(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 791 185**

(51) Int. CI.:

G06Q 20/38 (2012.01)
G06Q 20/42 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.03.2014 PCT/GB2014/050866**

(87) Fecha y número de publicación internacional: **25.09.2014 WO14147399**

(96) Fecha de presentación y número de la solicitud europea: **19.03.2014 E 14718448 (5)**

(97) Fecha y número de publicación de la concesión europea: **06.05.2020 EP 2976739**

(54) Título: **Método y sistema para transferir datos**

(30) Prioridad:

19.03.2013 GB 201305040

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.11.2020

(73) Titular/es:

VISA EUROPE LIMITED (100.0%)
1 Sheldon Square
London W2 6TT, GB

(72) Inventor/es:

TARATINE, BORIS

(74) Agente/Representante:

SÁNCHEZ SILVA, Jesús Eladio

DESCRIPCIÓN

Método y sistema para transferir datos

Campo de la invención

La presente invención se refiere a sistemas y métodos para transferir datos donde los datos de un primer tipo se transfieren a un nodo mediante el uso de un protocolo, y donde los segundos datos, de un tipo no incluido en el protocolo, se ponen a disposición para su recuperación por el nodo.

Antecedentes

En sistemas de comunicaciones, los protocolos se definen para permitir la transferencia de datos entre diferentes nodos de red. Cualquier protocolo dado puede especificar un número de aspectos de cómo se transfieren los datos. Los datos de un primer tipo, incluido en el protocolo, pueden transferirse mediante el uso de ese protocolo. Los datos de un segundo tipo, no incluido en el protocolo, pueden no ser transferibles.

Cualquier número de factores puede diferenciar los datos del primer tipo del segundo. Por ejemplo, un protocolo dado puede especificar determinados campos de datos. Los datos capaces de transferirse de conformidad con el protocolo, es decir los datos del primer tipo, deben corresponder a uno de los campos especificados. Los datos que no corresponden a un campo especificado, es decir, los datos del segundo tipo, no se incluyen en el protocolo y por lo tanto no pueden transferirse fácilmente.

Cuando se desea que los datos de este segundo tipo se transfieran de un primer a un segundo nodo, la solución típica es actualizar el protocolo para incluir este segundo tipo de datos; en otras palabras al actualizar un estándar de protocolo existente para incluir nuevos campos. Sin embargo esto puede ser difícil por varias razones. Por ejemplo, cualquier primer nodo dado (el nodo remitente) puede necesitar ser capaz de comunicarse con múltiples segundos nodos (receptores). Cuando solamente un subconjunto de los segundos nodos requiere los datos del segundo tipo, se puede dificultar asegurar la compatibilidad entre el primer nodo y todos los segundos nodos. Adicionalmente, en algunos sistemas, los datos se transfieren del primer nodo al segundo nodo a través de uno o más terceros nodos. Por lo tanto, la actualización del protocolo requiere la actualización no solamente del primer y del segundo nodo, sino también de todos los terceros nodos. Esto puede ser difícil, especialmente cuando los terceros nodos se operan por organizaciones diferentes a las que operan el primer y el segundo nodo.

Por lo tanto, es conveniente proporcionar métodos y sistemas que permitan la transferencia de tales datos.

El documento US 2012/072346 analiza una red de procesamiento de pagos que utiliza una tarjeta de pago de número doble que incluye dos números que son necesarios para la identificación y autenticación completa de la tarjeta. Al realizar una transacción en línea, el primer número de la tarjeta se suministra al sitio web comercial durante el pago, y posteriormente se le suministra un segundo número de la tarjeta, junto con un número de pedido recibido desde el sitio web comercial, a un sistema de validación por teléfono. El sistema de validación obtiene entonces el primer número de tarjeta del sitio web comercial y valida la transacción.

Resumen de la invención

De acuerdo con la invención, se proporciona un método para transferir datos de transacción en un sistema de procesamiento de pagos como se reivindica en la reivindicación independiente 1.

En muchos sistemas de comunicaciones, los protocolos se configuran para permitir que los datos se transfieran de un nodo a otro. Los protocolos establecen el tipo de contenido que puede transferirse mediante el uso del protocolo. Una vez establecidos, los protocolos se vuelven difíciles de cambiar, ya que cada nodo necesita actualizarse para poder usar un protocolo modificado. En consecuencia, es difícil cambiar los tipos de datos que pueden transferirse (es decir, al agregar nuevos campos, o expandir los campos existentes).

Las modalidades de la invención superan este problema al usar un primer protocolo para transferir los primeros datos de un primer tipo soportado por el primer protocolo, mientras almacena los segundos datos, que no se incluyen en los datos enviados de acuerdo con el primer protocolo, en una memoria. Estos segundos datos pueden recuperarse entonces por un segundo nodo según se requiera. Esto proporciona la ventaja de que pueden proporcionarse datos adicionales, es decir datos del segundo tipo, sin tener que modificar el protocolo.

Además, solo los segundos nodos que desean el segundo tipo de datos necesitan recuperar los segundos datos. Cualquier segundo nodo que no desee el segundo tipo de datos adicional, no necesita cambiar ninguna parte de su operación, ya que los datos proporcionados por el primer protocolo aún se proporcionarán de la manera habitual.

Los primeros datos pueden comprender una pluralidad de elementos de los primeros datos, y los segundos datos pueden comprender una pluralidad de elementos de los segundos datos asociados con los elementos de los primeros

datos correspondientes. Además, la solicitud puede comprender datos que identifican al menos un elemento de los segundos datos. Estos datos que identifican al menos un elemento de los segundos datos pueden corresponder a una identidad de dicho al menos un segundo nodo. Alternativa o adicionalmente, los datos que identifican al menos un elemento de los segundos datos pueden corresponder a los datos incluidos en un elemento de los primeros datos correspondiente. En algunas modalidades, los elementos de los primeros datos pueden comprender identificadores, y el al menos un elemento de los segundos datos puede almacenarse en conjunto con un identificador de un elemento de los primeros datos correspondiente.

En otras palabras, los elementos de datos dentro de los primeros datos se asocian con elementos de datos dentro de los segundos datos. Esto puede habilitarse mediante el uso de identificadores compartidos entre los elementos de los primeros y segundos datos correspondientes. Esto a su vez permite que un segundo nodo recupere fácilmente los segundos datos correspondientes a los primeros datos recibidos mediante el uso del primer protocolo. En algunas modalidades, la identidad del segundo nodo puede usarse para acceder a los datos, con una pluralidad de partes de los segundos datos que se proporcionan al segundo nodo en base a esa identidad.

