(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 021 818**

(51) Int. Cl.:

G06F 21/62 (2013.01)
G06F 16/21 (2009.01)
G06F 16/93 (2009.01)
H04L 9/32 (2006.01)
G06F 21/16 (2013.01)
G06Q 10/10 (2013.01)
H04L 9/40 (2012.01)
H04L 9/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.09.2021 PCT/EP2021/076095**

(87) Fecha y número de publicación internacional: **31.03.2022 WO22063844**

(96) Fecha de presentación y número de la solicitud europea: **22.09.2021 E 21783174 (2)**

(97) Fecha y número de publicación de la concesión europea: **01.01.2025 EP 4217898**

(54) Título: **Procedimiento y plataforma para la trazabilidad de un documento adjunto generado por un tercero a partir de un documento original a través de un sistema de cadena de bloques**

(30) Prioridad:

24.09.2020 FR 2009747

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.05.2025

(73) Titular/es:

DAVRON DIGITAL (100.00%)
8 Avenue Hoche
75008 Paris, FR

(72) Inventor/es:

DAVRON, ANNE-CÉCILE y
DAVRON, DAVID

(74) Agente/Representante:

ESPIELL GÓMEZ, Ignacio

DESCRIPCIÓN

Procedimiento y plataforma para la trazabilidad de un documento adjunto generado por un tercero a partir de un documento original a través de un sistema de cadena de bloques.

La presente invención se refiere a la trazabilidad de un documento adjunto generado por un tercero a partir de un documento original a través de un sistema de cadena de bloques.

Tiene una aplicación general en el establecimiento de un procedimiento de trazabilidad fehaciente de un documento destinado a ser tramitado por varios terceros, y más concretamente en el caso de procedimientos de legalización o apostilla por parte de autoridades habilitadas que requieran la comprobación de la autenticidad de las escrituras y documentos presentados.

Por tramitación de documentos se entiende aquí cualquier trámite informático de un documento digital perteneciente, sin carácter excluyente, al grupo formado por traducción, legalización, apostilla, documentación adjunta u otros trámites análogos.

En general, el procedimiento de legalización/apostilla requiere que un documento digital se someta a varias etapas de validación, a cargo de varios intervinientes/terceros de distinta naturaleza, tales como empresas, asociaciones, notarías, cámaras de comercio, ministerios de asuntos exteriores, consulados, ayuntamientos, traductores jurados y otros.

Las firmas electrónicas suelen realizarse de forma independiente entre sí. Los terceros firmantes de los documentos no tienen necesariamente conocimiento de la etapa de tramitación anterior o siguiente y en principio no se consultan entre sí.

Además, ciertos trámites se realizan físicamente sobre un documento, y dicho documento es escaneado y añadido por el autor de dicho trámite, lo que representa una dificultad adicional de autentificación con respecto a un documento de origen digital.

Cuantas más personas intervienen, más difícil, si no imposible, resulta rastrear el recorrido del documento en su totalidad y demostrar la correcta realización de cada etapa de la tramitación.

La dificultad de la trazabilidad es aún mayor si cabe cuando hay que anexar documentos adjuntos al original, tales como una traducción o un documento adjunto asociado a un documento original.

La dificultad de la trazabilidad se complica aún más si cabe por la variedad de normas técnicas aplicadas a la firma electrónica, así como por la gran variedad de proveedores de soluciones informáticas, muy a menudo incompatibles entre sí.

De hecho, cuando varios agentes tienen que firmar un mismo documento con diferentes soluciones de firma electrónica, ello puede causar un problema de compatibilidad entre programas informáticos de firma electrónica, como la sobreescritura de la(s) firma(s) anterior(es) en caso de firma con un programa informático diferente, de firma a posteriori, o de firma de un tercero respecto al contrato.

Además, la firma electrónica secuencial por parte de diferentes agentes presenta dificultades de uso, como la instalación local de programas de firma electrónica, la descarga del documento, la firma local y la exportación del documento firmado.

Ya se conocen procedimientos para verificar activamente la autenticidad de un documento almacenado analizando el documento y generando un acceso seguro correspondiente a una transacción almacenada en un sistema de cadena de bloques.

Sin embargo, estos procedimientos de un estadio anterior de la técnica no permiten establecer la trazabilidad de la autenticidad de un documento original que haya sido sometido a una sucesión de trámites por distintos terceros, ni establecer una comprobación o medio de prueba cuando concurran anexos como traducciones o apostillas adjuntados por el tercero a los documentos originales.

La presente invención subsana dichos inconvenientes.

Se refiere a un procedimiento de trazabilidad de un documento adjunto generado por un tercero a partir de un documento original a través de un sistema de cadena de bloques.

Según una definición general de la invención, el procedimiento de trazabilidad incluye las siguientes etapas:

- una etapa de inicialización que incluye el registro y análisis del documento original para obtener metadatos de inicialización que incluyen metadatos intrínsecos del documento original y metadatos extrínsecos que incluyen huellas digitales del documento original, de su contenido y de metadatos relacionados con el

documento original, depositándose los metadatos de inicialización en un contrato inteligente del sistema de cadena de bloques;

- una etapa de tramitación por parte del tercero que abarca la generación del documento adjunto por parte del tercero, el propio documento adjunto generado y el documento original recibido por el tercero para su tramitación, firmados ambos electrónicamente por el tercero con constancia de las huellas digitales de referencia del documento de referencia al que se adjunta y de su contenido extraído para la firma; y

- una etapa de recepción procedente del tercero que incluye el registro y análisis del documento original y del documento adjunto recibidos firmados procedentes del tercero para obtener datos de recepción que incluyen metadatos intrínsecos del documento original y huellas digitales del documento original recibido, del documento adjunto y del documento de referencia y de sus respectivos contenidos, así como metadatos en relación con el documento original y el documento adjunto, depositándose los metadatos de recepción en otro contrato inteligente del sistema de cadena de bloques;

- un contrato inteligente así archivado tras cada etapa de inicialización y tras cada etapa de recepción, lo que permite constituir una pista de auditoría y de trazabilidad del documento adjunto generado por el tercero a partir del documento original.

Gracias a la invención, la pista de auditoría así constituida, consolidada, provista de sello de tiempo y firmada en un sistema de cadena de bloques, por ejemplo público, es accesible por las autoridades competentes para la verificación y comprobación de la autenticidad del documento adjunto generado por un tercero a partir del documento original, así como del estado del documento original en cualquier momento del procedimiento (inicialización, tramitación y recepción).

Según una forma de realización, el procedimiento incluye asimismo una etapa de envío del documento original al tercero, mediante la cual los metadatos intrínsecos del documento original y los metadatos extrínsecos que incluyen las huellas digitales del documento original, de su contenido y de los metadatos relacionados con el documento original se depositan en un contrato inteligente del sistema de cadena de bloques.

Ventajosamente, los metadatos así obtenidos en cada etapa de inicialización, envío y recepción se almacenan en una base de datos para luego asociarse en un árbol de Merkle, cuyo hash raíz se deposita en el sistema de cadena de bloques.

Por ejemplo, los metadatos intrínsecos pertenecen al grupo formado por tipo, nombre, tamaño, fecha de registro e identificador de usuario.

En la práctica, las huellas digitales se calculan según una función hash elegida, por ejemplo SHA 256.

Según otra forma de realización, el documento adjunto pertenece al grupo formado por documento traducido, documento digital que contenga una legalización, documento digital apostillado.

La invención también se refiere a una plataforma para la trazabilidad de un documento adjunto generado por un tercero a partir de un documento original correspondiente mediante una herramienta interactiva a través de un sistema de cadena de bloques, para la implementación del procedimiento según la invención.

Según otro aspecto de la invención, la plataforma incluye:

- medios de registro y análisis del documento original para obtener metadatos de inicialización que incluyan metadatos intrínsecos del documento original y metadatos extrínsecos que incluyan huellas digitales del documento original, de su contenido y de metadatos relacionados con el documento original;

- -medios de recepción procedentes del tercero que incluyan medios de registro y análisis del documento original y del documento adjunto así recibidos firmados procedentes del tercero para obtener datos de recepción que incluyen metadatos intrínsecos del documento original y huellas digitales del documento original recibido, del documento adjunto y del documento de referencia y de sus contenidos respectivos, así como metadatos en relación con el documento original y el documento adjunto;

- medios para depositar los metadatos de inicio y los metadatos de recepción en un contrato inteligente respectivo del sistema de cadena de bloques.

