Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

F.747.10

(01/2022)

SERIE F: SERVICIOS DE TELECOMUNICACIÓN NO TELEFÓNICOS

Servicios multimedios

Requisitos de seguridad de los sistemas de libro mayor distribuido para los servicios personales

Recomendación UIT-T F.747.10

RECOMENDACIONES UIT-T DE LA SERIE F

SERVICIOS DE TELECOMUNICACIÓN NO TELEFÓNICOS

SERVICIO TELEGRÁFICO	
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	
Servicio móvil y servicios por satélite con destinos múltiples	F.110–F.159
SERVICIOS DE TELEMÁTICA	
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	
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 MULTIMEDIOS	**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.747.10

Requisitos de seguridad de los sistemas de libro mayor distribuido para los servicios personales

Resumen

La Recomendación UIT-T F.747.10 establece los requisitos generales y las capacidades funcionales de los sistemas de libro mayor distribuido (DLS) que permiten garantizar la seguridad de los servicios personales.

En esta Recomendación se describen los requisitos de seguridad del modelo de libro mayor distribuido para servicios personales que permiten conciliar los objetivos contradictorios de la protección de la privacidad y la utilización de macrodatos personales. En la Recomendación también se describen las capacidades funcionales de los nodos compartidos del libro mayor distribuido que posibilitan el aprendizaje automático sin descifrar los datos personales. Sin embargo, la carga computacional del aprendizaje automático para los datos cifrados puede ser excesiva. Para resolver este problema, el modelo de libro mayor distribuido para servicios personales que se presenta en este documento define los procedimientos que permiten el uso de dos o más pares de claves de cifrado y la notificación del tipo de clave. En la Recomendación se incluyen también requisitos para mantener la integridad, con objeto de garantizar la seguridad de los servicios personales y asegurar que los libros mayores distribuidos sean seguros y se verifiquen desde el principio del proceso, a efectos de la distribución de información personal. Por lo tanto, la puesta en marcha de un sistema de libro mayor distribuido para la distribución segura de información personal puede garantizar un seguimiento transparente del proceso de distribución hasta el trayecto de uso final.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T F.747.10	17-01-2022	16	11.1002/1000/14644

Palabras clave

Modelo de libro mayor distribuido para servicios, ampliación de la protección de la privacidad, seguridad de los servicios personales, control de la transparencia.

* 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 ha recibido notificación de la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores 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.747.10

Requisitos de seguridad de los sistemas de libro mayor distribuido para los servicios personales

1 Alcance

La presente Recomendación describe los requisitos de seguridad de los sistemas de libro mayor distribuido para los servicios personales y comprende:

– antecedentes;

– requisitos generales de seguridad de los sistemas de libro mayor distribuido para los servicios personales;

– capacidades funcionales de los sistemas de libro mayor distribuido para garantizar la seguridad de los servicios personales.

2 Referencias

Las siguientes Recomendaciones del UIT T y otras referencias contienen disposiciones que, mediante su referencia en el presente texto, constituyen disposiciones de la presente Recomendación. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones y demás referencias son objeto de revisión, por lo que se alienta a los usuarios de la presente Recomendación a utilizar 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 actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

La presente Recomendación utiliza los siguientes términos definidos en otros documentos:

3.1.1 bloque [b-ISO 22739]: Datos estructurados que comprenden los datos de bloque y una cabecera de bloque.

3.1.2 consenso [b-ISO 22739]: Acuerdo entre los nodos de la tecnología de libro mayor distribuido (DLT) de que 1) una transacción ha sido validada; y 2) que el libro mayor distribuido contiene un conjunto y un orden coherentes de transacciones validadas.

3.1.3 firma digital [b-ISO 22739]: Datos que, cuando se ingresan en un objeto digital, permiten al usuario del objeto digital autenticar su origen e integridad.

3.1.4 libro mayor distribuido [b-ISO 22739]: Libro mayor que se comparte entre un conjunto de nodos DLT y se sincroniza entre esos nodos mediante un mecanismo de consenso.

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

3.1.6 bifurcación [b-UIT-T TS FG DLT D1.1]: Creación de dos o más versiones diferentes de un libro mayor distribuido.

3.1.7 valores hash o resumen [b-ISO 22739]: Cadena de bits producida por una función de resumen (hash) criptográfica.

3.1.8 salud [b-WHO]: Un estado de bienestar físico, mental y social en el que no hay enfermedades ni dolencias.

3.1.9 libro mayor [b-ISO 22739]: Almacén de información que mantiene registros de transacciones destinadas a ser finales, definitivas e inmutables.

3.1.10 árbol de Merkle [b-NIST]: Estructura de datos en la que los datos son troceados y combinados hasta alcanzar un hash raíz único que representa toda la estructura de datos.

3.1.11 minería [b-UIT-T F.751.0]: Una actividad en la que se obtienen recompensas en determinados mecanismos de consenso.