El método comprende generar al menos una parte de un elemento de los segundos datos usando al menos una parte de un elemento de los primeros datos correspondiente como una entrada a un algoritmo de procesamiento de datos. El algoritmo de procesamiento de datos calcula una función resumen. Adicionalmente, el algoritmo de procesamiento de datos calcula una firma digital. Esta firma digital se calcula mediante el uso de una clave criptográfica.

En modalidades, los primeros datos, que son los datos soportados por el primer protocolo, se usan para generar los segundos datos. Los segundos datos se usan posteriormente para determinar si los primeros datos se han modificado en tránsito entre el primer y el segundo nodo. Para generar estos datos, el primer nodo genera una función resumen de los datos y posteriormente firma la salida de la función resumen. Los datos resumidos y/o firmados se almacenan entonces en la memoria.

El primer nodo y el segundo nodo pueden tener una relación de confianza. Además, los primeros datos pueden enviarse a través de al menos un tercer nodo que no tiene una relación de confianza con el primer y el segundo nodo. Los primeros datos enviados mediante el uso del primer protocolo pueden enviarse de acuerdo con un formato, dicho formato es uno que puede interpretarse por el tercer nodo. El primer, el segundo y el tercer nodo pueden disponerse para cooperar en una interacción para la cual tanto el segundo nodo como el tercer nodo requieren dichos primeros datos.

Al tener una relación de confianza, el al menos un segundo nodo sabe que los datos enviados, y almacenados en la memoria, por el primer nodo pueden ser confiables, es decir, son correctos y pueden ser confiables. Sin embargo, este puede no ser el caso del tercer nodo, y por lo tanto no puede confiar en cualquier dato enviado por medio del tercer nodo. Esto es particularmente significativo cuando el protocolo especifica que los datos son legibles, y por lo tanto editables, por el tercer nodo (esto puede contrastarse con un nodo de red que simplemente dirige los datos hacia el segundo nodo). El tercer nodo puede requerir que los datos sean legibles debido a que el primero, al menos un segundo y al menos un tercer nodo se disponen para cooperar en una interacción o que se requieren los primeros datos. Será evidente que cuando los segundos datos se cifran o se resumen, la memoria puede estar disponible públicamente, y los segundos datos pueden enviarse a través de una ruta alternativa que involucra transmitir datos a y desde nodos no confiables.

Los primeros datos pueden transferirse a la pluralidad de segundos nodos mediante uno o más nodos de red adicionales, cada uno de los cuales soporta el primer protocolo. Al menos uno del uno o más nodos de red adicionales puede no soportar un protocolo capaz de transferir datos del segundo tipo.

Como se describió anteriormente, la red, y en particular los nodos entre el primer y el segundo nodo, no necesitan ser capaces de soportar el segundo tipo de datos, y de hecho pueden no hacerlo. Esto significa que con cambios solamente al primer nodo, y cualquier segundo nodo relevante, tanto los primeros como los segundos tipos de datos pueden transferirse al segundo nodo. Esto facilita la transferencia de los segundos datos, ya que las modificaciones al sistema existente son pequeñas y, en algunos casos, pueden no requerirse en absoluto.

El primer protocolo puede definir una pluralidad de campos, y los primeros datos pueden comprender datos correspondientes a al menos uno de los campos.

En modalidades, la red puede comprender una red de procesamiento de pagos, y los primeros datos pueden comprender datos de transacción. Además, la red puede comprender uno o más terceros nodos entre el primer y el segundo nodo, el uno o más nodos pueden comprender al menos uno de: un sistema de procesamiento de datos de comerciante; un proveedor de servicios de pago (PSP); un sistema de procesamiento de datos bancarios de adquisición; y un sistema de procesamiento de datos del sistema de tarjetas. Adicionalmente, el al menos un segundo nodo comprende un sistema informático del banco emisor.

Las características y ventajas adicionales resultarán evidentes a partir de la siguiente descripción de las modalidades preferidas, dadas a manera de ejemplo solamente, que se hacen con referencia a los dibujos acompañantes.

Breve descripción de los dibujos

Los sistemas, aparatos y métodos se describirán ahora como modalidades, a manera de ejemplo solamente, con referencia a las figuras acompañantes en las cuales:
la Figura 1 muestra un diagrama esquemático de un sistema de comunicaciones a manera de ejemplo que no es parte de la presente invención;
la Figura 2 ilustra un método a manera de ejemplo que no es parte de la presente invención;
la Figura 3 muestra un diagrama esquemático adicional de un sistema de comunicaciones a manera de ejemplo que no es parte de la presente invención;
la Figura 4 muestra un sistema en el que pueden transferirse los datos de pago y en el que pueden practicarse las modalidades de la invención; y la Figura 5 muestra un diagrama esquemático de un nodo de red que puede usarse en modalidades de la invención.

Algunas partes, componentes y/o etapas aparecen en más de una Figura; en aras de claridad el mismo número de referencia se usará para referirse a la misma parte, componente o etapa en todas las Figuras.

Descripción detallada de modalidades ilustrativas

La Figura 1 muestra, a manera de ejemplo que no es parte solamente de la presente invención, un sistema de comunicaciones 10 en el que los datos de un primer tipo pueden enviarse desde un primer nodo 11 a una pluralidad de segundos nodos 12A y 12B mediante el uso de un primer protocolo, y en el que los datos de un segundo tipo, no incluido en el primer protocolo, pueden transferirse a uno de los segundos nodos 12A.

El primer nodo 11 se conecta a los segundos nodos 12A y 12B a través de una red 13. La red 13 puede comprender cualquier número de terceros nodos, con uno, el nodo 14 que se muestra. El primer nodo 11 se conecta al tercer nodo 14, que a su vez se conecta a los segundos nodos 12A y 12B. Todos los primer, segundo y tercer nodos 11, 12A/12B y 14 son capaces de transferir datos de conformidad con un primer protocolo. Además, el primer nodo 11 y el segundo nodo 12A tienen conexiones con una memoria 16.

Un método para transferir datos en el sistema de comunicaciones 10 se describirá ahora con referencia a la Figura 2. Como se indicó anteriormente, el sistema de comunicaciones comprende un primer nodo 11 el cual se dispone para enviar datos a los segundos nodos 12A y 12B.

En una primera etapa 21, el primer nodo 11 puede generar, identificar o de otra manera determinar los datos que se envían al segundo nodo 12A. Si bien algunos de los datos se enviarán mediante el uso de un primer protocolo, el segundo nodo 12A requiere datos que no se incluyen en este primer protocolo. Como tal, los datos pueden separarse en dos tipos, un primer tipo de datos que pueden enviarse usando el primer protocolo, y un segundo tipo, al menos una parte de los cuales no se incluye en el primer protocolo y por lo tanto no puede enviarse mediante el uso del primer protocolo. La etapa 21 puede incluir las etapas de identificar que los datos se envían a un segundo nodo 12A que requiere los segundos datos, y que separa los datos en consecuencia.

