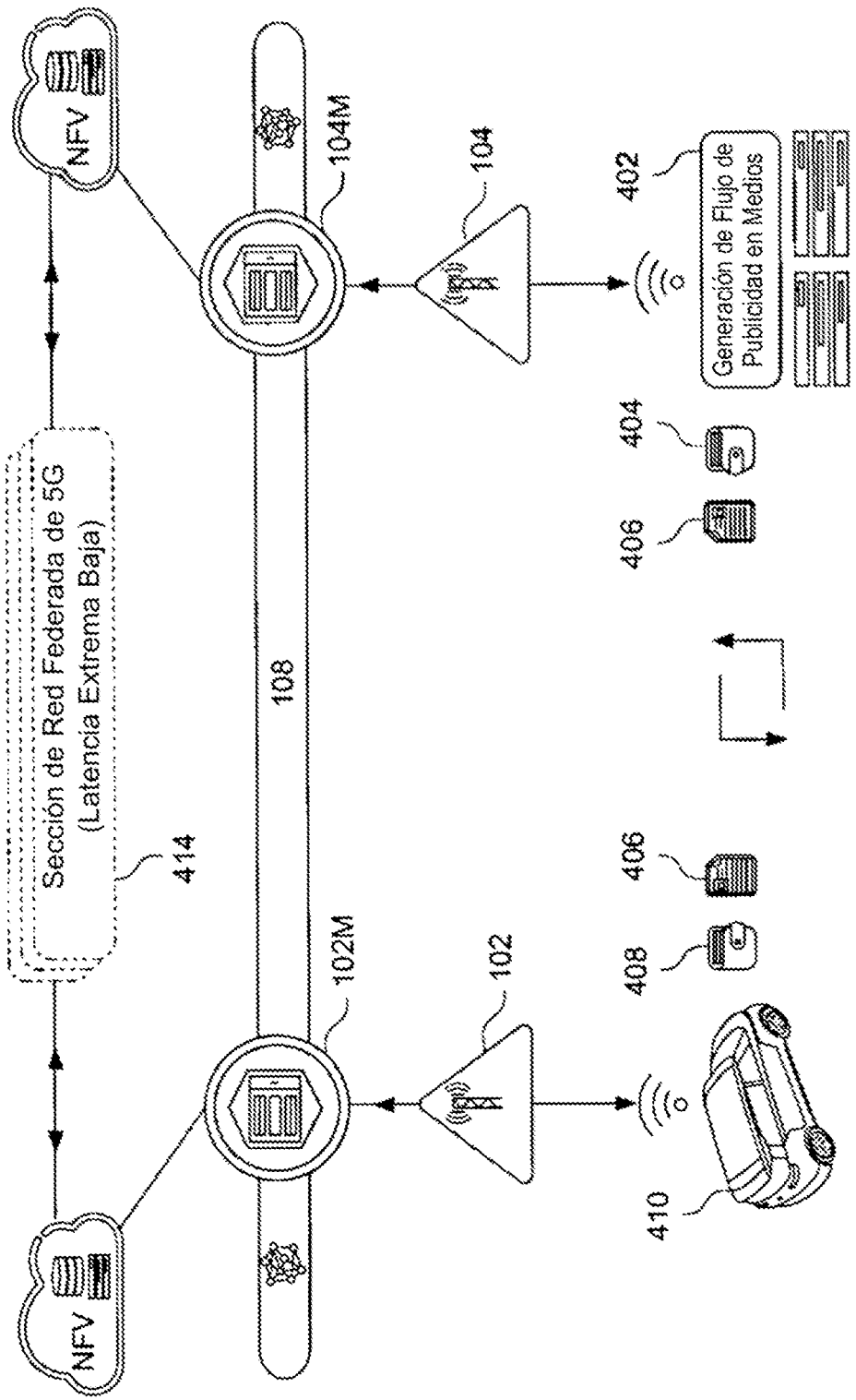
NFV
104M
104
402
Generación de Flujo de Publicidad en Medios
404
406
Sección de Red Federada de 5G
(Latencia Extrema Baja)
414
108
406
102M
102
408
NFV
410

