(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 869 166**

(51) Int. CI.:

H04L 9/32 (2006.01)
G06Q 20/06 (2012.01)
G06Q 20/10 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.01.2019 PCT/CN2019/074057**

(87) Fecha y número de publicación internacional: **18.04.2019 WO19072317**

(96) Fecha de presentación y número de la solicitud europea: **31.01.2019 E 19717101 (0)**

(97) Fecha y número de publicación de la concesión europea: **28.10.2020 EP 3602956**

(54) Título: **Comercio de activos cruzados dentro de redes de cadena de bloques**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.10.2021

(73) Titular/es:

ADVANCED NEW TECHNOLOGIES CO., LTD., (100.0%)
Cayman Corporate Centre, 27 Hospital Road
George Town, Grand Cayman KY1-9008, KY

(72) Inventor/es:

ZHANG, WENBIN;
LEI, HAO;
LI, LICHUN y
HUANG, ZHANGJIE

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Comercio de activos cruzados dentro de redes de cadena de bloques

ANTECEDENTES

Los sistemas de contabilidad distribuida (DLS), que también pueden denominarse redes de consenso y/o redes de cadena de bloques, permiten a las entidades participantes almacenar datos de forma segura e inmutable. Los DLS se conocen comúnmente como redes de cadena de bloques sin hacer referencia a un caso de uso en particular. Los tipos de ejemplo de redes de cadena de bloques pueden incluir redes de cadena de bloques públicas, redes de cadena de bloques privadas y redes de cadena de bloques de consorcio. Una red de cadena de bloques pública está abierta para que todas las entidades utilicen el DLS y participen en el proceso de consenso. Se proporciona una red de cadena de bloques privada para una entidad particular, que controla de forma centralizada los permisos de lectura y escritura. Se proporciona una red de cadena de bloques de consorcio para un grupo selecto de entidades, que controlan el proceso de consenso e incluye una capa de control de acceso.

Las redes de cadena de bloques se pueden utilizar para negociar valor a través de la transferencia y el intercambio de activos digitales, tal como divisas. Se pueden intercambiar varios tipos diferentes de activos digitales dentro de una red de cadena de bloques transfiriendo los activos digitales desde un nodo de una red de cadena de bloques a otro nodo. En algunos casos, la transferencia de activos digitales dentro de una red de cadena de bloques implica el intercambio de un tipo de activo digital por un segundo tipo de activo digital en base a un tipo de cambio.

Sin embargo, los participantes en una red de cadena de bloques pueden desear privacidad en sus transacciones, de modo que otros participantes, incluidos los nodos de consenso, desconozcan los detalles de la transacción (p. ej., cantidades de transacciones, tipos de cambio). Para proporcionar privacidad, se pueden utilizar esquemas de cifrado. Sin embargo, algunos esquemas de cifrado no soportan operaciones de multiplicación, tal como la multiplicación homomórfica. Aunque algunos esquemas de cifrado soportan tales operaciones de multiplicación, están limitados a una sola operación de multiplicación. Esto inhibe la capacidad de los participantes en una transacción de activos cruzados que incluye, por ejemplo, un tipo de cambio, para mantener la privacidad del tipo de cambio.

El documento CN 108335106 A de publicación de Solicitud de Patente China da a conocer un método de transferencia de canje de libros múltiples de conocimiento cero en base a una cadena de bloques.

S. Park, R. Rivest: "Towards Secure Quadratic Voting" da a conocer el uso del cifrado Boneh-Goh-Nissim, BGN, en aplicaciones de cadena de bloques que requieren una sólida preservación de la privacidad.

RESUMEN

Las implementaciones de esta memoria descriptiva incluyen métodos implementados por computadora para transferir divisa dentro de una red de cadena de bloques. Más particularmente, las implementaciones de esta memoria descriptiva están dirigidas a transacciones de activos cruzados dentro de una red de cadena de bloques utilizando datos de transacciones cifrados y tipos de cambio cifrados.

En algunas implementaciones, las acciones incluyen generar, por un primer nodo en la red de cadena de bloques y utilizando cifrado Boneh-Goh-Nissim (BGN), textos cifrados en base a un primer valor y un segundo valor, siendo el segundo valor determinado en base a una multiplicación homomórfica del primer valor y un tipo de cambio cifrado proporcionado por un segundo nodo en la red de cadena de bloques,
en donde los textos cifrados y el tipo de cambio cifrado están en una misma curva elíptica; transmitir, por el primer nodo al segundo nodo, el primer valor y los textos cifrados, recibir, por el primer nodo y desde el segundo nodo, un primer conjunto de evidencia que incluye un conjunto de datos que se pueden utilizar para verificar el tipo de cambio en un rutina de prueba de conocimiento cero (ZKP) sin revelar el tipo de cambio, generar, por el primer nodo, un segundo conjunto de evidencia que incluye un conjunto de datos que se pueden utilizar para verificar, utilizando la rutina ZKP, que los textos cifrados están cifrados por una clave pública de BGN del primer nodo, definir, por el primer nodo, una transacción que incluye una primera transacción entre el primer nodo y el segundo nodo para la transferencia del primer valor desde el primer nodo al segundo nodo, y una segunda transacción entre el segundo nodo y un tercer nodo para transferir el segundo valor desde el segundo nodo al tercer nodo, y transmitir, por el primer nodo, la transacción a al menos un nodo de consenso de la red de cadena de bloques para la verificación y ejecución de la transacción, verificándose la transacción en base al primer conjunto de evidencia y el segundo conjunto de evidencia, y en respuesta a la verificación de la transacción, ejecutar la primera transacción y la segunda transacción para disminuir un saldo del primer nodo por el primer valor, aumentar un primer saldo del segundo nodo por el primer valor, disminuir un segundo saldo del segundo nodo por el segundo valor y aumentar un saldo del tercer nodo por el segundo valor. Otras implementaciones incluyen sistemas, aparatos y programas informáticos correspondientes, configurados para realizar las acciones de los métodos, codificados en dispositivos de almacenamiento informáticos.

Cada una de estas y otras implementaciones puede incluir opcionalmente una o más de las siguientes características: el primer conjunto de evidencia lo proporciona el segundo nodo en base al primer valor, un par de números aleatorios

proporcionados por el primer nodo y los textos cifrados; verificar la transacción por el al menos un nodo de consenso incluye verificar una firma digital del primer nodo y una firma digital del segundo nodo; verificar la transacción por el al menos un nodo de consenso incluye verificar una primera prueba de rango proporcionada por el primer nodo y una segunda prueba de rango proporcionada por el segundo nodo; la primera prueba de rango incluye una ZKP para probar que el primer valor es mayor que cero, y que el saldo del primer nodo es mayor o igual que el primer valor; la segunda prueba de rango incluye una ZKP para probar que el segundo saldo del segundo nodo es mayor o igual que el segundo valor; la transacción incluye además un conjunto de datos que incluye un conjunto de textos cifrados generados al menos parcialmente en base al cifrado BGN, utilizándose el conjunto de datos para verificar la transacción por el al menos un nodo de consenso; las acciones incluyen además recibir, por el primer nodo, el tipo de cambio del segundo nodo a través de un canal de subcadena de la red de cadena de bloques; al menos un texto cifrado de los textos cifrados se proporciona utilizando el Compromiso de Pedersen; el conjunto de datos del primer conjunto de evidencia incluye un primer valor de datos y un segundo valor de datos, determinándose cada uno del primer valor de datos y del segundo valor de datos en base a los parámetros utilizados para generar una clave pública BGN del segundo nodo; y el conjunto de datos del segundo conjunto de evidencia incluye un conjunto de textos cifrados y un conjunto de valores, basándose cada uno de los valores en el conjunto de valores al menos parcialmente en un resumen del conjunto de textos cifrados

Esta memoria descriptiva también proporciona uno o más medios de almacenamiento legibles por computadora no transitorios acoplados a uno o más procesadores y que tienen instrucciones almacenadas en los mismos que, cuando se ejecutan por uno o más procesadores, hacen que el uno o más procesadores realicen operaciones de acuerdo con las implementaciones de los métodos proporcionados en el presente documento.

Esta memoria descriptiva proporciona además un sistema para implementar los métodos proporcionados en el presente documento. El sistema incluye uno o más procesadores y un medio de almacenamiento legible por computadora acoplado al uno o más procesadores que tiene instrucciones almacenadas en el mismo que, cuando se ejecutan por el uno o más procesadores, hacen que el uno o más procesadores realicen operaciones de acuerdo con las implementaciones de los métodos proporcionados en el presente documento.

Se aprecia que los métodos de acuerdo con esta memoria descriptiva pueden incluir cualquier combinación de los aspectos y características descritos en el presente documento. Es decir, los métodos de acuerdo con esta memoria descriptiva no se limitan a las combinaciones de aspectos y características descritas específicamente en el presente documento, sino que también incluyen cualquier combinación de los aspectos y características proporcionados.

Los detalles de una o más implementaciones de esta memoria descriptiva se establecen en los dibujos adjuntos y la descripción a continuación. Otras características y ventajas de esta memoria descriptiva serán evidentes a partir de la descripción y los dibujos, y de las reivindicaciones.

El alcance de la protección está definido por las reivindicaciones.

DESCRIPCION DE LOS DIBUJOS

FIG. 1 muestra un ejemplo de un entorno que se puede utilizar para ejecutar implementaciones de esta memoria descriptiva.
FIG. 2 representa un ejemplo de una arquitectura conceptual de acuerdo con implementaciones de esta memoria descriptiva.
FIG. 3 representa un ejemplo de una plataforma de comercio de activos cruzados de acuerdo con implementaciones de esta memoria descriptiva.
FIG. 4 representa un ejemplo de un diagrama de señales para ejecutar una transacción de activos cruzados de acuerdo con implementaciones de esta memoria descriptiva.
FIG. 5 representa un ejemplo de un proceso que se puede ejecutar de acuerdo con implementaciones de esta memoria descriptiva.
FIG. 6 representa ejemplos de módulos de un aparato de acuerdo con implementaciones de esta memoria descriptiva.

Los símbolos de referencia similares en los diversos dibujos indican elementos similares.

DESCRIPCIÓN DETALLADA

Las implementaciones de esta memoria descriptiva incluyen métodos implementados por computadora para transferir activos dentro de una red de cadena de bloques. Más particularmente, las implementaciones de esta memoria descriptiva están dirigidas a transacciones de activos cruzados dentro de una red de cadena de bloques utilizando datos de transacciones cifrados y tipos de cambio cifrados.

Para proporcionar un contexto adicional para las implementaciones de esta memoria descriptiva, y como se introdujo anteriormente, los sistemas de contabilidad distribuida (DLS), que también pueden denominarse redes de consenso (p. ej., compuestas por nodos de igual a igual) y redes de cadena de bloques, permiten realizar a entidades participantes transacciones de forma segura e inmutable y almacenar datos. Aunque el término cadena de bloques se

asocia generalmente con redes particulares y/o casos de uso, cadena de bloques se utiliza en el presente documento para referirse generalmente a un DLS sin referencia a un caso de uso particular.

Una cadena de bloques es una estructura de datos que almacena transacciones de manera que las transacciones sean inmutables. Por lo tanto, las transacciones registradas en una cadena de bloques son confiables y dignas de confianza. Una cadena de bloques incluye uno o más bloques. Cada uno de los bloques de la cadena está vinculado a un bloque anterior inmediatamente antes de él en la cadena al incluir un resumen criptográfico del bloque anterior. Cada uno de los bloques también incluye una marca de tiempo, su propio resumen criptográfico y una o más transacciones. Las transacciones, que ya han sido verificadas por los nodos de la red de cadena de bloques, se procesan y codifican en un árbol Merkle. Un árbol Merkle es una estructura de datos en la que los datos en los nodos hoja del árbol están resumidos, y todos los resúmenes en cada una de las ramas del árbol se concatenan en la raíz de la rama. Este proceso continúa subiendo por el árbol hasta la raíz de todo el árbol, que almacena un resumen que es representativo de todos los datos del árbol. Un resumen que pretende ser de una transacción almacenada en el árbol se puede verificar rápidamente determinando si es consistente con la estructura del árbol.

Mientras que una cadena de bloques es una estructura de datos descentralizada o al menos parcialmente descentralizada para almacenar transacciones, una red de cadenas de bloques es una red de nodos informáticos que gestionan, actualizan y mantienen una o más cadenas de bloques al transmitir, verificar y validar transacciones, etc. Una red de cadena de bloques de consorcio es privada entre las entidades participantes. En una red de cadena de bloques de consorcio, el proceso de consenso está controlado por un conjunto autorizado de nodos, uno o más nodos siendo operados por una respectiva entidad (p. ej., una institución financiera, una compañía de seguros). Por ejemplo, un consorcio de diez (10) entidades (p. ej., instituciones financieras, compañías de seguros) puede operar una red de cadena de bloques de consorcio, cada una de las cuales opera al menos un nodo en la red de cadena de bloques de consorcio. En consecuencia, la red de cadena de bloques de consorcio puede considerarse una red privada con respecto a las entidades participantes. En algunos ejemplos, cada una de las entidades (nodo) debe firmar cada uno de los bloques para que el bloque sea válido y se añada a la cadena de bloques. En algunos ejemplos, al menos un subconjunto de entidades (nodos) (p. ej., al menos 7 entidades) debe firmar cada uno de los bloques para que el bloque sea válido y se añada a la cadena de bloques.

