(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 881 319**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.11.2018 PCT/CN2018/114344**

(87) Fecha y número de publicación internacional: **18.04.2019 WO19072264**

(96) Fecha de presentación y número de la solicitud europea: **07.11.2018 E 18867268 (7)**

(97) Fecha y número de publicación de la concesión europea: **28.04.2021 EP 3545483**

(54) Título: **Protección de datos de cadena de bloques mediante cifrado homomórfico**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.11.2021

(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:

MA, BAOLI y
ZHANG, WENBIN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

Observaciones:

Véase nota informativa (Remarks, Remarques o Bemerkungen) en el folleto original publicado por la Oficina Europea de Patentes

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

Protección de datos de cadena de bloques mediante cifrado homomórfico

ANTECEDENTES

Las redes de cadena de bloques, que también pueden denominarse sistemas de cadena de bloques, redes de consenso, redes de sistema de libro mayor distribuido o cadena de bloques, permiten a las entidades participantes almacenar datos de forma segura e inmutable. Una cadena de bloques puede describirse como un sistema de libro mayor de transacciones, y múltiples copias del libro mayor se almacenan en la red de cadena de bloques. Tipos de ejemplos de cadenas de bloques pueden incluir cadenas de bloques públicas, cadenas de bloques autorizadas y cadenas de bloques privadas. Una cadena de bloques pública está abierta para que todas las entidades utilicen la cadena de bloques y participen en el proceso de consenso. Una cadena de bloques autorizada es similar a una cadena de bloques pública, pero abierta solo para entidades con permiso para unirse. Una cadena de bloques privada se proporciona a una entidad en particular, que controla de manera centralizada los permisos de lectura y escritura.

Las cadenas de bloques se utilizan en redes de criptomonedas, que permiten a los participantes realizar transacciones para comprar/vender bienes y/o servicios utilizando una criptomoneda. Una criptomoneda común incluye Bitcoin. En las redes de criptomonedas, los modelos de mantenimiento de registros se utilizan para registrar transacciones entre usuarios. Ejemplos de modelos de mantenimiento de registros incluyen el modelo de salida de transacción no gastada (UTXO) y el modelo de saldo de cuenta. En el modelo UTXO, cada una de las transacciones gasta la salida de transacciones anteriores y genera nuevas salidas que se pueden gastar en transacciones posteriores. Se registran las transacciones no gastadas de un usuario, y el saldo que el usuario posee se calcula como la suma de todas las transacciones no gastadas del usuario. En el modelo de saldo de cuenta, el saldo de cuenta de cada uno de los usuarios se registra como un estado global. Para cada transacción, se comprueba el saldo de una cuenta de gastos para garantizar que sea mayor o igual que el importe de la transacción. Esto es comparable a la banca tradicional.

Un libro mayor de cadena de bloques incluye una serie de bloques, cada uno de los cuales contiene una o más transacciones ejecutadas en la red. Cada uno de los bloques puede ser análogo a una página del libro mayor, mientras que la cadena de bloques en sí es una copia completa del libro mayor. Las transacciones individuales se confirman y se añaden a un bloque, que se añade a la cadena de bloques. Las copias del libro mayor de cadena de bloques se repiten en los nodos de la red. De esta manera, existe un consenso global sobre el estado de la cadena de bloques. Además, la cadena de bloques está abierta para que todos los nodos la vean, al menos en el caso de las redes públicas. Para proteger la privacidad de los usuarios de cadenas de bloques, se pueden implementar tecnologías de cifrado. El documento de B. F. França, "Homomorphic Mini-blockchain Scheme", XP055624506, 24 de abril de 2015, describe un esquema de criptomonedas basado en el esquema de minicadenas de bloques y compromisos homomórficos concebidos con el objetivo de mejorar la privacidad de la minicadena de bloques. França también describe una comparación del esquema con Bitcoin con respecto a la capacidad de resistir el análisis de cadenas de bloques.

Según el modelo de cuenta, los esquemas de compromiso pueden utilizarse para ocultar valores con los que ambas partes de una transacción se comprometen. Los esquemas de compromiso pueden surgir de la necesidad de que las partes se comprometan con una elección o valor y, a continuación, comuniquen ese valor a las otras partes involucradas. Por ejemplo, en un Compromiso de Pedersen interactivo, la parte A puede comprometerse con un importe de transacción *t* enviando un PC de valor de compromiso *(r, t)* que se genera en base al valor aleatorio *r*. Se genera el valor de compromiso, y la parte B solo puede revelar el importe de transacción *t* mediante la obtención del número aleatorio *r*.

RESUMEN

La invención se define en las reivindicaciones adjuntas. Las implementaciones de la presente divulgación incluyen procedimientos implementados por ordenador para la verificación protegida con privacidad de transacciones de cadena de bloques sin confirmación del usuario, interacción y revelación de importes de transacciones o saldos de cuentas. Más en particular, las implementaciones de la presente divulgación se refieren a validar transacciones entre usuarios de cadena de bloques en base a esquemas de compromiso y cifrado homomórfico sin revelar importes de transacciones, saldos de cuentas o números aleatorios para generar compromisos con otros nodos de cadena de bloques.

En algunas implementaciones, las acciones incluyen recibir, desde una primera cuenta, una copia firmada digitalmente de un valor de compromiso de un primer importe de un importe de transacción que se transferirá desde una primera cuenta a una segunda cuenta, generado en base a un primer número aleatorio, donde el primer importe de la transferencia de saldo y el primer número aleatorio cifrados usan una clave pública de la primera cuenta, un segundo importe de la transferencia de saldo y un segundo número aleatorio cifrados usan una clave pública de la segunda cuenta, una o más pruebas de intervalo y un conjunto de valores generados en base a uno o más números aleatorios seleccionados; verificar una firma digital correspondiente a la copia firmada digitalmente usando una clave pública de la primera cuenta correspondiente a una clave privada utilizada para generar la firma digital; determinar que la una o

más pruebas de intervalo prueban que el importe de la transferencia de saldo es mayor que cero e inferior o igual a un saldo de la primera cuenta; determinar si el primer importe y el segundo importe son iguales y si el primer número aleatorio y el segundo número aleatorio son iguales en base al conjunto de valores;

y actualizar el saldo de la primera cuenta y un saldo de la segunda cuenta en base al primer importe de la transferencia de saldo si el primer importe y el segundo importe son iguales y el primer número aleatorio y el segundo número aleatorio son iguales. Otras implementaciones incluyen sistemas, aparatos y programas informáticos correspondientes, configurados para realizar las acciones de los procedimientos, codificados en dispositivos de almacenamiento informático.

Estas y otras implementaciones pueden incluir opcionalmente una o más de las siguientes características: el valor de compromiso se genera utilizando un esquema de compromiso que es homomórfico; el esquema de compromiso es un esquema de compromiso de Pedersen; el primer importe de la transferencia de saldo y el primer número aleatorio se cifran utilizando la clave pública de la primera cuenta en base a un algoritmo de cifrado homomórfico (HE) probabilístico, y donde el segundo importe de la transferencia de saldo y un segundo número aleatorio se cifran utilizando la clave pública de la segunda cuenta en base al algoritmo HE probabilístico; el algoritmo HE probabilístico es un algoritmo HE de Okamoto-Uchiyama; los números aleatorios seleccionados están representados por r^*, t^*, $z1^*$ y $z2^*$, y los números aleatorios seleccionados se utilizan para generar *a, b, c* y *d,* donde $a = r^* + xr$, $b = t^* + xt$, $c = z1^* + xz1$ y $d = z2^* + xz2$, *r* es el primer número aleatorio, *t* es el primer importe de la transferencia de saldo, *x* es un valor *hash*; el conjunto de valores se genera adicionalmente en base a C, D y E, donde $C = g^{r^*}h^{t^*}$, $D = u2^{r^*}v2^{z1^*}$, $E = u2^{t^*}v2^{z2^*}$, donde *g, h, u2 y v2* son generadores de una curva elíptica, y donde x se genera aplicando la función *hash* a C, D y E; el primer importe y el segundo importe se determinan como iguales y el primer número aleatorio y el segundo número aleatorio se determinan como iguales en base a las propiedades de HE probabilístico; el primer importe y el segundo importe se determinan como iguales y el primer número aleatorio y el segundo número aleatorio se determinan como iguales si $g^a h^b = CT^x$, $u2^a v2^c = DZ\_B1^x$ y $u2^b v2^d = EZ\_B2^x$, donde $T = g^r h^t$ es el valor de compromiso del importe de la transferencia de saldo, $Z\_B1 = u2^r v2^{z1}$, $Z\_B2 = u2^t v2^{z2}$, y donde *z1* y *z2* son números aleatorios utilizados para cifrar el segundo importe de la transferencia de saldo y el segundo número aleatorio en base al esquema HE probabilístico; y la actualización del saldo de la primera cuenta y un saldo de la segunda cuenta se realiza en base a HE.

La presente divulgación también proporciona uno o más medios de almacenamiento legibles por ordenador no transitorios acoplados a uno o más procesadores y que tienen instrucciones almacenadas en los mismos que, cuando se ejecutan por el uno o más procesadores, hacen que el uno o más procesadores realicen operaciones de acuerdo con implementaciones de los procedimientos proporcionados en el presente documento.

La presente divulgación proporciona además un sistema para implementar los procedimientos proporcionados en el presente documento. El sistema incluye uno o más procesadores y un medio de almacenamiento legible por ordenador acoplado al uno o más procesadores que tienen instrucciones almacenadas en los mismos que, cuando se ejecutan por el uno o más procesadores, hacen que el uno o más procesadores realicen operaciones de acuerdo con implementaciones de los procedimientos proporcionados en el presente documento.

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

Los detalles de una o más implementaciones de la presente divulgación se establecen en los dibujos adjuntos y en la siguiente descripción. Otras características y ventajas de la presente divulgación serán evidentes a partir de la descripción y los dibujos, y de las reivindicaciones.

DESCRIPCIÓN DE LOS DIBUJOS

La FIG. 1 representa un entorno de ejemplo que puede ser utilizado para ejecutar implementaciones de la presente divulgación.

La FIG. 2 representa una arquitectura conceptual de ejemplo de acuerdo con las implementaciones de la presente divulgación.

La FIG. 3 representa un procedimiento de ejemplo de validación protegida con privacidad de una transacción de cadena de bloques en base a cifrado homomórfico de acuerdo con implementaciones de la presente divulgación.

La FIG. 4 representa una transacción de cadena de bloques de ejemplo en base a cifrado homomórfico de acuerdo con implementaciones de la presente divulgación.

La FIG. 5 representa otro procedimiento de ejemplo de validación protegida con privacidad de una transacción de cadena de bloques en base a cifrado homomórfico de acuerdo con implementaciones de la presente divulgación.

La FIG. 6 representa otra transacción de cadena de bloques de ejemplo en base a cifrado homomórfico de acuerdo con implementaciones de la presente divulgación.

La FIG. 7 representa un proceso de ejemplo que puede ser ejecutado de acuerdo con implementaciones de la presente divulgación.

La FIG. 8 representa otro proceso de ejemplo que puede ser ejecutado de acuerdo con implementaciones de la presente divulgación.

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

DESCRIPCIÓN DETALLADA

Las implementaciones de la presente divulgación incluyen procedimientos implementados por ordenador para la verificación protegida con privacidad de transacciones de cadena de bloques sin confirmación del usuario, interacción y revelación de importes de transacciones o saldos de cuentas. Más en particular, las implementaciones de la presente divulgación se refieren a validar transacciones entre usuarios de cadena de bloques en base a esquemas de compromiso y cifrados homomórficos (HE) sin revelar importes de transacciones, saldos de cuentas o números aleatorios para generar compromisos con otros nodos de cadena de bloques.

Para proporcionar un contexto adicional para las implementaciones de la presente divulgación, y como se ha introducido anteriormente, las redes de cadena de bloques, que también pueden denominarse redes de consenso (por ejemplo, formada por nodos de igual a igual), sistema de libro mayor distribuido o simplemente cadena de bloques, permiten a las entidades participantes realizar transacciones de forma segura e inmutable y almacenar datos. Una cadena de bloques se puede proporcionar como una cadena de bloques pública, una cadena de bloques privada o una cadena de bloques de consorcio. Las implementaciones de la presente divulgación se describen con más detalle en el presente documento con referencia a una cadena de bloques pública, que es pública entre las entidades participantes. Sin embargo, se contempla que las implementaciones de la presente divulgación se puedan realizar en cualquier tipo apropiado de cadena de bloques.