3.1.12 nodo [b-ISO 22739]: Componente elemental a partir del cual se construye una estructura de datos.

3.1.13 sistema de libro mayor distribuido público [b-UIT-T F.751.0]: Sistema DLT que es accesible al público.

3.1.14 transacción [b-ISO 22739]: Unidad más pequeña de un proceso de trabajo, que consta de una o más secuencias de acciones necesarias para producir un resultado que cumple con las normas de aplicación.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 profundidad de bloque: Nivel de un bloque que se añade a la cadena del sistema de libro mayor distribuido desde su bloque inicial.

3.2.2 registros electrónicos personales: Recopilación sistematizada de información relativa a personas y poblaciones, que es almacenada electrónicamente en un formato digital.

3.2.3 de la persona/personal: Principios relativos a la creación de las condiciones óptimas de vida que atañen al bienestar, la seguridad y la salud de las personas, con inclusión del desarrollo de las tecnologías existentes y la adquisición de tecnologías nuevas.

NOTA – Adaptado de [b-ISO 6385] y [b-Wickens].

3.2.4 información de la persona/personal: Información recolectada mediante la medición directa del cuerpo humano y de su entorno y que se transmite a dispositivos personales u otros dispositivos a través de una red de comunicaciones para ser utilizada en los registros electrónicos personales.

3.2.5 dispositivo personal: Clase de dispositivo que mide el cuerpo humano y su entorno, y que intercambia la información recolectada con otros dispositivos personales.

3.2.6 aspectos personales y seguridad: Aspectos relativos a la persona en el contexto de la seguridad de la información.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las abreviaturas y los acrónimos siguientes:

CPU Unidad central de procesamiento (*central processing unit*)

DLS Sistemas de libro mayor distribuido (*distributed ledger systems*)

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

IP Protocolo de Internet (*Internet protocol*)

PDLS Sistema de libro mayor distribuido público (*public distributed ledger systems*)

UUID Identificador único universal (*universally unique identifier*)

VRF Función aleatoria verificable (*verifiable random function*)

5 Convenios

En esta Recomendación:

– La expresión "**se requiere**" indica 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 o proveedor 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 Recomendación.

6 Antecedentes

En los últimos años se ha constatado un aumento espectacular del volumen de información personal debido al desarrollo de dispositivos personales de recogida de datos sanitarios y al incremento de los datos personales en los historiales médicos de los hospitales. El modelo de libro mayor distribuido para servicios figura entre los mejores modelos actuales para la gestión e intercambio de datos personales. Las características de los sistemas de libro mayor distribuido ofrecen fiabilidad al utilizar una base de datos distribuida en la que intervienen múltiples nodos, y garantizan la transparencia de la recuperación de los datos mediante firmas digitales y valores hash. Sin embargo, los datos personales pueden ser muy sensibles desde la perspectiva de la protección de la información. Por consiguiente, el modelo de libro mayor distribuido público para servicios requiere el cumplimiento de requisitos de protección de la información personal (véase la Figura 1).

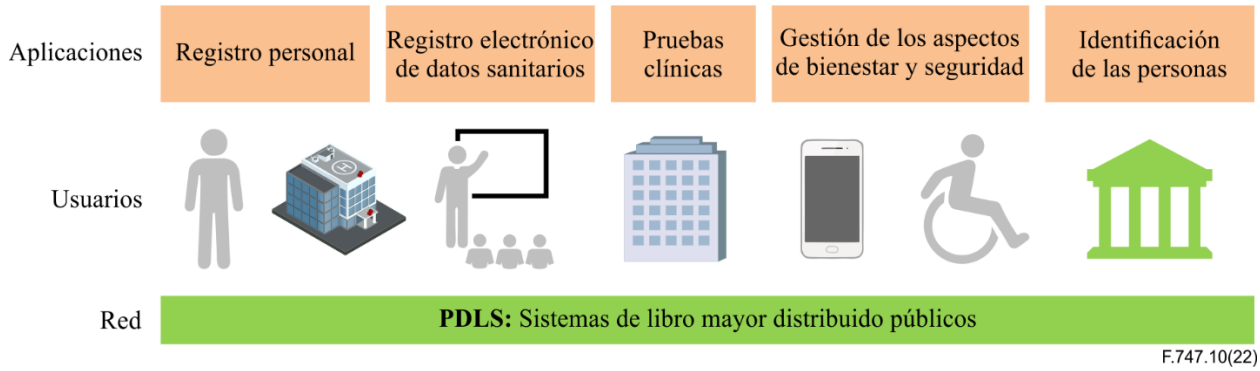

Figura 1 – Modelo de libro mayor distribuido para servicios personales

En esta Recomendación se describen los requisitos de seguridad del modelo de libro mayor distribuido para servicios personales que permite alcanzar los objetivos de protección de la privacidad y utilización de macrodatos de salud personal. En la Recomendación también se presentan los requisitos funcionales de los nodos compartidos del libro mayor distribuido que aseguran el aprendizaje automático sin descifrar los datos cifrados. Se describen asimismo los requisitos de incentivos del modelo de libro mayor distribuido para servicios que tienen por objeto mejorar la calidad de vida, mediante la automatización de la distribución de productos sanitarios directamente a los consumidores y los fabricantes. Para poner en marcha la tecnología de libro mayor distribuido es preciso, en primer lugar, tener la capacidad para asegurar el seguimiento y la gestión de la producción y distribución de información sanitaria. En otras palabras, la aplicación de la tecnología de libro mayor distribuido para la distribución de información personal permite garantizar un seguimiento transparente desde el proceso de distribución hasta el trayecto de uso final. Así, las personas

