

DISPOSICIÓN DE CADENAS DE BLOQUES CON UNA TRANSACCIÓN RESTRINGIDA

Objeto

La presente invención se refiere a la transferencia o transacción de información y, más específicamente, a un proveedor de una solución blockchain; a saber, red de bloques en
5 cadena distribuida que valida y distribuye bloques de registros de transacciones de información que pueden estar encriptadas, de manera que, al menos un miembro destinatario, conectado a la red de bloques en cadena, es capaz de descifrar, leer y ejecutar los bloques de registro de transacciones de información encriptados por los nodos validadores o mineros de la red de bloques en cadena.

10 Estado de la técnica

Dentro de cualquier industria, existen numerosas redes privadas construidas alrededor de servicios y o activos de servicios específicos. Una red privada construida alrededor de un activo financiero puede incluir una pluralidad de miembros de la red tal como un proveedor de servicios; por ejemplo, bancos, agencias de compensación o similar; instituciones
15 reguladoras, clientes, etc. que solicitan la transferencia de un activo financiero.

Una de las principales preocupaciones de las redes privadas, y de cualquier red en general, es garantizar que el contenido de las transacciones que ejecutan sus sistemas, únicamente sean reveladas a los participantes de las transacciones.

Por ejemplo, un proveedor de servicios que procesa una transferencia de información de
20 un activo financiero de un primer cliente no revelaría el contenido de esa transferencia de información a clientes no autorizados que no están involucrados en la transferencia.

Aunque el proveedor de servicios desarrolle un sistema propio para que los demás actores interactúen con su sistema, el resto de los integrantes de la red también desarrollan sus propios sistemas para que sea posible la integración con el proveedor de servicios. Este
25 escenario conlleva intrínsecamente la convivencia de numerosos sistemas creados con tecnologías diferentes e interconectados además con diferentes protocolos. Esta diversidad de sistemas conduce a varios problemas de difícil solución:

Primero, cada sistema individual es intrínsecamente diferente a otro sistema individual ya sea por la tecnología utilizada para su desarrollo, así como las adaptaciones propias de
30 cada participante. Además de requerir una inversión significativa y particularizada de cada uno de los participantes para integrar y transmitir la información entre los sistemas de forma adecuada.

Segundo, cada sistema individual puede diferir en el nivel de seguridad implementada. Por ejemplo, cada red puede proporcionar diferentes protocolos para el cifrado, la autenticación, el enmascaramiento de datos y similares. Por lo tanto, algunos sistemas pueden ser más susceptibles de verse comprometidos, afectando tanto al sistema
5 comprometido como a los datos que el resto de los sistemas hayan compartido con este.

En tercer lugar, la diferente naturaleza de cada sistema implica que los datos se almacenan de forma no estandarizada. Esto hace que se deban producir repetitivas conciliaciones de datos para verificar que los subconjuntos de datos compartidos entre los diferentes sistemas son equivalentes.

10 Por último, en cuarto lugar, ante una eventual pérdida de información de uno de los participantes la recuperación de la información será considerablemente costosa y requerirá de un tiempo considerable en la que el sistema afectado no estará disponible.

Sumario

La presente invención busca resolver uno o más de los inconvenientes expuestos
15 anteriormente mediante una disposición de cadena de bloques con al menos una transacción restringida tal como es definida en las reivindicaciones.

El sistema blockchain propuesto proporciona capacidades de anonimato y privacidad inexistentes actualmente en otros sistemas blockchain. Estas dos nuevas capacidades se desarrollan como elemento diferenciador en una única cadena de bloques, que es
20 compartida por todos los nodos integrantes de una red de bloques en cadena.

La red de bloques en cadena comprende una pluralidad de nodos participantes y nodos validadores o mineros con un mecanismo de consenso de prueba de autoridad.

El método proporciona, a la pluralidad de nodos validadores, la capacidad de transformar un bloque de registro de transacción de información propuesto para una transacción
25 restringida desde un nodo participante proponente, en un bloque de registro de transacción de información restringido y anónimo, que es transmitido hacia la pluralidad de nodos participantes destinatarios o nodos blockchain de la red de bloques en cadena.

Los nodos validadores receptores están configurados para transmitir bloques con registros de transacciones de información encriptados hacia los nodos participantes destinatarios de
30 la red de bloques en cadena.