Posteriormente, en las etapas 22 y 23, los primeros datos, que son del primer tipo incluido en el protocolo, se transfieren del primer nodo 11 al segundo nodo 12A a través del tercer nodo 14. Además, como se muestra en la etapa 24, los segundos datos, que son del segundo tipo y no se incluyen en el protocolo, se almacenan en la memoria 16. Después de estas etapas, en las etapas 25 y 26, el segundo nodo 12A puede acceder a los segundos datos almacenados en la memoria 16. Para permitir este acceso, el segundo nodo 12A puede, en la etapa 25, determinar que se han recibido los primeros datos, y en consecuencia, en la etapa 26, solicitar acceso a los segundos datos en la memoria 16.

Además, el primer nodo 11 puede transferir datos a un segundo nodo 12B adicional. Este segundo nodo 12B adicional no requiere datos del segundo tipo. Como tal, en la etapa 27, análoga a la etapa 21, el primer nodo 11 genera los datos que se envían al segundo nodo 12B. Esta etapa puede incluir el primer nodo 11 que identifica el segundo nodo 12B, y determinar que el segundo nodo 12B adicional no requiere datos del segundo tipo, es decir datos no incluidos en el protocolo. Después de la etapa 27, en la etapa 28, el primer nodo 11 puede transferir los primeros datos (del primer tipo) al tercer nodo 14, desde donde, en la etapa 29, se transfieren al segundo nodo 12B.

Como tal, es posible transferir los datos del segundo tipo al segundo nodo 12A el cual lo requiere, sin ningún otro cambio en el protocolo. En particular, ni el segundo nodo 12B, ni el tercer nodo o nodos 14 en la red 13 necesitaban modificación para que funcionen los anteriores.

Para permitir la transferencia efectiva de los datos, los primeros y segundos datos pueden comprender una pluralidad de elementos de los primeros y segundos datos respectivamente. Los elementos de los segundos datos pueden asociarse con los elementos de los primeros datos correspondientes. Como tal, en la etapa 26, el segundo nodo 12A puede hacer que una solicitud comprenda datos que identifican uno o más de los elementos de los segundos datos que se desean por el segundo nodo 12A.

Estos datos de identificación pueden ser la identidad del segundo nodo 12A. En respuesta, la memoria 16 puede proporcionar todos los elementos de los segundos datos que se asocian con los elementos de los primeros datos enviados a ese segundo nodo 12A particular. Alternativamente, los datos de identificación pueden corresponder a los datos incluidos en un elemento de los primeros datos correspondiente. Como tal, el segundo nodo 12A, en la etapa 25, puede usar un elemento de los primeros datos recibido para determinar los datos de identificación que se proporcionan en la solicitud en la etapa 26. Un método mediante el cual esto puede hacerse es incluir un identificador en el elemento de los primeros datos, y almacenar el elemento de los segundos datos en conjunto con el identificador proporcionado.

El primer protocolo puede definir una pluralidad de campos, y los primeros datos en consecuencia pueden comprender datos correspondientes a al menos uno de los campos. Como tal, los segundos datos pueden comprender al menos algunos datos que no corresponden a los campos del primer protocolo. Estos datos fuera del protocolo pueden incluir información que es solamente relevante para el segundo nodo 12A.

Sin embargo, los elementos de los segundos datos pueden generarse a partir de los elementos de los primeros datos. Por ejemplo, al menos una parte de un elemento de los segundos datos puede generarse usando al menos una parte de un elemento de los primeros datos correspondiente como una entrada a un algoritmo de procesamiento de datos. Este algoritmo de procesamiento de datos puede calcular una función resumen de los primeros datos. Alternativa o adicionalmente, el algoritmo de procesamiento de datos puede calcular una firma digital. Para generar la firma, el primer nodo puede usar una clave privada. Alternativamente, el primer y el segundo nodo pueden compartir un secreto y la firma digital puede calcularse mediante el uso del secreto compartido.

Al almacenar estos datos resumidos y/o firmados en la memoria 16, el segundo nodo 12A es capaz de determinar si los primeros datos se han modificado en tránsito entre el primer y el segundo nodo, es decir por el tercer nodo 14. Los datos resumidos/firmados pueden almacenarse en conjunto con un identificador que se proporciona en el elemento de los primeros datos correspondiente. Por ejemplo, el elemento de los primeros datos (D_1) puede tener el siguiente formato:

$$D_1 = \{ID, F_1, F_2, F_3, \ldots, F_N\}$$

donde ID es un identificador y F_1 etc. representan los campos dentro de los primeros datos. Como será evidente, estos campos se incluyen en el primer protocolo.

El elemento de los segundos datos correspondiente (D_2) puede tener el siguiente formato:

$$D_2 = \{ID, S(H(D_1))\}$$

donde las funciones S() y H() representan funciones para generar una firma digital y resumen respectivamente.

Al firmar los primeros datos, o un resumen de los primeros datos, el segundo nodo 12A puede ser capaz posteriormente de confirmar que los primeros datos recibidos mediante el uso del protocolo a través de la red 13 fueron los mismos que los enviados originalmente por el primer nodo 11. Esto se debe a que la firma digital se llevará a cabo mediante el uso de la clave privada del primer nodo y, por lo tanto, solamente la clave pública del primer nodo devolverá los primeros datos (o resumen de los primeros datos, que puede compararse contra un resumen de los primeros datos generados de manera similar).

El primer nodo puede cifrar además los segundos datos, usando la clave pública del segundo nodo 12A. Además, si la integridad y el no repudio de los datos son importantes, el primer nodo puede firmar además los segundos datos mediante el uso de la clave privada del primer nodo 11), esto puede hacerse para garantizar que solamente el segundo nodo 12A pueda interpretar los segundos datos. El cifrado puede no ser necesario cuando el único objetivo es que el segundo nodo 12A sea capaz de confirmar que los primeros datos no se han modificado, ya que un resumen de los primeros datos, a partir del cual no se pueden derivar los primeros datos, puede ser suficiente. Sin embargo, cuando los segundos datos contienen datos que no están soportados por el primer protocolo (es decir datos adicionales), entonces los segundos datos pueden cifrarse para asegurar que estos datos no puedan leerse por ningún nodo diferente del segundo nodo 12A.

