

IGNACIO ALAMILLO DOMINGO

Los libros mayores electrónicos distribuidos, blockchain y la gestión de documentos de archivo

Distributed electronic ledgers, blockchain, and records management

Ignacio Alamillo Domingo
nacho@astrea.cat
Grupo de investigación iDerTec, Universidad de Murcia

*Citación: Alamillo Domingo, Ignacio (2021). "Los libros mayores electrónicos distribuidos, blockchain y la gestión de documentos de archivo". *Tábula*, n. 24, pp. 21-43*

Recibido: 2-3-2020. Aceptado: 5-10-2020
DOI: <https://doi.org/xxx>

Resumen analítico / Analytic summary

Las tecnologías de libro mayor distribuido y, en especial, las cadenas de bloques ofrecen oportunidades muy relevantes para la transformación de los procesos digitales, al sustentar tratamientos de datos y documentos que hasta la aparición de estas tecnologías requerían de bases de datos de terceros. En este trabajo abordamos los rasgos fundamentales de estas tecnologías y su aplicación como soporte para la gestión de documentos, e introducimos la novedosa regulación propuesta en relación con las mismas en el derecho de la Unión Europea.

LIBRO MAYOR DISTRIBUIDO | CADENA DE BLOQUES | eIDAS

Distributed ledger technologies and, especially, blockchains offer very relevant opportunities for the transformation of digital processes, by supporting data and document processing that until the appearance of these technologies required third-party databases. In this work we address the fundamental features of these technologies and their application as a support for records management, and we introduce the new regulation proposed in relation to them in the law of the European Union.

DISTRIBUTED LEDGER | BLOCKCHAIN | eIDAS

Una breve introducción a las tecnologías de libro mayor distribuido

Las tecnologías de libro mayor distribuido (*distributed ledger technologies* o DLT, en inglés) y, en particular, la tecnología de cadenas de bloques (*blockchain*, en inglés), permiten la creación de una suerte de libro mayor inalterable y gestionado de forma absolutamente descentralizada (*distributed ledger*, en inglés), que posibilita nuevas aplicaciones, con un potencial transformador muy importante en todos los órdenes, que afecta necesariamente a la gestión de documentos.

Como se explica en el borrador de norma ISO 23257:2021, en fase final de desarrollo en el TC 307 de ISO, un libro mayor electrónico (ésta es la traducción más precisa del término inglés “ledger”, adoptada en la propuesta de Reglamento europeo a que luego me referiré, aunque parece haberse adoptado más el término “registro”) es un almacén de información que mantiene registros finales y definitivos de transacciones. Si bien el concepto de libro mayor fue definido originalmente en la práctica contable y financiera, se puede emplear para el registro de cualesquiera tipos de transacciones, como los movimientos y transferencias de bienes muebles.

Una propiedad muy deseable de un libro mayor es la resistencia a la manipulación; es decir, que los registros de transacciones, una vez ingresados en el libro mayor, sean extraordinariamente difíciles de alterar por diseño y no puedan modificarse sin que la alteración sea claramente evidente, sea ésta deliberada o accidental, maliciosa o benigna. Aunque normalmente se parte de que la información incluida en la *blockchain* es inalterable, en realidad existen mecanismos que permiten su modificación controlada, mediante técnicas como el empleo de

hashes camaleónicos, por ejemplo, a emplear cuando deba legalmente procederse a la eliminación de informaciones, por lo que debemos referirnos a una inmutabilidad relativa.

Un libro mayor distribuido tiene sus entradas almacenadas en una serie de nodos en una red, en lugar de en una sola ubicación. De esta forma, los diferentes nodos de la red pueden ser propiedad de diversas entidades que interactúan entre ellas, disponiendo de una copia del libro mayor.

Las tecnologías de libro mayor distribuido (DLT) permiten el funcionamiento y uso de libros mayores distribuidos. Un libro mayor distribuido se define en la ISO 22739:2020 como un libro mayor que se comparte entre un conjunto de nodos DLT y se sincroniza entre los nodos DLT mediante un mecanismo de consenso.

Desde un punto de vista abstracto, la tecnología de libro mayor distribuido permite la actualización de todos los nodos de una red, en un entorno de computación distribuida, del estado actual del mundo, por lo que permite conferir un estado compartido de confianza a un sistema distribuido; es decir, que cuando se registra una actuación empleando estas tecnologías, lo que realmente sucede es que ese registro es realizado en una gran cantidad de lugares diferentes, en lugar de un único lugar centralizado, por lo que podemos considerar que dicho registro es auténtico.