La transacción validada por el nodo validador receptor; a saber, nodo minero, se transmitirá desde el nodo validador receptor hacia todos los nodos participantes destinatarios de la

red de bloques en cadena al igual que lo haría un registro de transacción de información público; esto es, dentro de un bloque de la cadena de bloques.

La transacción validada es encriptada por el nodo validador receptor para que los nodos participantes de la transacción sean los únicos capaces de leerla y ejecutarla.

- 5 Por lo tanto, la cadena de bloques estará formada por bloques que contendrán indistintamente registros de transacciones de información públicos y/o restringidos; a saber, privados.

Es importante resaltar que la solución sólo emplea una única cadena de bloques en la que coexisten al menos dos tipos de registros de transacciones de información; esto es
10 registros de transacciones de información públicos y/o registros de transacciones de información restringidos (privados y anónimos).

Un nodo validador está configurado para encriptar los registros de transacciones de información propuestos desde los nodos participantes proponentes; de manera que, el nodo validador proporciona registros de transacciones de información restringidos al final
15 de la etapa de encriptado.

Los registros de transacciones de información encriptados sólo pueden ser descifrados y ejecutados por los nodos participantes de la red de bloques en cadena, que estén en posesión de una clave de privacidad de encriptado correspondiente al grupo de privacidad dentro del que se realiza la transacción restringida propuesta.

- 20 Se ha de entender por grupo de privacidad a un subconjunto de nodos de la red de bloques en cadena que comparten, al menos, una clave de privacidad de encriptado para leer las transacciones restringidas realizadas entre los nodos del grupo de privacidad.

Un miembro de la red de bloques en cadena puede formar parte de al menos un grupo de privacidad y, como máximo, puede pertenecer a tantos grupos de privacidad como
25 combinaciones de miembros diferentes comprenda la red de bloques en cadena.

Un nodo participante o nodo blockchain de la red de bloques en cadena, se refiere a una persona física o jurídica que mantiene, comparte y opera con su propia copia local de la cadena de bloques; a saber, libro de registros o ledger.

- Además, un miembro se refiere a una persona física o jurídica que realiza transacciones
30 de información y está autorizada para acceder a determinados registros de transacciones de información de la cadena de bloques.

Los nodos participantes contendrán una pluralidad de claves de privacidad de encriptado destinado a realizar registros de transacciones de información restringidas dentro de los grupos de privacidad en los que estén incluidos.

5 El nodo validador encripta un registro de transacción de información propuesto desde el nodo participante proponente con la clave de privacidad de encriptado de un determinado grupo de privacidad y, adicionalmente, marca el bloque de datos de registro de transacción encriptado como restringido y, seguidamente, el bloque creado, que comprende un registro de transacción de información encriptado, es ensamblado en la cadena de bloques para la posterior distribución desde los nodos validadores hacia el resto de nodos integrantes de la red de bloques en cadena.

Por lo tanto, cualquier miembro del grupo de privacidad conectado a la red de bloques en cadena puede acceder a los detalles de determinadas transacciones de información incluidas en el nuevo bloque creado.

15 El nodo participante destinatario descifra los registros de transacciones de información restringidas del bloque creado utilizando la correspondiente clave de privacidad de encriptado de entre su conjunto de claves de privacidad de encriptado asignada a cada grupo de privacidad.

20 Por lo tanto, el sistema proporciona registros de transacciones restringidas o privadas y públicas contenidas en un bloque y que finalmente son ensambladas en la cadena de bloques y distribuidas uniformemente a todos los miembros de la red, proporcionando no solo privacidad a las transacciones por la encriptación, sino anonimato porque los bloques son distribuidos sólo por los nodos validadores.

Todos los miembros de la red de la cadena de bloques utilizan una única cadena o ledger y, por lo tanto, se eliminan los recursos redundantes para administrar sistemas individuales.

25 La privacidad se logra a través del encriptado ya que los miembros de la red de cadenas de bloques solo pueden acceder a los detalles de las transacciones de información a las que tienen derecho; es decir, son miembros de una porción de nodos o grupo de privacidad de la red de cadenas de bloques.

