(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 817 433**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.12.2017 PCT/EP2017/082625**

(87) Fecha y número de publicación internacional: **21.06.2018 WO18109010**

(96) Fecha de presentación y número de la solicitud europea: **13.12.2017 E 17821863 (2)**

(97) Fecha y número de publicación de la concesión europea: **17.06.2020 EP 3556045**

(54) Título: **Distribución y recuperación de datos de una red P2P usando un registro de cadena de bloques**

(30) Prioridad:

15.12.2016 LU 93377

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.04.2021

(73) Titular/es:

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY (LIST) (100.0%)
5, avenue des Hauts-Fourneaux
4362 Esch-sur-Alzette, LU

(72) Inventor/es:

ROTH, UWE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Distribución y recuperación de datos de una red P2P usando un registro de cadena de bloques

Campo técnico

[0001] La invención se refiere al campo de redes informáticas entre pares y más particularmente al campo del intercambio de datos entre diferentes socios o nodos pares a través de una red informática.

Estado de la técnica

[0002] Las tecnologías entre pares (P2P) constituyen una alternativa a los sistemas de información centralizados tradicionales debido a su potencial para escalar a tamaños realistas y a su tolerancia inherente a los fallos. En los sistemas P2P, los ordenadores se comunican directamente entre sí, en lugar de a través de servidores que pueden convertirse en cuellos de botella de rendimiento y puntos únicos de fallo. Las redes P2P autoorganizadas han demostrado ser altamente adaptables a los cambios en la conectividad de la red y resistentes a los fallos de los nodos o las redes. Mientras que la tecnología P2P actual puede proporcionar un almacenamiento de objetos de datos distribuidos escalable y robusto, las soluciones P2P actuales no se usan ampliamente debido, al menos en parte, a cuestiones de seguridad. Por ejemplo, las redes P2P se usan generalmente para compartir datos libremente, tal como información o música. Sin embargo, las redes P2P generalmente no proporcionan la seguridad y el control de acceso necesarios con la funcionalidad de consulta requerida para sistemas de información más sofisticados.

[0003] El documento de patente de la técnica anterior publicado US 2005/0240591 A1 divulga un sistema de redes entre pares que forma un gran repositorio con un mecanismo de acceso a datos de objetos distribuidos que concede acceso a objetos de datos a usuarios autorizados. Los datos pueden dividirse y distribuirse según una tabla *hash* a diferentes nodos pares. Los datos también se pueden encriptar utilizando una clave de encriptación secreta que se divide en una serie de partes secretas distribuidas entre los nodos pares. Mediante la recuperación de estas partes secretas, la clave secreta correspondiente se puede reconstruir y los datos encriptados se pueden descifrar y acceder a ellos. Esto proporciona la ventaja de que una versión completa de la clave de encriptación secreta no se transmite nunca a través de la red. Sin embargo, la seguridad de una red de ese tipo permanece limitada en cuanto a que un nodo malicioso podría solicitar copias de cada una de las partes secretas para reconstruir la clave de encriptación.

[0004] El documento de patente de la técnica anterior US 2016/162897 A1 divulga la división de un secreto en partes usando una red de cadena de bloques.

[0005] El documento de patente de la técnica anterior US 2015/261973 A1 divulga la división de datos encriptados y la clave usada para su encriptación.

Resumen de la invención

Problema técnico

[0006] La invención tiene como problema técnico proporcionar una solución a al menos un defecto de la técnica anterior citada anteriormente. Más específicamente, la invención tiene como problema técnico proporcionar una red P2P con una mayor seguridad y transparencia con respecto al acceso por un nodo par a datos encriptados.

Solución técnica

[0007] La invención se refiere a un método de distribución y recuperación de datos en una red informática con nodos pares, que comprende: (a) encriptar, con una clave secreta, un fichero que contiene dichos datos; (b) dividir el fichero encriptado en bloques y dividir la clave secreta en partes secretas; (c) distribuir los bloques y las partes secretas a los nodos pares; (d) tras la solicitud de un cliente de acceder al fichero, recuperar a través de uno de los nodos pares los bloques encriptados para reconstruir el fichero encriptado, recuperar al menos algunas de las partes secretas para reconstruir la clave secreta y desencriptar el fichero encriptado con la clave secreta reconstruida; donde los nodos pares comparten una cadena de bloques para formar una red de cadena de bloques; en el paso (a), las partes secretas se transmiten a los nodos pares a través de mensajes enviados sobre la red de cadena de bloques; y en el paso (d), la solicitud y la recuperación de las partes secretas se hace a través de mensajes enviados sobre la red de cadena de bloques.

[0008] La cadena de bloques forma un libro mayor descentralizado que almacena información para siempre sin ninguna posibilidad de adición, cambio o deleción fraudulentos u ocultos de contenido.

[0009] Una cadena de bloques debe entenderse como una base de datos o estructura de datos de los registros de datos con las propiedades siguientes: cada nodo de una red de cadena de bloques mantiene una copia de la base de datos o estructura de datos. Una mayoría de nodos iguales alcanza un consenso acerca del estado actual de la base de datos o estructura de datos. Para cada dos registros de datos en la base de datos o estructura de datos acordada, se conoce cuál de los dos registros de datos se añadió antes y cuál se añadió después a la base de datos o estructura de datos acordada. En consecuencia, un nuevo registro de datos que se añade a la base de datos o estructura de datos acordada es el último registro de datos en la base de datos o estructura de datos acordada y no es posible añadir un registro de datos a la base de datos o estructura de datos acordada de manera que cualquier otro registro de datos existente en la base de datos o estructura de datos acordada se vea como un registro de datos que se añadió después a la base de datos o estructura de datos acordada. No es posible modificar o alterar ningún registro de datos que ya se haya añadido a la base de datos o estructura de datos acordada. No es posible eliminar ningún registro de datos que ya se haya añadido a la base de datos o estructura de datos acordada.

[0010] Un registro de cadena de bloques es un registro de mensajes descentralizado almacenado dentro de una cadena de bloques. La invención está definida por las reivindicaciones anexas.

Ventajas de la invención

[0011] La invención es particularmente interesante por el hecho de que el proveedor de ficheros en la red no necesita ser accesible durante el acceso de los datos, mientras que es capaz de rastrear el acceso a sus ficheros por los socios de la red. Además, el acceso a los ficheros no está restringido a solo algunos nodos sino a todos los nodos. No se requiere ninguna autorización particular. Tampoco se requiere ninguna instancia de administración y control central.

[0012] El uso de una red de cadena de bloques que registra las acciones de transmisión, solicitud y recuperación de datos por los socios proporciona una solución útil e interesante al problema de mantener el control de la información y la transparencia de su acceso. La tecnología de cadena de bloques se usa normalmente para transferir activos (por ejemplo, bitcoines) entre socios. Aquí, esa tecnología se implementa de una manera particular para proporcionar un libro mayor o registrador completo de toda la información intercambiada en relación con las partes secretas para desencriptar los datos, sin necesidad de una instancia de registro central. La solicitud y el acceso a partes secretas por un nodo se ponen al mismo nivel que tener un acceso innegable al fichero no encriptado por ese nodo.