Figura 4

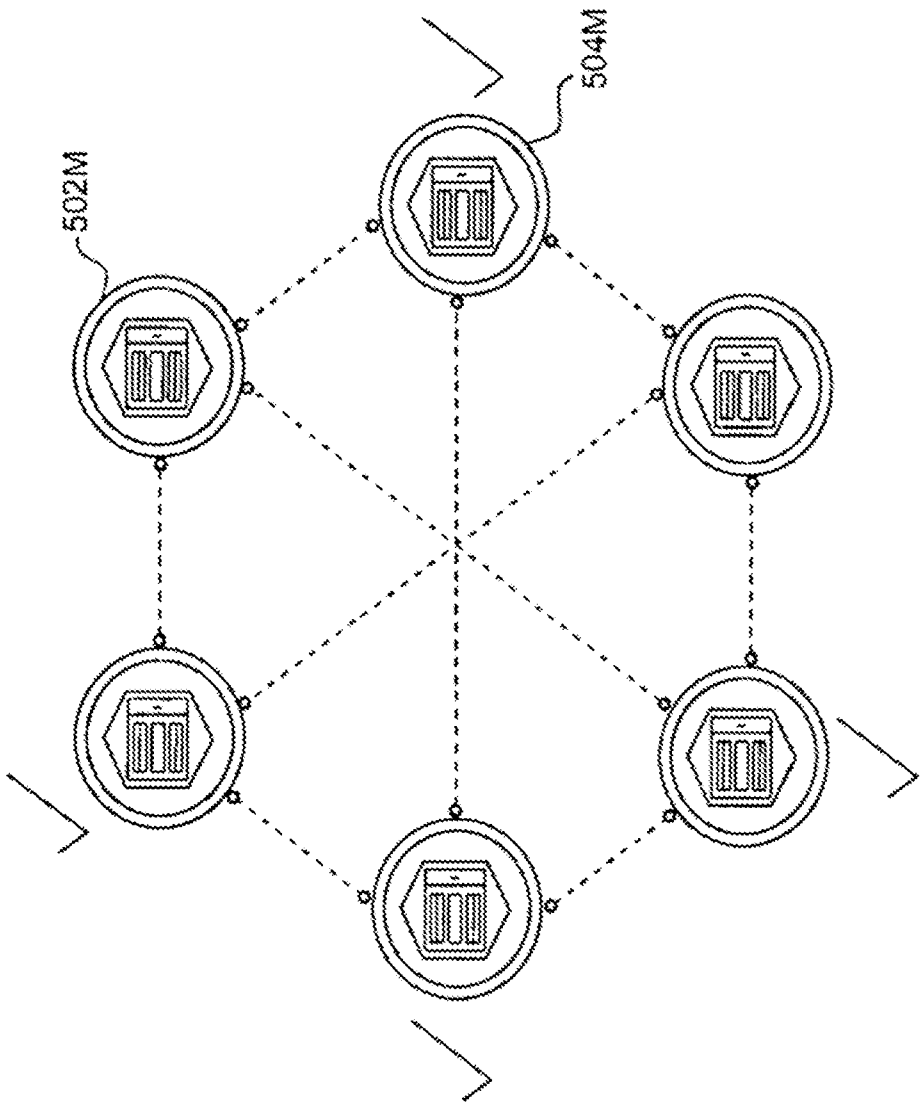

Figura 5

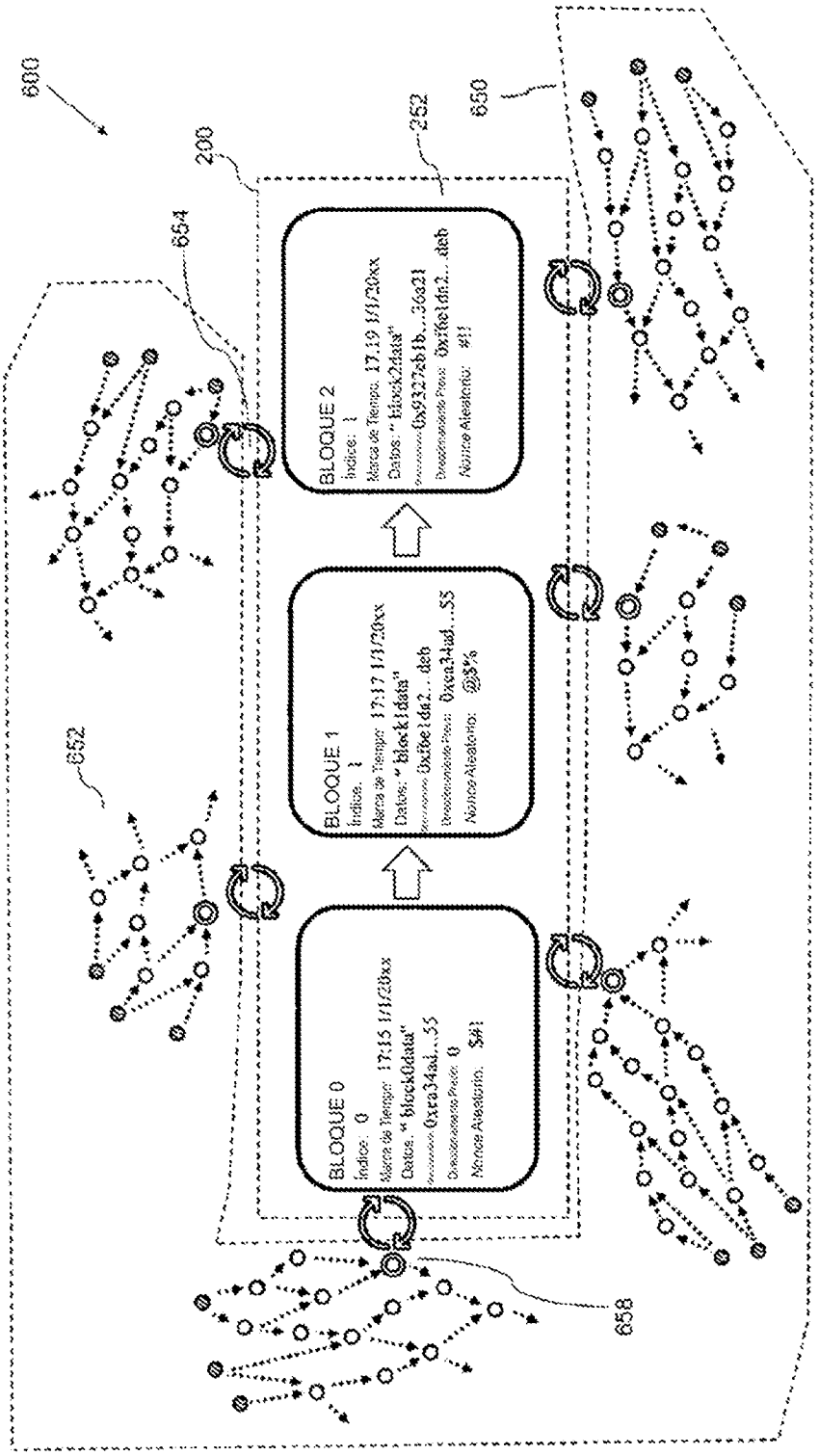
600
200
252
650
654
652
658
BLOQUE 0
Índice: 0
Marca de Tiempo: 17:15 1/1/20xx
Datos: " block0data"
Dirección Hash Previo: 0
Nonce Aleatorio: $#1
BLOQUE 1
Índice: 1
Marca de Tiempo: 17:17 1/1/20xx
Datos: " block1data"
Nonce Aleatorio: @8%
BLOQUE 2
Índice: 1
Marca de Tiempo: 17:19 1/1/20xx
Datos: " block2data"
Nonce Aleatorio: #1!

