Unión Internacional de Telecomunicaciones

UIT-T X.1407

(01/2022)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios seguros (2) – Seguridad de tecnología de libro mayor distribuido (DLT)

Requisitos de seguridad para el servicio de validación de la integridad digital basado en la tecnología de libro mayor distribuido

Recomendación UIT-T X.1407

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web (1)	X.1140–X.1149
Seguridad de las aplicaciones	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1319
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350–X.1369
Seguridad en los sistemas de transporte inteligente (STI)	X.1370–X.1399
Seguridad de tecnología de libro mayor distribuido (DLT)	**X.1400–X.1429**
Seguridad de las aplicaciones (2)	X.1450–X.1459
Seguridad de la web (2)	X.1470–X.1489
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
Ciberdefensa	X.1590–X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
Protección de datos	X.1770–X.1789
SEGURIDAD DE IMT-2020	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1407

Requisitos de seguridad para el servicio de validación de la integridad digital basado en la tecnología de libro mayor distribuido

Resumen

En la Recomendación UIT-T X.1407 se especifican las amenazas y los requisitos de seguridad del servicio de validación de la integridad digital basado en la tecnología de libro mayor distribuido (DLT).

La prueba original protegida se almacena fuera de la cadena de bloques. Los valores de los datos encriptados se almacenan en la cadena, la Recomendación UIT-T X.1407 analiza las amenazas de seguridad para dichos servicios de validación de la integridad digital basados en DLT, es decir, el registro de prueba y el origen de la prueba. En esta Recomendación, también describe los requisitos de seguridad que pueden hacer frente a estas amenazas de la seguridad.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1407	07-01-2022	17	11.1002/1000/14800

Palabras clave

Validación de la integridad digital, tecnologías de libro mayor distribuido, amenazas y requisitos de seguridad.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT T disponibles en el sitio web del UIT-T http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

1 Alcance 1
2 Referencias 1
3 Definiciones 1
3.1 Términos definidos en otros documentos 1
3.2 Términos definidos en esta Recomendación 2
4 Abreviaturas y acrónimos 2
5 Convenios 2
6 Generalidades 2
7 Partes interesadas y procesos para la prueba de integridad digital basada en DLT 3
7.1 Partes interesadas 3
7.2 Procesos de la prueba de integridad digital basada en DLT 4
8 Amenazas de seguridad para la comprobación de la integridad digital basada en DLT 4
8.1 Amenazas de seguridad con respecto al usuario 4
8.2 Amenazas a la seguridad en la inscripción de pruebas 5
8.3 Amenazas a la seguridad en relación con la procedencia de las pruebas 6
9 Requisitos de seguridad para la prueba de integridad digital basada en DLT 6
9.1 Requisitos de seguridad para el usuario 7
9.2 Requisitos de seguridad para la inscripción de pruebas 7
9.3 Requisitos de seguridad para la procedencia de la prueba 9
Apéndice I – Caso de uso de la factura electrónica basada en la tecnología de libro mayor distribuido 10
Apéndice II – Caso de uso para la verificación de certificados académicos basado en la tecnología de libro mayor distribuido 13
Bibliografía 15

Recomendación UIT-T X.1407

Requisitos de seguridad para el servicio de validación de la integridad digital basado en la tecnología de libro mayor distribuido

1 Alcance

En esta Recomendación se especifican las amenazas y los requisitos de seguridad en la realización de pruebas digitales de la integridad de una entidad basadas en la tecnología de libro mayor distribuido (DLT). La plataforma de comprobación digital de la integridad basada en DLT proporciona servicios de distribución, consulta y seguimiento de la prueba digital de la integridad de una entidad mediante tecnologías de libro mayor distribuido.

2 Referencias

Las siguientes Recomendaciones del UIT T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se alienta a los usuarios de esta Recomendación a que investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT T actualmente vigentes. En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

[UIT-T X.1401] Recomendación UIT-T X.1401 (2019), *Amenazas a la seguridad de tecnología de libro mayor distribuido*.

[UIT-T X.1402] Recomendación UIT-T X.1402 (2020), *Marco de seguridad para la tecnología de libro mayor distribuido*.

[UIT-T X.1404] Recomendación UIT-T X.1404 (2020), *Garantía de seguridad para la tecnología de libro mayor distribuido*.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos definidos en la sección 1.4 de [b-ISO 23257], y en otros documentos:

3.1.1 libro mayor distribuido [b-UIT-T X.1400]: Tipo de libro mayor que se comparte, replica y sincroniza de manera distribuida y descentralizada.

3.1.2 tecnologías de libro mayor distribuido [b-ISO 22739]: Tecnología que hace posible el funcionamiento y la utilización de libros mayores distribuidos.

3.1.3 plataforma de tecnología de libro mayor distribuido [b-ISO 22739]: Conjunto de entidades de procesamiento, almacenamiento y comunicación que en conjunto proporcionan las capacidades del sistema DLT en cada nodo DLT.

3.1.4 integridad [b-ISO 13491-2]: Propiedad que evita la alteración o supresión de los datos de forma no autorizada.

3.1.5 libro mayor [b-UIT-T X.1400]: Almacén de información que mantiene registros de transacciones finales, definitivas e inmutables.

3.1.6 contrato inteligente [b-ISO 22739]: Programa informático almacenado en un sistema DLT en el que el resultado de cualquier ejecución del programa se registra en el libro mayor distribuido.

3.1.7 amenaza [b-ISO/CEI 27000]: Posible causa de un incidente no deseado, que puede dañar un sistema o perjudicar a una organización.