Según otra forma de realización de la invención, la plataforma incluye un módulo aplicativo capaz de registrar los parámetros de tramitación del documento deseados por un usuario, capaz de identificar al menos un trámite necesario, capaz de seleccionar para cada tipo de trámite necesario al menos un tercero en cada base de datos necesaria, y

capaz de permitir la invocación del tercero adicional siguiente tras la tramitación y registro del documento tramitado por el tercero corriente.

El procedimiento según la invención permite trazar en su totalidad el recorrido del documento original y de cualquier anexo o adjunto correspondiente generado durante uno o varios trámites, y acreditar la correcta realización de cada una de las etapas de tramitación, a la vez que la integración de múltiples terceros en la cadena de tramitación, así como resuelve el problema de disparidad de normas utilizadas por cada uno de los terceros.

Ventajosamente, la incorporación de la información objeto del procedimiento según la invención a un contrato inteligente depositado en un sistema de cadena de bloques permite también la fijación de la información depositada en cuanto a los metadatos de los documentos, sus huellas digitales en cualquier estadio de la tramitación y, por ende, garantiza la consolidación de la información que forma la pista de auditoría para las entidades que verifican la autenticidad de los documentos.

Otras características y ventajas de la invención se desprenderán de la siguiente descripción detallada y de los dibujos y tablas en que:

la **[fig. 1]** describe esquemáticamente las etapas del procedimiento de trazabilidad según la invención;

la **[fig. 2]** describe esquemáticamente una forma de realización concreta del procedimiento de trazabilidad según la invención;

la **[fig. 3]** describe esquemáticamente las subetapas de la etapa de inicialización según la invención;

la **[fig. 4]** muestra esquemáticamente un ejemplo concreto de la etapa de tramitación según la invención;

la **[fig. 5];** describe esquemáticamente una forma de realización de los datos almacenados en las subetapas de almacenamiento en un sistema de bloques del procedimiento según la invención;

la **[fig. 6]** describe esquemáticamente una forma de realización concreta de los metadatos intrínsecos recabados durante la implementación del procedimiento según la invención;

la **[fig. 7]** describe esquemáticamente la arquitectura de hardware de la plataforma según la invención; y

la **[fig. 8]** describe esquemáticamente las funciones del módulo aplicativo de la plataforma según la invención.

En referencia a las figuras 1 a 5, el procedimiento de trazabilidad de acuerdo con la invención incluye una sucesión de etapas en la siguiente secuencia: una etapa de inicialización S0 encaminada a analizar, calcular y registrar la información de un documento original D1 de una transacción en un sistema de cadena de bloques B para establecer el primer eslabón de la cadena de trazabilidad; una etapa de tramitación S1, realizada por un tercero 100, que incorpora la generación de un documento original firmado electrónicamente, así como un documento adjunto DA del documento original firmado D2, y una etapa de recepción S2 procedente del tercero 100 que incluye el registro y análisis de los documentos D2 y DA generados durante el trámite S1, y el cálculo de las huellas digitales electrónicas correspondientes que se almacenarán en un sistema de cadena de bloques B.

Según una primera etapa de inicialización S0, un usuario registra un documento original D1 digital. A continuación, se analiza el documento original D1 para obtener los datos sobre su contenido visible, así como metadatos de inicialización.

En la práctica, los datos de contenido visibles pertenecen, sin carácter excluyente, al grupo formado por texto, imagen, objeto digital integrado al documento D1, o datos similares.

Según una forma de realización de la invención, la subetapa de análisis del documento original D1 incluye una herramienta de reconocimiento de texto, que permite la extracción en forma de texto de cualquier contenido textual reconocido dentro del documento.

A título de ejemplo no limitativo, la herramienta de reconocimiento de texto pertenece al grupo formado por reconocimiento de voz de archivos originales de audio y vídeo, reconocimiento visual óptico de caracteres de archivos de imagen.

Entre los metadatos obtenidos figuran metadatos intrínsecos del documento original D1 y metadatos extrínsecos del documento original D1.

Los metadatos intrínsecos MID1 del documento original D1 pertenecen al grupo formado sin carácter limitativo por nombre del documento, tamaño, datos de firmas electrónicas, de certificado, identificación del proyecto, objeto adjunto, número de procedimiento.

A modo de ejemplo no limitativo, los metadatos intrínsecos de un documento pertenecen al grupo formado por tipo de documento, tipo de trámite, identidad del tercero firmante, firma(s) electrónica(s) y certificado(s) correspondiente(s), validez de certificado(s) a la fecha de firma, título, autor(es), empresa, fecha, lugar, idioma de origen, país de emisión.

Alternativamente, si el documento es un adjunto de un documento tramitado, los metadatos intrínsecos pertenecen, sin carácter limitativo, al grupo formado por tipo de documento, idioma de destino, país de destino, función del tercero 100, autoridad bajo la que opera el tercero 100, firma(s) electrónica(s) y certificados correspondientes del tercero 100, identidad de tercero(s) firmante(s), firma(s) electrónica(s) y certificados correspondientes, validez de certificado(s) a la fecha de la firma, título, fecha, lugar, naturaleza del sello o timbre.

Los metadatos extrínsecos MED1 del documento original D1 se definen como los metadatos generados por la aplicación que implementa el procedimiento según la invención, y que incluyen al menos el sellado de tiempo del registro por parte del usuario, así como el identificador del usuario que ha realizado el registro de dicho documento original D1.

Según una subetapa de la etapa de inicialización S0 del procedimiento según la invención, se calculan huellas digitales seleccionadas que definen metadatos extrínsecos del documento original D1 que se va a generar.

En la práctica, se aplica una función hash elegida para calcular las huellas digitales.

Por ejemplo, las huellas digitales se calculan utilizando una función hash SHA 256.

La subetapa de cálculo de la etapa de inicialización S0 según la invención incluye el cálculo de la huella digital del documento original HD1, de la huella digital HB1 del contenido analizado, así como la huella digital HM1 de los metadatos intrínsecos relacionados con el documento original D1.

Según una última subetapa de la etapa de inicialización S0, las huellas digitales HD1, HB1, HM1 así calculadas, así como los metadatos intrínsecos extraídos y extrínsecos generados se almacenan en una transacción mediante un contrato inteligente B1, dentro de un sistema de cadena de bloques B.

[Tabla 1]

CARGA INICIAL	
Tipo	Original para legalizar
Nombre	REGISTRO MERCANTIL EMPRESA PDF
Tamaño	17Kb
Fecha de carga	08/09/2020 a 11:10 am
Carga de usuario IS	ABL
HD1	3j4XH
HB1	Lolp3
HM1	X059
Datos de firmas	N/A
ID «PROYECTO» interno Davron	7

El procedimiento de trazabilidad según la invención incluye además una etapa de tramitación S1 por un tercero 100.

Se entiende por tercero cualquier agente habilitado para llevar a cabo un trámite seleccionado.

A modo de ejemplo no limitativo, el tercero 100 puede ser un notario, un traductor jurado, una entidad gubernamental nacional o extranjera, o cualquier otro agente asimilable habilitado para certificar un documento.

La tramitación se define como cualquier acto de firma electrónica de un documento que permita la certificación de dicho documento por un tercero 100 habilitado, así como cualquier otro documento adjunto que se genere.

A título de ejemplo no limitativo, la tramitación pertenece al grupo formado por la estampación de una firma electrónica en un documento original D1 por un tercero jurado y la generación de un documento adjunto DA al documento original firmado electrónicamente D2, la traducción y firma de un documento original D1 generando un documento adjunto DA traducido, la legalización o apostillado en al menos un documento D1 a tramitar.

En la práctica, el documento adjunto DA pertenece al grupo formado por documento traducido, documento digital que contenga una legalización, documento digital apostillado.

La firma electrónica aplicada al documento original D1 y a su adjunto DA permite la incorporación de metadatos intrínsecos del documento, entre ellos los datos de firma, y el certificado o certificados correspondientes.

