(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 987 642**

(51) Int. Cl.:

G06Q 20/00 (2012.01)
G06F 21/64 (2013.01)
H04L 9/32 (2006.01)
H04L 9/00 (2012.01)
G06Q 20/02 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.11.2020 PCT/US2020/059473**

(87) Fecha y número de publicación internacional: **14.05.2021 WO21092434**

(96) Fecha de presentación y número de la solicitud europea: **06.11.2020 E 20885493 (5)**

(97) Fecha y número de publicación de la concesión europea: **14.02.2024 EP 4032052**

(54) Título: **Ejecución de transacciones usando cadenas de bloques privadas y públicas**

(30) Prioridad:

08.11.2019 US 201962933091 P
24.04.2020 US 202063015040 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.11.2024

(73) Titular/es:

ALGORAND LABS S.R.L. (100.0%)
Piazza di Monte Citorio 115
00186 Rome, IT

(72) Inventor/es:

GORBUNOV, SERGEY;
MICALI, SILVIO y
HERLIHY, MAURICE

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Ejecución de transacciones usando cadenas de bloques privadas y públicas

Campo técnico

La presente descripción se refiere en general a la ejecución de transacciones usando cadenas de bloques privadas y públicas.

Antecedentes

Los sistemas de cadena de bloques están ganando popularidad y adopción debido a las sólidas propiedades de seguridad, transparencia e integridad que proporcionan los mismos. Los sistemas de cadena de bloques suelen funcionar en un modelo público o sin permisos, en donde cualquier entidad puede unirse al consenso y participar en el mismo. Como resultado, las transacciones y los saldos son visibles para las entidades que entran en la red.

El documento CN107767267 divulga un método de transferencia de recursos virtuales, y el método se usa para un sistema de descentralización que comprende una cadena secundaria de cadena de bloques y una cadena principal.
El documento WO 2018/189658 divulga un método implementado por ordenador que incluye: i) unirse a un congreso transfiriendo, mediante un nodo que opera en una red de cadena de bloques de prueba de trabajo, uno o más activos digitales a una agrupación de congreso que tiene otros uno o más activos digitales asociados con otros miembros de un congreso; ii) detectar, por el nodo, una transacción especial de activos digitales en la red de cadena de bloques de prueba de trabajo a una dirección asociada con la agrupación de congreso, satisfaciendo la transacción especial unos criterios determinados; y iii) acuñar, por el nodo, uno o más activos digitales en una red de cadena de bloques de prueba de participación en respuesta a detectar la transacción especial.
El documento US 2016/330034 divulga métodos para transferir un activo desde una cadena progenitora a una cadena secundaria.

Sumario

Se divulgan aspectos de la invención en las reivindicaciones independientes. Entre otras cosas, se describe un método que posibilita que una o más entidades de un sistema de cadena de bloques lleven a cabo una serie de operaciones. El sistema de cadena de bloques incluye una cadena principal, una cadena conjunta, en donde la cadena conjunta tiene una cuenta correspondiente en la cadena principal, un activo propiedad de la cuenta correspondiente en la cadena principal y propiedad de una cuenta en la cadena conjunta, y una cuenta de cadena conjunta que posee el activo. Las operaciones incluyen publicar una transacción autenticada en la cadena conjunta, autorizando la transacción autenticada una transferencia del activo de la cuenta de cadena conjunta a una cuenta de la cadena principal, determinar que la transacción autenticada se publica en la cadena conjunta, y publicar, en la cadena principal, una transacción asignando el activo a la cuenta de la cadena principal.

Los beneficios y ventajas de las implementaciones incluyen la mejora de la seguridad, la escalabilidad y la descentralización de los protocolos de pago usando cadenas de bloques privadas con permisos en comparación con los métodos tradicionales. Un bloque de pago trans-cadena se produce en un tiempo más corto en comparación con otras técnicas y las transacciones del bloque se finalizan inmediatamente. Otros beneficios y ventajas son la mejora de la privacidad y la confidencialidad de los miembros de cada cadena de bloques privada. Cada cadena de bloques privada puede ajustarse a un régimen normativo para asegurar la honestidad de las transacciones. Las implementaciones divulgadas en el presente documento implementan mecanismos más rápidos, más seguros y más eficientes en comparación con los métodos tradicionales que usan mecanismos más lentos, *ad hoc* y más vulnerables.

Breve descripción de los dibujos

La figura 1 muestra un diagrama de bloques de ejemplo de una red de pagos que usa múltiples cadenas de bloques privadas con permisos.
La figura 2 muestra un caso de uso de ejemplo de una red de pagos que usa múltiples cadenas de bloques privadas con permisos, de acuerdo con una o más implementaciones.
La figura 3 muestra un proceso de ejemplo para usar cadenas conjuntas.
La figura 4 muestra un proceso de ejemplo para transferir un activo usando una cadena conjunta.
La figura 5 muestra una máquina de ejemplo para implementar una red de pagos que usa múltiples cadenas de bloques privadas con permisos, de acuerdo con una o más implementaciones.

Descripción detallada

Esta especificación describe técnicas para el uso de cadenas de bloques públicas y privadas y la interoperabilldad entre las mismas. Una cadena de bloques privada acoplada comunicativamente e interoperable con una cadena de bloques pública se denomina "cadena conjunta". Puede crearse una cadena conjunta que tenga acceso restringido a

un número limitado de entidades (una característica que a veces se denomina "con permisos") y que sea privada para aquellos a los que se les ha concedido acceso (por ejemplo, aquellos a los que no se les ha concedido acceso no pueden observar actividad en la cadena conjunta y/o realizar transacciones en la cadena conjunta). Por ejemplo, las cadenas conjuntas privadas pueden ser instanciadas por instituciones o individuos para preservar la privacidad de las transacciones y los saldos de los individuos. Además, las cadenas conjuntas pueden ampliarse para satisfacer la alta velocidad y los requisitos normativos de sus interesados. Una cadena conjunta de este tipo pueden usar el protocolo de consenso de Algorand para las transacciones. Por lo tanto, puede implementarse un homólogo privado de la cadena de bloques de Algorand pública.

Aunque la cadena conjunta privada cuenta con permisos, los validadores se usan para registrar transacciones de cadena conjunta privada con la cadena principal. Por ejemplo, una vez que se crea una transacción en la cadena conjunta privada, se transmite una solicitud de validación asociada con la transacción a los dispositivos de validador de la cadena conjunta privada. Los validadores generan un compromiso asociado con la transacción como validación de la misma. El compromiso puede usarse para verificar que una transacción que se produce en la cadena conjunta privada es válida (por ejemplo, para confirmar que una entidad que está intercambiando un activo de hecho posee ese activo). El compromiso puede ser de "conocimiento cero" y no necesita revelar ninguna información acerca de los bloques individuales o la transacción de criptoactivos en la cadena conjunta privada. Además, el compromiso puede añadirse tanto a la cadena conjunta privada como a la cadena principal.

Las cadenas conjuntas se usan para realizar transacciones de criptoactivos, tales como la transferencia de cantidades de criptodivisas, la ejecución de transferencias de criptoactivos o transacciones que usan testigos fungibles. Una institución puede emitir una transacción en la cadena de bloques pública que asigna activos particulares a la cadena conjunta privada. La correlación entre la cadena conjunta privada y su lista completa de activos se registrará y actualizará a través de la cadena de bloques pública. Los métodos descritos en el presente caso implementan mecanismos más rápidos, más seguros y más eficientes en comparación con los métodos tradicionales que usan mecanismos más lentos, *ad hoc* y más vulnerables.

Escenario de ejemplo usando cadenas de bloques privadas

Como un ejemplo de una cadena conjunta en uso, una cadena conjunta C se asocia con una cuenta A en la cadena principal. Para los fines de este ejemplo, una "cadena principal" es una cadena de bloques pública, y una "cadena conjunta" es una cadena de bloques privada, por ejemplo, una cadena de bloques cuyas transacciones solo son visibles para un conjunto particular de entidades y que solo acepta transacciones realizadas por ese conjunto particular de entidades. Una "cuenta", a veces denominada dirección, es un valor que posee criptoactivos mediante una asociación matemática entre el valor y los activos. A veces, una cuenta está representada por una clave pública, de tal modo que el propietario de la clave pública (por ejemplo, el propietario de la clave privada correspondiente) puede acceder a los activos que posee la cuenta. Dicho de otro modo, el propietario de la clave pública posee la cuenta correspondiente a la clave pública. Las entidades que poseen o son "dueñas" de las cuentas de una cadena de bloques, se denominan a veces miembros de la cadena de bloques.

La cadena principal incluye registros que indican que la cuenta A de la cadena principal posee un conjunto de activos. Esos activos son propiedad de una o más cuentas de la cadena conjunta C. Los miembros de la cadena principal no tienen acceso a información acerca de qué cuentas X de la cadena conjunta C poseen los activos particulares de la cuenta A. En algunos ejemplos, la cadena principal no necesita conservar la información de que la cuenta A se asocia con la cadena conjunta C específica. Esto, en esos ejemplos, los miembros de la cadena principal pueden no saber siquiera que la cuenta A corresponde a la cadena conjunta C.

Cuando una cuenta de cadena conjunta X desea transferir el activo B a una clave pública PK (por ejemplo, una clave pública de destino) en la cadena principal, la cuenta X autentica lo que pretende hacer, por ejemplo, calculando la firma digital SIGx(B,PK,MAIN) y publicando esta firma en un bloque de la cadena conjunta C como parte de una transacción T. Tal publicación tiene éxito debido a que es cierto de hecho que la cuenta X posee el activo B en la cadena conjunta C (por ejemplo, el bloque que contiene el no se añadirá a la cadena conjunta C a menos que la transacción T sea válida). Los validadores de la cadena conjunta C autentican a la cuenta A que, en la cadena principal, debería transferir el activo B a PK. Por ejemplo, pueden entregar a la cuenta A (por ejemplo, hacer que la cuenta A reciba) "SIGc(B,PK)". En el presente caso, "SIGc(B,PK)" se refiere a un conjunto de firmas digitales de los validadores de la cadena conjunta C que corresponden a la mayoría de la participación en la votación de los validadores de la cadena conjunta C. Por ejemplo, si cada validador de la cadena conjunta C tiene el mismo poder de voto que cualquier otro validador de la cadena conjunta C, y si hay 100 validadores en la cadena conjunta C, entonces SIGc(B,PK) corresponde a una firma digital de 80 validadores de (B,PK).

Como otro ejemplo, los validadores de la cadena conjunta C pueden usar un esquema de firma de umbral. En un esquema de este tipo, una clave (de verificación) pública PK puede no tener una clave (de firma) secreta SK que sea conocida por una única entidad. Más bien, cada validador i solo conoce una cuota SKi de SK. Usando SKi, el validador i puede calcular su propia "firma parcial" (B,PK). Sin embargo, dado un número suficiente de tales firmas parciales (por ejemplo, 66 de 100) puede calcularse la firma completa SIG(B,PK), que es una firma ordinaria en relación con PK y, por lo tanto, puede verificarse fácilmente conociendo solo PK. En este caso, puede establecerse SIGc(B, PK) =

SIG(B, PK). La ventaja de este enfoque es que (B, PK) se autentica mediante una única firma, en lugar de múltiples firmas, pero se garantiza que un número suficiente de verificadores debe haber colaborado en su cálculo y, por lo tanto, que un número suficiente de verificadores avala la transferencia del activo B a PK en la cadena principal.

En algunos ejemplos, la cuenta A correspondiente a la cadena conjunta C en la cadena principal, puede ser también una cuenta de la cadena conjunta C. Como otro ejemplo, la cuenta A está autorizada a supervisar la cadena conjunta C. En estos ejemplos, los validadores de la cadena conjunta C no necesitan enviar un SIGc(B,PK) por separado a la cuenta A. Por ejemplo, la cuenta A puede publicar en la cadena principal una transacción que asigna B a PK en el momento en que ve que una cuenta X de la cadena conjunta C publica una transacción adecuada que autoriza la transferencia del activo B a una clave PK en la cadena principal.

Para evitar que las cuentas A puedan asignar activos pertenecientes a las cuentas de la cadena conjunta C (a una o más claves públicas PK) sin la autorización de la cadena conjunta C, nos aseguramos de que la clave pública PKa de la cuenta A en la cadena principal (por ejemplo, la clave pública que la cuenta A usa para autorizar la transferencia del activo B a PK en la cadena principal) sea una clave pública de un esquema de firma de umbral y que la clave secreta correspondiente no sea conocida por la cuenta A (ni por ninguna otra entidad asociada con el sistema de cadena de bloques). Más bien, cada uno de los verificadores de la cadena conjunta C posee una cuota de SK y puede usarla para calcular la firma digital por la que la cuenta A autoriza la transferencia del activo B a PK en la cadena principal. Es decir, suponiendo que esta firma sea SIG(B,PK), entonces cada verificador produce su propia firma parcial y la firma completa es ensamblada a partir de tales firmas parciales por la cuenta A, o la firma completa se ensambla en primer lugar (por ejemplo, por cualquier entidad asociada con la cadena de bloques) y luego se pone a disposición de la cuenta A. De esta forma, solo los verificadores de c pueden calcular una firma que autorice la transferencia del activo B a PK en la cadena principal, y lo harán solo en respuesta a una publicación adecuada del activo B en la cadena conjunta C.

Las técnicas descritas en este ejemplo se describen más adelante con respecto a la figura 4.

Implementaciones de ejemplo de cadenas conjuntas

La figura 1 muestra un diagrama de bloques de ejemplo de una red de pagos que usa múltiples cadenas conjuntas 120, 140. La red de pagos incluye las cadenas conjuntas 120, 140, una cadena de bloques pública 104 y una red 116. La red 116 puede incluir porciones de Internet o una red local. En otras implementaciones, la red de pagos puede incluir componentes adicionales o menos componentes, y los componentes pueden conectarse de una forma diferente.

Las cadenas conjuntas 120, 140 pueden usarse para realizar transacciones de criptoactivos, tales como la transferencia de cantidades de criptodivisas, la ejecución de transferencias de criptoactivos o transacciones que usan testigos fungibles. Una institución o administrador (por ejemplo, de la cadena de bloques pública 104) y el cadena conjunta 120 acuerdan un conjunto de activos que pertenecen a la cadena conjunta 120. Por ejemplo, la institución puede emitir una transacción en la cadena de bloques pública 104 que asigna activos particular a la cadena conjunta 120. La correlación entre la cadena conjunta 120 y su lista completa de activos se registrará y actualizará a través de la cadena de bloques pública 104. Por ejemplo, los activos pertenecientes a las cuentas de la cadena conjunta 120 pueden ser asignados a una cuenta particular en la cadena de bloques pública 104, de tal modo que, desde la perspectiva de los miembros de la cadena de bloques pública 104, la cuenta posee todos los activos pertenecientes a las cuentas de la cadena conjunta 120.

Una transacción de criptoactivos transfiere una cantidad particular de un criptoactivo de una cuenta de criptoactivos a otra. Un criptoactivo puede referirse a una criptodivisa, por ejemplo, Algo, que se diseña para funcionar como un medio de intercambio que usa criptografía para asegurar transacciones financieras, controlar la creación de unidades adicionales, o verificar la transferencia de criptoactivos. Un criptoactivo también puede referirse a un registro seguro de un activo, tal como la titularidad de un automóvil o una hipoteca que se gestiona mediante una cadena de bloques.

Una cuenta de criptoactivos posibilita que la entidad que la posee almacene criptoactivos y/o gestione saldos de criptodivisas. Cada cuenta de criptoactivos tiene un identificador de cuenta, que es un identificador singular. La cuenta de criptoactivos muestra el saldo actual del criptoactivo y presenta las transacciones de la entidad. Una entidad puede enviar una solicitud a otra parte que tenga otra cuenta de criptoactivos para una cantidad específica de criptoactivos.