Breve descripción de los dibujos

[0013]

La figura 1 ilustra la arquitectura de una red P2P que opera un método para distribuir y recuperar datos según la invención.
La figura 2 es un diagrama de flujo que ilustra la encriptación de un fichero, según la invención.
La figura 3 ilustra la estructura de las tablas de almacenamiento de ficheros en cada nodo par de la red, según la invención.
La figura 4 ilustra la estructura de las tablas de almacenamiento de secretos en cada nodo par de la red, según la invención.
La figura 5 ilustra una estructura ejemplar de un registro de cadena de bloques en la red de la figura 1, conforme a la invención.
La figura 6 es un diagrama de flujo que ilustra la recuperación y la desencriptación de un fichero según la invención.
La figura 7 ilustra diferentes mensajes enviados en la red de cadena de bloques de la figura 1, conforme a la invención.

Descripción de una forma de realización

[0014] Una forma de realización de la invención se describirá en relación con las figuras 1 a 7. En estas figuras, los números de referencia se usan para designar elementos físicos y también elementos de información como la ID de fichero, la parte secreta, etc. Para estos elementos de información, se utilizan diferentes números de referencia que designan la misma información en diferentes puntos de tiempo y/o en diferentes ubicaciones en el almacenamiento del ordenador y/o el tratamiento de la información. Esto es para una mayor claridad y no debe interpretarse como una falta de consistencia.

[0015] La figura 1 ilustra la arquitectura de una red P2P conforme a la invención. La red forma un de grupo de datos compartidos 1 que comprende una serie de sistemas de almacenamiento en red distribuido 5 y 15, que forman nodos pares. Cada nodo 5 y 15 posee un identificador o ID de nodo 12 único y un par de claves que consisten en una clave privada 14 y una clave pública 13. La clave privada y la pública forman un sistema criptográfico asimétrico que usa pares de claves: claves públicas que pueden difundirse ampliamente y claves privadas que son conocidas solo por el propietario. Tales sistemas son como tales bien conocidos por la persona experta. La ID de nodo 12 y la clave pública 13 son conocidas por los otros nodos, mientras que la clave privada 14 se mantiene secreta en el nodo. Cada nodo 5 y 15 comprende un gestor de redes 6 y un almacenamiento interno 7 de datos.

[0016] El gestor de redes 6 de un nodo administra dos redes: una red de cadena de bloques 4 que se utiliza para tener un registro de cadena de bloques 10 sincronizado y acordado a través de todos los nodos y una red de tabla *hash* distribuida 2 que se usa para distribuir ficheros entre nodos asociados. La tecnología de cadena de bloques es como tal conocida por la persona experta, en particular para transferir activos (por ejemplo, bitcoines) entre socios. Las redes de tablas *hash* distribuidas son como tales conocidas por la persona experta, en particular para el almacenamiento eficiente descentralizado y distribuido de pares (clave, valor).

[0017] El proceso de carga y acceso de ficheros dentro del grupo de datos compartidos se describirá en relación con las figuras 1-7.

[0018] Con referencia a la figura 1, un fichero que es añadido por un cliente de acceso 11 al grupo de datos compartidos 1 se carga a su nodo de almacenamiento en red distribuido 5 local a través de un protocolo de carga especial 16.

[0019] El fichero se añade a la tabla de ficheros 41 (figura 3) en el almacenamiento de ficheros 8/40 del almacenamiento interno 7.

[0020] Con referencia a la figura 3, la entrada en la tabla de ficheros 41 consiste en una única ID de fichero 42, el nombre de fichero del fichero 60 y el fichero mismo 43.

[0021] Basándose en el algoritmo de tabla *hash* distribuida, el nodo comparte el fichero con otros nodos en la red de tabla *hash* distribuida 2 (figura 1).

[0022] Con referencia a la figura 2, para asegurar la confidencialidad del fichero antes de compartirlo con otros nodos, el fichero 20 es primero encriptado 21 con el uso de una clave secreta 22 que es única por fichero. El fichero encriptado 23 se divide luego en bloques 24 con un tamaño fijo por bloque 25. El algoritmo de tabla *hash* distribuida prevé que, basándose en un algoritmo de *hash* 26 dado, se calcula el valor de *hash* 27 para cada bloque 25. El número de bloque 46 (figura 3) y su valor de *hash* 47 asociado (figura 3), junto con la ID de fichero 45, se comparten entre todos los nodos a través de la red de tabla *hash* distribuida 2 (figura 1) y se almacenan en la tabla de búsqueda de *hash*es local 44 de cada nodo (figura 3).

[0023] Los bloques del fichero encriptado se distribuyen a través del gestor de redes del nodo 6 (figura 1) entre los nodos asociados implicados basándose en la red de tabla *hash* distribuida 2. En dependencia de la estrategia de distribución de esa red de tabla *hash* distribuida, se decide si un nodo almacenará el bloque 50 (figura 3) y su valor de *hash* 49 en su tabla *hash* 48 local o no.

[0024] Todavía con referencia a la figura 2, para ser capaz de acceder a un fichero, no solo los bloques del fichero encriptado tienen que cargarse desde los varios nodos, sino también la clave secreta 22 usada. Esta clave secreta 22 se puede concatenar con una sal 28 aleatoria. Se transforma en un secreto de división 32 de *k* partes 33 según la técnica de compartición de secretos de Shamir 29. Requiere *n* (30) de *k* (31) partes para reconstruir la clave de encriptación original. El parámetro *n* se puede establecer para que sea el valor redondeado superior de (2/3*k*) y *k* equivale al número de nodos actuales en el grupo de datos compartidos.

[0025] Con referencia a la figura 4, la ID de fichero 62, los valores *n* (64) y *k* (65) más el número de versión de ese conjunto de parámetros 69 y la clave secreta 63 usada se almacenan en la tabla de claves 61 del almacenamiento de secretos 51, 9 del almacenamiento interno 7 (figura 1).

[0026] Si durante el funcionamiento de la infraestructura, el número de nodos se vuelve permanentemente menor que *n*, el nodo que cargó el fichero al grupo de datos compartidos 1 (figura 1) puede recalcular y redistribuir las partes secretas como una nueva versión en función de una nueva sal y nuevos valores *n* y *k*. El nuevo valor de sal hace que las nuevas partes secretas sean incompatibles con las partes ya distribuidas.

[0027] Con referencia a la figura 7, todas las ***k*** partes secretas y su número de versión se envían como mensajes 80 dedicados a través de la red de cadena de bloques 4 (figura 1) a los nodos del grupo de datos compartidos 1 (figura 1). Cada mensaje está encriptado para el receptor con la clave pública 13 (figura 1) de ese receptor de modo que cada socio solo tiene acceso a una parte del secreto. Todos los nodos restantes del grupo de datos compartidos sabrán entonces que esa parte secreta está disponible de ese nodo.

[0028] Con referencia a la figura 4, cada nodo que recibe una parte secreta 59 la almacenará con la ID de fichero 57 y su número de parte 58 y el número de versión 79 en su tabla de partes secretas 56 local.