El primer nodo y el segundo nodo tienen una relación de confianza. Además, el tercer nodo o nodos 14, a través de los cuales se envían los primeros datos, puede no tener una relación de confianza con el primer y el segundo nodo. Como tal, mientras el segundo nodo 12A puede confiar en los segundos datos en la memoria 16, el segundo nodo no puede confiar en los primeros datos enviados a través de los terceros nodos no confiables 14. Esto puede ser particularmente relevante cuando los primeros datos, enviados usando el primer protocolo, se envían de acuerdo con un formato que puede interpretarse por el tercer nodo 14. Este requisito puede especificarse por el primer protocolo. Será evidente que, al ser capaz de interpretar los primeros datos, el tercer nodo 14 puede modificar adicionalmente los datos. Una razón para que el tercer nodo 14 pueda interpretar los datos es porque el primer, el segundo y el tercer nodo se disponen para cooperar en una interacción para la cual tanto el segundo nodo como el tercer nodo requieren

los primeros datos.

Será evidente que si se usan cifrado y/o firma, entonces la memoria 16 en sí puede estar disponible públicamente, ya que solo el primer nodo puede crear los datos debidamente firmados o cifrados. Se apreciará que si no hay repudio, es decir la capacidad de confirmar la fuente de los datos, es posible que se firmen los segundos datos. De igual manera, si se requiere confidencialidad, los datos pueden cifrarse. Será evidente que uno o ambos pueden usarse juntos.

Como se mencionó anteriormente, los primeros datos se transfieren a los segundos nodos 12A y 12B mediante uno o más terceros nodos de red 14. Será evidente que cada tercer nodo 14 respaldará el primer protocolo. Como tal, puede ser el caso que el uno o más terceros nodos 14 no soporten un protocolo capaz de transferir datos del segundo tipo. Sin embargo, cualquier tercer nodo 14 no requiere modificación para que los segundos datos se transfieran al segundo nodo 12A. Esto facilita la transferencia de los segundos datos, ya que las modificaciones al sistema existente son pequeñas.

Se describirá una alternativa al sistema 10 a manera de ejemplo que no es parte de la presente invención, con referencia a la Figura 3. Muchos componentes del sistema 10 son los mismos, y por lo tanto tienen los mismos números de referencia. En este sistema alternativo 10', el primer nodo 11 transfiere datos a los segundos nodos 12A y 12B a través de una red 13. A su vez, la red comprende el tercer nodo 14 y un cuarto nodo 15. El cuarto nodo 15 difiere del tercer nodo 14 en que el cuarto nodo 15 comprende la memoria 16'.

Durante el uso, el primer nodo 11 transmite los primeros datos al tercer nodo 14, y los segundos datos al cuarto nodo 15. El cuarto nodo 15 puede mantener los segundos datos en la memoria 16' hasta que se soliciten por el segundo nodo 12A. Sin embargo, el cuarto nodo 15 puede combinar los primeros y segundos datos y proporcionar la combinación al segundo nodo 12A, es decir, el cuarto nodo permite el acceso a los segundos datos al enviar los mismos al segundo nodo 12A con los primeros datos correspondientes. Esta disposición permite que el tercer nodo 14 sea saltado por los segundos datos, lo que puede requerirse si el tercer nodo 14 no es confiable, o no es capaz de manejar los segundos datos, es decir si el tercer nodo 14 solo soporta protocolos que no son capaces de transferir los segundos datos.

En algunas modalidades, el sistema de comunicaciones comprende una red de procesamiento de pagos. Como tal, los primeros datos pueden comprender datos de transacción. Un ejemplo de un sistema de procesamiento de pagos 40 en el que pueden practicarse las modalidades se describirá con referencia a la Figura 4.

Como con la descripción anterior, los datos, en este caso los datos de transacción, se envían desde un primer nodo 11 a los segundos nodos 12A y 12B a través de una red 13. Los datos comprenden los primeros datos, enviados mediante el uso de un primer protocolo y los segundos datos que se almacenan en una memoria 16.

El primer nodo 11 puede ser una fuente de datos de transacción o datos de pago. Por ejemplo, el primer nodo puede ser un intermediario confiable dispuesto para proporcionar datos de transacción a nombre de un cliente. El intermediario confiable puede almacenar detalles de los métodos de pago, tales como un número de cuenta principal o PAN de una tarjeta de crédito, y puede acceder a un cliente como parte de una transacción en línea. De conformidad con la invención, en una modalidad el primer nodo 11 es un teléfono móvil, capaz de comunicar tanto los primeros como los segundos datos. En particular, el teléfono móvil se dispone para proporcionar los primeros datos a un comerciante para efectuar una transacción. Estos primeros datos se transfieren mediante el uso de comunicaciones de campo cercano. Adicionalmente, el primer nodo 11 proporciona segundos datos a través de una red de comunicaciones móviles.

Los segundos nodos 12A y 12B pueden ser sistemas de procesamiento de pagos de bancos emisores (en lo adelante, bancos emisores).

En esta modalidad, la red 13 comprende una pluralidad de proveedores de servicios de pago, o PSP, 41A y 41B; una pluralidad de sistemas de procesamiento de pagos del banco adquirente 42A y 42B captados (en lo adelante, banco adquirente); y un sistema de procesamiento de datos del sistema de tarjetas 43. Se entenderá que esta lista de posibles entidades que componen los nodos no es limitante, y los nodos dentro de la red pueden incluir, por ejemplo, un sistema de procesamiento de comerciante.

En este ejemplo, el primer nodo 11 se conecta a la pluralidad de PSP 41A y 41B. Los PSP 41A y 41B se conectan cada uno a su vez a los bancos adquirentes 42A y 42B. Típicamente un PSP dado se conecta a múltiples bancos adquirentes, y un banco adquirente dado se conectará a múltiples PSP. Esto conduce a la superposición en las conexiones mostradas. Los bancos adquirentes 42A y 42B se conectan al sistema de procesamiento de datos del sistema de tarjetas 43, que se conecta a los bancos emisores 12A y 12B.

Durante el uso, los datos de pago, es decir los primeros datos descritos anteriormente, pueden transmitirse desde el primer nodo 11 a través de la red 13 a los bancos emisores 12A y 12B mediante el uso de protocolos conocidos para transmitir los datos de pago. Los datos de pago se transmiten típicamente a través de un PSP y un banco adquirente

al sistema de tarjetas, y desde allí hacia los bancos emisores 12A y 12B. Este proceso se conoce en la técnica y no necesita describirse en detalle. No obstante, dado que la elección del PSP y del banco adquirente se realiza típicamente por un comerciante, para cualquier transacción dada, cualquier combinación de PSP y banco adquirente puede transferir los primeros datos.