Las implementaciones en el presente documento se refieren a métodos y mecanismos para transferir un criptoactivo desde una cadena de bloques privada (por ejemplo, la cadena conjunta 120) a una cadena de bloques pública 104. Las implementaciones divulgadas en el presente documento implementan mecanismos más rápidos, más seguros y más eficientes en comparación con los métodos tradicionales que usan mecanismos más lentos, *ad hoc* y más vulnerables. Las implementaciones pueden usarse para implementar un sistema de control y transferencia de activos, por ejemplo, para la financiación relacionada con titularidades de automóviles o hipotecas relacionadas con bienes inmuebles. Las transacciones criptográficas multicadena pueden abordar muchos escenarios y reducir la necesidad de contratos inteligentes más complejos y computacionalmente costosos. Puede implementarse un intercambio de activos en donde una transacción incluye el intercambio de alguna cantidad de un activo por otra. Puede implementarse un intercambio de testigos no fungibles (NFT) en donde se intercambia un NFT por alguna cantidad de

un testigo fungible (por ejemplo, Algo).

Puede crearse una cadena conjunta (por ejemplo, las cadenas conjuntas 120, 140) que tiene acceso restringido (con permisos) y es privada. En algunos ejemplos, una cadena conjunta usa el protocolo de consenso de Algorand. Aunque la cadena conjunta cuenta con permisos, las implementaciones divulgadas en el presente documento buscan usar tantos validadores 152 como estén disponibles, para mejorar la seguridad. Por lo tanto, puede crearse una versión privada de la cadena de bloques pública de Algorand 104 que puede realizar permutas atómicas en la capa 1. La Capa 1 se refiere a la arquitectura de la cadena de bloques principal subyacente. Usando esta arquitectura, una cadena conjunta puede comunicarse fácilmente con una cadena de bloques pública (por ejemplo, la cadena de bloques pública 104) y sirve de puente a la cadena de bloques pública. De este modo, los activos pueden transferirse a la cadena de bloques pública. Por ejemplo, una entidad puede querer vender un activo. Si la entidad subasta el activo, la subasta puede realizarse en la cadena de bloques pública con más postores de los que habría en una cadena conjunta.

En algunas implementaciones, un activo se transfiere desde una cuenta de una entidad en la cadena conjunta 120 a una clave pública 144 de la entidad en la cadena de bloques pública 104. Debido a que la cadena de bloques pública 104 no cuenta con permisos, la cadena de bloques pública 104 acepta la clave pública 144, por ejemplo, cuando se genera la clave pública 144. La cadena de bloques pública 104 registra que una clave pública 144 ha obtenido el activo. Por ejemplo, un conjunto de activos puede transferirse desde la cadena conjunta 120 a la cadena de bloques pública 104 usando un único bloque 124 de la cadena conjunta. Antes de la transferencia, el bloque 124 se estructura usando troceos. La entidad que transfiere firma un troceo del bloque 124.

En algunas implementaciones, una transferencia de la cadena conjunta 120 a la cadena de bloques pública 104 se somete a troceo. Una transferencia de la cadena conjunta 120 a la cadena conjunta 120 también se somete a troceo. Ambos troceos aparecen en el bloque 124. Ambos troceos se certifican para revelar la transferencia de la cadena conjunta 120 a la cadena de bloques pública 104 sin revelar la transferencia de la cadena conjunta 120 a la cadena conjunta 120. Se realiza una comprobación para determinar si someter a troceo las transferencias da la cantidad del activo que es parte del bloque 124.

Se informará a una primera entidad que tenga acceso a la cadena de bloques pública 104 acerca de la transferencia de la cadena conjunta 120 a la cadena de bloques pública 104. Cuando una segunda entidad afirma que es un validador 152 de la cadena conjunta 120, la primera entidad determina si el certificado es firmado de hecho por la segunda entidad usando técnicas de comparación. Los validadores 152 pueden ser ponderados, por ejemplo, a un validador de confianza se le asigna un peso más alto. Si la suma de pesos es suficiente, la primera entidad determina que el bloque 124 es válido. La clave del transferente de activos y la clave de beneficiario 144 se registran en el bloque 148.

Un método adicional para realizar una transferencia de activos es transferir el activo a una clave (por ejemplo, la clave 144) en la cadena de bloques pública 104. La primera entidad hace entonces un registro indicando que la clave 144 en la cadena de bloques pública 104 y el activo están unidos. La cadena de bloques pública 104 conoce las identidades de los validadores 152. Cada vez que se cambia un validador 152 (por ejemplo, se añade o se resta un peso, o se vuelve a ponderar el validador 152), un *quorum* del conjunto previo de validadores 152 especifica o firma el conjunto de nuevos validadores 152. En algunas implementaciones, la cadena de bloques pública 104 está configurada para tolerar un pequeño cambio en la información del validador. Una parte de los bloques 124, 148 puede reservarse para incluir nuevos validadores 152. Por ejemplo, cuando el bloque 124 incluye una transferencia de criptoactivos desde la cadena conjunta 120 a la cadena conjunta 140, el bloque 124 incluye un campo para un cambio de validador. Un primer nodo de la cadena de bloques pública 104 se habilita para observar las funciones de la cadena conjunta 120. Por lo tanto, el primer nodo está al tanto de las transferencias en la cadena conjunta 120. Un segundo nodo de la cadena de bloques pública 104 se habilita para observar las funciones de la cadena conjunta 140.

En algunas implementaciones, se usa un portavoz 156 para facilitar las transferencias. Por ejemplo, 100 validadores pueden estar presentes en el sistema cadena de bloques ilustrado en la figura 1. Una transacción necesitaría al menos 60 validadores para firmar el bloque 148. En tales implementaciones, puede usarse un portavoz 156. Una única firma del portavoz 156 sería suficiente para la validación. Sin embargo, el portavoz 156 podría representar un único punto de fallo. Por ejemplo, si el portavoz 156 firma la información de las transferencias en la cadena conjunta 120 y el portavoz 156 es malicioso o está comprometido, habrá 20 bloques que objetar. Los validadores 152 pueden bloquear la validación y la transferencia queda sin ningún valor y efecto. Puede(n) usarse un único portavoz o más portavoces. Solo los validadores 152 se habilitan para informar a la cadena de bloques pública 104 que el portavoz 156 ha cambiado.

En algunas implementaciones la entidad gestora de la cadena de bloques pública 104 no está representada por una clave *ad hoc* 144, sino por una entidad conocida contra la que se tiene derecho a recurrir, por ejemplo, un derecho de auditoría o de sanción. Puede añadirse un campo de nota adicional al bloque 148 que contiene instrucciones para el procesamiento posterior del activo, por ejemplo, llevar a cabo una subasta. El campo de nota puede cifrarse. El campo de nota puede indicar una transferencia a un gestor de la cadena conjunta 120 o a otra clave. El campo de nota puede indicar una instrucción para desechar los activos. En algunas implementaciones, el tiempo de curación es cero, es

decir, el portavoz 156 es de confianza. Por lo tanto, se usan cadenas de bloques tanto sin permisos como con permisos.

En algunas implementaciones, los validadores 152 asociados con una cadena conjunta 120 reciben una solicitud de validación asociada con una transacción de criptoactivos. La solicitud de validación pide a cada validador 152 que valide la transacción de criptoactivos. Se identifica al menos un portavoz 156 para certificar datos en nombre de los validadores 152. El portavoz 156 publica los datos en la cadena de bloques pública 104 que se acopla de forma comunicable a la cadena conjunta 120. Los validadores 152 determinan si los datos son válidos. En respuesta a la determinación, los validadores 152 publican una impugnación a los datos en la cadena de bloques pública 104. En algunas implementaciones, la impugnación se publica en la cadena de bloques pública 104 antes de que se haya añadido un número umbral de nuevos bloques (por ejemplo, 20 bloques) a la cadena de bloques pública 104. En algunas implementaciones, los datos se asocian con un compromiso 128.

A cada validador 152 se le puede asignar un peso que indica el grado de confianza del validador 152. La determinación de que los datos son válidos se realiza en respuesta a una suma de pesos de los validadores 152 que supera un peso umbral. En algunas implementaciones, la cadena de bloques pública 104 recibe un mensaje que indica la identidad de cada validador, el peso asignado a cada validador y la determinación de que la suma de pesos de los validadores 152 supera el peso umbral. La cadena de bloques pública 104 registra una primera clave 144 de un transferente de criptoactivos de la transacción de criptoactivos y una segunda clave de un beneficiario de criptoactivos de la transacción de criptoactivos en un nuevo bloque 148 de la cadena de bloques pública 104.

En algunas implementaciones, la cadena de bloques pública 104 recibe un mensaje que indica una transferencia deseada del criptoactivo al receptor de la misma. La cadena de bloques pública 104 registra una transferencia del criptoactivo al beneficiario del criptoactivo. En algunas implementaciones, un tiempo de curación asociado con la transacción de criptoactivos es menor que un tiempo umbral para curar que indica que el al menos un portavoz 156 es de confianza. La transacción de criptoactivos puede transferir un criptoactivo de la cadena conjunta 120 a la cadena de bloques pública 104. La transacción de criptoactivos puede transferir un criptoactivo desde la cadena de bloques pública 104 a la cadena conjunta 120. La transacción de criptoactivos puede transferir un criptoactivo de la cadena conjunta 120 a una segunda cadena conjunta 140. La transacción de criptoactivos es facilitada por la cadena de bloques pública 104. Se usa una arquitectura de paso de mensajes, de tal modo que las cadenas conjuntas privadas 120, 140 pueden estar aún más descentralizadas que la cadena de bloques pública 104.

La cadena conjunta 120 puede ser propiedad de o estar administrada por un gran banco o un estado nacional. La cadena conjunta 120 puede usar la cadena de bloques pública 104 como mecanismo de seguridad para sí misma. Por ejemplo, los participantes de la cadena conjunta 120 pueden depositar un alto nivel de confianza en la cadena de bloques pública 104. Por lo tanto, la cadena conjunta 120 puede realizar un troceo de todo el bloque 124 y ponerlo en la cadena de bloques pública 104. Si cada 100 bloques se realiza un troceo de un bloque en la cadena conjunta 120, el cálculo puede reiniciarse desde ese bloque. En este caso, no solo las transacciones se someten a troceo, sino todo el saldo de cada entidad que posee un activo en un punto dado.

En algunas implementaciones, cuando una cadena conjunta 120 crea un nuevo activo, la cadena conjunta 120 puede crear el activo en la cadena de bloques pública 104 y entonces transferirlo de nuevo a la cadena conjunta 120. Esto se hace debido a que cuando un participante de la cadena conjunta 120 desea más tarde vender el activo, la cadena de bloques pública 104 tiene un registro de propiedad del activo en la cadena conjunta 120. Si la cadena conjunta 120 está comprometida, un activo creado en la cadena de bloques pública 104 es más difícil de vender doblemente (doble gasto) en la cadena conjunta 120 que si el activo se hubiera creado en primer lugar en la cadena conjunta 120. Por ejemplo, la cadena de bloques pública 104 puede realizar ciertas comprobaciones. La cadena de bloques pública 104 puede comprobar el portavoz 156 y también comprobar que el activo sigue siendo propiedad de la cadena conjunta 120.

Transferencia de criptoactivos entre dos cadenas conjuntas privadas facilitada por una cadena de bloques pública

En algunas implementaciones, un dispositivo de usuario instancia una transacción de criptoactivos en una primera cadena de bloques privada 120 para transferir una primera cantidad de un primer criptoactivo desde una primera cuenta de criptoactivos 124 a una segunda cuenta de criptoactivos 136 asociada con una segunda cadena de bloques privada 140. El dispositivo de usuario puede ser un teléfono móvil, ordenador o tableta implementado como se ilustra y se describe con más detalle con referencia a la figura 5. Los dispositivos de validador 152 validan la primera transacción de criptoactivos para generar un primer compromiso 128 asociado con una primera clave de un solo uso 144. Un primer dispositivo informático asociado con la primera cadena de bloques privada 120 publica el primer compromiso 128 en la cadena de bloques pública 104. El primer dispositivo informático puede ser un ordenador de escritorio, un portátil o un servidor implementado como se ilustra y se describe con más detalle en referencia a la figura 5. Un segundo dispositivo informático asociado con la cadena de bloques pública 104 asigna la primera cantidad del primer criptoactivo a la primera clave de un solo uso 144 en la cadena de bloques pública 104. El segundo dispositivo informático puede ser un ordenador de escritorio, un portátil o un servidor implementado como se ilustra y se describe con más detalle en referencia a la figura 5. El segundo dispositivo informático realiza una permuta atómica entre la primera cantidad del primer criptoactivo y una segunda cantidad de un segundo criptoactivo. La segunda cantidad del

segundo criptoactivo se asigna a una segunda clave de un solo uso asociada con un segundo compromiso 132. El segundo compromiso 132 debe transferir la segunda cantidad del segundo criptoactivo desde la segunda cuenta de criptoactivos 136 a la primera cuenta de criptoactivos 124.

En algunas implementaciones, se asigna al primer criptoactivo una clave distinta a la de un solo uso. Por ejemplo, la clave podría ser una clave usada por la primera cadena de bloques privada 120 para todas las transferencias de criptoactivos a la cadena de bloques pública 104.

En algunas implementaciones, un primer dispositivo de usuario asociado con una primera cuenta de criptoactivos 124 en la cadena conjunta 120 con permisos instala una transacción de criptoactivos. Un primer dispositivo informático (tal como un dispositivo de administrador) asociado con la cadena conjunta 120 genera una clave privada usando criptografía de curva elíptica. La clave privada es para firmar la transacción de criptoactivos por el primer dispositivo de usuario. La transacción de criptoactivos consiste en transferir una primera cantidad de un primer criptoactivo desde la primera cuenta de criptoactivos 124 (en la cadena conjunta 120) a una segunda cuenta de criptoactivos 136 (en la cadena conjunta 140). El primer criptoactivo puede incluir titularidades de automóviles, hipotecas, bonos o acciones, etc. Las transferencias entre la cadena de bloques pública 104 y la cadena conjunta 120 se realizan (a) retirando el primer criptoactivo de la cadena conjunta 120 y posteriormente (b) depositándolo en la cadena de bloques pública 104. La segunda cuenta de criptoactivos 136 se asocia con la cadena conjunta 140. La transacción es privada para la cadena conjunta 120. Una transacción de este tipo y el bloque 124 de la cadena conjunta 120 no se propagan a la cadena de bloques pública 104 a menos que sea publicada por un administrador de la cadena conjunta 120.

En algunas implementaciones, el primer dispositivo de usuario genera una primera clave de una sola vez 144 que anonimiza una identidad de la primera cuenta de criptoactivos 124. En otras implementaciones, un dispositivo de usuario puede transferir un criptoactivo a una clave de larga duración con menos dependencia del anonimato. Un conjunto de dispositivos de validador 152 de la cadena conjunta 120 recibe una solicitud de validación asociada con la transacción de criptoactivos. Los dispositivos de validador 152 se asocian con la cadena conjunta 120. El primer dispositivo informático (de la cadena conjunta 120) puede registrar los dispositivos de validador 152 en la cadena de bloques pública 104. Cada dispositivo de validador tiene una clave pública diferente para validar transacciones de criptoactivos. Por lo tanto, una cadena conjunta 120, 140 registra un conjunto de claves públicas de validadores en la cadena de bloques pública 104. Los administradores de la cadena conjunta privada pueden emitir una transacción "crear cadena privada" que incluye un conjunto de validadores 152 que deben firmar cada bloque 124.