Figura 6

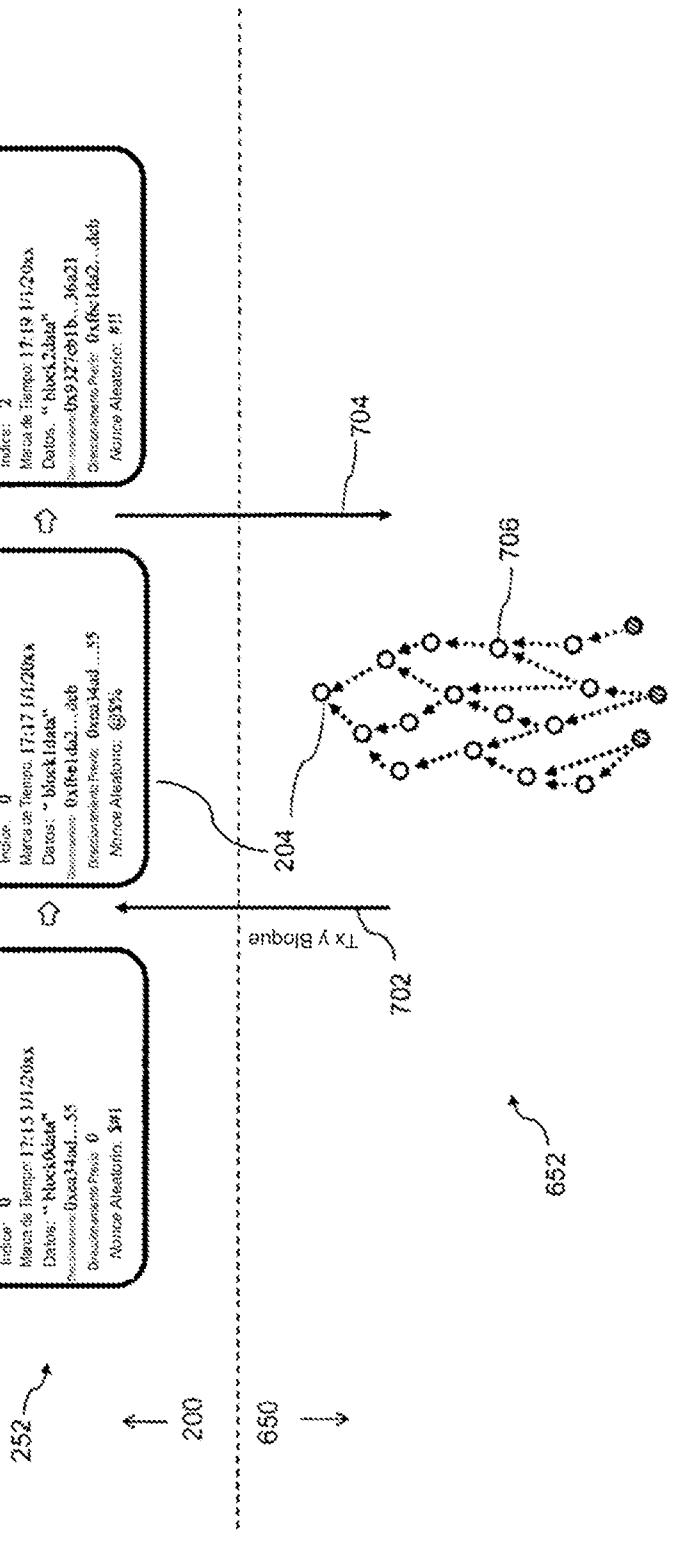
BLOQUE 0
Índice: 0
Marca de Tiempo: 12:15 1/1/20xx
Datos: "block0data"
Dirección Pedir: 0
Nonce Aleatorio: $#1
BLOQUE 1
Índice: 0
Marca de Tiempo: 17:17 1/1/20xx
Datos: "block1data"
Nonce Aleatorio: @$%
BLOQUE 2
Índice: 2
Marca de Tiempo: 17:19 1/1/20xx
Datos: "block2data"
Nonce Aleatorio: #!!
Tx y Bloque
252
200
650
652
702
704
706
204