30 El empleo de algoritmos de resumen de información establecen, además, la inmutabilidad de los registros de transacciones, protegiendo así contra posibles actos maliciosos. La resistencia de los datos se mejora a medida que los registros de transacciones cifrados son almacenados localmente por los miembros.

Breve descripción de las figuras

Una explicación más detallada se da en la descripción que sigue y que se basa en la figura adjunta:

la figura 1 muestra en un diagrama de bloques una red de bloques en cadena que comprende una pluralidad de nodos que están conectados a través de una red de telecomunicaciones para difundir o propagar simultáneamente registros de transacción de información públicos y privados de una cadena de bloques.

Descripción

En relación con la figura 1 donde se muestra esquemáticamente un entorno de una red de bloques en cadena 11 donde una pluralidad de nodos, participantes 12 y validadores o mineros 13, están conectados a través de una red de telecomunicaciones 14 para compartir y ejecutar transacciones distribuidas dentro de bloques de datos que se agregan a una cadena de bloques o blockchain.

La cadena de bloques es distribuida a través de la red de telecomunicaciones 14 desde un nodo validador 13 hacia el resto de los nodos 12, 13 de la red de bloques en cadena 11.

La red de telecomunicaciones 14 puede ser una red del tipo red de área local, LAN, cableada o inalámbrica, red de área amplia, WAN, tal como una intranet, una extranet o Internet; o similar. La red de telecomunicaciones 14 facilita las comunicaciones entre los nodos 12, 13 de la red de bloques en cadena 11.

Los nodos 12, 13 de la red de bloques en cadena 11 son dispositivos electrónicos del tipo un ordenador que ejecuta un sistema operativo.

Los nodos 12, 13 que integran la red de bloques en cadena 11 están configurados para ejecutar instrucciones almacenadas en un medio de almacenamiento legible por ordenador. Asimismo, todos los nodos 12, 13 ejecutan protocolos de comunicación para interactuar con los servicios y/o el contenido proporcionado por la red de bloques en cadena 11.

Todos los nodos 12, 13 de la red de bloques en cadena 11 tienen acceso de lectura a los datos de la cadena en su propia copia local. Sólo los nodos validadores o mineros 13 pueden emitir o crear nuevos bloques con registros de transacciones públicas y restringidas.

Una transacción pública y/o restringida; a saber, privada se transmite desde un nodo validador 13 hacia otros nodos validadores para validación y consenso. Una vez que la transacción es validada y consensuada, el nodo validador genera un bloque de datos para

agregar a la cadena de bloques. Cada bloque de datos incluye un hash relativo al bloque de datos inmediatamente anterior para así evitar la modificación de la información previa.

Sin embargo, si un nodo participante 12 propone una transacción privada o restringida, la transacción propuesta tiene que ser validada por la mayoría de los nodos validadores o mineros 13. Esta transacción se transmite a los nodos validadores o mineros 13 mediante una red de telecomunicaciones 14.

El nodo validador 13 receptor del mensaje de solicitud de ejecución de transacción restringida determina los nodos participantes 12 en función de los integrantes introducidos en un determinado grupo de privacidad preconfigurado.

El mensaje de solicitud de ejecución de la transacción restringida comprende además de los datos propios de la transacción propuesta los metadatos relativos al contexto de privacidad para el que se ejecuta la transacción restringida.

La transacción restringida propuesta es transmisible desde el nodo validador 13 receptor a al menos uno o más nodos validadores 13 para su validación y consenso. Cada nodo validador 13 determina si una transacción es válida y si consensua con el resto de nodos validadores 13 si debe integrarse en siguiente bloque de la cadena.

Por lo tanto, la red 11 de nodos participantes 12 y validadores 13 mantienen y gestionan la cadena de bloques de datos compuestos simultáneamente por transacciones públicas y/o restringidas; de manera que, cada nodo 12, 13 tiene acceso a la totalidad de bloques de datos, ya sean registro de transacciones de información públicas o restringidas, aunque sólo los nodos participantes 12 del determinado grupo de privacidad tienen acceso simultáneo a la transacción restringida y a transacciones públicas.

Una transacción propuesta por un nodo participante 12 de la red de bloques en cadena tiene un identificador único que corresponde con la ejecución de una función matemática de resumen como MD5, un algoritmo de algoritmo hash seguro, SHA, BLAKE u otras funciones hash similares sobre su contenido binario. A este identificador único se le denominará hash de la transacción.