[0029] En los mensajes 80 que envían las partes secretas a nodos dedicados y almacenados en la cadena de bloques 70 (figura 5), se publica qué ID de nodo 55 (figura 4) es responsable de qué número de parte 54 (figura 4) de qué ID de fichero 53 (figura 4). Adicionalmente, se adjuntan los parámetros *n* (66) y *k* (67) que se usan para calcular la parte más el número de versión 68 de ese conjunto de parámetros. Toda la información puede firmarse digitalmente, por ejemplo, mediante el uso del certificado, por el nodo 5, 15 que está publicando esa información.

[0030] Cada nodo en la red de cadena de bloques 4 leerá esa información (ID de fichero 53, número de parte 54, ID de nodo 55 responsable, *n* (66), *k* (67), número de versión 68) y la copiará a su tabla de búsqueda de partes secretas 52 local en su almacenamiento de secretos 51.

[0031] Con referencia de nuevo a la figura 1, un cliente asociado 14 que quiere acceder a un fichero pedirá al almacenamiento en red distribuido 5 local que busque en la red de tabla *hash* distribuida 2 la ID de fichero 42 (figura 3) de un nombre de fichero dado 60. Basándose en la tabla de consulta de tabla *hash* 44 y la ID de fichero 45, se puede determinar el valor de *hash* 47 de cada bloque 46 requerido. En función de ese valor de *hash* 49, el nodo descarga entonces los bloques de ficheros encriptados 50 enumerados en la red de tabla *hash* distribuida 2.

[0032] Con referencia a la figura 7, el nodo envía entonces una solicitud para las partes secretas 81 a través de la cadena de bloques 70 (figura 5). Cada nodo proporciona la información solicitada a través de un mensaje 82 a través del registro de cadena de bloques 70 (figura 5). Los mensajes incluyen información acerca de quién accedió a qué parte de qué fichero 82. La información puede firmarse digitalmente, por ejemplo, por el uso del certificado, por el nodo 5, 15 que está proporcionando esa información.

[0033] Con referencia a la figura 6, después de descargar un mínimo de *n* (93) partes 91 de todas las *k* (94) partes 90, el nodo es capaz de realizar una reconstrucción basándose en el algoritmo de Shamir 92. El resultado 95 consiste en dos partes: la sal aleatoria 96 que se puede ignorar y la clave secreta 97. Todos los bloques que se han descargado 98 forman el fichero encriptado 99. Junto con la clave secreta 97 y el uso del algoritmo de desencriptación 100, se puede descifrar el fichero original 101.

[0034] El fichero descifrado puede almacenarse para un futuro acceso en la tabla de ficheros 41 (figura 3) del almacenamiento de ficheros 40 (figura 3) y hacerse disponible a través de un protocolo de descarga 16 (figura 1) al cliente de acceso 11 (figura 1).

[0035] En el caso de que el número de nodos en la red se esté volviendo inferior al número mínimo requerido de partes *n*, el proveedor de un fichero puede recalcular y distribuir las nuevas partes secretas (33) en función de una nueva sal (28) y nuevos *n* (30) y *k* (31). El nodo envía entonces un mensaje de revocación de partes secretas 84 (figura 7) a través de la cadena de bloques 70 (figura 5) para revocar la última versión del conjunto de partes secretas. Este mensaje puede usarse también para hacer inaccesible un fichero en el grupo de datos compartidos 1 (figura 1), porque no habrá ninguna parte secreta disponible para reconstruir la clave de desencriptación.

[0036] Con referencia a la figura 5, los mensajes (80, 81, 82, 84) se almacenan en el registro de cadena de bloques (70) dentro de una estructura de mensajes (76) como parte de un árbol *hash* (74, 75), dentro de un bloque (71) que está vinculado irreversiblemente a los bloques precedentes (72), incluyendo información administrativa específica de la cadena de bloques (73).

REIVINDICACIONES

1. método de distribución y recuperación de datos en una red informática (2, 4) con nodos pares (5,15), que comprende:

(a) encriptar, con una clave secreta (22), un fichero (20) que contiene dichos datos;
(b) dividir (24) el fichero encriptado (23) en bloques (25, 50) y dividir (32) la clave secreta (22) en partes secretas (33, 59);
(c) distribuir los bloques (50) y las partes secretas (59) a los nodos pares (5, 15);
(d) tras la solicitud de un cliente (11) de acceder al fichero (20), recuperar a través de uno de los nodos pares (5, 15) los bloques encriptados (50, 98) para reconstruir el fichero (23) encriptado, recuperar al menos algunas de las partes secretas (59, 90) para reconstruir la clave secreta (22, 97) y desencriptar el fichero encriptado (23, 99) con la clave secreta reconstruida (97);
caracterizado por el hecho de que
los nodos pares (5, 15) comparten una cadena de bloques (10, 70) para formar una red de cadena de bloques (4);
en el paso (c), las partes secretas (33,59) se transmiten a los nodos pares (5, 15) a través de mensajes (80) enviados sobre la red de cadena de bloques (4); y en el paso (d), la solicitud y la recuperación de las partes secretas (59, 90) se hace a través de mensajes (81, 82) enviados sobre la red de cadena de bloques (4).

2. Método según la reivindicación 1, donde en cada mensaje (80, 81, 82) de transmisión, solicitud y recuperación de las partes secretas (59, 90) en los pasos (c) y (d), respectivamente, dichas partes secretas (59, 90) se encriptan con una clave pública (13) del nodo par (5, 15) que es el receptor de dicho mensaje.

3. Método según una de las reivindicaciones 1 y 2, donde cada mensaje (80, 81, 82) de transmisión, solicitud y recuperación de las partes secretas (59, 90) en los pasos (c) y (d), respectivamente, contiene información que identifica el nodo par (5, 15) que envía el mensaje, identifica el receptor del/de los nodo(s) par(es) (5,15) de dicho mensaje e identifica la parte secreta (59, 90) que se transmite o recupera, donde dicha información es accesible públicamente a todos los nodos pares (5, 15) de la red (2, 4), preferiblemente donde la información que identifica la parte secreta (59, 90) en cada mensaje (80, 81, 82) de transmisión, solicitud y recuperación de las partes secretas (33, 59, 90) en los pasos (c) y (d), respectivamente, identifica el número (54, 58) de la parte secreta (33, 59, 90) en relación con la clave secreta (22) y el fichero (42, 60, 43) asociado a dicha parte secreta.

4. Método según la reivindicación 3, donde la información que identifica la parte secreta (33, 59, 90) en cada mensaje (80, 81, 82) de transmisión, solicitud y recuperación de las partes secretas (33, 59, 90) en los pasos (c) y (d), respectivamente, identifica la versión (68, 69, 79) de la parte secreta, preferiblemente donde una versión (68, 69, 79) de las partes secretas se puede revocar por un mensaje (84) enviado desde uno de los nodos pares a todos los nodos restantes.