En una cadena de bloques pública, el proceso de consenso está controlado por nodos de la red de consenso. Por ejemplo, cientos, miles, incluso millones de entidades pueden participar en una cadena de bloques pública, cada una de las cuales opera al menos un nodo en la cadena de bloques pública. En consecuencia, la cadena de bloques pública puede considerarse una red pública con respecto a las entidades participantes. En algunos ejemplos, la mayoría de las entidades (nodos) deben firmar cada uno de los bloques para que el bloque sea válido y se añada a la cadena de bloques. Un ejemplo de cadena de bloques pública incluye la cadena de bloques utilizada en la red Bitcoin, que es una red de pago de igual a igual (red de criptomonedas). Aunque el término cadena de bloques se menciona habitualmente junto con la red de Bitcoin, cadena de bloques generalmente se refiere, como se utiliza en el presente documento, a libros mayores distribuidos sin una referencia particular a la red de Bitcoin.

En general, una cadena de bloques pública admite transacciones públicas. Una transacción pública se comparte con todos los nodos de la cadena de bloques y el libro mayor de cadena de bloques se repite en todos los nodos. Es decir, todos los nodos están en perfecto estado de consenso con respecto a la cadena de bloques. Para lograr un consenso (p. ej., un 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. Un ejemplo de protocolo de consenso incluye, sin limitación, prueba de trabajo (POW) implementado en la red Bitcoin.

Las implementaciones de la presente divulgación se describen con más detalle en el presente documento en vista del contexto anterior. Más en particular, como se ha introducido anteriormente, las implementaciones de la presente divulgación se refieren a validar transacciones entre usuarios de cadena de bloques en base a esquemas de compromiso y HE sin revelar importes de transacciones, saldos de cuentas o números aleatorios para generar los compromisos con otros nodos de cadena de bloques.

De acuerdo con las implementaciones de la presente divulgación, las transacciones de cadena de bloques pueden validarse y registrarse en una cadena de bloques (libro mayor) en base al compromiso sin revelar el saldo de cuenta de transacción, el importe de transacción o el número aleatorio utilizado para generar el compromiso. Un esquema de compromiso, tal como el compromiso de Pedersen (PC), puede utilizarse para generar un compromiso de un importe de transacción utilizando un número aleatorio. El importe de transacción y el número aleatorio pueden cifrarse utilizando HE probabilístico o determinista. El importe de transacción y el número aleatorio también pueden utilizarse para generar un conjunto de valores como pruebas para validar la transacción en base a las propiedades de HE. El compromiso de la transacción, el importe de transacción cifrado, el número aleatorio cifrado y las pruebas pueden ser

utilizados por un nodo de cadena de bloques para verificar si la transacción es válida sin que se revele el saldo de cuenta, el importe de transacción o el número aleatorio.

La FIG. 1 representa un entorno 100 de ejemplo que puede ser utilizado para ejecutar implementaciones de la presente divulgación. En algunos ejemplos, el entorno 100 de ejemplo permite a las entidades participar en una cadena de bloques pública 102. El entorno 100 de ejemplo incluye sistemas informáticos 106, 108 y una red 110. En algunos ejemplos, la red 110 incluye una red de área local (LAN), una red de área amplia (WAN), e Internet, o una combinación de las mismas, y conecta sitios web, dispositivos de usuario (p. ej., dispositivos informáticos) y sistemas de procesamiento. 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 informáticos 106, 108 pueden incluir cada uno cualquier sistema informático apropiado que permita la participación como nodo en la cadena de bloques pública 102. Dispositivos informáticos de ejemplo incluyen, sin limitación, un servidor, un ordenador de sobremesa, un ordenador portátil, una tableta electrónica y un teléfono inteligente. En algunos ejemplos, los sistemas informáticos 106, 108 alojan uno o más servicios implementados por ordenador para interactuar con la cadena de bloques pública 102. Por ejemplo, el sistema informático 106 puede alojar servicios implementados por ordenador de una primera entidad (p. ej., el usuario A), tal como un sistema de gestión de transacciones que la primera entidad utiliza para gestionar sus transacciones con otra u otras entidades (p. ej., otros usuarios). El sistema informático 108 puede alojar servicios implementados por ordenador 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 otra u otras entidades (p. ej., otros usuarios). En el ejemplo de la FIG. 1, la cadena de bloques pública 102 se representa como una red de nodos de igual a igual, y los sistemas informáticos 106, 108 proporcionan nodos de la primera entidad, y de la segunda entidad respectivamente, que participan en la cadena de bloques pública 102.

La FIG. 2 representa una arquitectura conceptual 200 de ejemplo de acuerdo con las implementaciones de la presente divulgación. La arquitectura conceptual 200 de ejemplo incluye una capa de entidad 202, una capa de servicios alojados 204 y una capa de cadena de bloques pública 206. En el ejemplo representado, la capa de entidad 202 incluye tres entidades, Entidad_1 (E1), Entidad_2 (E2) y Entidad_3 (E3), teniendo cada una de las entidades un respectivo sistema de gestión de transacciones 208.

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

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

La FIG. 3 representa un procedimiento 300 de ejemplo de validación protegida con privacidad de una transacción de cadena de bloques en base a HE de acuerdo con implementaciones de la presente divulgación. En un nivel alto, el procedimiento 300 de ejemplo se lleva a cabo por un nodo de usuario A 302, un nodo de usuario B (no mostrado en la FIG. 3) y un nodo de cadena de bloques 304, también denominado nodo de consenso. Una transacción, tal como una transferencia de valor, se puede realizar desde el nodo de usuario A 302 al nodo de usuario B. Para proteger la privacidad de la cuenta, el nodo de usuario A 302 puede generar un compromiso de un importe de transacción t utilizando un esquema de compromiso, tal como PC, en base a un número aleatorio r. El compromiso generado utilizando PC puede expresarse como *PC(r, t)*. El nodo de usuario A 302 también puede cifrar el número aleatorio utilizando HE en base a una clave pública del nodo de usuario B. Esto se puede expresar como *HE(r)*. Un texto cifrado del importe de transacción *t*, expresado como (*PC*(*r, t*), *HE*(*r*)) se puede transmitir al nodo de usuario B. Después de recibir el texto cifrado, el nodo de usuario B puede descifrar el número aleatorio *r* usando una clave privada. El nodo de usuario B puede usar el número aleatorio *r* para descifrar el importe de transacción *t*. Para probar la validez de la transacción, el nodo de cadena de bloques 304 puede comparar el número aleatorio del compromiso y el número

aleatorio cifrado usando HE. Si los números aleatorios coinciden, se determina que la transacción es válida por el nodo de cadena de bloques 304 con conocimiento nulo de los datos de transacción. Más detalles del procedimiento 300 de ejemplo se analizan en la siguiente descripción de la FIG. 3.

En 306, el nodo de usuario A 302 genera un valor de compromiso de un importe de transacción en base a un primer número aleatorio, y cifra, en base a HE, un segundo número aleatorio utilizando una clave pública del nodo de usuario A 302, y un tercer número aleatorio utilizando una clave pública del nodo de usuario B. El primer número aleatorio, el segundo número aleatorio y el tercer número aleatorio pueden ser el mismo número aleatorio r utilizado para generar un compromiso de un importe de transacción t utilizando un esquema de compromiso. En algunas implementaciones, el esquema de compromiso puede tener una forma exponencial doble, tal como el PC. Usando el PC como ejemplo no limitativo, el valor de compromiso generado por el primer número aleatorio *r* puede expresarse como $PC(r, t) = g^r h^t$, donde *g* y *h* pueden ser generadores de una curva elíptica, *PC*(*r, t*) es una multiplicación escalar de puntos de curva, y *t* es el importe de transacción con el que hay que comprometerse. Debe entenderse que otros esquemas de compromiso basados en HE, tales como el HE de Okamoto-Uchiyama (OU) y el HE de Boneh-Goh-Nissim también pueden utilizarse para generar el valor de compromiso.

El cifrado del segundo número aleatorio *r* cifrado usando la clave pública del nodo de usuario A 302 puede expresarse como *HE_A(r)*. El cifrado del tercer número aleatorio *r* cifrado usando la clave pública del nodo de usuario B puede expresarse como *HE_B(r)*.

En algunas implementaciones, el cifrado de HE de clave pública puede ser un HE determinista que se puede obtener de esquemas de HE probabilísticos, tales como HE de Paillier, HE de Benaloh, HE de OU, HE de Naccache-Stern, HE de Damgard-Jurik o HE de Boneh-Goh-Nissim, estableciendo el número aleatorio a un valor fijo. En algunas implementaciones, los esquemas de HE deterministas que satisfacen las propiedades lineales de que $HE(a + b) = HE(a) + HE(b)$ y $HE(ab) = HE(b)^a$, donde *a* y *b* son texto plano utilizado para HE, se pueden utilizar para la presente divulgación.

En algunos ejemplos, T = *PC(r, t),* T' = *HE_A(r)* y T" = *HE_B(r)*, y el texto cifrado del importe de transacción se puede expresar como (T, T' y T"). Se puede determinar que la transacción es válida si se cumplen las condiciones de ejemplo. En primer lugar, el importe de transacción *t* es mayor que o igual a 0, y menor que o igual a un saldo de cuenta s_A del nodo de usuario A 302. En segundo lugar, la transacción está firmada digitalmente por la clave privada del nodo de usuario A 302, clave privada para demostrar que la transacción está autorizada por el nodo de usuario A 302. En tercer lugar, el número aleatorio *r* en el *PC(r, t)* de compromiso es el mismo que el *r* cifrado en el texto cifrado *HE_A(r)* y *HE_B(r)* utilizando las claves públicas del nodo de usuario A 302 y el nodo de usuario B, respectivamente.

En algunas implementaciones, el texto cifrado también puede separarse como un texto cifrado de un importe enviado (*t'*), que puede expresarse como (*PC*(*r', t'*), *HE_A*(*r'*)), y un texto cifrado de un importe recibido (*t"*), que puede expresarse como (*PC*(*r", t"*), *HE_B*(*r"*)). En tales casos, también debe determinarse que el importe enviado *t'* es el mismo que el importe recibido *t"* para validar la transacción.

En 308, el nodo de usuario A 302 genera una o más pruebas de intervalo. En algunas implementaciones, las pruebas de intervalo pueden incluir una prueba de intervalo *RP1* para mostrar que el importe de transacción t es mayor que o igual a cero, y una prueba de intervalo *RP2* para mostrar que el importe de transacción t es menor que o igual a un saldo de cuenta del nodo de usuario A.

En 310, el nodo de usuario A 302 genera un conjunto de valores usando HE en base a uno o más números aleatorios seleccionados. El conjunto de valores, denotado como *Pf*, puede incluir pruebas utilizadas para demostrar que el número aleatorio *r* en el *PC(r, t)* de compromiso es el mismo que el *r* cifrado en el texto cifrado *HE_A(r)* y *HE_B(r)* utilizando las claves públicas del nodo de usuario A 302 y el nodo de usuario B, respectivamente. En algunas implementaciones, se pueden seleccionar dos números aleatorios *r1* y *t1* para calcular otro conjunto de textos cifrados de *t1* denotados como (T1, T1', T1"), donde $T1 = g^{r1} h^{r1}$, T1' = *HE_A(r1),* T1" = *HE_B(r1).* Dos pruebas adicionales *r2* y *t2* se pueden calcular como *r2 = r1 + xr, t2 = t1 + xt*, donde *x* es el *hash* de T1, T1' y T1". El conjunto de valores puede denotarse como *Pf* = (T1, T1', T1", *r2, t2*).

En 312, el nodo de usuario A 302 utiliza su clave privada para firmar digitalmente el texto cifrado (T, T', T"), el texto cifrado (T1, T1', T1"), *r2, t2,* las pruebas de intervalo *RP1* y *RP2*, y las claves públicas del nodo de usuario A 302 y el nodo de usuario B. La firma digital agregada por el nodo de usuario A 302 puede usarse para mostrar que la transacción está autorizada por el nodo de usuario A 302. La copia firmada digitalmente se envía a la red de cadena de bloques en 314.

En 316, el nodo de cadena de bloques 304 verifica la firma digital usando una clave pública del nodo de usuario A 302. El nodo de cadena de bloques 304 puede ser un nodo de consenso que puede probar la validez de transacciones en la red de cadena de bloques. Si el nodo de cadena de bloques 304 no puede verificar la firma digital del nodo de usuario A 302 usando la clave pública, se puede determinar que la firma digital es incorrecta y se puede denegar la transacción. En algunas implementaciones, el nodo de cadena de bloques 304 también puede incluir un mecanismo de evitación de doble gasto. El nodo de cadena de bloques 304 puede verificar si la transacción ya se ha ejecutado o

registrado. Si la transacción ya se ha ejecutado, la transacción puede ser rechazada. De lo contrario, se puede proceder a la validación de la transacción.

En 318, el nodo de cadena de bloques 304 verifica la una o más pruebas de intervalo. Por ejemplo, la prueba de intervalo *RP1* puede utilizarse para probar que el importe de transacción *t* es mayor que o igual a cero, y la prueba de intervalo *RP2* puede utilizarse para probar que el importe de transacción *t* es menor que o igual a un saldo de cuenta del nodo de usuario A 302.

