(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 872 101**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.04.2019 PCT/CN2019/084530**

(87) Fecha y número de publicación internacional: **18.07.2019 WO19137565**

(96) Fecha de presentación y número de la solicitud europea: **26.04.2019 E 19739185 (7)**

(97) Fecha y número de publicación de la concesión europea: **10.03.2021 EP 3643041**

(54) Título: **Gestión de claves distribuidas para entornos de ejecución confiables**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.11.2021

(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:

WEI, CHANGZHENG;
YAN, YING;
ZHAO, BORAN y
SONG, XUYANG

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Gestión de claves distribuidas para entornos de ejecución confiables

CAMPO TÉCNICO

Esta memoria descriptiva se refiere a entornos de ejecución confiables.

ANTECEDENTES

Los sistemas de contabilidad distribuida (DLS), que también pueden denominarse redes de consenso y/o redes de cadena de bloques, permiten a las entidades participantes almacenar datos de forma segura e inmutable. Los DLS se conocen comúnmente como redes de cadena de bloques sin hacer referencia a un caso de uso en particular. Un ejemplo de un tipo de red de cadena de bloques puede incluir redes de cadena de bloques de consorcio proporcionadas para un grupo selecto de entidades, que controlan el proceso de consenso, e incluye una capa de control de acceso.

Un entorno de ejecución confiable (TEE) es un área aislada y segura de un microprocesador que garantiza que las instrucciones y los datos del software que se ejecutan o almacenan dentro del microprocesador no se han visto comprometidos o alterados. Las aplicaciones ejecutadas dentro del TEE se verifican por una autoridad confiable (p. ej., la fabricación del microprocesador) y se emiten claves de cifrado tras la verificación para permitir la comunicación entre la aplicación y otros nodos y aplicaciones confiables. Estas claves de cifrado pueden emitirse por un sistema de gestión de claves (KMS) centralizado que facilita la verificación de la aplicación con la autoridad de confianza (también conocida como "atestación").

Un problema potencial con un KMS centralizado es la introducción de un único punto de falla. Una interrupción en el KMS centralizado puede evitar que las aplicaciones que se ejecutan en los TEE se verifiquen hasta que se resuelva. Además, un atacante puede comprometer el sistema en su conjunto al obtener el control del KMS centralizado. Por lo tanto, sería deseable un sistema distribuido y seguro que funcione como KMS.
El documento US 2018/227275 A1, está dirigido, en general, a cadena de bloques y otras tecnologías de seguridad.
El documento US 2018/247063 A1, se refiere a un acuerdo de intercambio de datos entre un primer usuario y un segundo usuario que se escribe, mediante una plataforma de intercambio de datos, en una cadena de bloques.

RESUMEN

Esta memoria descriptiva describe tecnologías para implementar un sistema de gestión de claves distribuido que incluye un conjunto de nodos de gestión de claves (KM). Cada uno de los nodos de KM ejecuta aplicaciones de gestión de claves dentro de los TEE y cada uno realiza un proceso de atestación mutua con uno o más de los otros nodos de KM en base a una lógica de atestación mutua para establecer relaciones de confianza que conectan todos los nodos de KM en el conjunto. Una vez que se establece esta confianza, los nodos de KM pueden llegar a un consenso para asignar claves de cifrado a uno o más TEE de servicio para ejecutar de forma segura una o más operaciones de contrato inteligente en un entorno de confianza.

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

Esta memoria descriptiva proporciona además un sistema para implementar los métodos proporcionados en el presente documento. El sistema incluye uno o más procesadores y un medio de almacenamiento legible por computadora acoplado al uno o más procesadores que 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 las realizaciones de los métodos proporcionados en este documento.

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

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

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La FIG. 1 es un diagrama que ilustra un ejemplo de un entorno que puede utilizarse para ejecutar realizaciones de esta memoria descriptiva.

La FIG. 2 es un diagrama que ilustra un ejemplo de una arquitectura de acuerdo con realizaciones de esta memoria descriptiva.

La FIG. 3 es un diagrama que ilustra un ejemplo de un sistema de acuerdo con realizaciones de esta memoria descriptiva.

La FIG. 4 es un diagrama que ilustra un ejemplo de un sistema de acuerdo con realizaciones de esta memoria descriptiva.

La FIG. 5 representa un ejemplo de un proceso que se puede ejecutar de acuerdo con realizaciones de esta memoria descriptiva.

La FIG. 6 representa ejemplos de módulos de un aparato de acuerdo con realizaciones de esta memoria descriptiva.

FIG. 7 es un diagrama que ilustra un ejemplo de una lógica de atestación mutua de acuerdo con realizaciones de esta memoria descriptiva.

La FIG. 8 es un diagrama que ilustra un ejemplo de otra lógica de atestación mutua de acuerdo con realizaciones de esta memoria descriptiva.

Los números de referencia y las designaciones similares en los diversos dibujos indican elementos similares.

DESCRIPCIÓN DETALLADA

Esta memoria descriptiva describe tecnologías para implementar un sistema de gestión de claves distribuido que incluye un conjunto de nodos de gestión de claves (KM). Cada uno de los nodos de KM ejecuta aplicaciones de gestión de claves dentro de los TEE y cada uno realiza un proceso de atestación mutua con uno o más de los otros nodos de KM en base a una lógica de atestación mutua para establecer relaciones de confianza que conectan todos los nodos de KM en el conjunto. Una vez que se establece esta confianza, los nodos de KM pueden llegar a un consenso para asignar claves de cifrado a uno o más TEE de servicio para ejecutar de forma segura una o más operaciones de contrato inteligente en un entorno de confianza.

Para proporcionar un contexto adicional para las realizaciones de esta memoria descriptiva, y como se introdujo anteriormente, los sistemas de contabilidad distribuida (DLS), que también pueden denominarse redes de consenso (p. ej., compuestas por nodos de igual a igual) y redes de cadena de bloques, permiten a las entidades participantes realizar transacciones de forma segura e inmutable y almacenar datos. Aunque el término cadena de bloques se asocia generalmente con redes particulares y/o casos de uso, cadena de bloques se utiliza en el presente documento para referirse generalmente a un DLS sin referencia a un caso de uso particular.

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

Mientras que una cadena de bloques es una estructura de datos descentralizada o al menos parcialmente descentralizada para almacenar transacciones, una red de cadenas de bloques es una red de nodos informáticos que administran, actualizan y mantienen una o más cadenas de bloques mediante la difusión, verificación y validación de transacciones, etc., Como se introdujo anteriormente, una red cadena de bloques se puede proporcionar como una red cadena de bloques pública, una red cadena de bloques privada o una red cadena de bloques de consorcio. Las realizaciones de esta memoria descriptiva se describen con más detalle en el presente documento con referencia a una red de cadena de bloques de consorcio. Sin embargo, se contempla que las realizaciones de esta memoria descriptiva se puedan realizar en cualquier tipo apropiado de red de cadena de bloques.

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

En algunos ejemplos, dentro de una red de cadena de bloques de consorcio, se proporciona una cadena de bloques global como una cadena de bloques que se replica en todos los nodos. Es decir, todos los nodos de consenso están

en perfecto estado de consenso con respecto a la cadena de bloques global. Para lograr el consenso (p. ej., acuerdo para la adición de un bloque a una cadena de bloques), se implementa un protocolo de consenso dentro de la red de cadena de bloques de consorcio. Por ejemplo, la red de cadena de bloques del consorcio puede implementar un consenso de tolerancia práctica a fallas bizantinas (PBFT), que se describe con más detalle a continuación.

La FIG. 1 es un diagrama que ilustra un ejemplo de un entorno 100 que puede utilizarse para ejecutar realizaciones de esta memoria descriptiva. En algunos ejemplos, el entorno 100 de ejemplo permite a las entidades participar en una red 102 de cadena de bloques de consorcio. El entorno 100 de ejemplo incluye dispositivos informáticos 106, 108 y una red 110. En algunos ejemplos, la red 110 incluye una red de área local (LAN) , red de área amplia (WAN), el Internet o una combinación de las mismas, y conecta sitios web, dispositivos de usuario (p. ej., dispositivos informáticos) y sistemas de servidor. En algunos ejemplos, se puede acceder a la red 110 a través de un enlace de comunicaciones cableado y/o inalámbrico.

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

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

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

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

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

Antes de almacenarlos en un bloque, los datos de transacción se resumen. El resumen es un proceso de transformación de los datos de transacción (proporcionados como datos de cadena) en un valor de resumen de longitud fija (también proporcionado como datos de cadena). No es posible deshacer el resumen del valor de resumen para obtener los datos de transacción. El resumen asegura que incluso un pequeño cambio en los datos de transacción

da como resultado un valor de resumen completamente diferente. Además, y como se indicó anteriormente, el valor de resumen es de longitud fija. Es decir, no importa el tamaño de los datos de transacción, la longitud del valor de resumen es fija. El resumen incluye procesar los datos de transacción a través de una función de resumen para generar el valor de resumen. Un ejemplo de función de resumen incluye, sin limitación, el algoritmo de resumen seguro (SHA) -256, que genera valores de resumen de 256 bits.

Los datos de transacción de múltiples transacciones se resumen y almacenan en un bloque. Por ejemplo, se proporcionan valores de resumen de dos transacciones y ellos mismos se resumen para proporcionar otro resumen. Este proceso se repite hasta que, para que todas las transacciones a ser almacenadas en un bloque, se proporciona un único valor de resumen. Este valor de resumen se denomina resumen de raíz de Merkle y se almacena en un encabezado del bloque. Un cambio en cualquiera de las transacciones dará como resultado un cambio en su valor de resumen y, en última instancia, un cambio en el resumen de raíz de Merkle.

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

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

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

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

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

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

El cifrado asimétrico se utiliza para proporcionar firmas digitales, lo que permite a los participantes en una transacción confirmar a otros participantes en la transacción, así como la validez de la transacción. Por ejemplo, un nodo puede

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

En algunas realizaciones, los nodos de la red de cadena de bloques y/o los nodos que se comunican con la red de cadena de bloques pueden operar utilizando los TEE. A alto nivel, un TEE es un entorno confiable dentro del hardware (uno o más procesadores, memoria) que está aislado del entorno operativo del hardware (p. ej., sistema operativo (SO), sistema básico de entrada/salida (BIOS)). Más en detalle, un TEE es un área separada y segura de un procesador que asegura la confidencialidad e integridad del código que se ejecuta y los datos cargados dentro del procesador principal. Dentro de un procesador, el TEE se ejecuta en paralelo con el SO. Al menos partes de las llamadas aplicaciones de confianza (TA) se ejecutan dentro del TEE y tienen acceso al procesador y la memoria. A través del TEE, las TA están protegidas de otras aplicaciones que se ejecutan en el SO principal. Además, el TEE aísla criptográficamente las TA entre sí dentro del TEE.