5. Método según cualquiera de las reivindicaciones 1 a 4, donde cada mensaje (80, 81, 82) de transmisión, solicitud y recuperación de las partes secretas (33, 59, 90) en los pasos (c) y (d), respectivamente, es firmado digitalmente por el nodo par que envía el mensaje.

6. Método según cualquiera de las reivindicaciones 1 a 5, donde el paso (d) comprende enviar un mensaje (81) de solicitud de partes secretas, desde uno de los nodos a todos los nodos pares restantes, antes de enviar mensajes (82) de recuperación de dichas partes secretas, desde dichos nodos pares restantes.

7. Método según cualquiera de las reivindicaciones 1 a 6, donde el registro de cadena de bloques (10, 70) contiene todos los mensajes (80, 81, 82, 84) de transmisión, solicitud y recuperación de las partes secretas en los pasos (c) y (d), respectivamente, preferiblemente donde los mensajes (80, 81, 82, 84) están contenidos en un árbol *hash* de la cadena de bloques (70).

8. Método según cualquiera de las reivindicaciones 1 a 7, donde en el paso (b), una clave secreta (22) salada (28) se divide en *k* partes secretas (33, 59) basándose en una técnica de compartición de secretos donde *n* partes secretas, $n<k$, son suficientes para reconstruir la clave secreta (22, 63, 97), preferiblemente donde *k*l2<n3/4*k* y $k>2$.

9. Método según la reivindicación 8, donde cada mensaje (80, 81, 82) de transmisión, solicitud y recuperación de las partes secretas (33, 59, 90) en los pasos (c) y (d), respectivamente, contiene información que identifica la parte secreta y los valores *n* y *k* y la versión de dicha parte secreta.

10. Método según cualquiera de las reivindicaciones 1 a 9, donde cada nodo par (5, 15) comprende un identificador (12) único, un espacio de almacenamiento de datos (7), un gestor de redes (6), una clave pública (13),

proporcionada preferiblemente dentro de un certificado, y una clave privada (14), preferiblemente donde en el paso (c) los bloques (50) y las partes secretas (59) se almacenan en el espacio de almacenamiento de datos (7) de los nodos pares (5, 15).

11. Método según cualquiera de las reivindicaciones 1 a 10, donde en el paso (a) la clave secreta (22) se genera de forma aleatoria, preferiblemente con sales (23).

12. Método según cualquiera de las reivindicaciones 1 a 11, donde en el paso (c) los bloques (50) se asocian y distribuyen a nodos pares (5, 15) según un algoritmo de *hash* distribuido, donde el paso (c) produce una red distribuida (2).

13. Programa informático que comprende instrucciones que son ejecutables por un ordenador, **caracterizado por el hecho de que** las instrucciones están configuradas para ejecutar los pasos del método según cualquiera de las reivindicaciones 1 a 12 cuando se ejecutan en dicho ordenador.

14. Servidor de almacenamiento de datos informático (5), preferiblemente del tipo almacenamiento en red, con medio de almacenamiento (7) y **caracterizado por el hecho de que** el medio de almacenamiento almacena un programa informático según la reivindicación 13.

15. Red informática (2, 4) con nodos pares (5, 15), donde cada nodo par (5, 15) comprende un único identificador (12), un espacio de almacenamiento de datos (7), un gestor de redes (6), una clave pública (13), proporcionada preferiblemente dentro de un certificado, y una clave privada (14); donde cada gestor de redes (6) comprende medios configurados para ejecutar los pasos del método según cualquiera de las reivindicaciones 1 a 12.

