ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T F.751.8 (07/2023)

SERIE F: Servicios de telecomunicación no telefónicos

Servicios multimedia

Marco técnico de la tecnología de libro mayor distribuido (DLT) para hacer frente a la regulación

RECOMENDACIONES UIT-T DE LA SERIE F

Servicios de telecomunicación no telefónicos

SERVICIO TELEGRÁFICO	F.1-F.109
Métodos de explotación del servicio público internacional de telegramas	F.1-F.19
La red géntex	F.20-F.29
Conmutación de mensajes	F.30-F.39
El servicio internacional de telemensajes	F.40-F.58
El servicio internacional télex	F.59-F.89
Estadísticas y publicaciones relativas a los servicios telegráficos internacionales	F.90-F.99
Servicios de telecomunicación a horas fijas y arrendados	F.100-F.104
Servicio de telefotografía	F.105-F.109
SERVICIO MÓVIL	F.110-F.159
Servicio móvil y servicios por satélite con destinos múltiples	F.110-F.159
SERVICIOS DE TELEMÁTICA	F.160-F.399
Servicio facsímil público	F.160-F.199
Servicio teletex	F.200-F.299
Servicio videotex	F.300-F.349
Aspectos generales de los servicios de telemática	F.350-F.399
SERVICIOS DE TRATAMIENTO DE MENSAJES	F.400-F.499
SERVICIOS DE DIRECTORIO	F.500-F.549
COMUNICACIÓN DE DOCUMENTOS	F.550-F.599
Comunicación de documentos	F.550-F.579
Interfaces de comunicación de programación	F.580-F.599
SERVICIOS DE TRANSMISIÓN DE DATOS	F.600-F.699
SERVICIOS MULTIMEDIA	**F.700-F.799**
SERVICIOS DE LA RDSI	F.800-F.849
TELECOMUNICACIÓN PERSONAL UNIVERSAL	F.850-F.899
ACCESIBILIDAD Y FACTORES HUMANOS	F.900-F.999

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

Recomendación UIT-T F.751.8

Marco técnico de la tecnología de libro mayor distribuido (DLT) para hacer frente a la regulación

Resumen

En la Recomendación UIT-T F.751.8 se define el marco técnico de la tecnología de libro mayor distribuido (DLT) para hacer frente a la regulación, y se incluyen los retos que ésta plantea, así como las capacidades técnicas. El diseño del marco técnico de DLT de esta Recomendación está estrechamente relacionado con las propiedades de la DLT, incluidas la descentralización, la inmutabilidad y la apertura. Esta Recomendación puede servir de guía para que los sistemas DLT hagan frente a la regulación impuesta a los proveedores de servicio DLT y los creadores de sistemas DLT.

Historia *

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único
1.0	UIT-T F.751.8	2023-07-10	16	11.1002/1000/15174

Palabras clave

Cadena de bloques, reglamentación, tecnología de libro mayor distribuido.

* Para acceder a la Recomendación, sírvase digitar el URL https://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación.

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 se pronuncia en lo que respecta a la existencia, validez o aplicabilidad de los derechos de propiedad intelectual reclamados, 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 patentes/derechos de autor de *software*, 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 en http://www.itu.int/ITU-T/ipr/.

Índice

Recomendación UIT-T F.751.8

Marco técnico de la tecnología de libro mayor distribuido (DLT) para hacer frente a la regulación

1 Alcance

En esta Recomendación se define un marco técnico para que la tecnología de libro mayor distribuido (DLT) puede hacer frente a la regulación. Dentro del alcance de esta Recomendación se incluyen:

– los retos reglamentarios en relación con la DLT;

– las capacidades técnicas de la DLT para hacer frente a la regulación.

Esta Recomendación está destinada a los proveedores de servicio DLT y a los creadores de sistemas DLT, no a los reguladores de la DLT. El objetivo de esta Recomendación no es ofrecer soluciones reglamentarias para los reguladores de DLT, sino proponer soluciones técnicas a los retos que plantea la regulación de la DLT.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

[UIT-T F.751.0] Recomendación UIT-T F.751.0 (2020), *Requirements for distributed ledger systems*.

[UIT-T X.1401] Recomendación UIT-T X.1401 (2019), *Seguridad de tecnología de libro mayor distribuido (DLT)*.

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 consenso [b-UIT-T X.1400]: Acuerdo sobre la validez de un conjunto de transacciones.

3.1.2 mecanismo de consenso [b-UIT-T X.1400]: Reglas y procedimientos mediante los cuales se alcanza el consenso.