Un ejemplo de un TEE incluye Software Guard Extensions (SGX) proporcionada por Intel Corporation de Santa Clara, California, Estados Unidos. Aunque SGX se discute en el presente documento a modo de ejemplo, se contempla que las realizaciones de esta memoria descriptiva se puedan realizar utilizando cualquier TEE apropiado.

SGX proporciona un TEE basado en hardware. En SGX, el hardware confiable es la matriz de la unidad central procesamiento (CPU), y una porción de la memoria física está aislada para proteger el código y los datos seleccionados. Las porciones aisladas de la memoria se conocen como enclaves. Más particularmente, un enclave se proporciona como una caché de página de enclave (EPC) en memoria y se asigna a un espacio de direcciones de la aplicación. La memoria (p. ej., DRAM) incluye una memoria aleatoria preservada (PRM) para SGX. La PRM es un espacio de memoria continuo en el nivel más bajo de BIOS y ningún software puede acceder a él. Cada una de las EPC es un conjunto de memoria (p. ej., 4 KB) que se asigna por un SO para cargar datos y código de aplicación en la PRM. Los metadatos de EPC (EPCM) son la dirección de entrada para los respectivos EPC y garantizan que cada una de las EPC solo pueda compartirse por un enclave. Es decir, un solo enclave puede utilizar múltiples EPC, mientras que una EPC está dedicada a un solo enclave.

Durante la ejecución de una TA, el procesador opera en un llamado modo enclave cuando accede a los datos almacenados en un enclave. La operación en el modo enclave impone una verificación de hardware adicional para cada uno de los accesos a memoria. En SGX, una TA se compila en una porción confiable y una porción no confiable. La porción confiable es inaccesible, por ejemplo, para el SO, la BIOS, el código de sistema privilegiado, el administrador de máquina virtual (VMM), el modo de administración del sistema (SMM) y similares. En la operación, la TA se ejecuta y crea un enclave dentro de la PRM de la memoria. Una función confiable ejecutada por la porción confiable dentro del enclave se llama por la porción no confiable, y el código que se ejecuta dentro del enclave ve los datos como datos de texto plano (sin cifrar) y se niega el acceso externo a los datos. La porción confiable proporciona una respuesta cifrada a la llamada y la TA continúa ejecutándose.

Se puede realizar un proceso de atestación para verificar que el código esperado (p. ej., la porción confiable de la TA) se esté ejecutando de manera segura dentro de un TEE autenticado. En general, el proceso de atestación incluye un TEE que recibe una solicitud de atestación de un desafiador (p. ej., un sistema de gestión de claves (KMS) de la red de cadena de bloques). En respuesta, el TEE puede producir una cotización para realizar una atestación remota. Realizar la atestación remota incluye que una atestación local se envíe desde el enclave a un enclave de cotización, que verifica la atestación local y convierte la atestación local en la atestación remota firmando la atestación local utilizando una clave asimétrica de atestación. La cotización se proporciona al desafiador (p. ej., el KMS de la red de cadena de bloques).

El desafiador utiliza un servicio de verificación de atestación para verificar la atestación remota. Para SGX, Intel proporciona el Servicio de Atestación de Intel (IAS), que recibe la atestación remota del desafiador y verifica la atestación remota. Más particularmente, el IAS procesa la atestación remota y proporciona un informe (p. ej., informe de verificación de atestación (AVR)), que indica si se verifica la atestación remota. Si no se verifica, se puede indicar un error. Si se verifica (el código esperado se está ejecutando de forma segura en el TEE), el desafiador puede iniciar o continuar interacciones con el TEE. Por ejemplo, en respuesta a la verificación, el KMS (como desafiador) puede emitir claves de cifrado asimétricas (p. ej., un par de clave pública y clave privada) al nodo que ejecuta el TEE (p. ej., a través de un proceso de intercambio de claves, tal como la curva elíptica Diffie-Hellman (ECDH)) para permitir que el nodo se comunique de forma segura con otros nodos y/o clientes.

Un proceso de atestación mutua implica que un nodo que ejecuta un primer TEE que realiza una atestación remota de un nodo que ejecuta un segundo TEE, después de lo cual el nodo que ejecuta el segundo TEE realiza una

atestación remota del nodo que ejecuta el primer TEE. Una vez que ambos nodos se han verificado entre sí, los nodos pueden realizar un proceso de intercambio de claves para permitir una comunicación segura entre ellos.

En algunas redes de cadena de bloques, se pueden ejecutar los llamados contratos inteligentes. Los contratos inteligentes se pueden describir como representaciones digitales de contratos legales del mundo real que tienen términos contractuales que afectan a diversas partes. Un contrato inteligente se implementa, almacena, actualiza (según sea necesario) y se ejecuta dentro, en el contexto de ejemplo, una red de cadena de bloques de consorcio. Las partes contratantes asociadas con el contrato inteligente (p. ej., compradores y vendedores) se representan como nodos en la red de cadena de bloques de consorcio. En algunos ejemplos, las partes contratantes pueden incluir entidades (p. ej., empresas comerciales) que están asociadas con el contrato inteligente (p. ej., como partes del contrato inteligente).

Con más detalle, los contratos inteligentes se proporcionan como programas ejecutables por computadora que se ejecutan en cadenas de bloques (p. ej., un nodo dentro de una red de cadenas de bloques). Un contrato inteligente contiene un conjunto de reglas predefinidas bajo las cuales las partes de ese contrato inteligente acuerdan interactuar entre sí. Si se cumplen las reglas predefinidas del contrato inteligente, el acuerdo definido en el contrato inteligente se aplica automáticamente. Un contrato inteligente suele ser resistente a la manipulación y facilita, verifica y aplica la negociación o ejecución de un acuerdo o transacción.

La FIG. 3 es un diagrama que ilustra un ejemplo de un sistema 300 de acuerdo con realizaciones de esta memoria descriptiva. Como se muestra, el sistema 300 incluye una red 302 de cadena de bloques que incluye los nodos 304a-d de cadena de bloques. Los nodos 304a-d de cadena de bloques incluyen los TEE 306a-d de servicio y los TEE 308a-d de gestión de claves (KM). Los nodos 304a-d tienen acceso a la lógica 330 de servicio de contrato inteligente. Un centro 310 de gestión de claves está acoplado de forma comunicable a los nodos 304a-d.

Cada uno de los nodos 304a-d es un nodo de cadena de bloques que participa en la red 302 de cadena de bloques y contribuye al mantenimiento de una cadena de bloques asociada con la red (no mostrada) 302 de cadena de bloques. Como se describió anteriormente, los nodos 304a-d pueden participar en un proceso de consenso asociado con la red 302 de cadena de bloques, pueden recopilar transacciones en bloques para añadirlos a la cadena de bloques, pueden procesar transacciones solicitadas por los usuarios de la red 302 de cadena de bloques, pueden ejecutar operaciones codificadas en contratos inteligentes y realizar otras tareas relacionadas con la gestión de la cadena de bloques. En algunas realizaciones, cada uno de los nodos puede ser un dispositivo informático (p. ej., un servidor) que incluye uno o más procesadores, dispositivos de almacenamiento y otros componentes. En algunos casos, los nodos 304a-d se comunican a través de una red (no mostrada) de comunicaciones entre sí y con otros nodos que participan en la red 302 de cadena de bloques. Para el resto de la descripción de la FIG. 3, el nodo 304a se describirá como un ejemplo, entendiendo que los nodos 304b-d también pueden incluir las características del nodo 304a.

El nodo 304a incluye un TEE 306a de servicio. En algunas realizaciones, el TEE 306a de servicio es un entorno de aplicación seguro implementado utilizando una tecnología de TEE (p. ej., Intel SGX). El TEE 306a de servicio puede ejecutar uno o más programas o bibliotecas de software. Para los propósitos de la presente memoria descriptiva, el TEE 306a de servicio se refiere al entorno seguro (el TEE) así como al software que se ejecuta dentro del TEE que realiza las operaciones descritas. En algunas realizaciones, el TEE 306a de servicio ejecuta operaciones de contrato inteligente especificadas por solicitudes de cliente cifradas y genera resultados cifrados asociados con las operaciones de contrato inteligente. Esta funcionalidad se describe con mayor detalle con respecto a la FIG. 4 a continuación.

El nodo 304a también incluye un TEE 308a de gestión de claves (TEE de KM). En algunas realizaciones, el TEE 308a de KM es un entorno de aplicación seguro implementado utilizando una tecnología de TEE (p. ej., Intel SGX). El TEE 308a de KM puede ejecutar uno o más programas o bibliotecas de software. Para los propósitos de la presente memoria descriptiva, el TEE 308a de KM se refiere al entorno seguro (el TEE) así como al software que se ejecuta dentro del TEE que realiza las operaciones descritas. En algunas realizaciones, el TEE 308a de KM obtiene claves de cifrado del centro 310 de gestión de claves como se describe con mayor detalle con respecto a la FIG. 4 a continuación.

El centro 310 de gestión de claves puede generar, almacenar y mantener claves de cifrado. El centro 310 de gestión de claves también puede autenticar identidades de los TEE 308a-d de KM y proporcionar las claves de cifrado a los nodos 304a-d a través de un proceso 320 de despliegue de claves y atestación remota. En algunas realizaciones, la gestión de claves puede proporcionar claves de cifrado a clientes para interactuar con los nodos 304a-d. Esta funcionalidad se describe con mayor detalle con respecto a la FIG. 4 a continuación. En algunas realizaciones, el centro 310 de gestión de claves puede ser uno o más servidores u otros dispositivos informáticos en comunicación con uno o más nodos de la red 302 de cadena de bloques a través de una red (no mostrada) de comunicaciones. El centro 310 de gestión de claves también puede incluir uno o más dispositivos de almacenamiento acoplados al centro 310 de gestión de claves o accesibles a través de la red de comunicaciones para almacenar las claves de cifrado y otros datos.

En algunos casos, el centro 310 de gestión de claves opera para autenticar las identidades de los TEE 308a-d de KM antes de realizar despliegues de claves de cifrado. Por ejemplo, antes de proporcionar la una o más claves de cifrado (descritas a continuación) al TEE 308a de KM, el centro 310 de gestión de claves puede verificar la autenticidad del

TEE 308a de KM. Esta verificación asegura que el software ejecutado por el TEE 308a de KM no haya sido manipulado después de haber sido provisto. En algunas realizaciones, la verificación puede incluir un proceso 320 de atestación remota, tal como los descritos anteriormente.

Después de que los TEE 308a-d de KM obtengan la una o más claves de cifrado del centro 310 de gestión de claves, las claves se pueden reenviar a los TEE 306a-d de servicio para realizar operaciones criptográficas. En algunos casos, aunque un par de TEE de KM y TEE de servicio (p. ej., TEE 308a de KM y TEE 306a de servicio) operan en un solo nodo (p. ej., nodo 304a), cada uno tiene sus propios TEE independientes. Como resultado, la información comunicada entre los TEE 308a-d de KM y los TEE 306a-d de servicio se transmite a través de un área no confiable. En tales casos, los TEE 308a-d de KM pueden autenticar las identidades de los TEE 306a-d de servicio, por ejemplo, realizando un proceso de atestación local.