[Tabla 2]

<table>
<tr><td>•Certificado X509 correspondiente a la firma electrónica

o Número de versión
o Número de serie
o ID del algoritmo de firma
o Nombre del emisor
o Período de validez
-No antes
-No después
o Nombre del sujeto
o Información de la clave pública del sujeto
-Algoritmo de la clave pública
-Clave pública del sujeto
o Identificador único del emisor (opcional)
o Identificador único del sujeto (opcional)
o Extensiones (opcional)</td><td>Datos de firma electrónica

-Fecha y hora de firma
-ID de transacción
-Estado
-Tipo de firma
-Plataforma de firma</td></tr>
<tr><td>•Algoritmo de firma de certificado</td><td></td></tr>
<tr><td>•Firma de certificado</td><td></td></tr>
</table>

La etapa de tramitación S1 según la invención incluye además la generación de un documento adjunto DA por el tercero 100, y tanto dicho el documento adjunto DA así generado como el documento original D1 son firmados electrónicamente ambos por el tercero 100.

El documento adjunto así generado también incorpora las huellas digitales de referencia HRA del documento original de referencia D1 al cual corresponde el documento adjunto, así como la huella digital HRBA del contenido del documento original D1 al cual corresponde el documento adjunto DA recabado para su firma.

Una vez realizado el trámite por el tercero 100, el documento original firmado D2 y el adjunto firmado DA así generados se reciben según una etapa de recepción S2 a través de la aplicación que implementa el procedimiento según la invención.

Según una forma de realización de la invención, la etapa de tramitación S1 incluye una subetapa de análisis en tiempo real del documento original D1, D2 en trámite o modificación, y/o del documento adjunto DA correspondiente que se está generando para obtener, para cada documento respectivamente, los metadatos intrínsecos del documento o documentos en trámite, así como los metadatos extrínsecos del documento o documentos en trámite o generación.

La etapa de tramitación S1 incluye además una segunda subetapa de cálculo de las huellas digitales del documento o documentos en trámite, y de su contenido según uno o varios estadios de progreso de la tramitación efectuada, así como de las huellas digitales de los metadatos intrínsecos del documento o documentos en trámite o generación.

La etapa de tramitación S1 incluye además una tercera subetapa de depósito dentro de un contrato inteligente (B1) de un sistema de cadena de bloques (B) los metadatos intrínsecos, y los metadatos extrínsecos extraídos que

incorporan las huellas digitales calculadas, todo ello iterado según uno o varios estadios de progreso de la tramitación realizada respecto al documento o documentos sometidos a la etapa de tramitación S1.

Ventajosamente, el depósito dentro de un contrato inteligente de los metadatos relativos a un documento en trámite en varios estadios de la fase de tramitación permite asimismo certificar en tiempo real del estado del documento.

El procedimiento según la invención incluye una etapa de recepción S2 procedente del tercero 100 de los documentos generados por la etapa de tramitación S1, y que incluye una primera subetapa de registro y análisis paralelo del documento original firmado D2 y del documento adjunto firmado DA así recibido, lo que permite obtener los datos relativos al contenido visible de dichos documentos D2 y DA, así como los correspondientes metadatos intrínsecos MID2 y MIDA y extrínsecos MED2 y MEDA.

El registro del documento original firmado D2 y del adjunto firmado DA comporta un sellado de tiempo desde la recepción, y cada sello de tiempo se incorpora a los metadatos extrínsecos MED2 y MEDA de cada documento D2 y DA.

[Tabla 3]

RECEPCIÓN DOCUMENTO ORIGINAL FIRMADO	
Tipo	Original para legalizar
Nombre	REGISTRO MERCANTIL EMPRESA PDF
Tamaño	17Ko
Fecha de carga	09/09/2020 a 10:50 am
Carga de usuario IS	ABL
Origen declarado	DAVRON TRADUCTION
ID de usuario declarante	ABL
HD2	98JI
HB2	**LoIp3**
HM2	tDk8
Datos de firmas	08/09/20Certificado**DavronDelivréparChamberSignDatedutxx…..
	Etc.
ID «PROYECTO» interno Davron	7

[Tabla 4]

RECEPCIÓN DOCUMENTO ADJUNTO (TRADUCCIÓN)	
Tipo	Adjunto
Nombre	REGISTRO MERCANTIL TRADUCIDO RUSO
Tamaño	19Kb
Fecha de carga	09/09/2020 a 10:50 am
Carga de usuario IS	ABL
Origen declarado	DAVRON TRADUCTION
ID de usuario declarante	ABL
HDA	5Hhu
HBA	PooT
HMA	56jU
HRA	98JI
HRBA	**Lolp3**
Datos de firmas	08/09/20Certificado**DavronDelivréparChamberSignDatedutxx.....
	Etc.
ID «PROYECTO» interno Davron	7

Para el documento original firmado D2, primero se extraen los metadatos intrínsecos MID2, entre ellos el nombre, el tamaño, así como los datos de firmas electrónicas y certificados correspondientes.

Según una subetapa de cálculo de la etapa de recepción S2, se calculan la huella digital del documento original firmado HD2, la huella digital HB2 del contenido así analizado, así como la huella digital HM1 de los metadatos intrínsecos del documento original firmado D2, incorporándose dichas huellas digitales a los metadatos extrínsecos al documento original firmado D2.

Para el documento adjunto DA firmado, se extraen los metadatos MIDA intrínsecos, entre ellos el nombre, el tamaño, así como los datos de firmas electrónicas y certificados correspondientes, así como las huellas digitales de referencia HRA del documento de referencia D2 al cual corresponde el documento adjunto DA, y la huella digital HRBA del contenido del documento original D2 al cual corresponde el documento adjunto DA.

Según una subetapa de cálculo de la etapa de recepción S2, se calculan la huella digital del documento adjunto firmado HDA, la huella digital del contenido del documento adjunto HBA, así como la huella digital de los metadatos intrínsecos recabados del documento adjunto HMA, incorporándose dichas huellas digitales a los metadatos extrínsecos del documento adjunto DA.

Una vez calculadas las huellas digitales del documento original firmado D2 y del documento adjunto DA, la etapa de recepción S2 incluye además una subetapa de almacenamiento mediante una transacción, implementada por un segundo contrato inteligente B2, en el sistema de cadena de bloques (B), incluyendo el segundo contrato inteligente B2 los metadatos intrínsecos y extrínsecos generados del documento original firmado D2 y del adjunto DA.

[Tabla 5]

Sello de tiempo de recepción del documento de generación de metadatos extrínsecos (MEDA)	Registro del archivo original firmado (D2) y del documento adjunto (DA) correspondiente firmado	Sello de tiempo de recepción del documento de generación de metadatos extrínsecos (MED2)
Documento adjunto (DA) -Metadatos intrínsecos del documento (MIDA) -Contenido visible del documento adjunto (DA)	Análisis de documentos	Documento original firmado -Metadatos intrínsecos del documento (MID2) -Contenido visible del documento original firmado (D2)
Cálculo de huellas digitales: - del documento adjunto (HDA) - del contenido del documento adjunto (HBA) - de los metadatos recabados del documento adjunto (HMA)	Cálculo de las huellas digitales originales	Cálculo de huellas digitales: - del documento original firmado (HD2) - del contenido del documento original firmado (HB2) - de los metadatos recogidos del documento original firmado (HM2)
Almacenamiento de los metadatos y huellas digitales del documento adjunto, así como de las huellas digitales del documento original firmado (D2) y del contenido del documento original firmado (D2) correspondiente al documento adjunto (DA)	Almacenamiento a través de una transacción dentro de un contrato inteligente (B1) a un sistema de cadena de bloques (B)	Almacenamiento de los metadatos y huellas digitales del documento original firmado, así como las huellas digitales del documento original firmado (D2) calculadas

La tabla 5 describe esquemáticamente las subetapas de la etapa de recepción según la invención.

Según una realización particular de la invención, en la etapa de recepción S2, los metadatos así obtenidos en cada etapa de inicialización S0 y en la etapa de recepción S2 se almacenan en una base de datos para ser asociados posteriormente en un árbol de Merkle, cuya huella digital raíz se almacena mediante una transacción en el sistema de cadena de bloques B.

Según una realización particular de la invención, la subetapa de almacenamiento de la etapa de recepción del procedimiento según la invención incluye una subetapa de comprobación de la identidad de los documentos cuya trazabilidad debe acreditarse.

La subetapa de comprobación incluye una primera comparación entre la huella digital del contenido del documento original D1 y la huella digital del contenido del documento original firmado D2. Si el resultado es positivo, los documentos son idénticos.

La subetapa de comprobación incluye además una segunda comparación entre las huellas digitales de referencia HRA del documento de referencia D2 al cual corresponde el documento adjunto DA y la huella digital del documento original firmado D2, así como la comparación entre la huella digital HRBA del contenido del documento de referencia al cual corresponde el documento adjunto DA y la huella digital del contenido del documento original firmado D2.