ISO 23257 también explica que los sistemas DLT están diseñados para implementar libros mayores distribuidos, un desafío importante debido a la necesidad de acordar y mantener los registros de transacciones en el libro mayor distribuido. En un sistema DLT, el consenso asegura que cada versión replicada de una transacción sea la misma en todos los nodos donde se almacena, y que su contenido sea generalmente acordado entre las partes involucradas en la transacción. Asimismo, el conjunto de registros en el libro mayor distribuido debe ser verificable y auditable, siendo uno de los principales objetivos de DLT el proporcionar registros de transacciones en línea no repudiables entre las partes.

Por lo que se refiere al nodo DLT a que nos hemos referido ya, el mismo se define en ISO 22739:2020 como un dispositivo o proceso que participa en una red y almacena una réplica completa o parcial de los registros del libro mayor, y un registro del libro mayor se define como un registro que contiene registros de transacciones, valores resumen de transacciones, de registros o de referencias a registros de transacciones registrados en un libro mayor distribuido.

Nuevamente, de acuerdo con ISO 23257, los sistemas *blockchain* son un subconjunto de tecnologías de libro mayor distribuido en el que el estado de un libro mayor distribuido se mantiene procesando lotes de transacciones en estructuras de datos seguras criptográficamente conocidas como bloques.

En la ilustración 1 se muestra la estructura de un bloque de Ethereum, para cuyo análisis detallado remitimos a:

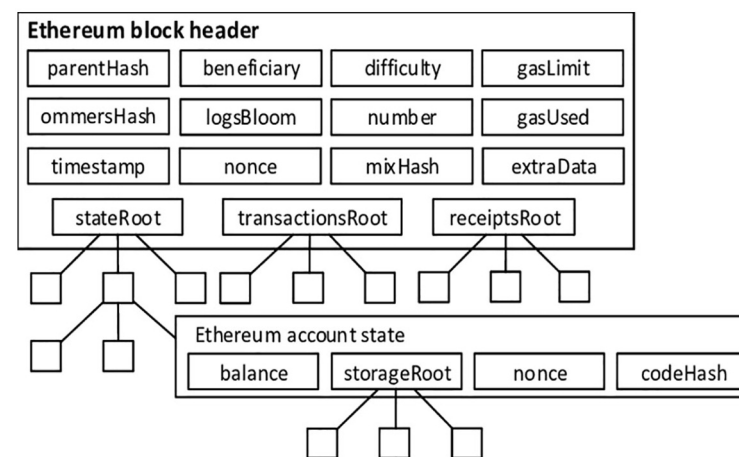


Figura 1. Estructura de bloque de Ethereum

Un protocolo válido debe garantizar que cada bloque esté vinculado criptográficamente a un bloque inmediatamente anterior que forme una secuencia única de bloques en el tiempo. La secuencia completa de bloques asociados criptográficamente forma una estructura de datos de solo anexo accesible globalmente, la cadena de bloques, que proporciona la versión canónica del historial de transacciones global.

Para garantizar que el proceso de actualización del libro mayor dé como resultado un solo estado del libro mayor para un bloque determinado, los protocolos de *blockchain* incluyen un mecanismo de consenso que proporciona un orden total de todas las transacciones dentro del bloque. La acción colectiva de todos los nodos en el sistema *blockchain* funciona como un servidor de marca de tiempo que valida las transacciones pendientes y actualiza el estado actual del libro mayor agregando bloques secuencialmente al *blockchain*.

Para implementar un libro mayor distribuido, por tanto, los sistemas de cadena de bloques requieren un mecanismo para distribuir nuevos bloques a todos los nodos, un mecanismo para validar transacciones y un mecanismo para garantizar la coherencia de todas las copias de la cadena de bloques. Existe una rica variedad de mecanismos de consenso, incluyendo prueba de trabajo, empleado en redes abiertas, como Bitcoin y Ethereum, o prueba de autoridad, empleado en redes permissionadas, públicas o privadas, como Alastria o la European Blockchain Services Infrastructure (EBSI), a la que posteriormente nos referiremos.

Finalmente, es importante recordar que el término *blockchain* se aplica comúnmente tanto a la estructura de datos como a la implementación completa de

un libro mayor distribuido que utiliza la estructura de datos *blockchain*. Desde este punto de vista, resulta indudable el interés que presenta el libro mayor, en tanto objeto documental.