representadas por los nodos individuales que participan en el sistema de libro mayor distribuido pueden confiar en la información distribuida y utilizarla. Además, es posible utilizar un método para bloquear radicalmente la distribución ilegal de información personal.

7 Requisitos generales de seguridad de los sistemas de libro mayor distribuido para los servicios personales

En esta cláusula se describen los requisitos que permiten garantizar la seguridad de los procedimientos de gestión de los movimientos del libro mayor distribuido, y conciliar los objetivos contradictorios de protección de la información personal y la utilización de macrodatos personales. Presenta los requisitos funcionales de los nodos compartidos del libro mayor distribuido para asegurar el aprendizaje automático sin descifrar los datos cifrados. Por ejemplo, el cifrado homomórfico es una técnica criptográfica que permite realizar todos los cálculos efectuados por una computadora sin descifrar, incluso datos cifrados. Incluso cuando se trata de análisis de datos que incluyen información personal que debe protegerse, el aprendizaje automático puede realizarse opcionalmente sin que se filtre información personal o se pierdan datos.

7.1 Requisitos funcionales de los nodos compartidos del libro mayor distribuido público

Los requisitos funcionales para los nodos compartidos del libro mayor distribuido público son los siguientes:

– Los nodos deben almacenar los datos de la cadena del libro mayor distribuido acumulados desde el primer bloque.

– El estado de finalización debe notificarse a los demás nodos, ya que un nodo ejecuta el algoritmo de confirmación distribuido en el momento en que se verifica la transacción.

– Para verificar la validez del libro mayor distribuido generado en cada ronda, el nodo debe comprobar la validez del bloque generado, comparándolo con el valor hash establecido.

– Cada nodo debe actualizar y mantener los datos compartidos, como la lista de claves públicas de todos los demás nodos y el libro mayor distribuido.

– El nodo debe propagar la transacción a los demás nodos hasta alcanzar la fase de acuerdo (por ejemplo, la finalización de la confirmación de la transacción) en el proceso de verificación de la transacción.

– El nodo debe cifrar los datos de las transacciones que deban ser seguras mediante la utilización de claves criptográficas (por ejemplo, el certificado de clave pública [b-UIT-T X.509], el cifrado homomórfico [b-ISO 18033-6], la función aleatoria verificable (VRF) [b-IETF draft-irtf-cfrg-vrf-08] y notificar el tipo de clave de cifrado utilizado.

– El nodo debe determinar si es necesario descifrar datos. En caso afirmativo, descifra los datos y los transmite al nodo solicitante. Si no es necesario descifrar datos, el nodo los cifra con la clave pública del nodo solicitante y los transmite.

7.2 Requisitos de autenticación para los nuevos nodos participantes

Se recomienda que los nodos existentes cumplan las funciones descritas en las cláusulas 7.2.1 a 7.2.3, para autenticar a los nuevos nodos participantes en un sistema compartido de libro mayor distribuido.

7.2.1 Requisitos para solicitar la autenticación de un nuevo nodo

– Se recomienda que el nuevo nodo disponga de al menos dos pares de claves de cifrado (por ejemplo, un certificado de clave pública [b-UIT-T X.509] o claves de cifrado homogéneas [b-ISO 18033-6]), antes de hacer una solicitud.

– Se recomienda que el nuevo nodo cifre el mensaje de solicitud con su propia clave privada y envíe los datos cifrados y su clave pública junto con el nodo.

– Se recomienda que cada nodo actualice la lista de claves públicas verificadas de los nodos nuevos y existentes y que almacene la lista de claves públicas del sistema compartido de libro mayor distribuido para poder participar, una vez que el nodo verifique y transmita la información autenticada.

7.2.2 Requisitos funcionales para la autenticación del nodo

– Se recomienda que el nodo verifique la validez, mediante el descifrado de los datos encriptados transmitidos por el nuevo nodo que se desea participar recibidos junto con la clave pública, encripte la información verificada y la lista de claves públicas con la clave pública del nuevo nodo, y transmita la información cifrada.

– Se recomienda que el nodo consista en una lista de claves públicas de todos los nodos que participan en el sistema compartido de libro mayor distribuido y actualice su lista de claves públicas correspondiente cada vez que tenga que autenticar un nuevo nodo.