Como se presentó anteriormente, una red de cadena de bloques se puede proporcionar como una red de cadena de bloques pública, una red de cadena de bloques privada o una red de cadena de bloques de consorcio. Las implementaciones de esta memoria descriptiva se describen con más detalle en el presente documento con referencia a una red de cadena de bloques de consorcio. Sin embargo, se contempla que las implementaciones de esta memoria descriptiva se puedan realizar en cualquier tipo apropiado de red de cadena de bloques. Aunque las técnicas descritas en esta memoria descriptiva se indican como relevantes para las redes de cadena de bloques de consorcio, las técnicas también se pueden utilizar, con o sin cambios, en otros tipos de redes de cadena de bloques, incluidas las redes de cadena de bloques públicas y las redes de cadena de bloques privadas.

En general, una red de cadena de bloques de consorcio es privada entre las entidades participantes. En una red de cadena de bloques de consorcio, el proceso de consenso está controlado por un conjunto autorizado de nodos, que pueden denominarse nodos de consenso, siendo uno o más nodos de consenso operados por una respectiva entidad (p. ej., una institución financiera, una compañía de seguros). Por ejemplo, un consorcio de diez (10) entidades (p. ej., instituciones financieras, compañías de seguros) puede operar una red de cadena de bloques de consorcio, cada una de las cuales opera al menos un nodo en la red de cadena de bloques del consorcio.

En algunos ejemplos, dentro de una red de cadena de bloques de consorcio, se proporciona una cadena de bloques global como una cadena de bloques que se replica en todos los nodos. Es decir, todos los nodos de consenso están en perfecto estado de consenso con respecto a la cadena de bloques global. Para lograr el consenso (p. ej., acuerdo para la adición de un bloque a una cadena de bloques), se implementa un protocolo de consenso dentro de la red de cadena de bloques de consorcio. Los protocolos de consenso de ejemplo incluyen, sin limitación, tolerancia práctica a fallas bizantinas (PBFT), prueba de trabajo (POW), prueba de participación (POS) y prueba de autoridad (POA).

Las redes de cadena de bloques de consorcio se pueden utilizar para realizar transferencias e intercambios de activos digitales. En algunos casos, un activo digital puede representar un activo del mundo real. En algunos casos, un activo digital puede representar un activo virtual. Por ejemplo, los activos virtuales pueden representar valor en el mundo real y pueden utilizarse para comprar productos y/o servicios. Los activos virtuales se proporcionan como una alternativa a los activos físicos del mundo real (p. ej., RMB chino, dólar estadounidense). La realización de transacciones dentro de una red de cadena de bloques de consorcio proporciona seguridad adicional, ya que la red de cadena de bloques de consorcio verifica y registra de manera inmutable la transacción. Las implementaciones de esta memoria descriptiva se describen con más detalle en el presente documento con referencia a divisas (p. ej., RMB, USD). Sin embargo, se contempla que las implementaciones se puedan realizar con cualquier activo digital apropiado.

FIG. 1 representa un ejemplo de un entorno 100 que puede utilizarse para ejecutar implementaciones de esta memoria descriptiva. En algunos ejemplos, el entorno 100 permite a las entidades participar en una red 102 de cadena de bloques de consorcio. El entorno 100 incluye dispositivos 106, 108 informáticos y una red 110. En algunos ejemplos, la red 110 incluye una red de área local (LAN), red de área amplia (WAN), el Internet o una combinación de las mismas,

y conecta sitios web, dispositivos de usuario (p. ej., dispositivos informáticos) y sistemas de servidor. En algunos ejemplos, se puede acceder a la red 110 a través de un enlace de comunicaciones cableado y/o inalámbrico.

En el ejemplo representado, los sistemas 106, 108 informáticos pueden incluir cada uno cualquier sistema informático apropiado que permita la participación como nodo en la red 102 de cadena de bloques de consorcio. Los dispositivos informáticos de ejemplo incluyen, sin limitación, un servidor, una computadora de escritorio, una computadora portátil, un dispositivo informático tableta y un teléfono inteligente. En algunos ejemplos, los sistemas 106, 108 informáticos alojan uno o más servicios implementados por computadora para interactuar con la red 102 de cadena de bloques de consorcio. Por ejemplo, el sistema 106 informático puede alojar servicios implementados por computadora de una primera entidad (p. ej., el usuario A) , tal como un sistema de gestión de transacciones que utiliza la primera entidad para gestionar sus transacciones con una o más entidades (p. ej., otros usuarios) distintas. El sistema 108 informático puede alojar servicios implementados por computadora de una segunda entidad (p. ej., el usuario B), tal como un sistema de gestión de transacciones que la segunda entidad utiliza para gestionar sus transacciones con una o más entidades (p. ej., otros usuarios) distintas. En el ejemplo de la FIG. 1, la red 102 de cadena de bloques de consorcio se representa como una red de nodos de igual a igual, y los sistemas 106, 108 informáticos proporcionan nodos de la primera entidad y la segunda entidad, respectivamente, que participan en la red 102 de cadena de bloques de consorcio.

FIG. 2 representa un ejemplo de una arquitectura 200 conceptual de acuerdo con implementaciones de esta memoria descriptiva. La arquitectura 200 conceptual incluye una capa 202 de entidad, una capa 204 de servicios alojados y una capa 206 de red de cadena de bloques. En el ejemplo representado, la capa 202 de entidad incluye tres participantes, Participante A, Participante B y Participante C, cada uno de los participantes tiene un respectivo sistema 208 de gestión de transacciones.

En el ejemplo representado, la capa 204 de servicios alojados incluye interfaces 210 para cada uno de los sistemas 210 de gestión de transacciones. En algunos ejemplos, un respectivo sistema 208 de gestión de transacciones se comunica con una respectiva interfaz 210 a través de una red (p. ej., la red 110 de la FIG 1)). En algunos ejemplos, cada una de las interfaces 210 proporciona una conexión de comunicación entre un respectivo sistema 208 de gestión de transacciones y la capa 206 de red de cadena de bloques. Más particularmente, la interfaz 210 se comunica con una red 212 de cadena de bloques de la capa 206 de red de cadena de bloques. En algunos ejemplos, la comunicación entre una interfaz 210 y la capa 206 de red de cadena de bloques se realiza utilizando llamadas a procedimiento remoto (RPC). En algunos ejemplos, las interfaces 210 "alojan" los nodos de red de la cadena de bloques para los respectivos sistemas 208 de gestión de transacciones. Por ejemplo, las interfaces 210 proporcionan la interfaz de programación de aplicaciones (API) para acceder a la red 212 de cadena de bloques.

Como se describe en el presente documento, la red 212 de cadena de bloques se proporciona como una red de igual a igual que incluye una pluralidad de nodos 214 que registran información de manera inmutable en una cadena 216 de bloques. Aunque se representa esquemáticamente una única cadena 216 de bloques, se proporcionan múltiples copias de la cadena 216 de bloques y se mantienen a través de la red 212 de cadena de bloques. Por ejemplo, cada uno de los nodos 214 almacena una copia de la cadena de bloques. En algunas implementaciones, la cadena 216 de bloques almacena información asociada con las transacciones que se realizan entre dos o más entidades que participan en la red de cadena de bloques de consorcio.

Una cadena de bloques (p. ej., la cadena 216 de bloques de la FIG. 2) está formada por una cadena de bloques, cada uno de los bloques almacena datos. Los datos de ejemplo incluyen datos de transacciones representativos de una transacción entre dos o más participantes. Si bien las transacciones se utilizan en el presente documento a modo de ejemplo no limitativo, se contempla que cualquier dato apropiado se pueda almacenar en una cadena de bloques (p. ej., documentos, imágenes, vídeos, audio). Las transacciones de ejemplo pueden incluir, sin limitación, intercambios de algo de valor (p. ej., activos, productos, servicios, divisas). Los datos de transacción se almacenan de forma inmutable dentro de la cadena de bloques. Es decir, los datos de transacción no se pueden cambiar.

Antes de almacenarlos en un bloque, los datos de transacción se resumen. El resumen es un proceso de transformación de los datos de transacción (proporcionados como datos de cadena) en un valor de resumen de longitud fija (también proporcionado como datos de cadena). No es posible deshacer el resumen del valor de resumen para obtener los datos de transacción. El resumen asegura que incluso un pequeño cambio en los datos de transacción da como resultado un valor de resumen completamente diferente. Además, y como se indicó anteriormente, el valor de resumen es de longitud fija. Es decir, no importa el tamaño de los datos de transacción, la longitud del valor de resumen es fija. El resumen incluye procesar los datos de transacción a través de una función de resumen para generar el valor de resumen. Un ejemplo de función de resumen incluye, sin limitación, el algoritmo de resumen seguro (SHA)-256, que genera valores de resumen de 256 bits.

Los datos de transacción de múltiples transacciones se resumen y almacenan en un bloque. Por ejemplo, se proporcionan valores de resumen de dos transacciones y ellos mismos se resumen para proporcionar otro resumen. Este proceso se repite hasta que, para que todas las transacciones a ser almacenadas en un bloque, se proporciona un único valor de resumen. Este valor de resumen se denomina resumen de raíz de Merkle y se almacena en un

encabezado del bloque. Un cambio en cualquiera de las transacciones dará como resultado un cambio en su valor de resumen y, en última instancia, un cambio en el resumen de raíz de Merkle.

Los bloques se agregan a la cadena de bloques a través de un protocolo de consenso. Múltiples nodos dentro de la red de cadena de bloques participan en el protocolo de consenso y realizan un trabajo para añadir un bloque a la cadena de bloques. Dichos nodos se denominan nodos de consenso. PBFT, presentado anteriormente, se utiliza como un ejemplo no limitativo de un protocolo de consenso. Los nodos de consenso ejecutan el protocolo de consenso para añadir transacciones a la cadena de bloques.

Con más detalle, el nodo de consenso genera un encabezado de bloque, resume todas las transacciones en el bloque y combina el valor de resumen en pares para generar valores de resumen adicionales hasta que se proporciona un solo valor de resumen para todas las transacciones en el bloque (el resumen de raíz de Merkle). Este resumen se añade al encabezado del bloque. El nodo de consenso también determina el valor de resumen del bloque más reciente en la cadena de bloques (es decir, el último bloque añadido a la cadena de bloques). El nodo de consenso también añade un valor nonce y una marca de tiempo al encabezado de bloque.

En general, PBFT proporciona una replicación de máquina de estado bizantina práctica que tolera fallas bizantinas (p. ej., nodos defectuosos, nodos maliciosos). Esto se logra en PBFT asumiendo que ocurrirán fallas (p. ej., asumiendo la existencia de fallas de nodos independientes y/o mensajes manipulados enviados por nodos de consenso). En PBFT, los nodos de consenso se proporcionan en una secuencia que incluye un nodo de consenso primario y nodos de consenso de respaldo. El nodo de consenso primario se cambia periódicamente, las transacciones se añaden a la cadena de bloques por todos los nodos de consenso dentro de la red de la cadena de bloques y llegan a un acuerdo sobre el estado mundial de la red de cadena de bloques. En este proceso, los mensajes se transmiten entre los nodos de consenso y cada uno de los nodos de consenso prueba que se recibe un mensaje desde un nodo igual especificado y verifica que el mensaje no se modificó durante la transmisión.

En PBFT, el protocolo de consenso se proporciona en múltiples fases con todos los nodos de consenso comenzando en el mismo estado. Para comenzar, un cliente envía una solicitud al nodo de consenso primario para invocar una operación de servicio (p. ej., ejecutar una transacción dentro de la red de cadena de bloques). En respuesta a la recepción de la solicitud, el nodo de consenso primario transmite la solicitud a los nodos de consenso de respaldo. Los nodos de consenso de respaldo ejecutan la solicitud y cada uno envía una respuesta al cliente. El cliente espera hasta que se recibe un número umbral de respuestas. En algunos ejemplos, el cliente espera que se reciban $f + 1$ respuestas, donde f es el número máximo de nodos de consenso defectuosos que se pueden tolerar dentro de la red de cadena de bloques. El resultado final es que una cantidad suficiente de nodos de consenso llegan a un acuerdo sobre el orden del registro que se añadirá a la cadena de bloques, y el registro se acepta o se rechaza.

En algunas redes de cadena de bloques, la criptografía se implementa para mantener la privacidad de las transacciones. Por ejemplo, si dos nodos quieren mantener una transacción privada, de modo que otros nodos en la red de cadena de bloques no puedan discernir los detalles de la transacción, los nodos pueden cifrar los datos de transacción. La criptografía de ejemplo incluye, sin limitación, cifrado simétrico y cifrado asimétrico. El cifrado simétrico se refiere a un proceso de cifrado que utiliza una única clave tanto para el cifrado (generar texto cifrado a partir del texto plano) como para el descifrado (generar texto plano a partir del texto cifrado). En el cifrado simétrico, la misma clave está disponible para múltiples nodos, de modo que cada uno de los nodos puede cifrar/descifrar datos de transacción.