En algunas implementaciones, la solicitud de validación pide a cada validador 152 que valide la transacción de criptoactivos. La cadena de bloques pública 104 rastrea un conjunto de claves públicas autorizadas para ser validadores 152 para cada cadena conjunta 120, 140. Los validadores 152 validan la transacción de criptoactivos para generar un compromiso 128 asociado con la primera clave de un solo uso 144. Los validadores 152 pueden ser teléfonos móviles, ordenadores o tabletas, etc. De esta forma, cada cadena conjunta 120 puede realizar un consenso independiente en cada bloque 124 de transacciones. El primer dispositivo informático asociado con la cadena conjunta 120 publica el compromiso 128 en la cadena de bloques pública 104. De esta forma, la cadena conjunta 120 puede cumplir con las obligaciones normativas. Para publicar el compromiso 128 en la cadena de bloques pública 104, el primer dispositivo informático cifra información auxiliar asociada con la transacción de criptoactivos usando un cifrado basado en atributos. Por ejemplo, cada entrada en una tabla de saldo se denota por Ei. Los validadores de cadena conjunta privada 152 producen un compromiso: Ronda_R_Compromiso_Cadena_1 en la colección de entradas E1, ... , EN. Al final de la ronda, los validadores de cadena conjunta 152 producen un certificado Ronda_R_Cert_Cadena_1 que autoriza el compromiso Ronda_R_Compromiso_Cadena_1.

Pueden crearse transacciones de autovalidación en diferentes implementaciones. En algunas implementaciones, los compromisos 128 con los registros se instancian al mismo tiempo que se realizan transacciones de autovalidación. Por ejemplo, los validadores de cadena conjunta privada 152 pueden producir dos compromisos. Un compromiso corresponde a solicitudes de retirada, y el segundo compromiso corresponde a otros saldos dentro de la cadena conjunta 120. En otras implementaciones, los validadores 152 pueden revelar cada solicitud de retirada, sin necesidad de generar pruebas adicionales. En otras implementaciones, una transacción de autovalidación incluye una transacción que se publica en un área no privada de un bloque 124. Una transacción de este tipo puede ser parte de un encabezamiento de bloque que puede incluir un troceo de un bloque previo, un número de bloque, un conjunto de transacciones no privadas y un compromiso 128 con un conjunto de transacciones privadas. Por lo tanto, un encabezamiento de bloque certificado de una cadena conjunta 120 posibilita que se validen transacciones que transfieren activos de una cadena conjunta 120 a una cadena 140 con permisos.

En algunas implementaciones, el primer dispositivo de usuario (asociado con la primera cuenta de criptoactivos 124 de la cadena conjunta 120) autentica una prueba 112 de la transacción de criptoactivos. La prueba 112 se asocia con el compromiso 128. El primer dispositivo de usuario publica la prueba 112 autenticada en la cadena de bloques pública 104. Por lo tanto, un certificado y el compromiso 128 se publican en la cadena de bloques pública 104. El compromiso 128 se diseña para ser de "conocimiento cero" y no revela ninguna información acerca de las entradas individuales E1, ... , EN en la cadena de bloques 104.

Un segundo dispositivo informático (tal como un dispositivo de administrador de la cadena de bloques pública 104) se

asocia con la cadena de bloques pública 104. El segundo dispositivo informático asigna la primera cantidad del primer criptoactivo a la primera clave de un solo uso 144 en la cadena de bloques pública 104. La cadena de bloques 104 puede almacenar la asignación en una entrada de tabla de saldo. Para cada ronda, los validadores 152 de la cadena conjunta 120 llegan a un acuerdo acerca de la tabla de saldo de activos. Por lo tanto, cada bloque 124 producido por la cadena conjunta 120 incluye el compromiso 128 con las entradas de tabla de saldo. El segundo dispositivo informático quita la primera cantidad del primer criptoactivo de una tabla de saldo asociada con la cadena conjunta 120. El segundo dispositivo informático (de la cadena de bloques 104) también quita la segunda cantidad del segundo criptoactivo de otra tabla de saldo de la cadena de bloques pública 104 que se asocia con la cadena conjunta 140. En algunas implementaciones, el segundo dispositivo informático asigna la segunda cantidad del segundo criptoactivo a una segunda clave de un solo uso en la cadena de bloques pública 104. La segunda clave de un solo uso anonimiza una identidad de la segunda cuenta de criptoactivos 136 en la cadena conjunta 140. En otras implementaciones, un segundo dispositivo de usuario puede transferir el segundo criptoactivo a una segunda clave de larga duración con menos dependencia del anonimato.

El segundo dispositivo informático realiza una permuta atómica entre la primera cantidad del primer criptoactivo y la segunda cantidad del segundo criptoactivo. La permuta entre la primera cantidad del primer criptoactivo y la segunda cantidad del segundo criptoactivo es atómica, lo que significa que el intercambio está aislado de otras transacciones que puedan estar teniendo lugar al mismo tiempo. La permuta es, por lo tanto, indivisible, de tal modo que el intercambio se realiza sin que aparezca ninguna otra transacción entre medias. La segunda clave de un solo uso se asocia con el compromiso 132. El compromiso 132 debe transferir la segunda cantidad del segundo criptoactivo desde la segunda cuenta de criptoactivos 136 a la primera cuenta de criptoactivos 124. El compromiso 132 resulta de un bloque en la cadena conjunta 140. Por lo tanto, dos cadenas conjuntas privadas honestas 120, 140 pueden intercambiar criptoactivos a través de la cadena de bloques pública 104. La cadena de bloques pública 104 actualizará los saldos de cadena conjunta en consecuencia.

En algunas implementaciones, el segundo dispositivo informático (de la cadena de bloques 104) almacena un registro de la permuta atómica en un libro de contabilidad distribuido de la cadena de bloques pública 104. El registro hace referencia a las cadenas conjuntas privadas 120, 140. Por lo tanto, dos usuarios U1 y U2 que pertenecen a dos cadenas conjuntas privadas 120, 140 separadas pueden permutar activos capturados en los registros E1 y E2 en las cadenas conjuntas privadas 120, 140 respectivas. En algunas implementaciones, la cadena de bloques pública 104 incluye un intercambio de divisa. Un primer criptoactivo puede ser una primera divisa, y un segundo criptoactivo puede ser una segunda divisa.

En algunas implementaciones, la cadena de bloques pública 104 incluye un intercambio de testigos no fungibles (NFT). El primer criptoactivo es un NFT y el segundo criptoactivo es un conjunto de testigos fungibles. Por lo tanto, la red de pagos puede generar y realizar transacciones con testigos de criptodivisa fungibles asociados con una criptodivisa particular. Un testigo es fungible si dos de sus unidades son intercambiables. Un ejemplo de un testigo fungible es cuando dos unidades cualesquiera tienen el mismo poder adquisitivo. En algunas implementaciones, la cadena de bloques pública 104 incluye un intercambio de NFT, en donde el primer criptoactivo es un primer NFT y el segundo criptoactivo es un segundo NFT. Por ejemplo, el segundo dispositivo informático puede generar un NFT en la cadena de bloques 104. El NFT transforma en testigos primer criptoactivo. En algunas implementaciones, un gobierno o una institución desea transformar en testigos un activo. La institución puede crear un nuevo testigo en la cadena de bloques 104 usando llamadas a API de creación de testigos estándar. La institución puede entonces permanecer como el administrador de activos.

El segundo dispositivo informático (de la cadena de bloques 104) actualiza una tabla de saldo de la cadena de bloques pública 104 con la segunda cantidad del segundo criptoactivo. La tabla de saldo se asocia con la cadena conjunta 120. La cadena de bloques pública 104 mantiene "saldos" de activos para cada cadena conjunta 120, 140, de tal forma que las cadenas conjuntas privadas 120, 140 pueden realizar transacciones con otras cadenas conjuntas. El primer dispositivo de usuario (asociado con la primera cuenta de criptoactivos 124) inicia otra transacción de criptoactivos para transferir la segunda cantidad del segundo criptoactivo desde la cadena de bloques pública 104 a la cadena conjunta 120. En algunos casos, el administrador de la cadena conjunta privada puede ser el mismo que la institución que crea el activo en la cadena de bloques pública 104. Por lo tanto, los criptoactivos se han intercambiado.

En algunas implementaciones, un dispositivo de usuario genera una primera clave de un solo uso 144 que anonimiza una identidad de una primera cuenta de criptoactivos 124 de la cadena conjunta 120. Por lo tanto, las cadenas conjuntas privadas permiten que los usuarios realicen transacciones privadas en entornos de red cerrados. Las transacciones que se propagan en la cadena conjunta 120 no son visibles para todo el mundo. El dispositivo de usuario instala una transacción de criptoactivos en la cadena conjunta 120 para transferir una cantidad de un criptoactivo desde la primera cuenta de criptoactivos 124 a una segunda cuenta de criptoactivos 136 de la cadena conjunta 120. Un dispositivo informático (administrador de la cadena conjunta 120) puede generar una clave privada usando criptografía de curva elíptica, la clave privada para firmar la transacción de criptoactivos por el dispositivo de usuario. La identidad de la segunda cuenta de criptoactivos 136 se anonimiza mediante una segunda clave de un solo uso. El dispositivo informático (administrador de la cadena conjunta 120) registra un conjunto de validadores 152 en la cadena de bloques pública 104. Cada validador 152 tiene una clave pública diferente para validar transacciones de criptoactivos. Para cada ronda R de este tipo, los validadores 152 de la cadena conjunta 120 llegan a un acuerdo

acerca de la tabla de saldo de activos. Cada bloque 124 producido por la cadena conjunta 120 incluye un compromiso de las entradas de tabla de saldo.

Los validadores 152 asociados con la cadena conjunta 120 reciben una solicitud de validación asociada con la transacción de criptoactivos. La solicitud de validación pide a cada validador 152 que valide la transacción de criptoactivos. Cada cadena conjunta 120, 140 puede realizar un consenso independiente en cada bloque de transacciones. Los validadores 152 validan la primera transacción de criptoactivos para generar un compromiso 128 asociado con la primera clave de un solo uso 144 y la segunda clave de un solo uso. El dispositivo de usuario autentica una prueba 112 de la transacción de criptoactivos. La prueba 112 se asocia con el primer compromiso 128. El dispositivo de usuario publica la prueba 112 autenticada en la cadena de bloques pública 104. De este modo, la cadena conjunta 120 puede cumplir con las obligaciones normativas. El dispositivo informático (administrador) asociado con la cadena conjunta 120 añade la transacción de criptoactivos a un bloque 124 de la cadena conjunta 120. El bloque 124 hace referencia al compromiso 128. Por lo tanto, las transacciones y los bloques 124 de las cadenas conjuntas privadas 120 no se propagan a la cadena de bloques pública 104.

En respuesta a la adición de la transacción de criptoactivos al bloque 124, el dispositivo informático publica el compromiso 128 en la cadena de bloques pública 104 que se acopla de forma comunicable a la cadena conjunta 120. El dispositivo informático cifra la información auxiliar asociada con la transacción de criptoactivos usando un cifrado basado en atributos. Los administradores de la cadena conjunta pueden gestionar la visibilidad de las transacciones individuales y los activos de la cadena conjunta utilizando protocolos de red estándar y políticas de control de acceso. Además, los administradores pueden cumplir con sus obligaciones normativas y los requisitos de velocidad de sus clientes. El certificado 112 y el compromiso 128 se publican en la cadena de bloques 104. El dispositivo informático realiza una permuta atómica de la cantidad del criptoactivo desde la primera cuenta de criptoactivos 124 a la segunda cuenta de criptoactivos 136 en la cadena conjunta 120. La cadena de bloques pública 104 almacena un registro 108 de la transacción de criptoactivos en un libro de contabilidad distribuido de la cadena de bloques pública 104. El registro 108 hace referencia al compromiso 128.

En algunas implementaciones, un dispositivo de usuario genera una primera clave de un solo uso 144 que anonimiza una identidad de la primera cuenta de criptoactivos 124 de la cadena de bloques privada 120. El dispositivo de usuario se asocia con la primera cuenta de criptoactivos 124. El dispositivo de usuario instala una transacción de criptoactivos en la cadena de bloques privada 120 para transferir una cantidad de un criptoactivo desde la primera cuenta de criptoactivos 124 a una segunda cuenta de criptoactivos 136 de la cadena de bloques privada 140, una identidad de la segunda cuenta de criptoactivos 136 anonimizada por una segunda clave de un solo uso. Los dispositivos de validador 152 asociados con la cadena de bloques privada 120 reciben una solicitud de validación asociada con la transacción de criptoactivos. La solicitud de validación pide a cada dispositivo de validador 152 que valide la transacción de criptoactivos. Los dispositivos de validador 152 validan la transacción de criptoactivos para generar un compromiso 128 asociado con la primera clave de un solo uso 144 y la segunda clave de un solo uso. Un dispositivo informático asociado con la cadena de bloques privada 120 publica la transacción de criptoactivos en un bloque de la cadena de bloques privada 120. El dispositivo informático puede ser un ordenador de escritorio, un portátil o un servidor implementado como se ilustra y se describe con más detalle en referencia a la figura 5. El bloque hace referencia al compromiso 128. En respuesta a la publicación de la transacción de criptoactivos en el bloque, el dispositivo informático publica el compromiso 128 en la cadena de bloques pública 104 que se acopla de forma comunicable a la cadena de bloques privada 120.

Transferencia entre una cadena conjunta privada y la cadena de bloques pública.

En algunas implementaciones, un dispositivo de usuario instala una transacción de criptoactivos en una cadena de bloques privada 120 para transferir una cantidad de un criptoactivo desde una primera cuenta de criptoactivos 124 en la cadena de bloques privada 120 a una segunda cuenta de criptoactivos en una cadena de bloques pública 104. Los dispositivos de validador 152 validan la transacción de criptoactivos para generar un compromiso 128 asociado con una clave de un solo uso 144. Un primer dispositivo informático asociado con la cadena de bloques privada 120 publica el compromiso 128 en la cadena de bloques pública 104. Un segundo dispositivo informático asociado con la cadena de bloques pública 104 asigna la cantidad del criptoactivo a la clave de un solo uso 144 en la cadena de bloques pública 104. El segundo dispositivo informático realiza una permuta atómica de la cantidad del criptoactivo entre la clave de un solo uso 144 y la segunda cuenta de criptoactivos, de tal modo que la cantidad del criptoactivo se asigna a la segunda cuenta de criptoactivos en la cadena de bloques pública 104.

En algunas implementaciones, un dispositivo de usuario instala una transacción de criptoactivos en una cadena de bloques pública 104 para transferir una cantidad de un criptoactivo desde una primera cuenta de criptoactivos de la cadena de bloques pública a una segunda cuenta de criptoactivos en una cadena de bloques privada 120. Los dispositivos de validador 152 validan la transacción de criptoactivos para generar un compromiso 128 asociado con una clave de un solo uso 144. Un dispositivo informático asociado con la cadena de bloques pública 104 publica el compromiso 128 en la cadena de bloques pública 104. El dispositivo informático asocia la clave de un solo uso 144 con la segunda cuenta de criptoactivos. El dispositivo informático asigna la cantidad del criptoactivo a la clave de un solo uso 144. El dispositivo informático transfiere la cantidad del criptoactivo a la cadena de bloques privada 120.

En algunas implementaciones, un primer dispositivo informático asociado con una cadena conjunta 120 genera una cantidad de un criptoactivo en una cadena de bloques pública 104. La cantidad del criptoactivo se asigna a una clave de un solo uso 144 que anonimiza una cuenta de criptoactivos 124 de la cadena de bloques privada 120 que se acopla de forma comunicable a la cadena de bloques pública 104. El primer dispositivo informático instala una transacción de criptoactivos para transferir la cantidad del criptoactivo desde la cadena de bloques pública 104 a la cuenta de criptoactivos 124 de la cadena de bloques privada 120 usando la clave de un solo uso 144. Al menos un portavoz 156 de los múltiples validadores 152 valida la transacción de criptoactivos. Un segundo dispositivo informático asociado con la cadena de bloques pública 104 realiza al menos una comprobación asociada con la transacción de criptoactivos. El primer dispositivo informático transfiere la cantidad del criptoactivo desde la cadena de bloques pública 104 a la cuenta de criptoactivos 124 de la cadena de bloques privada 120 usando la clave de un solo uso 144.

En algunas implementaciones, se asigna al primer criptoactivo una clave distinta a la de un solo uso. Por ejemplo, la clave podría ser una clave usada por la primera cadena de bloques privada 120 para todas las transferencias de criptoactivos a la cadena de bloques pública 104.