Esto ilustra un problema con un sistema de procesamiento de pagos típico. Una extensión de los protocolos existentes para transmitir datos adicionales necesitaría ser implementada por todos, o al menos la mayoría, de los PSP, los bancos adquirentes y el sistema de tarjetas 43. Dado que los PSP, los bancos adquirentes y el sistema de tarjetas 43 pueden ser operados por una empresa diferente, la puesta en práctica de esta implementación de un cambio en el protocolo sería difícil, y requerirá una coordinación sustancial entre las organizaciones.

Por el contrario, las modalidades proporcionan una alternativa más conveniente. Los primeros datos, los datos de pago, se envían a través de la red de pago convencional 13 y pueden procesarse por lo tanto de la manera convencional para efectuar una transacción. Además, los segundos datos pueden almacenarse en la memoria 16, y recuperarse posteriormente por un segundo nodo 12A (es decir, un banco emisor).

En modalidades de la invención, los segundos datos pueden usarse para verificar los primeros datos. Como tal, los segundos datos son un resumen firmado de los primeros datos. En consecuencia, un banco emisor, que recibe los datos de pago, será capaz de verificar que los primeros datos se generaron por el primer nodo 11, y que los primeros datos no se hayan alterado en tránsito. La relación de confianza entre el primer y el segundo nodo descrita anteriormente puede usarse para permitir que el segundo nodo confíe en el primer nodo.
Será evidente que cualquier dato, relacionado con una transacción, pero que no se procese convencionalmente por los sistemas de procesamiento de pagos existentes dentro de la red 13, puede almacenarse en la memoria 16. Por ejemplo, puede proporcionarse una copia del recibo, o de la información contenida en un recibo. Esta información puede incluir una descripción detallada de los bienes o servicios comprados, una ubicación del punto de venta, una dirección para la entrega, si se aplican descuentos, una geolocalización del instrumento de pago en relación con cualquier dispositivo del punto de venta usado, un identificador del dispositivo del punto de venta, una dirección IP de un dispositivo del punto de venta o de un ordenador usado para realizar una compra en línea, movimientos espaciales, información biométrica, etc.

Posteriormente, estos datos pueden combinarse con los datos de pago reales transmitidos a través de la red de pago 13. Cuando el segundo nodo es un sistema contable, o un programa contable proporcionado por un banco emisor, los datos pueden ser aportados en un programa contable, lo que permite a los clientes revisar el gasto en detalle.

Aunque la memoria 16 se ha mostrado por separado, se apreciará que la memoria puede combinarse con cualquiera de los nodos de la red.

Como tal, en resumen, las modalidades pueden proporcionar un método para procesar los datos de pago asociados con transacciones de pago realizadas a través de una red, donde la red comprende,
- al menos un sistema de procesamiento de datos del banco adquirente,
- al menos un primer nodo de red, que es un teléfono móvil, dispuesto para proporcionar datos de pago a al menos uno de los sistemas de procesamiento de datos del banco adquirente, y
- al menos un segundo nodo de red, que es un sistema de procesamiento de datos del banco emisor como se describió anteriormente, dispuesto para recibir datos de pago de al menos uno del sistema de procesamiento de datos del banco adquirente.

Durante una transacción de pago dada, los datos de pago asociados con la transacción de pago pueden enviarse desde el primer nodo de la red al segundo nodo de la red mediante el sistema de procesamiento de datos del banco adquirente. Además, otros datos asociados con la transacción, al menos algunos de los datos adicionales que no sean los datos de pago, pueden almacenarse en un nodo de la red diferente del al menos un sistema de procesamiento de datos del banco adquirente. Posteriormente, puede permitirse acceso a los datos adicionales, por el segundo nodo de la red.

Los datos de pago asociados con la transacción de pago pueden enviarse desde el primer nodo de la red al segundo nodo de la red mediante al menos un sistema de procesamiento de datos del banco adquirente usando al menos un primer protocolo, y los datos adicionales pueden comprender datos no incluidos en el primer protocolo.

Se entenderá que los datos almacenados en la memoria 16 pueden, en algunos casos, no recuperarse. Como tal, el segundo nodo 12A puede ser selectivo sobre qué datos se recuperan. Alternativamente, el primer nodo 11 puede almacenar los segundos datos independientemente del segundo nodo al cual se envían los primeros datos correspondientes, en otras palabras, la etapa de identificación 21 y 27 puede simplificarse u omitirse. Solo los segundos nodos que requieren los segundos datos, o que desean segundos datos para un caso particular, pueden recuperar los segundos datos. Sin embargo, en tales circunstancias, el primer nodo no requiere información sobre qué nodos requieren datos y cuáles no. La memoria puede almacenar datos con una vida limitada. Es decir, que los datos pueden ser eliminados para determinar si se ha recuperado después de un periodo de tiempo predeterminado.

Los nodos de la red, incluyendo los descritos en relación con el sistema de pago y la memoria 16, pueden comprender soporte físico informatizado como se conoce en la técnica.

Sin embargo, para la completitud, un sistema informatizado ilustrativo 50, capaz de realizar las etapas del método descrito anteriormente, se describirá ahora con referencia a la Figura 5.

El sistema informatizado 50 comprende un sistema de procesamiento 51, tal como un CPU, o un conjunto de CPU. El sistema de procesamiento 51 se conecta a una memoria 52, tal como una memoria volátil (por ejemplo RAM) o una memoria no volátil, por ejemplo una memoria de estado sólido (SSD) o memoria de disco duro. La memoria 52 almacena instrucciones legibles por ordenador 53. El sistema 50 puede comprender además una interfaz 54, capaz de transmitir y/o recibir datos de otros nodos de red.

Durante el uso, el sistema de procesamiento 51 puede recuperar las instrucciones informáticas 53 de la memoria 52 y ejecutar estas instrucciones para realizar las etapas descritas anteriormente. Al hacerlo, el sistema de procesamiento 51 puede provocar que la interfaz transmita o reciba datos según sea necesario. Estos datos pueden almacenarse por sí mismos en la memoria 52, y recuperarse según sea necesario, por ejemplo, para transmitirse a través de la interfaz.