Figura 7

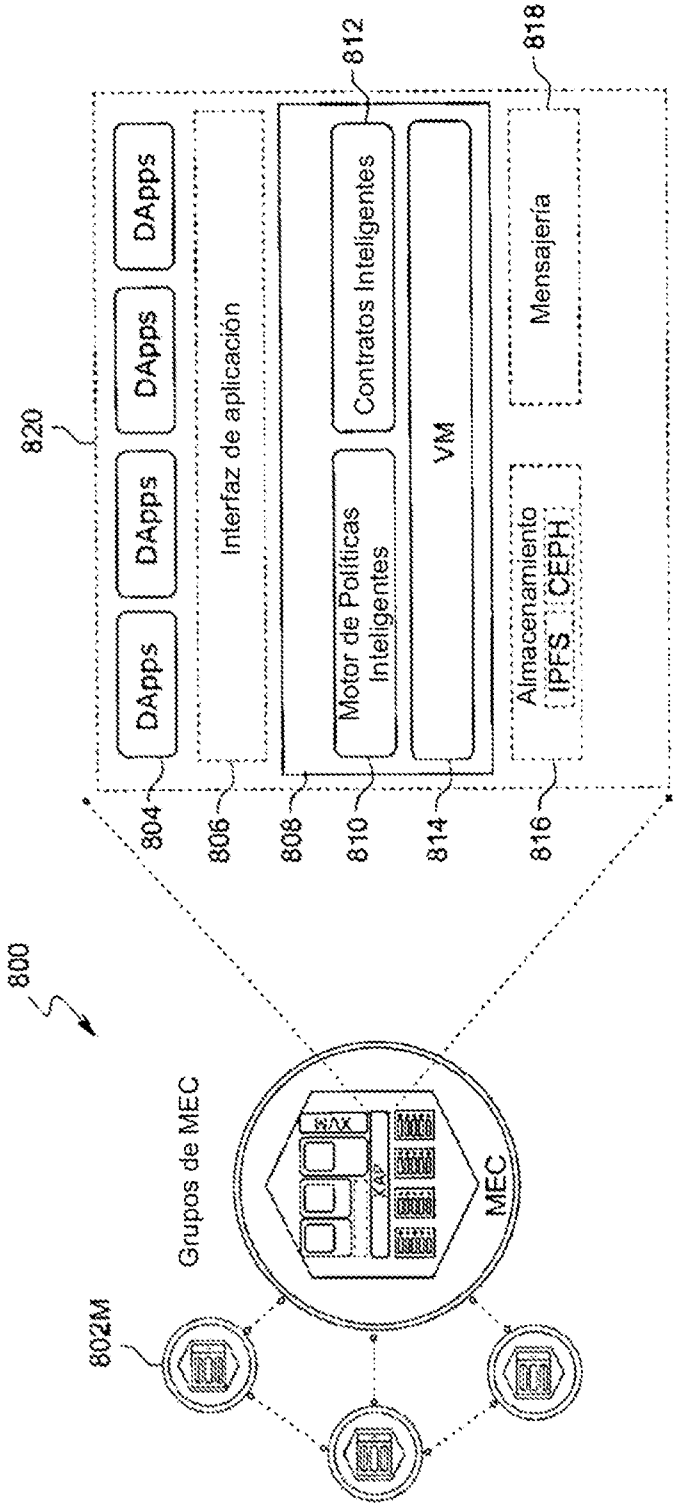
800
802M
Grupos de MEC
MEC
820
DApps
DApps
DApps
DApps
804
Interfaz de aplicación
806
808
Motor de Políticas Inteligentes
810
812
Contratos Inteligentes
VM
814
Almacenamiento
IPFS
CEPH
816
818
Mensajería

Figura 8

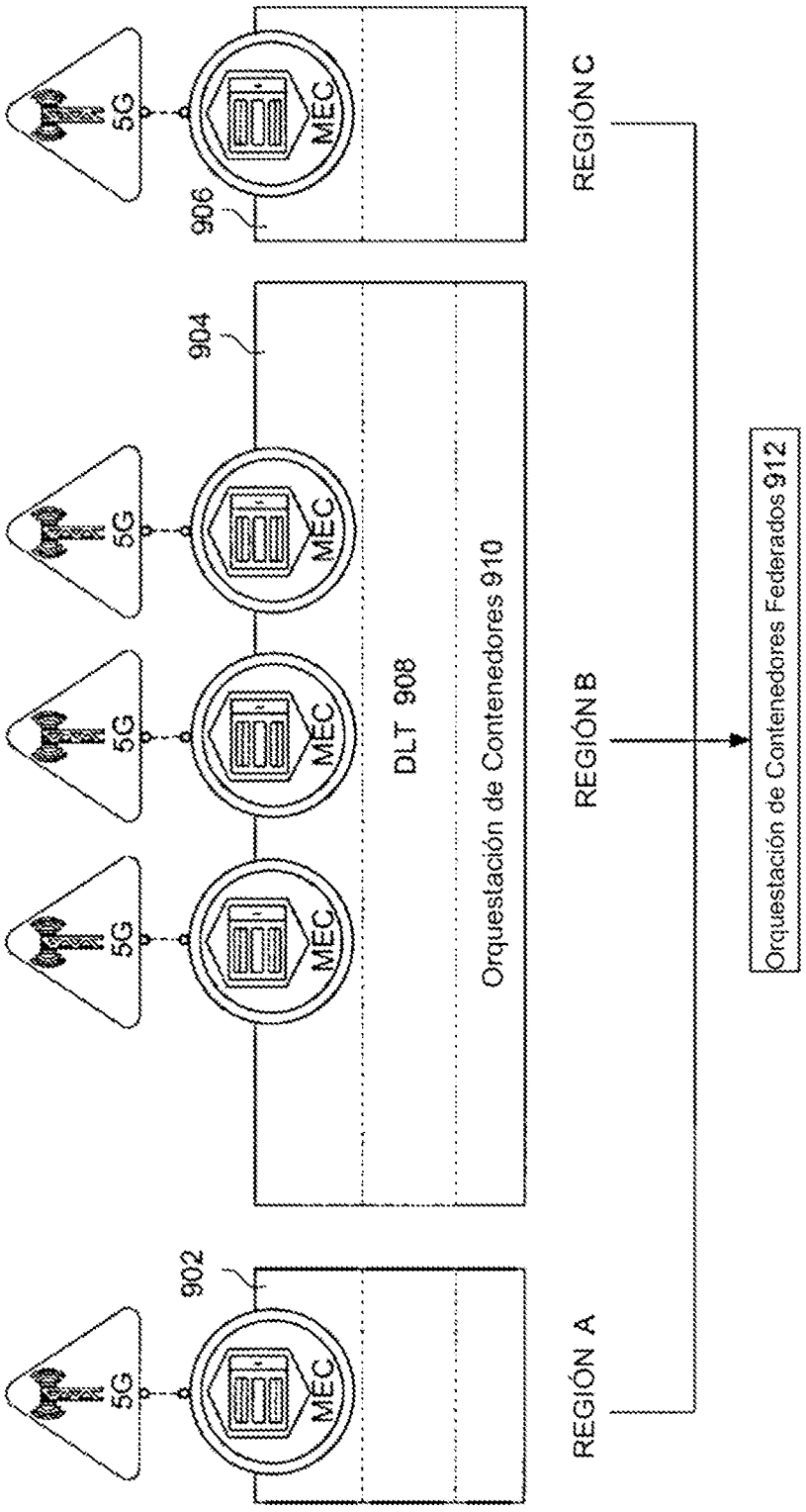
5G
MEC
902
904
906
DLT 908
Orquestación de Contenedores 910
REGIÓN A
REGIÓN B
REGIÓN C
Orquestación de Contenedores Federados 912