En 320, el nodo de cadena de bloques 304 determina que el primer número aleatorio, el segundo número aleatorio y el tercer número aleatorio son iguales en base al conjunto de valores. En algunas implementaciones, la determinación incluye determinar si las condiciones de ejemplo $g^{r2}h^{t2} = T^xT1$, $HE\_A(r2) = T'^xT1'$ y $HE\_B(r2) = T''^xT1''$ son verdaderas en base a las propiedades de un HE determinista, como se analizó anteriormente. Si son verdaderas, esto puede indicar que el número aleatorio en el compromiso es el mismo que los números aleatorios cifrados homomórficamente utilizando las claves públicas del nodo de usuario A 302 y el nodo de usuario B, y la transacción es válida.

En 322, el nodo de cadena de bloques 304 actualiza los saldos de cuenta del nodo de usuario A 302 y el nodo de usuario B. Las actualizaciones de saldo se pueden realizar en base a las propiedades de HE sin revelar los saldos de cuenta del nodo de usuario A 302 o el nodo de usuario B. La actualización de los saldos de cuenta se describe con más detalle en el presente documento con referencia a la FIG. 4.

La FIG. 4 representa una transacción de cadena de bloques 400 de ejemplo en base a HE de acuerdo con implementaciones de la presente divulgación. Como se muestra en la transacción de cadena de bloques 400 de ejemplo, un nodo de usuario A 402 transfiere un importe de transacción t a un nodo de usuario B 406. Antes de la transacción, el nodo de usuario A 402 tiene un saldo de cuenta de s_A y el nodo de usuario B 406 tiene un saldo de cuenta de s_B.

Utilizando los esquemas de cifrado y el proceso de transacción descritos en el presente documento con referencia a la FIG. 3 como ejemplo, el saldo de cuenta *s_A* puede cifrarse utilizando un número aleatorio *r_A* basado en PC, y el número aleatorio *r_A* puede cifrarse en base a HE. El texto cifrado del saldo de cuenta s_A puede expresarse como (S_A, S'_A) = ($g^{r\_A}h^{s\_A}$, HE_A(*r*_A)), donde *g* y *h* pueden ser generadores de una curva elíptica para generar el PC del saldo de cuenta s_A. De manera similar, un saldo de cuenta s_B del nodo de usuario B 406 puede cifrarse utilizando un número aleatorio *r_B* basado en PC. El texto cifrado del saldo de cuenta *s_B* puede expresarse como (S_B, S'_B) = ($g^{r\_B}h^{s\_B}$, HE_A(*r*_B)).

En 404, el nodo de usuario A 402 puede agregar una firma digital a las pruebas utilizadas para validar la transacción y enviar la copia firmada digitalmente a la red de cadena de bloques 408. Tal como se describió anteriormente con referencia a la FIG. 3, las pruebas pueden incluir el texto cifrado del importe de transacción (T, T', T"), una o más pruebas de intervalo (*RP1*, *RP2*) y otras pruebas (T1, T1', T1", r2, *t2*).

Después de la transacción, el saldo de cuenta del nodo de usuario A 402 puede expresarse como *s_A - t'*, y el saldo de cuenta del nodo de usuario B 406 puede expresarse como *s_B + t"*, donde *t'* es el importe enviado por el nodo de usuario A 402 y *t"* es el importe recibido por el nodo de usuario B. El texto cifrado del saldo de cuenta del nodo de usuario A 402 después de la transacción puede expresarse como (S_A / T, S'_A / T') y el texto cifrado del saldo de cuenta del nodo de usuario B 406 después de la transacción puede expresarse como (S_B * T, S'_B * T"). Dado que S_A, S'_A, S_B, S'_B, T, T', T" se cifran cada uno usando HE con forma exponencial doble, la suma y resta se pueden realizar en su forma cifrada sin descifrar los valores de texto plano.

La FIG. 5 representa otro procedimiento 500 de ejemplo de validación protegida con privacidad de una transacción de cadena de bloques en base a HE de acuerdo con implementaciones de la presente divulgación. En un nivel alto, el procedimiento 500 de ejemplo se lleva a cabo por un nodo de usuario A 502, un nodo de usuario B (no mostrado en la FIG. 5) y un nodo de cadena de bloques 504, que puede denominarse nodo de consenso. Una transacción, tal como una transferencia de valor, se puede realizar desde el nodo de usuario A 502 al nodo de usuario B. Para proteger la privacidad de la cuenta, el nodo de usuario A 502 puede generar un compromiso del importe de transacción *t* utilizando un esquema de compromiso, tal como PC, en base a un número aleatorio *r*. El compromiso generado utilizando PC puede expresarse como *PC(r, t)*. El nodo de usuario A 502 también puede cifrar el importe de transacción *t* y el número aleatorio *r* usando HE que tiene una forma exponencial doble, tal como OU.

Un texto cifrado del importe de transacción *t* puede enviarse a la red de cadena de bloques. Después de recibir el texto cifrado, el nodo de cadena de bloques 504 puede determinar si el número aleatorio *r* oculto en PC coincide con el número aleatorio *r* cifrado en OU utilizando las claves públicas del nodo de usuario A 502 y el nodo de usuario B, respectivamente. Además, el nodo de cadena de bloques 504 puede determinar si el importe de transacción *t* oculto en PC coincide con el importe de transacción *t* cifrado en OU utilizando las claves públicas del nodo de usuario A 502 y el nodo de usuario B, respectivamente. Si tanto los números aleatorios como los importes de transacción coinciden, puede determinarse que la transacción es válida por el nodo de cadena de bloques 504 con conocimiento nulo de los datos de transacción.

En 506, el nodo de usuario A 502 genera un valor de compromiso de un primer importe de transacción en base a un primer número aleatorio, y el primer importe de transacción y el primer número aleatorio se cifran utilizando una clave pública del nodo de usuario A 502. Un segundo importe de transacción y un segundo número aleatorio se cifran utilizando una clave pública del nodo de usuario B. El primer importe de transacción y el segundo importe de transacción pueden ser el mismo importe *t*. El primer número aleatorio y el segundo número aleatorio pueden ser el mismo número aleatorio *r* utilizado para generar un compromiso del importe de transacción *t* utilizando un esquema de compromiso. En algunas implementaciones, el esquema de compromiso puede tener una forma exponencial doble, tal como el PC. Utilizando el PC como ejemplo, el valor de compromiso generado por el primer número aleatorio *r* puede expresarse como $PC(r, t) = g^r h^t$, donde *g* y *h* pueden ser generadores de una curva elíptica, *PC*(*r, t*) es una multiplicación escalar de puntos de curva, y *t* es el importe de transacción con el que hay que comprometerse. Debe entenderse que otros esquemas de compromiso basados en HE tales como el HE de OU y el HE de Boneh-Goh-Nissim también pueden utilizarse para generar el valor de compromiso.

El nodo de usuario A 502 también puede cifrar el primer número aleatorio y el primer importe de transacción utilizando la clave pública del nodo de usuario A 502, y cifrar el segundo número aleatorio y el segundo importe de transacción utilizando la clave pública del nodo de usuario B. En algunas implementaciones, el cifrado de los números aleatorios y de los importes de transacción puede basarse en un HE probabilístico, tal como OU. Usando OU como ejemplo, el cifrado del primer número aleatorio y del primer importe de transacción utilizando la clave pública del nodo de usuario A 502 puede expresarse como $OU\_A(r) = u1^r v1^{y1}$ y $OU\_A(t) = u1^t v1^{y2}$, respectivamente, donde *u1* y *v1* son generadores en la curva elíptica, y *y1* e *y2* son números aleatorios utilizados para generar OU_A(r) y OU_A(*t*). El segundo número aleatorio y el segundo importe de transacción cifrados se pueden expresar como $OU\_B(r) = u2^r v2^{z1}$ y $OU\_B(t) = u2^t v2^{z2}$, respectivamente, donde *u2* y *v2* son generadores en la curva elíptica y *z1* y *z2* son números aleatorios utilizados para generar OU_B(*r*) y OU_B(*t*), respectivamente. Un OU probabilístico satisface la propiedad de que $OU(a + b) = OU(a) * OU(b)$, donde *a* y *b* son el texto plano utilizado para OU.

El texto cifrado del importe de transacción *t* puede expresarse como (*PC*(*r, t*), OU_A(*r*), OU_A(*t*), OU_B(*r*), OU_B(*t*)). Se puede determinar que la transacción es válida si se cumplen las siguientes condiciones de ejemplo. En primer lugar, el importe de transacción *t* es mayor que o igual a 0, y menor que o igual al saldo de cuenta s_A del nodo de usuario A 502. En segundo lugar, la transacción está firmada digitalmente utilizando la clave privada del nodo de usuario A 502, clave privada para demostrar que la transacción está autorizada por el nodo de usuario A 502. En tercer lugar, el número aleatorio *r* en el *PC(r, t)* de compromiso es el mismo que el *r* cifrado en el texto cifrado OU_A(*r*) y OU_B(*r*) utilizando las claves públicas del nodo de usuario A 502 y el nodo de usuario B, respectivamente. En cuarto lugar, el importe de transacción *t* en el PC(*r*, *t*) de compromiso es el mismo que el *t* cifrado en el texto cifrado OU_A(*t*) y OU_B(*t*) utilizando las claves públicas del nodo de usuario A 502 y el nodo de usuario B, respectivamente.

En algunas implementaciones, el texto cifrado también puede separarse como un texto cifrado de un importe enviado (*t'*), que puede expresarse como (*PC*(*r', t'*), *OU_A*(*r'*), *OU_A*(*t'*)), y un texto cifrado de un importe recibido (*t''*), que puede expresarse como (*PC*(*r'', t''*), *OU_B*(*r''*), *OU_B*(*t''*)). En tales casos, también debe determinarse que el importe enviado *t'* es el mismo que el importe recibido *t*'' para validar la transacción.

En 508, el nodo de usuario A 502 genera una o más pruebas de intervalo. En algunas implementaciones, las pruebas de intervalo pueden incluir una prueba de intervalo *RP1* para mostrar que el importe de transacción *t* es mayor que o igual a cero, y una prueba de intervalo *RP2* para mostrar que el importe de transacción *t* es menor que o igual a un saldo de cuenta del nodo de usuario A.

En 510, el nodo de usuario A 502 genera un conjunto de valores usando HE en base a uno o más números aleatorios seleccionados. El conjunto de valores denotado como *Pf* puede incluir pruebas utilizadas para demostrar que el número aleatorio *r* en el *PC*(*r, t*) de compromiso es el mismo que el *r* cifrado en el texto cifrado OU_A(*r*) y OU_B(*r*), y el importe de transacción *t* en el *PC*(*r, t*) de compromiso es el mismo que el *t* cifrado en el texto cifrado OU_A(*t*) y OU_B(t). En algunas implementaciones, se pueden seleccionar cuatro números aleatorios *r**, *t*, z1** y *z2** para calcular otro conjunto de textos cifrados denotados como (C, D, E), donde $C = g^{r*} h^{t*}$, $D = u2^{r*} v2^{z1*}$ y $E = u2^{t*} v2^{z2*}$, donde *g, h, u2* y *v2* son generadores de una curva elíptica. Cuatro pruebas adicionales *a, b, c* y *d* se pueden calcular como $a = r^* + xr$, $b = t^* + xt$, $c = z1^* + xz1$ y $d = z2^* + xz2$, donde x es una función *hash* de *g, h, u2, v2,* C, D y E. El conjunto de valores se puede denotar entonces como *Pf* = (C, D, E, *a, b, c, d*).

En 512, el nodo de usuario A 502 utiliza su clave privada para firmar digitalmente el texto cifrado (*PC*(*r, t*), OU_A(*r*), OU_A(*t*), OU_B(*r*), OU_B(*t*)), las pruebas de intervalo *RP1* y *RP2* y el conjunto de valores *Pf*. La firma digital añadida por el nodo de usuario A 502 se puede utilizar para mostrar que la transacción está autorizada por el nodo de usuario A 502. La copia firmada digitalmente se envía a la red de cadena de bloques en 514.

En 516, el nodo de cadena de bloques 504 verifica la firma digital usando una clave pública del nodo de usuario A 502. El nodo de cadena de bloques 504 puede ser un nodo de consenso que puede probar la validez de transacciones en la red de cadena de bloques. Si el nodo de cadena de bloques 504 no puede verificar la firma digital utilizando la clave pública del nodo de usuario A, se puede determinar que la firma digital es incorrecta y se puede denegar la transacción. En algunas implementaciones, el nodo de cadena de bloques 504 también puede incluir un mecanismo de evitación de doble gasto. El nodo de cadena de bloques 504 puede verificar si la transacción ya se ha ejecutado o registrado.

Si la transacción ya se ha ejecutado, la transacción puede ser rechazada. De lo contrario, se puede proceder a la validación de la transacción.

En 518, el nodo de cadena de bloques 504 verifica la una o más pruebas de intervalo. Por ejemplo, la prueba de intervalo *RP1* puede utilizarse para probar que el importe de transacción *t* es mayor que o igual a cero, y la prueba de intervalo *RP2* puede utilizarse para probar que el importe de transacción *t* es menor que o igual a un saldo de cuenta del nodo de usuario A 502.