REIVINDICACIONES

1. Un método para transferir datos de transacciones en un sistema de procesamiento de pagos, el sistema de procesamiento de pagos comprende un teléfono móvil dispuesto para enviar datos de transacciones a una pluralidad de sistemas informáticos del banco emisor (12A, 12B) a través de una red de pagos (13) usando un primer protocolo, en donde la red de pago (13) comprende i) una pluralidad de proveedores de servicios de pago (41A, 41B), ii) una pluralidad de sistemas informáticos de datos del banco adquirente (42A, 42B) y un sistema de procesamiento de datos del sistema de tarjetas (43), y en donde el primer protocolo define una pluralidad de campos y permite la transferencia de datos de un primer tipo, y en donde al menos uno de los sistemas informáticos del banco emisor (12A, 12B) requiere además datos de un segundo tipo, no incluidos en los datos enviados de acuerdo con el primer protocolo, el método comprende:
transferir los primeros datos a una pluralidad de sistemas informáticos del banco emisor (12A, 12B) usando el primer protocolo, los primeros datos son del primer tipo y comprenden datos correspondientes a al menos uno de los campos definidos por el primer protocolo, en donde los primeros datos se transfieren a la pluralidad de sistemas informáticos del banco emisor (12A, 12B) a través de uno de la pluralidad de proveedores de servicios de pago (41A, 41B) y uno de la pluralidad de sistemas de procesamiento de datos del banco adquirente (42A, 42B) que soportan el primer protocolo al sistema de procesamiento de datos del sistema de tarjetas (43) y del sistema de procesamiento de datos del sistema de tarjetas (43) a la pluralidad de bancos emisores (12A, 12B), en donde la transferencia comprende proporcionar los primeros datos a un comerciante usando comunicaciones de campo cercano; almacenar, por el teléfono móvil, los segundos datos en una memoria (16), los segundos datos son del segundo tipo y comprenden al menos algunos datos que no corresponden a los campos definidos por el primer protocolo; y
en respuesta a una solicitud de un sistema informático del banco emisor (12A, 12B), proporcionar, por el teléfono móvil, los segundos datos al sistema informático del banco emisor (12A, 12B) que requiere datos del segundo tipo a través de una red de comunicaciones móviles,
en donde al menos uno de los sistemas informáticos de datos bancarios de adquisición (42A, 42B) no soporta un protocolo capaz de transferir datos del segundo tipo,
en donde los primeros datos comprenden una pluralidad de elementos de los primeros datos, y los segundos datos comprenden una pluralidad de elementos de los segundos datos asociados con los elementos de los primeros datos correspondientes,
el método comprende generar al menos una parte de un elemento de los segundos datos usando al menos una parte de un elemento de los primeros datos correspondiente como una entrada a un algoritmo de procesamiento de datos el cual calcula una función resumen del elemento de datos correspondiente y firma digitalmente la salida de la función resumen.

2. El método de conformidad con la reivindicación 1, en donde la solicitud comprende datos que identifican el sistema informático del banco emisor (12A, 12B).