El cifrado asimétrico utiliza pares de claves, cada uno de los cuales incluye una clave privada y una clave pública, siendo la clave privada conocida solo por un respectivo nodo y la clave pública siendo conocida por cualquiera o todos los demás nodos en la red de cadena de bloques. Un nodo puede utilizar la clave pública de otro nodo para cifrar datos, y los datos cifrados se pueden descifrar utilizando la clave privada de otro nodo. Por ejemplo, y haciendo referencia de nuevo a la FIG. 2, el participante A puede utilizar la clave pública del participante B para cifrar los datos y enviar los datos cifrados al participante B. El participante B puede utilizar su clave privada para descifrar los datos cifrados (texto cifrado) y extraer los datos originales (texto plano). Los mensajes cifrados con la clave pública de un nodo solo se pueden descifrar utilizando la clave privada del nodo.

El cifrado asimétrico se utiliza para proporcionar firmas digitales, lo que permite a los participantes en una transacción confirmar a otros participantes en la transacción, así como la validez de la transacción. Por ejemplo, un nodo puede firmar digitalmente un mensaje y otro nodo puede confirmar que el mensaje fue enviado por el nodo en base la firma digital del Participante A. Las firmas digitales también se pueden utilizar para garantizar que los mensajes no sean manipulados en tránsito. Por ejemplo, y haciendo referencia de nuevo a la FIG. 2, el participante A debe enviar un mensaje al participante B. El participante A genera un resumen del mensaje y luego, utilizando su clave privada, cifra el resumen para proporcionar una firma digital como resumen cifrado. El participante A agrega la firma digital al mensaje y envía el mensaje con la firma digital al participante B. El participante B descifra la firma digital utilizando la clave pública del participante A y extrae el resumen. El participante B resume el mensaje y compara los resúmenes. Si los resúmenes son iguales, el participante B puede confirmar que el mensaje era realmente del participante A y que no se manipuló.

Al igual que con las transferencias de divisa físicas del mundo real, la transferencia efectiva de una representación digital de una divisa a veces requiere que el cesionario cambie un primer tipo de divisa por un segundo tipo de divisa. Por ejemplo, un primer miembro de una red de cadena de bloques de consorcio (p. ej., Participante A) que solo tiene un primer tipo de divisa (p. ej., dólares estadounidenses ($)) puede querer transferir divisa a un segundo miembro de la red de cadena de bloques de consorcio (p. ej., Participante C) en un segundo tipo de divisa (p. ej., RMB chino). Para que el Participante A transfiera valor al Participante C, se cambia una cantidad del primer tipo de divisa por un valor equivalente del segundo tipo de divisa antes de la transferencia al Participante C.

De acuerdo con las implementaciones de esta memoria descriptiva, y como se describe con más detalle en el presente documento, el intercambio de tipos de divisas se puede lograr a través de un tercer miembro de la red de cadena de bloques de consorcio (p. ej., el Participante B) como intermediario. Por ejemplo, el participante A puede transferir una cantidad del primer tipo de divisa al participante B, y el participante B puede transferir al participante C una cantidad del segundo tipo de divisa que tenga un valor equivalente en base a un tipo (ER) de cambio utilizado por el Participante B. En algunos ejemplos, el Participante B es una institución financiera que brinda servicios de cambio de divisa a los miembros de una red de cadena de bloques de consorcio.

Para garantizar la privacidad de las partes involucradas en los intercambios de divisas dentro de las redes de cadena de bloques, los datos de transacción subyacentes a los intercambios se cifran antes de la verificación y publicación del intercambio dentro de la red de cadena de bloques. En algunos ejemplos, los datos de transacción incluyen la cantidad transferida de la primera divisa (t_1) y la cantidad de una segunda divisa (t_2) proporcionada a cambio de la primera cantidad. Por lo general, los datos de transacción enviados a la cadena de bloques para su verificación se cifran mediante un esquema de cifrado homomórfico, tal como el cifrado Boneh-Goh-Nissim (BGN). Bajo esquemas de cifrado homomórfico, dos o más elementos de datos cifrados se pueden añadir juntos sin limitación. A diferencia de otros esquemas de cifrado (p. ej., cifrado de clave pública (PKE) de Paillier), el cifrado BGN permite la multiplicación homomórfica sobre dos textos cifrados (p. ej., multiplicación de β cifrado y t_1 cifrado). Sin embargo, los elementos de datos cifrados utilizando cifrado homomórfico se limitan a una sola multiplicación. Esto se debe a que el emparejamiento multiplicativo de dos elementos de datos cifrados utilizando cifrado homomórfico genera un producto cifrado que es de un orden diferente al de los multiplicadores cifrados.

La siguiente ecuación demuestra la naturaleza de una sola vez del homomorfismo multiplicativo, que generalmente se denomina emparejamiento en la curva elíptica

$\mathcal{G}$

:

$$e: \mathcal{G} \times \mathcal{G} \longrightarrow \mathcal{G}_1$$

donde cada uno de los elementos de datos cifrados que se multiplica se encuentra en una curva elíptica diferente

$\mathcal{G}$

que el producto de la multiplicación que está en

$\mathcal{G}_1$

. Los elementos de datos cifrados generados por el homomorfismo multiplicativo no se pueden multiplicar ni dividir adicionalmente debido a este cambio de las curvas elípticas subyacentes. Además, los elementos de datos cifrados generados por el homomorfismo multiplicativo no se pueden comparar con los elementos de datos generados por el cifrado homomórfico directo. Por ejemplo, los dos primeros elementos de datos cifrados en la ecuación anterior en la misma curva elíptica

$\mathcal{G}$

se pueden comparar entre sí, pero no se pueden comparar con el tercer elemento de datos cifrados en la curva elíptica

$\mathcal{G}_1$

generado por homomorfismo multiplicativo debido a la diferencia en las curvas elípticas subyacentes

$\mathcal{G}$

y

$\mathcal{G}_1$

.

En el cifrado BGN, cada uno de los participantes i que va a utilizar el cifrado BGN recibe una clave pública (PK) BGN, un par de claves privadas (SK) (p. ej., PK_{BGN_i}, SK_{BGN_o}) a través de un proceso de generación de claves. A través del proceso de generación de claves, se proporciona lo siguiente:

$$PK_{BGN_i} = \{N, \mathcal{G}, \mathcal{G}_1, e, P, Q\}_i$$

$$SK_{BGN\_i} = p$$

dónde:

$N = pq$

p, q son números primos grandes

$\mathcal{G}$
una curva elíptica de orden *N*

$e: \mathcal{G} \times \mathcal{G} \longrightarrow \mathcal{G}_1$
es una pareja

$P \in \mathcal{G}$
un generador
$Q = q\alpha P$ (un generador aleatorio de un subgrupo de
$\mathcal{G}$
cuyo orden es p)
$\alpha < N$

En el contexto de esta memoria descriptiva, bajo esquemas de cifrado homomórfico, las transacciones de intercambio que involucran un tipo de cambio público pueden ser verificadas y registradas por una red de cadena de bloques de consorcio sin revelar o publicar la cantidad transferida y/o las cantidades intercambiadas. Por ejemplo, tanto la cantidad de una primera divisa (t_1) transferida por el Participante A al proveedor de servicios de cambio Participante B, como la cantidad de una segunda divisa (t_2) proporcionada por el Participante B a cambio de la primera cantidad se pueden cifrar utilizando cifrado homomórfico. Bajo este esquema, tanto t_1 cifrado como t_2 cifrado están en la curva elíptica
$\mathcal{G}$
. La cantidad t_1 de transferencia cifrada se puede multiplicar por un tipo de cambio público del Participante B para determinar la cantidad de la segunda divisa que debe proporcionar el Participante B a cambio de t_1. Debido a que el tipo de cambio del participante B es un valor público no cifrado en este ejemplo, el producto de t_1 y el tipo de cambio público es un elemento de datos cifrado que está una misma curva elíptica
$\mathcal{G}$
t_1. La transacción de intercambio entre el Participante A y el Participante B puede ser verificada por la red de cadena de bloques comparando el producto cifrado de t_1 y el tipo de cambio público con el elemento t_2 de datos cifrado. Si el producto cifrado de t_1 multiplicado por el tipo de cambio público es igual al elemento t_2 de datos cifrados, entonces la transacción se verifica y se registra en la cadena de bloques.

Si bien este esquema de verificación proporciona un medio eficaz para verificar las transacciones de cambio que involucran tipos de cambio públicos, los miembros de la red de cadena de bloques que proporcionar servicios de cambio de divisas a menudo compiten con otros proveedores similares. En consecuencia, no quieren que sus tipos de cambio sean públicos dentro de la red de cadena de bloques. Por lo tanto, es deseable que el tipo de cambio, así como los datos de transacción, estén cifrados para las transacciones de intercambio realizadas dentro y verificadas por una red de cadena de bloques.

Sin embargo, cuando se utiliza la verificación descrita anteriormente, la limitación de la multiplicación única para el cifrado homomórfico crea una barrera para la verificación de las transacciones de intercambio, en las que tanto los datos de transacción como el tipo de cambio se cifran mediante cifrado homomórfico. Por ejemplo, la cantidad de una primera divisa (t_1) transferida por el Participante A al proveedor de servicios de cambio Participante B, la cantidad de una segunda divisa (t_2), por la cual el Participante B cambió la cantidad transferida de la primera divisa, y el tipo de cambio (β) del Participante B pueden cifrarse cada uno utilizando cifrado homomórfico. Bajo este esquema, t_1 cifrado, t_2 cifrado y β cifrado están todos en la misma curva elíptica
$\mathcal{G}$
.

Como se discutió anteriormente, siempre que el tipo de cambio involucrado en la transacción de intercambio sea público, la transacción de intercambio puede ser verificada por la red de cadena de bloques comparando el producto de t_1 y un tipo de cambio público con el elemento t_2 de datos cifrados. Sin embargo, cuando el tipo de cambio está cifrado (β), el producto de t_1 y el tipo de cambio cifrado (β) está en la curva elíptica
$\mathcal{G}_1$
que difiere de la curva subyacente
$\mathcal{G}$
de t_2. En base a esta diferencia de orden resultante del homomorfismo multiplicativo, el producto de t_1 multiplicado por el tipo de cambio cifrado (β) no se puede comparar con t_2. Como resultado, bajo los esquemas de verificación actuales, la verificación de las transacciones de intercambio que involucran el cifrado tanto de los datos de transacción como del tipo de cambio no se puede realizar dentro de una red de cadena de bloques.

En vista del contexto anterior, y como se describe con más detalle en el presente documento, las implementaciones de esta memoria descriptiva están dirigidas al comercio de activos cruzados dentro de una red de cadena de bloques utilizando datos de transacción cifrados y tipos de cambio cifrados. Más particularmente, la plataforma de comercio de activos cruzados de esta memoria descriptiva permite transacciones que se pueden realizar con verificación de tipo de cambio privada (cifrada).

FIG. 3 representa un ejemplo de una plataforma 300 de comercio de activos cruzados de acuerdo con implementaciones de esta memoria descriptiva. En el ejemplo representado, la plataforma 300 de comercio de activos cruzados de ejemplo incluye tres participantes, el participante A, el participante B y el participante C, asociados con los respectivos dispositivos 302, 304, 306. La plataforma 300 de comercio de activos cruzados de ejemplo también incluye un canal 308 de subcadena, una red 310 y una red 312 de cadena de bloques de consorcio.

En algunos ejemplos, la red 310 incluye una red de área local (LAN), red de área amplia (WAN), el Internet o una combinación de las mismas, y conecta sitios web, dispositivos de usuario (p. ej., dispositivos informáticos) y sistemas de servidor. En algunos ejemplos, se puede acceder a la red 110 a través de un enlace de comunicaciones cableado y/o inalámbrico.

Como se describe en el presente documento, la red 312 de cadena de bloques se proporciona como una red de igual a igual que incluye una pluralidad de nodos 314 que registran información de manera inmutable en una cadena 322 de bloques. Aunque se representa esquemáticamente una única cadena 322 de bloques, se proporcionan múltiples copias de la cadena 322 de bloques y se mantienen a través de la red 312 de cadena de bloques. Por ejemplo, cada uno de los nodos 314 almacena una copia de la cadena 322 de bloques. En algunas implementaciones, la cadena 322 de bloques almacena información asociada con transacciones que se realizan entre dos o más entidades que participan en la red 312 de cadena de bloques de consorcio. En algunos ejemplos, los dispositivos 302, 304, 306 son parte de los respectivos nodos 314 en la red 312 de cadena de bloques de consorcio.

En algunas implementaciones, el dispositivo 302, el dispositivo 304 y el dispositivo 306 incluyen las respectivas cuentas, Cuenta 316 A , Cuenta 318 B y Cuenta 320 C. En algunos ejemplos, la Cuenta 316 A, la Cuenta 318 B y la Cuenta 320 C almacenan activos financieros. En algunos ejemplos, la Cuenta 316 A, la Cuenta 318 B y la Cuenta 320 C almacenan cantidades de uno o más tipos de divisa.