La atestación local puede permitir que un enclave demuestre su identidad o autenticidad a otro enclave dentro de la misma plataforma local. Por ejemplo, un TEE 308a de KM puede enviar un desafío para verificar la autenticidad del TEE 306a de servicio. Al recibir el desafío, el TEE 306a de servicio puede solicitar a un hardware (p. ej., CPU) del nodo 304a que genere un informe, que incluye una prueba criptográfica de que el TEE 306a de servicio existe en el nodo 304a. El informe se puede proporcionar al TEE 308a de KM para verificar que el informe del enclave se generó en la misma plataforma por el nodo 304a. En algunos casos, la atestación local se puede realizar en base un sistema de clave simétrica donde solo el TEE 308a de KM que verifica el informe y el hardware del enclave que genera el informe conocen la clave simétrica, que está incrustada en la plataforma de hardware del nodo 304a.

Después de que los TEE 306a-d de servicio se autentican mediante atestaciones locales, el TEE 308a-d de KM puede proporcionar la una o más claves de cifrado a los TEE 306a-d de servicio. En algunos casos, el TEE 308a-d de KM puede proporcionar las claves de cifrado en respuesta a la autenticación del TEE 306a-d de servicio, o puede proporcionar las claves en respuesta a una o más solicitudes del TEE 306a-d de servicio.

En lugar de confiar en el centro 310 de gestión de claves como autoridad central para desplegar claves de cifrado, esta memoria descriptiva proporciona además un esquema de gestión de claves descentralizado implementado por los TEE 308a-d de KM. Los TEE 308a-d de KM pueden establecer una relación de confianza y llegar a un consenso para proporcionar claves de cifrado a los respectivos TEE 306a-d de servicio.

A alto nivel, el esquema de gestión de claves descentralizado puede incluir una etapa de atestación mutua (MA) y una etapa de consenso. En la etapa de MA, cada uno de los TEE 308a-d de KM puede actuar como atestiguador y desafiador para realizar la MA con uno o más de otros TEE de KM en la red 302 de cadena de bloques. Las MA se pueden realizar en base a una lógica de MA para establecer una relación de confianza entre los TEE de KM en la red 302 de cadena de bloques. La lógica de MA para establecer la relación de confianza puede tener diferentes estructuras lógicas. En las descripciones de las FIG. 7 y 8 se analizan con más detalle dos lógicas de MA de ejemplo.

Después de que se establece una relación de confianza entre los TEE 308a-d de KM, el esquema de gestión de claves descentralizado puede entrar en la etapa de consenso. En la etapa de consenso, los TEE 308a-d de KM pueden generar y compartir claves de cifrado entre sí y llegar a un consenso sobre qué claves de cifrado se desplegarán a los TEE 306a-d de servicio. El consenso se puede alcanzar en base a realizar un proceso de consenso adecuado para una cadena de bloques de consorcio, tal como el PBFT descrito anteriormente. El despliegue de la clave de cifrado se puede realizar en base la autenticación de los respectivos TEE 306a-d de servicio a través de atestaciones locales.

En algunas realizaciones, los TEE 308a-d de KM pueden gestionar colectivamente el centro 310 de gestión de claves. En tales casos, las claves de cifrado aún pueden generarse por el centro 310 de gestión de claves y proporcionarse a los TEE 308a-d de KM después de atestaciones remotas exitosas. Sin embargo, qué claves de cifrado se desplegarán a cuál de los TEE 308a-d de KM o los TEE 306a-d de servicio se pueden determinar mediante un proceso de consenso entre los TEE 304a-d de KM.

En algunas realizaciones, los TEE 308a-d de KM pueden elegir, a través de un proceso de consenso, uno o más de los TEE 308a-d de KM para que actúen como el centro 310 de gestión de claves para generar y mantener claves de cifrado, y desplegar las claves de cifrado a los TEE confiables.

Haciendo referencia a la FIG. 7, la FIG. 7 es un diagrama que ilustra un ejemplo de una lógica 700 de MA de acuerdo con realizaciones de esta memoria descriptiva. Como se describió anteriormente, a alto nivel, un proceso de atestación mutua implica que un nodo que ejecuta un primer TEE realiza una atestación remota de un nodo que ejecuta un segundo TEE, después de lo cual el nodo que ejecuta el segundo TEE realiza una atestación remota del nodo que ejecuta el primer TEE. Una vez que ambos nodos se han verificado entre sí, los nodos pueden realizar un proceso de intercambio de claves para permitir comunicaciones seguras entre ellos.

Utilizando un proceso de atestación mutua entre TEE 308a de KM y TEE 308b de KM, por ejemplo, durante el proceso de atestación mutua, el TEE 308a de KM primero realiza una atestación remota del TEE 308b de KM. Durante el proceso de atestación remota, tanto el TEE 308a de KM como el TEE 308b de KM pueden derivar una clave compartida utilizando un protocolo de generación de claves, tal como un protocolo sigma. El TEE 308a de KM puede entonces

generar un número aleatorio utilizado solo una vez, calcular sus propios valores de resumen y los informes de SGX del TEE 308b de KM y luego los envía al TEE 308b de KM. El TEE 308b de KM puede entonces realizar una atestación remota del TEE 308a de KM y verificar las firmas de los informes resumidos. Si la verificación tiene éxito, se puede confirmar que el TEE 308b de KM se está comunicando con el TEE 308a de KM correcto. A continuación, el TEE 308b de KM genera una clave de sesión y envía tanto el número aleatorio utilizado solo una vez como la clave de sesión al TEE 308a de KM.

El TEE 308a de KM puede entonces realizar una comparación del número aleatorio utilizado solo una vez recibido con el enviado originalmente. Si coinciden, se puede confirmar que el TEE 308a de KM se está comunicando con el TEE 308b de KM correcto. Como tal, una MA se realiza con éxito. El TEE 308a de KM puede entonces comunicarse de forma segura con TEE 308b de KM utilizando la clave de sesión para el cifrado de datos. El MA entre otros TEE de KM se puede realizar de manera similar.

Bajo la lógica 700 de MA, uno cualquiera de los TEE 308a-d de KM realiza las MA con otros dos TEE 308a-d de KM para formar un "anillo" de autenticación de bucle cerrado. En algunos casos, un TEE de KM puede seleccionar los dos TEE de KM que están en estrecha proximidad geográfica o que tienen una alta eficiencia de comunicación para realizar las MA, siempre que las MA generales de los TEE 308a-d de KM se realicen en un circuito cerrado.

En el ejemplo ilustrado en la FIG. 7, el TEE 308a de KM realiza tanto el desafiador como el atestiguador en una MA con TEE 308b de KM, el TEE 308b de KM realiza tanto el desafiador como el atestiguador en una MA con TEE 308c de KM, el TEE 308c de KM realiza tanto el desafiador como el atestiguador en una MA con TEE 308d de KM, y el TEE 308d de KM realiza tanto el desafiador como el atestiguador en una MA con TEE 308a de KM. Dado que las MA se realizan para formar un bucle cerrado que involucra a todos los TEE 308a-d de KM, la identidad de cada uno de los TEE de KM se autentica sucesivamente y se forma una relación de confianza entre los TEE 308a-d de KM.

La FIG. 8 es un diagrama que ilustra un ejemplo de otra lógica 800 de MA de acuerdo con realizaciones de esta memoria descriptiva. En el ejemplo de la lógica 800 de MA, las MA se realizan de manera rotatoria. En otras palabras, cada uno de los TEE de KM realiza una MA una vez con cada uno de los otros TEE de KM en la red de cadena de bloques. Por ejemplo, además de realizar las MA bajo la lógica 700 de MA como se ha discutido en la descripción de la FIG. 7, el TEE 308a de KM realiza tanto el desafiador como el atestiguador en una MA con TEE 308c de KM, y el TEE 308b de KM realiza tanto el desafiador como el atestiguador en una MA con TEE 308d de KM.

Dado que las identidades de dos cualesquiera de los TEE de KM en la red de cadena de bloques se autentican mutuamente, la lógica 800 de MA puede ser más segura que la lógica 700 de MA. Por otro lado, dado que se realizan menos MA bajo la lógica 700 de MA, la lógica 700 de MA puede ser más eficiente en términos de velocidad de autenticación y consumo de recursos. La lógica 800 de MA puede ser más adecuada para redes de cadena de bloques con un número menor de nodos de consenso o requisito de seguridad más alto. La lógica de MA 700 puede ser más adecuada para redes de cadena de bloques con una mayor cantidad de nodos de consenso o requisito de seguridad más bajo.

Haciendo referencia de nuevo a la FIG. 3, la lógica 330 de servicio de contrato inteligente incluye una o más definiciones de contrato inteligente. Los nodos 304a-304d ejecutan operaciones particulares desde la lógica 330 de servicio de contrato inteligente (p. ej., a petición de un cliente, como se muestra en la FIG. 4). En algunas realizaciones, las definiciones de contrato inteligente en la lógica 330 de servicio de contrato inteligente incluyen instrucciones para ejecutar por los nodos de la red 302 de cadena de bloques. La lógica 330 de servicio de contrato inteligente puede incluir las definiciones de contrato inteligente almacenadas en una o más cadenas de bloques mantenidas por la red (no mostrada) 302 de cadena de bloques.

La FIG. 4 es un diagrama que ilustra un ejemplo de un sistema 400 de acuerdo con realizaciones de esta memoria descriptiva. Como se muestra, el sistema 400 incluye el nodo 304a (que incluye el TEE 306a de servicio y el TEE 308a de KM), y el centro 310 de gestión de claves descrito con respecto a la FIG. 3. El sistema 400 también incluye un cliente 480 acoplado comunicativamente al centro 310 de gestión de claves.

En operación, el sistema 400 puede ejecutar de forma segura instrucciones de contrato inteligente y producir resultados cifrados de la operación (p. ej., para la inclusión en una cadena de bloques). Como se discutió anteriormente, el centro 310 de gestión de claves puede realizar una atestación remota para autenticar la identidad del TEE 308a de KM antes de confiarle las claves de cifrado. Una vez autenticado el TEE 308 de KM, el centro 310 de gestión de claves puede proporcionar una clave 402 privada no sellada, una clave 404 raíz y una clave 406 privada de firma al TEE 308a de KM del nodo 304a. El centro 310 de gestión de claves también aloja una clave 414 pública sellada y una clave 416 pública de verificación. El centro 310 de gestión de claves proporciona estas claves a clientes autorizados para realizar el cifrado y descifrado de diversos datos asociados con el TEE 306a de servicio, como se describe a continuación.

Como se muestra, el centro 310 de gestión de claves proporciona la clave 414 pública sellada al cliente 480. En algunos casos, el centro 310 de gestión de claves autentica al cliente 480 y solo proporciona la clave 414 pública sellada si el cliente 480 está autorizado para acceder a ella. El centro 310 de gestión de claves puede consultar un recurso de permisos interno o externo para realizar esta determinación. La clave 414 pública sellada está asociada

con una clave 402 privada no sellada proporcionada al TEE 308a de KM. La clave 414 pública sellada y la clave 402 privada no sellada forman un par de claves, lo que significa que los datos cifrados con la clave 414 pública sellada se pueden descifrar utilizando la clave 402 privada no sellada.

