

■ **EL CONSULTOR**
DE LOS AYUNTAMIENTOS

Blockchain y automatización de procedimientos en la Administración Pública

*Pablo
García-Valdecasas
Rodríguez de Rivera*

Blockchain y automatización de procedimientos en la Administración Pública

Pablo García-Valdecasas Rodríguez de Rivera

© Pablo García-Valdecasas Rodríguez de Rivera, 2022
© Wolters Kluwer Legal & Regulatory España, S.A.

Wolters Kluwer Legal & Regulatory España

C/ Collado Mediano, 9

28231 Las Rozas (Madrid)

Tel: 91 602 01 82

e-mail: clienteslaley@wolterskluwer.es

<http://www.wolterskluwer.es>

Primera edición: Marzo 2022

Depósito Legal: M-5731-2022

ISBN versión impresa: 978-84-7052-900-9

ISBN versión electrónica: 978-84-7052-901-6

Diseño, Preimpresión e Impresión: Wolters Kluwer Legal & Regulatory España, S.A.

Printed in Spain

© **Wolters Kluwer Legal & Regulatory España, S.A.** Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, Wolters Kluwer Legal & Regulatory España, S.A., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.

El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.

WOLTERS KLUWER LEGAL & REGULATORY ESPAÑA no será responsable de las opiniones vertidas por los autores de los contenidos, así como en foros, chats, u cualesquiera otras herramientas de participación. Igualmente, WOLTERS KLUWER LEGAL & REGULATORY ESPAÑA se exime de las posibles vulneraciones de derechos de propiedad intelectual y que sean imputables a dichos autores.

WOLTERS KLUWER LEGAL & REGULATORY ESPAÑA queda eximida de cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a la falta de veracidad, exactitud, exhaustividad y/o actualidad de los contenidos transmitidos, difundidos, almacenados, puestos a disposición o recibidos, obtenidos o a los que se haya accedido a través de sus PRODUCTOS. Ni tampoco por los Contenidos prestados u ofertados por terceras personas o entidades.

WOLTERS KLUWER LEGAL & REGULATORY ESPAÑA se reserva el derecho de eliminación de aquellos contenidos que resulten inveraces, inexactos y contrarios a la ley, la moral, el orden público y las buenas costumbres.

Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de **Wolters Kluwer Legal & Regulatory España, S.A.**, es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

CAPÍTULO IV

LA TECNOLOGÍA DE REGISTROS DISTRIBUIDOS. «BLOCKCHAIN»

1. ÁMBITO CONCEPTUAL, ELEMENTOS IDENTIFICATIVOS Y OPERATIVA DE FUNCIONAMIENTO

La tecnología de registros distribuidos, como analizamos a continuación, es el embrión de la tecnología «blockchain» o, siendo más precisos, la tecnología que sirve de soporte para entender, plantear y configurar una cadena de bloques, y que a su vez ha permitido el desarrollo, por ejemplo, de criptomonedas como «bitcoin»⁽¹⁾. «Blockchain» ha sido definido como una herramienta tecnológica que posibilita «*un sistema de contabilidad distribuido digital que actúa como un registro abierto, compartido y de confianza que realiza transacciones entre las partes y no se almacena por una autoridad central y sigue manteniendo el enfoque tradicional*» (BERRYHILL, BOURGERY y HANSON, 2018⁽²⁾).

Esta tecnología se creó en los años 90, si bien ha sido posteriormente cuando ha sido más conocida y ha adquirido mayor expansión, sobre todo con motivo del desarrollo de las criptomonedas, como el precitado Bitcoin. Básicamente, esta tecnología opera generando un registro, denominado «token», por operación o actuación y, de este modo, el número o volumen de «tokens» (u operaciones ejecutadas), configuran un bloque que se vincula con el precedente y posteriores, sin que puedan ser separados ni alterar la secuencia dinámica que sigue todo el proceso. A su vez, cabe señalar que, por lo general, los sistemas basados en «blockchain» tienen como característica que son descentralizados y distribuidos, lo que asimismo significa que no concurre una autoridad reguladora o supervisora central, y tampoco es posible, —en principio—, modificar los contenidos registrados a través de una «cadena de bloques» (esto refiere una de sus características, permanencia o inmutabilidad de lo registrado). Por ello, por