En algunas implementaciones, el canal 308 de subcadena se puede utilizar para transferir información fuera de la red 312 de cadena de bloques entre dos miembros de la red 312 de cadena de bloques de consorcio. En algunos ejemplos, la información financiera privada se puede transferir desde un miembro de la red 312 de cadena de bloques de consorcio a otro miembro de la red 312 de cadena de bloques de consorcio fuera de la red 312 de cadena de bloques a través del canal 308 de subcadena. Por ejemplo, el dispositivo 304 puede transferir un tipo de cambio privado (β) al dispositivo 302 fuera de la red 312 de cadena de bloques transmitiendo el tipo de cambio sobre el canal 308 de subcadena.

En algunos ejemplos, una transacción entre dos o más miembros de la red 312 de cadena de bloques de consorcio puede enviarse a la red 312 de cadena de bloques para verificación y registro. En algunos ejemplos, una transacción de intercambio de activos (p. ej., divisa) entre dos o más miembros de la red 312 de cadena de bloques de consorcio puede enviarse a la red 312 de cadena de bloques para la verificación del intercambio. En algunos ejemplos, la información de transacción enviada a la red 312 de cadena de bloques está cifrada. En algunos ejemplos, la información de transacción enviada a la red 312 de cadena de bloques se cifra mediante cifrado homomórfico. En algunos ejemplos, la información de transacción incluye un tipo de cambio, una primera cantidad a ser transferida y una segunda cantidad a ser transferida. En algunos ejemplos, la segunda cantidad a transferir es igual al producto de la primera cantidad multiplicada por el tipo de cambio.

FIG. 4 representa un ejemplo de un diagrama 400 de señales para ejecutar una transacción de activos cruzados de acuerdo con implementaciones de esta memoria descriptiva. El diagrama 400 de señales de la FIG. 4 incluye una Cuenta 402 A (p. ej., un nodo en una red de cadena de bloques), una cuenta 404 B (p. ej., un nodo en la red de cadena de bloques) y un nodo 406 de consenso de la red de cadena de bloques. En algunos ejemplos, la Cuenta 402 A y la Cuenta 404 B se utilizan para gestionar activos de los participantes en la red de cadena de bloques (p. ej., Participante A y Participante B, respectivamente). En algunos ejemplos, la Cuenta 402 A y la Cuenta 404 B almacenan activos digitales del Participante A y del Participante B, respectivamente. En algunos ejemplos, el participante B es una institución financiera.

Un ejemplo de una transacción de activos cruzados se describe con más detalle en el presente documento con referencia a la FIG. 4. En la transacción de ejemplo, una cantidad (t_1) en una primera divisa (p. ej., USD) se transfiere desde la Cuenta A a una cuenta de otro participante en la red de cadena de bloques (p. ej., Participante C) en una cantidad (t_2) en una segunda divisa (p. ej., RMB). La cantidad (t_1) se transfiere utilizando la Cuenta 404 B, un intermediario, que proporciona un tipo de cambio privado (β) entre la primera divisa y la segunda divisa. La Cuenta 402 A incluye una cantidad de saldo (s_A), que es un saldo de valor en la primera divisa que la Cuenta 402 A tiene disponible. La Cuenta 404 B incluye una primera cantidad (s_{B1}) de saldo, que es un saldo de valor en la primera divisa

que la Cuenta 404 B tiene disponible, y una segunda cantidad (s_{B2}) de saldo, que es un saldo de valor en la segunda divisa que la Cuenta 404 B tiene disponible.

En la transacción de activos cruzados de ejemplo, el tipo de cambio privado (β) se transmite (408) desde la Cuenta 404 B a la Cuenta 402 A. El mensaje que transporta el tipo de cambio privado puede transmitirse a través de una red. En algunos ejemplos, el mensaje que transporta el tipo de cambio privado se transmite a través de un canal de subcadena (p. ej., el canal 308 de subcadena de la FIG. 3).

La cuenta A 402 genera (410) dos números (r_1, r_2) aleatorios. La cuenta de A 402 calcula (412) una cantidad (t_2) de cambio y conjuntos de textos cifrados (X_1, Y_1, Z_1) y (X_2, Y_2, Z_2). En algunas implementaciones, la cantidad (t_2) de cambio es igual al producto de la cantidad (t_1) a ser transferida y el tipo (β) de cambio privado como se muestra a continuación:

$$t_2 = \beta t_1$$

En algunas implementaciones, los conjuntos de textos cifrados (X_1, Y_1, Z_1) y (X_2, Y_2, Z_2) se determinan en base a un esquema de compromiso y un esquema de cifrado. Un esquema de compromiso de ejemplo incluye, sin limitación, el Compromiso de Pedersen (PC). Un esquema de cifrado de ejemplo incluye, sin limitación, el cifrado BGN. Para el cifrado BGN, cada uno de los participantes incluye un par de clave pública (PK) y clave privada (SK) BGN. Por ejemplo, la Cuenta 402 A tiene un par PK-SK BGN (p. ej., PK_{BGN_A}, SK_{BCN_A}) asignado, la Cuenta 404 B tiene un par BGN PK-SK (p. ej., PK_{BGN_B}, SK_{BGN_B}) asignado a la misma, y la Cuenta C (no representada en la FIG.

En algunas implementaciones, los conjuntos de textos cifrados (X_1, Y_1, Z_1) y (X_2, Y_2, Z_2) se determinan respectivamente como:

$$(X_1, Y_1, Z_1) = \big(PC(t_1, r_1), BGN_A(t_1, r_1), BGN_B(t_1, r_1)\big)$$

$$(X_2, Y_2, Z_2) = \big(PC(t_2, r_2), BGN_B(t_2, r_2), BGN_C(t_2, r_2)\big)$$

La notación $PC(t, r)$ indica el compromiso de Pedersen de t con un número aleatorio r como factor ciego. La notación BGN_A indica cifrado BGN utilizando la clave pública de la Cuenta 402 A, la notación BGN_B indica cifrado BGN utilizando la clave pública de la Cuenta 404 B y la notación BGN_C indica cifrado BGN utilizando la clave pública de la Cuenta C. En algunos ejemplos, la Cuenta 402 A proporciona un texto cifrado de saldo como:

$$\big(PC(s_A, \bar{r}_A), BGN_A(s_A, \bar{r}_A)\big)$$

donde r_A es un número aleatorio generado por la Cuenta 402 A.

Los subconjuntos de textos cifrados (X_1, Z_1) y (X_2, Y_2), los números (r_1, r_2) aleatorios y la cantidad (t_1) se envían (414) desde la Cuenta 402 A a la Cuenta 404 B. En algunas implementaciones, el mensaje desde la Cuenta 402 A a la Cuenta 404 B es un mensaje cifrado (p. ej., utilizando el cifrado asimétrico descrito anteriormente). En algunos ejemplos, el mensaje se transmite a través de un canal de subcadena (p. ej., el canal 308 de subcadena de la FIG. 3). En algunos ejemplos, el mensaje (cifrado) incluye el conjunto [t_1, r_1, r_2, X_1, Z_1, X_2, Y_2] de datos.

La cuenta B descifra el mensaje para revelar los datos (p. ej., [t_1, r_1, r_2, X_1, Z_1, X_2, Y_2]). Los datos de texto cifrado se verifican (416) por la Cuenta 404 B. En algunos ejemplos, la Cuenta 404 B verifica los datos de texto cifrado comprobando si los textos cifrados X_1, Z_1, X_2, Y_2 son correctos en base a t_1, r_1, r_2 proporcionados por la Cuenta 402 A. Es decir, la Cuenta B recalcula X_1, Z_1, X_2, Y_2 y determina si son iguales a lo que se recibió desde la Cuenta 402 A. Si los textos cifrados son no son iguales, se puede enviar un error a la cuenta A y la transacción finaliza.

Si se verifican los textos cifrados, la Cuenta 404 B genera (418) una prueba (RP_B) de rango. En algunas implementaciones, la prueba (RP_B) de rango es una prueba de conocimiento cero (ZKP) que se puede utilizar para confirmar si la Cuenta 404 B tiene fondos suficientes para realizar la transacción de intercambio. Por ejemplo, la prueba (RP_B) de rango se puede generar para probar lo siguiente:

$$s_{B_2} - t_2 \geq 0$$

En algunos ejemplos, la Cuenta 404 B proporciona un primer texto cifrado de saldo y un segundo texto cifrado de saldo, respectivamente como:

$$\Big(PC\big(s_{B_1}, \bar{r}_{B_1}\big), BGN_B\big(s_{B_1}, \bar{r}_{B_1}\big)\Big)$$

$$\Big(PC\big(s_{B_2}, \bar{r}_{B_2}\big), BGN_B\big(s_{B_2}, \bar{r}_{B_2}\big)\Big)$$

donde r_{B1} y r_{B2} son números aleatorios proporcionados por la Cuenta 404 B. En algunos ejemplos, la Cuenta 404 B proporciona un texto cifrado de intercambio como:

$$(E', E'') = \big(PC(\beta, \gamma), BGN_B(\beta, \gamma)\big)$$

donde y es un número aleatorio generado por la Cuenta 404 B, y se comparte con otras cuentas (p. ej., proporcionado a la Cuenta 402 A con el tipo (β) de cambio).

Se genera un conjunto (EX) de pruebas (420), que se puede utilizar para verificar el tipo (β) de cambio privado. En algunas implementaciones, el conjunto (EX) de pruebas del tipo de cambio se proporciona como:

$$EX = (U, V, t'', \tilde{r}'', \hat{r}'')$$

En algunos ejemplos, *U* y *V* se calculan respectivamente como:

$$U = e(P_B, P_B)^{t'} e(P_B, Q_B)^{\tilde{r}'} \quad \text{y} \quad V = e(P_B, P_B)^{t'} e(P_B, Q_B)^{\hat{r}'}$$

donde P_B y Q_B se proporcionan en PK_{BGN_A}, y *t', r̃'* y *r̂'* son números aleatorios generados por la Cuenta 404 B. En algunos ejemplos, *t'', r̃'', r̂''* se calculan respectivamente como:

$$t'' = t' + yt_2$$

$$\tilde{r}'' = \tilde{r}' + y\tilde{r}$$

$$\hat{r}'' = \hat{r}' + y\hat{r}$$

donde y = *Resumen(U, V)*, y *r̃* y *r̂* se calculan respectivamente como:

$$\tilde{r} = \beta t_1 + t_1\gamma + \gamma r_1 q_B \alpha_B$$

$$\hat{r} = 2t_2 + r_2 q_B \alpha_B$$

En algunos ejemplos, *Resumen* se puede proporcionar como cualquier función de resumen apropiada que sea públicamente conocida por los participantes, incluidos los nodos de consenso, en la red de cadena de bloques (p. ej., SHA-256).

En algunas implementaciones, la Cuenta 404 B devuelve (422) un mensaje cifrado a la Cuenta 402 A, que incluye el siguiente conjunto de datos de ejemplo:

$$(X_1, Z_1, X_2, Y_2; RP_B, EX;\ Sig_B)$$

donde Sig_B es la firma digital de la Cuenta 404 B. En algunos ejemplos, el mensaje se transmite a través de un canal de subcadena (p. ej., el canal 308 de subcadena de la FIG. 3).

La Cuenta 402 A genera (424) una prueba (RP_A) de rango que sirve como ZKP de que la transacción tiene algún valor y que la Cuenta 402 A tiene suficientes activos para realizar la transacción. En otros términos, la prueba (RP_A) de rango se puede utilizar para demostrar que:

$$t_1 \geq 0, \quad \text{y} \quad s_A - t_1 \geq 0$$

La Cuenta 404 A genera (426) subtransacciones que incluyen una primera subtransacción desde la Cuenta 402 A a la Cuenta 404 B por la cantidad (t_1), y una segunda subtransacción desde la Cuenta 404 B a la Cuenta C por la cantidad (t_2). En algunos ejemplos, la cuenta A genera números (*t'*, *r'*) aleatorios y proporciona un conjunto de textos cifrados como:

$$(X', Y', Z') = \left(PC(t', r'), BGN_A(t', r'), BGN_B(t', r')\right)$$

La cuenta A proporciona un conjunto de datos (PF) como:

$$PF = (X', Y', Z'; t_1', r_1', t_2', r_2')$$

donde:

$$t_1' = t' + xt_1\ , r_1' = r' + xr_2, t_2' = t' + xt_2, \quad \text{y} \quad r_2' = r' + xr_2$$

donde:

$$x = Hash(X', Y', Z')$$

La Cuenta 402 A proporciona la primera y segunda subtransacciones respectivamente como:

$$A, B: X_1, Y_1, Z_1$$

$$B, C: X_2, Y_2, Z_2$$

donde *A* es un identificador de la Cuenta 402 A, *B* es un identificador de la Cuenta 404 B y *C* es un identificador de la Cuenta C (p. ej., los identificadores se proporcionan como direcciones respectivas dentro de la red de cadena de bloques). Se proporciona una transacción, que incluye las subtransacciones primera y segunda, pruebas de rango y conjuntos de pruebas de soporte. Por ejemplo, la transacción se proporciona como

$$A, B: X_1, Y_1, Z_1; B, C: X_2, Y_2, Z_2; RP_A, PF; RP_B, EX$$

La transacción está firmada digitalmente (428) por la Cuenta 402 A e incluye tanto la firma de la Cuenta 402 A (Sig_A) como la firma de la Cuenta 404 B (Sig_B). La Cuenta 402 A envía (430) la transacción firmada al nodo 406 de consenso. La transacción firmada se puede proporcionar como:

$$(A, B: X_1, Y_1, Z_1; B, C: X_2, Y_2, Z_2; RP_A, PF; RP_B, EX;\ Sig_A, Sig_B)$$

El nodo 406 de consenso verifica (432) las firmas de la Cuenta 402 A y de la Cuenta 404 B. Si las firmas no se verifican, la transacción finaliza y se puede proporcionar un mensaje de error a la Cuenta 402 A. Si las firmas se verifican, la prueba de rango (RP_A) y la prueba de rango (RP_B) se verifican (434) por el nodo 406 de consenso. Debido a que las pruebas de rango son ZKP, cada una puede probarse como verdadera, o devolver falso sin revelar los datos de texto plano subyacentes. Si las pruebas de rango no se verifican, la transacción finaliza y se puede proporcionar un mensaje de error a la Cuenta 402 A. Si se verifican las pruebas de rango, se determina que la cantidad de la transacción es

mayor que 0 y que tanto la Cuenta 402 A como la Cuenta 404 B tienen activos suficientes en las respectivas divisas para realizar las transacciones.