Para el inicio de la emisión de una transacción de información restringida, el nodo participante 12 proponente envía a todos los nodos validadores 13 el contenido del registro de transacción de información t_x , junto con el identificador del grupo de privacidad.

Los nodos validadores 13 ejecutan la transacción de información y, una vez, que la transacción de información ha sido validada y consensuada por una mayoría de nodos validadores 13, el registro de transacción de información t_x es encriptado por un módulo encriptador del nodo validador 13.

La transacción de información t_x encriptada es recubierta por una nueva transacción de información t_x' ; de manera que, la transacción de información t_x' es forzada a mantener el mismo identificador hash que la transacción de información t_x . De esta forma, el bloque de datos encriptado es marcado como una transacción de información t_x restringida para la

5 que sólo los nodos participantes 12 que poseen la clave de privacidad de encriptado son capaces de leer y ejecutar la transacción de información t_x restringida.

El bloque de datos encriptado y marcado de la cadena de bloques será distribuido por los nodos validadores 13 de la red de bloques en cadena y comprenderá de 0 a N transacciones y, al menos, una transacción de información t_x' ; a saber, un bloque de datos

10 encriptado y marcado como restringido. A los nodos participantes 12 en el grupo de privacidad de t_x , se les informa además que t_x' es una transacción destinada a ese grupo de privacidad.

Los nodos validadores 13 están habilitados para, una vez recibidos los metadatos de restricción desde el nodo participante 12 proponente, ejecutar, validar, empaquetar y

15 entregar todas las transacciones restringidas a los nodos participantes 12 pertenecientes al grupo de privacidad.

Los nodos participantes 12, que desean realizar una transacción de información restringida dentro del grupo de privacidad, están configurados para desencriptar los bloques encriptado distribuidos desde los nodos validadores 13, mediante la correspondiente clave

20 de privacidad de encriptado correspondiente al grupo de privacidad de la transacción.

Los nodos validadores 13 están configurados para realizar tareas de administración del grupo de privacidad formado tal como distribuir un conjunto de claves de privacidad de encriptado. Una clave de privacidad del conjunto de claves de privacidad de encriptado es utilizada por los nodos validadores 13 para encriptar las transacciones de información

25 propuestas que tienen que ser encriptadas y marcadas como bloques de datos restringidos antes de ser ensamblados dentro de un bloque y, posterior, distribución a todos los nodos 12 de la red de bloques en cadena; es decir, a los nodos 12 del grupo de privacidad y al resto de nodos de la red de bloques en cadena 11.

Para que un nodo participante 12 de la red de bloques en cadena pueda realizar una transacción de información restringida con al menos un determinado nodo participante 12

30 de la red de bloques en cadena 11, ambos nodos participantes 12 de la red de bloques en cadena 11 tienen que pertenecer al mismo grupo de privacidad.

Todos los nodos 12 de la red de bloques en cadena 11 reciben cada uno de los bloques de datos de la cadena de bloques existente y, sucesivamente, de forma continua la cadena de bloques avanza.

5 Por lo tanto, todos los nodos 12, 13 de la red bloques en cadena de tienen almacenada la misma copia binaria de la cadena de bloques; a saber, libro de registros distribuido, ledger, inmutable, que incluye tanto las transacciones públicas como privadas. Los nodos participantes 12 y validadores 13 de la red de bloque en cadena 11 comprenden al menos una interfaz de entrada-salida para realizar comunicaciones entre los distintos nodos 12, 13 de la red de bloques en cadena 11, al menos un módulo encriptador-desencriptador, un
10 almacén de grupos de privacidad que comprende al menos un nodo participante 12 y al menos un conjunto de claves de privacidad de encriptado y un almacén de bloques en cadena; a saber, libro de registros distribuido, ledger.

El almacén de grupos de privacidad de los nodos participantes 12 almacenará sólo los grupos de privacidad en los que sea integrante el nodo participante 12. Por el contrario, el
15 almacén de grupos de privacidad de los nodos validadores 13 será el resultado del superconjunto de los grupos de privacidad de cada nodo, o lo que es lo mismo, los grupos de privacidad que se puedan formar con los n-1 nodos participantes 12 de la red de bloques en cadena 11.