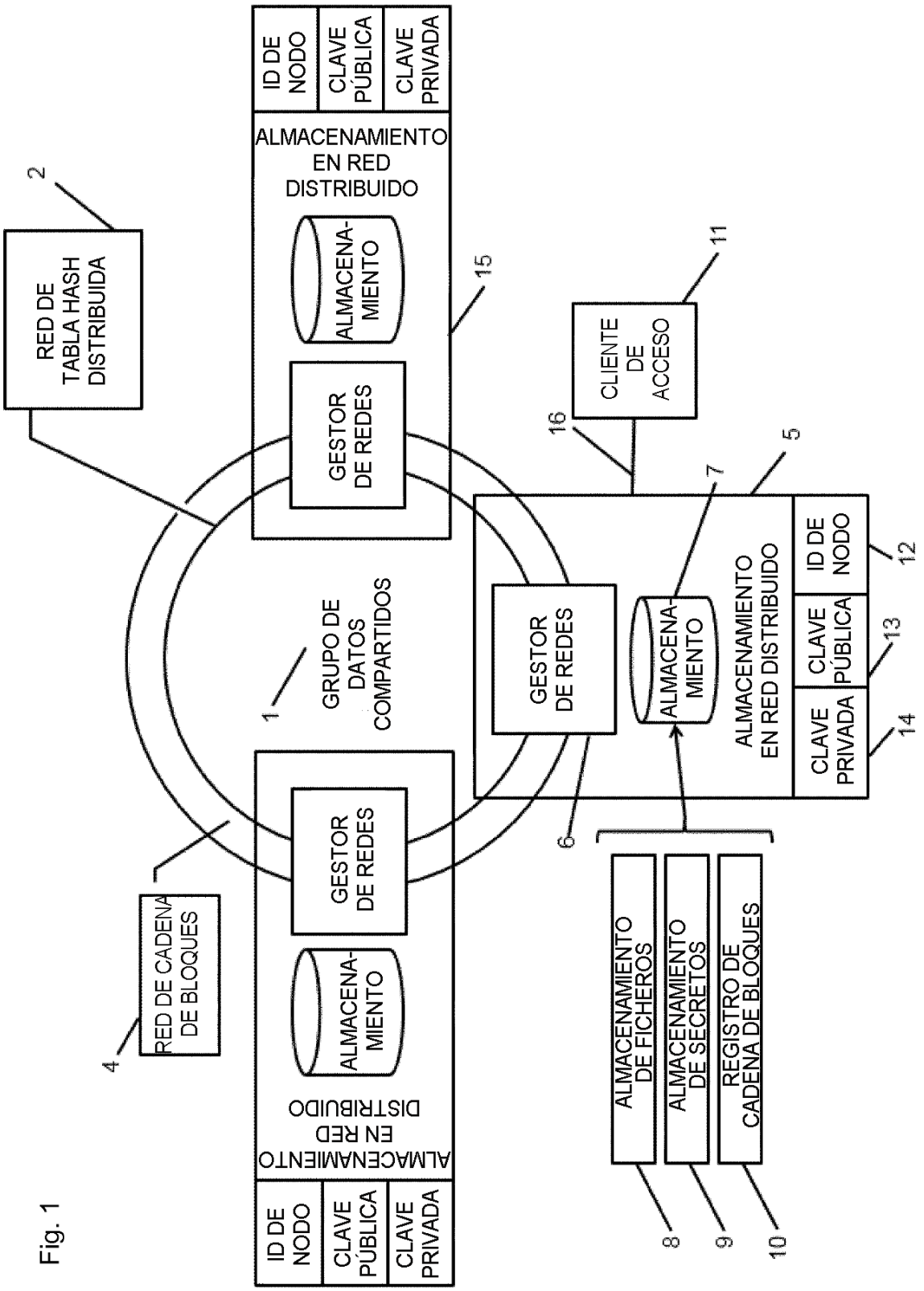

ID DE NODO
CLAVE PÚBLICA
CLAVE PRIVADA
ALMACENAMIENTO EN RED DISTRIBUIDO
ALMACENA-MIENTO
GESTOR DE REDES
15
2
RED DE TABLA HASH DISTRIBUIDA
11
CLIENTE DE ACCESO
16
5
7
GESTOR DE REDES
ALMACENA-MIENTO
ALMACENAMIENTO EN RED DISTRIBUIDO
ID DE NODO
CLAVE PÚBLICA
CLAVE PRIVADA
12
13
14
1
GRUPO DE DATOS COMPARTIDOS
6
4
RED DE CADENA DE BLOQUES
GESTOR DE REDES
ALMACENA-MIENTO
ALMACENAMIENTO EN RED DISTRIBUIDO
ID DE NODO
CLAVE PÚBLICA
CLAVE PRIVADA
ALMACENAMIENTO DE FICHEROS
ALMACENAMIENTO DE SECRETOS
REGISTRO DE CADENA DE BLOQUES
8
9
10

Fig. 1

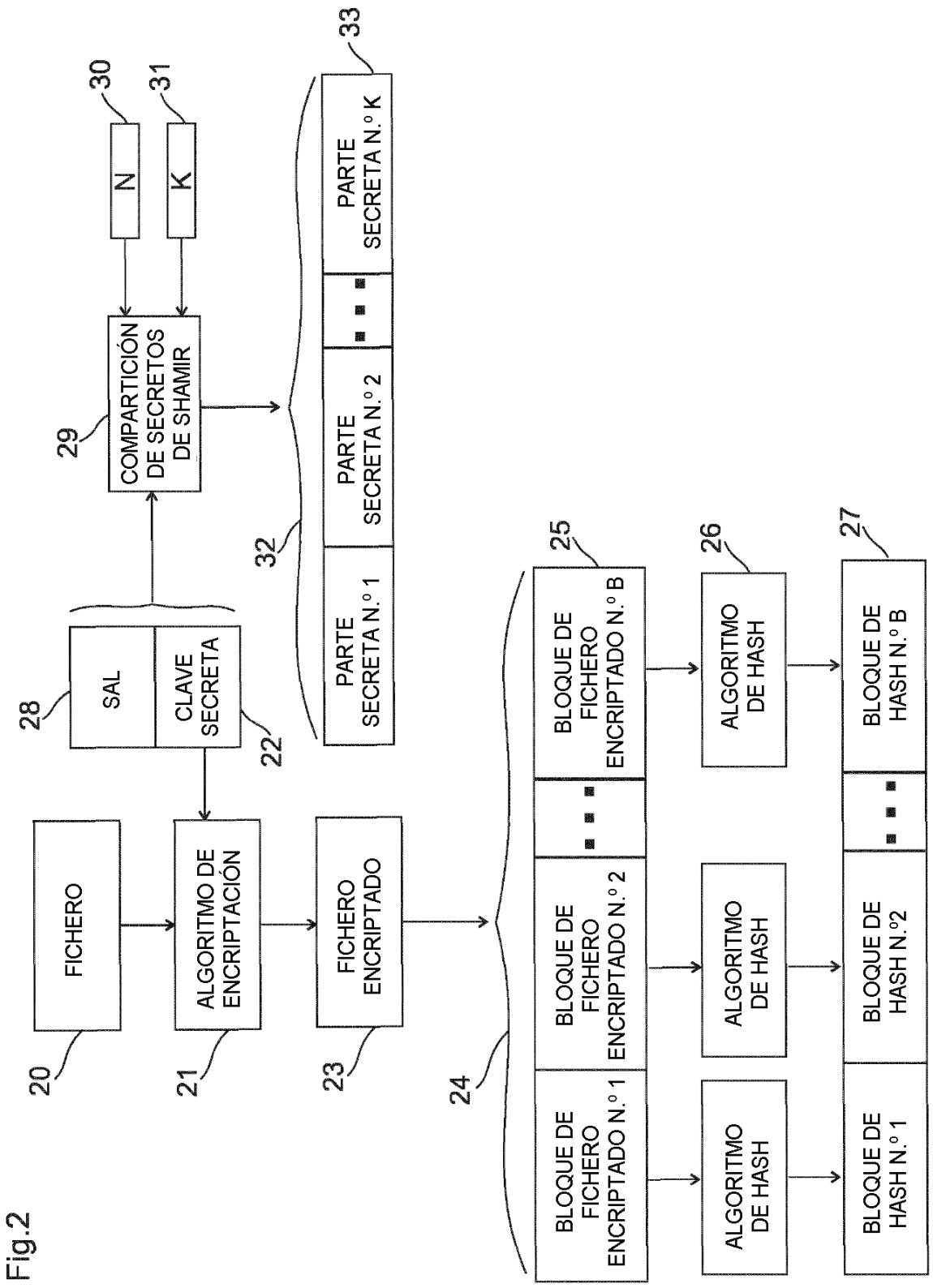

FICHERO
20
ALGORITMO DE ENCRIPTACIÓN
21
FICHERO ENCRIPTADO
23
SAL
CLAVE SECRETA
28
22
N
30
K
31
COMPARTICIÓN DE SECRETOS DE SHAMIR
29
PARTE SECRETA N.º 1
PARTE SECRETA N.º 2
PARTE SECRETA N.º K
32
33
BLOQUE DE FICHERO ENCRIPTADO N.º 1
BLOQUE DE FICHERO ENCRIPTADO N.º 2
BLOQUE DE FICHERO ENCRIPTADO N.º B
24
25
ALGORITMO DE HASH
ALGORITMO DE HASH
ALGORITMO DE HASH
26
BLOQUE DE HASH N.º 1
BLOQUE DE HASH N.º2
BLOQUE DE HASH N.º B
27