El cliente 480 identifica una operación 450 de contrato solicitada, que es una operación de contrato inteligente a ser ejecutada por una máquina 460 virtual (VM) de Ethereum desplegada en el TEE 306a de servicio. En algunos casos, las operaciones 450 de contrato inteligente incluyen una o más instrucciones codificadas en un lenguaje de programación de contrato inteligente para la ejecución por una VM operable para ejecutar instrucciones en ese lenguaje. Las operaciones 450 de contrato inteligente pueden incluir un estado de ejecución para el contrato inteligente asociado con la operación 450 de contrato de solicitud. Durante la ejecución de un contrato inteligente, múltiples nodos de una red de cadena de bloques ejecutan cada una de las instrucciones del contrato inteligente de forma individual y producen un resultado que indica un estado de ejecución del contrato inteligente después de la finalización de la instrucción. El estado de ejecución puede incluir datos asociados con el contrato inteligente. Cada una de las instrucciones ejecutada del contrato puede cambiar el contenido de los datos (p. ej., para almacenar un valor a ser utilizado por una instrucción posterior en el contrato inteligente). Después de la ejecución de una instrucción del contrato inteligente, los nodos de la red de cadena de bloques llegan a un consenso sobre el nuevo estado de ejecución después de la ejecución de la instrucción. Este proceso de consenso se realiza para cada una de las instrucciones ejecutada en un contrato inteligente, lo que lleva a un consenso sobre la ruta de ejecución del contrato inteligente y, en última instancia, sobre el resultado final de la ejecución.

En 452, el cliente 480 codifica (o sella) la operación 450 de contrato solicitada en una envolvente 454 digital para la transmisión al TEE 306a de servicio ejecutado por el nodo 304a. Por ejemplo, el cliente 480 genera una clave 408 simétrica temporal y cifra la operación 450 de contrato solicitada utilizando la clave 408. El cliente 480 luego cifra la clave 408 simétrica temporal utilizando la clave 414 pública sellada y concatena la operación 450 de contrato cifrada y el clave 408 cifrada para producir la envolvente 454 digital.

El cliente 480 transmite la envolvente 454 digital al nodo 304a, donde se proporciona al TEE 306a de servicio. En algunos casos, el cliente 480 puede enviar la envolvente 454 digital a múltiples nodos 304a-d para solicitar el procesamiento de la operación 450 de contrato solicitada. En algunos casos, el cliente 480 puede enviar envolventes digitales creadas utilizando claves públicas selladas específicas para los nodos particulares. El cliente 480 también puede difundir la envolvente 454 digital a los nodos 304a-d en los casos en los que la misma clave 414 pública sellada y la clave 402 privada no sellada están asociadas con todos los nodos 304a-d.

El TEE 306a de servicio recibe la envolvente 454 digital del cliente 480 y recupera la operación 450 de contrato solicitada de la envolvente 454 digital. Como se muestra, el TEE 306a de servicio decodifica la envolvente 454 digital utilizando la clave 402 privada no sellada obtenida del TEE 308a de KM. En algunos casos, el TEE 306a de servicio descifra (abre) la clave 408 simétrica temporal utilizando la clave 402 privada no sellada (en 456), y luego descifra la operación 450 de contrato solicitada utilizando la clave 408 simétrica temporal (en 458).

El TEE 306a de servicio ejecuta entonces la operación 450 de contrato solicitada utilizando una VM 460 desplegada en el TEE 306a de servicio. En algunas realizaciones, la VM 460 puede ser una VM configurada para ejecutar instrucciones de un lenguaje de programación de contrato inteligente, tal como una VM de Ethereum u otro tipo de VM. En algunos casos, la VM 460 puede acceder a recursos externos al TEE 306a de servicio durante la ejecución de la operación 450, tales como, por ejemplo, servidores externos, una cadena de bloques, una base de datos u otros recursos indicados por la operación 450. En algunas realizaciones, el acceso a recursos externos se puede restringir o denegar, de modo que la totalidad de la ejecución de la operación depende únicamente de los datos almacenados en el TEE 306a de servicio (tal como el estado del contrato inteligente). Este tipo de restricción puede reducir aún más la posibilidad de alterar la ejecución de la operación 450.

La ejecución de la operación 450 por la VM 460 puede producir uno o más resultados. En algunos casos, los resultados pueden incluir un estado de ejecución del contrato inteligente después de ejecutar la operación 450, como se describe anteriormente. En 462, el resultado de la operación 450 de contrato inteligente se cifra por el TEE 306a de servicio utilizando una clave 412 de contrato. La clave 412 de contrato se deriva (en 410) de una clave 404 raíz en base a una función de derivación de claves (KDF). En algunos ejemplos, la KDF se puede realizar en base a algoritmos de resumen iterativos, tal como la función de derivación de clave de extracción y expansión basada en HMAC (HKDF) o la función pseudoaleatoria (PRF). La clave de contrato se puede proporcionar por el TEE 308a de KM al TEE 306a de servicio. En algunas realizaciones, la clave 404 raíz puede ser una clave de cifrado simétrica asociada con el nodo 304a. La clave 404 raíz también puede incluir una o más subclaves que pueden derivarse de la clave 404 raíz. La clave 412 de contrato puede ser una de estas subclaves. En algunos casos, la clave 404 raíz se puede utilizar para cifrar el resultado en 462.

Después de cifrar el resultado, el TEE 308a de servicio, en 464, firma el resultado cifrado utilizando una clave 406 privada de firma proporcionada por el TEE 308a de KM al TEE 306a de servicio, para producir un resultado 466 firmado. Esto puede permitir la verificación posterior del resultado firmado por un tercero (por ejemplo., un cliente), utilizando la clave 416 pública de verificación (correspondientemente emparejada con la clave 406 privada de firma) mantenida por el centro 310 de gestión de claves. En algunos casos, firmar el resultado cifrado por la clave 406 privada de firma

puede incluir cifrar el resultado cifrado junto con la clave 412 de contrato utilizada para cifrar el resultado. En tal caso, un tercero que tiene la clave 416 pública de verificación puede descifrar en la clave 412 de contrato primero, y utilizar además la clave 412 de contrato para descifrar el resultado.

En algunos casos, el TEE 306a de servicio puede almacenar el resultado 466 firmado en una cadena de bloques. Como se describió anteriormente, un tercero que tiene la clave 416 pública de verificación puede utilizar la clave para descifrar el resultado 466 con el fin de inspeccionar. Por ejemplo, el cliente 480 puede recuperar la clave 416 pública de verificación del centro 310 de gestión de claves (p. ej., sujeto a autenticación como se describió anteriormente), y puede acceder y descifrar el resultado 466 firmado utilizando la clave 416 pública de verificación. El cliente 480 puede luego solicitar que la siguiente operación en el contrato inteligente se ejecute por el TEE 306a de servicio, y puede incluir la siguiente operación solicitada y el estado de ejecución del contrato inteligente (del resultado 466 firmado descifrado) en la envolvente digital enviada al TEE 306a de servicio.

La FIG. 5 representa un ejemplo de un proceso que se puede ejecutar de acuerdo con realizaciones de esta memoria descriptiva. En 502, un nodo (p. ej., 304a) de cadena de bloques que participa en una red (p. ej., 302) de cadena de bloques establece una relación de confianza con una pluralidad de TEE de KM en una pluralidad de nodos de KM en base a realizar atestaciones mutuas con la pluralidad de TEE de KM, en donde el nodo de KM y la pluralidad de nodos de KM están en una cadena de bloques de consorcio.

En 504, el nodo de cadena de bloques inicia un proceso de consenso con la pluralidad de TEE de KM para llegar a un consenso sobre la provisión de una o más claves de cifrado a un TEE de servicio del nodo de KM.

En 506, el nodo cadena de bloques inicia un proceso de atestación local con un TEE de servicio en el nodo de KM.

En 508, el nodo de cadena de bloques determina que el proceso de atestación local tiene éxito.

En 510, el nodo de cadena de bloques proporciona una o más claves de cifrado al TEE que se ejecuta en el dispositivo informático.

En algunos casos, el nodo de cadena de bloques almacena las claves de cifrado en la cadena de bloques de consorcio, en donde las claves de cifrado almacenadas en la cadena de bloques de consorcio representan una versión de consenso de las claves de cifrado accesibles por todos los nodos en la cadena de bloques de consorcio.

En algunos casos, el TEE de KM es un primer TEE de KM, y el establecimiento de la relación de confianza incluye que el primer TEE de KM realice un proceso de atestación mutua con un segundo TEE de KM y un tercer TEE en la pluralidad de TEE de KM.

En algunos casos, el TEE de KM y la pluralidad de TEE de KM forman un conjunto de TEE de KM de la cadena de bloques de consorcio, y en donde el establecimiento de la relación de confianza incluye además que cualquiera de la pluralidad de TEE de KM realice un proceso de atestación mutua con dos del conjunto de los TEE de KM.

En algunos casos, el establecimiento de la relación de confianza incluye además que el TEE de KM realice una atestación mutua con cada uno de la pluralidad de TEE de KM.

En algunos casos, las claves de cifrado se almacenan en la cadena de bloques de consorcio en respuesta a que el TEE de KM y la pluralidad de TEE de KM realizan con éxito un proceso de consenso sobre las claves de cifrado.

En algunos casos, el proceso de consenso es un proceso de tolerancia práctica a fallas bizantinas (PBFT).

En algunos casos, el TEE de KM es un primer TEE de KM, las claves de cifrado incluyen una clave pública de TEE y una clave privada de TEE asociada con el TEE de servicio, y el primer TEE de KM o un segundo TEE de KM recupera la clave pública de TEE de la cadena de bloques de consorcio y proporciona la clave pública de TEE a un cliente en respuesta a una solicitud.

La FIG. 6 representa ejemplos de módulos de un aparato 600 de acuerdo con realizaciones de esta memoria descriptiva. El aparato 600 puede ser una realización de ejemplo de un nodo de cadena de bloques que se ejecuta dentro de una red de cadena de bloques. El aparato 600 puede corresponder a las realizaciones descritas anteriormente, y el aparato 600 incluye lo siguiente: un módulo 602 de establecimiento que establece una relación de confianza con una pluralidad de TEE de KM en una pluralidad de nodos de KM en base a realizar atestaciones mutuas con la pluralidad de TEE de KM, en donde el nodo de KM y la pluralidad de nodos de KM están en una cadena de bloques de consorcio. Un módulo 604 de iniciación que inicia un proceso de consenso con la pluralidad de TEE de KM para llegar a un consenso sobre la provisión de una o más claves de cifrado a un TEE de servicio del nodo de KM e inicia un proceso de atestación local con un TEE de servicio en el nodo de KM. Un módulo 606 de determinación que determina que el proceso de atestación local tiene éxito; y un módulo 608 de transmisión que proporciona una o más claves de cifrado al TEE que se ejecuta en el dispositivo informático.