-
- (1) Al respecto, «Bitcoin» es una de las primeras monedas virtuales, exclusivamente digitales, que han surgido basadas en tecnología «blockchain», no existiendo una autoridad o ente de control que sea responsable de su emisión y registro de sus movimientos, de donde deriva la complejidad de su tratamiento legal y de su reconocimiento como moneda oficial.
 - (2) BERRYHILL, J., BOURGERY, T., y HANSON, A., «Blockchains Unchained: Blockchain Technology and its Use in the Public Sector», *OECD Working Papers on Public Governance*, n.º. 28, OECD Publishing, Paris, 2018. <https://doi.org/10.1787/3c32c429-en>. Disponible en (fecha última consulta: 03/06/2021): <https://www.oecd.org/gov/innovative-government/oecd-guide-to-blockchain-technology-and-its-use-in-the-public-sector.htm>

ejemplo, las transacciones realizadas solo podrían ser alteradas mediante el acuerdo entre las partes intervinientes, no existiendo *a priori* una autoridad competente que controle, de forma centralizada, ésta operativa. Estos son, entre otros, algunos de los elementos identificativos de esta tecnología, conforme se analiza en los siguientes apartados de este capítulo.

De este modo, en la actualidad, el interés que ha despertado el empleo de esta tecnología se debe a la utilidad que puede procurar —tal y como ulteriormente se detalla— el hecho de poder configurar un sistema operativo seguro que permita la realización de distintas acciones y una ágil dinámica o intercambio de datos e información, así como el desarrollo de transacciones, contratos u otros negocios jurídicos.

Esta tecnología, por tanto, plantea una forma innovadora y disruptiva de tratamiento, almacenaje y cesión de la información, que se separa de los tradicionales sistemas de centralización de datos, y que conviene tomar en consideración con las debidas cautelas, cuando de lo que se trata es de pretender su implantación en el ámbito de las Administraciones públicas. Además, esta tecnología añade elementos especialmente innovadores y disruptivos, en lo que se refiere a la tecnología y la digitalización, que refuerzan y dotan de especial seguridad y protección, al referido tratamiento distribuido de la información. Dichos elementos son, entre otros, el encriptado de los datos de la cadena de bloques, la automatización de las decisiones adoptadas en su seno, gracias a las preestablecidas normas o protocolos de consenso⁽³⁾, y la interconexión múltiple de cada bloque de la cadena, con la misma información replicada y validada en cada bloque por cada nodo, lo que complica posibles alteraciones externas de la información almacenada (la conocida como «inmutabilidad» de la información).

Estos elementos identificativos, y otros que son analizados en detalle, deben poder conjugarse adecuadamente con el marco jurídico vigente, con objeto de hacer compatible su aplicación en el Sector Público, con el adecuado respeto y protección de los Derechos Fundamentales, y de las debidas garantías y principios que rigen los procedimientos administrativos y la prestación de servicios públicos al ciudadano.

1.1. De la tecnología de registros distribuidos a «blockchain». Aproximación terminológica y referencia al contexto tecnológico

La tecnología de registros distribuidos es la que se basan las cadenas de bloques o «blockchain» y cuyo máximo exponente o, mejor dicho, cuyos princi-

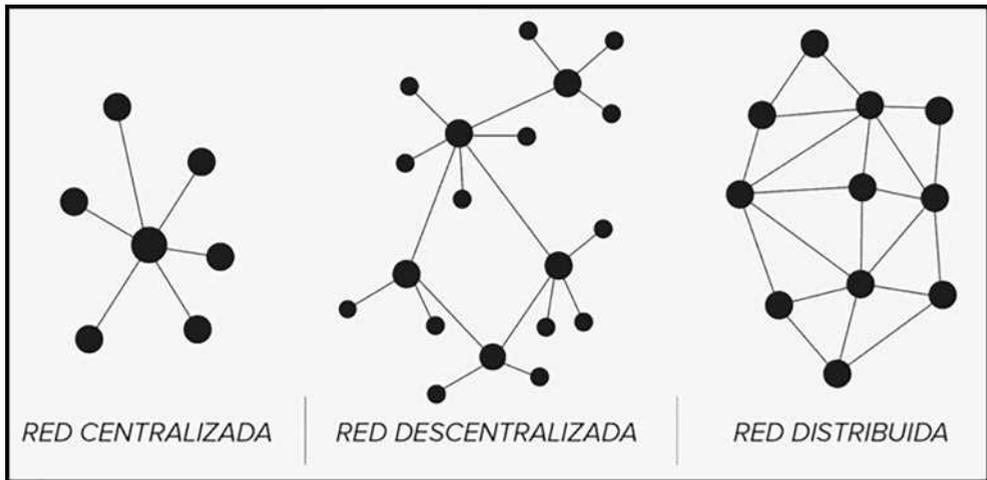
(3) Al respecto, las normas o protocolos de consenso utilizados en la tecnología «blockchain» son algoritmos que aseguran el cumplimiento automatizado de las reglas y principios a los que se someten los participantes de cada cadena de bloques, y que rigen en especial las relaciones de confianza de la red y la comunicación de los nodos de la misma.