3.2 Términos definidos en esta Recomendación

Ninguno.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

DDoS Denegación de servicio distribuido (*distributed denial of service*)

DLT Tecnología de libro mayor distribuido (*distributed ledger technology*)

PoS Prueba de participación (*proof of stake*)

PoW Prueba de trabajo (*proof of work*)

PBFT Tolerancia frente a fallos bizantinos (*practical byzantine fault tolerance*)

5 Convenios

La presente Recomendación se ajusta a las siguientes formas verbales de expresión de disposiciones:

a) "deberá" indica una obligación;

b) "debería" denota una recomendación;

c) "podría" significa que se da permiso;

d) "puede" indica posibilidad o capacidad.

6 Generalidades

El proceso de demostración de la integridad de ciertos datos supone un reto cuando los datos están dispersos en diferentes sistemas. Además, el proceso de comprobación de la integridad puede requerir la búsqueda en muchas bases de datos, sistemas o manualmente en copias impresas. Esta situación se ve afectada por la ausencia del historial completo de la transacción; como resultado, esto podría provocar retrasos, esfuerzos y costes adicionales, y una toma de decisiones incorrecta.

La DLT consiste en un libro mayor descentralizado y a prueba de manipulaciones que establece un nivel de confianza necesario para el intercambio de valor sin el uso de intermediarios. Se basa en bases de datos descentralizadas que proporcionan registros íntegros, colaborativos, transparentes, verificables y auditables para todas las transacciones. De este modo, las características rastreables y a prueba de manipulaciones de la DLT permiten una solución para la comprobación de la integridad digital en la que los datos originales no pueden ser creados o comprometidos de forma fraudulenta sin que exista una manera de detectar los cambios.

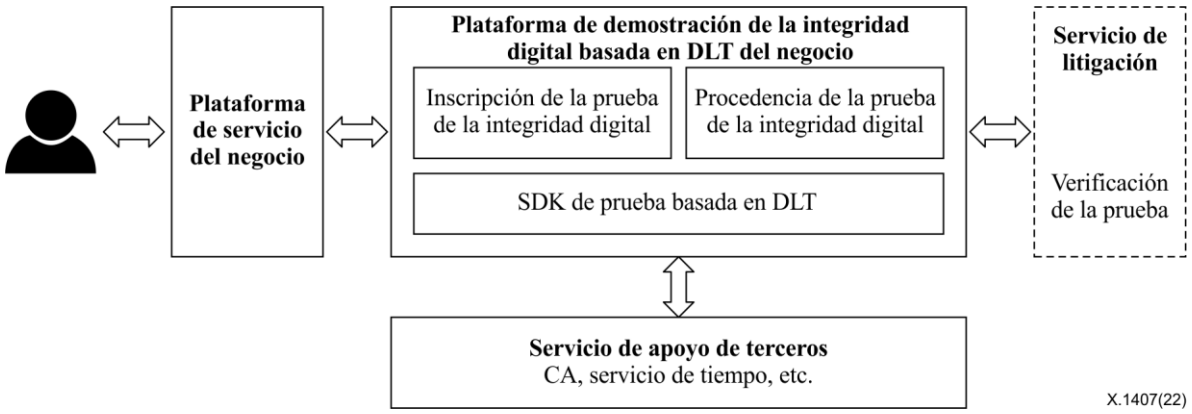

Figura 1 – Ilustración demostración de la integridad digital basada en DLT

Los escenarios básicos en las plataformas de pruebas de integridad digital basada en DLT implican la inscripción de las pruebas y la procedencia de las mismas. El usuario de la plataforma de servicios de negocio inicia una llamada al servicio de pruebas digitales e inscribe la prueba en la DLT y almacena el compendio (hash) de la firma digital extraída mediante el contrato de inscripción de la prueba IP. El proceso de comprobación de la integridad de la prueba depende de la comprobación del valor del compendio de la prueba y de la comparación del hash con los hash almacenados en la DLT. Además, para garantizar el uso legal de una prueba digital y proteger los derechos del usuario, se proporciona un servicio de consulta y comprobación de pruebas digitales para los forenses en casos de litigio en línea.

Aunque las características de trazabilidad y de no manipulación de la DLT permiten un mejor control y explotación de la integridad de los registros, la adopción de la DLT conlleva amenazas de seguridad. Algunas amenazas se dirigen a los usuarios, otras a las pruebas digitales y otras a los procesos de registro y procedencia de las pruebas. Por lo tanto, es necesario y útil resumir las amenazas a la seguridad en las diferentes categorías sobre la base de los análisis de las actividades relacionadas con la prueba de integridad digital basada en DLT. A partir del análisis de estas amenazas, se identifica un conjunto de requisitos de seguridad.

7 Partes interesadas y procesos para la prueba de integridad digital basada en DLT

7.1 Partes interesadas

7.1.1 Partes interesadas internas

Las partes interesadas internas deben incluir a:

a) el usuario;

b) la plataforma de servicio de negocio;

c) la plataforma de demostración de la integridad digital basada en DLT.

7.1.2 Partes interesadas externas

Las partes interesadas externas incluyen a:

a) Servicios de apoyo de terceros, incluidas organizaciones que expiden certificados CA, servicio de tiempo y otros servicios.

b) Organismos reguladores, incluidos los organismos judiciales nacionales y otras organizaciones relacionadas con los litigios.

7.2 Procesos de la prueba de integridad digital basada en DLT

7.2.1 Inscripción de la prueba de integridad digital

Los principales procesos de la inscripción de la prueba de integridad digital en la DLT son los siguientes:

a) El usuario interactúa con una plataforma de servicios comerciales y puede generar la necesidad de proteger la autenticidad de la información comercial. La plataforma comercial envía las características extraídas de la información original a la plataforma de comprobación de la integridad digital basada en DLT.

b) La plataforma de comprobación de la integridad digital basada en DLT genera pruebas electrónicas con las características extraídas, el sello de tiempo y otra información necesaria.

c) La plataforma de comprobación de la integridad digital basada en DLT genera un valor hash único para las pruebas electrónicas mediante funciones hash criptográficas (como SHA256).

d) La plataforma de servicios comerciales genera una firma digital para el valor del hash con la clave privada del propietario.

e) La plataforma de servicios comerciales envía el registro de la prueba a la dirección del contrato inteligente en los libros mayores distribuidos.

f) La plataforma de comprobación de la integridad digital basada en DLT comprueba si la firma digital y la información estás completas, ejecuta el contrato inteligente y genera un registro en el libro mayor.

g) El registro de pruebas se empaqueta en un nuevo bloque y el nuevo bloque se difunde a la red.