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

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

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

Haciendo referencia de nuevo a la FIG. 6, se puede interpretar como una ilustración de un módulo funcional interno y una estructura de un nodo de cadena de bloques que se ejecuta dentro de una red de cadena de bloques y funciona como un cuerpo de ejecución. En esencia, un organismo de ejecución puede ser un dispositivo electrónico, y el dispositivo electrónico incluye lo siguiente: uno o más procesadores; y una memoria configurada para almacenar una instrucción ejecutable del uno o más procesadores.

Las técnicas descritas en esta memoria descriptiva producen uno o más efectos técnicos. En algunas realizaciones, las técnicas descritas permiten que múltiples nodos funcionen como un centro de gestión de claves (KMC) distribuido para autorizar y configurar entornos de ejecución confiables en otros dispositivos informáticos con claves de cifrado. En algunos casos, las claves se almacenan en una cadena de bloques, lo que permite que cualquiera de los múltiples nodos atienda las solicitudes de claves de cifrado recibidas de otros dispositivos informáticos, incluso si las claves solicitadas se configuraron y almacenaron por un nodo diferente del nodo que recibe la solicitud. En algunos ejemplos, las técnicas también proporcionan una resistencia operativa adicional contra las interrupciones del sistema, ya que la falla de uno de los múltiples nodos no causará una interrupción en el servicio de gestión de claves (a diferencia de una solución centralizada). En algunas realizaciones, las técnicas pueden proporcionar una mayor seguridad, ya que un atacante tendría que tomar el control de todos los nodos de gestión de claves para comprometer el sistema, debido a los procesos de consenso asociados con el almacenamiento de las claves de cifrado en la cadena de bloques.

Las realizaciones descritas de la materia objeto pueden incluir una o más características, solas o en combinación. Una realización incluye un método implementado por computadora que comprende las acciones de recibir, por un nodo de cadena de bloques que participa en una red de cadena de bloques, una solicitud cifrada para ejecutar una operación de contrato inteligente de un cliente; descifrar, por el nodo cadena de bloques en un TEE alojado por el nodo cadena de bloques, la solicitud cifrada con una primera clave privada asociada con el TEE para producir una operación de contrato inteligente solicitada, en donde la primera clave privada corresponde a una clave pública asociada con el TEE que se utilizó para cifrar la solicitud cifrada; ejecutar, por el nodo cadena de bloques en el TEE, la operación de contrato inteligente solicitada para producir un resultado de contrato inteligente; cifrar, mediante el nodo de cadena de bloques en el TEE, el resultado del contrato inteligente con una clave simétrica asociada con el TEE para producir un resultado cifrado; firmar, por el nodo cadena de bloques en el TEE, el resultado cifrado utilizando una segunda clave privada asociada con el TEE para producir un resultado cifrado firmado, en donde la segunda clave privada es diferente de la primera clave privada; y almacenar, por el nodo de cadena de bloques, el resultado cifrado firmado en una cadena de bloques mantenida por la red de cadena de bloques.

Las realizaciones descritas anteriores y otras pueden cada una, opcionalmente, incluir una o más de las siguientes características:

Una primera característica, combinable con cualquiera de las siguientes características, especifica que el nodo de cadena de bloques almacena las claves de cifrado en la cadena de bloques de consorcio, en donde las claves de cifrado almacenadas en la cadena de bloques de consorcio representan una versión de consenso de las claves de cifrado accesibles por todos los nodos de la cadena de bloques de consorcio.

Una segunda característica, combinable con cualquiera de las características anteriores o siguientes, especifica que el TEE de KM es un primer TEE de KM, y el establecimiento de la relación de confianza incluye que el primer TEE de KM realice un proceso de atestación mutua con un segundo TEE de KM y un tercer TEE en la pluralidad de TEE de KM.

Una tercera característica, combinable con cualquiera de las características anteriores o siguientes, incluye que el TEE de KM y la pluralidad de TEE de KM forman un conjunto de TEE de KM de la cadena de bloques de consorcio, y en donde establecer la relación de confianza incluye además que cualquiera de la pluralidad de TEE de KM realice un proceso de atestación mutua con dos del conjunto de los TEE de KM.

Una cuarta característica, combinable con cualquiera de las características anteriores o siguientes, especifica que el establecimiento de la relación de confianza incluye además que el TEE de KM realice una atestación mutua con cada uno de la pluralidad de TEE de KM.

Una quinta característica, combinable con cualquiera de las características anteriores o siguientes, especifica que las claves de cifrado se almacenan en la cadena de bloques de consorcio en respuesta a que el TEE de KM y la pluralidad de TEE de KM realicen con éxito un proceso de consenso sobre las claves de cifrado.

Una sexta característica, combinable con cualquiera de las características anteriores o siguientes, especifica que el proceso de consenso es un proceso de tolerancia práctica a fallas bizantinas (PBFT).

Una séptima característica, combinable con cualquiera de las características anteriores o siguientes, especifica que el TEE de KM es un primer TEE de KM, las claves de cifrado incluyen una clave pública de TEE y una clave privada de TEE asociada con el TEE de servicio, y el primer TEE de KM o un segundo TEE de KM recupera la clave pública de TEE de la cadena de bloques de consorcio y proporciona la clave pública de TEE a un cliente en respuesta a una solicitud.

Las realizaciones de la materia objeto y las acciones y operaciones descritas en esta memoria descriptiva se pueden implementar en circuitería electrónica digital, en software o firmware informático incorporado de manera tangible, en hardware informático, incluidas las estructuras descritas en esta memoria descriptiva y sus equivalentes estructurales, o en combinaciones de uno o más de ellos. Las realizaciones de la materia objeto descrita en esta memoria descriptiva se pueden implementar como uno o más programas informáticos, p. ej., uno o más módulos de instrucciones de programa informático, codificados en un soporte de programa informático, para la ejecución por , o para controlar la operación de, aparato de procesamiento de datos. Por ejemplo, un soporte de programa informático puede incluir uno o más medios de almacenamiento legibles por computadora que tienen instrucciones codificadas o almacenadas en los mismos. El soporte puede ser un medio legible por computadora tangible no transitorio, tal como un disco magnético, magneto óptico u óptico, una unidad de estado sólido, una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM) u otros tipos de medios. Alternativa o adicionalmente, el soporte puede ser una señal propagada generada artificialmente, p. ej., una señal eléctrica, óptica o electromagnética generada por una máquina que se genera para codificar información para su transmisión a un aparato receptor adecuado para su ejecución por un aparato de procesamiento de datos. El medio de almacenamiento informático puede ser, o ser parte de, un dispositivo de almacenamiento legible por máquina, un sustrato de almacenamiento legible por máquina, un dispositivo de memoria de acceso aleatorio o en serie, o una combinación de uno o más de ellos. Un medio de almacenamiento informático no es una señal propagada.

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

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

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

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

pila de protocolo, un sistema de gestión de bases de datos, un sistema operativo o una combinación de uno o más de ellos.

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

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

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

Los componentes se pueden "acoplar" entre sí estando conectados conmutativamente, tal como eléctrica u ópticamente, entre sí, ya sea directamente o a través de uno o más componentes intermedios. Los componentes también se pueden "acoplar" entre sí si uno de los componentes está integrado en el otro. Por ejemplo, un componente de almacenamiento que está integrado en un procesador (p. ej., un componente de caché L2) está "acoplado" al procesador.

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

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

Si bien esta memoria descriptiva contiene muchos detalles de realización específicos, estos no deben interpretarse como limitaciones en el alcance de lo que se reivindica, que se define en las propias reivindicaciones, sino más bien como descripciones de características que pueden ser específicas de realizaciones particulares. Ciertas características que se describen en esta memoria descriptiva en el contexto de realizaciones separadas también se pueden realizar en combinación en una única realización. A la inversa, diversas características que se describen en

el contexto de una única realización también se pueden realizar en múltiples realizaciones por separado o en cualquier subcombinación adecuada. Además, aunque las características pueden describirse anteriormente como que actúan en ciertas combinaciones e incluso inicialmente reivindicarse como tales, una o más características de una combinación reivindicada pueden en algunos casos eliminarse de la combinación, y la reivindicación puede estar dirigida a una subcombinación o variación de una subcombinación.

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

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

REIVINDICACIONES

1. Un método (500) implementado por computadora para verificar la autenticidad de entornos de ejecución confiables, TEE, el método que comprende:
establecer (502), mediante un TEE de gestión de claves, KM, de un nodo de KM, una relación de confianza con una pluralidad de TEE de KM en una pluralidad de nodos de KM en base a realizar atestaciones mutuas con la pluralidad de TEE de KM, en donde el nodo de KM y la pluralidad de nodos de KM están en una cadena de bloques de consorcio;
iniciar (504), mediante el TEE de KM, un proceso de consenso con la pluralidad de TEE de KM para llegar a un consenso sobre la provisión de una o más claves de cifrado a un TEE de servicio del nodo de KM;
en respuesta a alcanzar el consenso con la pluralidad de TEE de KM, iniciar (506), mediante el TEE de KM, un proceso de atestación local con un TEE de servicio en el nodo de KM;
determinar (508), por el TEE de KM, que el proceso de atestación local tiene éxito; y
en respuesta a determinar que el proceso de atestación local tiene éxito, proporcionar (510), mediante el TEE de KM, una o más claves de cifrado al TEE que se ejecuta en el dispositivo informático.

2. El método implementado por computadora de la reivindicación 1, que comprende además:
almacenar, por el nodo de KM, las claves de cifrado en la cadena de bloques de consorcio, en donde las claves de cifrado almacenadas en la cadena de bloques de consorcio representan una versión de consenso de las claves de cifrado accesibles por todos los nodos en la cadena de bloques de consorcio.

3. El método implementado por computadora de una cualquiera de las reivindicaciones anteriores, en donde el TEE de KM es un primer TEE de KM y en donde el establecimiento de la relación de confianza incluye que el primer TEE de KM realice un proceso de atestación mutua con un segundo TEE de KM y un tercer TEE en la pluralidad de TEE de KM.

4. El método implementado por computadora de una cualquiera de las reivindicaciones anteriores, en donde el TEE de KM y la pluralidad de TEE de KM forman un conjunto de TEE de KM de la cadena de bloques de consorcio y en donde el establecimiento de la relación de confianza incluye además que cualquiera de la pluralidad de TEE de KM realice un proceso de atestación mutua con dos del conjunto de los TEE de KM.

5. El método implementado por computadora de una cualquiera de las reivindicaciones 1, 2 o 3, en donde establecer la relación de confianza incluye además que el TEE de KM realice una atestación mutua con cada uno de la pluralidad de TEE de KM.

6. El método implementado por computadora de una cualquiera de las reivindicaciones anteriores, en donde las claves de cifrado se almacenan en la cadena de bloques de consorcio en respuesta a que el TEE de KM y la pluralidad de TEE de KM realicen con éxito un proceso de consenso sobre las claves de cifrado.