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

3.1.4 privacidad [b-UIT-T J.160]: Medio de asegurarse de que no se revela información a nadie más que a las partes deseadas. Para proteger la confidencialidad la información suele encriptarse. Se conoce también como confidencialidad.

3.1.5 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 esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

AML Lucha contra el blanqueo de dinero (*anti-money-laundering*)

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

GAFI Grupo de Acción Financiera Internacional contra el blanqueo de capitales

IoT Internet de las cosas (*Internet of things*)

KYC Conocimiento del cliente (*know your customer*)

PKI Infraestructura de clave pública (*public key infrastructure*)

TEE Entorno de ejecución fiable (*trusted execution environment*)

5 Convenios

En esta Recomendación se utilizan los siguientes convenios:

– La expresión «**se requiere**» y la utilización del futuro «deberá» indican que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con esta Recomendación.

– La expresión «**se recomienda**» indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

– La expresión «**puede (opcionalmente)**» indica que el requisito se permite, sin que ello signifique que se recomienda. No se pretende implicar que el fabricante deba ofrecer esta opción y que el operador de red/operador de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

6 Generalidades

La tecnología de libro mayor distribuido (DLT) permite a grandes grupos de nodos de la red de libro mayor distribuido llegar a acuerdos y registrar información sin una autoridad central. El rápido Desarrollo de la DLT supone un reto para la regulación, entre otras cosas, de la protección de la privacidad/confidencialidad, la protección de los datos, el tratamiento de los ataques a la red y las criptodivisas. La DLT se utiliza en varios dominios, como las criptodivisas, la gestión de la cadena de producción y la Internet de las cosas (*IoT, Internet of Things*). Es, por tanto, necesario resumir los requisitos reglamentarios a partir del análisis de las funciones y propiedades de la DLT y definir un marco técnico para colmar la brecha entre la apertura y la regulación. Se ha realizado un trabajo precursor [b-DLT 4.1], que ha evolucionado en la especificación técnica que se presenta a continuación.

7 Retos reglamentarios

7.1 Fuga de información confidencial

Puede haber fugas de información confidencial directamente en la cadena, en las que se combinan datos externos con datos de dentro y fuera de la cadena. Puede haber transacciones y claves públicas directamente disponibles en la cadena, sobre todo en los sistemas DLT sin permisos. Los datos externos pueden permitir la identificación de claves púbicas con personas o empresas y, así, permitir la identificación de las transacciones.

En los libros distribuidos sin permisos no hay control de acceso y cualquiera puede acceder a todos los datos directamente almacenados en la cadena. El almacenamiento (no encriptado) de datos confidenciales en un libro distribuido sin permisos se considera una fuga de datos confidenciales.

7.2 Inmutabilidad de los registros y ausencia de funcionalidad para suprimir transacciones/contenido

En función de la aplicación DLT y del tipo de datos de que se trate, la regulación exige que se supriman los datos personales. Este requisito está inscrito en leyes y reglamentos, lo que puede entrar en conflicto con la inmutabilidad de los sistemas DLT.

NOTA – El «derecho al olvido» del Artículo 17 del Reglamento General de Protección de Datos de la Unión Europea ([b-RGPD]) es un ejemplo de requisito de supresión de datos.

La regulación de la protección de datos y otras legislaciones puede también exigir la corrección de las transacciones, lo que sólo es posible utilizando bifurcaciones que ponen en riesgo la fiabilidad de los sistemas de libro mayor distribuido.

7.3 Amenazas a la seguridad

Las amenazas a la seguridad de los componentes DLT se abordan en las cláusulas 5.1 (*threats to protocols* (amenazas a los protocolos)), 5.2 (*threats to networks* (amenazas a las redes)) y 5.3 (*threats to data* (amenazas a los datos)) de [UIT-T X.1401].

7.4 Pérdida de testigos, divisas digitales y otros activos

La pérdida de testigos, divisas digitales y otros activos suelen ser resultado de amenazas a los datos. Sin embargo, esas pérdidas también pueden tener su origen en engaños premeditados relacionados con monedas fraudulentas, sistemas de libro mayor distribuido fraudulentos o las entidades tras las direcciones de cuentas. Con ataques de usurpación de identidad también se puede engañar a la gente para que haga transacciones que no haría de otra manera.

7.5 Delitos financieros y de otro tipo

Los sistemas de libro mayor distribuido pueden utilizarse para cometer delitos financieros, como el blanqueo de capitales, o para facilitar la comisión de otros delitos como los ataques de *ransomware*, entre otros. Las transacciones pueden contener contenidos ilegales que obedecen a las reglas del protocolo, pero infringen los reglamentos y demás legislación.