El libro mayor distribuido en la gestión de documentos de archivo

Nos encontramos, por lo tanto, ante un sistema en el que podemos escribir cualquier información que queramos, remitiendo una transacción, bien sea actuando como nodo de la red o a través de un nodo de esta; desde ese momento, dicha transacción, y la información que contiene, se va a copiar a todos los restantes nodos de la red, por lo que ninguno de ellos va a poder eliminar dicha información de forma unilateral. Solo con el concurso de un gran número de nodos se podría eliminar una inserción en la red en cuestión, por lo que no resulta preciso confiar en ninguno de ellos en particular, y que se considere que una inserción de información, o el resultado de la ejecución de una transacción, que se ha propagado dentro de la red, sea considerada “verdadera”.

Esto no significa, por supuesto, que la información en sí sea verdadera, sino que es verdad que se registró esa información, y no otra información diferente, o que se realizó ese movimiento entre cuentas, y no otro diferente. Del mismo modo sucede cuando se emplea la firma electrónica avanzada basada en certificado electrónico para autenticar un documento privado: el contenido del documento resulta atribuible al firmante, con independencia de que dicho contenido sea verídico o no. Por ejemplo, cuando se realiza y se firma una declaración falsa, el documento es auténtico porque es imputable al firmante, pero su contenido es falso. Lo mismo sucede, en el fondo, con las tecnologías de registro distribuido.

Lo que verdaderamente diferencia ambos casos tiene que ver con una de las más singulares particularidades del documento electrónico, y consiste en la posibilidad de realizar infinitas copias idénticas del mismo, todas ellas con la condición de original, de forma simultánea.

En efecto, imaginemos que redactamos un contrato en un fichero PDF, y lo firmamos electrónicamente. En papel sería original el ejemplar físico en el que se contiene la firma, y dada la imposibilidad de duplicarlo, necesitaremos al menos dos ejemplares, cada uno de ellos firmados por ambas partes, para formalizar el contrato (que, por este motivo, se firma “por duplicado ejemplar”), teniendo cada uno de ellos esta condición de forma exclusiva. Por el contrario, en el citado soporte electrónico y formato PDF, solo es preciso firmar un ejemplar, que puede ser reproducido infinitas veces, mediante el simple copiado del correspondiente fichero informático, como por ejemplo cuando se almacena en un disco duro o removible, cuando se remite por correo electrónico o se carga en un servicio de

almacenamiento de ficheros en la Nube (motivo por el que, además, debería abandonarse la hoy ritual mención al “duplicado ejemplar” en beneficio del “ejemplar único electrónico”).

El ejemplo que se acaba de poner muestra una de las ventajas de firmar electrónicamente un documento, pero también da buena cuenta de una de sus limitaciones, que puede intuirse rápidamente. Y es que no es un mecanismo útil para aquellos casos en que la transferencia de un valor se produce mediante la entrega de un documento.

En efecto, las tecnologías de libro mayor distribuido permiten, por primera vez en la historia, aplicaciones como la realización de endosos –incluso en blanco–, facilitando por tanto la implementación de títulos-valores electrónicos de todo tipo, o la implantación eficiente e inalterable de registros jurídicos y administrativos inalterables, en especial en aquéllos que recogen transferencias de activos o asignaciones de atribuciones, que se realiza mediante la correspondiente firma electrónica de persona física o sello electrónico de persona jurídica de la transacción que se remite al sistema *DLT/Blockchain*.

A este respecto, han realizado un análisis de las propiedades del sello electrónico previsto en el Reglamento (UE) N° 910/2014, de 23 de julio (“Reglamento eIDAS”), con y sin uso de tecnologías de *blockchain*, concluyendo en su equivalencia, por lo que la elección de una u otra técnica depende solo del caso de uso. Siendo esto cierto desde una perspectiva técnica, no es menos cierto el que Reglamento eIDAS limita el reconocimiento transfronterizo de los sistemas de firma/sello a determinados formatos técnicos, que en la actualidad no soportan *DLT/Blockchain*, por lo que se han realizado diversas propuestas para poder realizar firmas/sellos en *DLT/Blockchain* con base en certificados cualificados empleando las tecnologías actuales, basadas en el estándar ITU-T Rec. X.509.

Hasta la aparición de estas tecnologías, el enfoque para la informatización (hoy hablaríamos, seguramente, de la digitalización) de los títulos-valores de todo tipo consistía en la sustitución del uso del título correspondiente por su “anotación en cuenta”; es decir, por la anotación en un registro centralizado de las titularidades y sus modificaciones ulteriores. De este modo ha sucedido en los mercados secundarios, en las transferencias dinerarias y otras operaciones de pago, o en los títulos de transporte.

Sin embargo, con las tecnologías de libro mayor distribuido ahora disponemos de la capacidad de realizar electrónicamente transferencias de títulos, mediante su endoso electrónico, eliminándose la necesidad de esos registros centralizados. En este ámbito resulta absolutamente ineludible referirse a la posibilidad de implementar, mediante las tecnologías de registro distribuido, sistemas de trazabilidad de todo tipo de objetos, tanto del mundo electrónico, como del mundo físico, mediante la técnica de la “tokenización”, en especial cuando los *tokens* representan activos.