En algunas implementaciones, el nodo 406 de consenso verifica (436) la transacción, utilizando evidencia en el conjunto (PF) de datos y el conjunto (EX) de evidencia. En algunos ejemplos, el nodo 406 de consenso verifica si las siguientes relaciones son verdaderas:

$$PC(t_1', r_1') = X' + xX_1$$

$$BGN_A(t_1', r_1') = Y' + xY_1$$

$$BGN_B(t_1', r_1') = Z' + xZ_1$$

$$PC(t_2', r_2') = X' + xX_2$$

$$BGN_B(t_2', r_2') = Y' + xY_2$$

$$BGN_C(t_2', r_2') = Z' + xZ_2$$

donde *x = Resumen(X',Y',Z')*. Si las relaciones anteriores son verdaderas, se confirma que el texto cifrado (texto cifrado BGN) está cifrado con la clave pública adecuada y que las cantidades de la transacción son correctas.

También se verifica que la transacción se realice al tipo de cambio publicado (aunque cifrado). Por ejemplo, el nodo 406 de consenso verifica el tipo de cambio utilizando evidencia en el conjunto (EX) de datos. En algunos ejemplos, el nodo 406 de consenso calcula y = *Resumen*(*U,V*) y utiliza y para verificar si las siguientes relaciones son verdaderas:

$$e(P_B, P_B)^{t''} e(P_B, Q_B)^{\tilde{r}''} = U * e(E_2, Z_1)^y$$

$$e(P_B, P_B)^{t''} e(P_B, Q_B)^{\hat{r}''} = V * e(BGN_B(1,1), Y_2)^y$$

Si las relaciones no son verdaderas, la transacción y/o el tipo de cambio no se verifican, la transacción finaliza y se puede proporcionar un mensaje de error a la Cuenta 402 A. Si las relaciones no son verdaderas, el nodo 406 de consenso registra (438) la transacción que se registra en la red de cadena de bloques de consorcio y se actualizan los saldos de las cuentas A 402, 404 B y C. Por ejemplo, el saldo (s_A) de la Cuenta 402 A se reduce en la cantidad (t_1), el saldo (s_{B1}) de la Cuenta 404 B se incrementa en la cantidad (t_1), el saldo (s_{B2}) de la Cuenta 404 B se reduce en la cantidad (t_2) y un saldo de la Cuenta C se incrementa en la cantidad (t_2).

FIG. 5 representa un ejemplo de un proceso 500 que puede ejecutarse de acuerdo con implementaciones de esta memoria descriptiva. En algunas implementaciones, el proceso 500 de ejemplo puede realizarse utilizando uno o más programas ejecutables por computadora ejecutados utilizando uno o más dispositivos informáticos. En algunos ejemplos, el proceso 500 de ejemplo puede realizarse por nodos de una red de cadena de bloques de consorcio para realizar transacciones de activos cruzados dentro de una red de cadena de bloques.

Se recibe un tipo de cambio (502). Por ejemplo, un primer nodo asociado con un primer participante en una red de cadena de bloques (p. ej., un nodo de la red de cadena de bloques) recibe un tipo de cambio, desde un segundo nodo asociado con un segundo participante en la red de cadena de bloques (p. ej., un nodo de la red de cadena de bloques). En algunos ejemplos, el tipo de cambio se recibe a través de un canal de subcadena. En algunos ejemplos, el tipo de cambio es un tipo de cambio privado del segundo participante. En algunas implementaciones, el segundo participante es una institución financiera. En algunas implementaciones, el tipo de cambio especifica un tipo al que el segundo participante cambia un primer tipo de divisa por un segundo tipo de divisa. Por ejemplo, el tipo de cambio puede especificar el tipo al que el segundo participante cambiará USD por RMB.

El primer nodo (504) genera un primer número aleatorio y un segundo número aleatorio. Una primera cantidad y una segunda cantidad se cifran dentro de un primer conjunto de textos cifrados y un segundo conjunto de textos cifrados, respectivamente, utilizando el primer número aleatorio y el segundo número aleatorio, respectivamente (506). En algunos ejemplos, la primera cantidad es una cantidad de un primer tipo de activo a ser transferida por el primer participante al miembro participante para su intercambio. En algunos ejemplos, la segunda cantidad es la cantidad de un segundo tipo de activo a ser intercambiada por la primera cantidad. En algunos ejemplos, la segunda cantidad es igual al producto de la primera cantidad multiplicada por el tipo de cambio del segundo participante.

En algunos ejemplos, el primer conjunto de textos cifrados incluye un compromiso de número aleatorio de la primera cantidad y el primer número aleatorio y dos cifrados homomórficos de la primera cantidad y el primer número aleatorio. En algunos ejemplos, el segundo conjunto de textos cifrados incluye un compromiso de número aleatorio de la segunda cantidad y el segundo número aleatorio y dos cifrados homomórficos de la segunda cantidad y el segundo número aleatorio. En algunos ejemplos, el primer conjunto de textos cifrados incluye un PC de la primera cantidad y el primer número aleatorio, y cifrados BGN de la primera cantidad y el primer número aleatorio utilizando la clave pública BGN del primer participante y la clave pública BGN del segundo participante, respectivamente. En algunos ejemplos, el

segundo conjunto de textos cifrados incluye un PC de la segunda cantidad y el segundo número aleatorio, y cifrados BGN de la segunda cantidad y el segundo número aleatorio utilizando la clave pública BGN del segundo participante y la clave pública BGN de un tercer participante, respectivamente.

La primera cantidad, el primer número aleatorio, el segundo número aleatorio y al menos una parte (subconjunto) del primer conjunto de textos cifrados, y al menos una parte (subconjunto) del segundo conjunto de textos cifrados se transmiten desde el primer nodo al segundo nodo (508). En algunas implementaciones, la primera cantidad, el primer número aleatorio, el segundo número aleatorio, la al menos una parte del primer conjunto de textos cifrados y la al menos una parte del segundo conjunto de textos cifrados se transmiten a través del canal de subcadena.

Se recibe una primera prueba de rango, un conjunto de evidencia del tipo de cambio y una primera firma (510). En algunas implementaciones, el primer nodo recibe la primera prueba de rango, el conjunto de evidencia del tipo de cambio y una primera firma desde el segundo nodo a través del canal de subcadena. En algunos ejemplos, la primera firma digital es la firma digital del segundo participante en base a un esquema de cifrado asimétrico. En algunos ejemplos, la primera prueba de rango proporciona evidencia de que una cuenta asociada con el segundo miembro tiene fondos suficientes del mismo tipo de activo que la segunda cantidad para intercambiar la primera cantidad por la segunda cantidad.

Se generan un conjunto de datos, una segunda prueba de rango y una segunda firma digital (512). En algunos ejemplos, el conjunto de datos se utiliza dentro de la red de cadena de bloques para confirmar al menos parcialmente la autenticidad de la transacción de activos cruzados. En algunos ejemplos, la segunda firma digital es la firma digital del primer participante en base al esquema de cifrado asimétrico. En algunos ejemplos, la segunda prueba de rango proporciona evidencia de que una cuenta asociada con el primer participante tiene fondos suficientes del mismo tipo de activo que la primera cantidad para transferir la primera cantidad al segundo participante, y que la primera cantidad no es negativa.

Se envía una transacción a la red de cadena de bloques para su verificación (514). En algunas implementaciones, la transacción enviada por el primer nodo a la red de cadena de bloques incluye el primer conjunto de textos cifrados, el segundo conjunto de textos cifrados, la primera prueba de rango, el conjunto de datos, la segunda prueba de rango, el conjunto de evidencia del tipo de cambio, la primera firma digital y la segunda firma digital. En algunas implementaciones, al menos un nodo de consenso dentro de la red de cadena de bloques verifica las firmas y las pruebas de rango. En algunas implementaciones, el al menos un nodo de consenso verifica la transacción sin que se revelen los datos de transacción (p. ej., la primera cantidad, la segunda cantidad, el tipo de cambio). En alguna implementación, en respuesta a la verificación exitosa de la transacción, la transacción se ejecuta dentro de la red de cadena de bloques. En algunos ejemplos, las cuentas del primer participante y del segundo participante se actualizan en la cadena de bloques para reflejar los activos intercambiados. En algunos ejemplos, la cuenta del tercer participante se actualiza para reflejar la recepción de la segunda cantidad.

FIG. 6 es un diagrama de un ejemplo de módulos de un aparato 600 de acuerdo con implementaciones de esta memoria descriptiva. El aparato 600 puede ser una implementación de ejemplo de un nodo de cadena de bloques configurado para participar en el comercio de activos cruzados privado en una red de cadena de bloques, en donde la red de cadena de bloques es una red de cadena de bloques de consorcio. El aparato 600 puede corresponder a las implementaciones descritas anteriormente, y el aparato 600 incluye lo siguiente:

Una unidad 602 de generación genera, utilizando cifrado BGN, textos cifrados en base a un primer valor y un segundo valor, determinándose el segundo valor en base al primer valor y un tipo de cambio proporcionado por un segundo nodo en la red de cadena de bloques. Una unidad 604 de transmisión transmite el primer valor y los textos cifrados a un segundo nodo. Una unidad 606 de recepción recibe un primer conjunto de evidencia que incluye un conjunto de datos que pueden utilizarse para verificar el tipo de cambio en una rutina ZKP sin revelar el tipo de cambio. La unidad 602 de generación genera un segundo conjunto de evidencia que incluye un conjunto de datos que pueden utilizarse para verificar, utilizando la rutina ZKP, que los textos cifrados están cifrados por una clave pública BGN.

Una unidad 608 de definición de transacción define una transacción que incluye una primera transacción entre el primer nodo y el segundo nodo para la transferencia del primer valor desde el primer nodo al segundo nodo, y una segunda transacción entre el segundo nodo y un tercer nodo para la transferencia. del segundo valor desde el segundo nodo al tercer nodo. La unidad 604 de transmisión transmite la transacción a al menos un nodo de consenso de la red de cadena de bloques para la verificación y ejecución de la transacción. Como se describe en el presente documento, la transacción se puede verificar en base al primer conjunto de evidencia y el segundo conjunto de evidencia. En respuesta a la verificación de la transacción, el nodo de consenso ejecuta la primera transacción y la segunda transacción para disminuir un saldo del primer nodo por el primer valor, aumentar un primer saldo del segundo nodo por el primer valor, disminuir un segundo saldo del segundo nodo por el segundo valor y aumentar el saldo del tercer nodo por el segundo valor.

En una implementación opcional, el primer conjunto de evidencia lo proporciona el segundo nodo en base al primer valor, un par de números aleatorios proporcionados por el primer nodo y los textos cifrados.

En una implementación opcional, verificar la transacción mediante el nodo de consenso incluye verificar una firma digital del primer nodo y una firma digital del segundo nodo.

En una implementación opcional, verificar la transacción mediante el nodo de consenso incluye verificar una primera prueba de rango proporcionada por el primer nodo y una segunda prueba de rango proporcionada por el segundo nodo.

En una implementación opcional, la primera prueba de rango incluye una ZKP para probar que el primer valor es mayor que cero y que el saldo del primer nodo es mayor o igual que el primer valor.

En una implementación opcional, la segunda prueba de rango incluye una ZKP para probar que el segundo saldo del segundo nodo es mayor o igual que el segundo valor.

En una implementación opcional, la transacción incluye además un conjunto de datos que incluye un conjunto de textos cifrados generados al menos parcialmente en base al cifrado BGN, utilizándose el conjunto de datos para verificar la transacción por el al menos un nodo de consenso.

En una implementación opcional, la unidad 606 de recepción recibe el tipo de cambio desde el segundo nodo a través de un canal de subcadena de la red de cadena de bloques.

En una implementación opcional, al menos un texto cifrado de los textos cifrados se proporciona utilizando PC.

En una implementación opcional, el conjunto de datos del primer conjunto de evidencia incluye un primer valor de datos y un segundo valor de datos, determinándose cada uno del primer valor de datos y del segundo valor de datos en base a los parámetros utilizados para generar una clave pública BGN del segundo nodo.