7.2.2 Procedencia de la prueba de integridad digital

Los principales procesos de la procedencia de la prueba de integridad digital son los siguientes:

a) El usuario consulta la prueba de la integridad digital en los libros mayores distribuidos.

b) En caso de litigio en línea, la plataforma de litigios lleva a cabo un análisis forense de la prueba digital basado en los registros de los libros mayores distribuidos.

8 Amenazas de seguridad para la comprobación de la integridad digital basada en DLT

En esta cláusula se analizan las amenazas a la seguridad de las partes interesadas, es decir, el usuario, la plataforma de prueba de la integridad digital basada en DLT y los procesos que intervienen en la prueba de la integridad digital basada en DLT, a saber, la inscripción de la prueba de la integridad digital y la procedencia de la prueba de la integridad digital. Las amenazas a los componentes de protocolo, red y datos en las aplicaciones basadas en DLT se describen en detalle en [UIT-T X.1401].

8.1 Amenazas de seguridad con respecto al usuario

8.1.1 Fraude de identidad del usuario

Los usuarios registrados realizan una solicitud ilegal utilizando identidades falsas para obtener un permiso que no se corresponde con su identidad.

8.1.2 Filtración de la clave privada

Las amenazas de filtración de la clave privada en un registro consisten principalmente en ataques a clientes de *software* y ataques físicos (por ejemplo, la exposición de las claves impresas a otras personas). La filtración de la clave privada permite a otros usuarios entrar en la plataforma de pruebas basada en DLT, poniendo en peligro su seguridad. La amenaza de filtración de la clave privada se describe en detalle en la cláusula 6.3.2 de [UIT-T X.1401].

8.1.3 Pérdida de la clave privada

Las amenazas de pérdida de la clave privada consisten principalmente en ataques de *malware*, ataques físicos (por ejemplo, pérdida de claves privadas impresas en papel), etc. Esta pérdida puede ocasionar la revelación de la privacidad del usuario, lo que permite a los usuarios fraudulentos entrar en la plataforma de pruebas basada en DLT y destruir su seguridad. La amenaza de pérdida de la clave privada se describe en detalle en la cláusula 6.3.3 de [UIT-T X.1401].

8.1.4 Divulgación de información privada

La información de la prueba del propietario puede implicar información personal sensible, como el nombre y la información de identificación, y puede existir un problema de filtración de la información privada del usuario durante el proceso de registro de la prueba. La amenaza de divulgación de información privada se describe detalladamente en la cláusula 6.3.1 de [UIT-T X.1401].

8.2 Amenazas a la seguridad en la inscripción de pruebas

8.2.1 Fraude de prueba

Basándose en el algoritmo de extracción de características de la prueba digital, el atacante podría construir diferentes valores de características de contenido similar a los del documento original. De este modo, el atacante podría escribir contenido ilegal en los libros mayores distribuidos.

8.2.2 Manipulación de la prueba

El usuario malicioso puede manipular la prueba del documento original o destruir la integridad y la disponibilidad de la prueba, lo que resulta en la inscripción de la prueba manipulada en los libros mayores distribuidos. Los ataques de algoritmo de cifrado asimétrico pueden dar lugar a una transmisión y un almacenamiento inseguros. El ataque de algoritmo de cifrado asimétrico se describe detalladamente en la cláusula 6.1.5 de [UIT-T X.1401].

8.2.3 Ataque por dependencia del sello de tiempo

Los ataques pueden manipular el servicio de sello de tiempo de la plataforma de pruebas basada en DLT, causando que la plataforma no pueda mantener la secuencia de eventos de inscripción de pruebas con precisión, por lo que carece de la capacidad de proporcionar una base forense eficaz para la procedencia de las pruebas.

8.2.4 Ataque de 51%

Cuando los atacantes dominan más del 51% de la potencia de cálculo, pueden construir una nueva cadena. La nueva cadena puede invalidar la prueba de la cadena principal. Además, un ataque del 51% puede dar lugar a la inscripción con éxito del infractor. El ataque del 51% se describe en detalle en la cláusula 6.1.1 de [UIT-T X.1401].

8.2.5 Ataque por soborno

Cuando los atacantes con recursos suficientes sobornan a los nodos con derecho a voto, pueden vulnerar los derechos e intereses de una red de libro mayor distribuido de pruebas. De este modo, los atacantes escriben información de pruebas ilegales en la red del libro mayor distribuido de pruebas El ataque de soborno se describe en detalle en la cláusula 6.1.1 de [UIT-T X.1401].

8.2.6 Ataque de retención de bloques

En una plataforma de pruebas basada en DLT y en el algoritmo de consenso de prueba de trabajo (PoW), un atacante puede conservar un bloque que hayan minado y minar el siguiente en secreto, si el atacante dispone de potencia suficiente. Al generar más de un bloque cuando otros mineros generan un bloque, el atacante puede hacer que otros mineros desperdicien su energía. El objetivo del ataque es un operador de plataforma que acepta la validación cero. Puede invalidar la prueba de la cadena

principal. También puede provocar la inscripción con éxito del infractor. El ataque de retención de bloques se describe en detalle en la cláusula 6.1.1 de [UIT-T X.1401].