Pero no es solo en este dominio en el que se han propuesto aplicaciones de las tecnologías de registro distribuido, puesto que esta tecnología permitiría la implantación de garantías de autenticidad en las bases de datos, actualmente centralizadas, impidiendo la modificación indetectable de los registros que contienen las mismas, algo importante tanto en el sector privado como en el público, dadas las exigencias legales respecto a la integridad de las bases de datos, especialmente en la normativa contable y tributaria.

La tecnología de libro mayor electrónico resulta particularmente apropiada para la gestión de la identidad digital y la gestión de registros y de documentos, presentando un potencial significativo para la transformación de la gestión documental segura en el sector público, en especial en lo relativo a las firmas digitales, los certificados y la autenticación de documentos, consideración que resulta aplicable también a otros sectores. Sin embargo, no se puede olvidar que esta tecnología presenta limitaciones inherentes, tanto tecnológicas como socio-económicas, especialmente en función del mecanismo de consenso utilizado y del modelo de gobernanza de la red, que deben ser objeto de consideración antes de adoptar su uso generalizado.

Uno de los casos de uso de *DLT/Blockchain* en apoyo de la gestión de documentos que mayor atención viene recibiendo es la expedición y gestión posterior de los certificados académicos.

Como tempranamente se propuso en la experiencia Blockcerts, resulta posible emplear una *blockchain* como *bitcoin* (hoy posiblemente se emplearía una red diferente, debido a los elevados costes transaccionales de dicha red) a los efectos de acreditar la existencia de un certificado académico, sin excesiva dependencia de terceros. En este sistema se crea un resumen criptográfico de cada certificado académico; se añade a un fichero índice en el que constan todos los resúmenes criptográficos de todos los certificados expedidos; se crea el resumen criptográfico del índice y el mismo se registra en la red *bitcoin* mediante una transacción; y para la verificación de la autenticidad del documento (el certificado académico) basta con acceder al fichero índice, publicado en la web de la Universidad, y comprobar el resumen criptográfico del índice (lo que permite comprobar su autenticidad) y del certificado. Como esta propuesta pueden encontrarse bastantes más, buena muestra del interés de la comunidad académica

Desde otra perspectiva, más centrada en el usuario y la analítica de datos, han definido una implementación práctica de una nueva plataforma para realizar un seguimiento de los logros de aprendizaje más allá de las transcripciones y los certificados tradicionales, manteniendo resúmenes digitales (hashes) de actividades de aprendizaje y administrando los derechos de acceso mediante el uso de contratos inteligentes en la cadena de bloques. Este sistema, al que se refieren como cadena de bloques de registros de aprendizaje (BOLL) es una plataforma que permite a los alumnos mover sus registros de aprendizaje de una institución a otra en

un formato seguro y verificable, lo que denota la transformación que permite, desde la perspectiva de la gestión de documentos, la utilización de estas tecnologías.

En todo caso, quizá sean quienes hayan identificado de forma más completa las problemáticas que resuelve la aplicación de esta tecnología en la gestión de expedientes académicos, especialmente en economías frágiles: en primer lugar, *blockchain* hace que sea muy difícil atacar o cambiar los registros académicos porque estos registros son mantenidos y almacenados por todos los nodos de la red. En segundo lugar, *blockchain* facilita el proceso de verificación de registros académicos al proporcionar una plataforma de grabación distribuida descentralizada. En tercer lugar, *blockchain* reduce los recursos humanos necesarios para brindar servicios educativos como la emisión, autenticación y verificación de registros académicos, o incluso el intercambio de información académica entre universidades. En cuarto lugar, el uso de *blockchain* para administrar los registros académicos puede resolver el problema de un solo punto de falla al distribuir una copia descentralizada de los datos a cada nodo de la red. En quinto lugar, *blockchain* permite rastrear cualquier cambio en la información de la red hasta la raíz.

Como se puede ver en los anteriores ejemplos, la *DLT/Blockchain* ofrece importantes posibilidades de innovación en la gestión de documentos, en especial en relación con las transacciones de datos y de los documentos, externos a esta, que la misma sustenta.

Sin embargo, el libro mayor electrónico es también un objeto con valor documental, que deberemos tratar adecuadamente, y sujeto a necesidades de conservación, igual que sucede con los documentos electrónicos, lo que exige la adopción de las correspondientes prácticas, por ejemplo, para su conservación.

