SISTEMA Y MÉTODO PARA LA VERIFICACIÓN DE LA AUTENTICIDAD DE LA INFORMACIÓN DE DOCUMENTOS

CAMPO DE LA INVENCIÓN

La presente invención se refiere a la verificación de la autenticidad de la información de documentos y en particular, pero no completamente necesario, a un sistema y método para la verificación de la autenticidad de la información de documentos para aplicaciones que incluyen verificar la autenticidad de la información de las declaraciones de logro de la documentación de cursos emitida por organizaciones de formación registradas, la verificación de documentos de viaje y otros documentos sensibles que requieren la verificación de autenticidad tales como los documentos emitidos por bufetes de abogados, firmas contables, instituciones gubernamentales y similares.

Además, las técnicas de verificación de autenticidad descritas en la presente descripción pueden aplicarse de forma general para diversos medios de documentos que incluyen en formato de copia dura (es decir, papel, documento de viaje de tarjeta inteligente) y copia digital (es decir, formatos electrónicos que incluyen en formato PDF que incluyen almacenarse dentro de repositorios de documentos).

ANTECEDENTES Y SUMARIO DE LA INVENCIÓN

La verificación de la autenticidad de documentos es deseable para aplicaciones que incluyen, por ejemplo, la verificación de la autenticidad de información en documentación legal, documentación de identidad personal, documentación de acreditación, documentación de acceso y similares.

Los problemas con estos documentos incluyen que la información contenida en los mismos puede modificarse en donde, por ejemplo, las acreditaciones se reclaman falsamente, los documentos se falsifican y similares.

D1: US 2011/0161674 A1 (MING), 30 de junio de 2011, busca tratar este problema mediante la descripción de un método para generar un documento de autoautenticación en donde la información de autenticación para el documento se codifica en un código de barras que se imprime en el documento. Una almohadilla se calcula a partir de la información de autenticación y se transmite a un servidor para almacenarse. Cuando se autentica una copia escaneada del documento, se lee el código de barras para extraer la información de autenticación. Una almohadilla objetivo se calcula a partir de la información de autenticación extraída y se transmite al servidor para la verificación. El servidor compara la almohadilla objetivo con la almohadilla almacenada previamente. Si no son la misma, el código de barras se ha alterado. Si son la misma, la información de autenticación extraída se usa para autenticar la copia escaneada. Una ID de documento puede generarse y transmitirse al servidor, y usarse por el servidor para indexar o buscar la almohadilla almacenada.

Sin embargo, el D1 sufre de la desventaja y de que el servidor puede comprometerse y la almohadilla almacenada en el mismo modificarse para coincidir con un documento alterado.

Como tal, el D1 no es adecuado para las aplicaciones que requieren exigencia de alta seguridad tal como para la utilización de tarjetas de embarque, documentación de identificación personal y similares.

Como tal, la presente invención utiliza, en una modalidad preferida, una cadena de bloques basada en escritura en clave distribuida para almacenar los registros de verificación de documentos de una manera que no puede alterarse.

Ahora, D2: "What is proof of existence?" [recuperado de internet el 20 de abril de 2016] <URL: https://web.archive.org/web/20151222163927/https://proofofexistence.com/about> publicado el 22 diciembre de 2015 de acuerdo con Wayback Machine D2 describe una cadena de bloques para almacenar una prueba de existencia de documentos distribuida en línea por medio del almacenamiento de compendios criptográficos individuales de los documentos respectivos en la cadena de bloques.

D2 crea una almohadilla de un documento electrónico (tal como un PDF) y almacena la almohadilla como una transacción especial de bitcoin que codifica/contiene la almohadilla a través de una escritura OP_RETURN. Este es un código operacional de programación de bitcoin que marca la salida de la transacción como que probablemente no se gasta y permite la inserción de una pequeña cantidad de datos, que en este caso es la almohadilla del documento, más un marcador para identificar todas las transacciones de D2.

Sin embargo, D2 no se dirige al problema de verificar la autenticidad de la información en un documento sino más bien a proporcionar que un documento particular existe en un formato electrónico particular en un momento particular.

Como tal, D2 no puede usarse para detectar si un documento se ha falsificado.

Además, D2 crea una almohadilla del archivo completo del documento electrónico y por lo tanto, no puede usarse para documentos en copia dura en donde la impresión pequeña, el escaneo, las anomalías que aparecen en las fotocopias generarían una almohadilla completamente diferente mediante el uso del sistema de D2 y por lo tanto, la información del documento contenida en el mismo no podría verificarse.

Como tal, en una modalidad preferida, la presente invención utiliza los metadatos del contenido del documento (almacenados mediante el uso de una almohadilla de metadatos, contrariamente a la almohadilla del documento de D1) como la base para la verificación y por lo tanto, pueden utilizarse para documentos en copia dura.

Además, D1 y D2 son deficientes en que la información del documento no puede actualizarse con el documento que permanece verificable.

Por ejemplo, mediante el uso de D2, se crearía una primera transacción de bitcoin para un documento original, y si el documento original estuviera actualizado, se crearía una segunda transacción de bitcoin para el documento actualizado.

Sin embargo, mediante el uso de D2, tanto el documento original como el documento alterado parecerían válidos, a pesar de que el documento original se haya suplantado.

Al contrario, en una modalidad, la presente invención utiliza transacciones de actualización de la cadena de bloques con el fin de actualizar de esta manera los campos de contenido del documento, durante la etapa de verificación de documentos, la cadena de bloques

puede inspeccionarse en orden cronológico inverso para detectar si un documento (o campos específicos de información del contenido del documento) se ha suplantado o no.

Además, tanto D1 como D2 son deficientes en que la verificación no puede ser durante un período predeterminado.

Al contrario, la presente invención, de acuerdo con una modalidad, crea transacciones de cadenas de bloques que especifican un período de validez.

Además, tanto D1 como D2 son deficientes en que un documento no puede revocarse.

Al contrario, la presente invención, de acuerdo con una modalidad, utiliza transacciones de cadenas de bloques del tipo de revocación de manera que la revocación de la autenticidad de un documento puede detectarse por una transacción del tipo de revocación posterior en el tiempo a una transacción de verificación anterior.

Además, D1 y D2 son deficientes en que la información verificada no puede mostrarse en colaboración con el documento para la comparación visual.

Al contrario, la presente invención, de acuerdo con una modalidad, almacena los metadatos, tal como en los datos legibles por computadora (es decir, el código de barras en 2D) dentro del documento en sí o dentro de la cadena de bloques de manera que la información puede extraerse posteriormente y mostrarse al usuario.

Debe entenderse que, si alguna información de la técnica anterior se referencia en la presente descripción, tal referencia no constituye una admisión de que la información forma parte del conocimiento general común en la técnica, en Australia o cualquier otro país.

Como tal, con lo anterior en mente, de acuerdo con una modalidad, se proporciona un método para la verificación de la autenticidad de la información de documentos, el método que comprende: una etapa de creación de registros de verificación que comprende: recibir los metadatos del contenido del documento desde un documento; generar una almohadilla de metadatos mediante el uso de los metadatos del contenido del documento; crear una transacción de la cadena de bloques que comprende la almohadilla de metadatos; y generar datos legibles por computadora que codifican la almohadilla de metadatos; actualizar el documento con los datos legibles por computadora; una etapa de verificación de documentos que comprende: recibir el documento; extraer la almohadilla de metadatos a partir de los datos legibles por computadora; e identificar la almohadilla de metadatos dentro de las transacciones de cadenas de bloques para verificar la autenticidad de los metadatos del documento.

Como puede apreciarse, D1 o D2 no describen la creación de una almohadilla de metadatos para la información de documentos de un documento, la creación de una transacción de la cadena de bloques asociada y la actualización del documento con datos legibles por computadora (es decir, código de barras en 2D) con la almohadilla de metadatos.

Los datos legibles por computadora pueden ser un código de barras.

El código de barras puede ser un código de barras de dos dimensiones.

La etapa del registro de verificación puede comprender además firmar el documento con una clave privada asociada con un servidor de verificación de documentos.

El método puede comprender además almacenar los metadatos del contenido del documento de manera que la etapa de verificación de documentos puede comprender además recuperar los metadatos del contenido del documento y mostrar los metadatos del contenido del documento.

Almacenar los metadatos del contenido del documento puede comprender codificar los metadatos dentro de los datos legibles por computadora.

Almacenar los metadatos del contenido del documento puede comprender codificar los metadatos dentro de la transacción de la cadena de bloques.

La etapa de creación de registros de verificación puede comprender además la identificación de los metadatos del contenido del documento a partir del documento.

La identificación de los metadatos del contenido del documento puede comprender el reconocimiento óptico de caracteres.

La identificación de los metadatos del contenido del documento puede comprender la realización de consultas de búsqueda de

cadenas contra el texto extraído mediante el uso del reconocimiento óptico de caracteres.

La identificación de los metadatos del contenido del documento puede comprender el aislamiento del texto dentro de al menos una región del documento definida por el usuario.

El método puede comprender además una etapa de actualización del contenido del documento que comprende: recibir los metadatos del contenido del documento actualizado para el documento; generar una nueva almohadilla de metadatos mediante el uso de los metadatos del documento actualizado; crear una transacción de la cadena de bloques adicional que comprende la nueva almohadilla de metadatos.

La etapa de verificación de documentos puede comprender: identificar dos o más transacciones de cadenas de bloques asociadas con el documento.

La etapa de verificación de documentos puede comprender además identificar que los metadatos del contenido del documento pueden suplantarse por los metadatos del contenido del documento actualizado.

El método puede comprender además identificar que parte del documento puede suplantarse.

El método puede comprender además una etapa de revocación de la verificación de documentos que comprende: crear una transacción de la cadena de bloques de revocación de manera que, durante la etapa de verificación de documentos, el método puede

comprender además: identificar la transacción de la cadena de bloques de revocación posterior en el tiempo a la transacción de la cadena de bloques para fallar en la verificación de la autenticidad de la información del documento.

La transacción de la cadena de bloques especifica además un período de validez, de manera que, durante la etapa de verificación de documentos, el método puede comprender además fallar en la verificación del documento si el período de validez ha expirado.

El método puede comprender además crear una transacción de la cadena de bloques de renovación del período de validez que comprende un período de validez adicional de manera que, durante la etapa de verificación de documentos, el período de validez adicional puede usarse cuando se determina la validez del documento.

De acuerdo con otro aspecto, puede proporcionarse un sistema para la verificación de la autenticidad de la información de documentos, el sistema que comprende: un servidor de verificación de información de documentos, el servidor de verificación de información de documentos que comprende: una base de datos que comprende: una cadena de bloques de la almohadilla; y una tabla de metadatos del documento almacenada con relación a la cadena de bloques de la almohadilla unidireccional; módulos de software que comprenden: un módulo de creación de documentos; y un módulo de verificación de la información del documento; un terminal de cliente en comunicación operable con el servidor de verificación de información de documentos, el terminal de cliente que comprende: un lector de datos legibles por computadora; una aplicación de software en comunicación operable con el lector de datos legibles por computadora, la aplicación de software que comprende: un módulo de verificación de la

información del documento; en donde, en uso, el sistema puede configurarse para una etapa de creación de registros de verificación que comprende: el módulo de creación de documentos del servidor de verificación de información de documentos: recibir metadatos del documento con relación a un documento; recibir o generar una almohadilla unidireccional a partir de los metadatos del documento mediante el uso de un algoritmo de creación de almohadilla; crear una entrada en la cadena de bloques de la almohadilla unidireccional para la almohadilla unidireccional; generar datos legibles por computadora que comprenden al menos uno de los metadatos del documento y la almohadilla unidireccional; y enviar los datos legibles por computadora al módulo de creación de documentos; y una etapa de verificación de la información del documento que comprende: el módulo de verificación de la información del documento del terminal de cliente que recibe los datos legibles por computadora a partir de un documento; al menos uno del terminal de cliente y el servidor de verificación de información de documentos que identifica al menos uno de los metadatos del documento y la almohadilla unidireccional a partir de los datos legibles por computadora en donde, si se reciben solamente los metadatos del documento, generar la almohadilla unidireccional mediante el uso del algoritmo de creación de la almohadilla unidireccional; y el módulo de verificación de la información del documento del servidor de verificación de información de documentos que verifica el documento mediante la comparación de la almohadilla unidireccional con la entrada en la cadena de bloques de la almohadilla para la almohadilla unidireccional.