8.2.7 Ataque de salto de cadena

Un atacante puede alternar entre varias cadenas de bloques aprovechando los difíciles algoritmos de ajuste de la cadena. Podría suponer una recompensa injusta para los atacantes con una pérdida para los demás usuarios. También puede provocar un aumento considerable de la potencia de cálculo efectiva en el parque minero. También puede dar lugar al registro exitoso del infractor. El ataque de salto de cadena se describe detalladamente en la cláusula 6.1.1 de [UIT-T X.1401].

8.2.8 Ataque por denegación de servicio distribuido

En una plataforma de pruebas basada en DLT, un atacante puede incapacitar la red mediante ataques por denegación de servicio distribuido (DDoS), siendo los métodos habituales el ataque Sybil y el ataque de eclipse. Esto puede resultar en la inscripción con éxito de una prueba maliciosa. El ataque Sybil se describe detalladamente en la cláusula 6.2.3 y el eclipse en la cláusula 6.2.1 de [UIT-T X.1401].

8.2.9 Ataque de secuestro de BGP

Un atacante puede aprovechar el protocolo de pasarela de frontera (BGP) secuestrado y los nodos de red de los libros mayores distribuidos quedan divididos en dos o más partes. Como resultado, la DLT se divide en dos o más cadenas paralelas. En este momento, la inscripción de pruebas y la inscripción de pruebas maliciosas pueden realizarse en ramas paralelas. Una vez finalizado el ataque, el libro mayor distribuido de pruebas se reunifica con la cadena principal más larga, las demás ramas se descartan, y todas las inscripciones de pruebas en estas cadenas quedan invalidadas, lo que puede dar lugar a la inscripción con éxito de pruebas maliciosas.

8.3 Amenazas a la seguridad en relación con la procedencia de las pruebas

8.3.1 Ataque de escritura de información maliciosa

Todos los datos de transacción en un DLT son inamovibles. Una vez que la información se escribe en el DLT, no puede borrarse. Los atacantes pueden escribir información maliciosa en los libros mayores distribuidos lanzando ataques de contratos inteligentes, por ejemplo, ataques de excepciones erróneamente tratadas, como se describe en detalle en la cláusula 6.1.2 de [UIT-T X.1401]. La plataforma genera nuevos bloques que dan lugar a ataques de bloques basura, afectando así al rendimiento de una plataforma de pruebas basada en DLT.

8.3.2 Revelación de información de prueba

En una prueba de procedencia, se debe utilizar un algoritmo para encriptar y almacenar la información de la prueba. Es importante garantizar la seguridad del algoritmo de cifrado. Los ataques al algoritmo de cifrado asimétrico pueden dar lugar a un estado inseguro de la plataforma de pruebas basada en DLT. El ataque al algoritmo de cifrado asimétrico se describe con detalle en la cláusula 6.1.5 de la norma [UIT-T X.1401].

9 Requisitos de seguridad para la prueba de integridad digital basada en DLT

En esta cláusula se describen los requisitos de seguridad para la comprobación de la integridad digital basada en la DLT, a partir del análisis de las amenazas a la seguridad descritas en la cláusula 7. Además, se describen los requisitos de seguridad para las partes interesadas, es decir, el usuario, la plataforma de comprobación de la integridad digital y los procesos que intervienen en los servicios de comprobación de la integridad digital basados en DLT, a saber, la inscripción de la prueba digital y la procedencia de la prueba digital. Los requisitos de seguridad de los datos, la red, el consenso y la aplicación se describen detalladamente en las cláusulas 8.1 a 8.4 de [UIT-T X.1402].

9.1 Requisitos de seguridad para el usuario

9.1.1 Protección de la identidad del usuario

Se definen los siguientes requisitos de seguridad para evitar el fraude de identidad en la plataforma de prueba de la integridad digital basada en DLT.

a) La plataforma de comprobación de la integridad digital basada en la DLT debería especificar la autoridad funcional de los distintos usuarios. La plataforma debería permitir al usuario utilizar la clave privada para firmar la información y enviarla a la DLT. La DLT debe recuperar la clave pública basándose en la firma, identificar a los usuarios basándose en la clave pública y autenticar las operaciones de los usuarios.

b) Cuando un usuario se inscribe en la plataforma, ésta primero audita la información de identidad del usuario, y luego puede asignar una etiqueta a cada usuario.

c) La plataforma de comprobación de la integridad digital basada en DLT debe escribir todas las operaciones de cada usuario en los libros mayores distribuidos.

d) La plataforma de comprobación de la integridad digital basada en DLT debería exigir la existencia de una función de autenticación de la identidad para cada inscripción de comprobación, incluyendo el control de acceso, la contraseña, la firma digital y el reconocimiento biométrico, etc.

9.1.2 Protección de la clave privada

Se definen los siguientes requisitos de seguridad relacionados con la protección de la clave privada para la plataforma de pruebas basada en DLT.

a) La plataforma de comprobación de la integridad digital basada en DLT debe evitar la filtración de la clave privada: el operador de una plataforma de comprobación basada en DLT debe evitar la intrusión de código malicioso en su cliente.

b) La plataforma de comprobación de la integridad digital basada en DLT debe evitar la pérdida de la clave privada: los usuarios de una plataforma de comprobación basada en DLT deben mantener la clave privada en un lugar seguro y evitar dejar las claves privadas en soportes físicos y no físicos de fácil acceso (por ejemplo, papel de impresión) sin ningún mecanismo de protección; entre las posibles contramedidas se encuentran los códigos numéricos de identificación personal, las contraseñas, las huellas dactilares y otra información biométrica, etc.

9.1.3 Protección de la privacidad

La plataforma de comprobación de la integridad digital basada en DLT debe adoptar las medidas de protección de seguridad pertinentes en las fases de procesamiento de la información de la recopilación, el almacenamiento, el uso, el intercambio, la transferencia, la divulgación pública, etc., para evitar la recopilación, el abuso y la filtración ilegal de la información del propietario, y para lograr la máxima protección de los derechos e intereses legítimos del propietario.