7. El método implementado por computadora de una cualquiera de las reivindicaciones anteriores, en donde el proceso de consenso es un proceso de tolerancia práctica a fallas bizantinas, PBFT.

8. El método implementado por computadora de una cualquiera de las reivindicaciones anteriores, en donde el TEE de KM es un primer TEE de KM, las claves de cifrado incluyen una clave pública de TEE y una clave privada de TEE asociadas con el TEE de servicio y en donde el primer TEE de KM o un segundo TEE de KM recupera la clave pública de TEE de la cadena de bloques de consorcio y proporciona la clave pública de TEE a un cliente en respuesta a una solicitud.

9. Un aparato para verificar la autenticidad de entornos de ejecución confiables, TEE, el aparato que comprende una pluralidad de módulos para realizar el método de una cualquiera de las reivindicaciones 1-8.

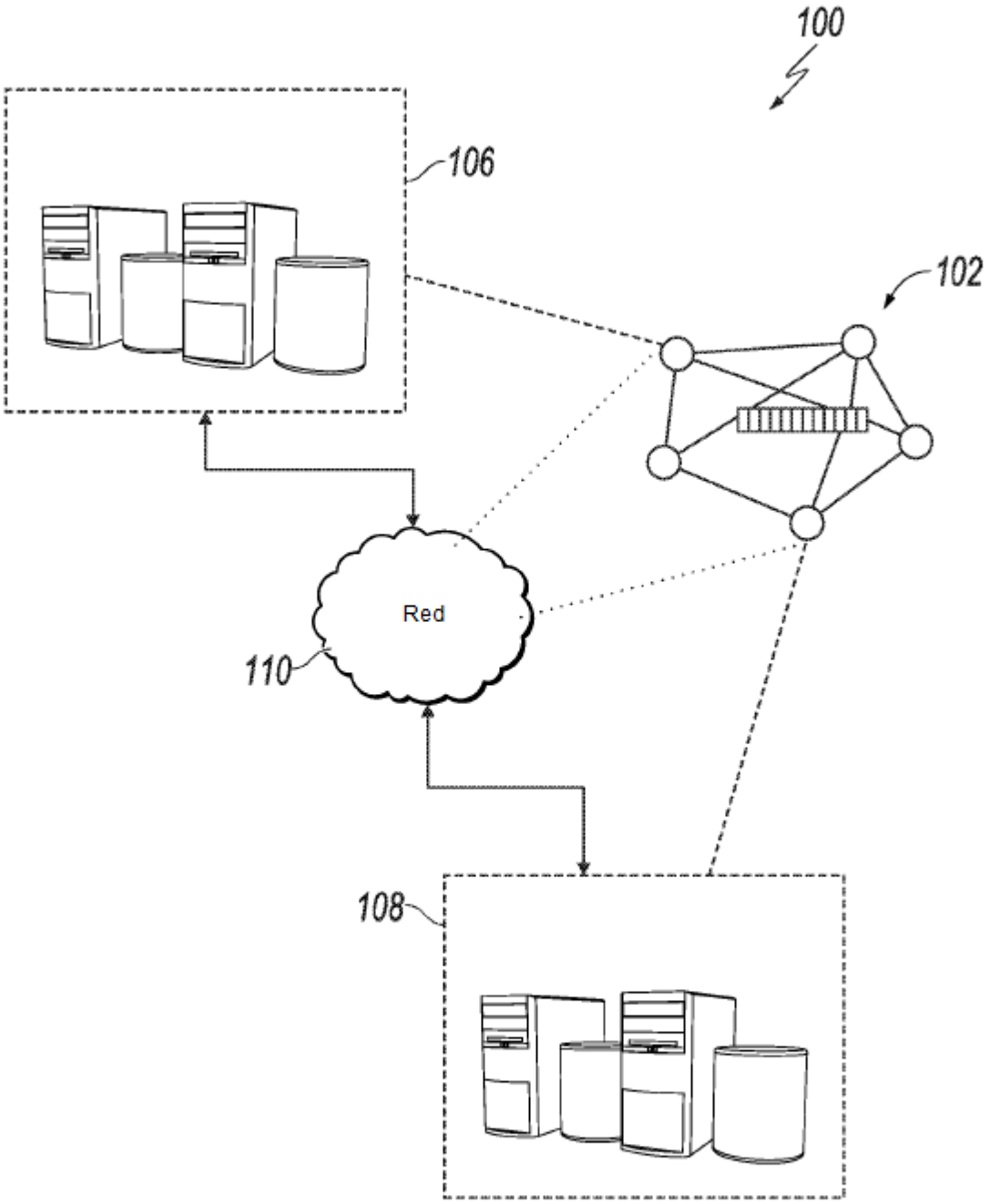

FIG. 1

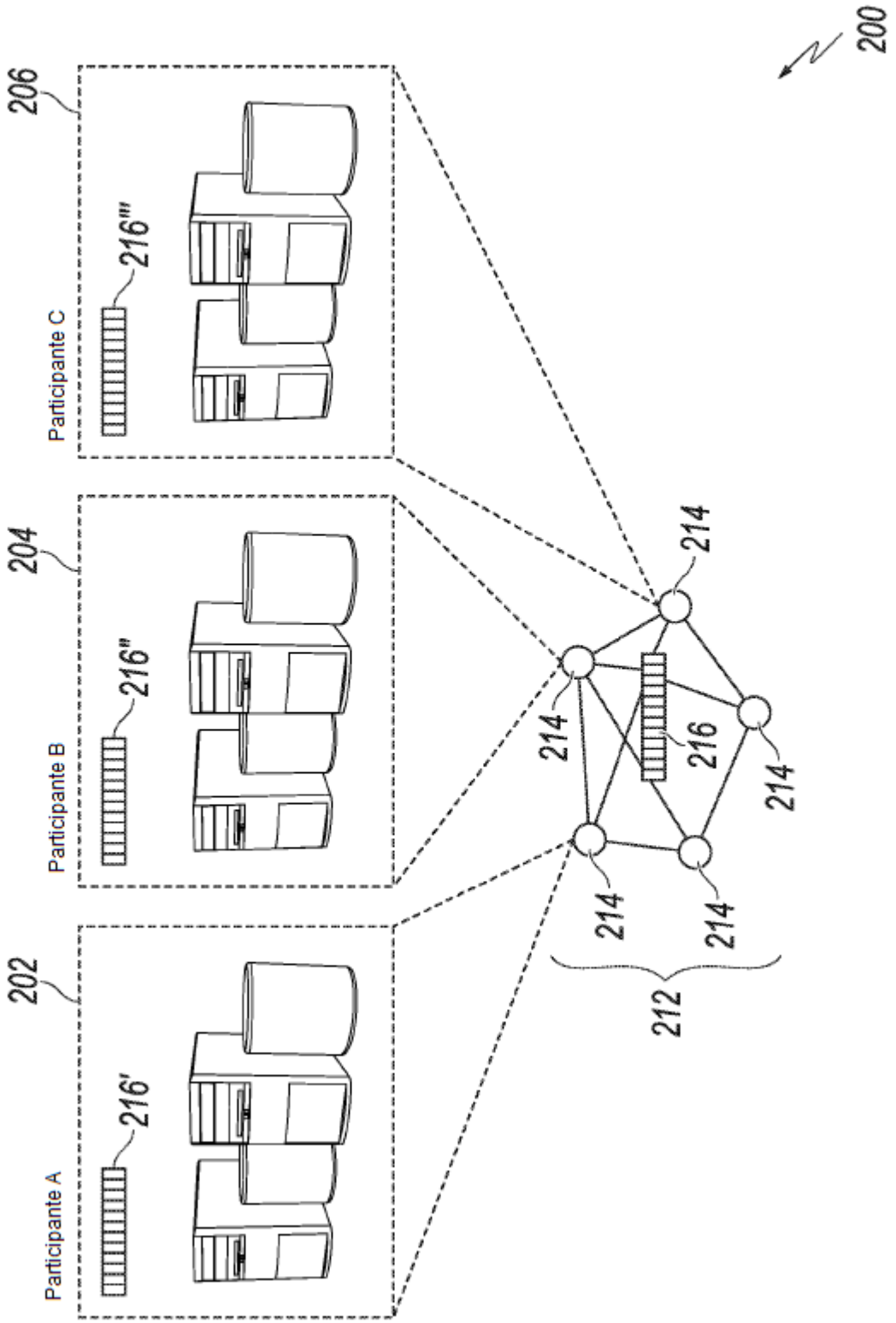
200
206
Participante C
216'''
204
Participante B
216''
202
Participante A
216'
214
214
214
214
214
216
212

FIG. 2

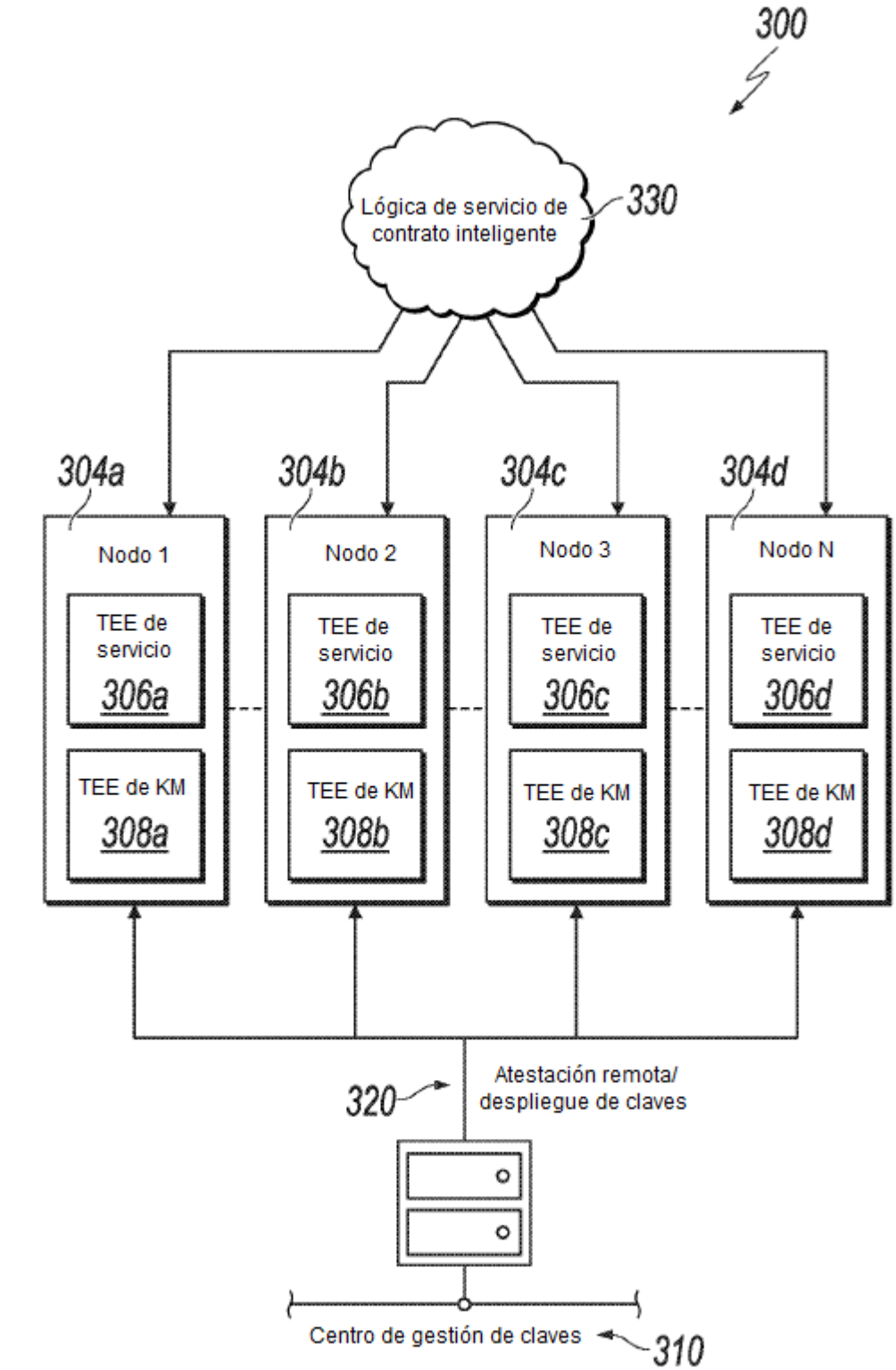
300
Lógica de servicio de contrato inteligente
330
304a
304b
304c
304d
Nodo 1
Nodo 2
Nodo 3
Nodo N
TEE de servicio
306a
TEE de servicio
306b
TEE de servicio
306c
TEE de servicio
306d
TEE de KM
308a
TEE de KM
308b
TEE de KM
308c
TEE de KM
308d
320
Atestación remota/ despliegue de claves
Centro de gestión de claves
310