– Se recomienda que cada vez que el nodo tenga que actualizar su lista de claves públicas, cifre la lista de claves públicas con su propia clave privada y la envíe a todos los nodos participantes en el sistema compartido de libro mayor distribuido.

– Se recomienda que el nodo almacene permanentemente la información verificada sobre los nodos que participan en el sistema compartido de libro mayor distribuido junto con la hora de verificación y la dirección del nodo participante.

7.2.3 Requisitos para la verificación de la autentificación de los nuevos nodos en los nodos existentes

– Se recomienda que los nodos existentes verifiquen la firma digital de la lista de claves públicas enviada por el nodo y la actualicen con la nueva lista de claves públicas.

– Se recomienda que los nodos existentes verifiquen la participación del nuevo nodo autenticado comprobando la nueva lista de claves públicas.

7.3 Requisitos de seguridad del sistema de libro mayor distribuido

Se recomienda que los nodos existentes cumplan las disposiciones de la presente cláusula.

– Los intentos de manipulación de la información en un libro mayor distribuido compartido existente deben ser verificados mediante la utilización de una firma electrónica y deben rechazarse en el libro mayor distribuido.

– De las principales cadenas que se utilizan en el sistema de libro mayor distribuido, deben rechazarse en el libro mayor distribuido las cadenas con contenidos diferentes de la cadena más larga antes de un bloque de profundidad b arbitraria en el momento en que se crea un nuevo bloque. En este caso b es un número superior a 1.

– Los datos deben ser rechazados durante el proceso de creación del libro mayor distribuido, cuando los datos con direcciones duplicadas (por ejemplo, IP, UUID) se añaden al sistema del libro mayor distribuido.

– Es necesario asegurar que la fuente aleatoria común (por ejemplo, el nonce criptográfico [b-NIST]) sea la misma para bloques de cualquier profundidad d. Los bloques que rebasan la profundidad d deben actualizar la fuente aleatoria común mediante una profundidad g. Se recomienda utilizar, una vez que haya sido actualizado, el hash del bloque recién añadido como fuente aleatoria.

  NOTA – En este caso la profundidad de bloque d y g se refiere a todos los bloques con una profundidad superior a 1.

– En el libro mayor distribuido se deben rechazar las cadenas que contengan bloques con valores hash diferentes de los bloques anteriores y diferentes valores raíz del árbol de Merkle.

– Si se produce un nodo de error entre los nodos constitutivos del sistema de libro mayor distribuido, se recomienda mantener los nodos sin errores si están por encima del nivel de consenso predefinido para el DLS.

7.4 Requisitos para mantener la integridad de los sistemas de libro mayor distribuido

Se recomienda que los nodos existentes cumplan las disposiciones de la presente cláusula.

– Se recomienda que cada nodo elimine todo intento de manipulación de la información en el libro mayor distribuido compartido existente. Si se detecta un ataque de este tipo, se recomienda agrupar el número de nodos con el fin de obtener la tasa de hash. Se recomienda comparar el número actual de árboles de bloques con el valor umbral para calcular la seguridad y transmitir (difundir) la información correspondiente y las direcciones de los nodos a todos los nodos.

– Se recomienda que cada nodo descarte del sistema de libro mayor distribuido las cadenas más largas que se suelen utilizar en el sistema de libro mayor distribuido y las cadenas con contenidos diferentes.

– Se recomienda que cada nodo descarte la cadena que contenga bloques con valores hash o valores raíz del árbol de Merkle diferentes de los bloques anteriores en el libro mayor distribuido y que calcule el número de nodos que fueron objeto de ataques, con objeto de determinar si el libro mayor distribuido es seguro, y que transmita (difunda) la información pertinente y la dirección del nodo.

– Cuando se detecta la presencia de un nodo erróneo o falsificado entre los componentes del sistema de libro mayor distribuido, se recomienda que cada nodo descarte y agrupe los nodos que han intentado producir un error o iniciar un ataque con el fin de obtener la tasa de potencia de hash. Se recomienda que el número de nodos seguros se mantenga por encima del valor umbral en el libro mayor distribuido y que se transmita (difunda) la información correspondiente y las direcciones de los nodos.

– Se recomienda que cada nodo rechace los datos durante el proceso de creación del libro mayor distribuido cuando los nuevos datos se añadan con direcciones duplicadas a los datos del sistema de libro mayor distribuido.

8 Capacidades funcionales de los sistemas de libro mayor distribuido para garantizar la seguridad de los servicios personales

Como incentivo, se requiere mejorar la calidad de vida en un modelo de libro mayor distribuido para servicios mediante la automatización de la distribución directa de la información personal. Para poner en marcha la tecnología de libro mayor distribuido es preciso, en primer lugar, tener la capacidad para asegurar el seguimiento y la gestión de la producción y distribución de información personal. En otras palabras, la aplicación de la tecnología de libro mayor distribuido para la distribución de información personal permite garantizar un seguimiento transparente desde el proceso de distribución hasta el trayecto de uso final. Así, las personas representadas por los nodos individuales que participan en el sistema de libro mayor distribuido pueden confiar en la información distribuida y utilizarla. Además, es posible utilizar un método para bloquear radicalmente la distribución ilegal de información personal.