Fig.2

Fig.3

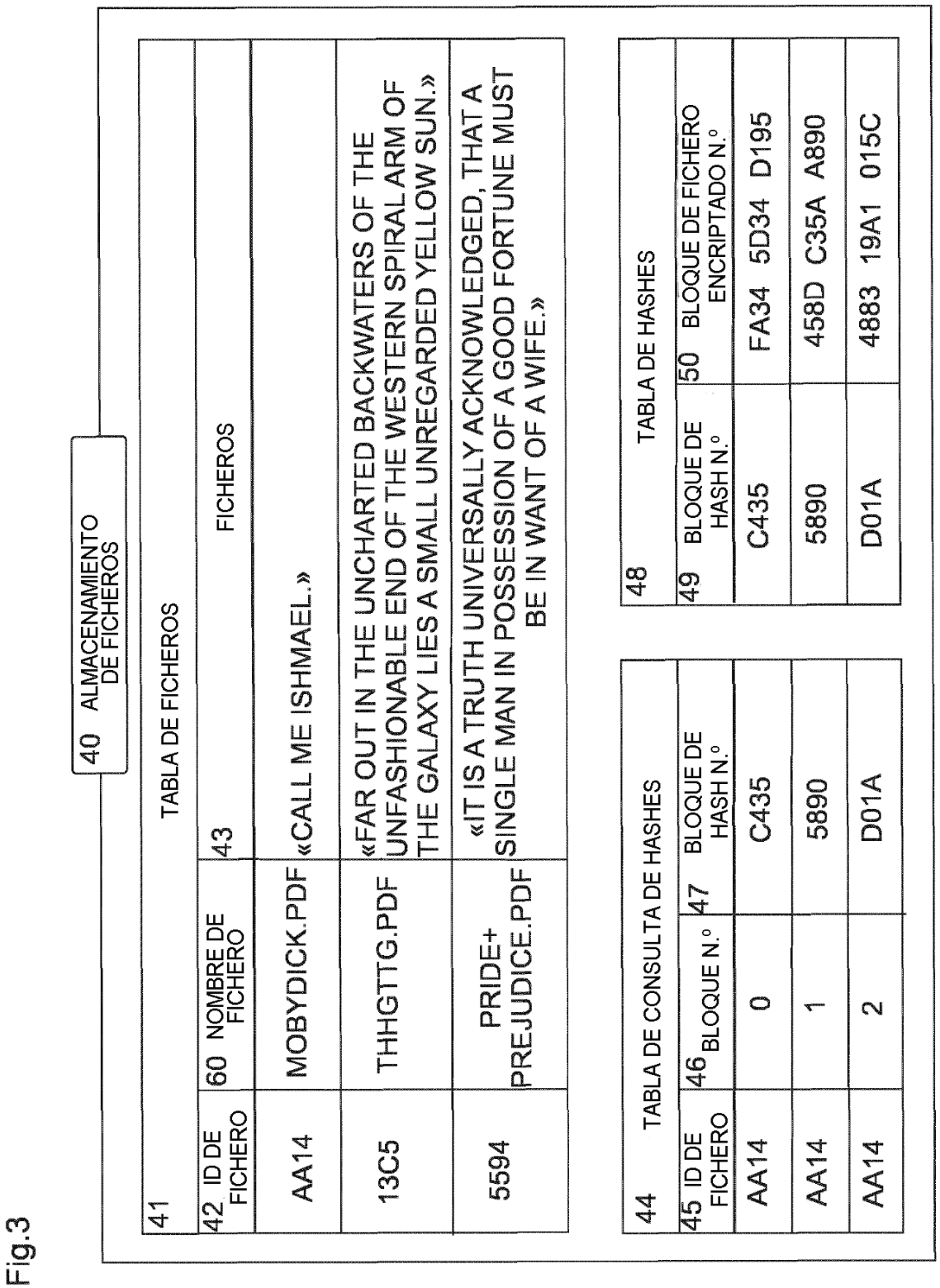

40 ALMACENAMIENTO DE FICHEROS
41 TABLA DE FICHEROS
42 ID DE FICHERO
60 NOMBRE DE FICHERO
43 FICHEROS
AA14
MOBYDICK.PDF
«CALL ME ISHMAEL.»
13C5
THHGTTG.PDF
«FAR OUT IN THE UNCHARTED BACKWATERS OF THE UNFASHIONABLE END OF THE WESTERN SPIRAL ARM OF THE GALAXY LIES A SMALL UNREGARDED YELLOW SUN.»
5594
PRIDE+ PREJUDICE.PDF
«IT IS A TRUTH UNIVERSALLY ACKNOWLEDGED, THAT A SINGLE MAN IN POSSESSION OF A GOOD FORTUNE MUST BE IN WANT OF A WIFE.»
44 TABLA DE CONSULTA DE HASHES
45 ID DE FICHERO
46 BLOQUE N.º
47 BLOQUE DE HASH N.º
AA14 0 C435
AA14 1 5890
AA14 2 D01A
48 TABLA DE HASHES
49 BLOQUE DE HASH N.º
50 BLOQUE DE FICHERO ENCRIPTADO N.º
C435 FA34 5D34 D195
5890 458D C35A A890
D01A 4883 19A1 015C