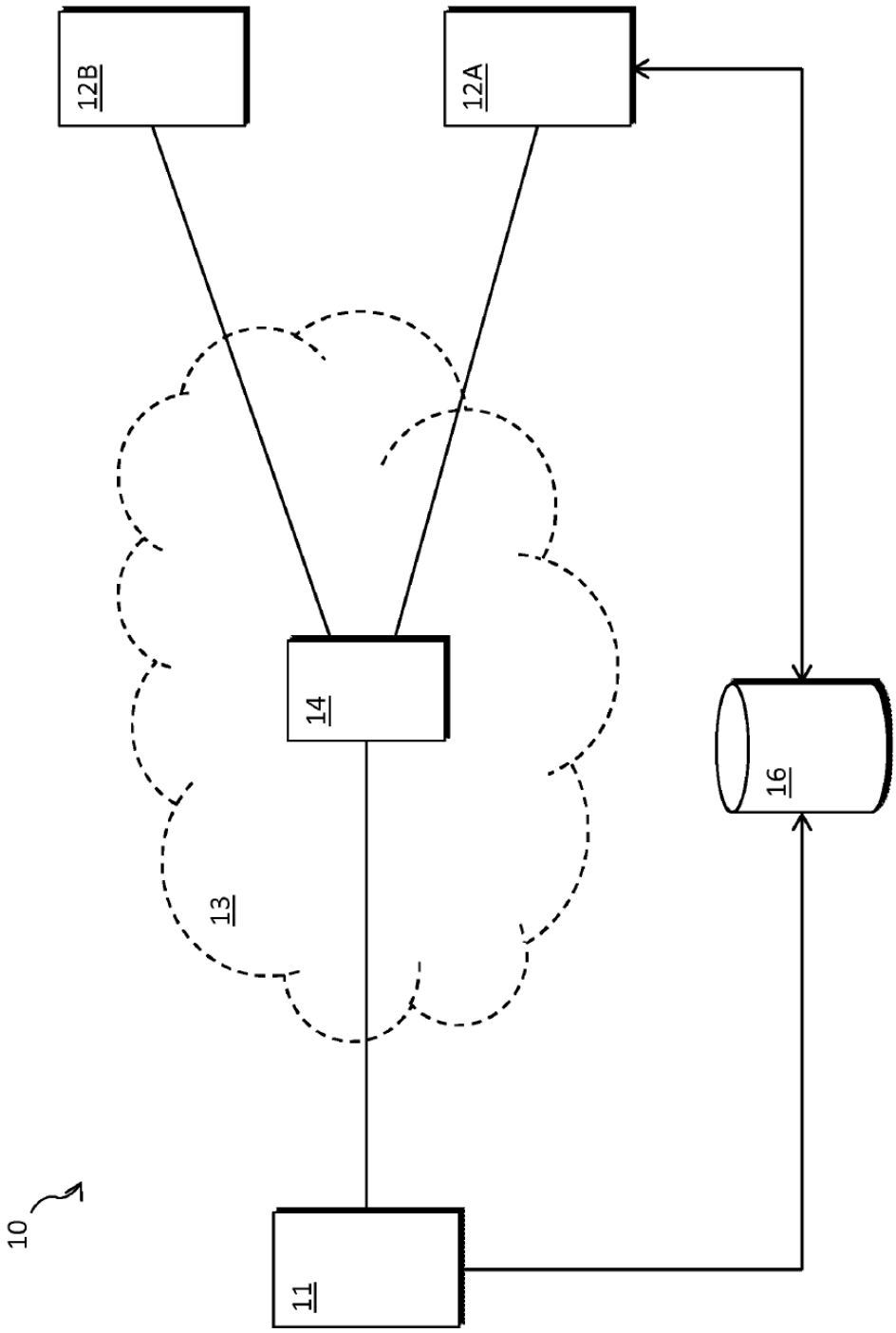

Figura 1

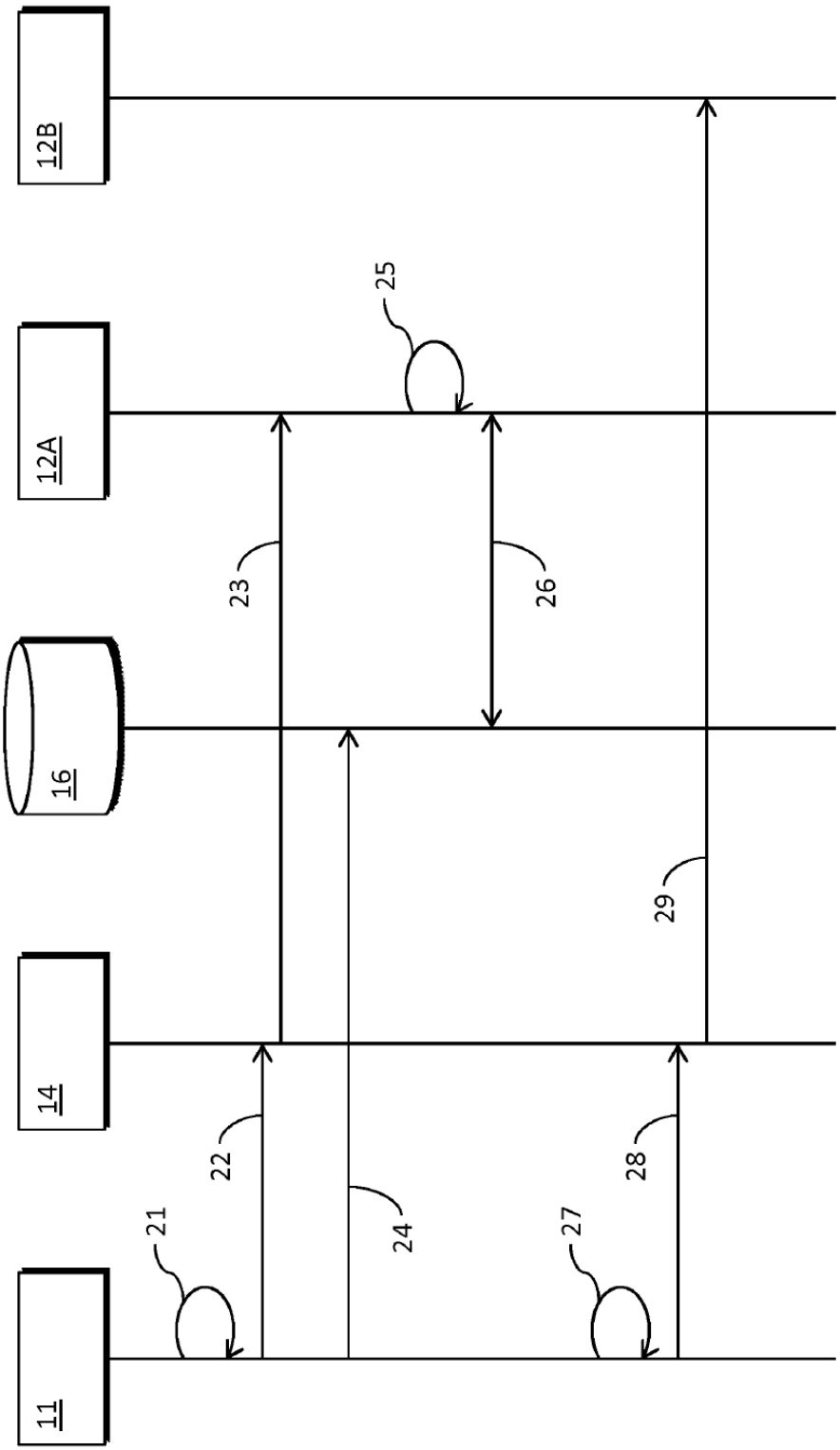

Figura 2

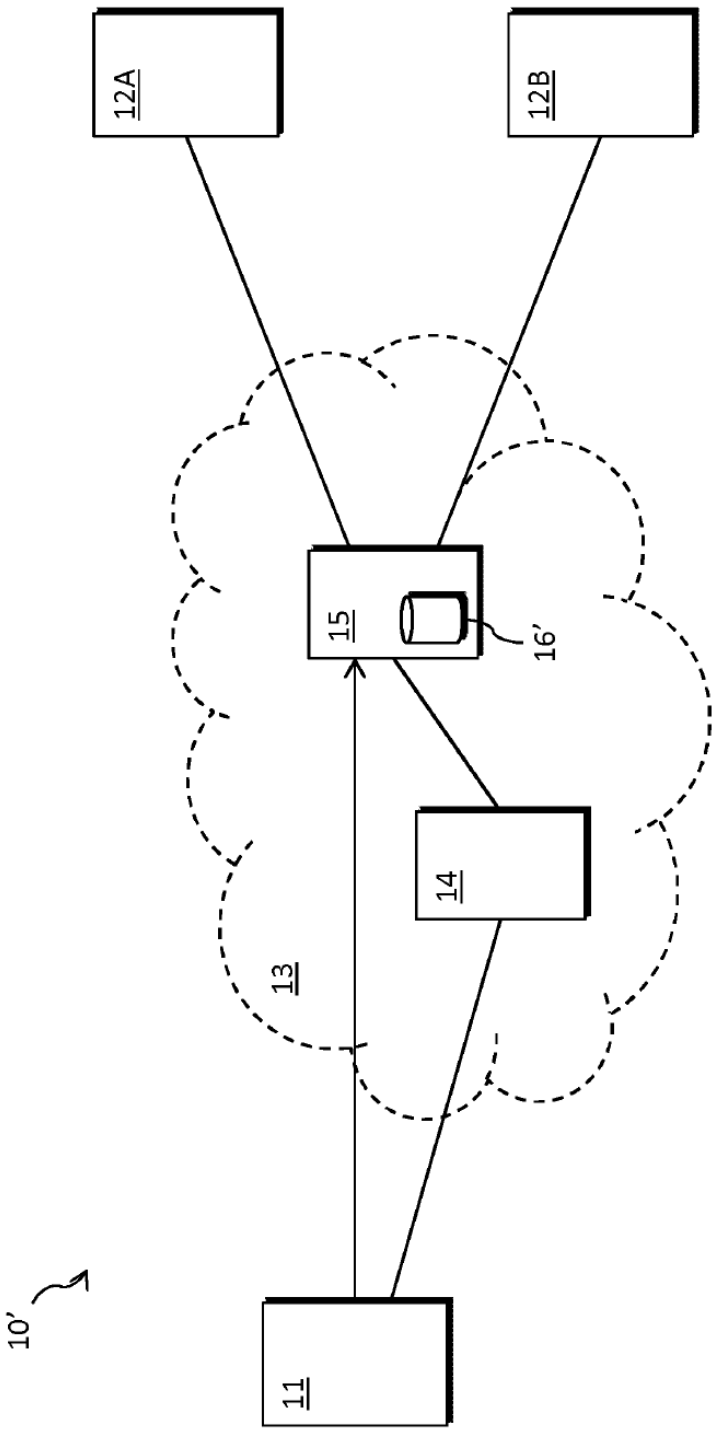