FIG. 3

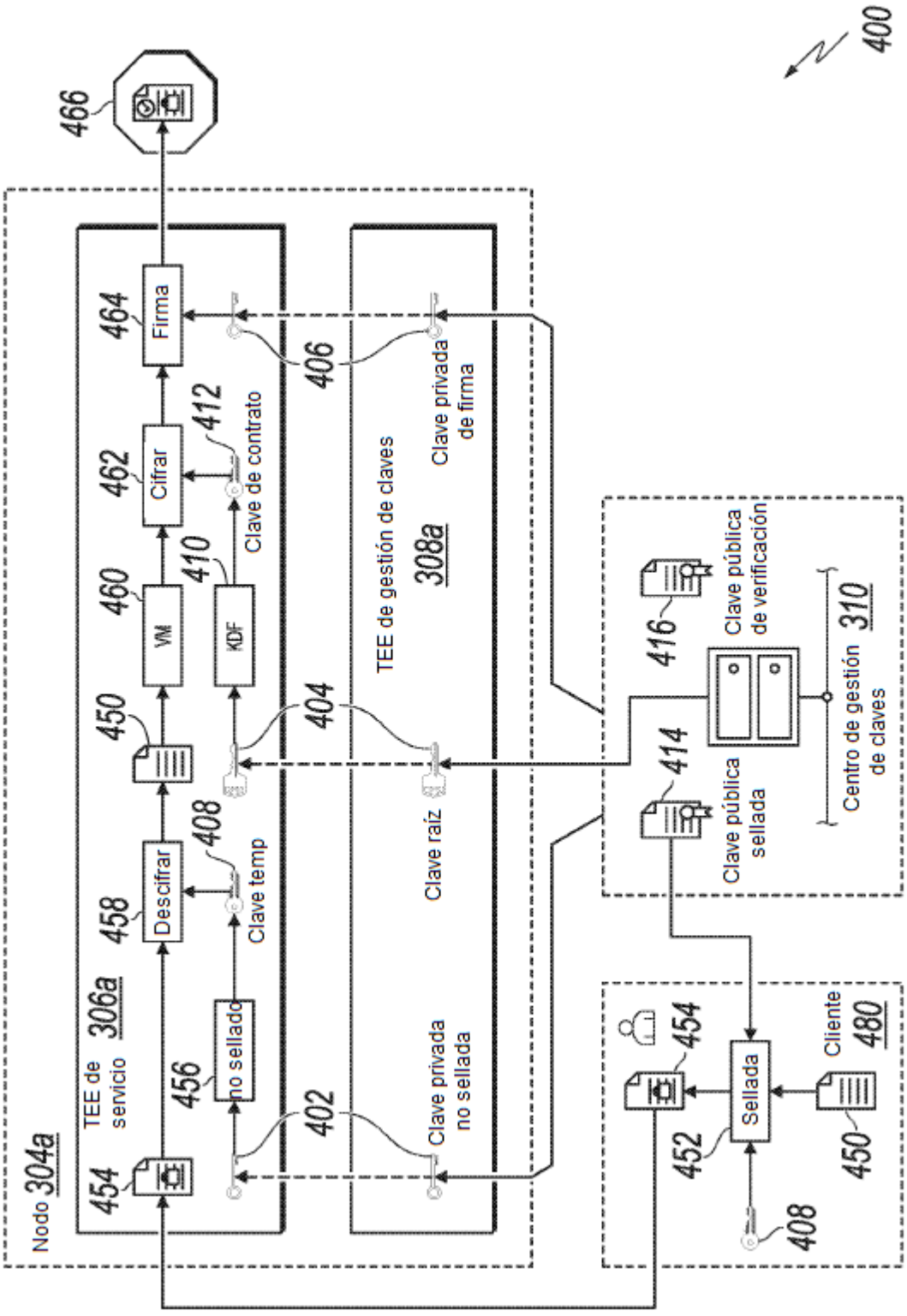
400
466
464
Firma
462
Cifrar
460
VM
450
458
Descifrar
456
no sellado
454
Nodo 304a
TEE de servicio 306a
412
Clave de contrato
410
KDF
408
Clave temp
402
Clave privada no sellada
404
Clave raíz
406
Clave privada de firma
TEE de gestión de claves 308a
416
Clave pública de verificación
414
Clave pública sellada
310
Centro de gestión de claves
454
452
Sellada
408
Cliente 480
450

FIG. 4

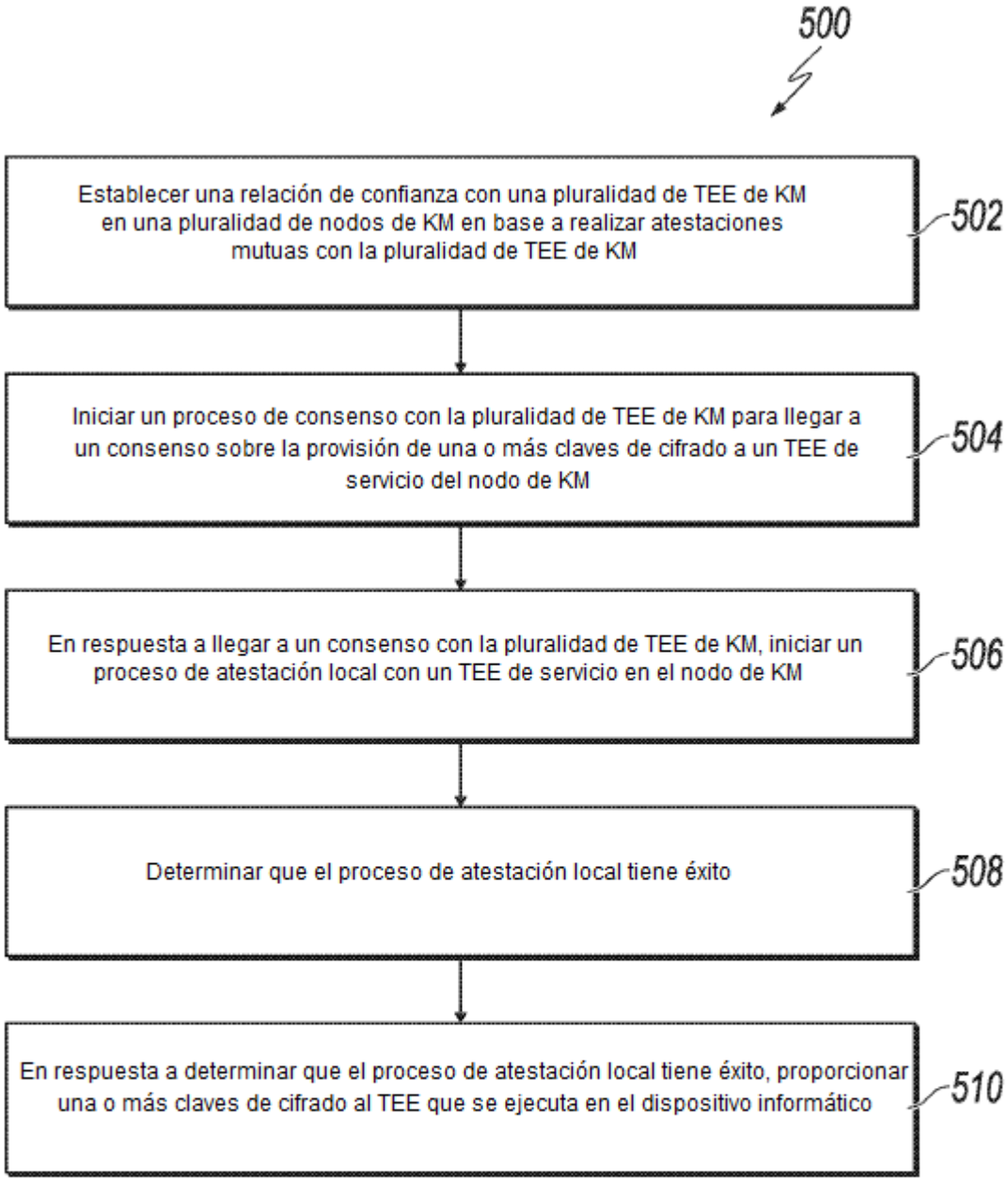
500
Establecer una relación de confianza con una pluralidad de TEE de KM en una pluralidad de nodos de KM en base a realizar atestaciones mutuas con la pluralidad de TEE de KM
502
Iniciar un proceso de consenso con la pluralidad de TEE de KM para llegar a un consenso sobre la provisión de una o más claves de cifrado a un TEE de servicio del nodo de KM
504
En respuesta a llegar a un consenso con la pluralidad de TEE de KM, iniciar un proceso de atestación local con un TEE de servicio en el nodo de KM
506
Determinar que el proceso de atestación local tiene éxito
508
En respuesta a determinar que el proceso de atestación local tiene éxito, proporcionar una o más claves de cifrado al TEE que se ejecuta en el dispositivo informático
510