pales abanderados que le han dado fama, han sido las criptomonedas, supone un cambio radical y opuesto al modelo tradicional de tratamiento, acceso y compartimentación de la información, que conlleva importantes implicaciones en cada uno de los sectores en los que podamos imaginar que puede resultar factible su aplicación. ROMERO UGARTE define un registro distribuido como «una base de datos de la que existen múltiples copias idénticas distribuidas entre varios participantes, las cuales se actualizan de manera sincronizada por consenso de las partes. Es decir, es una base de datos de la que existen múltiples copias idénticas que están distribuidas entre varios participantes y que se actualizan de manera sincronizada»⁽⁴⁾.

Tal y como continúa explicando el precitado autor, «una diferencia destacada entre un DLT y una base de datos distribuida "tradicional" radica en el procedimiento de actualización: mientras que en una base de datos distribuida tradicional los participantes confían unos en otros y colaboran para mantener la consistencia de los datos, en un DLT no existe confianza total entre las partes (o hay intereses contrapuestos), por lo que debe implantarse un mecanismo para verificar colectivamente los registros antes de compartirlos. En otras palabras, las actualizaciones no las realiza una autoridad central, sino que se producen por consenso de las partes, conforme a unas reglas o procedimientos aceptados por todos. Normalmente, los DLT se implementan mediante una blockchain o cadena de bloques, que es un tipo de base de datos en la que las transacciones individuales se procesan y almacenan en grupos o bloques, conectados unos a otros en orden cronológico para crear una cadena. La integridad y la seguridad de los datos almacenados en la cadena se garantizan mediante criptografía».

Por lo general, por tanto, las redes pueden clasificarse en función de los distintos tipos de almacenamiento de información que hayan adoptado en su configuración, según ésta esté centralizada, descentralizada, o distribuida. Las Administraciones públicas han venido operando de manera principalmente centralizada, donde cada registro de la red tiene su propia información, no compartida con otro registro, y donde la automatización en la consulta o, al menos, la consulta automática de la información, se paraliza ante la necesidad de habilitar los permisos adecuados y articular los mecanismos de interoperabilidad que sean necesarios. En el siguiente cuadro se observa mejor:

(4) ROMERO UGARTE, J.L., «Tecnología de registros distribuidos (DLT): una introducción». Banco de España. Boletín Económico 4/2018, artículos analíticos. 2018. Artículo completo disponible en el siguiente enlace (última consulta 03/11/2020): <https://repositorio.bde.es/bitstream/123456789/8390/1/beaa1804-art26.pdf>



Fuente (última consulta 03/11/2020): <https://academy.bit2me.com/tipos-redes-criptomonedas/>

Una red centralizada es aquella en la que cada ordenador que la conforma está conectado a una unidad o registro central. Sobre esta unidad central recae todo el control y gestión de la red. Es decir, toda la responsabilidad y poder de decisión recae sobre un solo elemento, en este caso una máquina o una entidad. Este es el caso que se da cuando accedemos a ciertas redes de entidades públicas, como un registro de alguna Administración pública, en sede electrónica, ya que la información se almacena solo en un punto y a ese punto es al cual debemos apuntar o dirigirnos para obtener la información.

En las redes descentralizadas, por su parte, no hay una única unidad o registro central, sino que existen una serie de ordenadores o unidades que funcionan en conjunto para controlar y manejar la red. Un buen ejemplo de este tipo de redes son Facebook o Google. Todos estos servicios cuentan con subredes dentro de una gran red y en su conjunto son capaces de manejar todos los servicios que prestan. Por último, las redes distribuidas carecen de una unidad o registro central. Los ordenadores en estas redes se unen unos a otros de tal forma que ninguno de ellos tiene poder de filtro sobre la información que se transmite en la red. Es esta forma de almacenamiento de la información y funcionamiento en red en la que se basa «blockchain» y la tecnología de registros distribuidos.