Figura 9

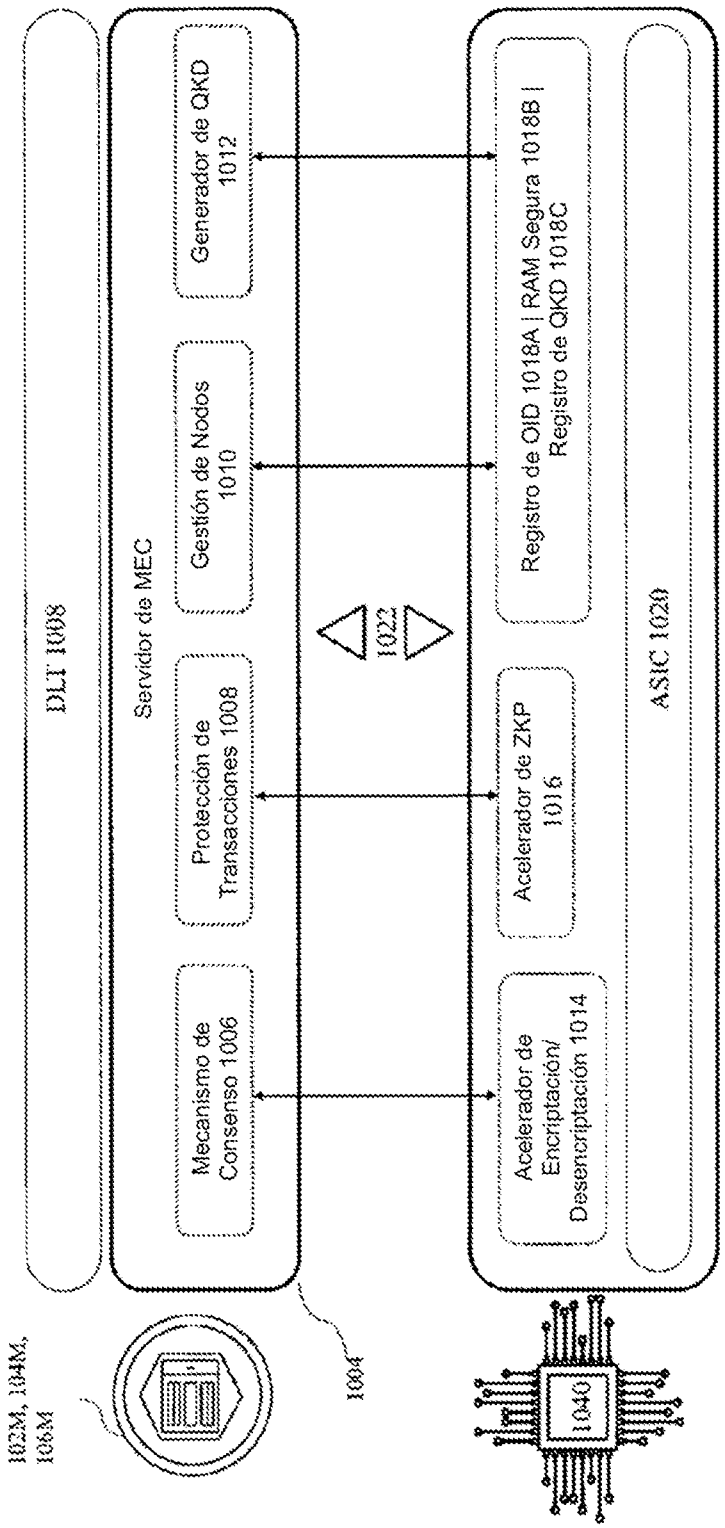
DLT 1008
Servidor de MEC
Generador de QKD 1012
Gestión de Nodos 1010
Protección de Transacciones 1008
Mecanismo de Consenso 1006
1022
Registro de OID 1018A | RAM Segura 1018B | Registro de QKD 1018C
Acelerador de ZKP 1016
Acelerador de Encriptación/ Desencriptación 1014
ASIC 1020
1040
1004
102M, 104M, 106M