Identificación de un portavoz para certificar datos

En algunas implementaciones, los validadores 152 asociados con una cadena de bloques privada 120 reciben una solicitud de validación asociada con una transacción de criptoactivos. La solicitud de validación pide a cada validador 152 que valide la transacción de criptoactivos. Se identifica al menos un portavoz 156 para certificar datos en nombre de los validadores 152. El al menos un portavoz 156 publica los datos en una cadena de bloques pública 104 que se acopla de forma comunicable a la cadena de bloques privada 120. Los validadores 152 determinan si los datos son válidos. En respuesta a la determinación, los validadores 152 publican una impugnación a los datos en la cadena de bloques pública 104. El portavoz puede entonces ser verificado cuando responde a la impugnación.

En algunas implementaciones, un portavoz 156 asociado con una cadena de bloques privada 120 identifica datos de uno o más bloques de la cadena de bloques privada 120. El portavoz 156 determina que los datos han sido validados por uno o más validadores 152 asociados con la cadena de bloques privada 120. El portavoz 156 genera una firma digital de los datos. En respuesta, los datos y la firma digital se publican en una cadena de bloques pública 104 asociada con la cadena de bloques privada 120.

Cadenas de bloques privadas y públicas

La figura 2 muestra un caso de uso de ejemplo de una red de pagos que usa múltiples cadenas conjuntas privadas 264, 268 con permisos, de acuerdo con una o más implementaciones. Las cadenas de bloques privadas y públicas desempeñan papeles complementarios. En una cadena conjunta privada 264 (por ejemplo, con permisos), las partes de una subcomunidad pueden realizar transacciones entre las mismas sin que sus identidades e interacciones sean visibles para las partes externas. En una cadena de bloques pública 200 (por ejemplo, sin permisos), todas las partes pueden observar todas las transacciones. Por ejemplo, los bancos 204 y 208 pueden llevar a cabo transacciones internas en sus propias cadenas conjuntas privadas 264, 268 para potenciar la velocidad, para ocultar sus actividades a los competidores y para facilitar el cumplimiento de la normativa.

Póngase por caso que una parte 212 en el banco 264 desea comerciar con activos 216 con una parte 236 en el banco 268. Debido a que ninguna de las partes quiere exponer su cadena conjunta privada a la otra, las partes 212, 236 mueven los activos 216, 240 con los que va a comerciarse desde sus propias cadenas conjuntas privadas 264, 268 a una cadena de bloques pública común 200, ejecutan la compraventa en la cadena de bloques 200, y entonces sus activos 240, 216 recién adquiridos vuelven a sus cadenas conjuntas privadas 264, 268 respectivas. Las entidades 212, 220, 228 se refieren a usuarios o a una cuenta en la cadena conjunta privada 264. Las entidades 216, 234, 232 son activos. Cuando el banco 204 crea una transacción privada 244, publica el compromiso 252 en la cadena de bloques pública 200 anonimizando la identidad de la cuenta 212. La cadena de bloques pública crea un bloque 248 para representar la transacción 244. De forma similar, se generan los bloques 256, 260.

Ejecutar compraventas moviendo activos entre cadenas de bloques privadas y públicas proporciona una forma rápida y segura de liquidar transacciones entre 204, 208. Además, una compraventa de este tipo no compromete la privacidad de las partes, debido a que ninguna de las mismas necesita aprender la identidad exacta de la otra. En los sistemas financieros tradicionales, los bancos mantienen libros de contabilidad privados y ocasionalmente (al final de la hora, del día o de la semana) realizan liquidaciones entre los mismos. Sin embargo, la capa de liquidación tradicional es lenta y costosa. Por ejemplo, se tarda hasta 3 días en liquidar las transacciones entre libros de contabilidad bancarios. Una red de pagos trans-cadena global basándose en las implementaciones divulgadas permite que los usuarios realicen transacciones entre libros de contabilidad privados de forma casi instantánea y a un coste bajo. Las implementaciones divulgadas permiten que las partes 212, 236 en distintas cadenas conjuntas privadas 264, 268 permuten activos 216, 240 de una forma eficiente sin comprometer la privacidad o la seguridad. Específicamente, una colección de cadenas conjuntas privadas 264, 268 usan una cadena de bloques pública común 200 como "territorio neutral" para los intercambios.

Cadenas conjuntas acopladas de forma comunicable

En algunas implementaciones, las cadenas conjuntas ejecutan una variante del consenso tolerante a fallos bizantinos (BFT). Los protocolos de BFT proporcionan seguridad incluso cuando la comunicación es asíncrona, y aseguran la capacidad de respuesta cuando la comunicación se convierte en síncrona durante un período de tiempo suficiente. En los protocolos de BFT, un conjunto de validadores 152 (ConjuntoV) aprueba cada bloque de transacciones. Los validadores 152 se ilustran y se describen con más detalle con referencia a la figura 1. Los validadores 152 se identifican por sus claves públicas en el conjunto ConjuntoV. En algunas implementaciones, se usan activos no fungibles (por ejemplo, las titularidades de coches, los identificadores de las tarjetas de regalo, etc.). En otras implementaciones, la arquitectura soporta activos fungibles).

Las cadenas conjuntas según las implementaciones divulgadas tienen las siguientes propiedades. En primer lugar, las cadenas conjuntas (por ejemplo, la cadena conjunta 120) producen compromisos 128 con los activos de la cadena conjunta. La cadena conjunta 120 y el compromiso 128 se ilustran y se describen con más detalle con referencia a la figura 1. Una cadena conjunta 120 produce un compromiso criptográfico 128 (C_r) de toda la tabla de saldo de la cadena conjunta 120 (la correlación de todos los activos y sus propietarios) en cada bloque 124. Este compromiso 128 soporta pruebas eficientes de pertenencia y no pertenencia. En segundo lugar, se generan certificados de bloque. Para cada ronda r, los validadores 152 confirman cada bloque B_r de transacciones y producen un certificado de ronda correspondiente, $Cert_r$, y un compromiso de ronda C_r. Una entidad puede verificar la tupla (C_r, $Cert_r$) dado un compromiso de bloque previo con el certificado asociado (C_{r-1}, $Cert_{r-1}$) y un algoritmo de verificación (VerificarBloque) que es conocido públicamente por participantes en la red. Por ejemplo, el algoritmo de verificación podría simplemente especificar un umbral T (*quorum*) de los validadores 152 que deben aprobar la transición de estado.

En tercer lugar, una vez que se crea un certificado de ronda, las transacciones en el bloque se consideran definitivas y no pueden ser revocadas o modificadas. Además, en cualquier punto en el tiempo, solo existe un único certificado válido, $Cert_r$, que certifica un único compromiso C_r para cualquier ronda r.

Una cadena conjunta privada se refiere, por lo tanto, a una cadena conjunta con permisos en donde un conjunto seleccionado de validadores 152 (ConjuntoV), identificados por sus claves públicas, aprueba cada bloque de transacciones. El conjunto de validadores 152 puede cambiar, siempre que un conjunto actual de validadores 152 apruebe los cambios. De forma similar, cualquier persona que quiera unirse a la cadena conjunta privada debe ser aprobada por los validadores presentes 152. Todos los cambios en la pertenencia del conjunto de validadores 152 o de los participantes se registran como transacciones especiales en la cadena de bloques. Las cadenas conjuntas privadas pueden desplegar diversas reglas de visibilidad a nivel de red acerca de las transacciones y los saldos. Por ejemplo, la cadena conjunta puede ser configurada de tal forma que solo los validadores 152 puedan ver las transacciones y los saldos, o la identidad de un participante. Una cadena de bloques pública permite que cualquiera se una a la red sin necesidad de aprobaciones. Todas las transacciones y los saldos de los usuarios son visibles para cualquiera que se una a la red. Sujeto a las reglas de consenso, cualquier participante puede convertirse en un validador 152 en la red.

Compromisos criptográficos

El esquema de compromiso usado en las implementaciones divulgadas tiene las siguientes propiedades. En primer lugar, Compromiso(E_1, E_N) = C. El algoritmo de compromiso toma como entrada una colección de registros (por ejemplo, cada registro es una correlación entre una clave pública y un activo). Emite un compromiso corto para todo el conjunto (por ejemplo, 32 bytes). En segundo lugar, Abrir(E_1, ... , E_N, C, i) = P_i. El algoritmo de apertura toma como entrada la colección de registros con el compromiso correspondiente y un índice $i \leq N$. Este emite una prueba sucinta P_i para el registro E_i. En tercer lugar, Verificar(C, E_i, P_i, i) = 1. El algoritmo de verificación toma como entrada un compromiso y un registro con la prueba correspondiente. Emite 1 si y solo si y solo si E_i se confirmó de hecho en la posición i. En cuarto lugar, ActualizarCompromiso(C, P_i, E_i, E'_i, i) = C'. La función de actualización del compromiso toma como entrada un compromiso, un registro con una prueba y un registro modificado. Emite un nuevo compromiso C' que sustituye el registro E_i por E'_i en la posición i.

Los esquemas de compromiso satisfacen las propiedades de vinculación de posición y ocultación. La vinculación de posición se refiere a la funcionalidad de que ningún adversario puede producir un compromiso válido C y dos pruebas válidas para los registros E_i, E'_i para la misma posición i. La propiedad de ocultación se refiere a la funcionalidad de que, dado un compromiso C y cualquier número de aperturas con las pruebas correspondientes {E_i, P_i, i}, no se revela ninguna información acerca de los registros restantes no abiertos.

Compromisos con transacciones de autovalidación

En algunas implementaciones, se construyen transacciones de autovalidación a partir de compromisos criptográficos eficientes en una cadena conjunta basada en cuentas. Supóngase que, para cada bloque r, los validadores de la cadena conjunta 152 producen (B_r, $Cert_r$, C_r), en donde C_r es un compromiso criptográfico con los saldos que especifica la entidad que posee cada activo. Supóngase que los validadores 152 solo almacenan C_r después de que se haya finalizado la ronda r. Un usuario que desee instanciar una transacción T que afecte a su registro E_i en la tabla de saldo puede ejecutar (o delegar en alguien) Abrir(E_1, ... , E_N, C_r, i) = P_i. El usuario propaga (T, E_i, P_i, i) a la red. Entonces,

cualquier validador 152 que tenga C_r para el bloque r puede verificar T usando las cinco etapas siguientes. En primer lugar, comprueba que Verificar(C_r, E_i, P_i, i) = 1. En segundo lugar, comprueba que T es válido según la lógica de transacción. Por ejemplo, la comprobación debería incluir que la transacción se firma bajo PK especificada en E_i, y la transacción especifica una nueva clave pública PK*.

En tercer lugar, todos los validadores 152 actualizan E_i --> E'_i para reflejar la transferencia de la propiedad de los activos, como se especifica en T. En cuarto lugar, los validadores 152 actualizan el compromiso ActualizarCompromiso(C_r, P_i, E_i, E'_i, i) = C_{r+1} para reflejar el cambio en la tabla de saldo. En quinto lugar, los validadores 152 se ponen de acuerdo acerca del compromiso actualizado C_{r+1} a través del protocolo de consenso.

En este modelo, no se requiere que los validadores 152 almacenen todas las entradas de saldo. En su lugar, solo participan en el consenso y acuerdan el nuevo compromiso C_{r+1} que refleja todas las transacciones que se aceptan en el bloque B_{r+1}. Esto posibilita una verificación más eficiente de transacciones con menos recursos. Por ejemplo, en la red puede operar un único servicio de archivo no fiable que todos los usuarios consultan para generar pruebas de propiedad. Tal servicio no es de confianza para la seguridad, debido a que, por las propiedades de seguridad de los compromisos criptográficos, solo puede generar pruebas para los registros que están incluidos en el compromiso.

Partes, activos y transferencias

En algunas implementaciones, la cadena de bloques 104 es un libro de contabilidad (o base de datos) distribuido, de lectura pública y a prueba de manipulaciones indebidas, que rastrea la propiedad de activos entre diversas partes. La cadena de bloques pública 104 se ilustra y se describe con más detalle con referencia a la figura 1. Un activo puede ser fungible, tal como una suma de dinero, o no fungible, tal como una entrada de teatro. Una parte se refiere a una persona, una organización o incluso un contrato. Cada cadena conjunta 120, 140 gestiona su propio libro de contabilidad, aplica sus propias reglas de validación e implementa su propio mecanismo de consenso. Las cadenas conjuntas 120, 140 se ilustran y se describen con más detalle con referencia a la figura 1. Además, cada cadena conjunta 120, 140 puede establecer sus propias políticas que rigen la visibilidad de sus propias transacciones. Por ejemplo, una política puede establecer que las transacciones sean visibles solo para los validadores 152 de la cadena conjunta, o que sean visibles para cualquiera.

En algunas implementaciones, se implementan cadenas conjuntas 120 que rastrean la propiedad de activos y transacciones que transfieren la propiedad de activos de una parte a otra. Las transferencias de valor se representan explícitamente en la cadena conjunta 120. Existe un primer dominio de partes y un segundo dominio de activos. Cada activo es propiedad de una parte. El predicado PoseeX (P, a) es verdadero si la parte P posee el activo a en la cadena conjunta X. Existe una parte distinguida N denotada como "nadie". Cada activo es propiedad de una parte en una cadena conjunta (por ejemplo, la cadena conjunta 120). En algunas implementaciones, cada activo "a" es propiedad de una parte P ≠ N en una cadena conjunta X: PoseeX (P, a), y es propiedad de "nadie" (N) en cada una de las otras cadenas conjuntas Y ≠ X: Posee_Y (N, a).

Una transferencia dentro de la cadena se refiere a una transición de estado en donde la parte P ≠ N transfiere un activo "a" a la parte Q en la cadena conjunta X. Por ejemplo, la transferencia puede representarse como: Previa:

$$\text{Owns}_X(P, a) \text{ and } P \neq N \qquad (1)$$

Posterior:

$$\text{Owns}_X(Q, a) \qquad (2)$$

La condición previa (1) establece que P debe poseer "a" en X y que P no debe ser N. La condición posterior (2) establece que Q ahora posee "a" en X (e implícitamente que P ya no posee "a"). Si Q es N, entonces el activo "a" ya no es gastable en X.

Una transferencia trans-cadena se refiere a una transición de estado en donde la parte P de la cadena conjunta X transfiere un activo "a" a la parte Q de una cadena conjunta distinta Y. La transferencia puede representarse como: Previa:

$$\text{Owns}_X(P, a) \text{ and } P \neq N \text{ and } X \neq Y \qquad (3)$$

Posterior:

$$\text{Owns}_X(N, a) \text{ and } \text{Owns}_Y(Q, a) \qquad (4)$$

La condición previa (3) establece que P debe poseer "a" en X, P no debe ser N, y X e Y son cadenas conjuntas distintas. La condición posterior (4) establece que Q ahora posee "a" en Y (e implícitamente que P ya no posee "a"). P y Q pueden ser partes distintas. Una transferencia trans-cadena asegura que el activo "a" ya no es gastable en la cadena conjunta X (debido a que es propiedad de N en X), y si el objetivo Q ≠ N, entonces "a" es gastable ahora en la cadena conjunta Y.

En algunas implementaciones, las transacciones en las cadenas conjuntas privadas 120, 140 no son visibles para otras cadenas conjuntas, incluyendo la cadena de bloques pública 104. La cadena de bloques pública 104 rastrea los "saldos" de los activos de cada cadena conjunta 120, 140. Una parte que posea un activo en una cadena conjunta 120 puede transferir el activo de la cadena conjunta 120 a la cadena de bloques pública 104, y viceversa. Las cadenas conjuntas privadas 120, 140 intercambian activos (1) transfiriendo esos activos a la cadena de bloques pública 104, (2) permutando los activos en la cadena de bloques pública 104, y (3) transfiriendo los activos recién adquiridos de vuelta. Si una cadena conjunta 120 es "honesta", entonces un activo transferido a la cadena de bloques pública 104 ya no puede gastarse en la cadena conjunta 120. Si la cadena conjunta 120 es "deshonesta", un activo puede gastarse dos veces en la cadena conjunta 120, pero no puede gastarse dos veces en la cadena de bloques pública 104, y mientras el activo resida en la cadena de bloques pública 104, su propiedad es pública.