La European Blockchain Services Infrastructure

Como ejemplo de sistema que ya empieza a madurar en nuestro entorno, podemos referirnos a la Infraestructura Europea de Servicios Blockchain (*European Blockchain Services Infrastructure* o EBSI, en inglés), una iniciativa conjunta entre la Comisión Europea y la Asociación Europea de Blockchain (EBP) para brindar servicios públicos transfronterizos en toda la UE mediante el uso de la tecnología *blockchain*. Para ello, la EBSI se materializará como una red de nodos distribuidos en toda Europa, la infraestructura *blockchain*, aprovechando un número cada vez mayor de aplicaciones centradas en casos de uso específicos.

EBSI es también un bloque de construcción del Mecanismo Conectar Europa que proporciona software, especificaciones y servicios reutilizables para respaldar la adopción por parte de las administraciones públicas, las empresas y los ciudadanos, y ha definido una completa arquitectura tecnológica para facilitar el desarrollo y despliegue de casos de uso.

En la actualidad, EBSI se encuentra formada por dos sistemas de *blockchain*; i.e. Ethereum pública permissionada con base en Hyperledger BESU, y Hyperledger Fabric, que se utilizan en función de las exigencias y características de cada caso de uso.

Los casos de uso actualmente considerados en EBSI incluyen:

- Marco de Trabajo de Identidad Auto-Soberana Europea (*European Self-Sovereign Identity Framework* o ESSIF, en inglés), que, con base en la lógica del Reglamento eIDAS, ha desarrollado los fundamentos para un sistema de obtención y compartición de credenciales de identidad, bajo el control y autonomía personal del interesado, tanto para identificación electrónica cuanto para otras informaciones personales.
- Diplomas, que supone una implementación práctica de ESSIF, adaptada a las particularidades de las evidencias de cualificación profesional, con especial foco en el empleo de *blockchain* como registro de emisores confiables.
- Trazabilidad de documentos, anteriormente conocido como Notarización, un confuso nombre –por no referirse a la actividad de los Notarios– que sustenta un servicio de prueba digital descentralizada de documentos y metadatos asociados a los mismos, el cual podría ser empleado como prueba de existencia de documentos, y de los eventos asociados a la gestión de los mismos.
- Intercambio fiable de datos (*Trusted Data Sharing*, en inglés), un nuevo enfoque para construir un sistema distribuido y descentralizado mediante la interconexión de las entidades públicas y privadas de todos los Estados miembros en una plataforma dedicada para compartir datos en lugar de intercambiarlos, ofreciendo trazabilidad completa, gestión de la propiedad y gestión del ciclo de vida de los datos, con el objetivo de desarrollar una infraestructura de plataforma *blockchain*, que técnicamente permita a las entidades de los Estados miembros compartir datos de manera pública o privada y verificar la validez, la propiedad y la autenticidad de estos datos.

EBSI representa una oportunidad importante para la transformación digital de las Administraciones, facilitando la implementación de nuevos mecanismos de actuación electrónica en entornos complejos, y sustentando los datos como evidencia jurídica de dicha actuación.

Como se puede ver, EBSI ha abordado algunas de las funcionalidades relevantes en el ámbito de la gestión documental, ciertamente limitadas, pero transformadoras en la práctica de negocio, especialmente desde la perspectiva de la adopción del libro mayor como evidencia de documentos, sean éstos acreditativos de la identidad personal, de otras atribuciones personales (como sucede con las titulaciones académicas, y en el futuro otros muchos atributos) o, en general, de cualquier tipo.

La acreditación de la existencia de transacciones y de documentos con base en el libro mayor distribuido puede transformar la forma en la que se capturan los documentos y, lo que es más importante, las evidencias acerca de los eventos acerca de los documentos, que en la actualidad se encuentran centralizadas en bases de datos o, en demasiados casos, simplemente no se capturan.

Sin embargo, para que podamos confiar en estas tecnologías, a mi juicio es ineludible que las mismas ofrezcan garantías apropiadas, y a pesar de que existen diversas opciones para “regular lo desconocido”, en mi opinión resulta oportuno y conveniente proceder al establecimiento de un marco regulatorio, como veremos a continuación.

Una propuesta de régimen jurídico para *blockchain*

El pasado 3 de junio, Margrethe Vestager, Vicepresidenta Ejecutiva de la Comisión Europea para Una Europa Adaptada a la Era Digital, y Thierry Breton, Comisario de Mercado Interior, presentaron en Bruselas el esperado texto de la propuesta de modificación del Reglamento eIDAS, para establecer un marco para la Identidad Digital Europea (COM 2021 281 final), y que viene, entre otras cuestiones, a regular los libros mayores electrónicos, incluyendo aquellos basados en *Blockchain*.