FIG. 5

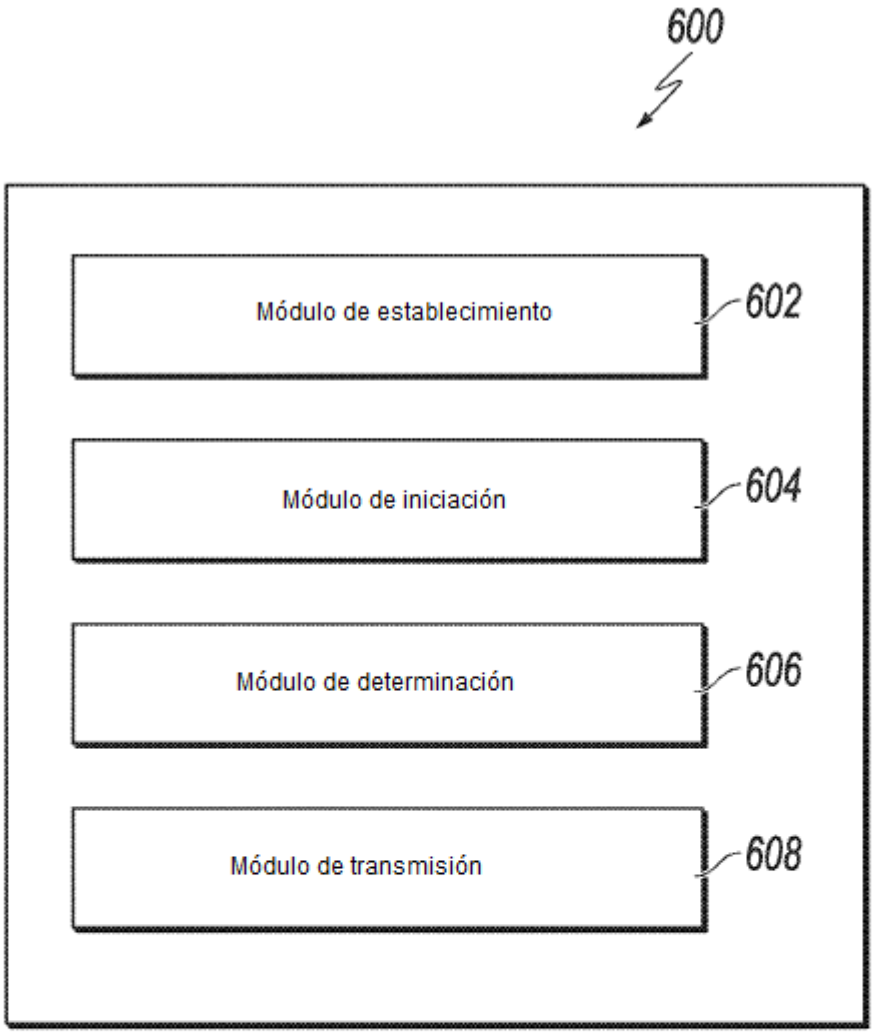
600
Módulo de establecimiento
602
Módulo de iniciación
604
Módulo de determinación
606
Módulo de transmisión
608

FIG. 6

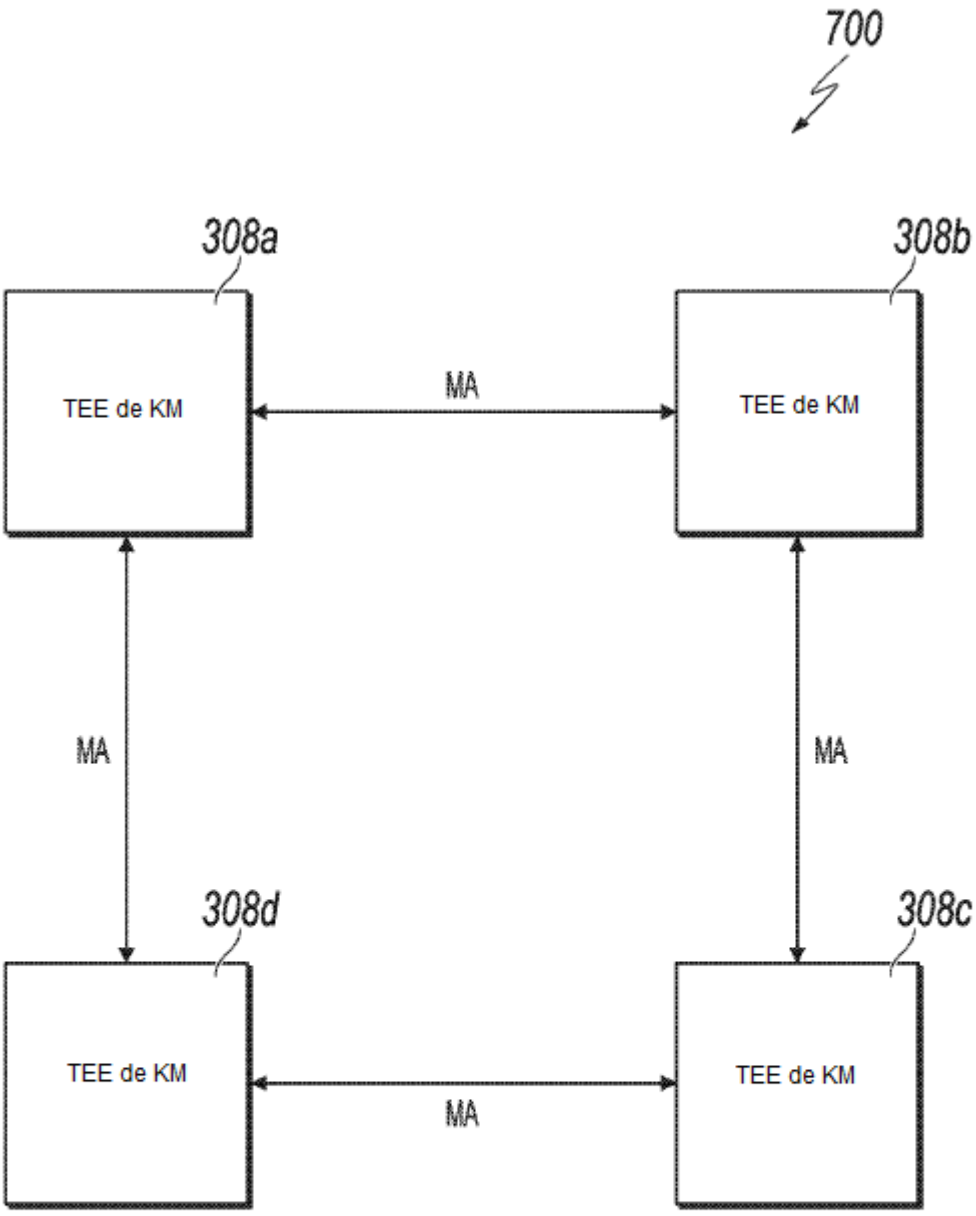
700
308a
308b
TEE de KM
MA
TEE de KM
MA
MA
308d
308c
TEE de KM
MA
TEE de KM

FIG. 7

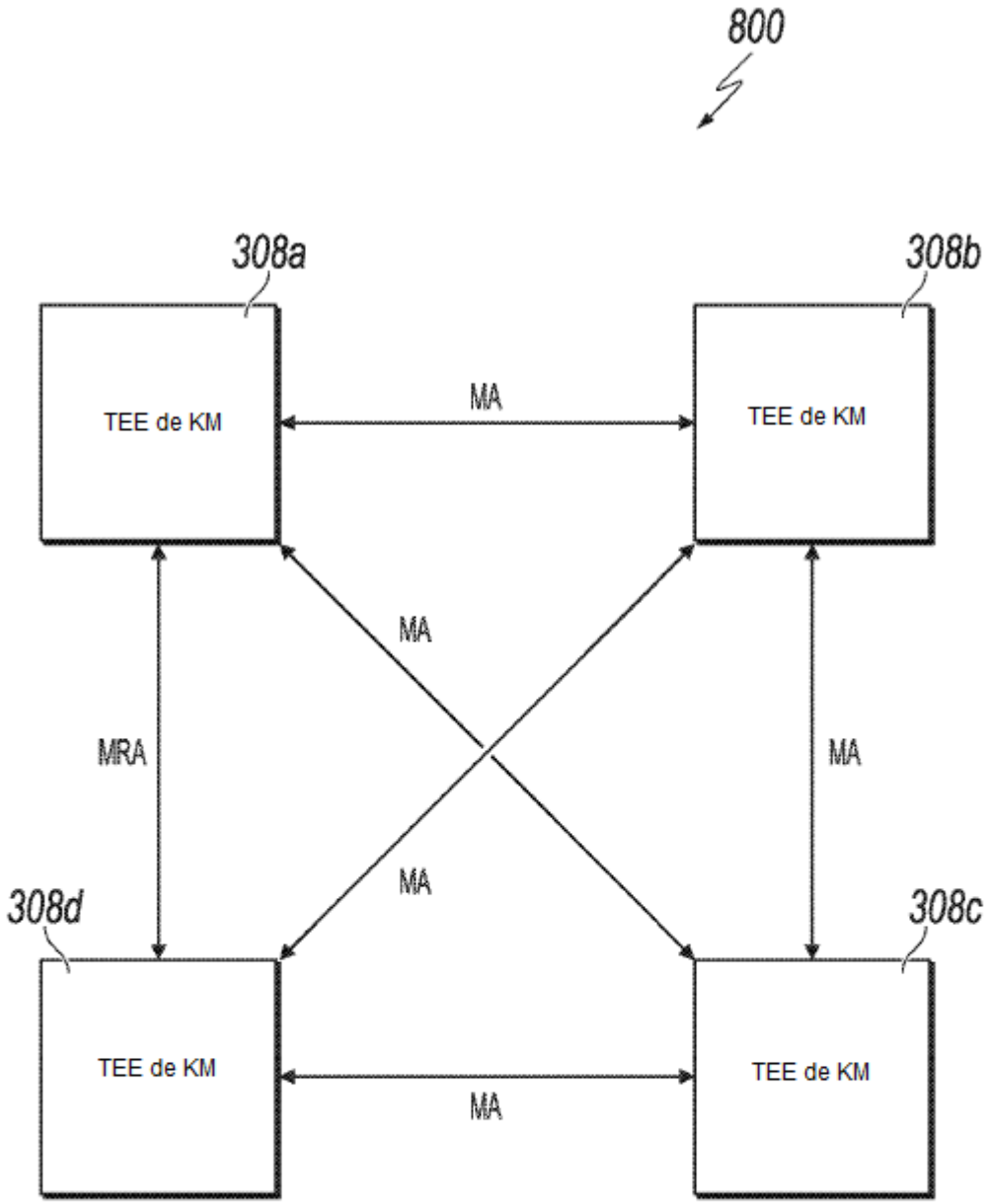
800
308a
308b
TEE de KM
TEE de KM
MA
MA
MRA
MA
MA
308d
308c
TEE de KM
TEE de KM
MA

FIG. 8