En algunas implementaciones, cada transferencia trans-cadena es entre la cadena de bloques pública 104 y una cadena conjunta privada (por ejemplo, la cadena conjunta 120), y no entre cadenas conjuntas privadas 120, 140. Cada cadena conjunta 120, 140 proporciona su propio protocolo de transferencia dentro de la cadena que satisface la condición previa (1) y la condición posterior (2). Un protocolo común de transferencia trans-cadena satisface la condición previa (3) y la condición posterior (4). Una cadena conjunta X se denomina "deshonesta" si su protocolo de transferencia dentro de la cadena no satisface la condición previa (1) y la condición posterior (2), lo que implica que más de una parte puede poseer el mismo activo en X, una propiedad conocida como doble gasto.

En algunas implementaciones, hay una cadena de bloques pública 104, que es honesta, y muchas cadenas conjuntas privadas 120, 140, algunas de las cuales pueden ser deshonestas. El protocolo de transferencia de cadenas cruzadas proporciona la siguiente propiedad de no gasto doble trans-cadena: si "a" es un activo y X e Y son cadenas conjuntas honestas (públicas o privadas), entonces si "a" es propiedad de P en X y Q en Y, entonces P o Q es N. En algunas implementaciones, no se revela al público ninguna información acerca de la cadena conjunta 120 (es decir, qué entidad posee qué activo), excepto la información que se especifica explícitamente en la transferencia de una cadena conjunta privada X a la cadena de bloques pública Y. Más formalmente, esto se captura mediante un experimento de simulación. En el mundo real, el adversario recibe mensajes (en forma de transacciones) que se publican desde la cadena conjunta X a la cadena conjunta Y.

Por ejemplo, $(\alpha, \{Q : a\})$ denota la visión real del adversario a partir de la observación de la cadena de bloques pública Y, en donde $(Q : a\}$ captura un conjunto de todas las transferencias de activos "a" a las partes Q. En el mundo simulado, α_S es producido por un simulador de tiempo polinómico sin conocimiento de la información acerca de la cadena conjunta X. Además, $\{R : a\}s$ denota el conjunto de transferencias en donde cada identificador de la parte R es elegido aleatoriamente del conjunto de todos los identificadores posibles. Las dos distribuciones siguientes son computacionalmente indistinguibles: $(\alpha, \{Q : a\}) \sim_c (\alpha_S, \{R : a\}s)$. Esto proporciona las tres funciones siguientes. En primer lugar, cuando P en la cadena conjunta privada X transfiere "a" a Q en la cadena de bloques pública Y, se espera que P y Q representen a la misma persona o pertenezcan a la misma organización. Sin embargo, no debería haber forma de vincular a las dos partes: alguien que observe las transacciones en la cadena de bloques pública Y puede ser capaz de decir que el activo fue transferido desde X, pero no puede identificar quién era el propietario de ese activo en X.

En segundo lugar, si P transfiere en primer lugar "a" y entonces "a"', un observador no puede vincular las dos transferencias al mismo propietario previo. En tercer lugar, se aplican restricciones similares a las transferencias de las cadenas conjuntas públicas a las privadas: si Q transfiere "a" a R en la cadena conjunta privada Z, un observador no puede identificar a R, y si dos partes transfieren "a" y entonces "a"' a R en Z, las dos transferencias no pueden identificarse como destinadas al mismo destinatario.

Implementación de cadena conjunta privada

En algunas implementaciones, una cadena de bloques pública 104 es una red sin permisos a la que cualquier entidad puede unirse y participar. Cualquier entidad puede escribir y leer en la cadena de bloques pública 104, sujeta al pago de tasas de transacción, si es necesario. Cada cadena conjunta 120, 140 pasa en primer lugar por una fase de "incorporación" para registrarse. Las cadenas conjuntas privadas 120, 140 son redes con permisos, con validadores definidos explícitamente 152 y algoritmos de verificación de bloques. La fase de inicialización incluye etapas tales como el registro de los activos, el registro de la cadena conjunta privada y la distribución inicial de los activos. El orden de estas etapas puede variar.

Cada cadena conjunta 120, 140 registra en la cadena de bloques pública 104 si desea transferir activos entre las mismas. Puede emitirse una transacción especial en la cadena de bloques pública 104 que incluye un conjunto de claves públicas de validador, ConjuntoV = (VPK_1, VPK_2, ... , VPKn). La transacción de registro también incluye una descripción de un algoritmo VerificarBloque que introduce ($Cert_{r-1}$, C_{r-1}, $Cert_r$, C_r) y da como resultado "válido/no válido". Es decir, dado un compromiso de bloque para las rondas r-1, r con el certificado correspondiente, el algoritmo acepta si y solo si C_r es un compromiso válido de activos después de la ronda r. Después de que se haya aceptado la transacción de registro, la cadena de bloques pública 104 devuelve un identificador singular PrilD.

Cada clase de activo se registra en la cadena de bloques pública 104. El registrador puede especificar el suministro de activos total, la asignación inicial de los propietarios de los activos, o cómo se "acuñan" nuevos activos. Cada clase de activos recibe un identificador singular IDClaseActivo. Para simplificar, todos los activos se registran en "registros" (E_1, ... , E_N). Cada registro se identifica de forma singular mediante un índice i. El registro puede incluir información acerca del propietario actual del activo y cualquier información auxiliar adicional. Tras la inicialización, una función pública de consulta HallarActivo en la cadena de bloques pública 104 introduce (IDClaseActivo, índice i) y devuelve una tupla (IDCadena, j) que especifica el IDCadena de propietario de cadena conjunta actual, y un número de secuencia j monótonamente creciente para el activo (lo que se usará para evitar ataques de doble gasto más adelante).

Cada cadena conjunta 120, 140 ejecuta su propio algoritmo de consenso, funcionando a velocidad independiente. Para cada ronda r, los validadores de la cadena conjunta 152 producen una tupla (B_r, $Cert_r$, C_r), en donde C_r es un compromiso con la tabla de saldo de los titulares de activos. En algunas implementaciones, los validadores privados de la cadena conjunta 152, indexados por PrilD, producen una tupla (B_r, $Cert_r$, C_r). Se instancia una transacción especial (por los validadores 152 u otro miembro de la cadena conjunta 120) que incluye (IDCadena, Cr, Certr). Esta transacción se envía a la cadena de bloques pública 104. Cualquiera puede publicar esta tupla en la cadena de bloques pública 104. Esta parte no es de confianza para la seguridad, pero es de confianza para la capacidad de respuesta. Si la cadena conjunta 120 funciona más rápido que la cadena de bloques pública 104 (por ejemplo, la cadena conjunta 120 genera múltiples bloques de transacciones por cada bloque producido en la cadena de bloques pública 104), entonces una colección de compromisos con los correspondientes certificados IDCadena : (C_r, $Cert_r$, C_{r+1}, $Cert_{r+1}$, ...) puede publicarse simultáneamente en la cadena de bloques pública 104. La cadena de bloques pública 104 acepta tales transacciones solo si para todas las rondas r: VerificarBloque(Cr_{-1}, $Cert_{r-1}$, C_r, $Cert_r$) = 1. Por lo tanto, la cadena de bloques pública 104 verifica que existe un conjunto válido de validadores 152 que aprobó cada bloque. Obsérvese que, por sí mismo, ni el certificado ni el compromiso con los activos de la cadena conjunta revelan ninguna información acerca de los propietarios individuales de los activos.

Transferencias trans-cadena

Las entidades CadenaCoPriv (con el identificador PrilD) y CadenaCoPub denotan dos cadenas conjuntas. En algunas implementaciones, un activo se mueve de una clase de activo IDClaseActivo de una cadena conjunta 120, 140 a la cadena de bloques pública 104 (y a la inversa). Las implementaciones divulgadas preservan las propiedades de privacidad de la cadena conjunta privada y las propiedades de anonimato de sus usuarios. En algunas implementaciones, un usuario con una clave pública PK que posee el activo "i" de IDClaseActivo quiere transferir el activo a la cadena de bloques pública 104. Se siguen las siguientes etapas. En primer lugar, el usuario crea un nuevo par de claves (PK*, SK*). En segundo lugar, el usuario presenta una transacción especial en la cadena conjunta 120 que coloca el activo en una cuenta de "retirada" y asigna a PK* como el propietario. La cuenta también incluye una secuencia singular j' que es mayor que el último número de secuencia j de este activo, que puede obtenerse mediante una consulta en la cadena de bloques pública 104 (IDClaseActivo, i). Todo el estado de la cuenta se registra en un nuevo registro E'i. El usuario envía la transacción cambiando de ese modo el estado del activo "i" a E'_i. Una vez que el activo se ha transferido a este estado, no ha de realizarse ninguna transacción en la cadena conjunta 120, y permanece bloqueado.

En tercer lugar, la transacción es aceptada por los validadores de cadena conjunta privada 152 en la ronda r que produce (B_r, $Cert_r$, C_r). La tupla (IDCadena, $Cert_r$, C_r) se publica a través de una transacción en la cadena de bloques pública 104. En cuarto lugar, el usuario obtiene una prueba P_i con respecto a C_r de que puso de hecho el activo E'_i en el estado de retirada bajo la clave PK*. En quinto lugar, el usuario presenta la tupla (P_i, E'_i, i) a la cadena de bloques pública 104 mediante una transacción especial. En sexto lugar, la cadena de bloques pública 104 acepta la transacción si se cumplen las tres condiciones siguientes:

(a) Verificar(C_r, E'_i, P_i, i) = 1.
(b) E'_i está en el estado de "retirada" de la cadena conjunta 120.
(c) Consultar(IDCadena, j) basándose en el activo (IDClaseActivo, i). Validar que IDCadena coincide con la cadena conjunta 120 desde la que se presentó la retirada, y que el último número de secuencia j es menor que el número de secuencia j' especificado en E'_i.

En séptimo lugar, si las comprobaciones se superan, la cadena de bloques pública 104 crea el activo, lo quita de la cadena conjunta 120 y asigna al nuevo propietario el activo:

(a) La correlación de (IDClaseActivo, i) se actualiza para incluir el ID de la cadena de bloques pública, y el número de secuencia se establece en j' (la secuencia especificada en la retirada).
(b) El usuario PK* se asigna entonces como el propietario del activo "i" en la cadena de bloques pública 104.

Análisis de seguridad

Para lograr la privacidad (anonimato) de los usuarios que participan en los pagos trans-cadena, cada usuario U1 y U2 crea claves de un solo uso a las que transfiere activos en las cadenas conjuntas privadas 120, 140. Posteriormente, los usuarios realizan pagos trans-cadena usando estas claves de un solo uso. Las claves de un solo uso anonimizan los activos acumulados de los usuarios U1 y U2 en las cadenas conjuntas 120, 140 respectivas. En algunas implementaciones, las correlaciones individuales entre usuarios y sus activos dentro de una cadena conjunta 120 permanecen privados. La cadena de bloques pública 104 ve: (A) compromisos y certificados de validador con tablas de saldo de cadena conjunta individuales, (B) transacciones entre una cadena conjunta 120 y la cadena de bloques pública 104, y (C) registros auto-autenticados. La privacidad de la cadena conjunta se proporciona debido a que (B) no revela ninguna información acerca de los usuarios o los activos dentro de la cadena conjunta 120, debido a que el usuario crea un par de claves de un solo uso para cada transacción trans-cadena. (A) y (C) no revelan ninguna información acerca de la cadena conjunta 120 al ocultar criptográficamente los compromisos; los validadores 152 solo firman el compromiso.

Para que una cadena conjunta 120 cumpla con sus obligaciones normativas, éstas se quitan de la cadena de bloques pública 104 y se trasladan a las cadenas conjuntas privadas 120, 140. Cada banco puede mantener una cadena conjunta 120 y seguir siendo responsable de satisfacer a sus reguladores, dadas sus jurisdicciones. Durante una transferencia entre una cadena conjunta 120 y la cadena de bloques pública 104, tanto el usuario como los administradores o validadores de la cadena conjunta 152 firman cada transacción. Los administradores o validadores de la cadena conjunta 152 pueden ejecutar una política para asegurar que debería autorizarse la transferencia. Los reguladores pueden consultar adicionalmente a los administradores de las cadenas conjuntas privadas. Adicionalmente, pueden usarse herramientas de cifrado (por ejemplo, cifrado basado en atributos), si es necesario, en las transferencias. Es decir, cada transacción desde una cadena conjunta 120 a la cadena de bloques pública 104 puede incluir el cifrado de información auxiliar que solo los reguladores pueden inspeccionar. Por ejemplo, una cadena conjunta 120 administrada por un banco puede generar un par de claves (PK, SK), y emitir diferentes claves de reguladores SK_{P1}, ... , SK_{Pn} que especifican las políticas P_1, ... , P_n bajo las cuales se permite que los reguladores inspeccionen transferencias. Cada transacción se asocia con un conjunto de atributos (por ejemplo, fecha, tipo de transacción, tipo de remitente, etc.) y con información auxiliar cifrada para los reguladores (por ejemplo, materiales de autorización de transferencias). Dada la transacción y la clave secreta de una política SKP "i", un regulador puede inspeccionar el contenido cifrado de la transacción.

Proceso de ejemplo usando cadenas conjuntas

La figura 3 muestra un proceso 300 de ejemplo usando cadenas conjuntas. En algunas implementaciones, el proceso de la figura 3 es realizado por la red de pagos ilustrada y descrita con más detalle con referencia a la figura 1. Otras entidades realizan algunas o todas las etapas del proceso en otras implementaciones. Asimismo, las implementaciones pueden incluir etapas diferentes y/o adicionales, o realizar las etapas en diferentes órdenes.

Un dispositivo de usuario de una primera cadena de bloques privada (por ejemplo, la cadena conjunta 120) de la red de pagos instancia (304) una transacción de criptoactivos en la primera cadena conjunta 120. La cadena conjunta 120 se ilustra y se describe con más detalle con referencia a la figura 1. El dispositivo de usuario puede ser un teléfono inteligente, una tableta, un ordenador portátil, etc. La transacción de criptoactivos consiste en transferir una primera cantidad de un primer criptoactivo desde una primera cuenta de criptoactivos 124 a una segunda cuenta de criptoactivos 136 asociada con una segunda cadena conjunta privada (por ejemplo, la cadena conjunta 140). La cadena conjunta 140 se ilustra y se describe con más detalle con referencia a la figura 1. La transacción de criptoactivos se refleja en un bloque (por ejemplo, el bloque 124) de la cadena conjunta 120. El bloque 124 se ilustra y se describe con más detalle con referencia a la figura 1.

Un conjunto de validadores 152 de la primera cadena conjunta 120 valida (308) la primera transacción de criptoactivos para generar un primer compromiso (por ejemplo, el compromiso 128) asociado con una primera clave de un solo uso 144. Los validadores 152 y el compromiso 128 se ilustran y se describen con más detalle con referencia a la figura 1. Los validadores 152 de la cadena conjunta 120 reciben una solicitud de validación asociada con la transacción de criptoactivos. El primer dispositivo informático (de la cadena conjunta 120) puede registrar los validadores 152 en la cadena de bloques pública 104. La cadena de bloques pública 104 se ilustra y se describe con más detalle con referencia a la figura 1. Cada validador 152 tiene una clave pública diferente para validar transacciones de criptoactivos.

Un primer dispositivo informático asociado con la primera cadena conjunta 120 publica (312) el primer compromiso en una cadena de bloques pública (por ejemplo, la cadena de bloques 104). El primer dispositivo informático es un dispositivo de administrador de la primera cadena conjunta 120. Por ejemplo, cada entrada en una tabla de saldo se denota por E_i. Los validadores de cadena conjunta privada 152 producen un compromiso:

Ronda_R_Compromiso_Cadena_1 en la colección de entradas E_1, ... , E_N. Al final de la ronda, los validadores de cadena conjunta 152 producen un certificado Ronda_R_Cert_Cadena_1 que autoriza el compromiso Ronda_R_Compromiso_Cadena_1.