9.2 Requisitos de seguridad para la inscripción de pruebas

9.2.1 Evitar el fraude en la prueba

Para la plataforma de pruebas basada en DLT se definen los siguientes requisitos de seguridad para evitar el fraude en las pruebas digitales.

a) La plataforma de pruebas basada en DLT debe proporcionar algoritmos de consenso, con un nivel de garantía de seguridad (LoSA) y una intensidad del mecanismo de consenso (CMS) [UIT-T X.1404], por ejemplo, tolerancia práctica frente a fallos bizantinos (PBFT) para evitar la falsificación de pruebas digitales.

b) La plataforma de pruebas basada en DLT debe supervisar la potencia de cálculo efectiva de la red, para detectar cambios anómalos y evitar ataques de salto de cadena.

c) La plataforma de pruebas basada en DLT debe aumentar la dificultad de los algoritmos de construcción de valores propios, al tiempo que garantiza que la eficiencia operativa del sistema se encuentra dentro de un rango razonable.

9.2.2 Evitación de la manipulación de pruebas

Para la plataforma de pruebas basada en DLT se definen los siguientes requisitos de seguridad relacionados con la evitación de la manipulación de las pruebas digitales.

a) La plataforma de pruebas basada en DLT debería utilizar equipos encriptados.

b) La plataforma de pruebas basada en la DLT debe utilizar algoritmos de encriptación para garantizar la transmisión segura de la información de las pruebas. Los servicios de terceros relacionados deben utilizar algoritmos de cifrado para garantizar el almacenamiento seguro de la información sobre pruebas. La plataforma y los servicios de terceros relacionados deben elegir algoritmos de encriptación apropiados, que deben ofrecer un compromiso entre la seguridad y el coste de computación, y la longitud de las claves – se puede optar por aumentar la longitud de las claves para compensar los riesgos causados por el aumento de la potencia de computación.

9.2.3 Protección de la inscripción de pruebas

Se definen los siguientes requisitos de seguridad relacionados con el control de seguridad de la inscripción para la plataforma de pruebas basada en DLT.

a) La plataforma de comprobación de la integridad digital basada en DLT deberá sincronizarse con un servicio horario de terceros de confianza.

b) La plataforma de comprobación de la integridad digital basada en DLT debe emitir avisos de ataque a la seguridad, vulnerabilidad, código malicioso, análisis de amenazas y filtración de datos, así como otra información de inteligencia sobre amenazas, e identificar los problemas existentes en la plataforma mediante la exploración de vulnerabilidades y la realización de pruebas de seguridad automatizadas.

c) La plataforma de comprobación de la integridad digital basada en DLT debe proporcionar autenticación de identidad y control de acceso para mitigar los riesgos de ataque a la seguridad, por ejemplo, la manipulación maliciosa y el ataque a distancia.

d) En el caso de las aplicaciones móviles, la plataforma de comprobación de la integridad digital basada en DLT debe proporcionar métodos de protección de la seguridad, por ejemplo, mediante el refuerzo y la dificultad de identificación de la fuente para evitar el análisis inverso, la descompilación y la incrustación de códigos maliciosos.

e) La plataforma puede utilizar la tecnología de punto de control para escribir al cliente mediante codificación sistemática de modo que el cliente aceptará todas las transacciones efectivas antes del punto de control, evitando así el ataque del 51%; el punto de control debería: introducir un mecanismo de consenso de prueba de participación (PoS) mejorado con medidas de margen y penalización; establecer un sello de tiempo para la transacción; establecer la autenticación de nodos fiables de terceros para autenticar la identidad; y no aceptar la confirmación cero.

f) La plataforma puede desplegar el filtrado de puertos para la limpieza del tráfico anormal, la defensa de la seguridad en la nube y la alta defensa para la resolución del sistema de nombres de dominio (DNS) en el sistema a fin de proporcionar una implementación segura, y debe regular el tamaño de los bloques de datos para evitar ataques de bloques basura.

g) La plataforma de comprobación de la integridad digital basada en DLT debe prever la recopilación de pruebas y el rastreo de los incidentes de seguridad, analizar los motivos y proporcionar métodos para frenar ataques.

9.3 Requisitos de seguridad para la procedencia de la prueba

9.3.1 Prevención contra la escritura de información maliciosa

Para garantizar la seguridad de la procedencia de las pruebas, la plataforma de comprobación de la integridad digital basada en DLT debe:

a) regular el tamaño del bloque de datos para evitar que los nodos generen bloques de *spam*;

b) garantizar que las entidades no autorizadas y anónimas no puedan buscar o acceder a los datos de las cuentas y las transacciones en los nodos del sistema de libro mayor distribuido;

c) utilizar bibliotecas que garanticen la seguridad del cálculo, como SafeMath;

d) revisar el código para evitar el desbordamiento de enteros y las excepciones mal manejadas a fin de evitar ataques en los contratos inteligentes;

e) utilizar generadores aleatorios imprevisibles para evitar que usuarios maliciosos controlen los resultados de los contratos inteligentes;

f) velar por que el diseño del control de acceso durante el desarrollo del programa sea lo más estricto posible a fin de evitar que la titularidad de las funciones de los contratos inteligentes sea manipulada por los atacantes para obtener la máxima autoridad de operación.

9.3.2 Protección de la información de prueba

Para garantizar la seguridad de la información de prueba, la plataforma de comprobación de la integridad digital basada en DLT debe:

a) utilizar equipos encriptados para almacenar la información de la prueba fuera de la cadena;

b) elegir los algoritmos de encriptación adecuados, que deben ofrecer un compromiso entre la seguridad y el coste informático, y la longitud de las claves: podría optar por aumentar la longitud de las claves para compensar los riesgos causados por el aumento de la potencia de cálculo;

c) utilizar un mecanismo eficaz de control de acceso para garantizar un acceso controlable a la información de prueba.