El sistema puede comprender además un servidor emisor de documentos en comunicación operable con el servidor de verificación de información de documentos.

El servidor de verificación de información de documentos puede configurarse para recibir los metadatos del documento desde el servidor emisor de documentos.

La etapa de verificación de información de documentos puede comprender además al menos uno del terminal de cliente y el servidor de verificación de información de documentos que envía al menos uno de la almohadilla unidireccional y los metadatos del documento al servidor emisor de documentos para la verificación adicional del documento.

El servidor emisor de documentos puede comprender una base de datos que comprende al menos uno de la almohadilla y los metadatos, y en donde la verificación adicional puede comprender una referencia cruzada a al menos uno de la almohadilla y los metadatos dentro de la base de datos del servidor emisor de documentos.

El módulo de verificación de información de documentos del servidor de verificación de información de documentos puede configurarse además para enviar un resultado de verificación al terminal de cliente.

La aplicación de software del terminal de cliente puede configurarse además para generar una interfaz de usuario gráfica, y en donde la interfaz de usuario gráfica puede configurarse para mostrar el resultado de la verificación.

La interfaz de usuario gráfica puede configurarse además para mostrar al menos un subconjunto de los metadatos del documento.

El sistema puede comprender una pluralidad de servidores de verificación de información de documentos, y en donde la cadena de bloques puede ser una cadena de bloques distribuida a través de la pluralidad de servidores de verificación de información de documentos.

Crear los datos legibles por computadora puede comprender crear datos ópticos legibles por computadora.

Los datos legibles por computadora pueden ser un código de barras en 2-D.

El sistema puede comprender además insertar los datos legibles por computadora en el documento.

Además, se describen otros aspectos de la invención.

BREVE DESCRIPCIÓN DE LAS FIGURAS

A pesar de cualquier otra forma que pueda estar dentro del alcance de la presente invención, las modalidades preferidas de la descripción se describirán ahora, a modo de ejemplo solamente, con referencia a los dibujos adjuntos en los que:

La Figura 1 muestra un sistema para la verificación de la autenticidad de la información de documentos de acuerdo con una modalidad de la presente descripción;

La Figura 2 muestra un método ilustrativo para la creación de registros de verificación de la autenticidad de la información de documentos de acuerdo con una modalidad;

La Figura 3 muestra un método ilustrativo para verificar la autenticidad de un documento mediante el uso de los registros de

verificación de autenticidad de documentos creados formalmente de acuerdo con una modalidad;

La Figura 4 muestra un método ilustrativo para actualizar la información del documento mientras aún es capaz de verificar la autenticidad del documento actualizado de acuerdo con una modalidad;

La Figura 5 muestra un método ilustrativo para revocar los registros de autenticidad de un documento particular de acuerdo con una modalidad; y

La Figura 6 muestra una interfaz de usuario gráfica ilustrativa mostrada por un terminal de cliente del sistema cuando se verifica un documento de la Figura 1 de acuerdo con una modalidad de la presente descripción.

DESCRIPCIÓN DE LAS MODALIDADES

Con el propósito de promover un entendimiento de los principios de acuerdo con la descripción, se hará referencia ahora a las modalidades ilustradas en los dibujos y se usará un lenguaje específico para describir las mismas. No obstante, se entenderá que de esta manera no se pretende ninguna limitación del alcance de la descripción. Cualquier alteración y modificaciones adicionales de las características de la invención ilustradas en la presente descripción, y cualquier aplicación adicional de los principios de la descripción como se ilustra en la presente descripción, que normalmente se le ocurriría a un experto en la técnica relevante y que posee esta descripción, deben considerarse dentro del alcance de la descripción.

Antes de describir las estructuras, sistemas y métodos asociados al sistema para la verificación de la autenticidad de la información de documentos, debe entenderse que esta descripción no se limita a las

configuraciones particulares, etapas de procesos, y materiales descritos en la presente descripción ya que tales pueden variar un poco. También debe entenderse que la terminología empleada en la presente descripción se usa con el propósito de describir modalidades particulares solamente y no pretende ser limitativa ya que el alcance de la descripción estará limitado sólo por las reivindicaciones y equivalentes de las mismas.

En la descripción y reivindicación de la materia de la descripción, la siguiente terminología se usará de acuerdo con las definiciones expuestas más abajo.

Debe observarse que, tal como se usa en esta descripción y en las reivindicaciones adjuntas, las formas singulares "un", "una" y "la" incluyen referencias plurales a menos que el contexto indique claramente lo contrario.

Como se usa en la presente descripción, "que comprende", "que incluye", "que contiene," "caracterizado porque," y sus equivalentes gramaticales son términos inclusivos o abiertos que no excluyen los elementos no citados, adicionales o las etapas del método.

En la siguiente descripción debe observarse que los números de referencia iguales o similares en diferentes modalidades denotan características iguales o similares.

ARQUITECTURA DEL SISTEMA PARA LA VERIFICACIÓN DE LA AUTENTICIDAD DE LA INFORMACIÓN DE DOCUMENTOS

Con referencia ahora a la Figura 1, se muestra un sistema 1 para la verificación de la autenticidad de la información de documentos.

Como será evidente a partir de la descripción que sigue, el sistema 1 se configura para verificar la autenticidad de documentos, tal como documentos impresos y electrónicos, especialmente la información presentada por dichos documentos para reducir o eliminar la falsificación de documentos, la falsificación de calificaciones y similares.

En la arquitectura ilustrativa proporcionada, el sistema 1 comprende un servidor de verificación de documentos 19. Como se describirá en detalles adicionales más abajo, el servidor de verificación de documentos 19 se configura con varios módulos de software para realizar las diversas tareas de procesamiento computacional descritas en la presente descripción.

En modalidades, el servidor de verificación de documentos 19 puede tener la forma de un servidor de computadora físico (tal como, montado en estante) pero, en modalidades alternativas, el servidor relacionado puede tener la forma de un ejemplo de servidor virtual, tal como ese que puede implementarse por Amazon Web Services (AWS).

Como se describirá en detalles adicionales más abajo, en modalidades, el servidor de verificación de documentos 19 mantiene copia de un libro mayor de la cadena de bloques y por lo tanto, los procesos descritos en la presente descripción del servidor de verificación de documentos 19 pueden compartirse entre una pluralidad de servidores 19.

Específicamente, además, el servidor de verificación de documentos 19 comprende un procesador 31 para procesar datos

digitales. En comunicación operable con el procesador 31 a través de un bus de sistema 33 se encuentra un dispositivo de memoria 29.

El dispositivo de memoria 29 se configura para almacenar datos digitales que incluyen código de programa informático. De esta manera, durante la operación, el procesador 31 puede buscar y ejecutar las instrucciones almacenadas dentro del dispositivo de memoria 29 y almacenar los resultados de los datos de dicha ejecución en el dispositivo de memoria 29.

La memoria 29 puede tener la forma de una combinación de almacenamiento volátil (RAM) y no volátil (HDD).

Para conveniencia de ilustración, la memoria 29 se muestra en la Figura 1 como que se configura con una pluralidad de módulos de software 15 y los datos asociados dentro de la base de datos neural 20.

Como puede verse, los módulos de software 15 pueden comprender un módulo de creación 14 para crear los registros de verificación de documentos que pueden verificarse posteriormente mediante el módulo de verificación 13 de una manera descrita en detalles adicionales más abajo.

Además, los datos mostrados dentro de la base de datos se han mostrado para conveniencia de ilustración ya que comprenden los metadatos de documentos 23 y, en modalidades donde se utiliza una cadena de bloques, los datos de la cadena de bloques 26 que comprenden una pluralidad de almohadillas de documentos 21, 22 representativas de los metadatos de documentos 23 de varios documentos verificados.

El servidor de verificación de documentos 19 comprende además una interfaz de E/S 30 para comunicarse con varios periféricos de computadora que incluyen periféricos de interfaz de usuario y similares.

La interfaz de E/S 30 puede interactuar además con periféricos de almacenamiento de datos tales como dispositivo de almacenamiento de memoria USB. De esta manera, los módulos de código de programa informático 15 pueden almacenarse en un medio legible por computadora que puede actualizarse al servidor de verificación 19 a través de la interfaz de E/S 30 (o interfaz de red 32) para así configurar el servidor de verificación de documentos 19 para realizar las tareas de procesamiento computacional específicas descritas en la presente descripción.

El servidor de verificación de documentos 19 comprende además una interfaz de red 32 para enviar y recibir datos a través de una red de computadoras ilustrada como la Internet 34 en el sistema 1 mostrado. De esta manera, el servidor de verificación de documentos 19 puede estar en comunicación operable con los otros actores informáticos mostrados en la Figura 1.

Con respecto a esto, el sistema 1, en modalidades, puede comprender además un servidor emisor de documentos 16. En términos generales, el servidor emisor de documentos 16 se utiliza por la persona, entidad, organización, autoridad o similares que emiten documentos sensibles que requieren la verificación de autenticidad de la manera descrita en la presente descripción.

Con respecto a esto, el emisor de documentos puede utilizar el servidor emisor de documentos 16 con el fin de almacenar los

metadatos del documento 16, compilar y generar documentos, almacenar y reenviar documentos a través de la Internet 34 y similares.

Con respecto a esto, el servidor emisor de documentos 16 puede comprender similarmente los módulos de software 10 que tienen los módulos de verificación 11 y creación 12. Adicionalmente, el servidor emisor de documentos 16 puede almacenar además los metadatos del documento 18 y las almohadillas asociadas 24.

Como tal, el servidor emisor de documentos 16 puede realizar, en modalidades, todas las tareas de verificación de autenticidad de documentos y datos tal como donde, por ejemplo, una organización utiliza el servidor emisor de documentos 16 para realizar la verificación de documentos de una manera aislada.

En modalidades alternativas, el emisor de documentos 16 puede utilizar el servidor de verificación de documentos 19 (tal como en una base API de suscripción) para realizar todas o al menos algunas de las tareas de verificación de documentos.

El sistema 1 comprende además un terminal de cliente 25 en comunicación operable con al menos uno del servidor emisor de documentos 16 y el servidor de verificación de documentos 19 a través de la Internet 34.

En términos generales, el terminal de cliente 25 puede utilizarse para mostrar la información indicativa de la autenticidad de un documento.

En una modalidad, el terminal de cliente 25 puede tener la forma de un dispositivo de computadora personal tal como una computadora portátil, un dispositivo de comunicación móvil (tal como un dispositivo de teléfono inteligente tal como un iPhone de Apple o similares) que puede utilizarse por un usuario para verificar la autenticidad de un documento.

Como puede verse, el terminal de cliente 25 puede comprender además una interfaz de red 32 para comunicarse a través de la Internet 34.