Figura 3

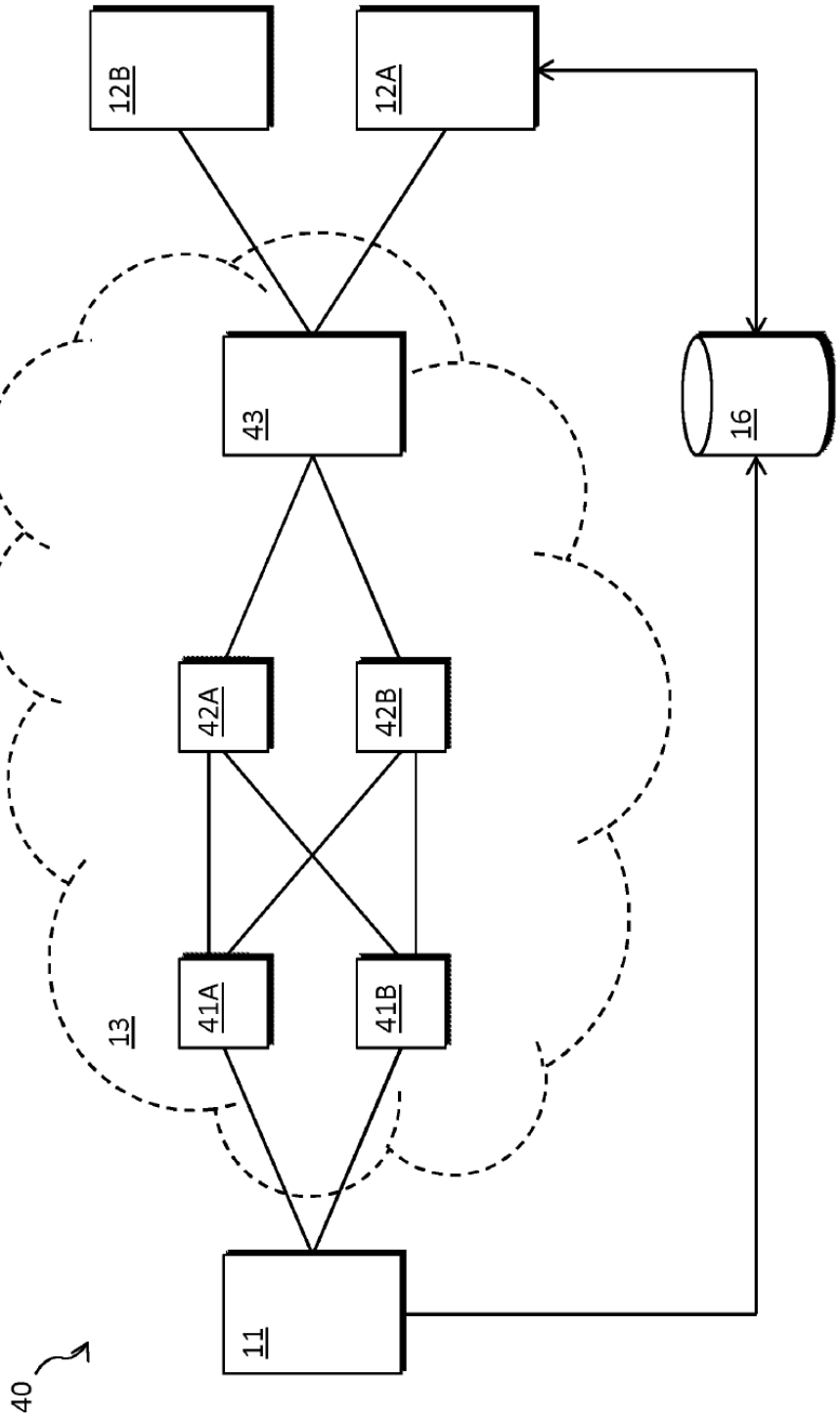

Figura 4

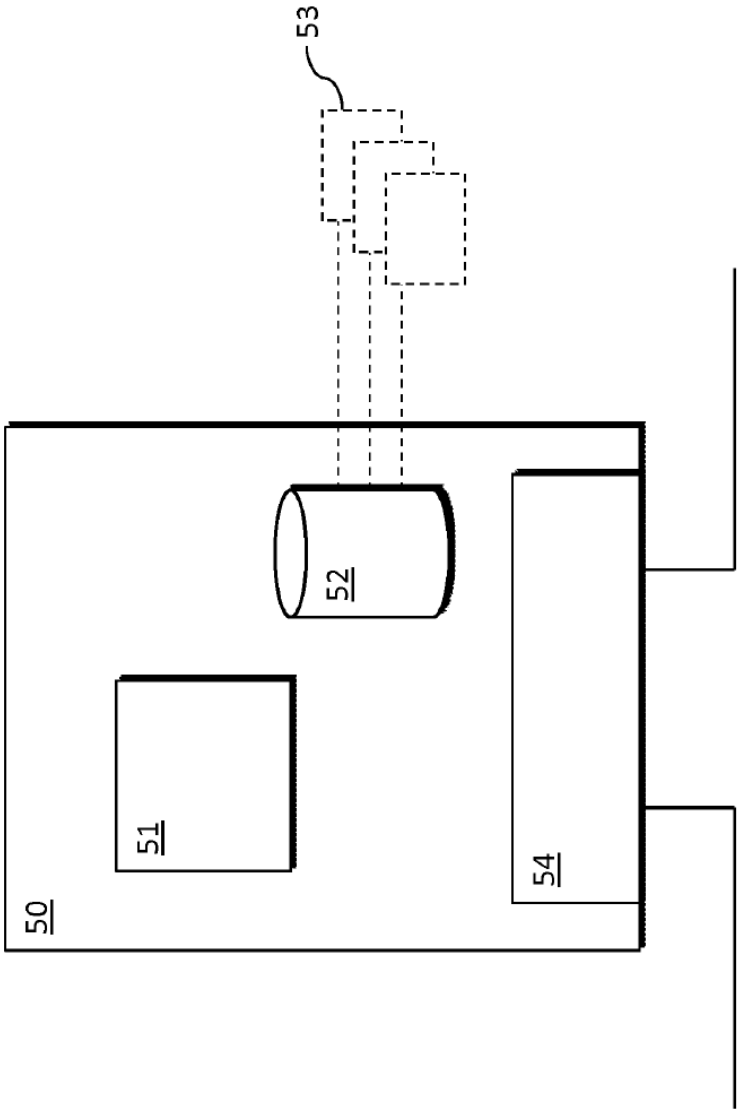

Figura 5