Apéndice I

Caso de uso de la factura electrónica basada en la tecnología de libro mayor distribuido

(Este apéndice no forma parte integrante de esta Recomendación.)

Con arreglo al mecanismo de consenso, sólo pueden verificarse y aprobarse las facturas emitidas por las autoridades fiscales, y las emitidas por cualquier otro nodo no pueden confirmarse, lo que garantiza la autenticidad de las facturas. Con los contratos inteligentes, las transacciones y la facturación se producen simultáneamente, y los pagos y la facturación de los consumidores se realizan sin problemas. En la Figura I.1 se ofrece una visión general. Para más detalles, consulte [b-IEEE 2142.1-2021] – *Recommended practice for e-invoice business using blockchain technology*.

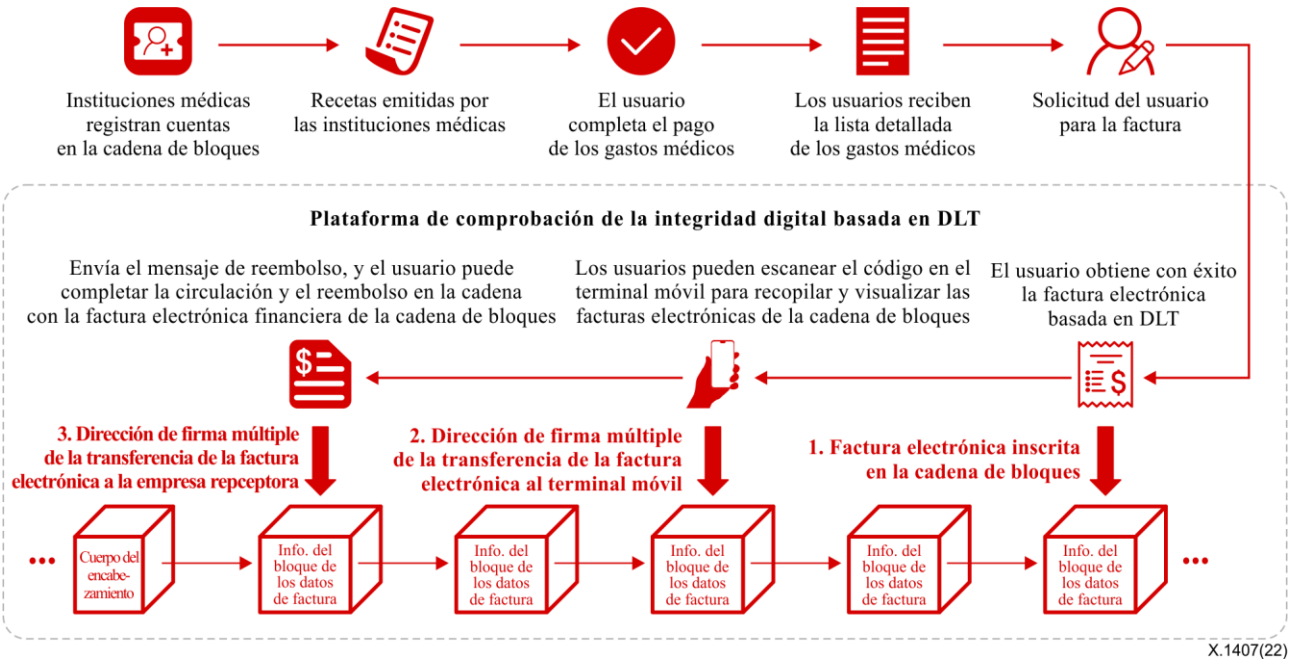

Figura I.1 – Visión general del caso de uso de la factura electrónica basada en DLT

El caso de uso de facturas electrónicas basadas en la tecnología de libro mayor distribuido por parte de las instituciones médicas se describe como sigue:

a) Las instituciones médicas registran una cuenta en la cadena de bloques, se conectan al sistema de facturación basado en DLT y establecen las condiciones de facturación en la cadena.

b) La institución médica emite una receta.

c) El usuario completa el pago de los gastos médicos con una receta.

d) El usuario recibe una lista detallada de los gastos médicos una vez completado el pago.

e) El usuario solicita la facturación.

f) El usuario obtiene con éxito una factura electrónica de la cadena de bloques.

g) Los usuarios pueden escanear el código en el terminal móvil para recibir y ver la factura electrónica de la cadena de bloques.

h) El terminal móvil puede enviar mensajes de reembolso, y los usuarios pueden utilizar la factura electrónica de la cadena de bloques para completar la circulación y el reembolso en la cadena.

El proceso de facturación basado en el pago puede incluir las siguientes fases:

– Fase A: transacción
– Fase B: emisión de factura
– Fase C: reembolso
– Fase D: liquidación fiscal