En la modalidad en donde el terminal de cliente 25 tiene la forma de un dispositivo de comunicación móvil 25, la interfaz de red 32 puede enviar y recibir los datos a través de la red celular tal como una red de datos celular de 3–5G.

El terminal de cliente 25 comprende de manera similar un procesador 31 para procesar los datos digitales y un dispositivo de memoria 29 en comunicación operable con el procesador 31 a través de un bus de sistema 33.

La memoria 29 del terminal de cliente 25 puede comprender además un sistema operativo 30 tal como los sistemas operativos de Apple OS o Android.

Además, el terminal de cliente 25 puede comprender además una interfaz de E/S 30 que, en las modalidades mostradas, puede interactuar con un lector de datos legibles por computadora 8. Con respecto a esto, y como se describirá en detalles adicionales más abajo, el lector 8 puede leer los datos legibles por computadora 27 de

un documento 2 para la verificación, para así verificar la autenticidad del documento.

En la modalidad en donde el terminal de cliente 25 tiene la forma de un dispositivo de comunicación móvil, el lector 8 puede tener la forma del dispositivo de captura de imágenes/cámara del terminal de cliente 25 y los datos legibles por computadora 27 pueden tener la forma de un código de barras de dos dimensiones (2D) (tal como una respuesta rápida (QR)). Como tal, con el fin de verificar el documento 2, el usuario capturaría una imagen del código de barras en 2D contenido por el documento 2 para así permitir al terminal de cliente 25 verificar la autenticidad del mismo.

En modalidades, el terminal de cliente 25 (que tiene la forma de un dispositivo de comunicación móvil) se configura mediante la utilización de una aplicación de software descargada “app” 9 que puede descargarse para la instalación y ejecución por el terminal de cliente 25 tal como desde una tienda de aplicaciones de software, tal como Apple App Store o similares.

Con respecto a esto, la aplicación de software 9 puede comprender varios submódulos/módulos de software que incluyen un módulo de verificación 6 y un módulo de interfaz de usuario gráfica 7.

La Figura 1 muestra además el sistema 1 que comprende un documento 2 que se verifica por el sistema 1. Como se hizo alusión anteriormente, el documento 2 puede tener la forma de documentos en copia dura y copia digital. Para el último, los documentos en copia digital (electrónicos, tal como en formato PDF) pueden almacenarse dentro de una base de datos de documentos 34. Con respecto a esto, pueden recuperarse documentos particulares mediante la utilización

de una URL e ID de documento u otro identificador único, tal como una almohadilla de documento.

Como se muestra, el documento 2 puede comprender el contenido del documento 5. Además, el documento 2 puede comprender los datos legibles por computadora 27 que, como se hizo alusión anteriormente, pueden tener la forma de un código de barras en 2D incluido o impreso en el documento 2. Como tal, los datos legibles por computadora 27 pueden leerse por el terminal de cliente 25 (u otro actor informático a través de la Internet 34) para así verificar la autenticidad de los mismos.

En modalidades, los datos legibles por computadora 27 pueden comprender una ID de documento, una almohadilla de metadatos del documento 4 o los metadatos del documento 3 o sus combinaciones en dependencia de la aplicación particular.

Debe observarse que la arquitectura de computadora proporcionada en la Figura 1 es principalmente para propósitos ilustrativos.

Específicamente, la arquitectura particular proporcionada en la Figura 1 es para la aplicación en donde un servidor de verificación de documentos 19 se despliega para la utilización sobre una base de suscripción de manera que varios emisores de documentos, usuarios y similares pueden acceder selectivamente a las funciones de red expuestas por el servidor de verificación de documentos 19 para la verificación de documentos.

Sin embargo, debe observarse específicamente que la arquitectura particular puede modificarse mientras aún se realizan las

mismas tareas de verificación de autenticidad de documentos y la funcionalidad dentro del alcance intencional de las modalidades descritas en la presente descripción.

Método ilustrativo 35 para la creación de registros de autenticidad de documentos.

Después de describir generalmente la arquitectura computacional anterior, ahora se proporcionarán varios métodos ilustrativos para la utilización del sistema 1 para la verificación de autenticidad de documentos que incluyen el método 35 mostrado en la Figura 3 para la creación de registros de autenticidad de documentos.

El método 35 se utiliza para crear registros de autenticidad de documentos que pueden utilizarse posteriormente y las etapas de verificación posteriores.

Debe observarse que el método 35 es solamente ilustrativo y que ninguna limitación técnica debería imputarse necesariamente a todas las modalidades en consecuencia.

En la etapa 39 del método 35, se obtiene el contenido del documento.

Donde el documento 2 es un documento físico, el documento puede escanearse mediante la utilización de un escáner y el contenido del documento obtenerse mediante la utilización del reconocimiento óptico de caracteres (OCR).

Alternativamente, donde el documento 2 es un documento en copia digital, el contenido del documento puede leerse desde el

documento del sistema de archivos electrónicos en sí (tal como mediante la lectura de varios metadatos del documento o contenido del documento, que incluye en donde el contenido del documento puede reconocerse además mediante el uso de OCR) o alternativamente recuperarse desde una base de datos adecuada, tal como la base de datos 17 del servidor emisor de documentos 16.

Generalmente, el contenido del documento es el contenido del documento importante (referido en la presente descripción como metadatos, de los que puede crearse una almohadilla en una almohadilla de metadatos tal como la almohadilla MD5, SHA256 u otra almohadilla unidireccional adecuada) para que las alteraciones o modificaciones posteriores a este contenido importante del documento puedan detectarse por el sistema 1. En otras modalidades puede crearse una almohadilla de todo el documento en una almohadilla de documento de manera que puede detectarse cualquier alteración al documento.

Además, como se describirá en detalles adicionales más abajo, el sistema 1 puede comprender una funcionalidad para la actualización del contenido del documento/metadatos, o para la revocación de la acreditación de autenticidad.

En la etapa 40, pueden identificarse varios metadatos. Como se aludió anteriormente, los metadatos representan la información importante contenida dentro del documento.

Por ejemplo, para un documento de declaración de logro, los metadatos pueden representar el nombre de la organización emisora, el nombre del que lo consigue y el nombre de la calificación. En un ejemplo adicional, para una tarjeta de embarque, los metadatos

pueden representar el nombre del pasajero, el número de vuelo, la puerta de embarque, el número de pasaporte, el destino y similares.

En modalidades, el sistema 1 se configura para crear una almohadilla de metadatos 4 de los metadatos de manera que la falsificación de los metadatos importantes puede detectarse por el sistema 1. Además, los metadatos pueden guardarse en formato sin almohadilla (ya sea en texto sin formato o encriptado) para así permitir la visualización posterior por el terminal de cliente 25 durante la verificación.

El uso de los metadatos en la etapa 40 (que representan cierta información importante del documento) puede ser útil para documentos en copia dura de manera que la información importante presentada en el mismo se aísla para la verificación. De esta manera, el documento puede modificarse de otras maneras, tales como que incluyen anomalías de fotocopias y escaneado, la impresión en diferentes membretes o similares sin afectar la capacidad para verificar la autenticidad del mismo.

Sin embargo, como se hizo alusión anteriormente, debe observarse que en modalidades, especialmente para documentos electrónicos, los metadatos no necesitan aislarse necesariamente del documento en lugar de la almohadilla que se crea de todos los contenidos del archivo de datos electrónicos. Específicamente, en esta modalidad, contrario a la codificación de metadatos, el archivo del documento electrónico puede codificarse, tal como la almohadilla MD5, SHA256 o similares. En modalidades, pueden utilizarse una almohadilla de metadatos separada y una almohadilla de documento de manera que la modificación del documento o los metadatos sensibles en el mismo pueden detectarse independientemente.

En modalidades, los metadatos usados pueden ser especificados por el usuario. Por ejemplo, ciertos metadatos se usan a partir de la base de datos del emisor del documento 29 que se especifica por el usuario.

En modalidades alternativas, donde los metadatos se extraen del documento en sí, pueden especificarse filtros de cadenas de búsquedas para permitir al sistema 1 extraer (que incluyen mediante el uso de OCR) los metadatos adecuados.

Por ejemplo, para la documentación de declaración de logro, solamente pueden especificarse el nombre de la organización, el que lo consigue y la calificación para guardarse como los metadatos para los propósitos de verificación de manera que el otro contenido del documento puede modificarse sin afectar la capacidad para verificar la autenticidad de los metadatos del documento.

Como tal, varias cadenas de búsqueda pueden utilizarse para así permitir al sistema 1 extraer estos campos de metadatos.

Aún en modalidades adicionales, pueden especificarse regiones/rectángulos del documento (que representan la ubicación de los metadatos del documento dentro del documento) para así permitir al sistema extraer sólo texto de las regiones especificadas.

En la etapa 41, puede obtenerse o generarse una ID de documento. En una modalidad preferida, la ID de documento es globalmente única (GUID) para así evitar o eliminar sustancialmente las colisiones de la ID de documento.

La ID de documento puede utilizarse para identificar exclusivamente documentos para la verificación. Por ejemplo, la ID de documento puede utilizarse para recuperar documentos desde la base de datos de documentos 34 mediante la utilización de una URL que comprende la ID de documento. Además, la ID de documento puede utilizarse para actualizar documentos para revocar documentos.

En modalidades, la ID de documento puede generarse por el sistema 1. Sin embargo, en modalidades alternativas, la ID del documento 1 puede proporcionarse por el emisor de documentos tal como en donde, por ejemplo, una organización de formación registrada emite documentos de declaración de logro en orden numérico secuencial.

En modalidades, puede crearse además una almohadilla de la ID del documento como parte de la almohadilla de metadatos o la almohadilla de documento para así evitar la falsificación de la ID del documento.

Debe observarse, sin embargo, que en ciertas modalidades, una ID de documento no se requiere necesariamente. Por ejemplo, un documento en copia dura puede comprender un código de barras en 2D en el mismo que representa una almohadilla de los metadatos, los metadatos que representan la información mostrada por el documento. Como tal, el código de barras en 2D puede escanearse para verificar el contenido del documento sin tener que usar necesariamente una ID de documento.

En modalidades adicionales, la almohadilla generada a partir del archivo del documento o los metadatos puede servir como la ID de documento única.

En la etapa 42, se crea una almohadilla 4. Preferentemente, la almohadilla es una almohadilla unidireccional tal como MD5, SHA256 o similares. La almohadilla proporciona la capacidad de reducir potencialmente una gran cantidad de información en un tamaño pequeño pero, lo que es más importante, en donde la falsificación incluso con una sola letra del contenido afecta drásticamente la almohadilla.

En una modalidad preferida, la almohadilla 4 es una almohadilla de metadatos de manera que se crea una almohadilla de los metadatos (información importante del documento) para que sea capaz de detectar alteraciones posteriores de esta información importante del documento. Sin embargo, como se hizo alusión además anteriormente, en otra modalidad, la almohadilla 4 puede ser una almohadilla de documento del archivo del documento electrónico.

Además, puede crearse una almohadilla de otra información dentro de la almohadilla 4, que incluye la ID del documento.

En una modalidad, puede crearse una almohadilla de una combinación de la información anterior para formar la almohadilla 4.

En una modalidad preferida, el sistema 1 utiliza una cadena de bloques con el fin de almacenar las almohadillas 4 para ser capaz de proporcionar un libro mayor de confianza y distribuido inalterable de verificación de documentos.

Específicamente, como se muestra en la Figura 1, el servidor de verificación de documentos 19 puede almacenar una copia de un libro mayor de cadena de bloques 26 dentro de la base de datos 20 que

puede sincronizarse con otro servidor de verificación de documentos 19.