De forma novedosa, entre los contenidos del borrador, encontramos una regulación del libro mayor electrónico (*electronic ledger*), en línea con mi propuesta contenida en el SSI eIDAS Legal Report, desarrollada con una elevada discreción en el marco de EBSI V2.0.

La necesidad de establecer este régimen jurídico se viene a mencionar en la memoria que acompaña a la propuesta de Reglamento eIDAS 2, que explica que los libros mayores electrónicos aportan a los usuarios prueba y una pista inmutable de auditoría para la secuenciación de transacciones y registros de datos, protegiendo la integridad de los datos. Entre los casos de uso que se citan encontramos su utilidad para la compartición de datos desde fuentes descentralizadas, para las soluciones de identidad auto soberana o para la atribución de titularidad en los activos digitales, entre otros.

Asimismo, la propuesta enfatiza que, al objeto de prevenir la fragmentación, es necesario definir un único marco paneuropeo que permita el reconocimiento transfronterizo de los servicios de confianza que ofrezcan soporte a la operación de los libros mayores electrónicos, algo que es especialmente relevante cuando el enfoque técnico sea el de una DLT o *Blockchain*.

No es la primera vez que se propone una regulación generalista de la *DLT/Blockchain* como tal, debiéndonos referir a como ha sucedido en España con la normativa aragonesa, o en Italia con el decreto-ley 135/2018 (convalidado por

Ley 12/2019) otorgando a estas tecnologías efecto jurídico equivalente al sello electrónico de tiempo, o en Andorra con la recientísima Ley 29/2021, de 29 de abril, pero se trata de la primera ocasión en la que se propone una visión completa, con un enfoque neutral que también incluye soluciones centralizadas, incluyendo la definición del concepto, el establecimiento de requisitos y del efecto jurídico.

Siguiendo el enfoque de doble nivel propio del Reglamento eIDAS se garantiza, en primer lugar, que todo libro mayor electrónico gozará del principio de no discriminación, pero que, en el caso de que el mismo sea cualificado, gozará de una presunción de unicidad y autenticidad de los datos que contiene, de la precisión de su fecha y hora, y de su ordenación secuencial cronológica dentro del libro.

La definición del libro mayor electrónico contenida en la Propuesta se refiere a un “registro electrónico inviolable de datos que garantiza la autenticidad y la integridad de los datos que contiene, la exactitud de su fecha y hora y su orden cronológico”, en una aproximación tecnológicamente neutral, que permite sistemas centralizados y distribuidos, como la *DLT/Blockchain*.

En mi opinión, este marco puede suponer la superación de algunas de las problemáticas que están impidiendo el despliegue de las soluciones de SSI y *DLT/Blockchain*, en especial desde la óptica del uso de *blockchain* como instrumento acreditativo y de transferencia de responsabilidad legal.

A diferencia de lo expresado por autores como, que se refiere a la necesaria decisión judicial en caso de controversia, considerando que “para valorar este tipo de prueba, la comunidad jurídica podrá en mi opinión optar entre la aceptación «ad mathematicatem» del procedimiento, asumiendo que nos encontraremos ante inmutables realidades estadísticas o analizar en profundidad los distintos procedimientos que se utilicen y ponderar su efectividad para concretos propósitos acreditativos”, parece que la propuesta de la Comisión Europea presenta un enfoque radicalmente diferente orientado a facilitar la adopción de estas tecnologías mediante su regulación como servicio de confianza, y el establecimiento de las correspondientes presunciones jurídicas.

En este sentido, el artículo 45h de la Propuesta establece los efectos jurídicos del libro mayor electrónico, partiendo del principio de no discriminación, en cuya virtud “no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un libro mayor electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos de los libros mayores electrónicos cualificados”; pero apostando porque “un libro mayor electrónico cualificado gozará de la presunción de unicidad y autenticidad de los datos que contiene, de la exactitud de su fecha y hora y del orden cronológico secuencial interno del libro mayor”, algo que realmente facilita la adopción de estas tecnologías para todo tipo de operativas.

En mi opinión, la regulación del libro mayor electrónico es un imperativo en orden a su adopción fiable, en especial debido a la sustitución de los protocolos

de consenso basados en prueba de trabajo (*proof of work*) por otros protocolos que no se basan en pruebas matemáticas intensivas, como sucede con prueba de autoridad (*proof of authority*) o prueba de participación (*proof of stake*).