8 Capacidades técnicas para hacer frente a la regulación

8.1 Marco técnico

El diseño del marco técnico de DLT para hacer frente a la regulación está muy relacionado con las propiedades de la DLT, incluidas la descentralización, la autonomía, la inmutabilidad, la apertura, la transparencia y la anonimia. Las capacidades técnicas de la DLT para hacer frente a la regulación se definen según los siguientes aspectos: nivel de aplicación, privacidad/confidencialidad, supresión de datos, seguridad de datos y nivel básico. En la DLT con permisos, la responsabilidad es esencial y se

recomienda a los proveedores de servicio DLT que definan una entidad jurídica orquestadora subyacente para reducir la incertidumbre de las medidas reglamentarias.

8.2 Capacidades a nivel de aplicación

– Se recomienda que los sistemas DLT que se utilizan para transferir activos digitales tengan incluido un módulo que soporte las normas del GAFI y/o de la reglamentación nacional específica.

– Se recomienda que la DLT con permisos soporte funcionalidades de conocimiento del cliente (KYC, *know your customer*) y de lucha contra el blanqueo de dinero (AML, *anti-money-laundering*) empleando técnicas como las firmas basadas en infraestructura de clave pública (PKI, *public key infrastructure*).

– Los proveedores de servicio DLT y los creadores de sistemas DLT pueden utilizar técnicas como la limitación de los derechos de transacción y el bloqueo de cuentas para intervenir las transacciones creadas por nodos malignos y anormales.

– Los proveedores de servicio DLT y los creadores de sistemas DLT pueden facilitar un enlace a una PKI reconocida oficialmente, que puede opcionalmente utilizarse para identificar las transacciones con una entidad legítima.

8.3 Capacidades de privacidad/confidencialidad

– Se recomienda que los sistemas DLT no publiquen información confidencial o datos personales que contengan información sobre la identidad de las cuentas, datos personales/información de identificación personal, datos de transacciones, información de activos digitales u otro tipo de información confidencial a menos que exista una justificación para publicarla.

– No se recomienda almacenar datos con este tipo de información en sistemas DLT sin permisos. Si un Sistema DLT necesita verificar este tipo de información, se recomienda almacenar únicamente un compromiso u otro tipo de prueba de los datos en el sistema DLT.

– De no poder evitarse el almacenamiento de los datos en un sistema DLT, se recomienda utilizar métodos criptográficos, como las pruebas de conocimiento cero, la confusión de cuentas o métodos basados en el aislamiento del *hardware* (es decir, entornos de ejecución fiables (TEE, *trusted execution environment*)) para proteger los datos confidenciales (datos personales o de empresas) contra su divulgación.

– Se recomienda proteger adecuadamente los datos confidenciales fuera de la cadena utilizando métodos criptográficos adecuados.

– Se recomienda que los sistemas DLT que almacenan información confidencial ofrezcan un control de acceso adecuado para garantizar que sólo es posible el acceso autorizado. Se recomienda limitar el acceso a aquéllos que poseen una autorización y/o en los casos en que el acceso esté autorizado.

– Se recomienda que el almacenamiento fuera de la cadena utilice métodos de control de acceso adecuados.

– Pueden utilizarse opcionalmente funciones de encriptación, pruebas de conocimiento cero y funciones de aleatorización criptográfica para proteger la información en la cadena. Sin embargo, el almacenamiento en la cadena inmutable plantea el problema de que los métodos de acceso comprometidos no pueden bloquearse. Se recomienda realizar un análisis de riesgos y/o un análisis de consecuencias de la protección de datos en relación con el almacenamiento en la cadena de datos personales/confidenciales.

8.4 Capacidades de supresión de datos

Una de las propiedades esenciales de los sistemas de libro mayor distribuido es la inmutabilidad de alto nivel. Eliminar por completo la inmutabilidad implicaría en muchos casos eliminar el motivo original por el que se opta por un sistema de libro mayor distribuido.

Cuando no se quiere la inmutabilidad para todos los atributos de una transacción se recomienda almacenar los datos fuera de la cadena y validarlos únicamente, por ejemplo, almacenando una prueba que valide los datos fuera de la cadena. Para ello pueden almacenarse en la cadena tecnologías como las pruebas de conocimiento cero, compromisos de datos o valores aleatorios. Se requiere tener mucho cuidado para que no se puedan derivar de los datos almacenados en la cadena informaciones no deseadas.