Como tal, en la etapa 43, la almohadilla se añade a una transacción de cadena de bloques que posteriormente se mina y añade a un bloque en la cadena de bloques. Existen diferentes maneras en las que la almohadilla puede añadirse a una cadena de bloques, que incluye, en donde se utiliza la cadena de bloques de bitcoin, dentro del código operacional de programación de bitcoin. En modalidades alternativas, puede utilizarse una cadena de bloques personalizada que comprende campos de datos adecuados.

Como tal, cuando se verifica un documento, la cadena de bloques puede inspeccionarse para determinar si la almohadilla 4 (que puede escanearse a partir del código de barras en 2D 27 o alternativamente calcularse sobre la marcha) reside dentro de la cadena de bloques.

En modalidades, puede buscarse una almohadilla en toda la cadena de bloques pero, en una modalidad preferida, puede usarse un índice de almohadilla separado para acelerar el proceso de localización de la almohadilla.

Debe observarse que no todas las modalidades utilizan necesariamente una cadena de bloques. Por ejemplo, el servidor emisor de documentos 16 puede mantener la base de datos de los metadatos del documento 18 (o contenido del documento) y las almohadillas de documentos asociadas 24 o ID de documentos con el fin de permitir la verificación de documentos por separado sin la utilización de un libro mayor compartido. De esta manera, el sistema 1 mantiene aún una copia de los metadatos 18 (para así, por ejemplo,

permitir la visualización de los metadatos durante el proceso de verificación para la comparación visual por el usuario) y las almohadillas asociadas para ser capaz de detectar la falsificación de los metadatos (aunque sin seguridad contra la falsificación de la base de datos 17 que puede evitarse mediante la utilización de la cadena de bloques).

En la etapa 44, pueden generarse los datos legibles por computadora que pueden utilizarse después junto con el documento para la verificación.

En la etapa 46, los datos legibles por computadora se insertan en el documento, ya sea de manera visible o invisible.

En una modalidad aludida anteriormente, los datos legibles por computadora 27 pueden tener la forma de un código de barras en 2D que comprende uno o más de la almohadilla del documento, la ID del documento y los metadatos del documento.

En una modalidad preferida, los datos legibles por computadora 27 son visibles para así permitir la impresión, escaneado y fotocopia del documento.

Por ejemplo, el documento puede modificarse para mostrar visualmente los datos legibles por computadora 27 tal como en donde, por ejemplo, un documento PDF se modifica para incluir una imagen del código de barras en 2D en el lado derecho inferior del documento. De esta manera, cuando se verifica posteriormente el documento electrónico, o una impresión del mismo, el usuario puede utilizar el dispositivo de cámara del teléfono inteligente 25 para capturar una

imagen del código de barras en 2D para verificar los contenidos o los metadatos del documento.

En modalidades alternativas, para documentos electrónicos que existen solamente en forma electrónica, los datos legibles por computadora 27 no necesitan necesariamente ser visibles a los humanos y pueden incorporarse dentro de, por ejemplo, los metadatos del documento. De esta manera, cuando se visualiza el documento, el software de visualización del documento puede inspeccionar, en segundo plano, los metadatos asociados y visualizar una indicación de si el documento se verifica o no.

Por ejemplo, un documento PDF puede actualizarse de manera que los metadatos del documento PDF comprenden los datos legibles por computadora 27 (que, como se hizo alusión anteriormente, pueden incluir uno o más de los metadatos del documento, la ID del documento y una almohadilla del documento). Como tal, cuando se muestran dentro de la aplicación PDF, tal como el lector Adobe Acrobat, el software PDF puede inspeccionar automáticamente los datos legibles por computadora 27 y mostrar una indicación de si el documento se verifica o no.

En modalidades alternativas, tal como cuando se utiliza para documentación de viaje y similares, pueden usarse etiquetas RFID.

En la etapa 46, donde el documento tiene la forma de un documento electrónico, el documento puede firmarse además digitalmente para así evitar la falsificación o la modificación de los datos legibles por computadora incluidos o insertados en el mismo.

En una modalidad, el servidor de verificación de documentos 19 puede firmar el documento mediante el uso de una clave privada de manera que otros pueden verificar posteriormente que el servidor de verificación de documentos 19 ha firmado efectivamente el documento mediante la utilización de la clave pública asociada.

Método ilustrativo 36 para la verificación de la autenticidad de documentos

Con referencia ahora a la Figura 2, se muestra un método ilustrativo 36 para la verificación de la autenticidad de documentos. Como será evidente a partir de la descripción que sigue, el método 36 se utiliza con el fin de verificar la autenticidad de un documento mediante la utilización de los datos legibles por computadora 27 asociados con el mismo.

El método 36 inicia en la etapa 47 en donde se obtiene el documento. Por ejemplo, un documento físico puede obtenerse en la mano o alternativamente, un documento electrónico puede recuperarse a partir de un sistema de archivos, descargarse desde una URL o similares.

En la etapa 48 se escanean o leen los datos legibles por computadora asociados con el documento.

Para un documento físico que comprende los datos legibles por computadora 27 en forma de un código de barras en 2D, el código de barras puede leerse mediante la utilización del lector 8 del terminal de cliente 25.

Para un documento electrónico, los datos legibles por computadora 27 pueden recuperarse por el software de visualización del documento (tal como Adobe Acrobat).

En la etapa 49, la almohadilla puede extraerse a partir de los datos legibles por computadora 27.

Donde los datos legibles por computadora comprenden la ID del documento, la ID del documento puede recuperarse además a partir de los datos legibles por computadora para ser capaz de compararse contra la ID del documento usada para recuperar el documento o asociada con el documento.

En la etapa 50, donde el sistema 1 utiliza una cadena de bloques, la cadena de bloques puede inspeccionarse para bloques que contienen transacciones que contienen la almohadilla y, en modalidades, la ID de documento asociada.

Si se encontrara una transacción coincidente dentro de la cadena de bloques, en la etapa 51, puede mostrarse una verificación al usuario que indica que el documento es auténtico.

Adicionalmente, en la etapa 52 los metadatos pueden extraerse a partir de los datos legibles por computadora que luego pueden mostrarse por el terminal de cliente 25 para así permitir al usuario comparar los metadatos extraídos a partir de los datos legibles por computadora con los que se muestran en el documento.

En ciertas otras modalidades, los metadatos 23 pueden almacenarse dentro de la cadena de bloques 26 en sí, de manera que los metadatos 23 pueden recuperarse a partir de la cadena de bloques

26 durante la verificación para así negar la necesidad de almacenar los metadatos 23 dentro del código de barras en 2D 27 en sí.

Método ilustrativo 37 para actualizar los metadatos del documento

Con referencia a la Figura 4, se muestra un método ilustrativo 37 para actualizar los metadatos del documento.

Específicamente, en modalidades, puede surgir una necesidad para actualizar los metadatos del documento.

Por ejemplo, para tarjetas de embarque, puede ocurrir un cambio de puerta. En un ejemplo adicional, para una declaración de logro, el nombre del que lo consigue puede cambiarse de un nombre de soltera.

Como tal, el método 37 puede utilizarse para permitir la actualización de ciertos campos del documento mientras aún es capaz de mantener la capacidad para verificar la autenticidad de un documento.

Como tal, en la etapa 52, puede generarse u obtenerse la ID de documento para el documento que va a actualizarse (u otro identificador único tal como la almohadilla del documento o metadatos).

En la etapa 54, se reciben los metadatos actualizados (o el contenido del documento). Por ejemplo, los metadatos actualizados pueden comprender un nuevo apellido.

En la etapa 55, se crea una almohadilla de los metadatos actualizados (o el contenido del documento actualizado).

Ahora, en la etapa 56, la nueva almohadilla se añade por medio de una transacción adicional a la cadena de bloques.

En las etapas 57 – 59, el documento puede modificarse para incorporar los nuevos datos legibles por computadora 27. Sin embargo, la actualización del código de barras en 2D 27 no tiene lugar necesariamente, especialmente para documentos que ya se han divulgado.

Como tal, cuando se verifica posteriormente el documento, las transacciones de cadenas de bloques pueden inspeccionarse en orden cronológico inverso en donde la transacción de verificación más reciente se utiliza como la transacción de verificación actual.

Alternativamente, si una almohadilla se extrae desde un documento asociado con una transacción de cadena de bloques para la cual existe una transacción de cadena de bloques más reciente, el terminal de cliente 25 puede informar al usuario que los metadatos/contenido del documento están desactualizados y que el documento se ha suplantado.

En modalidades, el resultado de la verificación puede indicar que el documento se ha suplantado. Sin embargo, en otras modalidades el resultado de la verificación puede indicar cuales metadatos del contenido del documento se han suplantado.

Por ejemplo, cuando se crea una primera transacción de verificación de la cadena de bloques, la ID del documento y la

almohadilla de metadatos original pueden almacenarse dentro de la cadena de bloques.

Luego, cuando se recibe una actualización de los metadatos del documento, una nueva transacción de la cadena de bloques puede crearse dentro de la cadena de bloques que comprende la ID del documento y la nueva almohadilla de metadatos (que representa los metadatos actualizados).

Como tal, durante la verificación posterior del documento, los datos legibles por computadora 27 pueden leerse por el terminal de cliente 25 para extraer la ID del documento y la almohadilla de metadatos.

Después, en la cadena de bloques pueden buscarse transacciones de cadenas de bloques asociadas con la ID del documento.

Sin embargo, si el sistema 1 identifica dos o más transacciones, el sistema 1 es capaz de comparar la almohadilla recuperada contra las dos o más transacciones para identificar si la transacción particular es actual o se ha suplantado.

Método ilustrativo 38 para la revocación de autenticidad de documentos

Con referencia ahora a la Figura 5, se muestra un método ilustrativo 38 para la revocación de autenticidad de documentos.

Específicamente, puede surgir una necesidad para revocar un documento. Por ejemplo, una persona que ha recibido una declaración

de logro, puede encontrarse posteriormente que ha obtenido fraudulentamente la calificación y por lo tanto, se requiere la revocación de la declaración de logro.

Cuando se utiliza la tecnología de la cadena de bloques, no es posible eliminar una transacción de la cadena de bloques.

Como tal, el método 38 utiliza una transacción de revocación que se añade a la cadena de bloques para revocar un documento.

Específicamente, el método 38 inicia en la etapa 60 en donde se recibe una solicitud de revocación para un documento particular que se identifica por una ID de documento (u otro identificador único tal como la almohadilla del documento o metadatos).

En la etapa 61, una transacción de revocación se añade a la cadena de bloques. La transacción de revocación se identifica por el tipo de transacción (el tipo de transacción de revocación, que puede almacenarse de nuevo en el código operacional de programación de bitcoin) y la ID del documento.

Como tal, durante la verificación posterior, en la etapa 62 los datos legibles por computadora se reciben por el documento, y la ID del documento y/o la almohadilla del documento se extraen desde el mismo.

En la etapa 63, en la cadena de bloques se buscan ID de documentos o almohadillas coincidentes.

Sin embargo, para cualquier transacción de verificación identificada dentro de la cadena de bloques, en la etapa 63, el sistema

1 identifica una transacción de revocación posterior dentro de la cadena de bloques asociada con la ID del documento o almohadilla y por lo tanto, en la etapa 64, la verificación falla.

Períodos de verificación de autenticidad finitos

En modalidades, los documentos pueden tener una autenticidad finita. En donde, por ejemplo, los documentos son válidos por 12 meses solamente, tal como puede ser el caso para licencias de conducción.