Figura 10

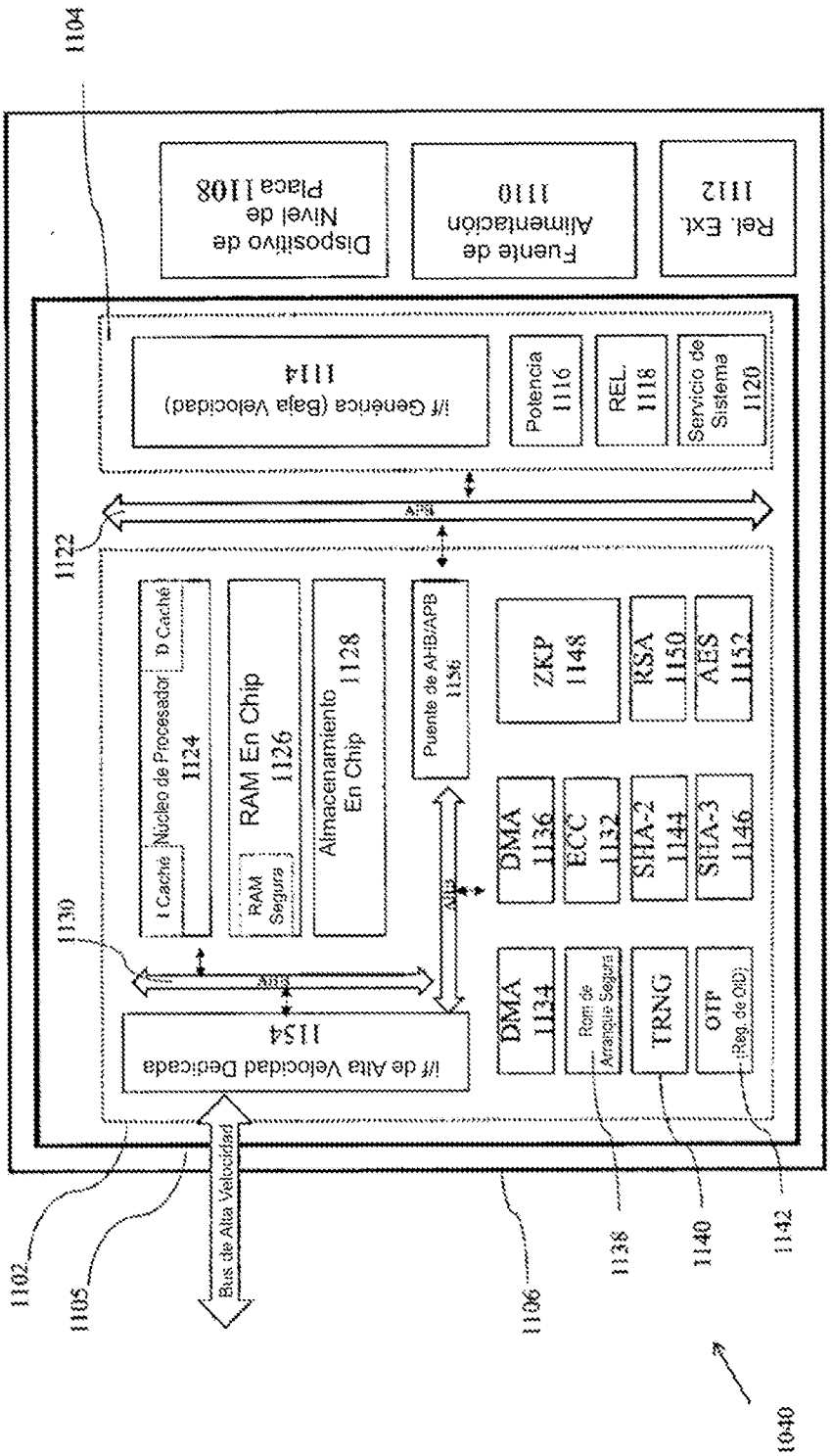
1104
Dispositivo de Nivel de Placa 1108
Fuente de Alimentación 1110
Rel. Ext. 1112
I/f Genérica (Baja Velocidad) 1114
Potencia 1116
REL 1118
Servicio de Sistema 1120
1122
AHB
I Caché
Núcleo de Procesador 1124
D Caché
RAM Segura
RAM En Chip 1126
Almacenamiento En Chip 1128
Puente de AHB/APB 1136
ZKP 1148
RSA 1150
AES 1152
DMA 1136
ECC 1132
SHA-2 1144
SHA-3 1146
1130
APB
DMA 1134
Rom de Arranque Segura
TRNG
OTP
(Reg. de OID)
I/f de Alta Velocidad Dedicada 1154
Bus de Alta Velocidad
1102
1105
1106
1138
1140
1142
1040