Un segundo dispositivo informático asociado con la cadena de bloques pública 104 asigna (316) la primera cantidad del primer criptoactivo a la primera clave de un solo uso 144 en la cadena de bloques pública 104. El segundo dispositivo informático es un dispositivo de administrador de la cadena de bloques 104. Por ejemplo, la cadena de bloques 104 puede almacenar la asignación en una entrada de tabla de saldo. Para cada ronda, los validadores 152 de la cadena conjunta 120 llegan a un acuerdo acerca de la tabla de saldo de activos. Por lo tanto, el bloque 124 producido por la cadena conjunta 120 incluye el compromiso 128 con las entradas de tabla de saldo. El segundo dispositivo informático quita la primera cantidad del primer criptoactivo de una tabla de saldo de la cadena conjunta 120 para reflejar que se está transfiriendo la primera cantidad del primer criptoactivo.

Proceso de ejemplo para transferir un activo usando cadenas conjuntas

La figura 4 muestra un proceso 400 de ejemplo para transferir un activo usando una cadena conjunta. En este proceso de ejemplo, un sistema de cadena de bloques tiene una cadena principal (por ejemplo, cadena de bloques pública), una cadena conjunta, en donde la cadena conjunta tiene una cuenta correspondiente en la cadena principal, un activo propiedad de la cuenta correspondiente en la cadena principal y propiedad de una cuenta en la cadena conjunta, y una cuenta de cadena conjunta que posee el activo. Una transacción autenticada se publica (402) en la cadena conjunta. Por ejemplo, la transacción es emitida por un miembro de la cadena conjunta y se incluye en un bloque de la cadena conjunta. La transacción autenticada autoriza una transferencia del activo desde la cuenta de cadena conjunta a la cadena principal. Los validadores de la cadena conjunta autentican (404) una cadena de datos que especifica el activo que va a transferirse y una clave pública de destino. La cadena de datos autenticada se entrega (406) a la cuenta de la cadena principal correspondiente a la cadena conjunta. Una transacción se publica (406) en la cadena principal. La transacción transfiere el activo a la clave pública de destino desde la cuenta de la cadena principal correspondiente a la cadena conjunta.

En algunas implementaciones, validadores de la cadena conjunta producen firmas parciales utilizables para calcular una firma digital basándose en una clave pública de destino, de tal modo que la firma digital es utilizable para autenticar la transferencia del activo a la cuenta de la cadena principal. Además, en algunas implementaciones, la firma digital se publica en la cadena principal.

En algunas implementaciones, se determina que la transacción autenticada se publica en la cadena conjunta antes de que la transacción que asigna el activo a la cuenta de la cadena principal se publique en la cadena principal.

En algunas implementaciones, la cuenta de la cadena principal correspondiente a la cadena conjunta es controlada por una entidad que controla una cuenta en la cadena conjunta.

Técnicas de ejemplo

En una técnica de ejemplo, una entidad (por ejemplo, una organización o entidad gubernamental) establece una cadena conjunta privada (por ejemplo, una de las cadenas conjuntas privadas 120, 140 mostradas en la figura 1) en la que esta lleva a cabo sus negocios internos. Un puente de testigos posibilita transferir ciertos activos no fungibles entre una cadena de bloques pública (por ejemplo, la cadena de bloques pública 104 mostrada en la figura 1), a veces denominada "cadena principal", y la cadena conjunta 120. Solo ciertas partes (por ejemplo, las partes asociadas con las claves públicas respectivas) en la cadena conjunta 120 están autorizadas a transferir a la cadena principal 104, y solo ciertas partes en la cadena principal 104 están autorizadas a transferir de vuelta a la cadena conjunta 120.

En un escenario de ejemplo, una entidad que tiene el título de propiedad en la cadena conjunta 120 decide subastar esa propiedad en la cadena principal 104. En primer lugar, la entidad da instrucciones a la cadena conjunta 120 para que transfiera la titularidad de la entidad a la cadena principal 104 junto con instrucciones a un agente de cadena principal para que subaste la propiedad y repatríe los ingresos a la cadena conjunta 120. Después de que la transacción sea validada y aparezca en la cadena conjunta 120, la transacción es enviada a la cadena principal 104 en donde es identificada y aceptada por el agente. Como parte de esta transferencia trans-cadena, los validadores 152 de la cadena conjunta comprueban que el propietario está autorizado a realizar transferencias trans-cadena, que su agente de cadena principal está autorizado a recibir tales transferencias, y que la transferencia y las instrucciones que la acompañan fueron validadas por un subconjunto correcto de validadores 152.

Árboles de Merkle en bloques

Una cadena conjunta 120, 140 es capaz de demostrar a la cadena principal 104 que ciertas transacciones tuvieron lugar. En algunas implementaciones, los bloques de la cadena conjunta organizan las transacciones en un árbol de Merkle en el que puede buscarse por cuenta, de tal modo que la cadena conjunta 120 puede demostrar que una transacción existe en la cadena conjunta 120, y que la transacción es autorizada por una de las claves públicas autorizadas para transferir activos a la cadena principal 104. De este modo, la cadena principal 104 puede recibir (1)

un compromiso de Merkle para la transacción, incluyendo instrucciones para el agente de cadena principal, y (2) un certificado firmado por un *quorum* de validadores de la cadena conjunta actual 152.

En algunos ejemplos, el propietario del activo en la cadena conjunta 120 paga tasas para transferir la titularidad a la cadena principal 104, para llevar a cabo la subasta, y para transferir los ingresos de vuelta. Por ejemplo, el propietario puede pagar un anticipo a su agente de cadena principal.

Campos de instrucción para las transacciones trans-cadena

En algunos ejemplos, una transferencia de activos trans-cadena puede ir acompañada de instrucciones para desechar activos en la cadena principal 104. Por ejemplo, estas instrucciones pueden ser secuencias de comandos (por ejemplo, secuencias de comandos del Lenguaje de Aprobación de Ejecución de Transacciones), llamadas a contratos inteligentes o texto en inglés notariado. Con este fin, en algunas implementaciones, el árbol de Merkle de transacciones del bloque de la cadena conjunta incluye un campo de instrucciones de una forma lo suficientemente flexible como para acomodar cualquier forma razonable de instrucciones.

Resumen de estructuras de datos merkelizadas

En algunos ejemplos, una cadena conjunta 120, 140 es capaz de producir síntesis compactas y a prueba de manipulaciones indebidas de los siguientes cuatro elementos. En primer lugar, la lista de activos que pueden intercambiarse actualmente con la cadena principal 104 (por ejemplo, la lista puede ser un requisito normativo). En segundo lugar, las claves públicas de las partes actualmente autorizadas a realizar transferencias trans-cadena desde la cadena conjunta a la cadena principal. En tercer lugar, el conjunto actual de validadores de la cadena conjunta 152. En cuarto lugar, la lista actual de portavoces. Las listas pueden cambiar y requerir actualizaciones. Por ejemplo, pueden ser aprobadas por un *quorum* de validadores de la cadena conjunta 152 para asegurar su validez. En algunas implementaciones, estas listas pueden ser organizadas como árboles de Merkle con capacidad de búsqueda, o podrían ser matrices no estructuradas, dependiendo de si deberían transmitirse parcial o completamente.

Cadencia de transferencia

En algunos ejemplos, hay varias opciones de política para la frecuencia de transferencia de activos entre cadenas de bloques. Una opción es hacer las transferencias periódicamente, por ejemplo, cada mil bloques. Otra es transferir bajo demanda. Es posible una combinación de estrategias, por ejemplo, ofrecer un servicio con recargo para las partes dispuestas a pagar por una respuesta oportuna, y un servicio económico básico para aquellos que deseen economizar en las tasas a cambio de una respuesta más lenta.

Portavoces

En algunas implementaciones, diversas estructuras de datos y mensajes enviados desde la cadena conjunta 120, 140 a la cadena principal 104 son certificados por un *quorum* de validadores de cadena conjunta 152. Para reducir el tamaño de tales certificaciones, los validadores de la cadena conjunta 152 pueden nombrar y certificar a uno o más "portavoces" (a veces denominados "voceros") para que certifiquen los datos en nombre de los validadores 152. Los validadores 152 pueden cambiar el portavoz 156, o bien de forma regular o bien en respuesta a un mal comportamiento percibido. Un portavoz 156 puede, en particular, notificar los siguientes datos. En primer lugar, las estructuras de datos merkelizadas 1 y 2. En segundo lugar, los activos que deben transferirse a la cadena principal 104 (incluyendo la instrucción de uso y las claves de compraventa que deben manejar los activos en la cadena principal 104).

Esta técnica puede asegurar que la información adecuada de un bloque de la cadena conjunta (por ejemplo, la incluida en cada décimo o centésimo bloque) se comunica de forma sucinta y eficiente a la cadena principal 104. En algunos ejemplos, un portavoz 156 de cadena conjunta no está autorizado a cambiar el conjunto de validadores 152 (por ejemplo, asegurando que no puede lanzar un "golpe", tal como cambiar maliciosamente los validadores 152 para beneficiar al portavoz 156) o el conjunto de los anteriores y un portavoz 156 recién nombrado.

En algunas implementaciones, los datos firmados digitalmente de los portavoces de la cadena conjunta se publican en la cadena principal 104, pero la cadena conjunta 120 no actúa sobre la misma (por ejemplo, no vende o permuta atómicamente un activo transferido a la cadena principal 104) durante un número determinado de bloques (por ejemplo, veinte bloques) para asegurar que los validadores 152 no objeten. En algunos ejemplos, los validadores de la cadena conjunta 152 pueden supervisar la cadena principal 104 y, si uno de los mismos se da cuenta de que un portavoz 156 publica información incorrecta, contrapublicará la correcta (por ejemplo, certificada por la mayoría adecuada de los validadores de la cadena conjunta 152). Pueden tomarse medidas para evitar múltiples publicaciones de información certificada por validador equivalente.

Por lo tanto, debido a que es más eficiente publicar elementos (por ejemplo, transacciones, activos, información, etc.) en la cadena principal 104 que son firmados digitalmente por una única clave 144 (por ejemplo, en nombre de toda la cadena conjunta 120), los elementos no necesitan ser firmados digitalmente por múltiples validadores 152. En su lugar, un elemento firmado por un portavoz 156 puede impugnarse dentro de una cantidad determinada de tiempo o

un número determinado de bloques, anulando la transferencia del portavoz 156. De este modo, estas técnicas posibilitan una acción centralizada y una rectificación distribuida.

Implementación de ejemplo de una red de pagos que incluye cadenas de bloques privadas con permisos

La figura 5 es un diagrama de bloques que ilustra un sistema informático 500, de acuerdo con una o más implementaciones. En una implementación, el sistema informático 500 es un dispositivo informático de propósito especial. El dispositivo informático de propósito especial puede cablearse físicamente para realizar las técnicas, o incluye dispositivos electrónicos digitales tales como uno o más circuitos integrados específicos de la aplicación (ASIC) o matrices de puertas programables en campo (FPGA) que se programan de forma persistente para realizar las técnicas, o puede incluir uno o más procesadores de hardware de propósito general programados para realizar las técnicas de conformidad con instrucciones de programa en firmware, memoria, otro almacenamiento o una combinación. Tales dispositivos informáticos de propósito especial también pueden combinar lógica físicamente cableada personalizada, ASIC o FPGA con programación personalizada para lograr las técnicas. En diversas implementaciones, los dispositivos informáticos de propósito especial son sistemas informáticos de escritorio, sistemas informáticos portátiles, dispositivos de mano, dispositivos de red o cualquier otro dispositivo que incorpore una lógica físicamente cableada y/o de programa para implementar las técnicas.

En algunas implementaciones, el sistema informático 500 incluye un bus 502 u otro mecanismo de comunicación para comunicar información, y un procesador de hardware 504 acoplado con un bus 502 para procesar información. El procesador de hardware 504 es, por ejemplo, un microprocesador de propósito general. El sistema informático 500 también incluye una memoria principal 506, tal como una memoria de acceso aleatorio (RAM) u otro dispositivo de almacenamiento dinámico, acoplado al bus 502 para almacenar información e instrucciones que van a ser ejecutadas por el procesador 504. En una implementación, la memoria principal 506 se usa para almacenar variables temporales u otra información intermedia durante la ejecución de instrucciones que van a ser ejecutadas por el procesador 504. Tales instrucciones, cuando se almacenan en medios de almacenamiento no transitorios accesibles para el procesador 504, convierten al sistema informático 500 en una máquina de propósito especial que se personaliza para realizar las operaciones especificadas en las instrucciones.

En algunas implementaciones, el sistema informático 500 puede incluir adicionalmente una memoria de solo lectura (ROM) 508 u otro dispositivo de almacenamiento estático acoplado al bus 502 para almacenar información estática e instrucciones para el procesador 504. Se proporciona un dispositivo de almacenamiento 510, tal como un disco magnético, un disco óptico, una unidad de disco de estado sólido o una memoria de puntos cruzados tridimensionales, acoplado al bus 502 para almacenar información e instrucciones.

En algunas implementaciones, el sistema informático 500 se acopla a través del bus 502 a una pantalla 512, tal como un tubo de rayos catódicos (CRT), una pantalla de cristal líquido (LCD), una pantalla de plasma, una pantalla de diodos emisores de luz (LED) o una pantalla de diodos emisores de luz orgánicos (OLED) para presentar información a un usuario de ordenador. Un dispositivo de entrada 514, que incluye teclas alfanuméricas y otras teclas, se acopla al bus 502 para comunicar información y ordenar selecciones al procesador 504. Otro tipo de dispositivo de entrada del usuario es un controlador de cursor 516, tal como un ratón, una bola de seguimiento, una pantalla habilitada para uso táctil o teclas de dirección de cursor para comunicar información de dirección y selecciones de comandos al procesador 504 y para controlar el movimiento del cursor en la pantalla 512. Este dispositivo de entrada tiene habitualmente dos grados de libertad en dos ejes, un primer eje (por ejemplo, el eje x) y un segundo eje (por ejemplo, el eje y), que permite que el dispositivo especifique posiciones en un plano.

De acuerdo con algunas implementaciones, las técnicas en el presente documento son realizadas por el sistema informático 500 en respuesta a que el procesador 504 ejecute una o más secuencias de una o más instrucciones contenidas en la memoria principal 506. Tales instrucciones se introducen por lectura en la memoria principal 506 desde otro medio de almacenamiento, tal como el dispositivo de almacenamiento 510. La ejecución de las secuencias de instrucciones contenidas en la memoria principal 506 hace que el procesador 504 realice las etapas de proceso descritas en el presente documento. En implementaciones alternativas, se usa una circuitería físicamente cableada en lugar de o en combinación con instrucciones de software.

La expresión "medios de almacenamiento" como se usa en el presente documento se refiere a cualquier medio no transitorio que almacena datos y/o instrucciones que hacen que una máquina funcione de una forma específica. Tales medios de almacenamiento incluyen medios no volátiles y/o medios volátiles. Los medios no volátiles incluyen, por ejemplo, discos ópticos, discos magnéticos, unidades de disco de estado sólido o memoria de puntos cruzados tridimensionales, tal como el dispositivo de almacenamiento 510. Los medios volátiles incluyen memoria dinámica, tal como la memoria principal 506. Las formas comunes de medios de almacenamiento incluyen, por ejemplo, un disco flexible, un disco flexible, disco duro, unidad de disco de estado sólido, cinta magnética, o cualquier otro medio de almacenamiento de datos magnético, un CD-ROM, cualquier otro medio de almacenamiento de datos óptico, cualquier medio físico con patrones de agujeros, una RAM, una PROM y EPROM, una FLASH-EPROM, NV-RAM o cualquier otro chip o cartucho de memoria.

Los medios de almacenamiento son distintos de los medios de transmisión pero pueden usarse junto con los mismos.