Como tal, la transacción de verificación almacenada dentro de la cadena de bloques puede especificar un período de validez (que puede almacenarse de nuevo en el código operacional de programación de bitcoin). Como tal, durante la verificación, el sistema 1 puede inspeccionar las fechas de entrada de las transacciones de verificación y si la fecha actual excede el período de validez, la verificación falla.

Por ejemplo, si el sistema 1 identifica una transacción de verificación dentro de la cadena de bloques de hace más de 12 meses, pero la transacción de verificación especifica que la verificación es válida por un período de 12 meses, y el sistema 1 es incapaz de identificar ninguna transacción de verificación adicional posterior en el tiempo asociada con el documento, entonces la verificación falla.

Con respecto a esto, el período de validez puede renovarse a través de la adición de transacciones de verificación de cadena de bloques posteriores en el tiempo.

Uso ilustrativo de la arquitectura del sistema 1 para la verificación de documentos de declaración de logro emitidos por organizaciones de formación registradas (RTO)

Después de describir la arquitectura del sistema anterior 1 y las metodologías asociadas, ahora se describirá un uso ilustrativo del sistema 1 para la utilización para la aplicación de la verificación de documentos de declaración de logro emitidos por organizaciones de formación registradas (RTO).

Como puede verse, el servidor emisor de documentos (RTO) 16 comprende una pluralidad de módulos de software 10.

En las modalidades descritas en la presente descripción, los módulos de software 10 pueden comprender un módulo de creación de registros de verificación 12 con el fin de crear un registro de documentos para la verificación posterior.

Como puede verse además, el servidor de verificación de información de documentos 19 puede comprender en sí una pluralidad de módulos de software 15 en sí que comprende un módulo de creación de registros de verificación 14.

Además, los módulos de software 10 del servidor emisor de documentos (RTO) 16 pueden comprender además un módulo de verificación 11 para la verificación posterior de documentos.

De manera similar, los módulos de software 15 del servidor de verificación de información de documentos 19 comprenden un módulo de verificación 13 con el fin de verificar los documentos como se describirá en detalles adicionales más abajo.

Como se aludió anteriormente, tal verificación y creación de funcionalidad pueden implementarse por los mismos módulos si la funcionalidad del servidor emisor de documentos (RTO) 16 y el servidor de verificación de información de documentos 19 se implementa por un único servidor.

En esta modalidad ilustrativa, una persona con el nombre de James Smith completa exitosamente un curso en una RTO particular.

Después de completar el curso, los detalles de la declaración de logro o curso se registran por la RTO.

Específicamente, como puede verse, el servidor emisor de documentos (RTO) 16 comprende una base de datos 17.

Además, la base de datos 17 puede comprender los metadatos 18, u otro tipo de datos estructurados, configurados para almacenar varios campos de información con relación al curso completado por James Smith.

Como tal, la siguiente información puede registrarse en la base de datos 17:

a. Nombre: James Smith
b. Fecha de emisión: 7 de julio de 2007
c. Número del documento: 0007/07/2007
d. RTO emisora: Allwest Training service
e. Código nacional de proveedor núm.: 51925
f. Tipo de certificación: Declaración de logro/Curso
g. Oficial que firma: Bob Cooper
h. Posición de oficial que firma: Director Ejecutivo

Ahora, durante la etapa de creación de registros de verificación, se crea una almohadilla de los metadatos anteriores. En una modalidad, los metadatos se concatenan tal como en una cadena que comprende:

i. James Smith|19051983|M|007 007 007|0007/07/2007|Allwest Training service|51925|07072007|Declaración de logro|Conducción de un camión volquete|Bob Cooper|Director Ejecutivo

Después, se crea una almohadilla de la cadena concatenada mediante el uso de un algoritmo de almohadilla unidireccional, tal como un algoritmo de almohadilla MD5, SHA256 u otro. Por ejemplo, tal creación de almohadilla puede generar la siguiente almohadilla:

j. 25908e49524e4828190dae3d79b894eec7ec3e4843c8bca6ef9f384c679167bc

k.

Luego, la almohadilla de metadatos se almacena para poder usarse para la posterior verificación de la información del documento.

Específicamente, como puede verse, el servidor de verificación de información de documentos 19 comprende una base de datos 20 para almacenar varias informaciones que incluyen los datos de la almohadilla.

Como tal, la almohadilla de metadatos anterior se inserta en la base de datos 20. Tal inserción puede comprender que el servidor de verificación de información de documentos 19 recibe los metadatos (o la almohadilla de metadatos) desde la base de datos 17 del servidor emisor de documentos (RTO) 16, tal como en intervalos periódicos, cuando se soliciten y similares.

Debe observarse que el algoritmo de creación de almohadillas descrito en la presente descripción puede realizarse por cualquiera de los actores informáticos dentro del alcance intencional de las modalidades descritas en la presente descripción. En otras palabras, por ejemplo, el servidor emisor de documentos (RTO) 16 o el servidor de verificación de información de documentos 19 pueden realizar la creación de almohadillas.

En una modalidad preferida, para evitar el fraude que surge a partir de la inserción de entradas de almohadillas fraudulentas en la base de datos 20, el sistema 1 puede implementar una cadena de bloques del libro mayor público distribuido 26 de manera que cada entrada de almohadillas puede verificarse de acuerdo con las otras entradas de almohadillas dentro de la base de datos 20.

En las modalidades descritas en la presente descripción, la verificación se realiza por un único servidor de verificación de información de documentos 19. Sin embargo, debe apreciarse que la cadena de bloques 26 puede ser una cadena de bloques distribuida a través de un número de servidores 19.

Debe observarse que cualquier criptografía distribuida basada en cadenas de bloques puede utilizarse dentro del alcance intencional de las modalidades descritas aquí y que incluyen esas que se usan en, o son similares a las cadenas de bloques de Bitcoin, ehterum, litecoin y similares.

En estas modalidades, a cada RTO 16 (“emisor de información de documentos”) y servidor de verificación de documentos 19 se les puede asignar una “dirección de emisión”, que puede ser una dirección de cartera de Bitcoin. Las transacciones capacitoras dentro de la

cadena de bloques de Bitcoin pueden asociarse únicamente con el servidor emisor de documentos 16 o el servidor de verificación de documentos 19 respectivo.

En modalidades, los metadatos pueden almacenarse además dentro de la base de datos 20 del servidor de verificación de información de documentos 19. De esta manera, al tener la almohadilla (o la ID del documento), pueden buscarse los metadatos.

En esta modalidad, la almohadilla puede servir como una clave primaria. Sin embargo, debe apreciarse que la base de datos 20 no necesita comprender necesariamente los metadatos 23 para comprender la almohadilla solamente con el fin de la verificación de información del documento.

Ahora, se generan los datos legibles por computadora que comprenden al menos uno de la almohadilla y los metadatos. La creación de los datos legibles por computadora permitirá la inserción de los datos legibles por computadora en un documento, tal como un certificado de logro, que es un documento impreso o electrónico (es decir, PDF) que puede leerse posteriormente mediante el uso del terminal de cliente 25 con el fin de verificar la autenticidad del documento y los metadatos del documento almacenados en el mismo.

En una modalidad preferida, los datos legibles por computadora se incorporan en un código de barras en 2D. Por ejemplo, cuando se generan los datos legibles por computadora en un código de barras en 2D, los siguientes formatos pueden utilizarse para la codificación de los datos:

I. [Almohadilla_clave] || [Nombre] || [Fecha de nacimiento en DD/MM/AAAA] || [Género] || [Número DL] || [Número de

documento] || [RTO emisora] || [Código nacional de proveedor núm.] || [Fecha de emisión en DD/MM/AAAA] || [Tipo de certificación] || [Tipo de licencia] || [Oficial que firma] || [Posición de oficial que firma]

Esto puede generarse mediante el uso de un algoritmo adecuado en el siguiente código de barras en 2-D:

[2]

Después de crear los datos legibles por computadora, los datos legibles por computadora se insertan en o imprimen sobre un documento.

Como puede verse a partir de la Figura 1, se muestra un documento 2 que es un certificado de logro para el curso completado por James Smith. En esta modalidad particular, el documento 2 se emite como un documento PDF por el servidor emisor de documentos (RTO) 16. Como tal, James Smith puede utilizar el documento PDF electrónico 2 como evidencia de su calificación para varios propósitos de empleo.

Como puede verse, el documento puede comprender el contenido del documento 5 que puede comprender la información legible por humanos usual que incluye al menos un subconjunto de los metadatos descritos anteriormente. Sin embargo, como se hizo alusión anteriormente, en arreglos de la técnica anterior el documento puede editarse, ya sea electrónica o físicamente para representar la información fraudulenta.

Como tal, el documento, al comprender adicionalmente los datos legibles por computadora 27 puede verificarse mediante el uso del terminal de cliente 25. Como puede verse, los datos legibles por computadora 27 contenidos por el documento 2 pueden comprender al menos uno de los metadatos 3, la almohadilla de metadatos o documento 4 y la ID del documento.

En modalidades, solamente los metadatos 3 se codifican dentro de los datos legibles por computadora 27 de manera que la almohadilla puede calcularse a partir de los metadatos para la verificación. En otras modalidades, solamente la almohadilla 4 se codifica dentro de los datos legibles por computadora 27 de manera que los metadatos pueden recuperarse desde la base de datos 20 del servidor de verificación de información de documentos 19 o la base de datos 17 del servidor emisor de documentos (RTO) 16 o la cadena de bloques.

Como puede verse, el terminal de cliente 25 comprende una aplicación de software 9 configurada para implementar las características y la funcionalidad descritas en la presente descripción. Como se aludió anteriormente, en una modalidad, el terminal de cliente 25 es un dispositivo de comunicación móvil, tal como un dispositivo de teléfono inteligente o similares. En la presente descripción, el terminal de cliente 25 puede comprender un lector 8, que, en modalidades puede tener la forma de la cámara de un teléfono móvil.

Durante el uso, la operación del terminal de cliente 25 puede descargar la aplicación de software 9 para la ejecución por el terminal de cliente 25, tal como desde una tienda de aplicaciones de software, tal como Apple iTunes store o similares.

Como puede verse, la aplicación de software 9 puede comprender un módulo de verificación 6 configurado para implementar la funcionalidad implementada del terminal de cliente para la verificación de información de documentos y además un módulo de interfaz de usuario gráfica (GUI) que presenta una interfaz de usuario gráfica para la visualización 7 con el fin de mostrar varias informaciones al usuario del terminal de cliente.

Como tal, con el fin de verificar la autenticidad del documento, el usuario del terminal de cliente, mediante el uso del lector 8, escaneará los datos legibles por computadora en el código de barras en 2-D 27 proporcionados en el documento. Después de recibir los datos legibles por computadora desde el documento 2, al menos uno del terminal de cliente 25 y el servidor de verificación de información de documentos 19 se configura para identificar al menos uno de los metadatos 3 y la almohadilla 4.

En una modalidad preferida, los metadatos 3 se codifican dentro de los datos legibles por computadora 27 de manera que la GUI 7 del terminal de cliente 25 puede mostrar los metadatos.

En una modalidad preferida adicional, tanto la almohadilla 4 como los metadatos 3 se codifican dentro de los datos legibles por computadora 27 de manera que el terminal de cliente 25 puede generar una almohadilla mediante el uso del algoritmo de creación de almohadillas mediante el uso de los metadatos codificados 3 para verificar al menos que la almohadilla codificada 4 coincide con los metadatos 3. En modalidades, puede utilizarse un algoritmo de almohadilla de propiedad para evitar que estafadores generen y codifiquen fraudulentamente la almohadilla mediante el uso de un algoritmo de creación de almohadillas conocido.