Si las comparaciones son positivas y las huellas digitales son idénticas, entonces el documento adjunto DA presentado corresponde efectivamente al documento original firmado D2.

La subetapa de comprobación garantiza la conformidad de la cadena de trazabilidad, al tiempo que permite la autentificación de un vínculo de asociación entre un documento firmado D2 y un documento adjunto DA, que forman así un árbol de trazabilidad.

Ventajosamente, la extracción del texto del documento durante cada subetapa de análisis documental D1, D2, DA, permite detectar únicamente el texto presente en el documento, de modo que una firma manuscrita en un documento, o un sello, no se reconocerían como contenido textual, lo que permite, según una forma de realización concreta, conservar una huella digital de contenido idéntico, y ello incluso después de determinados trámites como una firma, legalización o apostilla, y también permite introducir un documento físico digitalizado que no sea estrictamente idéntico al documento original debido a las condiciones de digitalización aplicadas.

Según una realización particular de la invención, el procedimiento de trazabilidad según ésta incluye una etapa de envío adicional, sucesiva a la etapa de inicialización S0, y anterior a la etapa de tramitación S1.

La etapa de envío incluye el envío del documento original D1 al tercero 100, los metadatos intrínsecos MID1 al documento original D1 y los metadatos extrínsecos MED1, que incluyen: las huellas digitales del documento original HD1, de su contenido HB1 y de metadatos HM1 en relación con el documento original D1, así como los metadatos de sello de tiempo de la acción de envío del documento original D1 al tercero 100, que se almacenan mediante una transacción implementada por un tercer contrato inteligente B3 en el sistema de cadena de bloques B.

[Tabla 6]

DECLARACIÓN ENVÍO AL TRADUCTOR	
Tipo	Original para legalizar
Nombre	REGISTRO MERCANTIL EMPRESA PDF
Tamaño	17Ko
Acción	Envío a la etapa 1
Destino	DAVRON TRADUCTION
Fecha envío declarado	08/09/2020 a 12:20 am
ID de usuario declarante	ABL
HD1	3j4XH
HB1	Lolp3
HM1	X059
Datos de firmas	N/A
ID «PROYECTO» interno Davron	7

Según una realización de la invención, la etapa de envío incluye además una subetapa de comprobación que precede al envío del documento original D1 que será tramitado por el tercero 100, de comprobación de la identidad del documento original D1 que será enviado.

La subetapa de comprobación incluye el cálculo de la huella digital del documento a enviar HD1, de la huella digital HB1 del contenido del documento a enviar, así como la huella digital HM1 de los metadatos intrínsecos en relación con el documento original D1 a enviar.

La subetapa de comprobación incluye además una etapa de comparación entre, por una parte, la huella digital del documento que se va a enviar HD1 y la huella digital HD1 del documento original D1, y, por otra, entre la huella digital HB1 del contenido del documento que se va a enviar y la huella digital del contenido HB1 del documento original D1.

Si la comparación resulta positiva, el documento que se envía al tercero corresponde al documento original D1.

[Tabla 7]

Sello de tiempo de recepción del documento de generación de metadatos extrínsecos (MEDA)	Registro del archivo original firmado (D2) y del documento adjunto (DA) correspondiente firmado	Sello de tiempo de recepción del documento de generación de metadatos extrínsecos (MED2)
Documento adjunto (DA) -Metadatos intrínsecos del documento (MIDA) -Contenido visible del documento adjunto (DA)	Análisis de documentos	Documento original firmado -Metadatos intrínsecos del documento (MID2) -Contenido visible del documento original firmado (D2)
Cálculo de huellas digitales: - del documento adjunto (HDA) - del contenido del documento adjunto (HBA) - de los metadatos recabados del documento adjunto (HMA)	Cálculo de las huellas digitales originales	Cálculo de huellas digitales: - del documento original firmado (HD2) - del contenido del documento original firmado (HB2) - de los metadatos recabados del documento original firmado (HM2)
Comprobaciones adicionales: ¿HB1 = HB2? En caso afirmativo, se trata del mismo documento. ¿HRA = HD1 y HRBA = HB1? En caso afirmativo, el documento adjunto remite al documento correcto		
Almacenamiento de los metadatos y huellas digitales del documento adjunto, así como de las huellas digitales del documento original firmado (D2) y del contenido del documento original firmado (D2) correspondiente al documento adjunto (DA)	Almacenamiento a través de una transacción dentro de un contrato inteligente (B1) a un sistema de cadena de bloques (B)	Almacenamiento de los metadatos y huellas digitales del documento original firmado, así como las huellas digitales del documento original firmado (D2) calculadas

La tabla 7 describe esquemáticamente una realización particular de las subetapas de la etapa de recepción según la invención.

Según una realización de la invención, la subetapa de comprobación incluye además una comprobación visual de conformidad.

La comprobación visual de conformidad puede efectuarse comparando el contenido visible extraído, por ejemplo, entre un documento original D1 y un documento original firmado D2, un documento original D1 y un documento adjunto correspondiente al documento original apostillado/legalizado, o cualquier documento correspondiente a otro documento cuyo contenido incluya elementos idénticos.

Por ejemplo, un documento original D1 que tenga un sello, estampilla o firma aplicada físicamente por un tercero 100 y luego digitalizado puede ser comparado con el documento original D1 correspondiente de modo que sus respectivos contenidos visibles sean comparados para confirmar la identidad de los dos documentos en al menos una parte de sus respectivos contenidos visibles.

Según otra realización de la invención, el procedimiento de trazabilidad es implementado por varios terceros sucesivos (100, 200).

La etapa de inicialización S0, la de tramitación S1 y la de recepción S2 son repetidas por el siguiente tercero (200) con arreglo al documento original firmado (D2) y el documento adjunto firmado (DA) generado por el tercero anterior (100).

De acuerdo con una realización particular de la invención, las subetapas de almacenamiento en un contrato inteligente (B1, B2, B3) a través de una transacción en el sistema de cadena de bloques B se realizan todas ellas en un único contrato inteligente que aglutina la información almacenada.

Ventajosamente, el almacenamiento en un único contrato inteligente permite a las entidades auditoras disponer de toda la información necesaria para validar la autentificación de los documentos en un mismo soporte en el sistema de cadena de bloques B.

Según una realización alternativa de la invención, la identidad del sistema de cadena de bloques B que se utilizará para las subetapas de almacenamiento puede ser seleccionada por un usuario en función de los parámetros de copia de seguridad elegidos por dicho usuario al guardar el documento original D1.

El depósito de metadatos de destino según la invención en cualquier punto del proceso en al menos un contrato inteligente B1 del sistema de cadena de bloques B permite asimismo certificar el estado de un documento, o de datos seleccionados de dicho documento o documentos o de su asociación con un documento adjunto, haciendo que la información que contiene sea inmutable y trazable en la pista de auditoría así creada y permitiendo consolidar la pista de auditoría durante los sucesivos ciclos de tramitación de los documentos.

La huella digital de los metadatos intrínsecos de cada documento D1, D2 y DA permite también hacer inmutables y certificar en especial los metadatos relativos a la(s) firma(s) electrónica(s) de cada tercero 100, así como sus metadatos correspondientes y obtener así un procedimiento que posibilita consecutivamente la multiplicidad de firmas de un documento o un documento y al menos un documento asociado de manera desincronizada.

Este procedimiento también permite evitar la sobreescritura de la(s) firma(s) anterior(es) en caso de firma por un programa informático distinto en el documento o documentos tramitados y, por tanto, rastrear individualmente en la pista de auditoría cada adición de firma a dicho documento o documentos.

Según una primera realización, el documento original D1 es certificado por un notario, se envía a un primer tercero 100 para su traducción, y la traducción así generada es firmada, luego los documentos D2 y DA se envían a otro tercero 200 para su legalización, siendo el otro tercero 200 una autoridad gubernamental, y los documentos así generados se envían a un segundo tercero 200 de tipo consular, siendo los documentos previamente generados sometidos a un trámite de tipo sobrelegalización.

Según una segunda realización, el documento original D1 es certificado por un notario, luego se envía a un primer tercero 100 para su traducción, y la traducción así generada es firmada, los documentos D2 y DA se envían a otro tercero 200 para su apostilla, siendo el otro tercero 200 una autoridad gubernamental.