Los medios de transmisión participan en la transferencia de información entre medios de almacenamiento. Por ejemplo, los medios de transmisión incluyen cables coaxiales, hilo de cobre y fibra óptica, incluyendo los hilos que incluyen el bus 502. Los medios de transmisión también pueden adoptar la forma de ondas acústicas o de luz, tales como las generadas durante las comunicaciones de datos por ondas de radio e infrarrojos.

En algunas implementaciones, diversas formas de medios están implicadas en portar una o más secuencias de una o más instrucciones al procesador 504 para su ejecución. Por ejemplo, las instrucciones se portan inicialmente en un disco magnético o en una unidad de disco de estado sólido de un ordenador remoto. El ordenador remoto carga las instrucciones en su memoria dinámica y envía las instrucciones a través de una línea telefónica usando un módem. Un módem local del sistema informático 500 recibe los datos en la línea telefónica y usa un transmisor de infrarrojos para convertir los datos en una señal de infrarrojos. Un detector de infrarrojos recibe los datos transportados en la señal de infrarrojos y una circuitería adecuada coloca los datos en el bus 502. El bus 502 porta los datos a la memoria principal 506, de la que el procesador 504 recupera y ejecuta las instrucciones. Las instrucciones recibidas por la memoria principal 506 pueden opcionalmente ser almacenadas en el dispositivo de almacenamiento 510 antes o después de la ejecución por el procesador 504.

El sistema informático 500 también incluye una interfaz de comunicación 518 acoplada al bus 502. La interfaz de comunicación 518 proporciona una comunicación de datos bidireccional que se acopla a un enlace de red 520 que se conecta a una red local 522. Por ejemplo, la interfaz de comunicación 518 es una tarjeta de red digital de servicio integrado (RDSI), un módem de cable, un módem de satélite o un módem para proporcionar una conexión de comunicación de datos a un tipo de línea telefónica correspondiente. Como otro ejemplo, la interfaz de comunicación 518 es una tarjeta de red de área local (LAN) para proporcionar una conexión de comunicación de datos a una LAN compatible. En algunas implementaciones, también se implementan enlaces inalámbricos. En cualquier implementación de este tipo, la interfaz de comunicación 518 envía y recibe señales eléctricas, electromagnéticas u ópticas que portan flujos de datos digitales que representan diversos tipos de información.

El enlace de red 520 proporciona habitualmente comunicación de datos a través de una o más redes a otros dispositivos de datos. Por ejemplo, el enlace de red 520 proporciona una conexión a través de la red local 522 a un ordenador anfitrión 524 o a un centro de datos en la nube o a un equipo operado por un proveedor de servicios de Internet (ISP) 526. El ISP 526 proporciona, a su vez, servicios de comunicación de datos a través de la red de comunicación de datos por paquetes mundial comúnmente denominada en la actualidad "Internet" 528. Tanto la red local 522 como Internet 528 usan señales eléctricas, electromagnéticas u ópticas que portan flujos de datos digitales. Las señales a través de las diversas redes y las señales en el enlace de red 520 y a través de la interfaz de comunicación 518, que portan los datos digitales a y desde el sistema informático 500, son formas de ejemplo de medios de transmisión. En algunas implementaciones, la red 520 contiene una red o servidor en la nube, o una parte de una nube.

El sistema informático 500 envía mensajes y recibe datos, incluyendo código de programa, a través de la(s) red(es), el enlace de red 520 y la interfaz de comunicación 518. En algunas implementaciones, el sistema informático 500 recibe código para su procesamiento. El código recibido es ejecutado por el procesador 504 a medida que se recibe, y/o se almacena en el dispositivo de almacenamiento 510, u otro almacenamiento no volátil para su ejecución posterior.

En la descripción en el presente caso, para los fines de explicación, se exponen numerosos detalles específicos con el fin de proporcionar un entendimiento completo de las implementaciones divulgadas. Será evidente, sin embargo, que las implementaciones pueden ponerse en práctica sin estos detalles específicos. En los dibujos, se muestran disposiciones u ordenaciones específicas de elementos esquemáticos, tales como los que representan dispositivos, módulos, bloques de instrucciones y elementos de datos, para facilitar la descripción. Sin embargo, los expertos en la materia deberían entender que la ordenación o disposición específica de los elementos esquemáticos en los dibujos no implica que se requiera un orden o secuencia particular de procesamiento o separación de procesos. Además, la inclusión de un elemento esquemático en un dibujo no implica que tal elemento sea necesario en todas las implementaciones o que las características representadas por tal elemento no puedan incluirse o combinarse con otros elementos en algunas implementaciones.

Además, en los dibujos, en donde se usan elementos de conexión, tales como líneas o flechas de trazo continuo o discontinuo, para ilustrar una conexión, relación o asociación entre otros dos o más elementos esquemáticos, la ausencia de tales elementos de conexión no implica que no pueda existir ninguna conexión, relación o asociación. En otras palabras, algunas conexiones, relaciones o asociaciones entre elementos no se muestran en los dibujos para no complicar la divulgación. Además, para facilitar la ilustración, se usa un único elemento de conexión para representar múltiples conexiones, relaciones o asociaciones entre elementos. Por ejemplo, en donde un elemento de conexión representa una comunicación de señales, datos o instrucciones, los expertos en la materia deberían entender que tal elemento representa uno o varios caminos de señales (por ejemplo, un bus), según sea necesario, para afectar a la comunicación.

A continuación, se hará referencia con detalle a implementaciones, ejemplos de las cuales se ilustran en los dibujos adjuntos. En la siguiente descripción detallada, se exponen numerosos detalles específicos con el fin de proporcionar

una comprensión completa de las diversas implementaciones descritas. Sin embargo, será evidente para un experto en la materia que las diversas implementaciones descritas pueden ponerse en práctica sin estos detalles específicos. Aunque se proporcionan encabezados, la información relacionada con un encabezado particular, pero que no se encuentra en la sección que tiene ese encabezado, también puede encontrarse en otras partes de esta descripción.

Aunque la materia objeto se ha descrito en lenguaje específico de características estructurales y/o actos, ha de entenderse que la materia objeto definida en las reivindicaciones adjuntas no está limitada necesariamente a las características o actos específicos descritos. Más bien, las características y actos específicos descritos se divulgan como ejemplos de aplicación de las reivindicaciones y se pretende que otras características y actos equivalentes estén dentro del alcance de las reivindicaciones. En la descripción anterior, se han descrito implementaciones con referencia a numerosos detalles específicos que pueden variar de una implementación a otra. La descripción y los dibujos han de considerarse, en consecuencia, en un sentido ilustrativo más que restrictivo. El único y exclusivo indicador del alcance de las implementaciones, y lo que los solicitantes pretenden que sea el alcance de las mismas, es el alcance literal y equivalente del conjunto de reivindicaciones que se desprenden de esta solicitud, en la forma específica en la que se desprenden tales reivindicaciones, incluyendo cualquier corrección posterior. Cualquier definición expuesta expresamente en el presente documento para términos contenidos en tales reivindicaciones deberá regir el significado de tales términos como se usan en las reivindicaciones. Además, cuando se usa la expresión "incluyendo además", en la descripción anterior o en las reivindicaciones siguientes, lo que sigue a esta locución puede ser una etapa o entidad adicional, o una sub-etapa/sub-entidad de una etapa o entidad mencionada previamente.

REIVINDICACIONES

1. Un método para posibilitar que una o más entidades de un sistema de cadena de bloques realicen una serie de operaciones, en donde el sistema de cadena de bloques comprende

una cadena principal,
una cadena conjunta, en donde la cadena conjunta tiene una cuenta correspondiente en la cadena principal,
un activo propiedad de la cuenta correspondiente en la cadena principal y propiedad de una cuenta en la cadena conjunta, y
la cuenta de cadena conjunta que posee el activo,
comprendiendo las operaciones:

publicar (402) una transacción autenticada en la cadena conjunta, autorizando la transacción autenticada una transferencia del activo desde la cuenta de cadena conjunta a la cadena principal;
autenticar (404), por validadores (152) de la cadena conjunta, una cadena de datos que especifica el activo que va a transferirse y una clave pública de destino (144);
entregar (406) la cadena de datos autenticada a la cuenta de la cadena principal correspondiente a la cadena conjunta para indicar que el activo debería transferirse a la clave pública de destino; y
publicar, en la cadena principal, una transacción que transfiere el activo a la clave pública de destino desde la cuenta de la cadena principal correspondiente a la cadena conjunta.

2. El método de la reivindicación 1, comprendiendo las operaciones generar la clave pública.

3. El método de la reivindicación 1, en donde los validadores (152) autentican la cadena de datos usando una firma digital de un esquema de firma de umbral.

4. El método de la reivindicación 3, en donde la firma digital se genera en relación con una clave pública que se asocia con la cuenta en la cadena principal, en donde una clave secreta correspondiente es mantenida colectivamente por los validadores de la cadena conjunta.

5. El método de la reivindicación 1, en donde la cuenta de la cadena principal correspondiente a la cadena conjunta es controlada por una entidad que controla la cuenta en la cadena conjunta.

6. Un método para posibilitar que una o más entidades de un sistema de cadena de bloques realicen una serie de operaciones, en donde el sistema de cadena de bloques comprende

una cadena principal (104),
una cadena conjunta (120, 140), en donde la cadena conjunta tiene una cuenta correspondiente en la cadena principal,
un activo propiedad de la cuenta correspondiente en la cadena principal y propiedad de una cuenta en la cadena conjunta, en donde la cuenta de cadena conjunta posee el activo,
comprendiendo las operaciones:

publicar (402) una transacción autenticada en la cadena conjunta, autorizando la transacción autenticada una transferencia del activo desde la cuenta de cadena conjunta a otra cuenta de la cadena principal;
determinar que la transacción autenticada se publica en la cadena conjunta; y
publicar (406), en la cadena principal, una transacción que asigna el activo a la otra cuenta de la cadena principal.

7. El método de la reivindicación 6, comprendiendo las operaciones generar una clave pública (144).

8. El método de la reivindicación 6, en donde unos validadores autentican una cadena de datos usando una firma digital de un esquema de firma de umbral.

9. El método de la reivindicación 8, en donde la firma digital se genera en relación con una clave pública que se asocia con la cuenta de la cadena principal, en donde una clave secreta correspondiente es mantenida colectivamente por los validadores de la cadena conjunta.

10. El método de la reivindicación 6, en donde la cuenta de la cadena principal correspondiente a la cadena conjunta es controlada por una entidad que controla la cuenta en la cadena conjunta.

11. El método de la reivindicación 6, comprendiendo las operaciones:

producir, por validadores de la cadena conjunta, firmas parciales utilizables para calcular una firma digital basándose en una clave pública de destino, utilizable la firma digital para autenticar la transferencia del activo a la cuenta de la cadena principal; y

publicar la firma digital en la cadena principal para autorizar la transferencia del activo a la clave pública en la cadena principal.

12. Un sistema que comprende:

uno o más procesadores informáticos; y
uno o más medios de almacenamiento no transitorios que almacenan instrucciones que, cuando son ejecutadas por los uno o más procesadores informáticos, provocan la ejecución de un método mencionado en una cualquiera de las reivindicaciones 1-10.

13. Uno o más medios de almacenamiento no transitorios que almacenan instrucciones que, cuando son ejecutadas por uno o más dispositivos informáticos, provocan la ejecución de un método mencionado en una cualquiera de las reivindicaciones 1-11.