Además, el terminal de cliente 25, al estar en comunicación operable con el servidor de verificación de información de documentos 19 a través de una red de datos, tal como la Internet, es capaz de enviar al menos uno de los metadatos 3 y la almohadilla 4 al servidor de verificación de información de documentos 19 para la verificación.

El servidor de verificación de información de documentos 19 se configura para comparar la almohadilla recibida desde el terminal de cliente 25 (o calculada a partir de los metadatos 3 leídos por el terminal de cliente 25) contra el valor de la almohadilla almacenada dentro de la cadena de bloques 26.

Si se encuentra una coincidencia, el servidor de verificación de información de documentos 19 es capaz de enviar un resultado de verificación de vuelta al terminal de cliente 25 que verifica que la información del documento es auténtica.

Alternativamente, si no se encuentra ninguna coincidencia, el servidor de verificación 19 se configura para enviar un resultado sin verificación de vuelta al terminal de cliente 25 que indica que la información del documento puede ser fraudulenta o se ha falsificado.

En cualquier caso, la GUI 7 se configura para mostrar los resultados de verificación al usuario del terminal de cliente. Adicionalmente, la GUI 7 puede mostrar los metadatos asociados.

Por ejemplo, y con referencia ahora a la Figura 6, se muestra una interfaz ilustrativa 28 mostrada por la GUI 7 donde el documento se ha verificado. Como puede verse, la interfaz 28 comprende varios de los metadatos y una confirmación de que la información del documento es auténtica.

En modalidades, el sistema 1 se configura para implementar una verificación adicional en donde los registros contenidos dentro de la base de datos 17 del servidor RTO se comparan por referencia cruzada adicionalmente (en caso de que los registros se hayan actualizado o revocado). Específicamente, la referencia cruzada puede realizarse mediante el uso de al menos uno de la almohadilla y los metadatos. Como puede verse, en una modalidad, la base de datos 17 del servidor emisor de documentos (RTO) 16 puede configurarse para almacenar los valores de la almohadilla 24 con relación a los metadatos 19. Como se aludió anteriormente, tales valores de la almohadilla 24 pueden recibirse desde el servidor de verificación de información de documentos 19 o alternativamente calcularse por el servidor emisor de documentos (RTO) 16 en sí. Como se aludió además anteriormente, en modalidades, la base de datos 17 no necesita comprender necesariamente los valores de la almohadilla 24 en donde los metadatos 18 se comparan por referencia cruzada.

Cuando los metadatos 18 se comparan por referencia cruzada, al menos uno del terminal de cliente 25 y el servidor de verificación de información de documentos 19 puede enviar una petición adicional al módulo de verificación 11 del servidor emisor de documentos (RTO) 16 para verificar los datos almacenados dentro de la base de datos 17. Por ejemplo, el terminal de cliente 25 puede enviar el número del documento al servidor RTO 16 para verificar que el número del documento es genuino. Otras referencias cruzadas pueden hacerse dentro del alcance intencional de las modalidades descritas en la presente descripción.

Uso ilustrativo del sistema 1 para documentación en copia dura

Ahora se describirá un uso ilustrativo del sistema 1 para documentación en copia dura.

Específicamente, como se hizo alusión anteriormente, los problemas de la documentación en copia dura pueden incluir la apariencia de la documentación que cambia con el tiempo, tal como la que se provoca por las anomalías de las fotocopias y similares.

Como tal, en este uso ilustrativo, se describirá el sistema 1 que aún es capaz de verificar el documento en copia dura a pesar de los cambios en la apariencia.

Específicamente, en este ejemplo, el documento en copia dura es un documento de contrato de venta que se ha refrendado por el vendedor, el comprador y el testigo. El documento en copia dura especifica además la propiedad inmueble que se vende, identificada por el número de lote.

Como tal, con el fin de crear los registros de verificación de documentos, el documento del contrato ejecutado puede escanearse mediante el uso de un escáner, y en donde el sistema 1 realiza entonces el reconocimiento de OCR del documento para identificar los metadatos relevantes del contrato de venta. En este ejemplo, los metadatos relevantes son los nombres del vendedor y el comprador y el número de lote.

Como tal, el sistema 1 se configura para extraer dichos metadatos a partir del documento. Por ejemplo, mediante la utilización de OCR, el sistema 1 puede configurarse para utilizar la coincidencia de cadenas o similares para extraer estos campos a partir de los datos.

Alternativamente, una imagen escaneada del documento puede mostrarse en el terminal de cliente 25 de manera que el abogado es capaz de delimitar los metadatos que van a verificarse, tal como mediante el arrastre de rectángulos alrededor del texto asociado mediante el uso del ratón.

Adicionalmente, una ID de documento puede especificarse por el abogado, que es una ID de documento generada por el sistema de archivos.

Después de obtener los metadatos relevantes, el sistema 1 crea una almohadilla de los metadatos (y la ID de documento en modalidades) y crea una transacción de verificación dentro de la cadena de bloques.

Además, el sistema 1 genera los datos legibles por computadora en forma de un código de barras en 2D que luego se imprime sobre el documento del contrato de venta.

El código de barras en 2D comprende la almohadilla de metadatos 4, la ID del documento y los metadatos.

Luego, el contrato de venta se fotocopia y se envía una fotocopia a un traspasador.

Sin embargo, ligeras anomalías visuales ocurren durante el proceso de fotocopiado.

No obstante, para verificar el contrato de venta, el traspasador captura una imagen del documento mediante la utilización de la cámara del dispositivo de comunicación móvil 25 del traspasador.

El dispositivo de comunicación móvil 25 comprende una aplicación 9 que identifica el código de barras en 2D y extrae la almohadilla de metadatos, la ID del documento y los metadatos desde el código de barras en 2D.

El dispositivo de comunicación móvil 25 envía entonces una solicitud de verificación a través de la Internet 34 al servidor de verificación de documentos 19. La solicitud de verificación comprende la almohadilla pero, en modalidades, puede incluir adicionalmente la ID del documento.

El servidor de verificación de documentos 19 busca después a través de las transacciones de verificación de la cadena de bloques e identifica la transacción de verificación anterior creada.

El servidor de verificación de documentos 19 envía después una respuesta de verificación al dispositivo de comunicación móvil 25 de manera que el dispositivo de comunicación móvil 25 es capaz de mostrar una indicación de que existe un registro de verificación.

Ahora, en una modalidad, el dispositivo de comunicación móvil 25 del traspasador puede mostrar los metadatos extraídos desde el código de barras en 2D. Como tal, el traspasador puede inspeccionar visualmente los nombres de las partes y el número de lote en el documento como se muestra por el dispositivo de comunicación móvil 25 para asegurar su consistencia.

Debe observarse que el terminal de cliente 25 puede volver a crear la almohadilla de metadatos almacenada dentro del código de barras en 2D para confirmar si la almohadilla generada coincide con la

almohadilla del código de barras en 2D (para así evitar la falsificación de los metadatos dentro del código de barras).

Alternativamente, durante la transacción de verificación inicial, los metadatos pueden además haberse almacenado dentro de la cadena de bloques de manera que los metadatos pueden enviarse al terminal de cliente 25 desde el servidor de verificación de documentos 19 para la visualización.

En modalidades alternativas, contrariamente a la visualización de los campos de los metadatos para la comparación visual por el traspasador, el dispositivo de comunicación móvil puede realizar el reconocimiento óptico de caracteres para leer el texto del documento (a pesar de las anomalías de las fotocopias) y confirmar si el texto reconocido coincide con los metadatos.

Por ejemplo, para los metadatos almacenados dentro del código de barras en 2D o la cadena de bloques, el terminal de cliente 25 puede buscar el texto OCR para identificar tales metadatos. Si no se identifican, tal como el documento escaneado no contiene el mismo número de lote, entonces la verificación falla.

En modalidades, los metadatos relevantes se delimitan dentro de límites tal como en donde, por ejemplo, en la modalidad descrita anteriormente, el abogado dibuja rectángulos sobre los metadatos mostrados en la pantalla que van a verificarse. Por ejemplo, el número de lote puede estar en el medio del centro superior de la página mientras que los nombres de las partes pueden estar en las esquinas inferiores izquierda y derecha del documento respectivamente.

Como tal, durante la verificación, el dispositivo de comunicación móvil 25 se configura para el reconocimiento de texto solamente dentro de los límites acotados y luego comparar el texto extraído desde estos límites acotados contra los metadatos. Cuando se utiliza la cámara, el dispositivo de comunicación móvil 25 puede identificar las esquinas de la página para la orientación para así ser capaz de colocar con precisión los límites acotados.

Uso ilustrativo de la arquitectura del sistema 1 para la verificación de tarjetas de embarque

Ahora se describirá el uso ilustrativo del sistema para la verificación de tarjetas de embarque.

Específicamente, existen problemas con los sistemas de tarjetas de embarque existentes en que los datos impresos en las mismas pueden falsificarse. Adicionalmente, las entradas de la base de datos pueden modificarse para coincidir con la impresión falsificada de manera que, durante el check-in, el personal de embarque puede no notar una tarjeta de embarque que se ha falsificado para coincidir con una entrada de la base de datos modificada.

Como tal, en esta modalidad, cuando las tarjetas de embarque se imprimen inicialmente, el sistema informático de registro de pasajeros envía los metadatos relevantes al servidor de verificación de documentos 19.

En esta modalidad, los metadatos relevantes pueden incluir la ID de la tarjeta de embarque, el nombre del pasajero, y la puerta de salida.

El servidor de verificación de documentos 19 puede crear una almohadilla de los metadatos y crear una entrada dentro de la cadena de bloques y enviar un código de barras en 2D al sistema informático de registro de pasajeros que luego se imprime sobre la tarjeta de embarque.

Ahora, antes de la salida, la reprogramación del vuelo puede resultar en una actualización del número de la puerta. Como tal, el sistema informático de registro de pasajeros identifica todos los pasajeros afectados y, para esos pasajeros afectados identificados, envía una notificación de actualización al servidor de verificación de documentos 19.

Por ejemplo, para cada tarjeta de embarque, el sistema informático de registro de pasajeros puede enviar la ID de la tarjeta de embarque y el número de la puerta actualizado.

Para cada actualización, el servidor de verificación de documentos 19 crea una nueva entrada dentro de la cadena de bloques.

Ahora, durante el check-in, los códigos de barras en 2D de las tarjetas de embarque se escanean y la ID de la tarjeta de embarque, y los metadatos (el nombre del pasajero y el número de la puerta) se extraen desde los códigos de barras. Al final, tal información puede recuperarse además a través de OCR a partir de la impresión de la tarjeta de embarque.

Tales metadatos extraídos pueden enviarse después al servidor de verificación de documentos 19 para la verificación.

En modalidades, la computadora de la puerta de embarque puede mantener una copia de la cadena de bloques para evitar las búsquedas que requieren mucho tiempo a través de la Internet al servidor de verificación de documentos 19.

Ahora, al suponer que hubo un intento de sustituir un pasajero con otro nombre, la tarjeta de embarque puede haberse falsificado para cambiar el nombre impreso en la tarjeta de embarque y además la entrada asociada dentro de la base de datos del sistema informático de registro de pasajeros. Los metadatos almacenados dentro del código de barras en 2D pueden haberse modificado adicionalmente.

Sin embargo, para tal modificación del nombre, la verificación por el servidor de verificación de documentos 19 podría fallar ya que el servidor de verificación de documentos 19 podría fallar en hacer coincidir una almohadilla del nuevo nombre contra una almohadilla almacenada dentro de la cadena de bloques.

Ahora, para el número de la puerta actualizado, la tarjeta de embarque puede representar aún el número de la puerta anterior.