En la práctica, las subetapas de registro de las etapas de inicialización S0 y de la etapa de recepción S2 se implementan temporalmente hasta que la información requerida se almacena en el sistema de cadena de bloques B, de modo que los documentos D1, D2 y DA no se archivan permanentemente, y así se garantiza la confidencialidad de los documentos D1, D2 y DA.

Por ejemplo, los documentos D1, D2 y DA son archivos PDF.

La pista de auditoría del sistema de cadena de bloques B se alimenta así sobre la marcha a partir de los trámites de los sucesivos terceros (100, 200), y cada etapa de inicialización S0 y de recepción S2 permite almacenar datos sucesivos relativos a cada tercero 100, 200, y garantiza así que cualquier tercero verificador pueda acceder a un árbol de autentificación del documento original D1.

Con respecto a las **figuras 6 y 7**, la invención también se refiere a una plataforma para la trazabilidad de un documento adjunto DA generado por un tercero 100 a partir de un documento original D1, interactuando dicha plataforma con un sistema de cadena de bloques B para la implementación del proceso de trazabilidad.

La plataforma de trazabilidad según la invención, de estructura seleccionada, que incluye:

- medios para registrar y analizar el documento original D1 para obtener metadatos de inicialización que incluyen metadatos MID1 intrínsecos del documento original D1 y metadatos extrínsecos MED1 que incluyen huellas digitales del documento original HD1, su contenido HB1 y metadatos HM1 en relación con el documento original D1;

- medios de recepción S2 procedentes del tercero 100, que incluyen medios de registro y análisis del documento original D2 y del documento adjunto DA así recibidos firmados procedentes del tercero 100 para obtener datos de recepción que incluyen metadatos intrínsecos del documento original y de las huellas digitales del documento original recibido HD2, del documento adjunto HDA y del documento de referencia HRA y de sus contenidos respectivos HBA, HB2, HBRA así como metadatos HM2 y HMA en relación con el documento original y el documento adjunto;

- medios para depositar los metadatos de inicialización y los metadatos de recepción en un contrato inteligente respectivo del sistema de cadena de bloques B.

En la práctica, la plataforma según la invención incluye al menos un servidor web capaz de conectarse a través de una red a un dispositivo de usuario, y capaz de recibir y registrar al menos un documento perteneciente al grupo formado por documento original D1, documento original firmado D2, y documento adjunto generado DA, procedente del usuario, o de un tercero 100 o 200.

Según un modo de realización de la invención, la plataforma según la invención incluye asimismo al menos un servidor de aplicaciones capaz de permitir el análisis de al menos un documento perteneciente al grupo formado por documento original D1, documento original firmado D2, y documento adjunto generado DA, y permitir el cálculo de las huellas digitales HD1, HB1, HM1, HD2, HB2, HM2, HDA, HBA, HMA necesarias durante la realización del procedimiento de trazabilidad según la invención.

La plataforma según la invención incluye además un módulo de almacenamiento, apto para el almacenamiento a través de transacciones ejecutadas en contratos inteligentes B1, B2, B3, en un sistema de cadena de bloques B.

Dicho módulo de almacenamiento incluye al menos un servidor nodo apto para formar parte integrante del sistema de cadena de bloques B, que consta de una multitud de nodos interconectados.

Según una realización de la invención, el sistema de cadena de bloques B es un sistema de cadena de bloques público.

Según una realización alternativa de la invención, el sistema de cadena de bloques B es un sistema de cadena de bloques privado.

Según una realización particular de la invención, la plataforma según la invención incluye además una pluralidad de bases de datos.

Cada base de datos incluye al menos una lista de terceros A, B, C aptos para realizar al menos un trámite seleccionado 101, 201, así como información relacionada con dichos terceros A, B, C, como sus datos de contacto, números de identificación de plataforma y similares.

Según una realización particular de la invención, la plataforma incluye un módulo aplicativo que permite guiar a un usuario a través del procedimiento de tramitación, seleccionando los terceros a los que se presentará el documento original D1 que se va a tramitar, según unos parámetros de tramitación predefinidos establecidos por el usuario.

El módulo aplicativo de la plataforma según la invención es capaz, en primer lugar, de registrar los parámetros de tramitación de documentos D1 deseados por un usuario.

Por ejemplo, si los parámetros de tramitación son la traducción y la certificación por parte de una entidad gubernamental, los terceros A, B, C que se seleccionen para el trámite deberán permitir la traducción y la legalización.

En la práctica, el módulo aplicativo de la plataforma según la invención es capaz de identificar al menos un trámite 101 perteneciente al grupo formado por traducción de un documento, legalización y generación de una apostilla.

Con arreglo a los parámetros de tramitación definidos, el módulo aplicativo es capaz de seleccionar, para cada tipo de trámite seleccionado, al menos un tercero A, B, C, capaz de realizar dicho trámite a partir de las bases de datos de terceros A, B, C, y capaz de permitir la invocación del siguiente tercero 200 tras el trámite y el registro del documento tramitado D2, DA por el tercero 100 en cuestión.

Según una realización particular de la invención, la plataforma según la invención incluye asimismo un módulo de tipo API, configurado para permitir la invocación de al menos una herramienta de firma electrónica externa destinada al tercero 100, y para recibir en forma de Iframe un ejecutable para su aplicación al documento que vaya a ser firmado electrónicamente por el tercero.

REIVINDICACIONES

1. Procedimiento de trazabilidad de un documento adjunto (DA) generado por un tercero (100) a partir de un documento original (D1) al cual corresponde, dicho procedimiento utiliza un sistema de cadena de bloques y se caracteriza porque incluye las siguientes etapas:

- una etapa de inicialización (S0) que incluye

  - el registro y análisis del documento original (D1) para obtener metadatos de inicialización del documento original (D1), que incluyen:

    -metadatos intrínsecos (MID1) del documento original (D1); y
    -metadatos extrínsecos (MED1) al documento original (D1) que incorporan los metadatos generados por la aplicación que ejecuta el proceso;

  - el cálculo de las huellas digitales (HD1) del documento original y de su contenido, y de las huellas digitales (HM1) de los metadatos intrínsecos (MID1) del documento original (D1);

  - depositar en un contrato inteligente (B1) de un sistema de cadena de bloques (B) metadatos de inicialización del documento original (D1), entre ellos los metadatos intrínsecos (MID1), y los metadatos extrínsecos (MED1), que incorporan las huellas digitales calculadas (HD1,HB1,HM1) ;

- una etapa de tramitación (S1) por el tercero (100), que incluye la generación del documento adjunto (DA) por el tercero (100), estando tanto el documento original (D1) recibido como dicho documento adjunto (DA) generado por el tercero (100) para su tramitación firmados electrónicamente por dicho tercero (100), incorporando el documento adjunto (DA) en sus metadatos extrínsecos (MEDA) las huellas digitales de referencia (HRA) del documento original (D1), al cual corresponde el documento adjunto (DA), y las huellas digitales (HRBA) del contenido del documento original (D1) tomado para su firma; y
- una etapa de recepción (S2) procedente del tercero (100), que incluye el registro y el análisis en paralelo del documento original firmado (D2) y del documento adjunto firmado (DA) recibido procedente del tercero (100), para obtener metadatos de recepción, que incluyen:

  - metadatos intrínsecos (MID2) del documento original firmado (D2) y los metadatos intrínsecos (MIDA) del documento adjunto firmado (DA);

  - metadatos extrínsecos (MED2) del documento original firmado (D2) y los metadatos extrínsecos (MEDA) del documento adjunto (DA) firmado, incluidas las huellas digitales:

    - del documento original recibido (HD2)

    - del documento adjunto (HDA) y del documento de referencia (HRA) y sus respectivos contenidos (HBA, HB2, HBRA);

    - de los metadatos (HM2, HMA) en relación con el documento original firmado (D2) y el documento adjunto firmado (DA); depositándose los metadatos de recepción en el contrato inteligente (B1) del sistema de cadena de bloques (B); y un contrato inteligente (B1) así depositado después de cada etapa de inicialización (S0) y después de cada etapa de recepción (S2), permitiendo así constituir una pista de auditoría y trazabilidad del documento adjunto (DA) generado por el tercero (100) a partir del documento original al cual corresponde (D1).

2. Procedimiento de trazabilidad según la reivindicación 1, caracterizado porque incluye además una etapa de envío del documento original (D1) al tercero (100), de tal forma que los metadatos intrínsecos (MID1) del documento original (D1) y los metadatos extrínsecos (MED1) incluyen las huellas digitales del documento original (HD1), de su contenido (HB1) y metadatos (HM1) relacionados con el documento original (D1) que se depositan en un contrato inteligente (B1) del sistema de cadena de bloques (B).