En una implementación opcional, el conjunto de datos del segundo conjunto de evidencia incluye un conjunto de textos cifrados y un conjunto de valores, basándose cada uno de los valores en el conjunto de valores al menos parcialmente en un resumen del conjunto de textos cifrados.

El sistema, aparato, módulo o unidad ilustrado en las implementaciones anteriores puede implementarse utilizando un chip de computadora o una entidad, o puede implementarse utilizando un producto que tenga una determinada función. Un dispositivo de implementación típico es una computadora, y la computadora puede ser una computadora personal, una computadora portátil, un teléfono móvil, un teléfono con cámara, un teléfono inteligente, un asistente digital personal, un reproductor multimedia, un dispositivo de navegación, un dispositivo de recepción y envío de correos electrónicos, una consola de juegos, una computadora tableta, un dispositivo ponible o cualquier combinación de estos dispositivos.

Para un proceso de implementación de funciones y roles de cada una de las unidades en el aparato, se pueden hacer referencias a un proceso de implementación de los pasos correspondientes en el método anterior. Los detalles se omiten aquí por simplicidad.

Debido a que la implementación de un aparato corresponde básicamente a la implementación de un método, para partes relacionadas, se pueden hacer referencias a descripciones relacionadas en la implementación del método. La implementación del aparato descrita anteriormente es simplemente un ejemplo. Las unidades descritas como partes separadas pueden estar o no físicamente separadas, y las partes mostradas como unidades pueden o no ser unidades físicas, pueden estar ubicadas en una posición o pueden estar distribuidas en varias unidades de red. Algunos o todos los módulos pueden seleccionarse en base a las demandas reales para lograr los objetivos de las soluciones de la memoria descriptiva. Un experto en la técnica puede comprender e implementar sin esfuerzos creativos las implementaciones de esta solicitud.

Haciendo referencia de nuevo a la FIG. 6, se puede interpretar como una ilustración de un módulo funcional interno y una estructura de un aparato de comercio de activos cruzados privado. El aparato de comercio de activos cruzados privado puede ser un ejemplo de un nodo de cadena de bloques configurado para participar en el comercio de activos cruzados privado dentro de la red de la cadena de bloques. En esencia, un organismo de ejecución puede ser un dispositivo electrónico, y el dispositivo electrónico incluye lo siguiente: uno o más procesadores; y una memoria configurada para almacenar una instrucción ejecutable del uno o más procesadores.

Las implementaciones de la materia objeto y las acciones y operaciones descritas en esta memoria descriptiva se pueden implementar en circuitería electrónica digitales, en software o firmware de computadora incorporados de manera tangible, en hardware de computadora, incluidas las estructuras descritas en esta memoria descriptiva y sus equivalentes estructurales, o en combinaciones de uno o más de ellos. Las implementaciones de la materia objeto descrita en esta memoria descriptiva se pueden implementar como uno o más programas informáticos, p. ej., uno o más módulos de instrucciones de programa informático, codificados en un soporte de programa informático, para su ejecución por, o para controlar la operación de, aparatos de procesamiento de datos. Por ejemplo, un soporte de programa informático puede incluir uno o más medios de almacenamiento legibles por computadora que tienen

instrucciones codificadas o almacenadas en los mismos. El soporte puede ser un medio legible por computadora tangible no transitorio, tal como un disco magnético, magneto óptico u óptico, una unidad de estado sólido, una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM) u otros tipos de medios. Alternativa o adicionalmente, el soporte puede ser una señal propagada generada artificialmente, p. ej., una señal eléctrica, óptica o electromagnética generada por una máquina que se genera para codificar información para su transmisión a un aparato receptor adecuado para su ejecución por un aparato de procesamiento de datos. El medio de almacenamiento informático puede ser, o ser parte de, un dispositivo de almacenamiento legible por máquina, un sustrato de almacenamiento legible por máquina, un dispositivo de memoria de acceso aleatorio o en serie, o una combinación de uno o más de ellos. Un medio de almacenamiento informático no es una señal propagada.

Un programa informático, que también puede denominarse o describirse como un programa, software, una aplicación de software, una app, un módulo, un módulo de software, un motor, una secuencia de comandos o código, se puede escribir en cualquier forma de lenguaje de programación, incluidos los lenguajes compilados o interpretados, o los lenguajes declarativos o procedimentales; y se puede desplegar en cualquier forma, incluso como un programa independiente o como un módulo, componente, motor, subrutina u otra unidad adecuada para ejecutarse en un entorno informático, cuyo entorno puede incluir una o más computadoras interconectadas por una red de comunicaciones de datos en una o más ubicaciones.

Un programa informático puede, pero no necesariamente, corresponder a un archivo en un sistema de archivos. Un programa informático puede almacenarse en una parte de un archivo que contiene otros programas o datos, p. ej., una o más secuencias de comandos almacenadas en un documento de lenguaje de marcado, en un solo archivo dedicado al programa en cuestión, o en múltiples archivos coordinados, p. ej.., archivos que almacenan uno o más módulos, subprogramas o partes de código.

Los procesadores para la ejecución de un programa informático incluyen, a modo de ejemplo, microprocesadores tanto de uso general como especial, y uno o más procesadores de cualquier tipo de computadora digital. Generalmente, un procesador recibirá las instrucciones del programa informático para su ejecución, así como los datos desde un medio legible por computadora no transitorio acoplado al procesador.

El término "aparato de procesamiento de datos" abarca todo tipo de aparatos, dispositivos y máquinas para procesar datos, incluidos, a modo de ejemplo, un procesador programable, una computadora o múltiples procesadores o computadoras. El aparato de procesamiento de datos puede incluir circuitería lógica de propósito especial, p. ej., una FPGA (matriz de compuertas programables en campo), un ASIC (circuito integrado de aplicación específica) o una GPU (unidad de procesamiento de gráficos). El aparato también puede incluir, además del hardware, código que crea un entorno de ejecución para programas informáticos, p. ej., código que constituye el firmware del procesador, una pila de protocolo, un sistema de gestión de bases de datos, un sistema operativo o una combinación de uno o más de ellos.

Los procesos y flujos lógicos descritos en esta memoria descriptiva pueden realizarse por una o más computadoras o procesadores que ejecutan uno o más programas informáticos para realizar operaciones operando con datos de entrada y generando salida. Los procesos y flujos lógicos también se pueden realizar mediante circuitería lógica de propósito especial, p. ej., una FPGA, un ASIC o una GPU, o mediante una combinación de circuitería lógica de propósito especial y uno o más computadoras programadas.

Las computadoras adecuadas para la ejecución de un programa informático pueden estar basadas en microprocesadores de propósito general o especial o ambos, o cualquier otro tipo de unidad central de procesamiento. Generalmente, una unidad central de procesamiento recibirá instrucciones y datos desde una memoria de solo lectura o una memoria de acceso aleatorio o ambas. Los elementos de una computadora pueden incluir una unidad central de procesamiento para ejecutar instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. La unidad central de procesamiento y la memoria pueden complementarse o incorporarse en circuitería lógica de propósito especial.

Generalmente, una computadora también incluirá, o estará acoplada operativamente para recibir datos desde o transferir datos a, uno o más dispositivos de almacenamiento. Los dispositivos de almacenamiento pueden ser, por ejemplo, discos magnéticos, magneto ópticos u ópticos, unidades de estado sólido o cualquier otro tipo de medio legible por computadora no transitorio. Sin embargo, una computadora no necesita tener tales dispositivos. Por tanto, una computadora puede estar acoplada a uno o más dispositivos de almacenamiento, tales como una o más memorias, que son locales y/o remotas. Por ejemplo, una computadora puede incluir una o más memorias locales que son componentes integrales de la computadora, o la computadora puede acoplarse a una o más memorias remotas que se encuentran en una red en la nube. Además, una computadora puede integrarse en otro dispositivo, p. ej., un teléfono móvil, un asistente digital personal (PDA), un reproductor de audio o vídeo móvil, una consola de juegos, un receptor del sistema de posicionamiento global (GPS) o un dispositivo de almacenamiento portátil, p. ej., una unidad flash de bus serie universal (USB), por nombrar solo algunas.

Los componentes se pueden "acoplar" entre sí estando conectados conmutativamente, tal como eléctrica u ópticamente, entre sí, ya sea directamente o a través de uno o más componentes intermedios. Los componentes

también se pueden "acoplar" entre sí si uno de los componentes está integrado en el otro. Por ejemplo, un componente de almacenamiento que está integrado en un procesador (p. ej., un componente de caché L2) está "acoplado" al procesador.

Para facilitar la interacción con un usuario, las implementaciones de la materia objeto descrita en esta memoria descriptiva se pueden implementar o configurar para comunicarse con una computadora que tenga un dispositivo de visualización, p. ej., un monitor LCD (pantalla de cristal líquido), para visualizar información al usuario, y un dispositivo de entrada mediante el cual el usuario puede proporcionar entrada a la computadora, p. ej., un teclado y un dispositivo señalador, p. ej., un ratón, una bola de seguimiento o un panel táctil. También se pueden utilizar otros tipos de dispositivos para proporcionar la interacción con un usuario; por ejemplo, la retroalimentación proporcionada al usuario puede ser cualquier forma de retroalimentación sensorial, p. ej., retroalimentación visual, retroalimentación auditiva o retroalimentación táctil; y la entrada del usuario se puede recibir de cualquier forma, incluida la entrada acústica, de voz o táctil. Además, una computadora puede interactuar con un usuario enviando documentos a y recibiendo documentos desde un dispositivo que se utiliza por el usuario; por ejemplo, enviando páginas web a un navegador web en el dispositivo de un usuario en respuesta a solicitudes recibidas desde el navegador web, o interactuando con una app que se ejecuta en un dispositivo de usuario, p. ej., un teléfono inteligente o tableta electrónica. Además, una computadora puede interactuar con un usuario enviando mensajes de texto u otras formas de mensaje a un dispositivo personal, p. ej., un teléfono inteligente que está ejecutando una aplicación de mensajería, y recibiendo de vuelta mensajes de respuesta del usuario.

Esta memoria descriptiva utiliza el término "configurado para" en relación con sistemas, aparatos y componentes de programas informáticos. Para que un sistema de una o más computadoras esté configurado para realizar operaciones o acciones particulares significa que el sistema tiene instalado software, firmware, hardware o una combinación de ellos que en funcionamiento hacen que el sistema realice las operaciones o acciones. Para que uno o más programas informáticos se configuren para realizar operaciones o acciones particulares significa que el uno o más programas incluyen instrucciones que, cuando se ejecutan por un aparato de procesamiento de datos, hacen que el aparato realice las operaciones o acciones. Para que la circuitería lógica de propósito especial se configure para realizar operaciones o acciones particulares, significa que la circuitería tiene lógica electrónica que realiza las operaciones o acciones.

Si bien esta memoria descriptiva contiene muchos detalles de implementación específica, estos no deben interpretarse como limitaciones en el alcance de lo que se reivindica, que está definido por las propias reivindicaciones, sino más bien como descripciones de características que pueden ser específicas de implementaciones particulares. Ciertas características que se describen en esta memoria descriptiva en el contexto de implementaciones separadas también se pueden realizar en combinación en una sola implementación. A la inversa, diversas características que se describen en el contexto de una sola implementación también se pueden realizar en múltiples implementaciones por separado o en cualquier subcombinación adecuada. Además, aunque las características pueden describirse anteriormente como que actúan en ciertas combinaciones e incluso inicialmente reivindicarse como tales, una o más características de una combinación reivindicada pueden en algunos casos eliminarse de la combinación, y la reivindicación puede estar dirigida a una subcombinación o variación de una subcombinación.

De manera similar, si bien las operaciones se describen en los dibujos y se enumeran en las reivindicaciones en un orden particular, esto no debe entenderse como que requiere que tales operaciones se realicen en el orden particular mostrado o en orden secuencial, o que se realicen todas las operaciones ilustradas, para lograr resultados deseables. En determinadas circunstancias, la multitarea y el procesamiento en paralelo pueden resultar ventajosos. Además, la separación de diversos módulos y componentes del sistema en las implementaciones descritas anteriormente no debe entenderse que requiera dicha separación en todas las implementaciones, y debe entenderse que los componentes y sistemas del programa descritos generalmente se pueden integrar juntos en un solo producto de software o empaquetarse en múltiples productos de software.

Se han descrito implementaciones particulares de la materia objeto. Otras implementaciones están dentro del alcance de las siguientes reivindicaciones. Por ejemplo, las acciones enumeradas en las reivindicaciones se pueden realizar en un orden diferente y aún así lograr resultados deseables. Como ejemplo, los procesos representados en las figuras adjuntas no requieren necesariamente el orden particular mostrado, o el orden secuencial, para lograr resultados deseables. En algunos casos, la multitarea y el procesamiento en paralelo pueden resultar ventajosos.