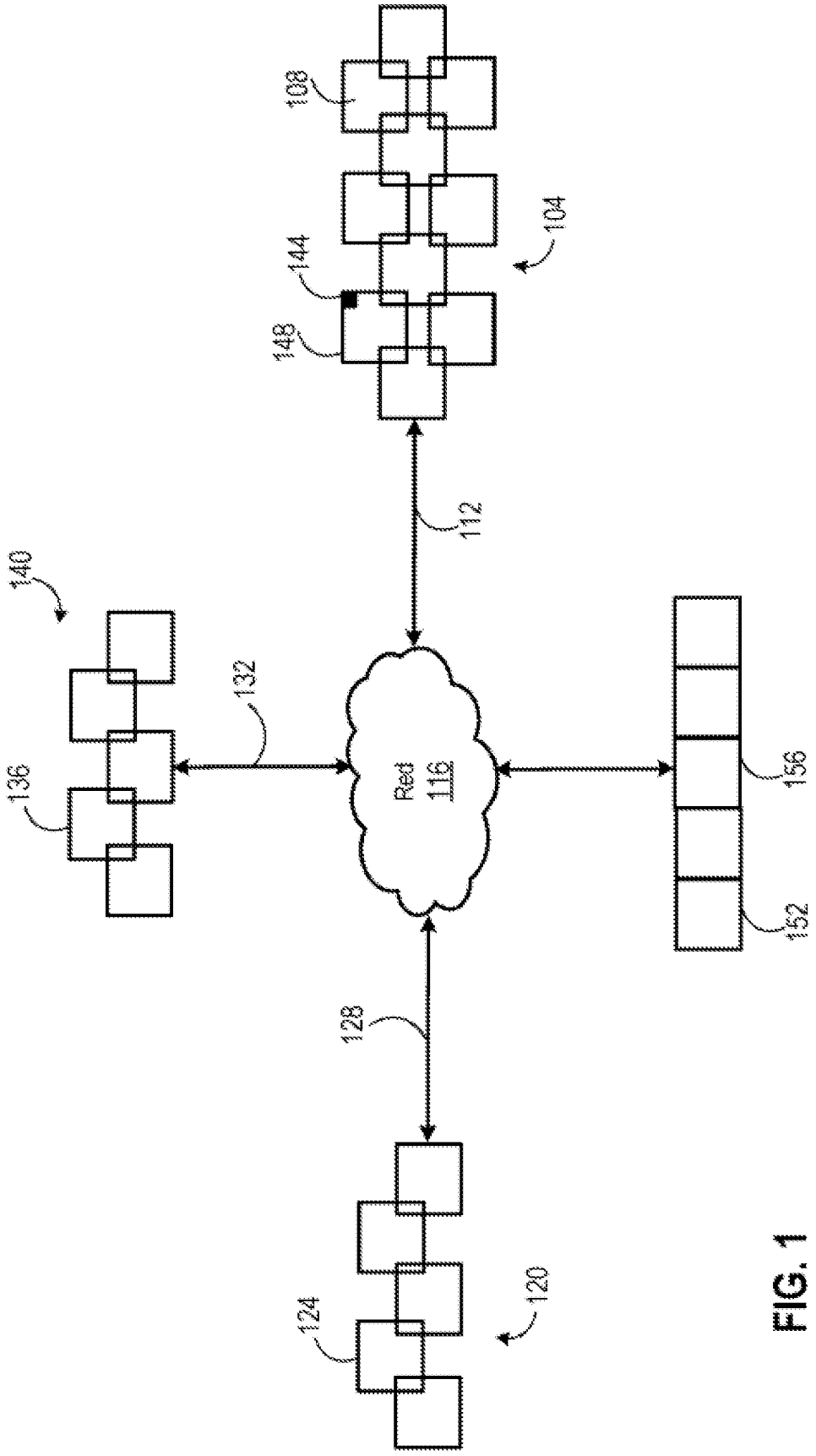

FIG. 1

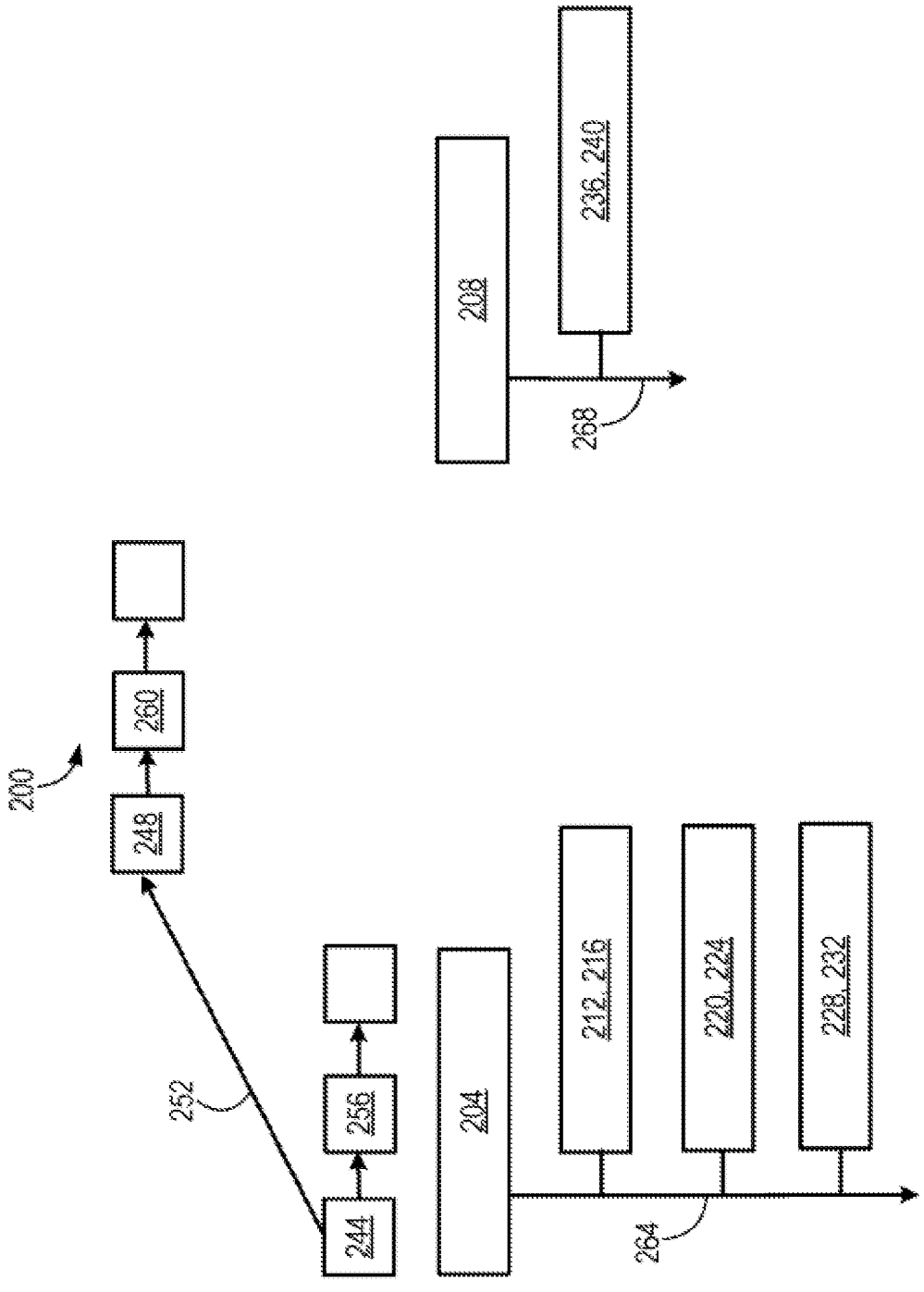
200
248
260
252
244
256
204
212, 216
220, 224
228, 232
264
208
236, 240
268

FIG. 2

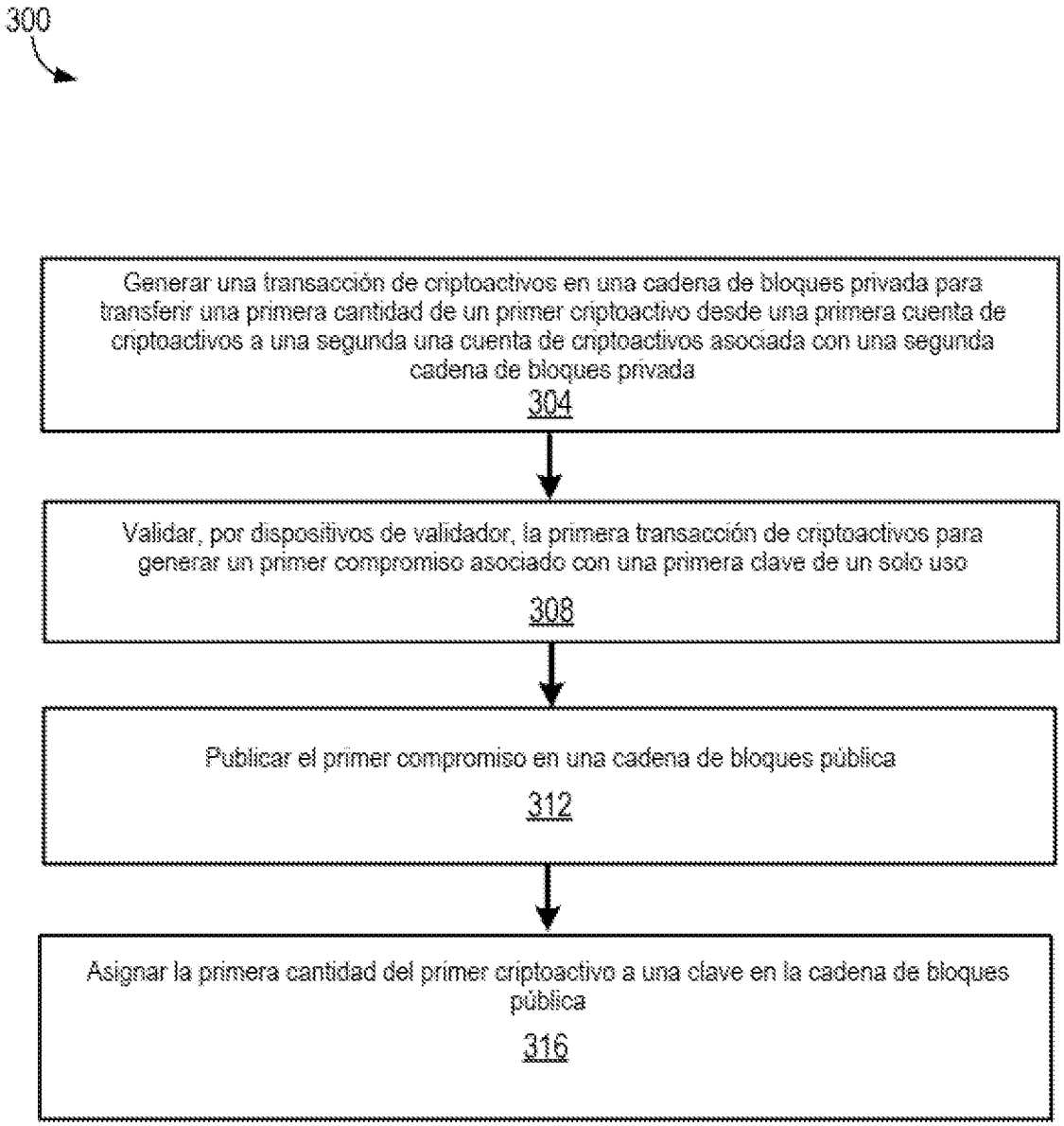
300
Generar una transacción de criptoactivos en una cadena de bloques privada para transferir una primera cantidad de un primer criptoactivo desde una primera cuenta de criptoactivos a una segunda una cuenta de criptoactivos asociada con una segunda cadena de bloques privada
304
Validar, por dispositivos de validador, la primera transacción de criptoactivos para generar un primer compromiso asociado con una primera clave de un solo uso
308
Publicar el primer compromiso en una cadena de bloques pública
312
Asignar la primera cantidad del primer criptoactivo a una clave en la cadena de bloques pública
316

FIG. 3

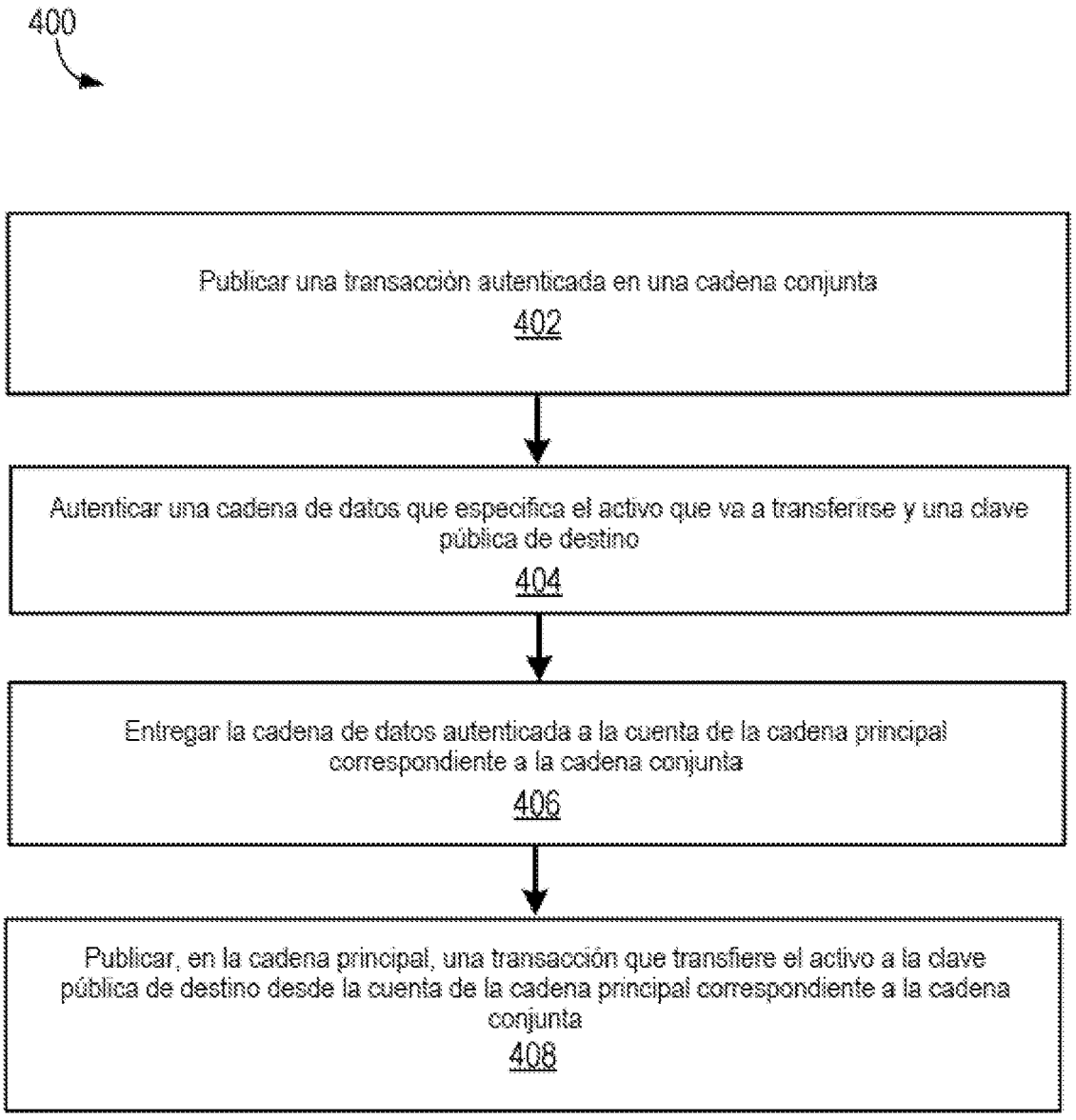
400
Publicar una transacción autenticada en una cadena conjunta
402
Autenticar una cadena de datos que especifica el activo que va a transferirse y una clave pública de destino
404
Entregar la cadena de datos autenticada a la cuenta de la cadena principal correspondiente a la cadena conjunta
406
Publicar, en la cadena principal, una transacción que transfiere el activo a la clave pública de destino desde la cuenta de la cadena principal correspondiente a la cadena conjunta
408

FIG. 4

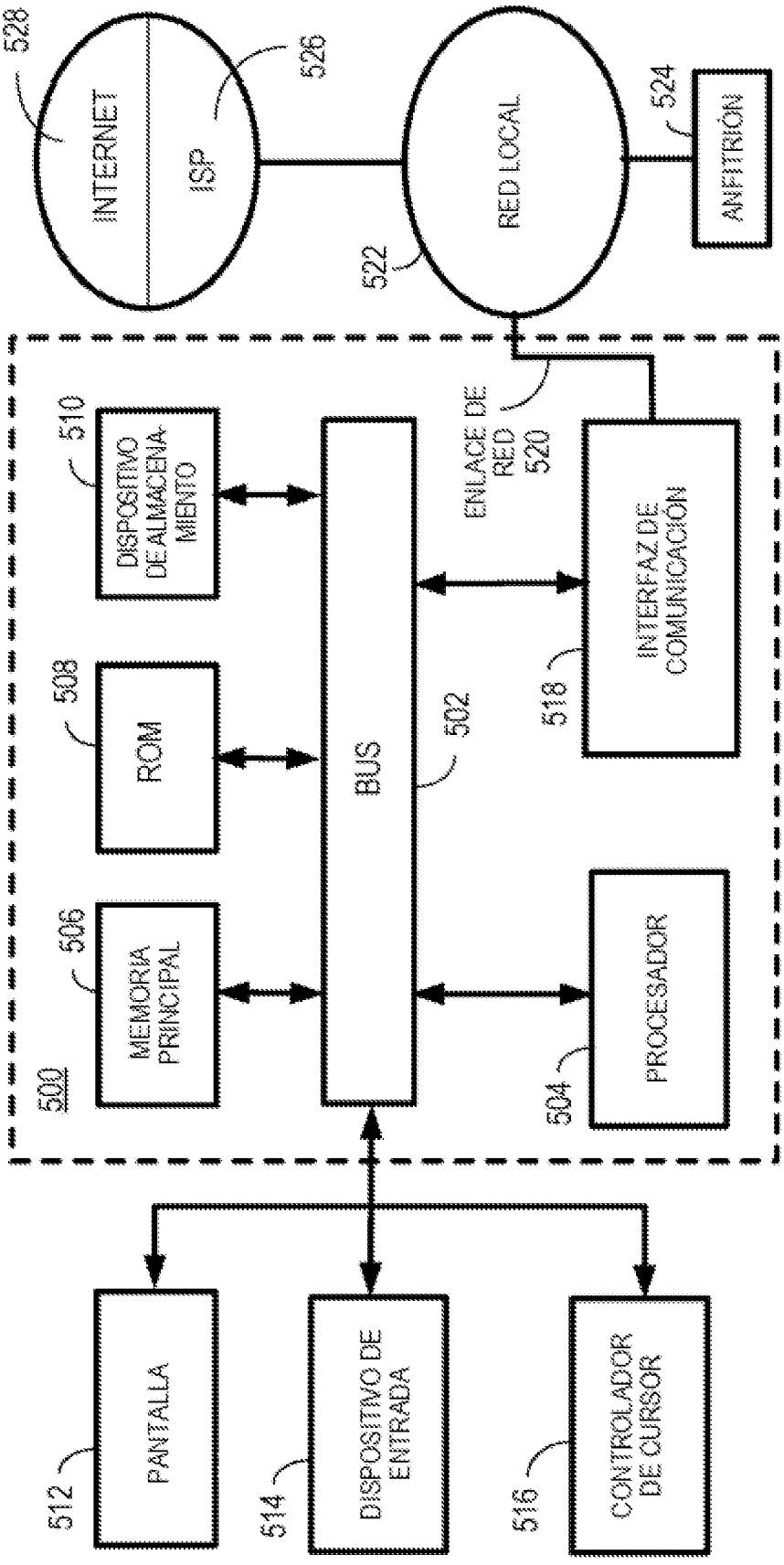
528
INTERNET
ISP
526
RED LOCAL
524
ANFITRIÓN
522
500
510
DISPOSITIVO DE ALMACENAMIENTO
508
ROM
506
MEMORIA PRINCIPAL
BUS
502
ENLACE DE RED 520
INTERFAZ DE COMUNICACIÓN
518
PROCESADOR
504
512
PANTALLA
514
DISPOSITIVO DE ENTRADA
516
CONTROLADOR DE CURSOR

FIG. 5