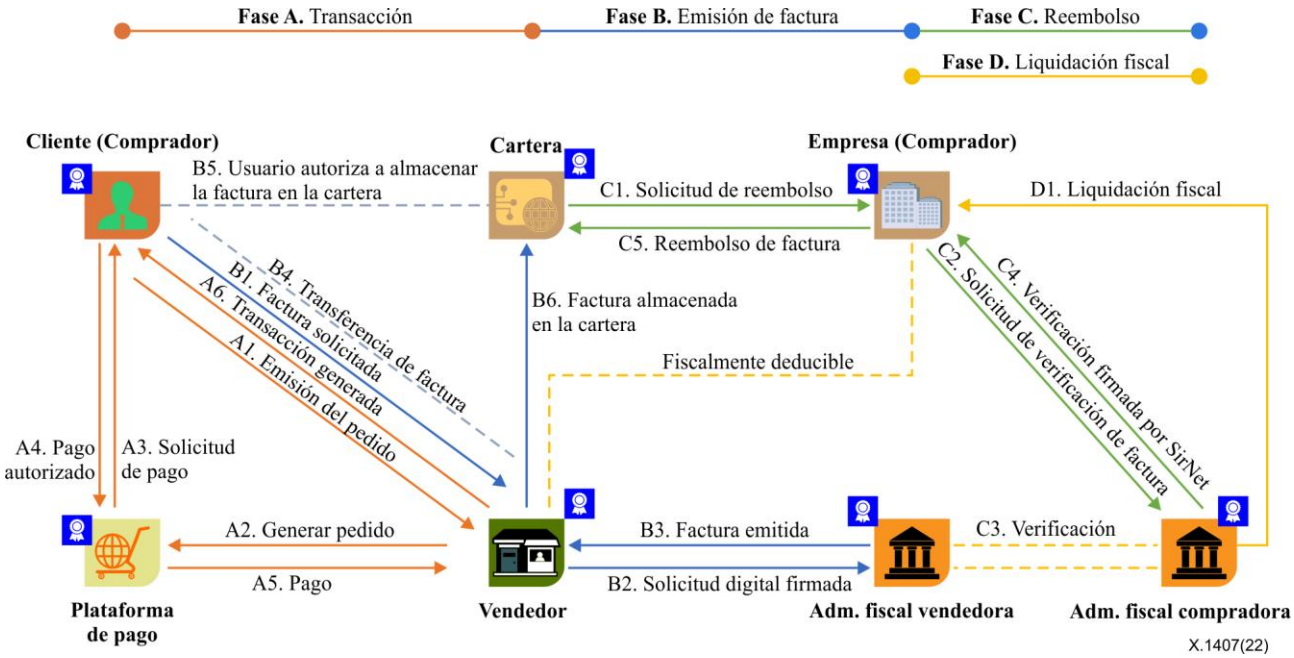

Figura I.2 – Gráfica de flujo del caso de uso de la factura electrónica basada en DLT

En la fase de transacción, cuando el cliente (es decir, el comprador) hace un pedido, el proveedor de servicios (es decir, el vendedor) genera el pedido a través de la plataforma de pago, la plataforma de pago confirma el pedido después de recibir la autorización del cliente, y el recibo se genera cuando se procesa el pago. El recibo puede adoptar la forma de un bloque de pago a través de una cadena de pago o de un registro en una base de datos centralizada.

En la fase de emisión de la factura, la administración fiscal (TAX) de origen del comerciante emite la factura basándose en la solicitud del cliente desde la cartera del mismo, por ejemplo, y el recibo de pago se utiliza como resultado de transacción no utilizado (UTXO) para la emisión de la factura. Los nodos participantes incluyen los nodos de consenso centrales anclados en la capa central del libro mayor, así como los nodos de verificación de pago simplificada (SPV), como el nodo del comerciante, el nodo de la cartera personal.

En la fase de reembolso, la empresa asociada al cliente (CAE) como nodo SPV verifica la factura cuando el cliente inicia el proceso de reembolso y la factura en la cartera personal se vuelve a pagar como UTXO.

En el proceso de liquidación de impuestos, los nodos de la administración tributaria (TAX) de destino y el nodo CAE SPV se unen al proceso, la factura se utiliza como UTXO para reembolsar el IVA.

El sistema de facturación electrónica mediante DLT presenta las siguientes ventajas:

1) Se garantiza la autenticidad de la factura y la trazabilidad de todo el proceso de cobro, emisión, circulación, ingreso y reembolso de la misma.

2) Los datos de la factura no pueden ser manipulados, y la agencia tributaria, la parte que factura, la parte que circula y la parte que reembolsa participan conjuntamente en el proceso contable.

3) La factura electrónica basada en DLT no necesita discos fiscales ni equipos especiales. En el caso de las facturas tradicionales, se requiere de múltiples discos fiscales para cada tienda de las cadenas de tiendas. La factura electrónica basada en DLT es reembolsada automáticamente por la ERP y el número de tiendas no supone un coste adicional.

4) En el caso de facturas tradicionales, si el número de facturas aprobadas por las autoridades fiscales no puede satisfacer las necesidades de la empresa debido al aumento temporal del volumen de negocio, el contribuyente puede solicitar facturas adicionales a las autoridades fiscales. Sin embargo, las facturas basadas en DLT se suministran a la demanda y no necesitan procesos de solicitud adicionales.

5) Se necesita tiempo y esfuerzo para recoger y comprar el papel de la factura tradicional de la oficina de impuestos, mientras que las facturas electrónicas basadas en DLT no necesitan papel.

Apéndice II

Caso de uso para la verificación de certificados académicos basado en la tecnología de libro mayor distribuido

(Este apéndice no forma parte integrante de esta Recomendación.)

La verificación de los certificados es un proceso que lleva mucho tiempo, ya que puede requerir días o semanas. Los empleadores se preocupan por la autentificación de las cualificaciones y dedican tiempo considerable a comunicarse con las universidades para verificar la integridad de los certificados y asegurarse de que los solicitantes tienen una cualificación impecable. La cadena de bloques proporcionará transparencia y simplificará el intercambio de los certificados autentificados con diversos empleadores o con cualquier otra parte.

Los empleadores pueden probar la integridad del certificado académico utilizando DLT. La DLT proporciona una fuente segura y reconocida para almacenar las calificaciones de los estudiantes, a la que pueden acceder diversas instituciones y universidades. Proporciona un registro público permanente, a salvo de los cambios de la institución o de la pérdida de sus registros privados.