Figura 11

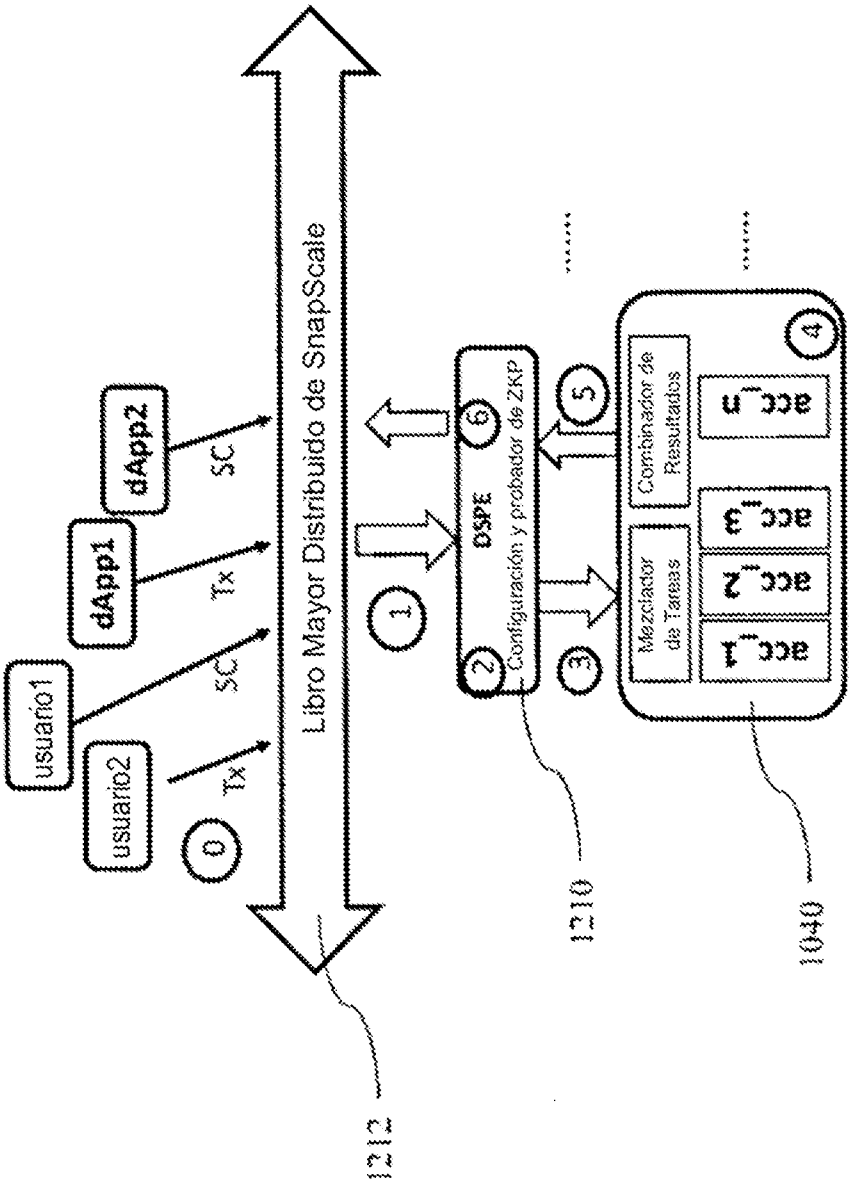
usuario1
usuario2
dApp1
dApp2
Tx
SC
Libro Mayor Distribuido de SnapScale
DSPE
Configuración y probador de ZKP
Mezclador de Tareas
Combinador de Resultados
acc_1
acc_2
acc_3
acc_n
1212
1210
1040

Figura 12

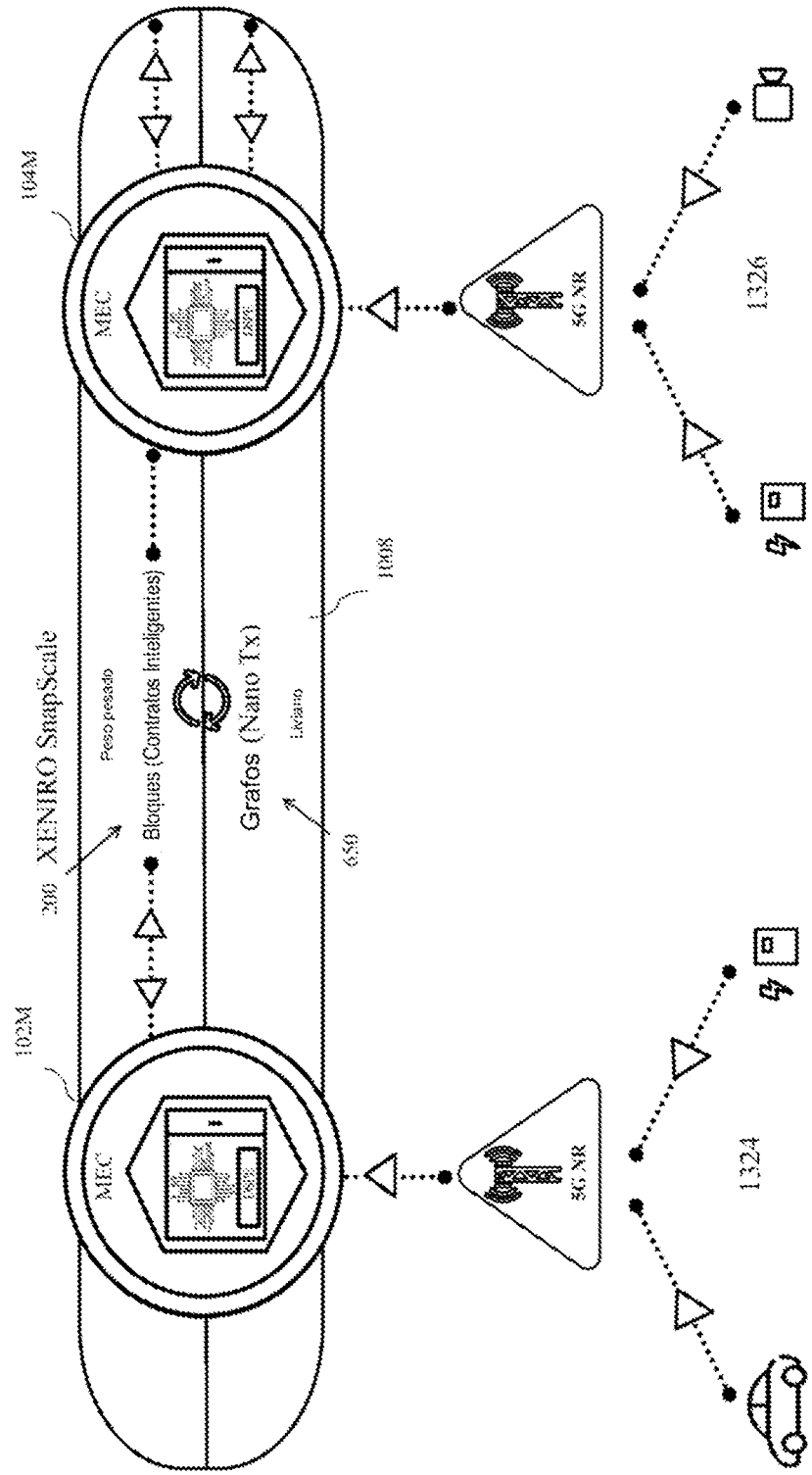
104M
MEC
5G NR
1326
1008
Grafos (Nano Tx)
Peso pesado
Ligero
650
206 XENIRO SnapScale
Bloques (Contratos Inteligentes)
102M
MEC
5G NR
1324