En este sentido, resulta muy interesante que el artículo 45i de la Propuesta haya establecido los requisitos que debe cumplir todo libro mayor electrónico, incluyendo su creación por uno o más proveedores de servicios de confianza cualificados, la garantía de la unicidad, autenticidad y secuencia correcta de las entradas de datos registradas en el libro mayor; la garantía del orden cronológico secuencial correcto de los datos en el libro mayor y la precisión de la fecha y hora de la entrada de datos; y el registrar de datos de tal manera que cualquier cambio posterior en los datos sea inmediatamente detectable.

Por otra parte, la Propuesta no aborda más que una pequeña parte de los desafíos jurídicos que plantea el uso de estas tecnologías, de los que da buena cuenta, por lo que, como se reconoce en la Propuesta, esta norma paneuropea para operadores de nodos se aplicará sin perjuicio de otra legislación secundaria de la UE, por lo que, cuando se utilicen libros de contabilidad electrónicos para respaldar la emisión y/o negociación de bonos, o para criptoactivos, los casos de uso deberán ser compatibles con todas las normas financieras aplicables, por ejemplo, con la Directiva sobre mercados de instrumentos financieros, la Directiva sobre servicios de pago y la Regulación de los mercados de criptoactivos.

Y, por supuesto, cuando los casos de uso involucren datos personales, los proveedores de servicios deberán cumplir con la correspondiente normativa reguladora, una de las cuestiones que más debate está generando, en particular desde la perspectiva de la posibilidad qué datos pueden ser considerados como no personales o datos seudonimizados, algo muy relevante cuando los mismos deben ser escritos en una *blockchain* pública o pública permissionada.

En definitiva, a mi juicio cabe realizar una valoración positiva de la Propuesta de Reglamento por su carácter innovador en cuanto a la regulación de una cuestión tan innovadora y compleja, si bien la misma deberá ser objeto de la necesaria discusión durante el correspondiente procedimiento. No faltarán voces argumentadas que apuesten por mantener esta tecnología sin regulación, pero lo cierto es que el Derecho debe reaccionar ante las disfunciones que hace ya tiempo vienen observándose en este ámbito.

Bibliografía

Alamillo Domingo, I. (2020). *SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market*. https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf. [Consulta: 28/07/2021]