El ejemplo más claro de este tipo de redes es Internet. Desde su nacimiento, Internet fue pensado para ser una red completamente distribuida. En principio, fue una red muy centralizada debido a los pocos ordenadores que estaban conectados en ese momento. Pero a medida que aumentaron los ordenadores interconectados, Internet pasó a convertirse en una red distribuida. Una cadena de bloques, o «blockchain», cuenta con varios elementos que, al menos de

manera somera, conviene definir y tener claro su función. Podemos encontrar «nodos», «bloques», y el «hash». Conviene que nos detengamos en cada uno de ellos. Los nodos, que pueden ser mineros o no, son los dispositivos que se conectan a la cadena de bloques o «blockchain». Estos nodos pueden crear, recibir o transmitir información. Por lo general suelen acceder de forma gratuita y libre, aunque, como explicaremos más adelante, hay cadenas de bloques privadas que requieren autenticación para su acceso.

El hash es una función o código criptográfico que se aplica al conjunto de transacciones para identificar de forma unívoca el contenido de cada bloque. Por su parte, los bloques de la cadena son creados por los nodos mineros, y validados por todos los nodos de la red, de tal forma que cada bloque contendría información validada por todos y cada uno de los nodos. Un bloque contiene, a su vez, distintos elementos, como la referencia al bloque anterior —el hash del bloque anterior— la referencia al hash del bloque actual, el número «nonce» —que se denomina por sus siglas en inglés «*number that can be only used once*», y que se trata de un número arbitrario que se emplea en criptografía dentro de los denominados protocolos de autenticación— y la marca de tiempo. Adicionalmente el bloque tiene un cuerpo donde se almacenan las transacciones. La primera diferencia de esta tecnología la encontramos, por tanto, en el número de bloques en los cuales la información está almacenada, y en la forma en la que los nodos actualizan o modifican dicha información.

A diferencia del sistema tradicional, en el cual la información se encuentra en un registro único, o en varios, de manera centralizada, al cual deben hacerse las oportunas consultas, aquí la información se encuentra compartida y almacenada en múltiples registros, de tal forma que el acceso a la información por parte de cualquiera de ellos, y en general de todos los usuarios de la red o de la cadena de bloques, es automática, pues toda la red comparte la información que está distribuida por todos los bloques de la cadena, tras la actuación de los nodos. La modificación o actualización de la información obrante en la cadena de bloques también es peculiar, pues requiere el consenso o aceptación de todos los nodos, lo que conlleva, primero, contar con unas reglas para configurar dicho consenso, segundo, que las posibilidades de atentar contra la privacidad de la información o contra la propia información son menores pues al estar almacenada en múltiples bloques y necesitar el consenso de todos los nodos, habría que «hackear» todos los bloques en los cuales la información está almacenada, y tercero que cada modificación o actualización de la información, al ser aceptada por consenso por todos los nodos, implica que la información actualizada vuelve a estar compartimentada y almacenada en todos los bloques, volviendo a ser de consulta o utilización automática.

Normalmente, y en función del tipo de acceso que se requiere a los usuarios para acceder a la red, como decíamos antes, podemos encontrar redes públicas y redes privadas. Al respecto, como continúa explicando el precitado autor, «una



La transformación digital está suponiendo un verdadero reto para los juristas, los cuales se enfrentan a una realidad cada vez más digital, globalizada y automatizada, necesitada de la cobertura legal suficiente que la dote de las mismas garantías jurídicas que la realidad cotidiana. En concreto, la aparición de la tecnología Blockchain y el desarrollo de la Inteligencia Artificial o de los Smart Contracts, han dado el impulso definitivo a la automatización, y han puesto sobre la mesa retos adicionales, por ejemplo, en el ámbito de la protección de datos personales. Sin duda, las Administraciones públicas afrontan un reto todavía mayor. Por un lado, por la necesidad de aprovechar el desarrollo tecnológico que impera, para que la Administración pública gane en eficiencia, y simplifique, agilice y automatice gran parte de sus procedimientos. Y, por otro lado, por el esfuerzo extraordinario que supone la adaptación a las nuevas tecnologías respetando los principios generales que rigen el Derecho Administrativo, en especial aquellos relativos a la actuación de las Administraciones públicas en sus relaciones con los ciudadanos.

La automatización vía tecnología, es decir, la posibilidad de que podamos asignar a un programa informático gobernado por un algoritmo la ejecución de una tarea, sin intervención de empleado público alguno, por referirse al ámbito de las Administraciones públicas, obliga a analizar con especial cuidado múltiples elementos característicos del Derecho Administrativo, tales como la discrecionalidad, la responsabilidad patrimonial o los conceptos de órgano administrativo y acto administrativo.

En esta monografía, se analizan en profundidad todas estas cuestiones.