En 520, el nodo de cadena de bloques 504 determina si el primer importe de transacción es el mismo que el segundo importe de transacción y si el primer número aleatorio es el mismo que el segundo número aleatorio en base al conjunto de valores. En algunas implementaciones, la determinación incluye determinar si $g^a h^b = CT^x$, $u2^a v2^c = DZ\_B1^x$ y $u2^b v2^d = EZ\_B2^x$, donde $T = g^r h^t$ es el valor de compromiso del primer importe de transacción *t,* $Z\_B1 = u2^r v2^{z1}$, $Z\_B2 = u2^t v2^{z2}$, y donde *z1* y *z2* son números aleatorios utilizados para cifrar el segundo importe de transacción y el segundo número aleatorio en base al esquema de HE probabilístico. Si se cumple, esto puede indicar que el número aleatorio y el importe de transacción en el compromiso son, respectivamente, los mismos que los números aleatorios y los importes de transacción cifrados homomórficamente utilizando la clave pública del nodo de usuario A 502 y el nodo de usuario B, y la transacción es válida.

En 522, el nodo de cadena de bloques 504 actualiza los saldos de cuenta del nodo de usuario A 502 y el nodo de usuario B. Las actualizaciones de saldo de cuenta se pueden realizar en base a las propiedades de HE sin revelar los saldos de cuenta del nodo de usuario A 502 y/o el nodo de usuario B.

La FIG. 6 representa otra transacción de cadena de bloques 600 de ejemplo en base a HE de acuerdo con implementaciones de la presente divulgación. Como se muestra en la transacción 600 de ejemplo, un nodo de usuario A 602 transfiere un importe de transacción *t* a un nodo de usuario B 606. Antes de la transacción, el nodo de usuario A 602 tiene un saldo de cuenta de *s_A* y el nodo de usuario B 606 tiene un saldo de cuenta de *s_B.*

En algunos ejemplos, el saldo de cuenta *s_A* puede ocultarse utilizando un número aleatorio *r_A* basado en PC utilizando los esquemas de cifrado y el proceso de transacción descritos en el presente documento con referencia a la FIG. 5. El número aleatorio *r_A* y el saldo de cuenta pueden cifrarse en base a OU. El texto cifrado del saldo de cuenta *s_A* puede expresarse como (S_A, R_A, Q_A) = ($g^{r\_A} h^{s\_A}$, OU_A(*r_A*), OU_A(*s_A*)), donde *g* y *h* pueden ser generadores de una curva elíptica para generar el PC del saldo de cuenta *s_A*. De manera similar, un saldo de cuenta s_B del nodo de usuario B 606 puede cifrarse utilizando un número aleatorio r_B basado en PC. El texto cifrado del saldo de cuenta *s_B* puede expresarse como (S_B, S'_B) = ($g^{r\_B} h^{s\_B}$, OU_B(r_B), OU_B(*s_B*)).

En 604, el nodo de usuario A 602 puede agregar una firma digital a las pruebas utilizadas para validar la transacción y enviar la copia firmada digitalmente a la red de cadena de bloques 608. Tal como se describe en el presente documento con referencia a la FIG. 5, las pruebas pueden incluir el texto cifrado del importe de transacción (PC(*r*, *t*), OU_A(*r*), OU_A(*t*), OU_B(*r*), OU_B(*t*)), la una o más pruebas de intervalo (*RP1*, *RP2*) y otras pruebas (C, D, E, *a, b, c, d*).

Después de la transacción, el saldo de cuenta del nodo de usuario A 602 puede expresarse como *s_A - t*, y el saldo de cuenta del nodo de usuario B 606 puede expresarse como *s_B + t*. El texto cifrado del saldo de cuenta del nodo de usuario A 602 después de la transacción puede expresarse como (S_A / T, R_A / Y_A1, Q_A / Y_A2), donde Y_A1 = OU_A(r) e Y_A2 = OU_A(t). El texto cifrado del saldo de cuenta del nodo de usuario B 606 después de la transacción se puede expresar como (S_B * T, R_B * Z_B1, Q_B * Z_B2), donde Z_B1 = OU_B(*r*) y Z_B2 = OU_B(*t*). Dado que S_A, S_B, R_A, R_B, Q_A, Q_B, Y_A1, Y_A2, Z_B1, Z_B2 y T están cifrados usando HE con forma exponencial doble, la suma y resta se pueden realizar en su forma cifrada sin descifrar los valores de texto plano.

La FIG. 7 representa un proceso 700 de ejemplo que puede ser ejecutado de acuerdo con implementaciones de la presente divulgación. Para mayor claridad de presentación, la siguiente descripción describe generalmente el procedimiento 700 en el contexto de las otras figuras de esta descripción. Sin embargo, se entenderá que el proceso 700 de ejemplo puede realizarse, por ejemplo, mediante cualquier sistema, entorno, software y hardware, o una combinación de sistemas, entornos, software y hardware, según sea apropiado. En algunas implementaciones, las etapas del proceso 700 de ejemplo pueden ejecutarse en paralelo, en combinación, en bucles o en cualquier orden.

En 702, un nodo de consenso recibe, desde una primera cuenta, una copia firmada digitalmente de un valor de compromiso de un importe de transacción que se transferirá desde la primera cuenta a una segunda cuenta, generado en base a un primer número aleatorio. El nodo de consenso también puede recibir de la primera cuenta un segundo número aleatorio cifrado utilizando una clave pública de la primera cuenta, un tercer número aleatorio cifrado utilizando una clave pública de la segunda cuenta, una o más pruebas de intervalo y un conjunto de valores generados utilizando HE en base a uno o más números aleatorios seleccionados. En algunas implementaciones, el valor de compromiso se genera utilizando un esquema de compromiso basado en HE. En algunas implementaciones, el segundo número aleatorio y el tercer número aleatorio están cifrados en base a un esquema de HE determinista.

En algunas implementaciones, el conjunto de valores se representa mediante (T1, T1', T1", *r2*, *t2*), donde *r2* = *r1* + *xr, t2* = *t1* + *xt,* donde *r1* y *t1* representan el uno o más números aleatorios seleccionados, *r* representa el primer número aleatorio y *t* representa el importe de la transferencia de saldo. En algunos ejemplos, $T1=g^{r1}h^{t1}$, T1'=HE_A(*r1*), T1"=HE_B(*r*1), donde *g* y *h* son generadores de una curva elíptica, HE_A (*r1*) se genera en base a HE de *r1* utilizando la clave pública de la primera cuenta, y HE_B (*r1*) se genera en base a HE de *r1* utilizando la clave pública de la segunda cuenta. En algunos ejemplos, *x* se genera aplicando la función *hash* a T1, T1' y T1".

En 704, el nodo de consenso verifica una firma digital correspondiente a la copia firmada digitalmente utilizando una clave pública de la primera cuenta correspondiente a una clave privada utilizada para generar la firma digital.

En 706, el nodo de consenso determina si la una o más pruebas de intervalo prueban que el importe de la transferencia de saldo es mayor que cero y menor que o igual a un saldo de la primera cuenta.

En 708, el nodo de consenso determina si el primer número aleatorio, el segundo número aleatorio y el tercer número aleatorio son iguales en base al conjunto de valores. En algunas implementaciones, se determina que el primer número aleatorio, el segundo número aleatorio y el tercer número aleatorio son iguales si $g^{r2}h^{t2} = T^{x}T1$, HE_A(*r2*) = $T'^{x}T1'$ y HE_B(r2) = $T"^{x}T1"$, donde $T = g^{r}h^{t}$ es el valor de compromiso del importe de la transferencia de saldo, T' = HE_A(r) y T" = HE_B(*r*), HE_A(*r*) se genera en base a HE de r utilizando la clave pública de la primera cuenta, HE_B(*r*) se genera en base a HE de r utilizando la clave pública de la segunda cuenta, HE_A(*r2*) se genera en base a HE de *r2* utilizando la clave pública de la primera cuenta y HE_B(*r2*) se genera en base a HE de *r2* utilizando la clave pública de la segunda cuenta, y *x* se genera aplicando la función *hash* a T1, T1' y T1". En algunas implementaciones, T, T' y T" forman el texto cifrado del importe del importe de transacción *t*.

En 710, el nodo de consenso actualiza el saldo de la primera cuenta y un saldo de la segunda cuenta en base al importe de transacción, si el primer número aleatorio, el segundo número aleatorio y el tercer número aleatorio son iguales. En algunas implementaciones, actualizar el saldo de la primera cuenta y el saldo de la segunda cuenta se realiza en base a HE.

La FIG. 8 representa otro proceso 800 de ejemplo que puede ser ejecutado de acuerdo con implementaciones de la presente divulgación. Para mayor claridad de presentación, la siguiente descripción describe generalmente el proceso 800 de ejemplo en el contexto de las otras figuras en esta descripción. Sin embargo, se entenderá que el proceso 800 de ejemplo puede realizarse, por ejemplo, mediante cualquier sistema, entorno, software y hardware, o una combinación de sistemas, entornos, software y hardware, según sea apropiado. En algunas implementaciones, las etapas del proceso 800 de ejemplo pueden ejecutarse en paralelo, en combinación, en bucles o en cualquier orden.

En 802, un nodo de consenso recibe, de una primera cuenta, una copia firmada digitalmente de un valor de compromiso de un primer importe de transacción para una transferencia desde una primera cuenta a una segunda cuenta. En algunos ejemplos, la copia firmada digitalmente del valor de compromiso se genera en base a un primer número aleatorio. El nodo de consenso también recibe el primer importe de transacción y el primer número aleatorio cifrados utilizando una clave pública de la primera cuenta, un segundo importe de la transferencia de saldo y un segundo número aleatorio cifrados utilizando una clave pública de la segunda cuenta, una o más pruebas de intervalo y un conjunto de valores generados utilizando HE en base a uno o más números aleatorios seleccionados. En algunas implementaciones, el valor de compromiso se genera utilizando el esquema de PC. En algunas implementaciones, el primer importe de la transferencia de saldo y el primer número aleatorio se cifran utilizando la clave pública de la primera cuenta en base a un algoritmo de HE probabilístico. En algunos ejemplos, el segundo importe de la transferencia de saldo y un segundo número aleatorio se cifran utilizando la clave pública de la segunda cuenta en base al algoritmo de HE probabilístico. En algunas implementaciones, el algoritmo de HE probabilístico es un algoritmo de HE de Okamoto-Uchiyama.

En algunas implementaciones, el conjunto de valores está representado por (C, D, E, *a, b, c, d*), donde *a* = *r** + *xr, b* = *t** + *xt, c* = *z1** + *xz1* y *d* = *z2** + *xz2,* donde *r**, *t*, z1** y z2* representan el uno o más números aleatorios seleccionados, r representa el primer número aleatorio, *t* representa el primer importe de la transferencia de saldo, $C = g^{r^*}h^{t^*}$, D = $u2^{r^*}v2^{z1^*}$, E = $u2^{t^*}v2^{z2^*}$, *g, h, u2* y *v2* son generadores de una curva elíptica, y *x* se genera aplicando la función *hash* a C, D y E.

En 804, el nodo de consenso verifica una firma digital correspondiente a la copia firmada digitalmente utilizando una clave pública de la primera cuenta correspondiente a una clave privada utilizada para generar la firma digital.

En 806, el nodo de consenso determina si la una o más pruebas de intervalo prueban que el importe de la transferencia de saldo es mayor que cero y menor que o igual a un saldo de la primera cuenta.

En 808, el nodo de consenso determina si el primer importe es igual al segundo importe y si el primer número aleatorio y el segundo número aleatorio son iguales en base al conjunto de valores. En algunas implementaciones, se determina que el primer importe y el segundo importe son iguales, y se determina que el primer número aleatorio y el segundo número aleatorio son iguales, si $g^{a}h^{b} = CT^{x}$, $u2^{a}v2^{c}$ = DZ_B1^{x} y $u2^{b}v2^{d}$ = EZ_B2^{x}, donde $T = g^{r}h^{t}$ es el valor de compromiso del importe de la transferencia de saldo, Z_B1 = $u2^{r}v2^{z1}$, Z_B2 = $u2^{t}v2^{z2}$. En algunos ejemplos, *z1* y *z2*

son números aleatorios utilizados para cifrar el segundo importe de transacción y el segundo número aleatorio en base al esquema de HE probabilístico.

En 810, el nodo de consenso actualiza un saldo de la primera cuenta y un saldo de la segunda cuenta en base al primer importe de la transferencia de saldo si el primer importe y el segundo importe son iguales y el primer número aleatorio y el segundo número aleatorio son iguales. En algunas implementaciones, actualizar el saldo de la primera cuenta y un saldo de la segunda cuenta se realiza en base a HE.