8.1 Estructura del libro mayor distribuido para la distribución de información personal

Por lo general, la primera transacción del libro mayor es una transacción especial que da lugar a un nuevo incentivo (por ejemplo, monedas virtuales [b-UIT-T F.751.0]) que se otorga al creador del libro mayor. Este incentivo recompensa a los nodos por mantener un libro mayor distribuido y se proporciona desde el principio para la distribución de información personal. Se recomienda acordar de antemano las técnicas para proporcionar y distribuir estos incentivos, ya que funcionan como sistemas distribuidos. Se suele añadir constantemente un cierto número de nuevos incentivos con

objeto de compensar a los nodos (mineros) por los recursos que consumen para hacer funcionar el sistema de libro mayor distribuido. Los nodos consumen potencia de cálculo de la unidad central de procesamiento (CPU), memoria y monedas.

8.2 Las dos funciones de la estructura del libro mayor distribuido para la distribución de información personal

Para reducir el tiempo de espera y aumentar la velocidad de extracción se puede utilizar una técnica para dividir la estructura del libro mayor distribuido básico en tres funciones. Este proceso consiste en seleccionar la cadena principal en el protocolo del libro mayor distribuido (por ejemplo, la técnica de selección de la cadena más larga), lo que conduce a elegir el libro mayor seguro entre todos los libros mayores en cada profundidad del árbol de libro mayor. Por profundidad del libro mayor se entiende la distancia a partir del libro mayor de origen (el número de bloques conectados en el libro mayor).

En un libro mayor distribuido, el libro mayor cumple tres funciones. Primero, sirve para elegir al capitán, añadir transacciones a la cadena principal y votar por el libro mayor antecesor a través de las relaciones padre-hijos. En términos conceptuales, el libro mayor se divide en dos funciones (véase la Figura 2). La función de propuesta agrupa las transacciones de la misma profundidad en el árbol del libro mayor original. La función de votación selecciona la parte correspondiente del libro mayor votando por la misma profundidad de las transacciones en el árbol del libro mayor. El libro mayor seleccionado toma los libros mayores parciales de las transacciones y forma el libro mayor final. Esta función de votación funciona en la misma profundidad que la del árbol del libro mayor y crea una conexión padre-hijo. Por consiguiente, la conexión padre-hijo del árbol de libro mayor original tiene dos funciones que están explícitamente separadas: 1) Determinar un cierto orden de los libros mayores en la parte de las transacciones a la misma profundidad; y 2) la función de votación, que permite votar unos por otros con el fin de evaluar el libro mayor. La estructura general del libro mayor distribuido para la distribución de la información personal que se describe a continuación se expone en la Figura 2.

Debido a su naturaleza distribuida, los sistemas de libro mayor distribuido (DLS) se enfrentan a problemas de estabilidad. En un sistema de libro mayor distribuido, cada nodo puede registrar una transacción, pero al final, el nodo seleccionado es el resultado del algoritmo de consenso [b-UIT-T F.751.0]. Cabe tener presente que el diseño de un DLS es uno de los muchos factores que afectan a la estabilidad, por lo que se recomienda asegurar que el libro mayor distribuido restablezca la estabilidad del servicio mediante el procesamiento adaptativo del sistema. Para resolver el problema de estabilidad del DLS, la fuente aleatoria común (por ejemplo, el nonce criptográfico [b-NIST]) se mantiene igual en bloques de profundidad d, y los bloques superiores a la profundidad d deben actualizar la fuente aleatoria común mediante bloques de profundidad g. Una vez que se actualiza, el hash del bloque recién añadido se utiliza como fuente aleatoria. Si $d = 1$, se vuelve a aplicar la regla de actualización básica que divide (bifurca) cada época (periodo de bloque), que es más vulnerable a los ataques de contaminación (estabilidad). Para aumentar normalmente el umbral de seguridad, se puede aumentar el valor de d. Cuando $d = \infty$, todos los bloques utilizan el nonce del bloque de origen como fuente aleatoria común. Este es el protocolo de la cadena más larga, que no admite la bifurcación y que permite al propietario de la clave secreta contaminado hacer predicciones privadas de la cadena.