REIVINDICACIONES

1. Un método (500) implementado por computadora para el comercio de activos cruzados privado en una red de cadena de bloques, el método es ejecutado por uno o más procesadores y comprende:
generar (506), por un primer nodo en la red de cadena de bloques y utilizando cifrado de Boneh-Goh-Nissim, BGN, textos cifrados en base a un primer valor y un segundo valor, siendo determinado el segundo valor en base una multiplicación homomórfica del primer valor y un tipo de cambio cifrado proporcionado por un segundo nodo en la red de cadena de bloques, en donde los textos cifrados y el tipo de cambio cifrado están en una misma curva elíptica;
transmitir (508), por el primer nodo al segundo nodo, el primer valor y los textos cifrados;
recibir (510), por el primer nodo y desde el segundo nodo, un primer conjunto de evidencia que comprende un conjunto de datos que se pueden utilizar para verificar el tipo de cambio en una rutina de prueba de conocimiento cero, ZKP, sin revelar el tipo de cambio;
generar (512), mediante el primer nodo, un segundo conjunto de evidencia que comprende un conjunto de datos que se pueden utilizar para verificar, utilizando la rutina ZKP, que los textos cifrados están cifrados por una clave pública BGN del primer nodo;
definir, por el primer nodo, una transacción que comprende una primera transacción entre el primer nodo y el segundo nodo para la transferencia del primer valor desde el primer nodo al segundo nodo, y una segunda transacción entre el segundo nodo y un tercer nodo para la transferencia del segundo valor desde el segundo nodo al tercer nodo; y
transmitir (514), por el primer nodo, la transacción a al menos un nodo de consenso de la red de cadena de bloques para la verificación y ejecución de la transacción, la transacción se verifica en base al primer conjunto de evidencia y al segundo conjunto de evidencia, y en respuesta a verificar la transacción, ejecutar la primera transacción y la segunda transacción para disminuir un saldo del primer nodo por el primer valor, aumentar un primer saldo del segundo nodo por el primer valor, disminuir un segundo saldo del segundo nodo por el segundo valor y aumentar el saldo del tercer nodo por el segundo valor.

2. El método de la reivindicación 1, en donde el primer conjunto de evidencia lo proporciona el segundo nodo en base al primer valor, un par de números aleatorios proporcionados por el primer nodo y los textos cifrados.

3. El método de la reivindicación 1, en donde verificar la transacción por el al menos un nodo de consenso comprende verificar una firma digital del primer nodo y una firma digital del segundo nodo.

4. El método de la reivindicación 1, en donde verificar la transacción por el al menos un nodo de consenso comprende verificar una primera prueba de rango proporcionada por el primer nodo y una segunda prueba de rango proporcionada por el segundo nodo.

5. El método de la reivindicación 4, en donde la primera prueba de rango comprende una ZKP para probar que el primer valor es mayor que cero, y que el saldo del primer nodo es mayor o igual que el primer valor.

6. El método de la reivindicación 4, en donde la segunda prueba de rango comprende un ZKP para probar que el segundo saldo del segundo nodo es mayor o igual que el segundo valor.

7. El método de la reivindicación 1, en donde la transacción comprende además un conjunto de datos que comprende un conjunto de textos cifrados generados utilizando cifrado BGN, utilizándose el conjunto de datos para verificar la transacción por el al menos un nodo de consenso.

8. El método de la reivindicación 1, que comprende además recibir, por el primer nodo, el tipo de cambio desde el segundo nodo a través de un canal de subcadena de la red de cadena de bloques.

9. El método de la reivindicación 1, en donde al menos un texto cifrado de los textos cifrados se proporciona utilizando el Compromiso de Pedersen.

10. El método de la reivindicación 1, en donde el conjunto de datos del primer conjunto de evidencia comprende un primer valor de datos y un segundo valor de datos, determinándose cada uno del primer valor de datos y del segundo valor de datos en base a parámetros utilizados para generar una clave pública BGN del segundo nodo.

11. El método de la reivindicación 1, en donde el conjunto de datos del segundo conjunto de evidencia comprende un conjunto de textos cifrados y un conjunto de valores, basándose cada uno de los valores del conjunto de valores en un resumen del conjunto de textos cifrados.

12. Uno o más medios de almacenamiento legibles por computadora codificados con instrucciones para el comercio de activos cruzados privado en una red de cadena de bloques, las instrucciones pueden ser ejecutadas por uno o más procesadores y hacen que el uno o más procesadores realicen un método de acuerdo con una cualquiera de las reivindicaciones anteriores.

13. Un sistema que comprende:
uno o más procesadores; y

una o más memorias legibles por computadora acopladas al uno o más procesadores y que tienen instrucciones almacenadas en las mismas para el comercio de activos cruzados privado en una red de cadena de bloques, las instrucciones pueden ser ejecutadas por el uno o más procesadores para realizar un método de acuerdo con una cualquiera de las reivindicaciones 1 a 11.

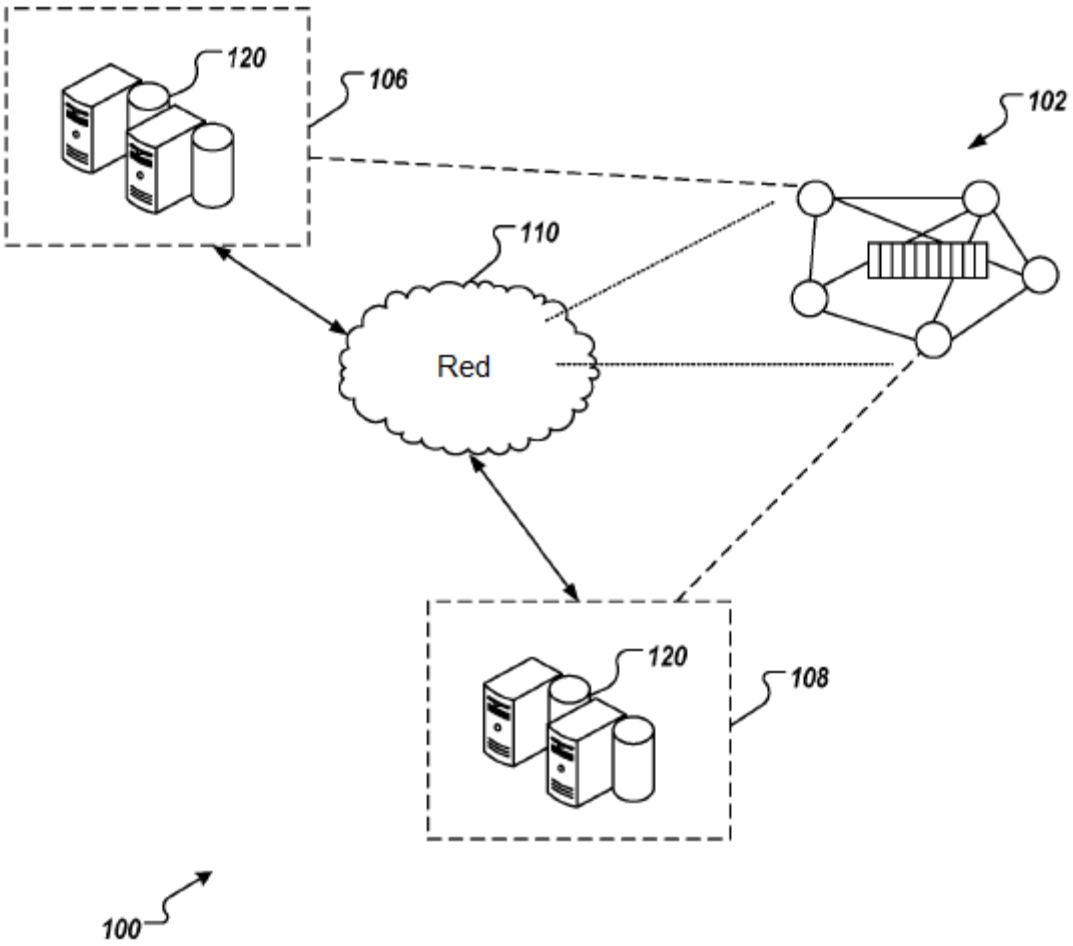

FIG. 1

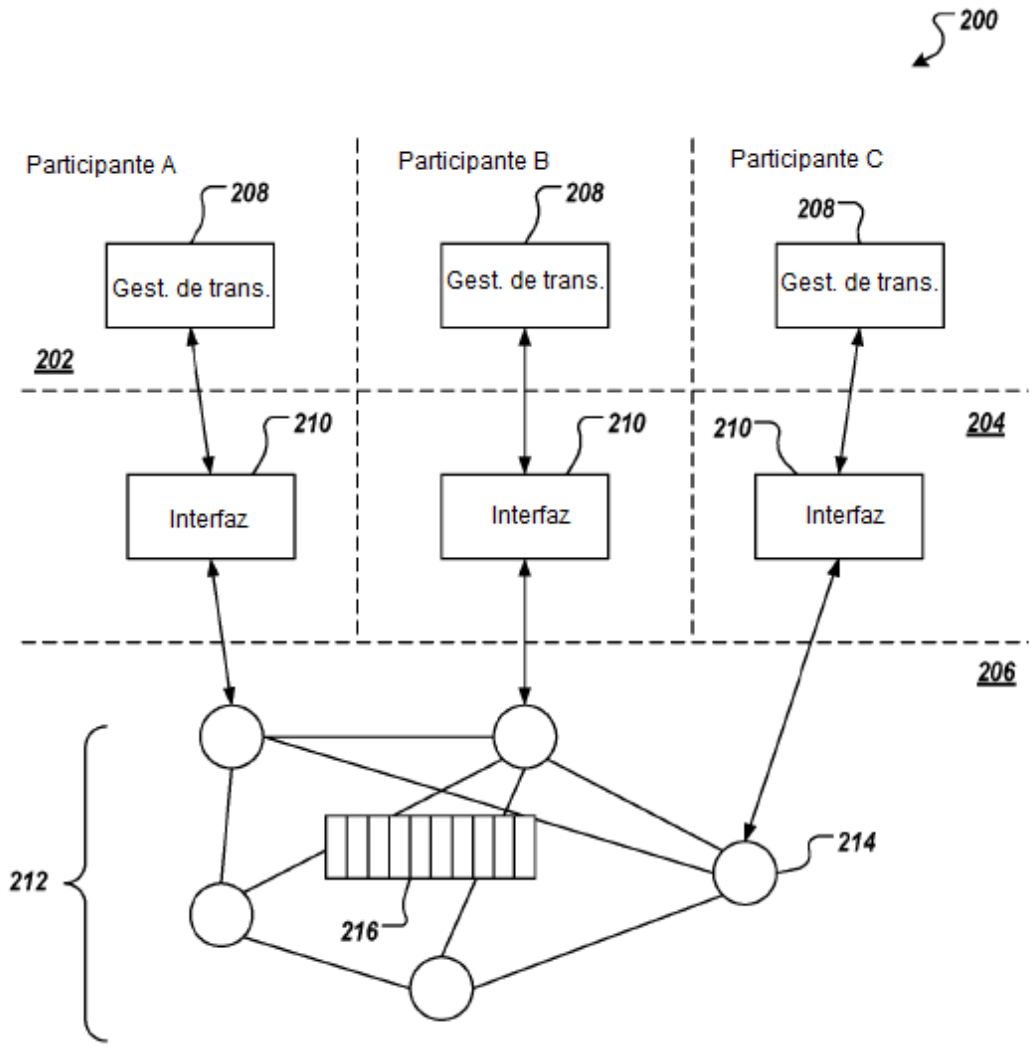
200
Participante A
Participante B
Participante C
208
208
208
Gest. de trans.
Gest. de trans.
Gest. de trans.
202
204
210
210
210
Interfaz
Interfaz
Interfaz
206
212
214
216