Las implementaciones de la materia objeto descrita en esta memoria descriptiva pueden implementarse para lograr ventajas o efectos técnicos particulares. Por ejemplo, las implementaciones de la presente divulgación permiten que el saldo de cuenta y el importe de transacción de nodos de cadena de bloques sean privados durante las transacciones. El destinatario de una transferencia de fondos no necesita confirmar la transacción o utilizar un número aleatorio para verificar un compromiso; la validación de transacción puede ser no interactiva. Un nodo de cadena de bloques puede validar la transacción en base a HE y esquemas de compromiso para permitir una prueba de conocimiento nulo.

La metodología descrita permite mejorar la seguridad de cuenta/datos de diversos dispositivos informáticos móviles. El saldo de las cuentas y los importes de transacción pueden cifrarse en base a HE y ocultarse mediante esquemas de compromiso. Por lo tanto, un nodo de consenso puede actualizar los saldos de cuenta en el libro mayor después de la transacción en base a las propiedades de HE sin revelar el saldo de cuenta real de la cuenta. Debido a que no es necesario enviar el número aleatorio a un destinatario para confirmar la transacción, se puede reducir el riesgo de fuga de datos y se necesitan menos recursos de cálculo y de memoria para gestionar el número aleatorio.

Las implementaciones y las operaciones descritas en esta memoria descriptiva se pueden implementar en circuitos de electrónica digital, o en software, firmware o hardware de ordenador, incluidas las estructuras divulgadas en esta memoria descriptiva o en combinaciones de una o más de las mismas. Las operaciones pueden implementarse como operaciones realizadas por un aparato de procesamiento de datos sobre datos almacenados en uno o más dispositivos de almacenamiento legibles por ordenador o recibidos desde otras fuentes. Un aparato de procesamiento de datos, ordenador o dispositivo informático puede abarcar aparatos, dispositivos y máquinas para el procesamiento de datos, incluidos, a modo de ejemplo, un procesador programable, un ordenador, un sistema en un chip, o múltiples chips, o combinaciones de lo anterior. El aparato puede incluir circuitos de lógica de propósito especial, por ejemplo, una unidad central de procesamiento (CPU), una matriz de puertas programables *in situ* (FPGA) o un circuito integrado específico de la aplicación (ASIC). El aparato también puede incluir código que crea un entorno de ejecución para el programa informático en cuestión, por ejemplo, código que constituye el firmware de procesador, una pila de protocolo, un sistema de gestión de bases de datos, un sistema operativo (por ejemplo, un sistema operativo o una combinación de sistemas operativos), un entorno de ejecución multiplataforma, una máquina virtual o una combinación de uno o más de los mismos. El aparato y el entorno de ejecución pueden realizar varias infraestructuras de modelos de computación diferentes, tales como servicios web, computación distribuida e infraestructuras de computación en red.

Un programa informático (también conocido, por ejemplo, como programa, software, aplicación de software, módulo de software, unidad de software, secuencia de comandos o código) se puede escribir en cualquier forma de lenguaje de programación, incluidos los lenguajes compilados o interpretados, los lenguajes declarativos o procedimentales, y se puede implementar en cualquier forma, incluso como un programa autónomo o como un módulo, componente, subrutina, objeto u otra unidad adecuada para su uso en un entorno informático. Un programa se puede almacenar en una porción de un archivo que contiene otros programas o datos (por ejemplo, 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 (por ejemplo, archivos que almacenan uno o más módulos, subprogramas o porciones de código). Un programa informático se puede ejecutar en un ordenador o en múltiples ordenadores que están ubicados en un emplazamiento o distribuidos en múltiples emplazamientos e interconectados por una red de comunicaciones.

Los procesadores para la ejecución de un programa informático incluyen, a modo de ejemplo, microprocesadores tanto de propósito general como especial, y uno o más procesadores de cualquier tipo de ordenador digital. Por lo general, un procesador recibirá instrucciones y datos de una memoria de sólo lectura o de una memoria de acceso aleatorio, o de ambas. Los elementos esenciales de un ordenador son un procesador para realizar acciones de acuerdo con instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. Por lo general, un ordenador también incluirá, o se acoplará de forma operativa para recibir datos desde o transferir datos a, o ambas cosas, uno o más dispositivos de almacenamiento masivo para almacenar datos. Un ordenador se puede integrar en otro dispositivo, por ejemplo, un dispositivo móvil, un asistente digital personal (PDA), una consola de juegos, un receptor del sistema de posicionamiento global (GPS) o un dispositivo de almacenamiento portátil. Dispositivos adecuados para almacenar instrucciones y datos de programa informático incluyen memorias no volátiles, medios y dispositivos de memoria, incluidos, a modo de ejemplo, dispositivos de memoria de semiconductores, discos magnéticos y discos magneto-ópticos. El procesador y la memoria se pueden complementar mediante, o incorporar en, circuitos lógicos de propósito especial.

Los dispositivos móviles pueden incluir microteléfonos, equipos de usuario (UE), teléfonos móviles (por ejemplo, teléfonos inteligentes), tabletas, dispositivos para llevar puestos (por ejemplo, relojes inteligentes y gafas inteligentes),

dispositivos implantados dentro del cuerpo humano (por ejemplo, biosensores, implantes cocleares), u otros tipos de dispositivos móviles. Los dispositivos móviles se pueden comunicar de forma inalámbrica (por ejemplo, utilizando señales de radiofrecuencia (RF)) con diversas redes de comunicación (descritas a continuación). Los dispositivos móviles pueden incluir sensores para determinar características del entorno actual del dispositivo móvil. Los sensores pueden incluir cámaras, micrófonos, sensores de proximidad, sensores GPS, sensores de movimiento, acelerómetros, sensores de luz ambiental, sensores de humedad, giroscopios, brújulas, barómetros, sensores de huellas dactilares, sistemas de reconocimiento facial, sensores de RF (por ejemplo, radios Wi-Fi y celulares), sensores térmicos u otros tipos de sensores. Por ejemplo, las cámaras pueden incluir una cámara orientada hacia delante o hacia atrás con lentes móviles o fijas, un flash, un sensor de imagen y un procesador de imágenes. La cámara puede ser una cámara de megapíxeles que puede capturar detalles para el reconocimiento facial y/o del iris. La cámara, junto con un procesador de datos y la información de autenticación almacenada en memoria o a la que se accede de forma remota, puede formar un sistema de reconocimiento facial. El sistema de reconocimiento facial o uno o más sensores, por ejemplo, micrófonos, sensores de movimiento, acelerómetros, sensores GPS o sensores RF, se pueden utilizar para la autenticación del usuario.

Para proporcionar interacción con un usuario, las implementaciones se pueden implementar en un ordenador que tenga un dispositivo de visualización y un dispositivo de entrada, por ejemplo, una pantalla de cristal líquido (LCD) o una pantalla de diodos orgánicos emisores de luz (OLED)/realidad virtual (VR)/realidad aumentada (AR) para mostrar información al usuario y una pantalla táctil, un teclado y un dispositivo señalador mediante el cual el usuario puede proporcionar datos de entrada al ordenador. También se pueden utilizar otros tipos de dispositivos para permitir la interacción con un usuario; por ejemplo, la retroalimentación proporcionada al usuario puede ser cualquier forma de retroalimentación sensorial, por ejemplo, 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, un ordenador puede interactuar con un usuario enviando documentos a y recibiendo documentos desde un dispositivo utilizado por el usuario; por ejemplo, enviando páginas web a un navegador web en el dispositivo cliente de un usuario en respuesta a las solicitudes recibidas desde el navegador web.

Las implementaciones se pueden implementar utilizando dispositivos informáticos interconectados mediante cualquier forma o medio de comunicación cableada o inalámbrica de datos digitales (o una combinación de los mismos), por ejemplo, una red de comunicaciones. Ejemplos de dispositivos interconectados son un cliente y un servidor generalmente remotos entre sí que normalmente interactúan a través de una red de comunicaciones. Un cliente, por ejemplo, un dispositivo móvil, puede realizar transacciones por sí mismo, con un servidor, o a través de un servidor, por ejemplo, realizando transacciones de compra, venta, pago, entrega, envío o préstamo, o autorizando las mismas. Dichas transacciones pueden ser en tiempo real de modo que una acción y una respuesta sean temporalmente próximas; por ejemplo, una persona percibe que la acción y la respuesta se producen casi simultáneamente, la diferencia de tiempo para una respuesta después de la acción de la persona es inferior a 1 milisegundo (ms) o inferior a 1 segundo (s), o la respuesta no tiene un retardo intencionado teniendo en cuenta las limitaciones de procesamiento del sistema.

Ejemplos de redes de comunicaciones incluyen una red de área local (LAN), una red de acceso por radio (RAN), una red de área metropolitana (MAN) y una red de área amplia (WAN). La red de comunicación puede incluir toda o una parte de Internet, otra red de comunicaciones o una combinación de redes de comunicaciones. La información se puede transmitir en la red de comunicaciones de acuerdo con diversos protocolos y normas, incluidos Evolución a Largo Plazo (LTE), 5G, IEEE 802, Protocolo de Internet (IP) u otros protocolos o combinaciones de protocolos. La red de comunicaciones puede transmitir datos de voz, vídeo, biométricos o de autenticación u otra información entre los dispositivos informáticos conectados.

Las características descritas como implementaciones separadas pueden implementarse, en combinación, en una sola implementación, mientras que las características descritas como una sola implementación pueden implementarse en múltiples implementaciones, por separado, o en cualquier subcombinación adecuada. No debe entenderse que las operaciones descritas y reivindicadas en un orden particular requieren ese orden particular, ni que todas las operaciones ilustradas deben realizarse (algunas operaciones pueden ser opcionales). Según corresponda, se puede realizar multitarea o procesamiento en paralelo (o una combinación de multitarea y procesamiento en paralelo).

REIVINDICACIONES

1. Un procedimiento implementado por ordenador (800), realizado por un nodo de consenso (304) de una red de cadena de bloques (102), que comprende:

recibir (802), desde una primera cuenta:

una copia firmada digitalmente de lo siguiente:

un valor de compromiso de un primer importe de una transferencia de saldo desde una primera cuenta a una segunda cuenta, generado en base a un primer número aleatorio, además del valor de compromiso,

el primer importe de la transferencia de saldo y el primer número aleatorio cifrados utilizando una primera clave pública de la primera cuenta en base a un algoritmo de cifrado homomórfico probabilístico,

un segundo importe de la transferencia de saldo y un segundo número aleatorio, donde el segundo importe y el segundo número aleatorio están cifrados utilizando una clave pública de la segunda cuenta en base al algoritmo de cifrado homomórfico probabilístico,

una o más pruebas de intervalo, y

un conjunto de valores generados en base a uno o más números aleatorios seleccionados;

verificar (804) una firma digital correspondiente a la copia firmada digitalmente utilizando una segunda clave pública de la primera cuenta correspondiente a una clave privada utilizada para generar la firma digital;

determinar (806) que la una o más pruebas de intervalo prueban que el importe de la transferencia de saldo es mayor que cero y menor que o igual a un saldo de la primera cuenta;

determinar (808) si el primer importe y el segundo importe son iguales y si el primer número aleatorio y el segundo número aleatorio son iguales, en base al segundo importe cifrado, el segundo número aleatorio cifrado, el valor de compromiso del primer importe de la transferencia de saldo generada en base al primer valor aleatorio y el conjunto de valores; y

actualizar (810) el saldo de la primera cuenta y un saldo de la segunda cuenta en base al primer importe de la transferencia de saldo en respuesta a determinar (808) que el primer importe y el segundo importe son iguales y el primer número aleatorio y el segundo número aleatorio son iguales.

2. El procedimiento implementado por ordenador (800) de la reivindicación 1, en el que el valor de compromiso se genera utilizando un esquema de compromiso que es homomórfico.

3. El procedimiento implementado por ordenador (800) de la reivindicación 2, en el que el esquema de compromiso es un esquema de compromiso de Pedersen.

4. El procedimiento implementado por ordenador (800) de una cualquiera de las reivindicaciones 1 a 3, en el que el algoritmo de cifrado homomórfico, HE, probabilístico es un algoritmo de HE de Okamoto-Uchiyama.

5. El procedimiento implementado por ordenador (800) de una cualquiera de las reivindicaciones 1 a 3, en el que los números aleatorios seleccionados están representados por r^*, t^*, $z1^*$ y $z2^*$, y los números aleatorios seleccionados se utilizan para generar a, b, c y d, donde $a = r^* + xr$, $b = t^* + xt$, $c = z1^* + xz1$ y $d = z2^* + xz2$, r es el primer número aleatorio, t es el primer importe de la transferencia de saldo, x es un valor *hash*.

6. El procedimiento implementado por ordenador (800) de la reivindicación 5, en el que el conjunto de valores se genera adicionalmente en base a C, D y E, donde $C = g^{r^*}h^{t^*}$, $D = u2^{r^*}v2^{z1^*}$, $E = u2^{t^*}v2^{z2^*}$, donde $g, h, u2$ y $v2$ son generadores de una curva elíptica, y donde x se genera aplicando una función *hash* a C, D y E.