Este patrón consta de los siguientes componentes:

Usuarios

– Emisor (Universidad)
– Receptor (Estudiantes)
– Verificador (Empleadores)

Sistemas

– Los nodos de las universidades
– La plataforma de la cadena de bloques

Datos

– Los hashes de los certificados
– Archivo del certificado electrónico

El proceso de comprobación de la integridad del certificado depende de la comprobación del valor hash del certificado y de la comparación del hash con los hashes almacenados en la cadena de bloques, tal y como se muestra en la Figura II.1. Los pasos son los siguientes:

– La universidad emite un nuevo certificado electrónico para un estudiante y carga el archivo en DLT.
– El DLT compendia y almacena el archivo del certificado.
– Para la prueba de integridad, el estudiante o el empleador suben el documento del certificado a la plataforma DLT.
– La DLT genera el hash del documento y luego compara el valor del hash generado con los hashes almacenados en la cadena de bloques.
– Si el hash generado coincide con uno de los hashes almacenados en la cadena de bloques, el certificado es auténtico.

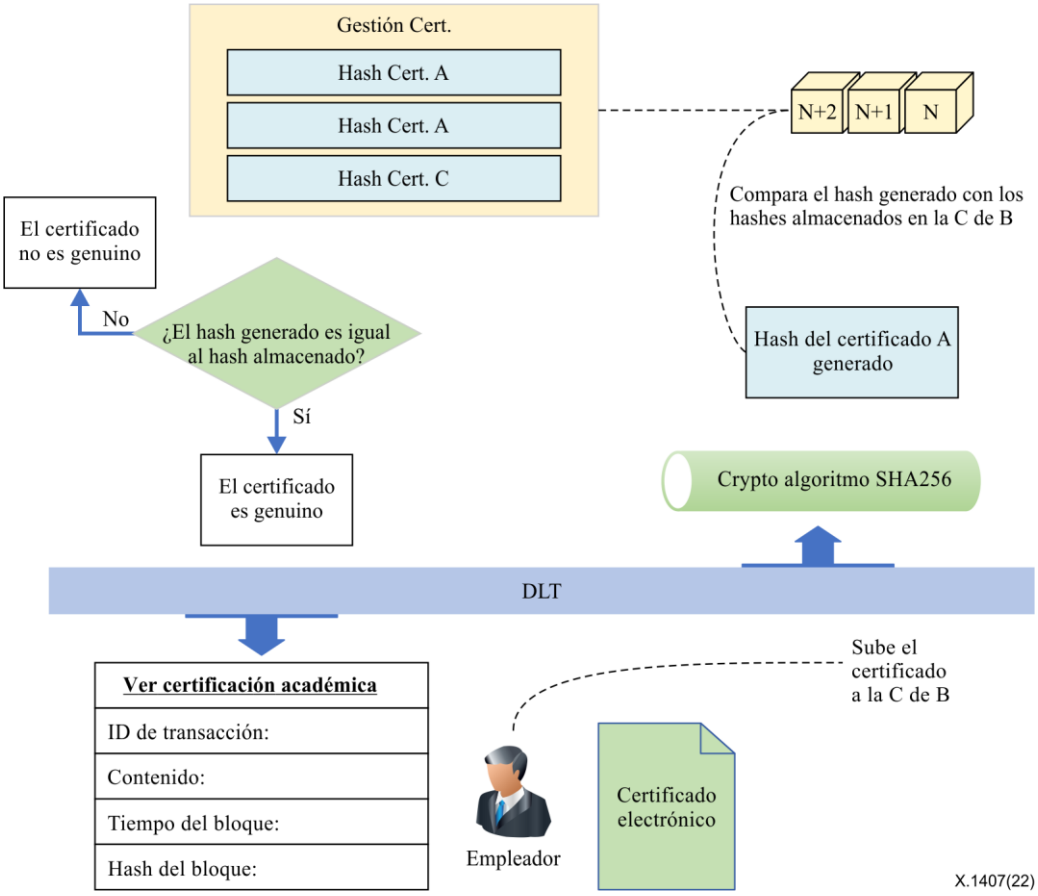

Figura II.1 – Visión general del caso de uso de la verificación de certificados académicos basada en DLT

Ventajas del uso de DLT para autenticar los certificados académicos:

– La DLT resuelve las dificultades actuales del proceso de validación y autenticación.

– La DLT puede agrupar a todas las universidades en una misma plataforma.

– La tecnología DLT insta a los empresarios a trabajar con las universidades de forma sistemática.

– La DLT ayuda a guardar y compartir información auténtica e integral como una fuente de verdad.

– La DLT ahorra tiempo, costes y esfuerzos.

Bibliografía

[b-UIT-T X.1400] Recomendación UIT-T X.1400 (2020), *Términos y definiciones utilizados en la tecnología de libro mayor distribuido*.

[b-ISO 13491-2] ISO 13491-2:2017(en), *Financial services – Secure cryptographic devices (retail) – Part 2: Security compliance checklists for devices used in financial transactions*.
<https://www.iso.org/obp/ui/#iso:std:iso:13491:-2:ed-4:v1:en>

[b-ISO 23257] ISO 23257:2022, *Blockchain and distributed ledger technologies – Reference architecture*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018(en), *Information technology – Security techniques –Information security management systems – Overview and vocabulary*.
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

[b-ISO 22739] ISO 22739: 2020, *Blockchain and distributed ledger technologies – Vocabulary*.
<https://www.iso.org/standard/73771.html>

[b-IEEE 2142.1-2021] IEEE 2142.1-2021, *IEEE Recommended practice for e-invoice business using blockchain technology*.
<https://standards.ieee.org/ieee/2142.1/7590/>

[b-ISO 56000] ISO 56000:2020, *Innovation management – Fundamentals and vocabulary*.
<https://www.iso.org/standard/69315.html>

[b-ISO 5807] ISO 5807:1985, Information processing – *Documentation symbols and conventions for data, program and system flowcharts, program network charts and system resources charts*.
<https://www.iso.org/standard/11955.html>

[b-Kaur] Kaur, S., Chaturvedi, S., Sharma, A. Kar, J. (2021), *A Research Survey on Applications of Consensus Protocols in Blockchain*, Security and Communication Networks, Vol. 2021, Article ID 6693731, enero, pp. 1-22. https://doi.org/10.1155/2021/6693731

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2022