3. Procedimiento de trazabilidad según una cualquiera de las reivindicaciones 1 o 2, caracterizado porque los metadatos así obtenidos en cada etapa de inicialización (S0), envío y recepción (S2) se almacenan en una base de datos para luego ser asociados en un árbol de Merkle, cuyo hash raíz se deposita en el sistema de cadena de bloques (B).

4.Procedimiento de trazabilidad según una de las reivindicaciones 1 a 3, caracterizado porque los metadatos intrínsecos (MID1, MID2, MIDA) pertenecen al grupo formado por tipo, nombre, tamaño, fecha de registro, identificador de usuario, datos de firma electrónica, y el certificado o certificados correspondientes a los datos de firma electrónica.

5. Procedimiento de trazabilidad según una de las reivindicaciones 1 a 4, caracterizado porque las huellas digitales (HD1, HB1, HM1, HD2, HB2, HM2, HDA, HBA, HMA) se calculan según una función hash seleccionada.

6.Procedimiento de trazabilidad según la reivindicación 5, caracterizado porque la función hash es SHA 256.

7. Procedimiento de trazabilidad según una cualquiera de las reivindicaciones 1 a 6, caracterizado porque el documento adjunto (DA) pertenece al grupo formado por documento traducido, documento digital que contiene una legalización, documento digital que incluye una apostilla.

8. Procedimiento según una cualquiera de las reivindicaciones 1 a 7, caracterizado por ser implementado por varios terceros sucesivos (100, 200), repitiéndose las etapas de inicialización (S0), tramitación (S1) y recepción (S2) por el tercero siguiente (200) con arreglo al documento original firmado (D2) y el documento adjunto (DA) generados por el tercero anterior (100), alimentándose así la pista de auditoría del sistema de cadena de bloques (B) sobre la marcha por la tramitación de los terceros sucesivos (100, 200).

9. Plataforma de trazabilidad de un documento adjunto (DA) generado por un tercero (100) a partir de un documento original (D1), interactuando dicha plataforma con un sistema de cadena de bloques (B) para la implementación del procedimiento según una cualquiera de las reivindicaciones 1 a 8, caracterizada porque incluye:

- medios de registro y análisis del documento original (D1) para obtener metadatos de inicialización que incluyen metadatos intrínsecos (MID1) del documento original (D1) y metadatos extrínsecos (MED1), que incluyen huellas digitales del documento original (HD1), de su contenido (HB1) y de metadatos (HM1) relacionados con el documento original (D1);
- medios de recepción procedentes del tercero (100), que incluyen medios de registro y análisis del documento original (D2) y del documento adjunto (DA) así recibidos firmados procedentes del tercero (100) para obtener datos de recepción que incluyen metadatos intrínsecos (MID1) del documento original (D1) y huellas digitales del documento original recibido (HD2), el documento adjunto (HDA) y el documento de referencia (HRA) y de sus contenidos respectivos (HBA, HB2, HBRA) así como los metadatos (HM2, HMA) relativos al documento original (D1) y al documento adjunto (DA);
- medios para depositar los metadatos de inicialización y los metadatos de recepción en un contrato inteligente (B1) del sistema de cadena de bloques (B), y en el que varios terceros sucesivos (100, 200) son capaces de alimentar a lo largo del tiempo la pista de auditoría del sistema de cadena de bloques (B) por el siguiente tercero (200) con arreglo al documento original firmado (D2) y el documento adjunto (DA) generados por el tercero anterior (100).

10. Plataforma de trazabilidad según la reivindicación 7, caracterizada porque incluye un módulo aplicativo capaz de registrar los parámetros de tramitación del documento (D1) deseado por un usuario, capaz de identificar al menos un trámite perteneciente al grupo formado por traducción de un documento, legalización, generación de una apostilla, capaz de seleccionar para cada tipo de trámite al menos un tercero (A, B, C) y capaz de permitir la invocación del siguiente tercero (200) tras el trámite y el registro del documento tramitado (D2, DA) por el tercero en cuestión (100).

11. Plataforma de trazabilidad según la reivindicación 8, caracterizada porque incluye una herramienta interactiva con una pluralidad de bases de datos cada una de las cuales incluye al menos una lista de terceros (A, B, C) capaces de realizar al menos un trámite seleccionado, así como información relativa a dichos terceros (A, B, C).

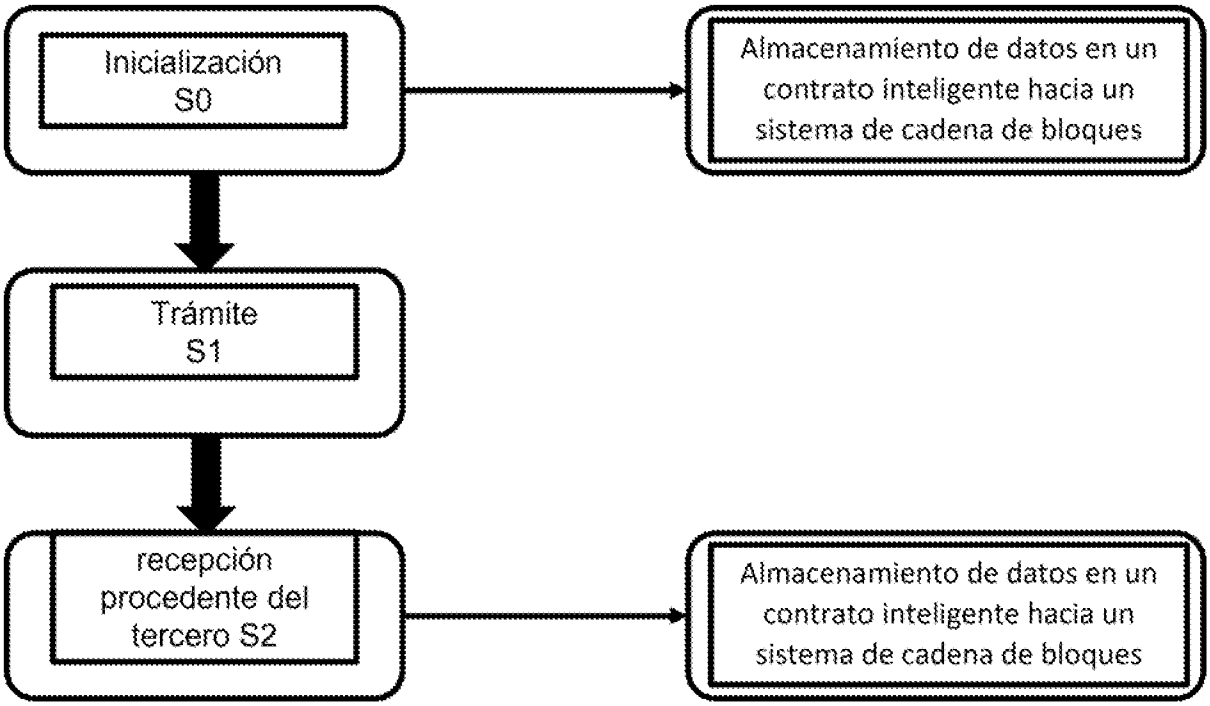
Inicialización
S0
Almacenamiento de datos en un contrato inteligente hacia un sistema de cadena de bloques
Trámite
S1
recepción procedente del tercero S2
Almacenamiento de datos en un contrato inteligente hacia un sistema de cadena de bloques