Como tal, la almohadilla codificada dentro del código de barras en 2D estaría obsoleta (ya que aún representa el número de la puerta anterior).

Sin embargo, en el check-in, el nuevo número de la puerta puede enviarse por la computadora de comprobación de pasajeros al servidor de verificación de documentos 19 en donde el servidor de verificación de documentos 19 es capaz de identificar una transacción de verificación adicional con relación a la ID de la tarjeta de embarque con el nuevo número de la puerta y por lo tanto, aprobar la verificación

de la tarjeta de embarque. Con respecto a esto, debe observarse que la verificación podría fallar para cualquier otro número de puerta proporcionado que no coincida con la transacción de actualización de la puerta dentro de la cadena de bloques.

Interpretación
Inalámbrica:

La invención puede llevarse a la práctica mediante el uso de dispositivos que cumplen con otros estándares de red y para otras aplicaciones, que incluyen, por ejemplo otros estándares WLAN y otros estándares inalámbricos. Las aplicaciones que pueden acomodarse incluyen LAN inalámbrica IEEE 802.11 y enlaces, y Ethernet inalámbrica.

En el contexto de este documento, el término “inalámbrica” y sus derivados pueden usarse para describir circuitos, dispositivos, sistemas, métodos, técnicas, canales de comunicación, etc., que pueden comunicar datos a través del uso de radiación electromagnética modulada a través de un medio no sólido. El término no implica que los dispositivos asociados no contengan ningún cable, aunque en algunas modalidades pueden no tener. En el contexto de este documento, el término “cableado” y sus derivados pueden usarse para describir circuitos, dispositivos, sistemas, métodos, técnicas, canales de comunicación, etc., que pueden comunicar datos a través del uso de radiación electromagnética modulada a través de un medio sólido. El término no implica que los dispositivos asociados se acoplen por cables eléctricamente conductores.

Procesos:

A menos que se indique específicamente de cualquier otra manera, como es evidente a partir de las descripciones que siguen, se

aprecia que a lo largo de las descripciones que utilizan los términos tales como, "procesar", "computar", "calcular", "determinar", "analizar" o similares, se refieren a la acción y/o procesos de una computadora o un sistema informático, o un dispositivo informático electrónico similar, que manipulan y/o transforman los datos representados como físicos, tal como cantidades electrónicas, en otros datos representados similarmente como cantidades físicas.

Procesador:

De manera similar, el término "procesador" puede referirse a cualquier dispositivo o parte de un dispositivo que procesa datos electrónicos, por ejemplo, de registros y/o memoria para transformar esos datos electrónicos en otros datos electrónicos que, por ejemplo, pueden almacenarse en registros y/o memoria. Una “computadora” o un “dispositivo informático” o una “máquina informática” o una “plataforma informática” pueden incluir uno o más procesadores.

Las metodologías descritas en la presente descripción, en una modalidad, pueden realizarse por uno o más procesadores que aceptan código legible por computadora (llamado también como legible por máquina) que contiene un conjunto de instrucciones que cuando se ejecutan por uno o más de los procesadores llevan a cabo al menos uno de los métodos descritos en la presente descripción. Se incluye cualquier procesador capaz de ejecutar un conjunto de instrucciones (secuenciales o de cualquier otra manera) que especifican acciones que se van a tomar. Por lo tanto, un ejemplo es un sistema de procesamiento típico que incluye uno o más procesadores. El sistema de procesamiento puede incluir además un subsistema de memoria que incluye una RAM principal y/o una RAM estática, y/o una ROM.

Medio legible por computadora:

Además, un medio portador legible por computadora puede formarse, o incluirse en un producto de programa informático. Un producto de programa informático puede almacenarse en un medio portador que puede usarse por computadora, el producto de programa informático que comprende un medio de programa legible por computadora para hacer que un procesador realice un método como se describe en la presente descripción.

Procesadores en red o múltiples:

En modalidades alternativas, el uno o más procesadores funcionan como un dispositivo independiente o pueden conectarse, por ejemplo, en red a otro(s) procesador(es), en una implementación en red, el uno o más procesadores pueden operar en la capacidad de un servidor o una máquina del cliente en el entorno de red servidor-cliente, o como una máquina par en un entorno de red distribuida o punto a punto. El uno o más procesadores pueden formar un aparato de red, un enrutador de red, conmutador o enlace, o cualquier máquina capaz de ejecutar un conjunto de instrucciones (secuenciales o de cualquier otra manera) que especifican las acciones que se van a tomar por la máquina.

Debe observarse que aunque algún(algunos) diagrama(s) solamente muestra(n) un único procesador y una única memoria que lleva el código legible por computadora, los expertos en la técnica entenderán que muchos de los componentes descritos anteriormente se incluye, pero no se muestran o describen explícitamente con el fin de ensombrecer el aspecto inventivo. Por ejemplo, aunque solamente se ilustra una única máquina, el término "máquina" también se tomará

para incluir cualquier colección de máquinas que ejecutan individualmente o en conjunto un conjunto (o múltiples conjuntos) de instrucciones para realizar cualquiera o más de las metodologías descritas en la presente descripción.

Modalidades adicionales:

Por lo tanto, una modalidad de cada uno de los métodos descritos en la presente descripción tiene la forma de un medio portador legible por computadora que lleva un conjunto de instrucciones, por ejemplo, un programa informático para la ejecución en uno o más procesadores. Por lo tanto, como se apreciará por los expertos en la técnica, las modalidades de la presente invención pueden llevarse a la práctica como un método, un aparato tal como un aparato de propósito específico, un aparato tal como un sistema de procesamiento de datos, o un medio portador legible por computadora. El medio portador legible por computadora lleva el código legible por computadora que incluye un conjunto de instrucciones que cuando se ejecutan en uno o más procesadores hace que un procesador o procesadores implementen un método. En consecuencia, los aspectos de la presente invención pueden tomar la forma de un método, una modalidad completamente de hardware, una modalidad completamente de software, o una modalidad que combina aspectos de software y hardware. Además, la presente invención puede tener la forma de un medio portador (por ejemplo, un producto de programa informático en un medio de almacenamiento legible por computadora) que lleva el código del programa legible por computadora incorporado en el medio.

Medio portador:

El software puede transmitirse o recibirse adicionalmente por una red a través de un dispositivo de interfaz de red. Aunque el medio portador se muestra en una modalidad ilustrativa como que es un único medio, el término "medio portador" debe tomarse para incluir un único medio o múltiples medios (por ejemplo, una base de datos centralizada o distribuida, y/o memorias cachés asociadas y servidores) que almacenan uno o más conjuntos de instrucciones. El término “medio portador” deberá tomarse además para incluir cualquier medio que es capaz de almacenar, codificar o transportar un conjunto de instrucciones para la ejecución por uno o más de los procesadores, y que hacen que el uno o más procesadores realicen cualquiera o más de las metodologías de la presente invención. Un medio portador puede tomar muchas formas, que incluyen pero no se limitan a, medios no volátiles, medios volátiles, y medios de transmisión.

Implementación:

Se debe entender que las etapas de los métodos descritos se realizan en una modalidad mediante un procesador adecuado (o procesadores) de un sistema de procesamiento (es decir, computadora) que ejecuta las instrucciones (código legible por computadora) almacenadas en el almacenamiento. Se debe entender además que la invención no se limita a ninguna implementación o técnica de programación particular y que la invención puede implementarse mediante el uso de cualquier técnica adecuada para implementar la funcionalidad descrita en la presente descripción. La invención no se limita a ningún lenguaje de programación o sistema operativo particular.

Medio para llevar a cabo un método o función

Además, algunas de las modalidades se describen en la presente descripción como un método o combinación de los elementos de un método que pueden implementarse por un procesador de un dispositivo procesador, sistema de computadora, o mediante otro medio para llevar a cabo la función. Por lo tanto, un procesador con las instrucciones necesarias para llevar a cabo un método o elemento de un método forma un medio para llevar a cabo el método o elemento de un método. Además, un elemento descrito en la presente descripción de la modalidad de un aparato es un ejemplo de un medio para llevar a cabo la función realizada por el elemento con el fin de llevar a cabo la invención.

Conectado

De manera similar, debe observarse que el término conectado, cuando se usa en las reivindicaciones, no debe interpretarse como que es limitativo solamente a conexiones directas. Por lo tanto, el alcance de la expresión un dispositivo A conectado a un dispositivo B no debe limitarse a dispositivos o sistemas en donde una salida del dispositivo A se conecta directamente a una entrada del dispositivo B. Esto significa que existe una trayectoria entre una salida de A y una entrada de B que puede ser una trayectoria que incluye otros dispositivos o medios. “Conectado” puede significar que dos o más elementos están en contacto físico o eléctrico directo, o que dos o más elementos no están en contacto directo entre sí pero aun así cooperan o interactúan entre sí.

Modalidades:

La referencia a lo largo de esta descripción a "una modalidad" o "la modalidad" significa que un rasgo, estructura o característica

particular que se describe en relación con la modalidad se incluye en al menos una modalidad de la presente invención. Así, las apariciones de las frases "en una modalidad" o "en la modalidad" en varios lugares a lo largo de esta descripción no se refieren necesariamente todas a la misma modalidad, pero pudieran. Además, los rasgos particulares, estructuras o características pueden combinarse de cualquier manera adecuada, como sería evidente para un experto en la técnica a partir de esta descripción, en una o más modalidades.

De manera similar debe apreciarse que en la descripción anterior de las modalidades ilustrativas de la invención, varias características de la invención a veces se agrupan juntas en una sola modalidad, Figura o descripción de la misma con el propósito de racionalizar la descripción y ayudar en la comprensión de uno o más de los diversos aspectos inventivos. Este método de descripción, sin embargo, no debe interpretarse como el reflejo de una intención de que la invención reivindicada requiere más características que se enumeran expresamente en cada reivindicación. Más bien, como reflejan las siguientes reivindicaciones, los aspectos inventivos descansan en menos de todas las características de una sola modalidad descrita con anterioridad. Por lo tanto, las reivindicaciones que siguen a la descripción detallada de las modalidades específicas se incorporan expresamente aquí dentro de esta descripción detallada de las modalidades específicas, con cada reivindicación que aparece por sí sola como una modalidad separada de esta invención.

Además, aunque algunas modalidades descritas en la presente descripción incluyen algunos pero no otros elementos incluidos en otras modalidades, las combinaciones de elementos de diferentes modalidades se entiende que están dentro del alcance de la invención, y forman diferentes modalidades, como podría entenderse por los

expertos en la técnica. Por ejemplo, en las siguientes reivindicaciones, cualquiera de las modalidades reivindicadas puede usarse en cualquier combinación.

Diferentes ejemplos de objetos

Como se usa en la presente descripción, a menos que se especifique de otra manera el uso de los adjetivos ordinales “primero”, “segundo”, “tercero”, etc., para describir un objeto común, simplemente indica que se referencian diferentes ejemplos de objetos iguales, y no pretende implicar que los objetos así descritos deben estar en una secuencia dada, ya sea de manera temporal, espacial, en clasificación, o de cualquier otra manera.

Detalles específicos

En la descripción proporcionada en la presente invención, se exponen numerosos detalles específicos. Sin embargo, se entiende que las modalidades de la invención pueden llevarse a la práctica sin estos detalles específicos. En otros casos, métodos, estructuras y técnicas bien conocidos no se han mostrado en detalle para no ensombrecer una comprensión de esta descripción.