FIG. 2

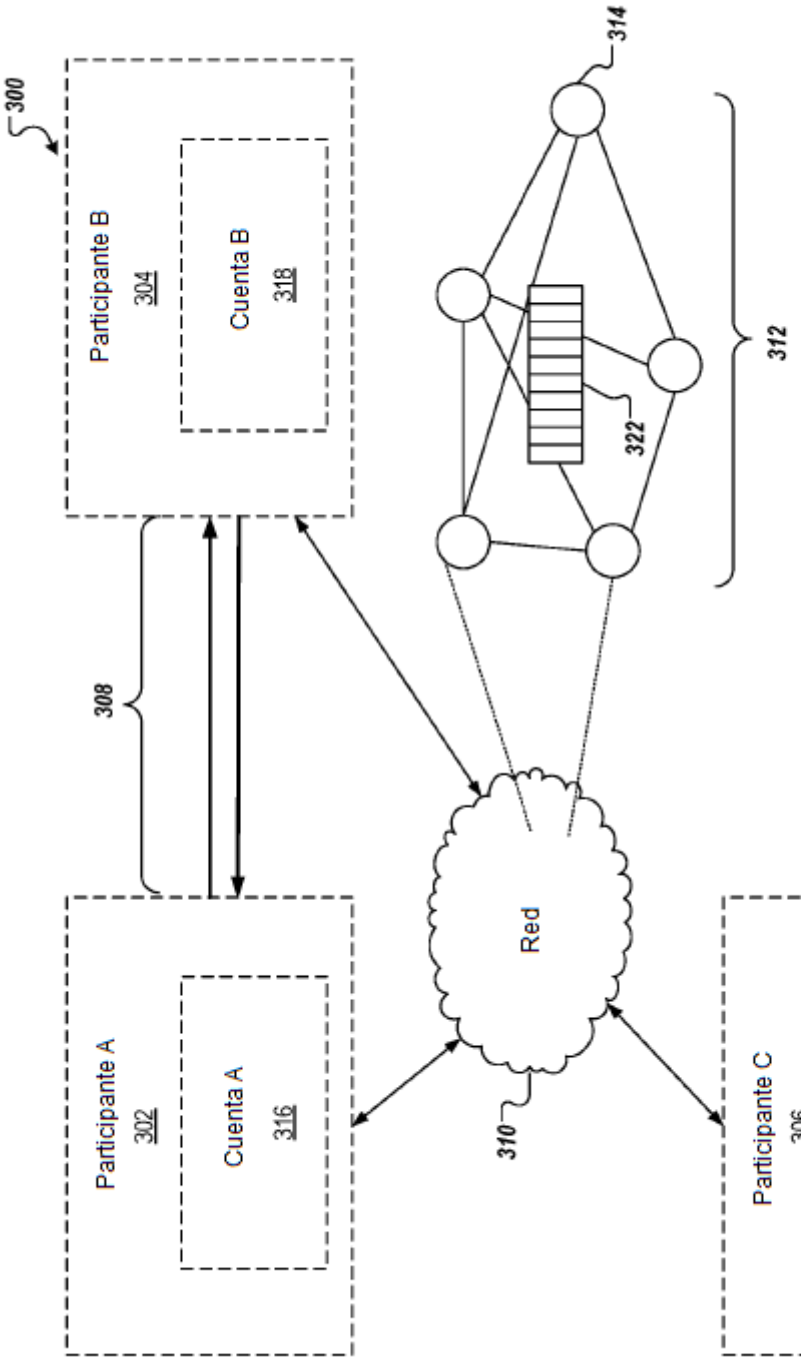
300
Participante B
304
Cuenta B
318
314
312
322
308
Red
310
Participante A
302
Cuenta A
316
Participante C
306
Cuenta C
320

FIG. 3

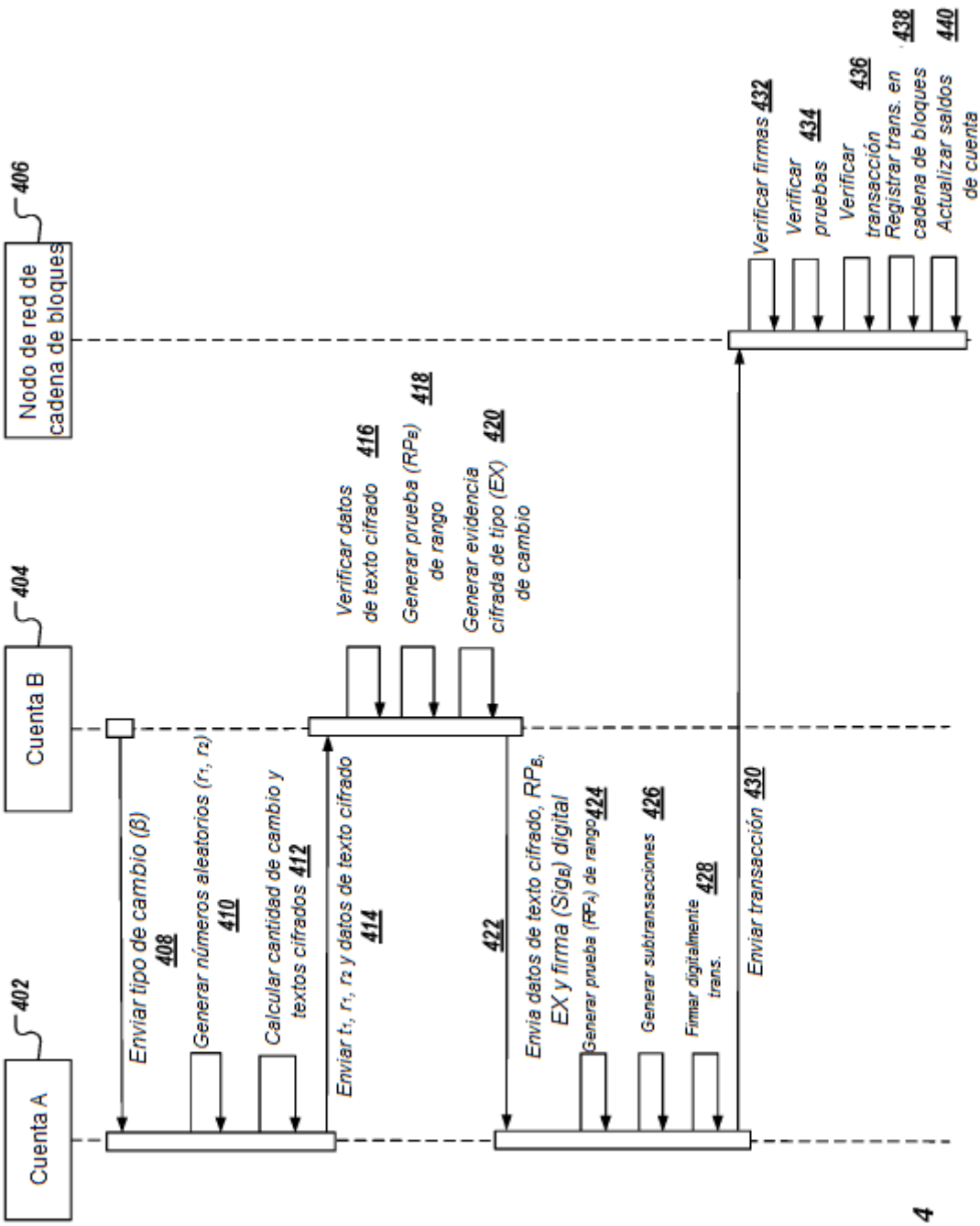
Cuenta A
402
Cuenta B
404
Nodo de red de cadena de bloques
406
Enviar tipo de cambio (β) 408
Generar números aleatorios (r1, r2) 410
Calcular cantidad de cambio y textos cifrados 412
Enviar t1, r1, r2 y datos de texto cifrado 414
Verificar datos de texto cifrado 416
Generar prueba (RPB) de rango 418
Generar evidencia cifrada de tipo (EX) de cambio 420
422
Envia datos de texto cifrado, RPB, EX y firma (SigB) digital
Generar prueba (RPA) de rango 424
Generar subtransacciones 426
Firmar digitalmente trans. 428
Enviar transacción 430
Verificar firmas 432
Verificar pruebas 434
Verificar transacción 436
Registrar trans. en cadena de bloques 438
Actualizar saldos de cuenta 440

FIG. 4

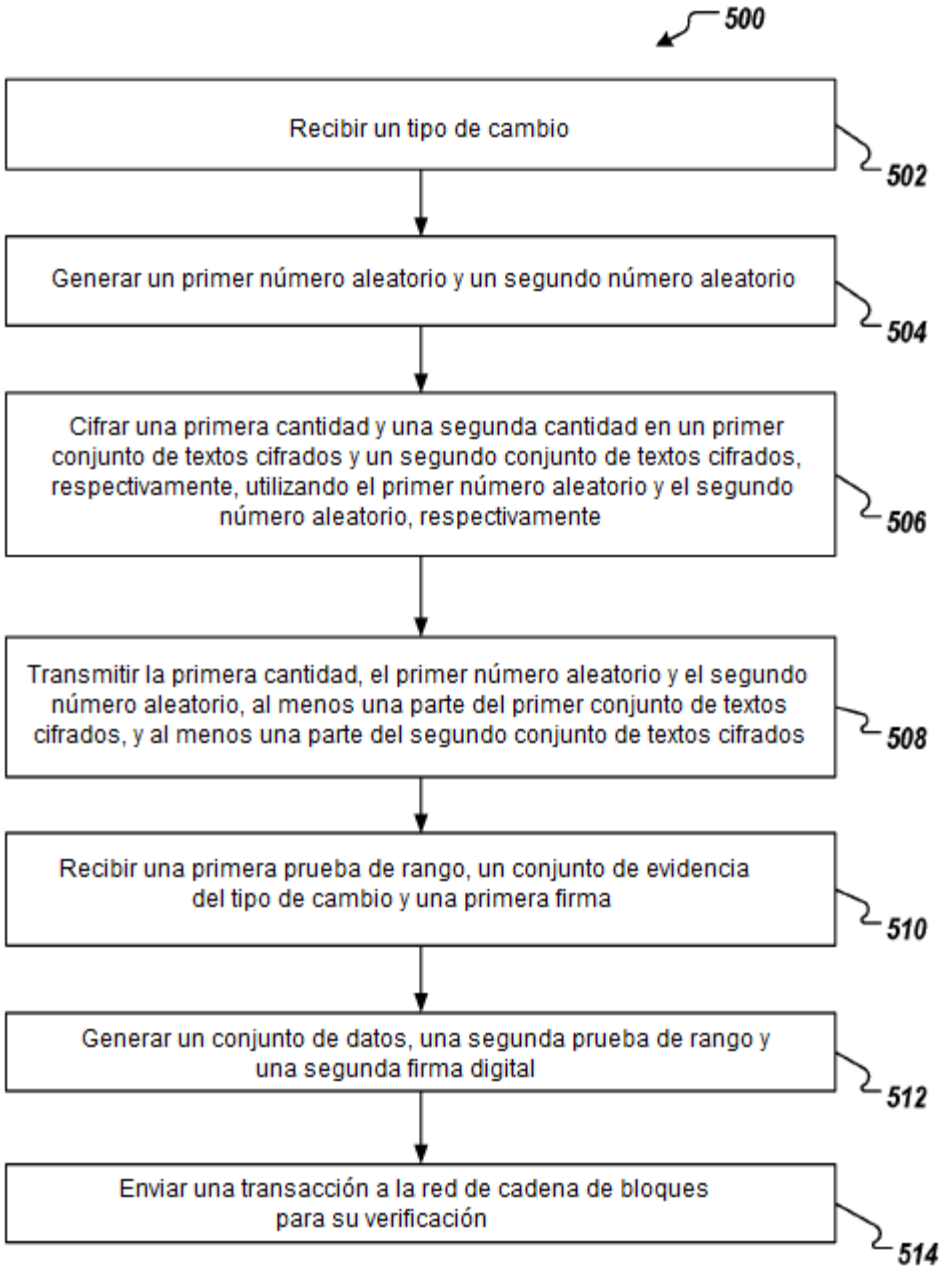
500
Recibir un tipo de cambio
502
Generar un primer número aleatorio y un segundo número aleatorio
504
Cifrar una primera cantidad y una segunda cantidad en un primer conjunto de textos cifrados y un segundo conjunto de textos cifrados, respectivamente, utilizando el primer número aleatorio y el segundo número aleatorio, respectivamente
506
Transmitir la primera cantidad, el primer número aleatorio y el segundo número aleatorio, al menos una parte del primer conjunto de textos cifrados, y al menos una parte del segundo conjunto de textos cifrados
508
Recibir una primera prueba de rango, un conjunto de evidencia del tipo de cambio y una primera firma
510
Generar un conjunto de datos, una segunda prueba de rango y una segunda firma digital
512
Enviar una transacción a la red de cadena de bloques para su verificación
514

FIG. 5

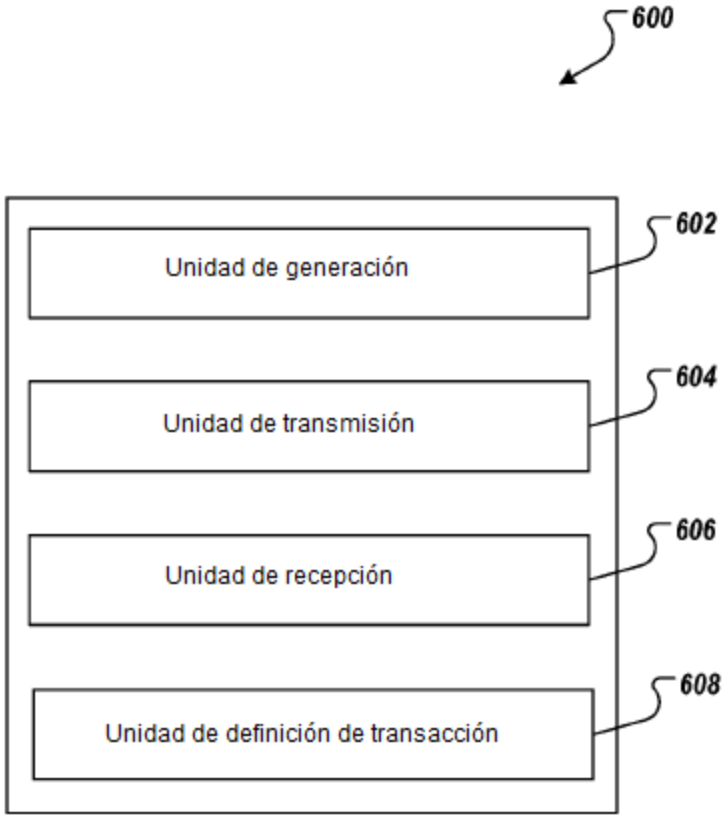
600
602
Unidad de generación
604
Unidad de transmisión
606
Unidad de recepción
608
Unidad de definición de transacción

FIG. 6