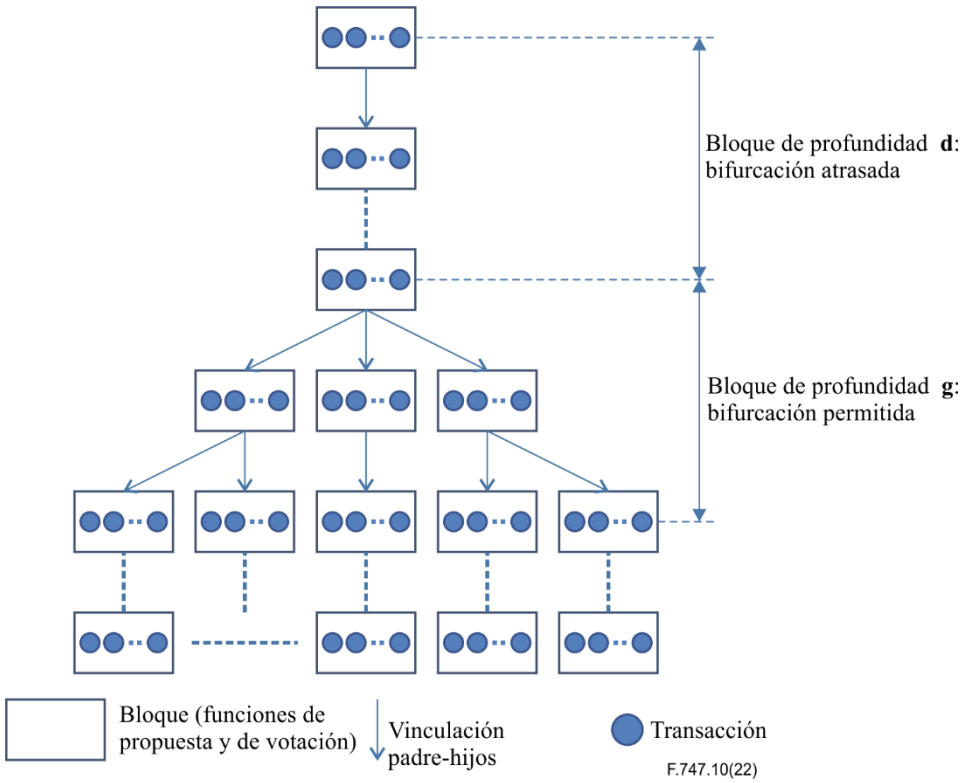

Figura 2 – Estructura del modelo de libro mayor distribuido para servicios

8.3 Metodologías para el mantenimiento de los sistemas de libro mayor distribuido

Esta representación de la separación funcional de un libro mayor distribuido, que es mucho más compleja que la de un libro mayor distribuido tradicional, puede mejorar el rendimiento del libro mayor distribuido, posibilitando un consenso más rápido. Esta función que posibilita el consenso rápido puede aumentar el número de libros mayores en la parte transacciones sin comprometer la seguridad del libro mayor distribuido en la función de propuesta. En consecuencia, el número de libros mayores se verá limitado únicamente por la capacidad de la red de comunicación subyacente. El consenso también puede confirmarse con baja latencia y alta fiabilidad, ya que la función de votación de transacciones múltiples se realizará en paralelo al libro mayor de la propuesta de confirmación rápida. El sistema de libro mayor distribuido de información personal resulta fácil de gestionar porque la tasa de generación de libros mayores generales ha aumentado considerablemente y que el número de libros mayores parciales de la función de propuesta por profundidad puede ser reducido.

Este sistema de libro mayor distribuido puede comprometer la transparencia al concentrar la potencia de hashing en la función de propuesta de una transacción específica en el proceso de selección del libro mayor. Como se muestra en la Figura 3, si la potencia de hashing de un atacante es fuerte en un libro mayor específico de la función de propuesta, puede ser muy vulnerable a la seguridad. En la Figura 3 se muestra un ejemplo de una cadena de libros mayores destruida o contaminada por la concentración de la potencia de hashing de un atacante. Si un atacante fuera capaz de reunir más potencia de cálculo de la CPU, memoria y monedas en un solo lugar respecto de todos los nodos seguros, tendría que decidir si conviene utilizarlas para robar los incentivos de los nodos honestos o bien para cooperar. Convendría contar con una política de incentivos que persuadiera a los atacantes de que es más beneficioso seguir las reglas que socavar la transparencia del sistema de libro mayor distribuido de información personal. Ese incentivo debe ajustarse para poderse distribuir entre los nodos participantes. El atacante puede prever una regla de ese tipo, que haga que resulte más rentable asociarse con todos los demás nodos. Se recomienda que en esa regla se mantenga el número de nodos honestos por encima del valor umbral (por ejemplo, CD $(1 + \alpha)/(\alpha\text{-}1)/\log(\alpha)$) según la tasa de hash del atacante (α). En este caso, C y D son la capacidad y el retardo de las redes de comunicación.

Lo que se desprende de esta fórmula es que, si el valor de α es cercano a 0, la potencia de hashing del atacante es débil, por lo que se puede afirmar que no hay ningún problema de seguridad en los sistemas de libro mayor distribuido, incluso si el número de árboles de bloques votantes es reducido. En cambio, si el valor de α se acerca a 1, es decir, si la potencia de hashing del atacante es fuerte, será preciso aumentar exponencialmente el número de árboles de bloques votantes. Si ha alcanzado ese punto, se puede considerar muy vulnerable a la seguridad.