Figura 13

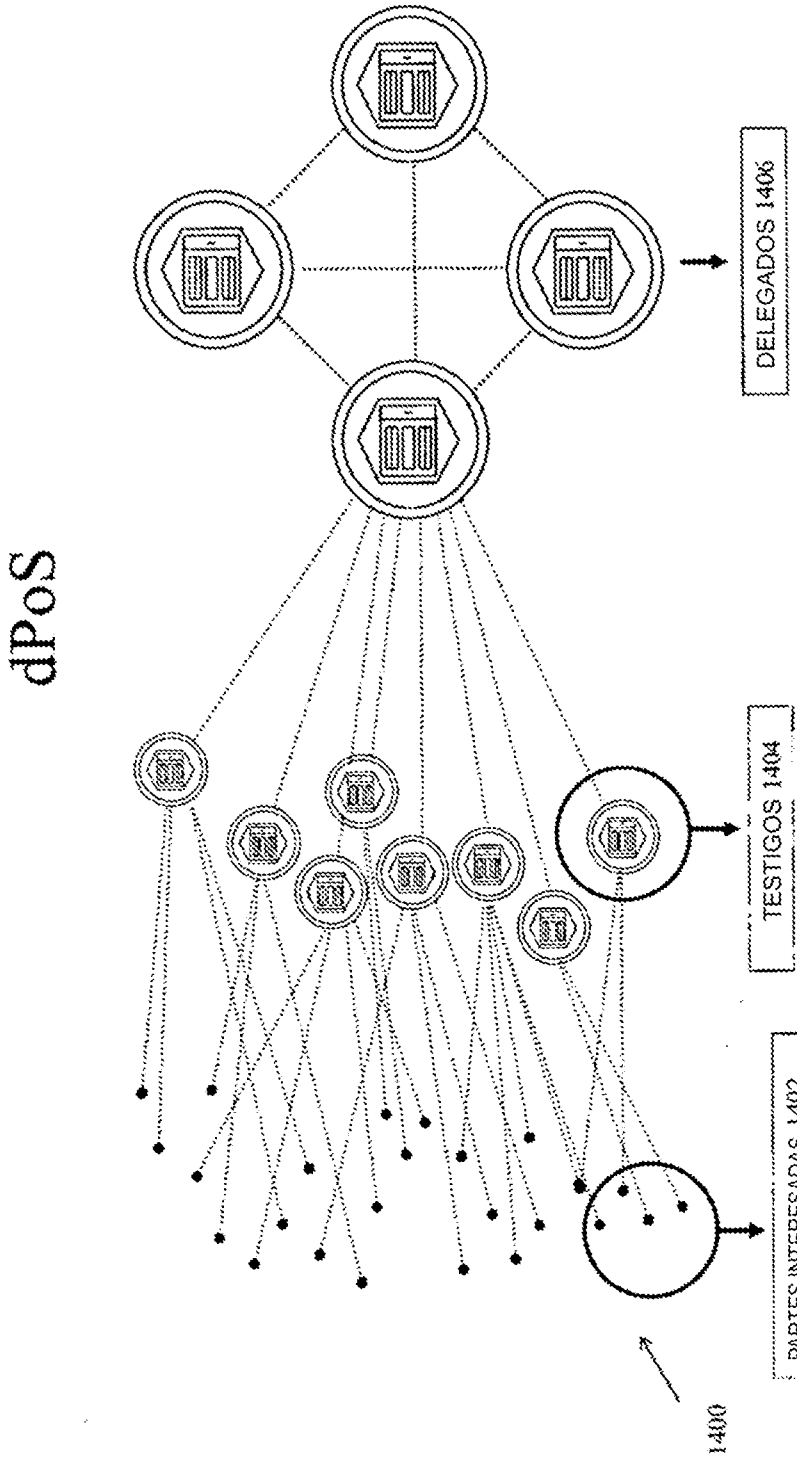
dPoS
DELEGADOS 1406
TESTIGOS 1404
PARTES INTERESADAS 1402
1400

Figura 14