Fig.4

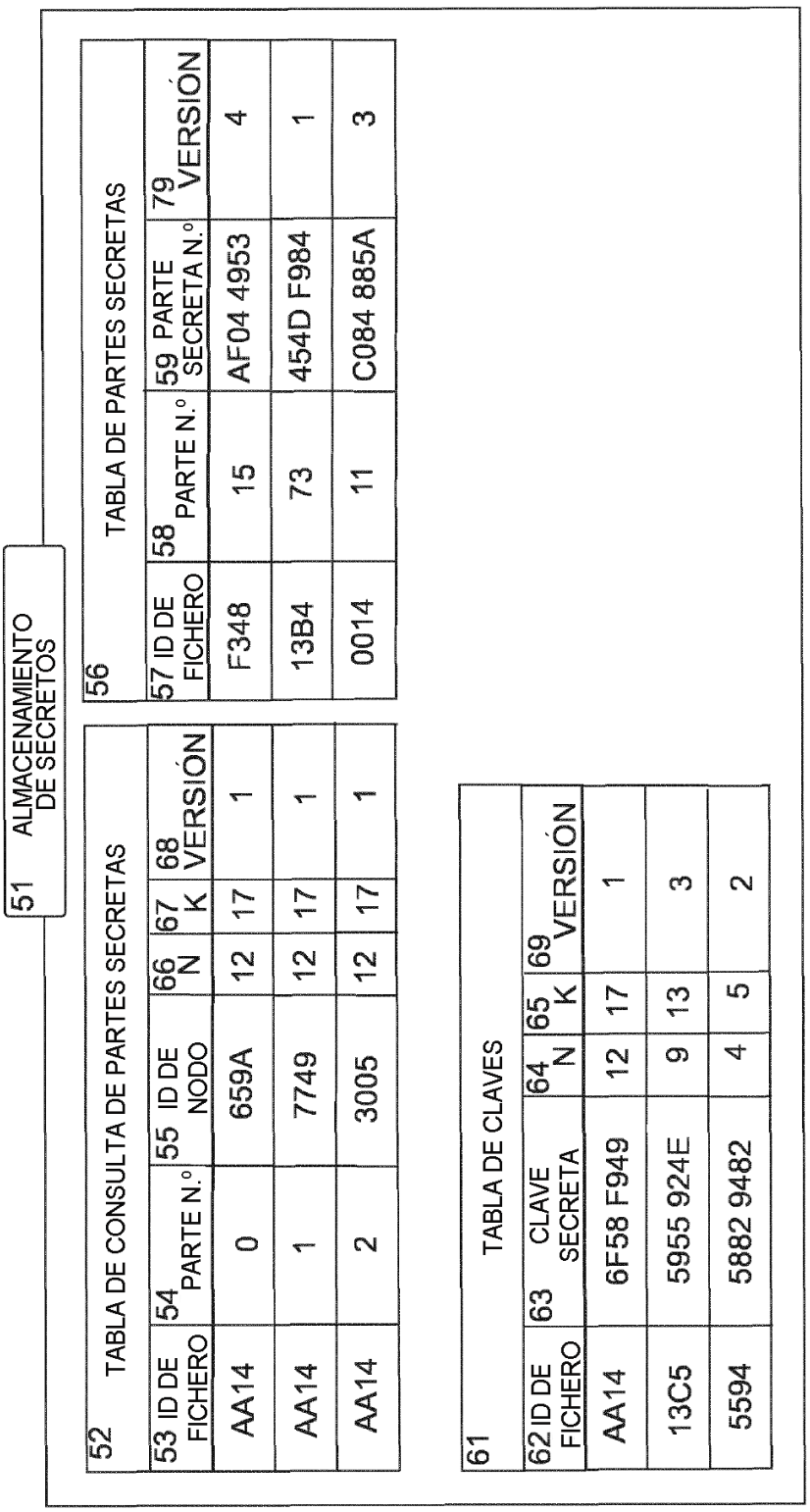
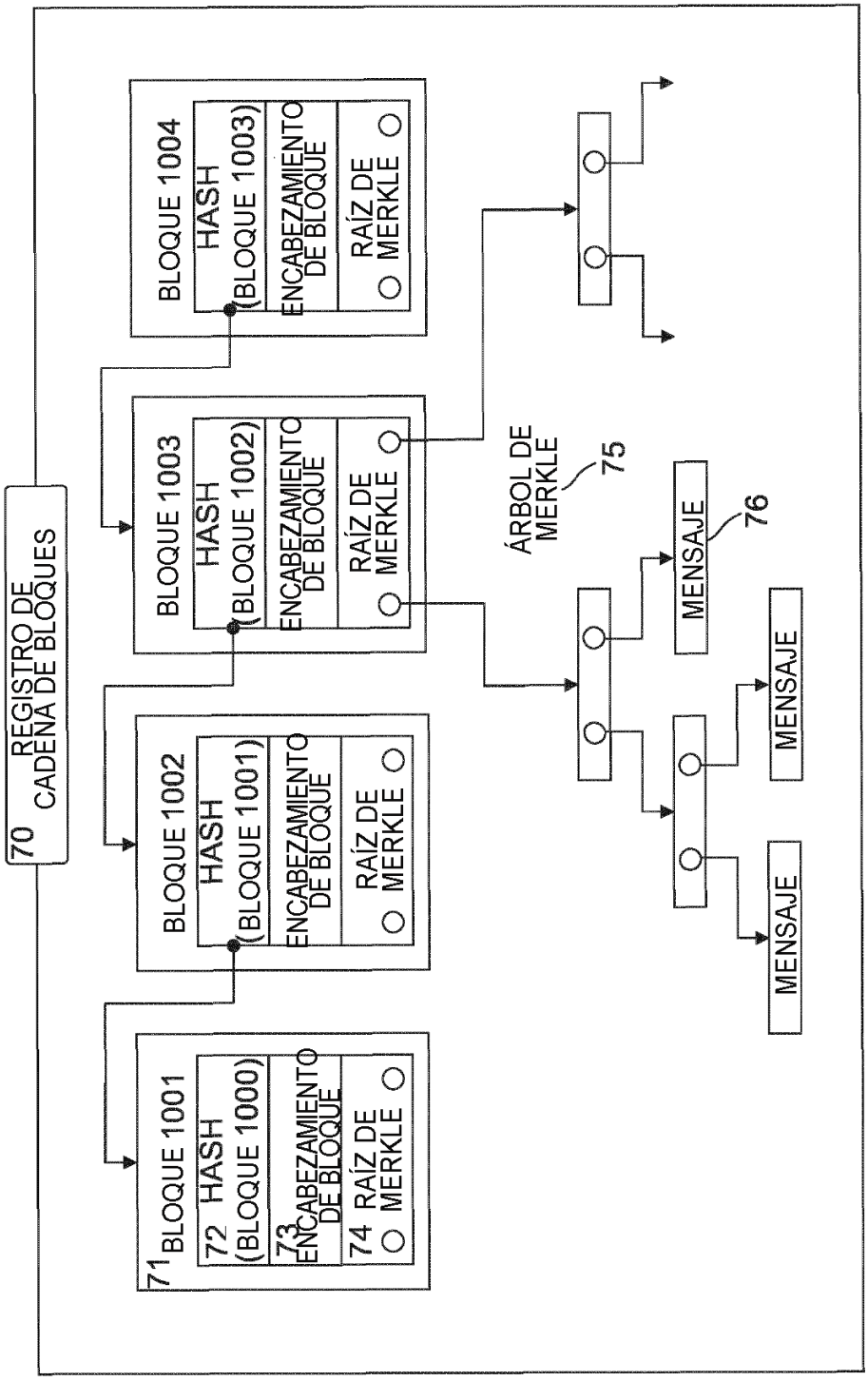

51 ALMACENAMIENTO DE SECRETOS
52 TABLA DE CONSULTA DE PARTES SECRETAS
53 ID DE FICHERO
54 PARTE N.º
55 ID DE NODO
66 N
67 K
68 VERSIÓN
AA14 0 659A 12 17 1
AA14 1 7749 12 17 1
AA14 2 3005 12 17 1
56 TABLA DE PARTES SECRETAS
57 ID DE FICHERO
58 PARTE N.º
59 PARTE SECRETA N.º
79 VERSIÓN
F348 15 AF04 4953 4
13B4 73 454D F984 1
0014 11 C084 885A 3
61 TABLA DE CLAVES
62 ID DE FICHERO
63 CLAVE SECRETA
64 N
65 K
69 VERSIÓN
AA14 6F58 F949 12 17 1
13C5 5955 924E 9 13 3
5594 5882 9482 4 5 2

Fig.5


70
REGISTRO DE CADENA DE BLOQUES
BLOQUE 1001
72 HASH (BLOQUE 1000)
73 ENCABEZAMIENTO DE BLOQUE
74 RAÍZ DE MERKLE
71
BLOQUE 1002
HASH (BLOQUE 1001)
ENCABEZAMIENTO DE BLOQUE
RAÍZ DE MERKLE
BLOQUE 1003
HASH (BLOQUE 1002)
ENCABEZAMIENTO DE BLOQUE
RAÍZ DE MERKLE
BLOQUE 1004
HASH (BLOQUE 1003)
ENCABEZAMIENTO DE BLOQUE
RAÍZ DE MERKLE
ÁRBOL DE MERKLE
75
MENSAJE
76
MENSAJE
MENSAJE