7. El procedimiento implementado por ordenador (800) de la reivindicación 6, en el que se determina que el primer importe y el segundo importe son iguales y se determina que el primer número aleatorio y el segundo número aleatorio son iguales en base a propiedades de cifrado homomórfico probabilístico.

8. El procedimiento implementado por ordenador (800) de la reivindicación 7, en el que se determina que el primer importe y el segundo importe son iguales y se determina que el primer número aleatorio y el segundo número aleatorio son iguales si $g^a h^b = CT^x$, $u2^a v2^c = DZ\_B1^x$ y $u2^b v2^d = EZ\_B2^x$, donde $T = g^r h^t$ es el valor de compromiso del importe de la transferencia de saldo, $Z\_B1 = u2^r v2^{z1}$, $Z\_B2 = u2^t v2^{z2}$, y donde $z1$ y $z2$ son números aleatorios utilizados para

cifrar el segundo importe de la transferencia de saldo y el segundo número aleatorio en base al esquema de HE probabilístico.

9. El procedimiento implementado por ordenador (800) de la reivindicación 1, en el que actualizar (810) el saldo de la primera cuenta y un saldo de la segunda cuenta se realiza en base al cifrado homomórfico.

10. Un medio de almacenamiento no transitorio legible por ordenador acoplado a uno o más procesadores y 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 el procedimiento (800) de una o más de las reivindicaciones 1-9.

11. Un sistema, que comprende:

un dispositivo informático; y

un dispositivo de almacenamiento legible por ordenador acoplado al dispositivo informático y que tiene instrucciones almacenadas en el mismo que, cuando se ejecutan por el dispositivo informático, hacen que el dispositivo informático realice operaciones de acuerdo con el procedimiento (800) de una o más de las reivindicaciones 1-9.

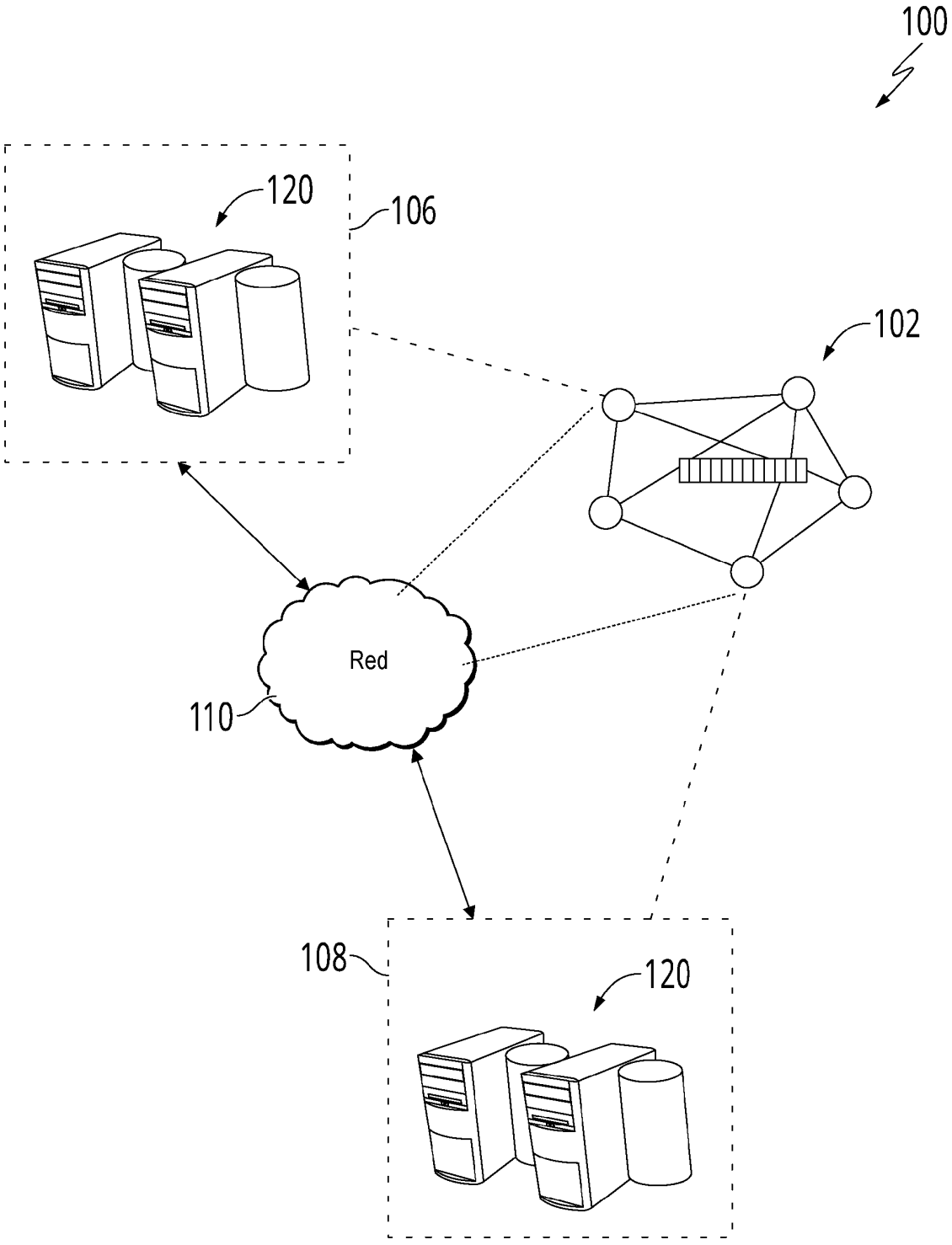

FIG. 1

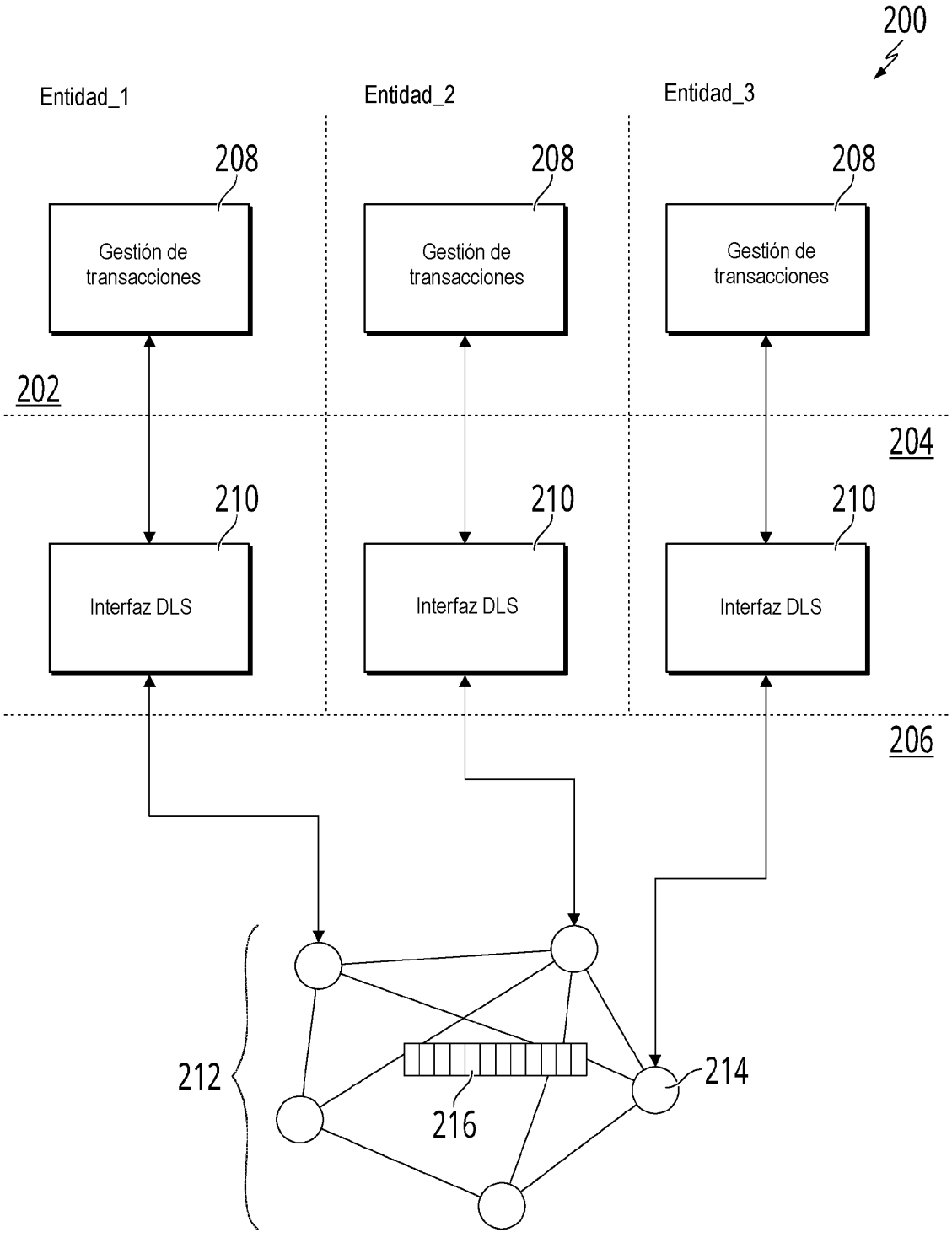
200
Entidad_1
Entidad_2
Entidad_3
208
208
208
Gestión de transacciones
Gestión de transacciones
Gestión de transacciones
202
204
210
210
210
Interfaz DLS
Interfaz DLS
Interfaz DLS
206
212
214
216

FIG. 2

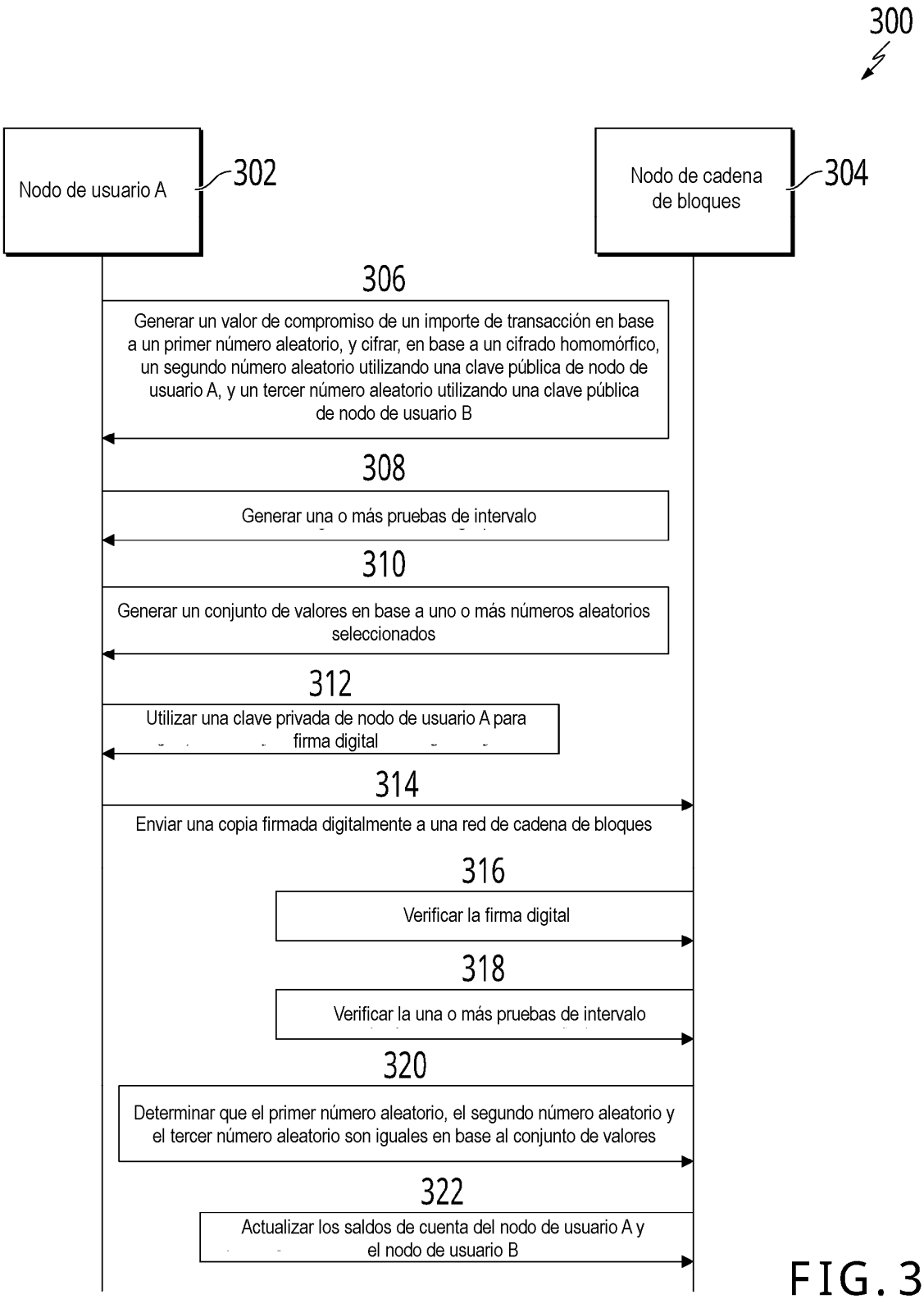
300
Nodo de usuario A
302
Nodo de cadena de bloques
304
306
Generar un valor de compromiso de un importe de transacción en base a un primer número aleatorio, y cifrar, en base a un cifrado homomórfico, un segundo número aleatorio utilizando una clave pública de nodo de usuario A, y un tercer número aleatorio utilizando una clave pública de nodo de usuario B
308
Generar una o más pruebas de intervalo
310
Generar un conjunto de valores en base a uno o más números aleatorios seleccionados
312
Utilizar una clave privada de nodo de usuario A para firma digital
314
Enviar una copia firmada digitalmente a una red de cadena de bloques
316
Verificar la firma digital
318
Verificar la una o más pruebas de intervalo
320
Determinar que el primer número aleatorio, el segundo número aleatorio y el tercer número aleatorio son iguales en base al conjunto de valores
322
Actualizar los saldos de cuenta del nodo de usuario A y el nodo de usuario B