En algunos casos es posible que no baste con la verificación de los datos fuera de la cadena y siga siendo necesaria la persistencia de los datos. Incluso entonces es posible que la persistencia de los datos sólo sea necesaria durante un periodo de tiempo concreto o mientras se cumplan determinadas condiciones. Ejemplos de ello son los datos de transacción que deben preservarse mientras no haya una transacción posterior y cuando los registros deban conservarse durante un periodo específico de tiempo (por ejemplo, 10 años). En tales casos, puede crearse un libro mayor distribuido que automáticamente suprima los datos cuando se haya completado la transacción siguiente o cuando se haya cumplido el plazo exigido. Puede utilizarse opcionalmente técnicas como la poda [b-Nakamoto] los generadores camaleón [b-Camenisch].

Cuando se utilicen esas tecnologías:

– Deberá definirse claramente qué partes del libro mayor deben permanecer inmutables.
– Deberá definirse claramente en qué condiciones pueden modificarse otras partes.
– El protocolo del libro mayor distribuido deberá definir cómo se suprimirán los datos.
– El protocolo del libro mayor distribuido deberá garantizar que los datos que no han de suprimirse o modificarse seguirán estando protegidos contra toda modificación.
– Deberá garantizarse que las copias de archivo del libro mayor sólo se mantendrán de conformidad con la reglamentación aplicable.

El objetivo de la supresión de datos es responder a las exigencias reglamentarias de la legislación, las recomendaciones o demás requisitos locales. Se recomienda limitar la funcionalidad de supresión a parte de los datos, a fin de conservar la confianza en la inmutabilidad del resto de los datos.

8.5 Capacidades de seguridad de datos

– Se recomienda que los proveedores de servicio DLT y los creadores de sistemas DLT garanticen que para el diseño de los sistemas DLT se utilizan tecnologías criptográficas y de otro tipo que cumplen los requisitos de seguridad y rendimiento de los servicios DLT, incluidas la fiabilidad, la integridad y la inmutabilidad, en particular utilizando algoritmos criptográficos y mecanismos de consenso adecuados.
– Se recomienda que los proveedores de servicio DLT y los creadores de sistemas DLT garanticen la coherencia de los datos en la cadena.

8.6 Capacidades a nivel básico

– Se recomienda que los proveedores de servicio DLT y los creadores de sistemas DLT presten la adecuada atención a garantizar la integridad, la confidencialidad, la aplicabilidad, la disponibilidad y la utilización de las redes DLT.
– Se recomienda que los creadores de sistemas DLT hagan frente a las amenazas a la red utilizando un marco de seguridad adecuado.

– Los proveedores de servicio DLT y los creadores de sistemas DLT pueden utilizar métodos como la expansión de la potencia de cálculo o los recursos de participación para evitar ataques de consenso.
– Se recomienda que los proveedores de servicio DLT y los creadores de sistemas DLT soporten la seguridad de los contratos inteligentes que se ejecutan en los sistemas DLT recurriendo a la verificación formal o utilizando otros métodos de detección de vulnerabilidades.
– Los creadores de sistemas DLT pueden integrar la tolerancia a fallos en los sistemas DLT para contrarrestar los nodos malignos. Se recomienda que los sistemas DLT se recuperen en caso de que un conjunto de nodos normales funcione mal o se conviertan en nodos malignos.

Bibliografía

[b-UIT-T J.160] Recomendación UIT-T J.160 (2005), *Arquitectura para la distribución de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable*.

[b-UIT-T X.1400] Recomendación UIT-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ISO/CEI 27000] ISO/CEI 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-Camenisch] Camenisch J., Derler D., Kernn S., Pöhls H. C., Samelin K., y Slamanig D. (2017), *Chameleon-hashes with ephemeral trapdoors and Applications to Invisible Sanitizable Signatures*, Public-Key Cryptography, Berlín, Springer, pp. 152-182. https://doi.org/10.1007/978-3-662-54388-7_6.

[b-Nakamoto] Nakamoto S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf.

[b-DIN SPEC 4997] DIN SPEC 4997 (2020), *Privacy by blockchain design: A standardised model for processing personal data using blockchain technology*.

[b-DLT 4.1] UIT-T HSTP.DLT-RF (2019), *Distributed ledger technologies: Regulatory framework*.

[b-RGPD] Reglamento General de Protección de Datos de la Unión Europea, Artículo 17, *Derecho de supresión («el derecho al olvido»)*. https://gdpr.eu/article-17-right-to-be-forgotten/.

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, 2023