FIGURA 1

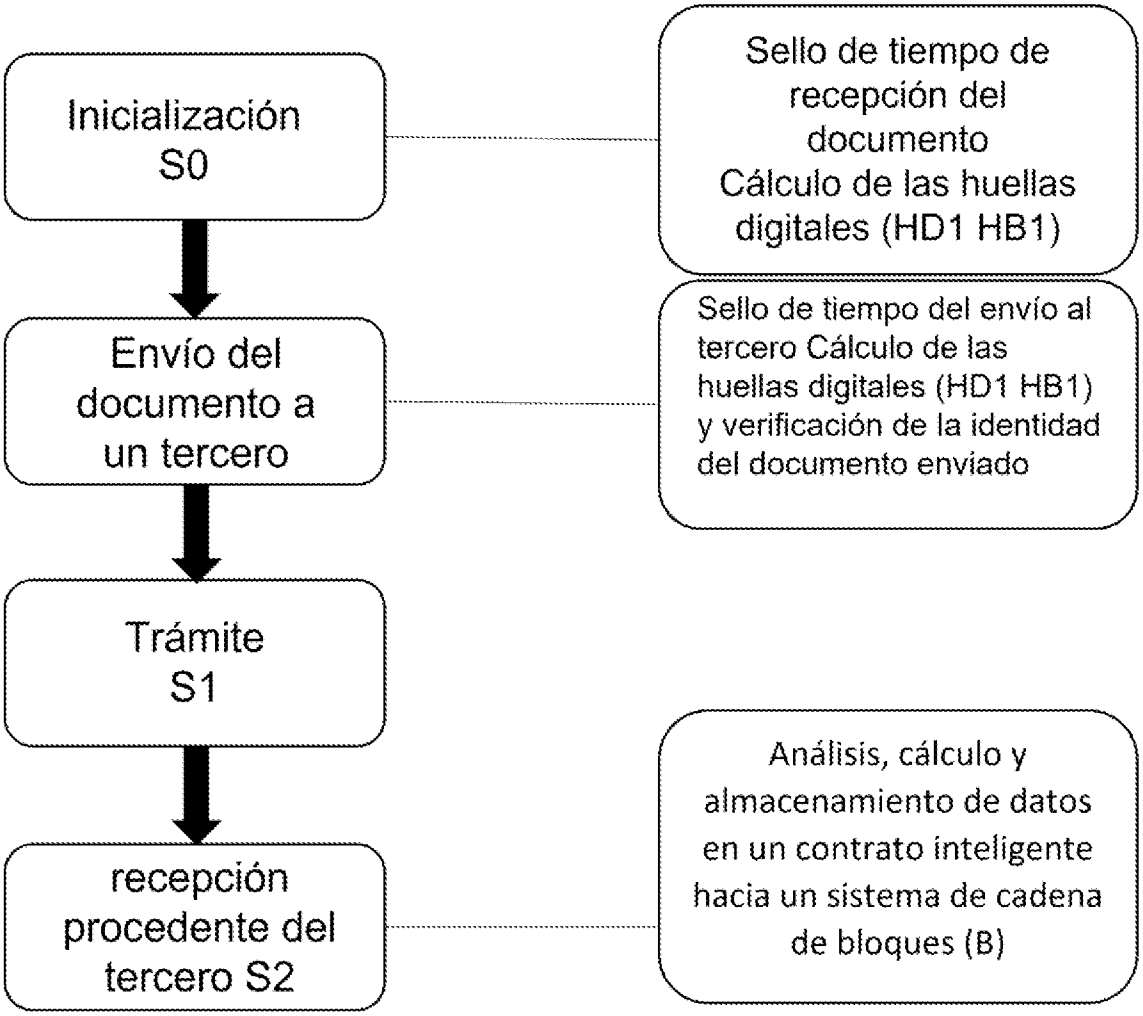
Inicialización
S0
Envío del documento a un tercero
Trámite
S1
recepción procedente del tercero S2
Sello de tiempo de recepción del documento
Cálculo de las huellas digitales (HD1 HB1)
Sello de tiempo del envío al tercero Cálculo de las huellas digitales (HD1 HB1) y verificación de la identidad del documento enviado
Análisis, cálculo y almacenamiento de datos en un contrato inteligente hacia un sistema de cadena de bloques (B)