FIG. 3

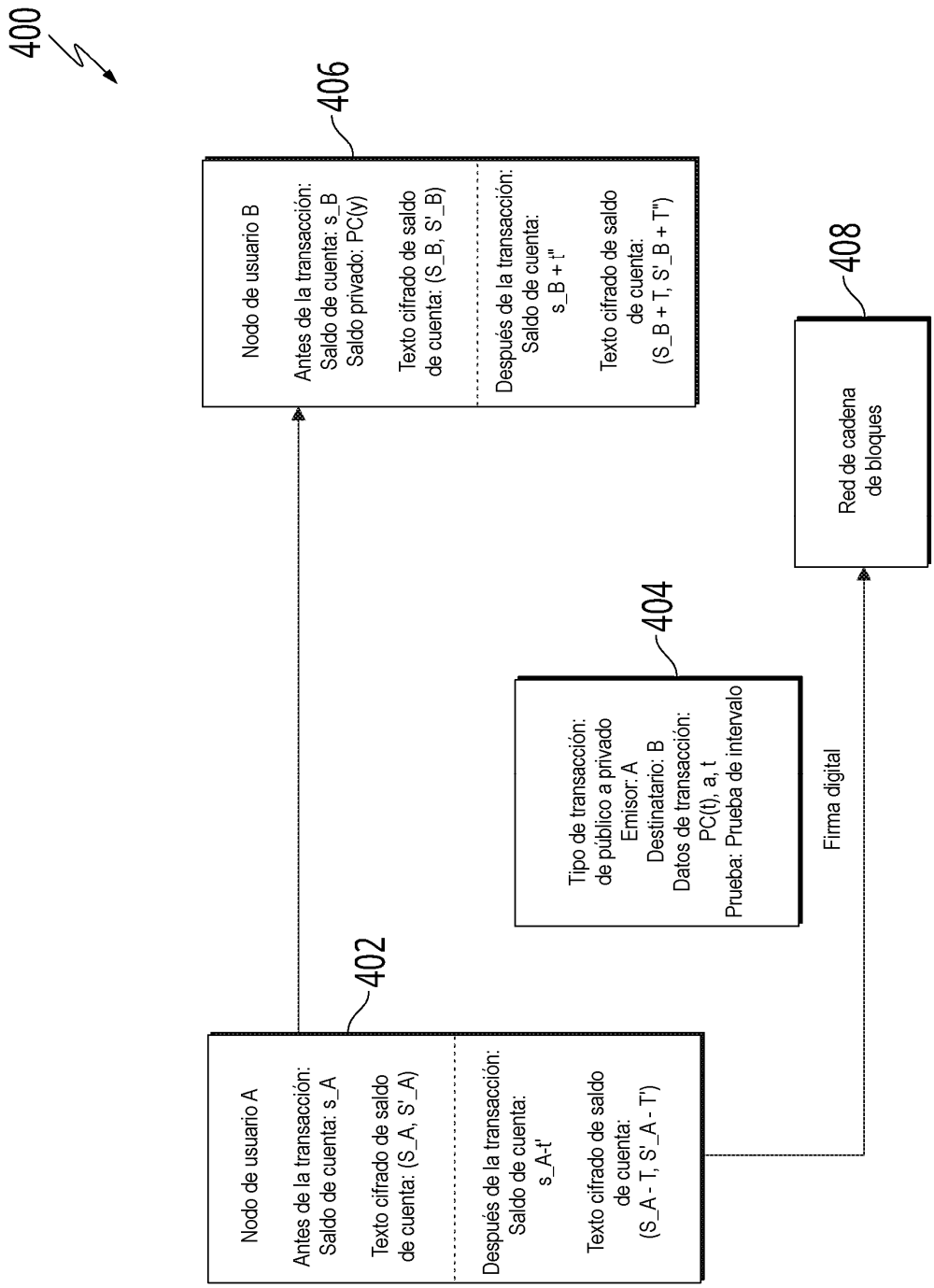
400
406
Nodo de usuario B
Antes de la transacción:
Saldo de cuenta: s_B
Saldo privado: PC(y)
Texto cifrado de saldo de cuenta: (S_B, S'_B)
Después de la transacción:
Saldo de cuenta:
s_B + t"
Texto cifrado de saldo de cuenta:
(S_B + T, S'_B + T")
408
Red de cadena de bloques
404
Tipo de transacción:
de público a privado
Emisor: A
Destinatario: B
Datos de transacción:
PC(t), a, t
Prueba: Prueba de intervalo
Firma digital
402
Nodo de usuario A
Antes de la transacción:
Saldo de cuenta: s_A
Texto cifrado de saldo de cuenta: (S_A, S'_A)
Después de la transacción:
Saldo de cuenta:
s_A-t'
Texto cifrado de saldo de cuenta:
(S_A - T, S'_A - T')

FIG. 4

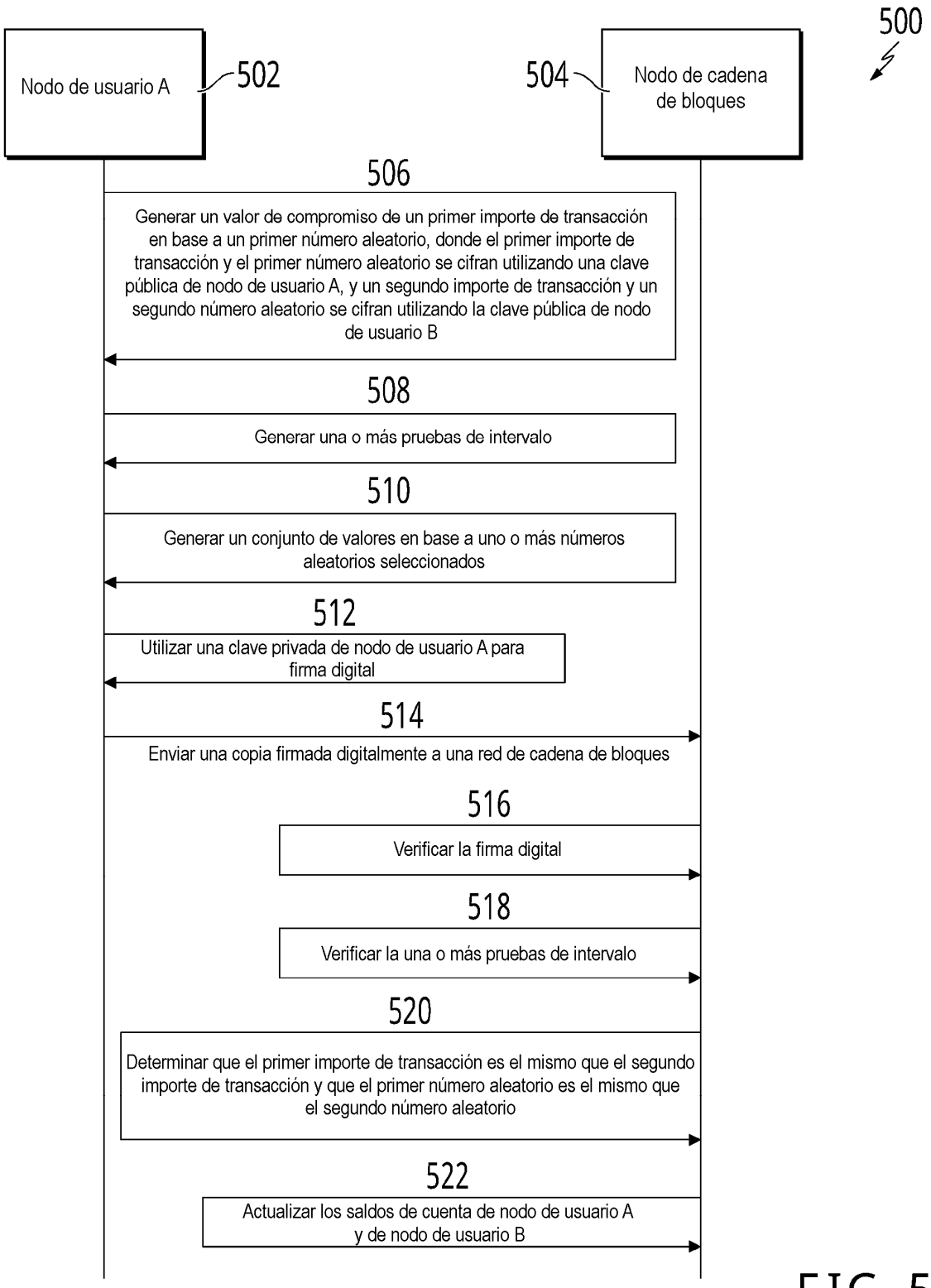
500
Nodo de usuario A
502
504
Nodo de cadena de bloques
506
Generar un valor de compromiso de un primer importe de transacción en base a un primer número aleatorio, donde el primer importe de transacción y el primer número aleatorio se cifran utilizando una clave pública de nodo de usuario A, y un segundo importe de transacción y un segundo número aleatorio se cifran utilizando la clave pública de nodo de usuario B
508
Generar una o más pruebas de intervalo
510
Generar un conjunto de valores en base a uno o más números aleatorios seleccionados
512
Utilizar una clave privada de nodo de usuario A para firma digital
514
Enviar una copia firmada digitalmente a una red de cadena de bloques
516
Verificar la firma digital
518
Verificar la una o más pruebas de intervalo
520
Determinar que el primer importe de transacción es el mismo que el segundo importe de transacción y que el primer número aleatorio es el mismo que el segundo número aleatorio
522
Actualizar los saldos de cuenta de nodo de usuario A y de nodo de usuario B