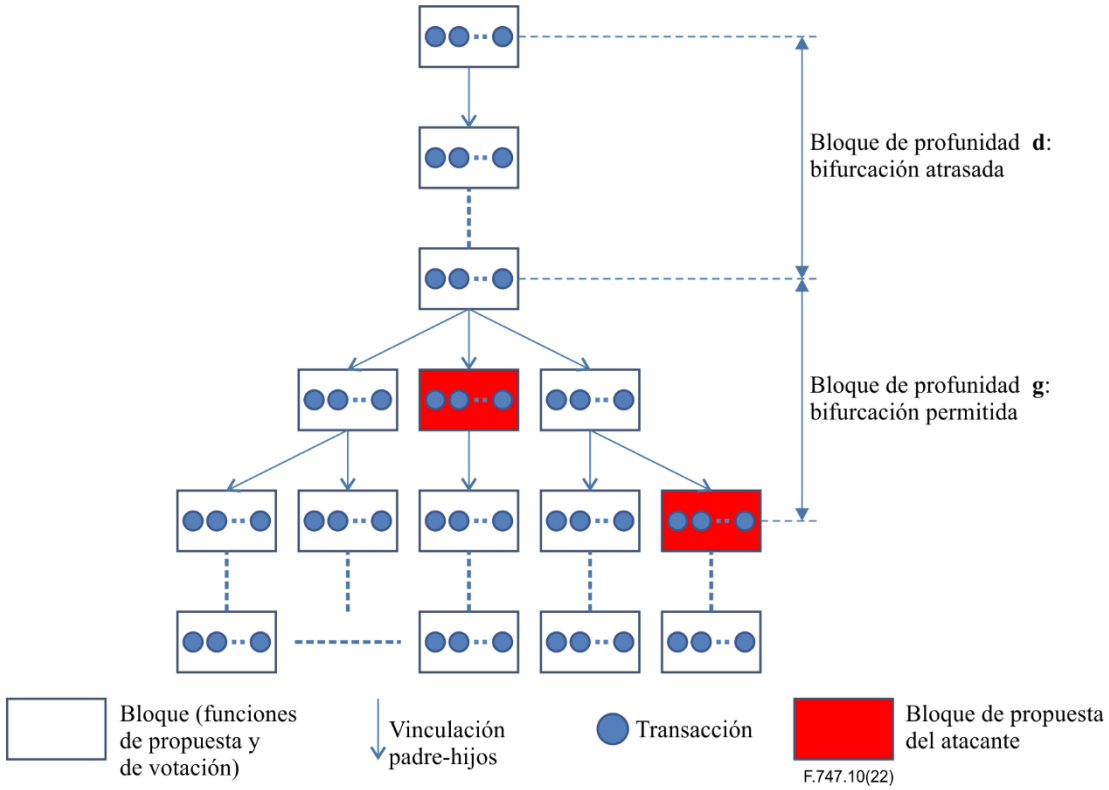

Figura 3 – Ejemplo de prevención de la contaminación del modelo de libro mayor distribuido para servicios

Al seleccionar el bloque de propuesta, se recomienda determinar la función del bloque, ajustando la potencia de hashing y las monedas. En ese momento se podrá constatar que, si la potencia de hashing y de las monedas del atacante es fuerte, el nivel de vulnerabilidad es muy elevado. Si un atacante logra reunir más potencia computacional y monedas que todos los nodos honestos, se le planteará la opción de utilizarlo para sustraer los beneficios de un nodo honesto, o para cooperar. Se recomienda prever la adopción de políticas de incentivos en virtud de las cuales resultaría más beneficioso para los atacantes cumplir las normas que socavar el sistema y la legitimidad de su propia riqueza. Se recomienda la adopción de una política que impida que los beneficios se puedan concentrar en un bloque de propuesta específico y que asegure también que los atacantes se beneficien más de la colaboración con todos los demás nodos.

Anexo A

Aplicación de los aspectos de seguridad del modelo de libro mayor distribuido para servicios personales

(Este anexo forma parte integrante de la presente Recomendación)

En el ejemplo de libro mayor distribuido que se muestra en la Figura A.1 se observa que es posible gestionar de forma segura y transparente no solo los datos personales asociados a los hospitales, sino también los datos centrados en la persona, como los dispositivos de recogida de datos sanitarios personales. En el ejemplo de intercambio de información sanitaria personal de la Figura A.1 se ilustra la manera en que se puede asegurar la fiabilidad de un libro mayor distribuido en el que participan múltiples nodos mediante la utilización de firmas digitales y valores hash que confieren transparencia a los datos de búsqueda. Sin embargo, los datos personales pueden ser muy sensibles desde una perspectiva de protección de datos. Por lo tanto, esos datos sensibles se registran en estado cifrado mediante el empleo de una técnica de cifrado capaz de procesar macrodatos. Por lo que se refiere al proceso de transmisión de información personal sensible, deberán cumplirse los requisitos y procedimientos del sistema de libro mayor distribuido compartido definidos en la cláusula 7.2, utilizando un algoritmo de cifrado (véase la Figura A.1). Por otra parte, se deberá asegurar que el funcionamiento del sistema de libro mayor distribuido para la información personal satisface los requisitos de la función de incentivo a la que se refiere la cláusula 8.3, en cuanto a su activación y mantenimiento.