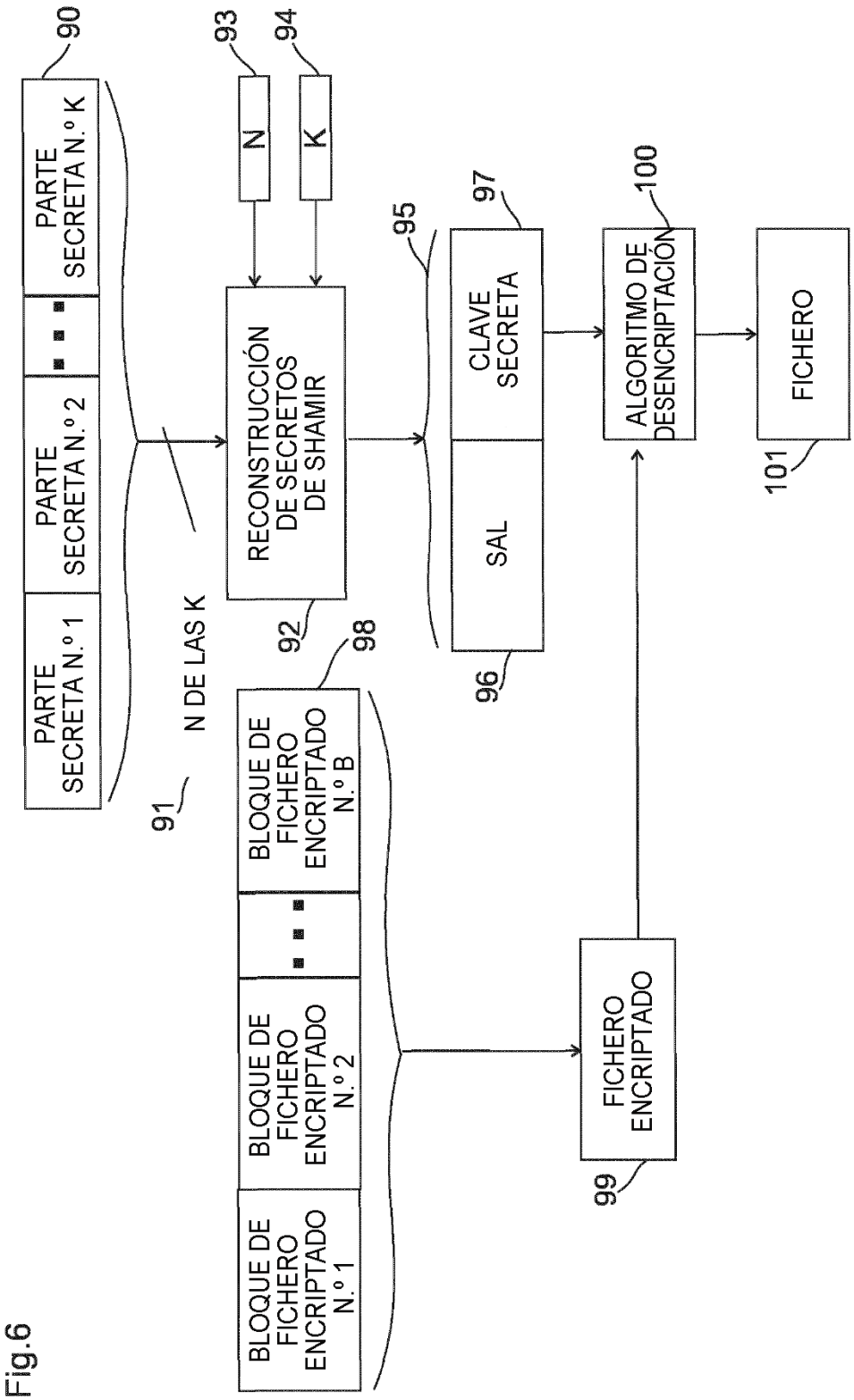

PARTE SECRETA N.º 1
PARTE SECRETA N.º 2
PARTE SECRETA N.º K
90
N DE LAS K
91
N
K
93
94
RECONSTRUCCIÓN DE SECRETOS DE SHAMIR
92
95
CLAVE SECRETA
SAL
96
97
ALGORITMO DE DESENCRIPTACIÓN
100
FICHERO
101
BLOQUE DE FICHERO ENCRIPTADO N.º 1
BLOQUE DE FICHERO ENCRIPTADO N.º 2
BLOQUE DE FICHERO ENCRIPTADO N.º B
98
FICHERO ENCRIPTADO
99

Fig.6

Fig. 7

PUBLICAR PARTE SECRETA 80

FIRMA (MENSAJE[
TIPO DE MENSAJE = PUBLICARPARTESECRETA
DEL NODO ID = AA49
AL NODO ID = 3005
ID DE FICHERO = AA14
PARTE N.º = 2
VERSIÓN = 1
N = 12, K = 17
ENC(PARTE SECRETA N.º2, PUB CLAVE (NODOID = 3005))]
CERT(NODOID=AA49))

EL NODO AA49 ENVÍA LA VERSIÓN 1 DE LA PARTE SECRETA N.º2 DEL FICHERO AA14 AL NODO 3005 ENCRIPTADA CON LA CLAVE PÚBLICA DEL NODO 3005, FIRMADA POR AA49
DE MODO QUE TODOS SABRÁN QUE ESTA PARTE SECRETA ESTÁ DISPONIBLE DEL NODO 3005

SOLICITAR PARTES SECRETAS 81

FIRMA (MENSAJE[
TIPO DE MENSAJE = SOLICITARPARTESSECRETAS
DEL NODO ID = 5456
AL NODO ID = TODOS
ID DE FICHERO = AA14],
CERT(NODOID = 5456))

EL NODO 5456 SOLICITA TODAS LAS PARTES SECRETAS DEL FICHERO AA14 DE TODOS LOS NODOS, FIRMADAS POR 5456
DE MODO QUE TODOS LOS NODOS QUE TENGAN UNA PARTE SECRETA SABRÁN QUE ESTAS PARTES SECRETAS SON SOLICITADAS POR EL NODO 5456

REVOCAR PARTE SECRETA 84

FIRMA (MENSAJE[
TIPO DE MENSAJE = REVOCARPARTESECRETA
DEL NODO ID = AA49
AL NODO ID = TODOS
ID DE FICHERO = AA14
VERSIÓN = 1
N = 12, K = 17
CERT(NODOID=AA49))

EL NODO AA49 REVOCA LA VERSIÓN 1 DE TODAS LAS PARTES SECRETAS DEL FICHERO AA14 A TODOS LOS NODOS 3005, FIRMADAS POR AA49
DE MODO QUE TODOS SABRÁN QUE ESTAS PARTES SECRETAS DE ESA VERSIÓN YA NO SON VÁLIDAS

PROPORCIONAR PARTE SECRETA 82

FIRMA (MENSAJE[
TIPO DE MENSAJE = PROPORCIONARPARTESECRETA
DEL NODO ID = 3305
AL NODO ID = 5456
ID DE FICHERO = AA14
PARTE N.º = 2
VERSIÓN = 1
N = 12, K = 17
ENC(PARTE SECRETA, PUB CLAVE (NODOID = 5456))]
CERT(NODOID = 3305))

EL NODO 3305 ENVÍA LA PARTE SECRETA N.º2 DEL FICHERO AA14 AL NODO 5456, ENCRIPTADA CON LA CLAVE PÚBLICA DEL NODO 5456, FIRMADA POR 3305
DE MODO QUE TODOS SABRÁN QUE A ESTA PARTE SECRETA ACCEDIÓ EL NODO 5456

ES 2 817 433 T3