FIG. 5

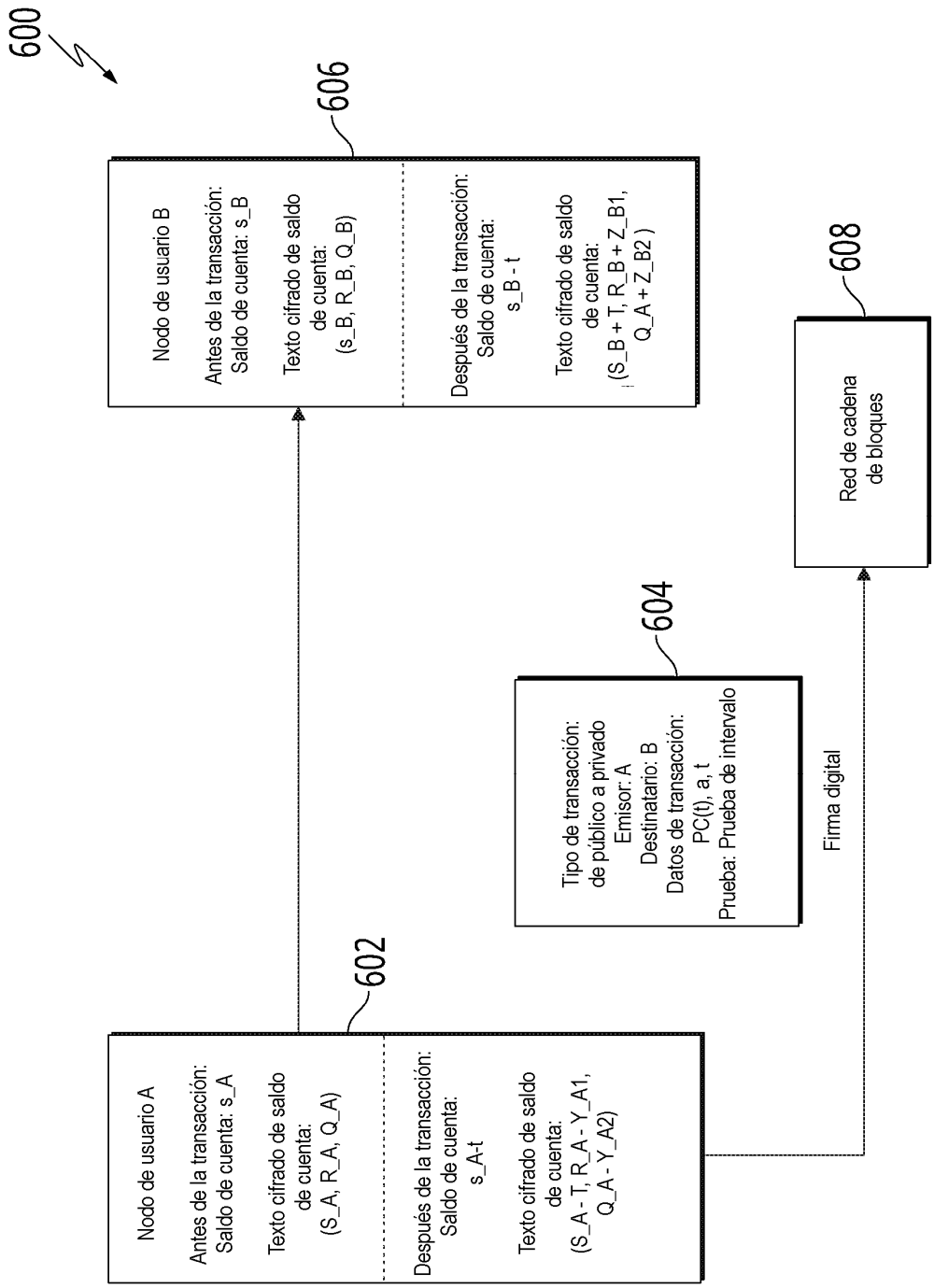
600
606
Nodo de usuario B
Antes de la transacción:
Saldo de cuenta: s_B
Texto cifrado de saldo de cuenta:
(s_B, R_B, Q_B)
Después de la transacción:
Saldo de cuenta:
s_B - t
Texto cifrado de saldo de cuenta:
(S_B + T, R_B + Z_B1, Q_A + Z_B2)
608
Red de cadena de bloques
604
Tipo de transacción:
de público a privado
Emisor: A
Destinatario: B
Datos de transacción:
PC(t), a, t
Prueba: Prueba de intervalo
Firma digital
602
Nodo de usuario A
Antes de la transacción:
Saldo de cuenta: s_A
Texto cifrado de saldo de cuenta:
(S_A, R_A, Q_A)
Después de la transacción:
Saldo de cuenta:
s_A-t
Texto cifrado de saldo de cuenta:
(S_A - T, R_A - Y_A1, Q_A - Y_A2)

FIG. 6

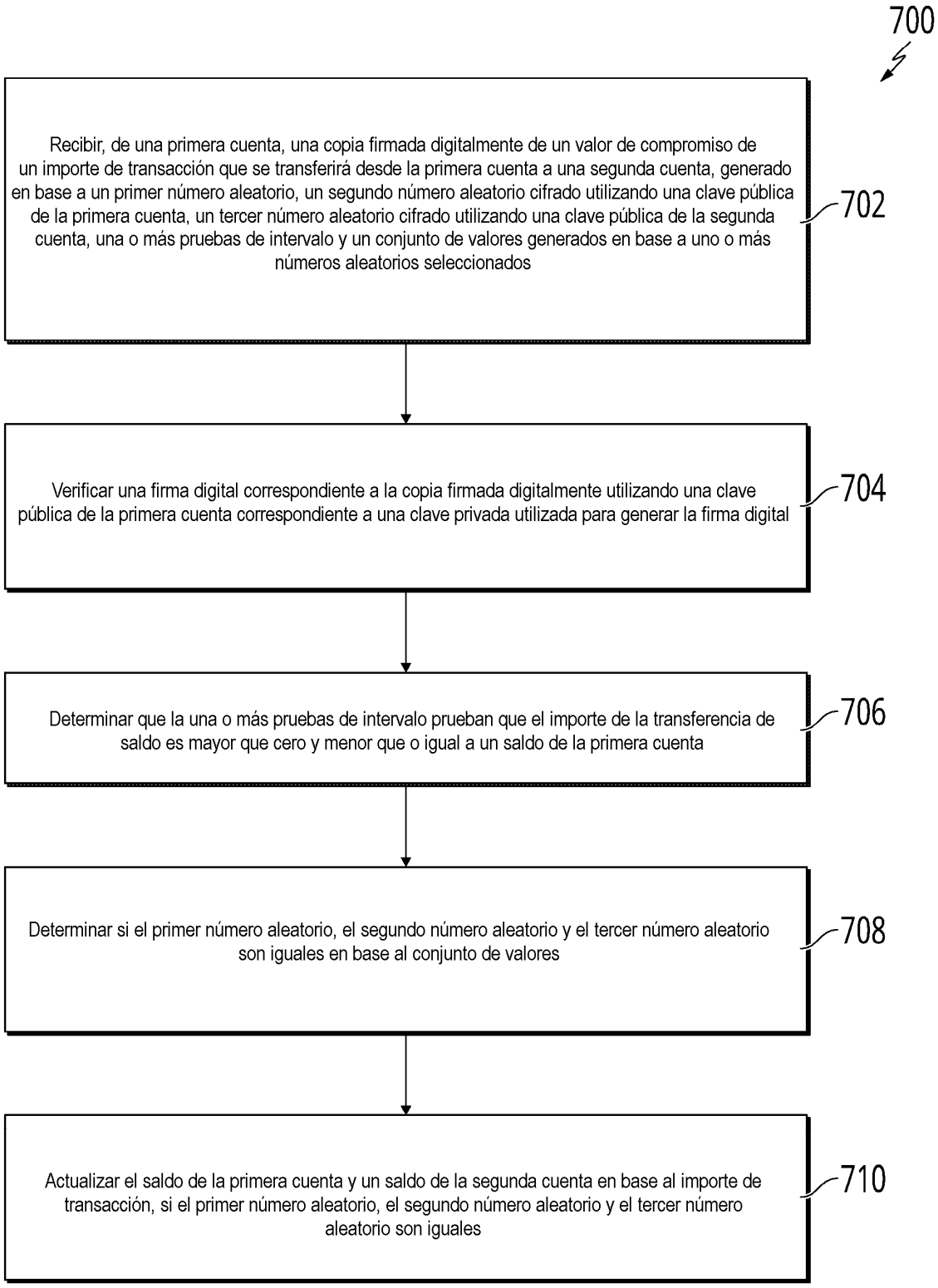
700
Recibir, de una primera cuenta, una copia firmada digitalmente de un valor de compromiso de un importe de transacción que se transferirá desde la primera cuenta a una segunda cuenta, generado en base a un primer número aleatorio, un segundo número aleatorio cifrado utilizando una clave pública de la primera cuenta, un tercer número aleatorio cifrado utilizando una clave pública de la segunda cuenta, una o más pruebas de intervalo y un conjunto de valores generados en base a uno o más números aleatorios seleccionados
702
Verificar una firma digital correspondiente a la copia firmada digitalmente utilizando una clave pública de la primera cuenta correspondiente a una clave privada utilizada para generar la firma digital
704
Determinar que la una o más pruebas de intervalo prueban que el importe de la transferencia de saldo es mayor que cero y menor que o igual a un saldo de la primera cuenta
706
Determinar si el primer número aleatorio, el segundo número aleatorio y el tercer número aleatorio son iguales en base al conjunto de valores
708
Actualizar el saldo de la primera cuenta y un saldo de la segunda cuenta en base al importe de transacción, si el primer número aleatorio, el segundo número aleatorio y el tercer número aleatorio son iguales
710

FIG. 7

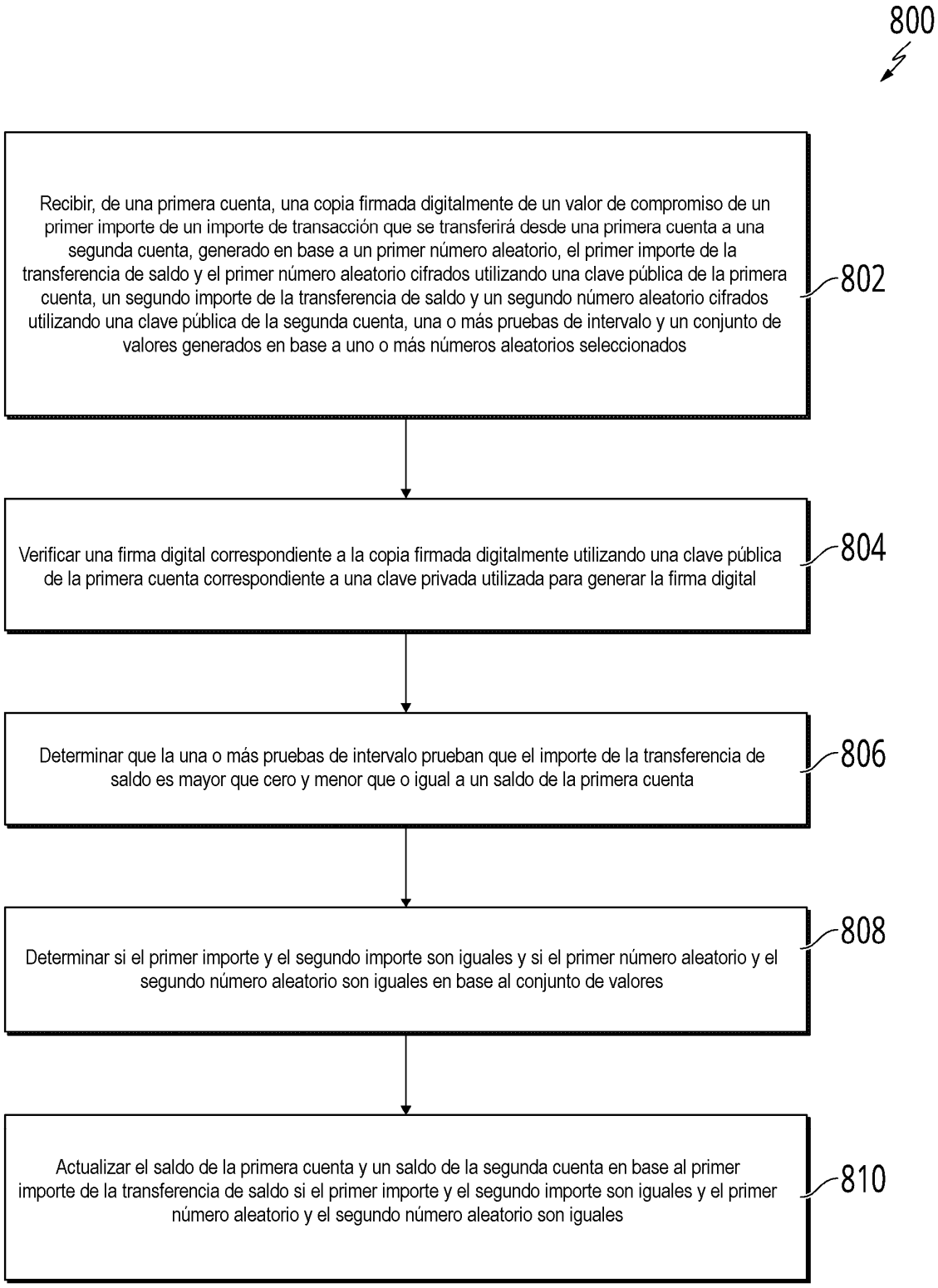
800
Recibir, de una primera cuenta, una copia firmada digitalmente de un valor de compromiso de un primer importe de un importe de transacción que se transferirá desde una primera cuenta a una segunda cuenta, generado en base a un primer número aleatorio, el primer importe de la transferencia de saldo y el primer número aleatorio cifrados utilizando una clave pública de la primera cuenta, un segundo importe de la transferencia de saldo y un segundo número aleatorio cifrados utilizando una clave pública de la segunda cuenta, una o más pruebas de intervalo y un conjunto de valores generados en base a uno o más números aleatorios seleccionados
802
Verificar una firma digital correspondiente a la copia firmada digitalmente utilizando una clave pública de la primera cuenta correspondiente a una clave privada utilizada para generar la firma digital
804
Determinar que la una o más pruebas de intervalo prueban que el importe de la transferencia de saldo es mayor que cero y menor que o igual a un saldo de la primera cuenta
806
Determinar si el primer importe y el segundo importe son iguales y si el primer número aleatorio y el segundo número aleatorio son iguales en base al conjunto de valores
808
Actualizar el saldo de la primera cuenta y un saldo de la segunda cuenta en base al primer importe de la transferencia de saldo si el primer importe y el segundo importe son iguales y el primer número aleatorio y el segundo número aleatorio son iguales
810

FIG. 8