FIGURA 2

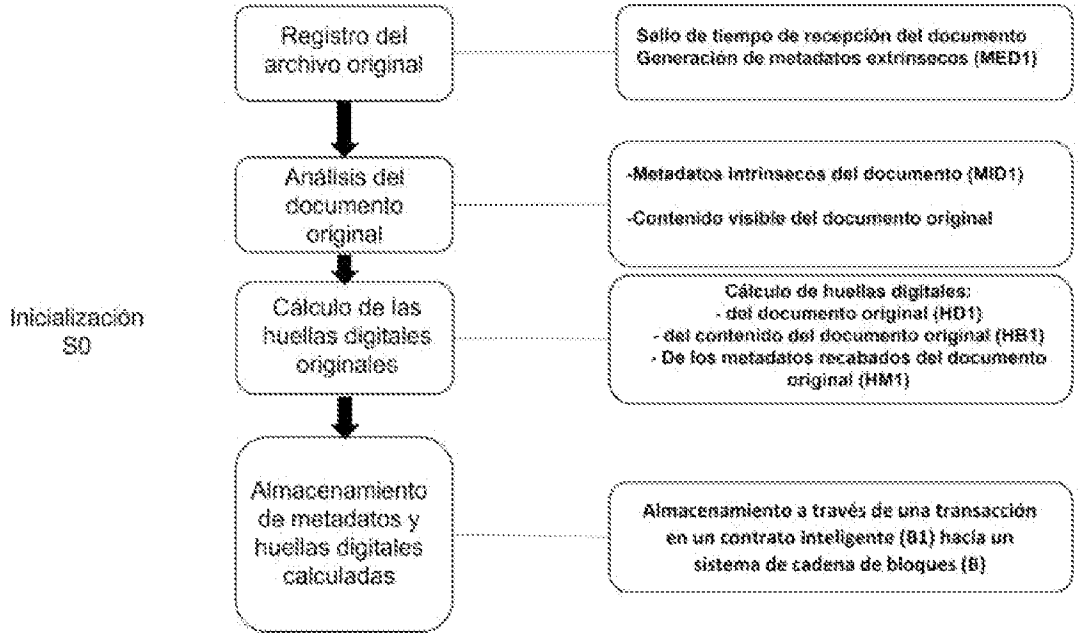

FIGURA 3

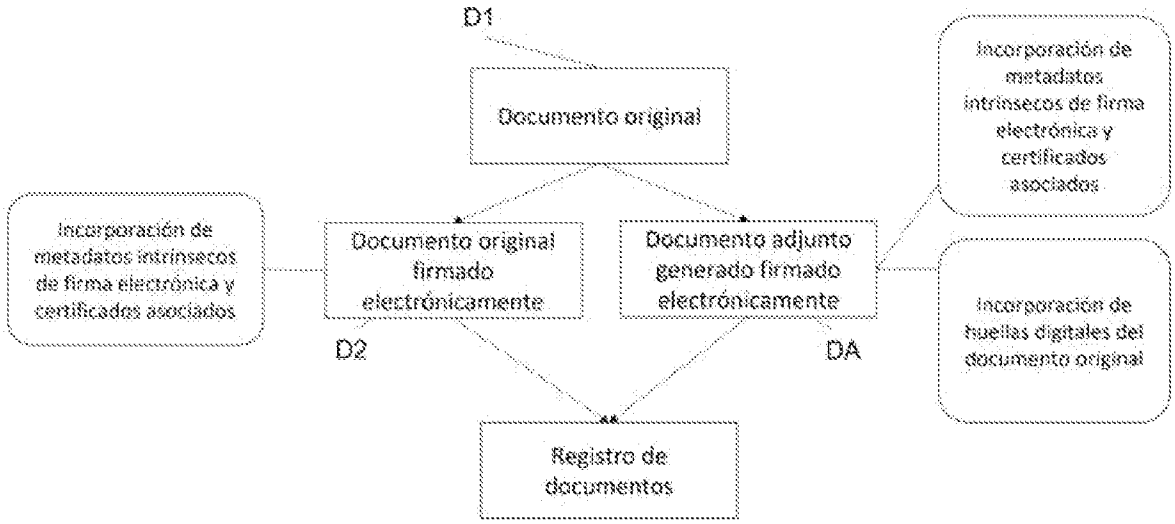

FIGURA 4

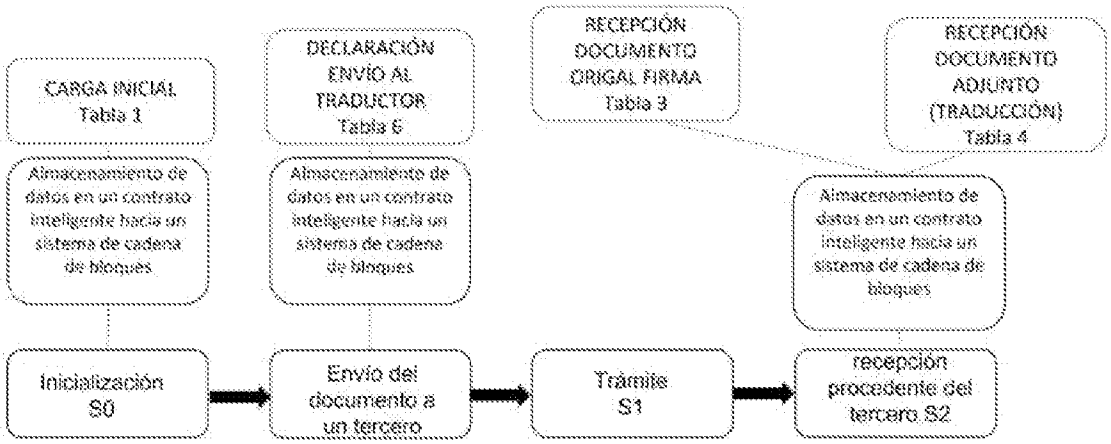

FIGURA 5

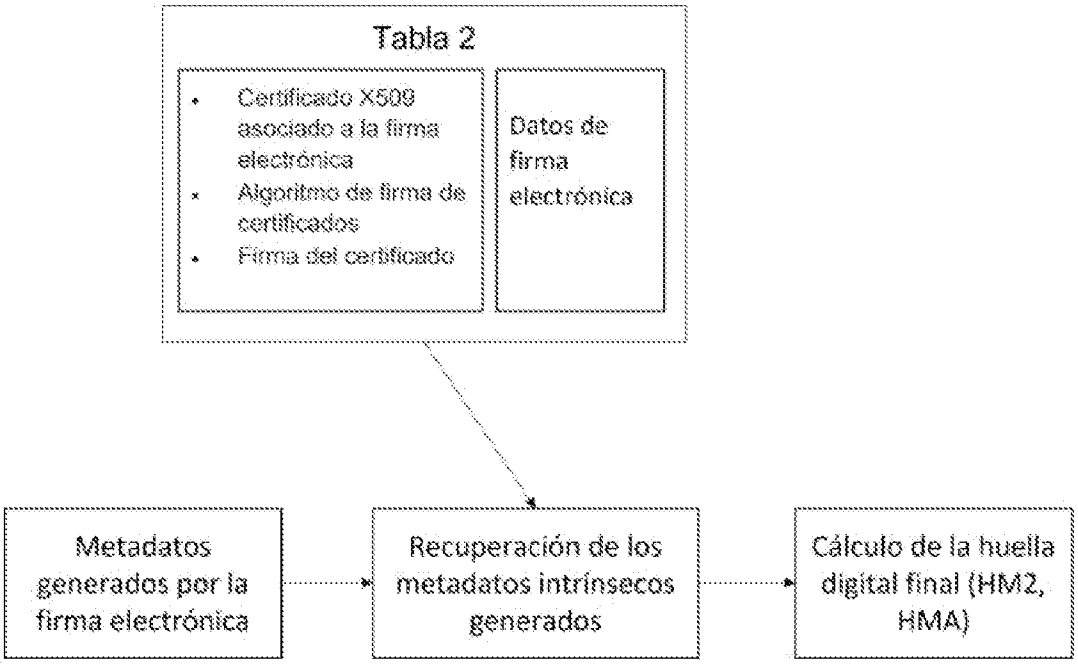

FIGURA 6

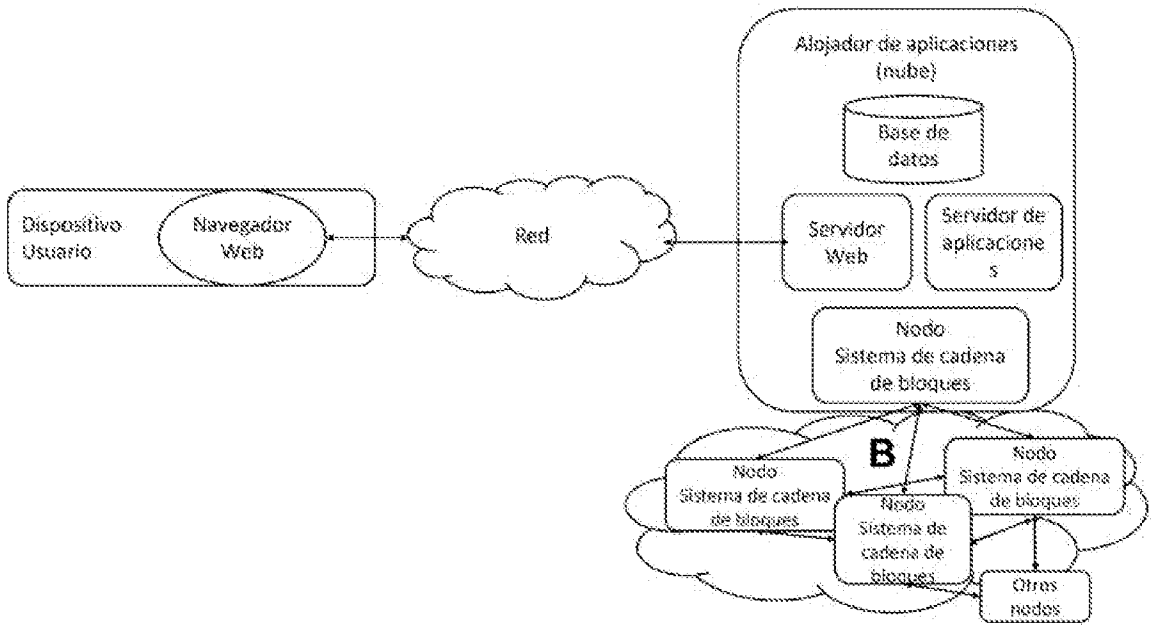

FIGURA 7

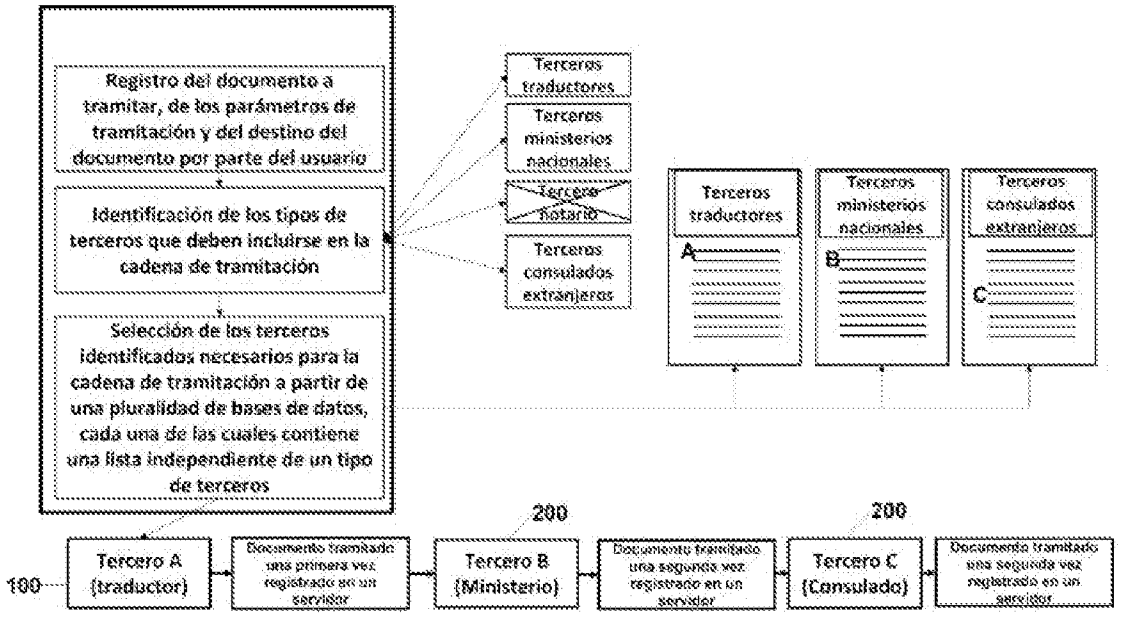

FIGURA 8

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Este listado de referencias citadas por el solicitante tiene como único fin la conveniencia del lector. No forma parte del documento de la Patente Europea. Aunque se ha puesto gran cuidado en la compilación de las referencias, no pueden excluirse errores u omisiones y la EPO rechaza cualquier responsabilidad en este sentido.

Documentos de patentes citados en la descripción

- US 2019356493 A1 **[0012]**