Terminología

En la descripción de la modalidad preferida de la invención ilustrada en los dibujos, se recurrirá a terminología específica por el bien de la claridad. Sin embargo, la invención no pretende limitarse a los términos específicos así seleccionados, y debe entenderse que cada término específico incluye todos los equivalentes técnicos que operan de manera similar para lograr un propósito técnico similar. Los

términos tal como “hacia adelante”, “hacia atrás”, “radialmente”, “periféricamente”, “hacia arriba”, “hacia abajo”, y similares se usan como palabras de conveniencia para proporcionar puntos de referencia y no deben interpretarse como términos limitantes.

Que comprende y que incluye

En las reivindicaciones que siguen y en la descripción anterior de la invención, excepto cuando el contexto requiere otra cosa debido al lenguaje expreso o implicación necesaria, la palabra "comprender" o variaciones tales como "comprende" o "que comprende" se usan en un sentido inclusivo, es decir, para especificar la presencia de las características indicadas pero no para excluir la presencia o adición de características adicionales en varias modalidades de la invención.

Cualquiera de los términos: que incluyen o que incluye o como se usa en la presente descripción es además un término abierto que también significa que incluye al menos los elementos/características que siguen al término, pero que no excluye otros. Por lo tanto, que incluye es sinónimo y significa que comprende.

Alcance de la invención

Por lo tanto, aunque se ha descrito lo que se cree que son las modalidades preferidas de la invención, los expertos en la técnica reconocerán que otras y modificaciones adicionales pueden realizarse en la misma sin apartarse del espíritu de la invención, y se pretende reivindicar todos estos cambios y modificaciones que caen dentro del alcance de la invención. Por ejemplo, cualquier fórmula dada anteriormente es simplemente representativa de procedimientos que pueden usarse. La funcionalidad puede agregarse o eliminarse de los

diagramas de bloques y las operaciones pueden intercambiarse entre bloques funcionales. Las etapas pueden añadirse o eliminarse a los métodos descritos dentro del alcance de la presente invención.

Aunque la invención se ha descrito con referencia a ejemplos específicos, se apreciará por los expertos en la técnica que la invención puede llevarse a la práctica de muchas otras formas.

REIVINDICACIONES

1. Un método para la verificación de la autenticidad de la información de documentos, el método que comprende:

una etapa de creación de registros de verificación que comprende:

recibir los metadatos del contenido del documento desde un documento;

generar una almohadilla de metadatos mediante el uso de los metadatos del contenido del documento;

crear una transacción de cadena de bloques que comprende la almohadilla de metadatos;

generar los datos legibles por computadora que codifican la almohadilla de metadatos; y

actualizar el documento con los datos legibles por computadora; y

una etapa de verificación de documentos que comprende:

recibir el documento;

extraer la almohadilla de metadatos a partir de los datos legibles por computadora; e

identificar la almohadilla de metadatos dentro de las transacciones de cadenas de bloques para verificar la autenticidad de los metadatos del documento.

2. Un método como se reivindicó en la reivindicación 1, en donde los datos legibles por computadora son un código de barras.

3. Un método como se reivindicó en la reivindicación 2, en donde el código de barras es un código de barras de dos dimensiones.

4. Un método como se reivindicó en la reivindicación 1, en donde la etapa de registro de verificación comprende además firmar el documento con una clave privada asociada con un servidor de verificación de documentos.

5. Un método como se reivindicó en la reivindicación 1, que comprende además almacenar los metadatos del contenido del documento de manera que la etapa de verificación de documentos comprende además recuperar los metadatos del contenido del documento y mostrar los metadatos del contenido del documento.

6. Un método como se reivindicó en la reivindicación 5, en donde almacenar los metadatos del contenido del documento comprende codificar los metadatos dentro de los datos legibles por computadora.

7. Un método como se reivindicó en la reivindicación 5, en donde almacenar los metadatos del contenido del documento comprende codificar los metadatos dentro de la transacción de la cadena de bloques.

8. Un método como se reivindicó en la reivindicación 1, en donde la etapa de creación de registros de verificación comprende además la identificación de los metadatos del contenido del documento desde el documento.

9. Un método como se reivindicó en la reivindicación 8, en donde la identificación de los metadatos del contenido del documento comprende el reconocimiento óptico de caracteres.

10. Un método como se reivindicó en la reivindicación 9, en donde la identificación de los metadatos del contenido del documento

comprende la realización de consultas de búsqueda de cadenas contra el texto extraído mediante el uso del reconocimiento óptico de caracteres.

11. Un método como se reivindicó en la reivindicación 9, en donde la identificación de los metadatos del contenido del documento comprende el aislamiento del texto dentro de al menos una región del documento definida por el usuario.

12. Un método como se reivindicó en la reivindicación 1, que comprende además una etapa de actualización del contenido del documento que comprende:

recibir los metadatos del contenido del documento actualizado para el documento;

generar una nueva almohadilla de metadatos mediante el uso de los metadatos del documento actualizado;

crear una transacción de la cadena de bloques adicional que comprende la nueva almohadilla de metadatos.

13. Un método como se reivindicó en la reivindicación 12, en donde la etapa de verificación de documentos comprende:

identificar dos o más transacciones de cadenas de bloques asociadas con el documento.

14. Un método como se reivindicó en la reivindicación 13, en donde la etapa de verificación de documentos comprende además identificar que los metadatos del contenido del documento se suplantaron por los metadatos del contenido del documento actualizado.

15. Un método como se reivindicó en la reivindicación 14, que comprende además identificar que parte del documento está suplantada.

16. Un método como se reivindicó en la reivindicación 1, que comprende además una etapa de revocación de la verificación de documentos que comprende:

crear una transacción de la cadena de bloques de revocación de manera que, durante la etapa de verificación de documentos, el método comprende además:

identificar la transacción de la cadena de bloques de revocación posterior en el tiempo a la transacción de la cadena de bloques para fallar en la verificación de la autenticidad de la información del documento.

17. Un método como se reivindicó en la reivindicación 1, en donde la transacción de la cadena de bloques especifica además un período de validez, de manera que, durante la etapa de verificación de documentos, el método comprende además fallar en la verificación del documento si el período de validez ha expirado.

18. Un método como se reivindicó en la reivindicación 17, que comprende además crear una transacción de la cadena de bloques de renovación del período de validez que comprende un período de validez adicional de manera que, durante la etapa de verificación de documentos, el período de validez adicional se usa cuando se determina la validez del documento.

19. Un sistema para la verificación de la autenticidad de la información de documentos, el sistema que comprende:

un servidor de verificación de información de documentos, el servidor de verificación de información de documentos que comprende:

una base de datos que comprende:

una cadena de bloques de almohadillas; y

una tabla de los metadatos del documento almacenada con relación a la cadena de bloques de almohadillas unidireccional;

módulos de software que comprenden:

un módulo de creación de documentos; y

un módulo de verificación de la información del documento;

un terminal de cliente en comunicación operable con el servidor de verificación de información de documentos, el terminal de cliente que comprende:

un lector de datos legibles por computadora;

una aplicación de software en comunicación operable con el lector de datos legibles por computadora, la aplicación de software que comprende:

un módulo de verificación de la información del documento;

en donde, en uso, el sistema se configura para

una etapa de creación de registros de verificación que comprende:

el módulo de creación de documentos del servidor de verificación de información de documentos:

recibir los metadatos del documento con relación a un documento;

recibir o generar una almohadilla unidireccional a partir de los metadatos del documento mediante el uso de un algoritmo de creación de almohadillas;

crear una entrada en la cadena de bloques de almohadillas unidireccional para la almohadilla unidireccional;

generar datos legibles por computadora que comprenden al menos uno de los metadatos del documento y la almohadilla unidireccional; y

enviar los datos legibles por computadora al módulo de creación de documentos; y

una etapa de verificación de información de documentos que comprende:

el módulo de verificación de información de documentos del terminal de cliente que recibe los datos legibles por computadora desde un documento;

al menos uno del terminal de cliente y el servidor de verificación de información de documentos que identifica al menos uno de los metadatos del documento y la almohadilla unidireccional a partir de los datos legibles por computadora en donde, si se reciben solamente los metadatos del documento, generar la almohadilla unidireccional mediante el uso de un algoritmo de creación de almohadillas unidireccional; y

el módulo de verificación de información de documentos del servidor de verificación de información de documentos que verifica el documento mediante la comparación de la almohadilla unidireccional con la entrada en la cadena de bloques de almohadillas para la almohadilla unidireccional.

20. Un sistema como se reivindicó en la reivindicación 19, en donde el sistema comprende además un servidor emisor de documentos en comunicación operable con el servidor de verificación de información de documentos.

21. Un sistema como se reivindicó en la reivindicación 20, en donde el servidor de verificación de información de documentos se configura para recibir los metadatos del documento desde el servidor emisor de documentos.

22. Un sistema como se reivindicó en la reivindicación 20, en donde la etapa de verificación de información de documentos comprende además al menos uno del terminal de cliente y el servidor de verificación de información de documentos que envía al menos uno de la almohadilla unidireccional y los metadatos del documento al servidor emisor de documentos para la verificación adicional del documento.

23. Un sistema como se reivindicó en la reivindicación 22, en donde el servidor emisor de documentos comprende una base de datos que comprende al menos uno de la almohadilla y los metadatos y en donde la verificación adicional comprende la referencia cruzada con al menos uno de la almohadilla y los metadatos dentro de la base de datos del servidor emisor de documentos.

24. Un sistema como se reivindicó en la reivindicación 19, en donde el módulo de verificación de información de documentos del servidor de verificación de información de documentos se configura además para enviar un resultado de verificación al terminal de cliente.

25. Un sistema como se reivindicó en la reivindicación 24, en donde la aplicación de software del terminal de cliente se configura además para generar una interfaz de usuario gráfica y en donde la interfaz de usuario gráfica se configura para mostrar el resultado de la verificación.

26. Un sistema como se reivindicó en la reivindicación 25, en donde la interfaz de usuario gráfica se configura además para mostrar al menos un subconjunto de los metadatos del documento.

27. Un sistema como se reivindicó en la reivindicación 19, en donde el sistema comprende una pluralidad de servidores de verificación de información de documentos y en donde la cadena de bloques es una cadena de bloques distribuida a través de la pluralidad de servidores de verificación de información de documentos.

28. Un sistema como se reivindicó en la reivindicación 19, en donde crear los datos legibles por computadora comprende crear datos ópticos legibles por computadora.

29. Un sistema como se reivindicó en la reivindicación 28, en donde los datos legibles por computadora son un código de barras en 2-D.

30. Un sistema como se reivindicó en la reivindicación 19, que comprende además insertar los datos legibles por computadora en el documento.

RESUMEN

Se proporciona un sistema y método para la verificación de la autenticidad de la información de documentos para aplicaciones que incluyen verificar la autenticidad de la información de las declaraciones de logro de la documentación de cursos emitidos por organizaciones de formación registradas, la verificación de documentos de viaje y otros documentos sensibles que requieren la verificación de autenticidad tal como los documentos emitidos por bufetes de abogados, firmas contables, instituciones gubernamentales y similares. El método puede comprender una etapa de creación de registros de verificación que comprende: recibir los metadatos del contenido del documento desde un documento; generar una almohadilla de metadatos mediante el uso de los metadatos del contenido del documento; crear una transacción de cadena de bloques que comprende la almohadilla de metadatos; y generar datos legibles por computadora que codifican la almohadilla de metadatos; actualizar el documento con los datos legibles por computadora y una etapa de verificación de documentos que comprende: recibir el documento; extraer la almohadilla de metadatos a partir de los datos legibles por computadora; e identificar la almohadilla de metadatos dentro de las transacciones de cadenas de bloques para verificar la autenticidad de los metadatos del documento