- Alimehaj, V., Halili, A., Dervishi, R., Neziri, V., & Rexha, B. (2021). Analysing and comparing the digital seal according to eIDAS regulation with and without blockchain technology. *International Journal of Information and Computer Security*, 14(2), 171. <<https://doi.org/10.1504/IJICS.2021.113174>>. [Consulta: 28/07/2021]
- Alnafrah, I., & Mouselli, S. (2021). Revitalizing blockchain technology potentials for smooth academic records management and verification in low-income countries. *International Journal of Educational Development*, 85, 102460. <<https://doi.org/10.1016/j.ijedudev.2021.102460>>. [Consulta: 28/07/2021]
- Anguiano Jiménez, J. M. (2018). Blockchain: Fundamentos y perspectiva jurídica. De la confianza al consenso. *Diario La Ley*, 18.
- Ateniese, G., Magri, B., Venturi, D., & Andrade, E. (2017, April). Redactable Blockchain – or – Rewriting History in Bitcoin and Friends. *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*. <<https://doi.org/10.1109/EuroSP.2017.37>>. [Consulta: 28/07/2021]
- Buldas, A., Draheim, D., Nagumo, T., & Vedeshin, A. (2020). Blockchain Technology: Intrinsic Technological and Socio-Economic Barriers. In T. K. Dang, J. Küng, M. Takizawa, & T. M. Chung (Eds.), *Future Data and Security Engineering* (pp. 3–27). Springer International Publishing.
- Cappiello, B., & Carullo, G. (2021). Introduction: The Challenges and Opportunities of Blockchain Technologies. In G. Cappiello Benedetta and Carullo (Ed.), *Blockchain, Law and Governance* (pp. 1–9). Springer International Publishing.
- Carullo, G. (2021). The Role of Blockchain in the Public Sector: An Overview. In G. Cappiello Benedetta and Carullo (Ed.), *Blockchain, Law and Governance* (pp. 43–57). Springer International Publishing.
- Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1). <<https://doi.org/10.1093/idpl/ipz026>>. [Consulta: 28/07/2021]
- Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J. (2020). A Survey on Blockchain Technology Concepts, Applications, and Issues. *SN Computer Science*, 1(2), 114. <<https://doi.org/10.1007/s42979-020-00123-0>>. [Consulta: 28/07/2021]
- Giordano, M. T. (2021). Blockchain and the GDPR: New Challenges for Privacy and Security. In G. Cappiello Benedetta and Carullo (Ed.), *Blockchain, Law and Governance* (pp. 275–286). Springer International Publishing.
- Hellwig, D., Karlic, G., & Huchzermeier, A. (2020). *Build Your Own Blockchain*. Springer International Publishing. <<https://doi.org/10.1007/978-3-030-40142-9>>. [Consulta: 28/07/2021]
- Ibáñez Jiménez, J. W. (2018). *Derecho de blockchain y de la tecnología de registros distribuido*. Aranzadi.
- Kusber, T., Schwalm, S., Shamburger, K., & Korte, U. (2020). Criteria for trustworthy digital transactions-Blockchain/ DLT between eIDAS, GDPR, Data and Evidence Preservation. In H. Roßnagel, C. H. Schunck, S. Mödersheim, & D. Hühnlein (Eds.), *Open Identity Summit 2020, Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)* (pp. 49–60).
- Lai, T. (2021). Blockchain, Law and Governance: General Conclusion. In G. Cappiello Benedetta and Carullo (Ed.), *Blockchain, Law and Governance* (pp. 289–304). Springer International Publishing.
- Liu, Y., Li, K., Huang, Z., Li, B., Wang, G., & Cai, W. (2021). EduChain: A Blockchain-Based Education Data Management System. In J. and S. X. and L. Z. Xu Ke and Zhu (Ed.), *Blockchain Technology and Application* (pp. 66–81). Springer Singapore.
- Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., Smith, H., Aidinlis, S., & Kaye, J. (2018). Are ‘pseudonymised’ data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review*, 34(2), 222–233. <<https://doi.org/10.1016/J.CLSR.2018.01.002>>. [Consulta: 28/07/2021]
- Ocheja, P., Flanagan, B., Ueda, H., & Ogata, H. (2019). Managing lifelong learning records through blockchain. *Research and Practice in Technology Enhanced Learning*, 14(1), 4. <<https://doi.org/10.1186/s41039-019-0097-0>>. [Consulta: 28/07/2021]
- Ølnes, S. (2016). Beyond Bitcoin Enabling Smart Government Using Blockchain Technology. In O. and J. M. and K. B. and L. I. and P. P. and T. E. and W. M. A. and J. T. and S. S. D. Scholl Hans Jochen and Glassey (Ed.), *Electronic Government* (pp. 253–264). Springer International Publishing.
- Ølnes, S., & Jansen, A. (2017). Blockchain Technology as a Support Infrastructure in e-Government. In M. Janssen, K. Axelsson, O. Glassey, B. Klievink, R. Krimmer, I. Lindgren, P. Parycek, H. J. Scholl, & D. Trutnev (Eds.), *Electronic Government* (pp. 215–227). Springer International Publishing.
- Rama Reddy, T., Prasad Reddy, P. V. G. D., Srinivas, R., Raghavendran, Ch. v, Lalitha, R. V. S., & Annapura, B. (2021). Proposing a reliable method of securing and verifying the credentials of graduates through blockchain. *EURASIP Journal on Information Security*, 2021(1), 7. <<https://doi.org/10.1186/s13635-021-00122-5>>. [Consulta: 28/07/2021]
- Swan, M. (2015). *Blockchain. Blueprint for a new economy*. O'Reilly Media, Inc.
- Turi, A. N. (2020). Blockchain and Distributed Ledger Technology Applications. In A. N. Turi (Ed.), *Technologies for Modern Digital Entrepreneurship: Understanding Emerging Tech at the Cutting-Edge of the Web 3.0 Economy* (pp. 123–154). Apress. <https://doi.org/10.1007/978-1-4842-6005-0_4>. [Consulta: 28/07/2021]
- Turkanović, M., & Podgorelec, B. (2020). Signing Blockchain Transactions Using Qualified Certificates. *IEEE Internet Computing*, 24(6), 37–43. <<https://doi.org/10.1109/MIC.2020.3026182>>. [Consulta: 28/07/2021]
- Weber, I., Lu, Q., Tran, A. B., Deshmukh, A., Gorski, M., & Strazds, M. (2019). A Platform Architecture for Multi-Tenant Blockchain-Based Systems. *2019 IEEE International Conference on Software Architecture (ICSA)*, 101–110. <<https://doi.org/10.1109/ICSA.2019.00019>>. [Consulta: 28/07/2021]
- Zhang, C., Ni, Z., Xu, Y., Luo, E., Chen, L., & Zhang, Y. (2021). A trustworthy industrial data management scheme based on redactable blockchain. *Journal of Parallel and Distributed Computing*, 152, 167–176. <<https://doi.org/https://doi.org/10.1016/j.jpdc.2021.02.026>>. [Consulta: 28/07/2021]