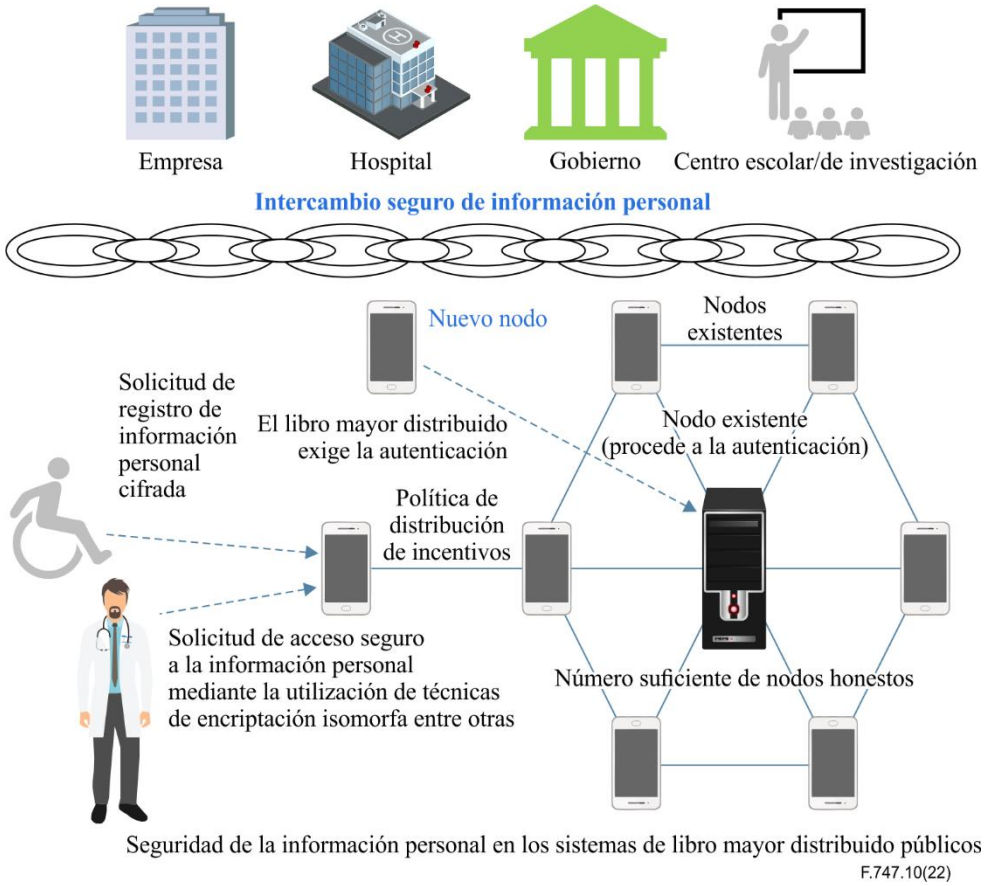

Figura A.1 – Ejemplos de modelos seguros de libro mayor distribuido para servicios

Bibliografía

[b-UIT-T F.751.0] Recomendación UIT-T F.751.0 (2020), *Requisitos para los sistemas de libro mayor distribuido.*

[b-UIT-T X.509] Recomendación UIT-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-UIT-T TS FG DLT D1.1] Technical Specification ITU-T FG DLT D1.1 (2019), *Distributed ledger technology terms and definitions.*

[b-IETF draft-irtf-cfrg-vrf-08] IETF draft-irtf-cfrg-vrf-08 (2020), *Verifiable Random Functions (VRFs).* https://tools.ietf.org/html/draft-irtf-cfrg-vrf-08

[b-ISO 6385] ISO 6385:2016, *Ergonomics principles in the design of work systems*.

[b-ISO 18033-6] ISO 18033-6:2019, *IT Security techniques –Encryption algorithms– Part 6: Homomorphic encryption*.

[b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies – Vocabulary*.

[b-NIST] NISTIR 8202 (2018). *Blockchain Technology Overview.*

[b-WHO] World Health Organization (2006), *Constitution of the World Health Organization – Basic Documents, Forty-fifth edition, Supplement*.

[b-Wickens] Wickens, D., Gordon, S., Liu, Y. (1997), *An Introduction to Human Factors Engineering*. pp.2-7. New York, NY: Longman.

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