BANCO DE ESPAÑA
Eurosistema

BOLETÍN ECONÓMICO 4/2018
ARTÍCULOS ANALÍTICOS

16 de octubre de 2018

Tecnología de registros distribuidos *(DLT):* una introducción

José Luis Romero Ugarte

Resumen

La tecnología de registros distribuidos está atrayendo la atención del sector financiero, tanto por su uso en la operativa con criptoactivos como por la proliferación de iniciativas que prometen incrementar la eficiencia, transparencia, velocidad y resiliencia de algunos de los procesos que subyacen a las transacciones financieras. El presente artículo pretende ser una introducción a esta tecnología, exponiendo una serie de cuestiones básicas en torno a ella y tratando de identificar oportunidades y limitaciones intrínsecas a ella. Adicionalmente, considera posibles aplicaciones en el sector financiero y esboza algunos de los principales retos que su uso plantea para las autoridades.

Palabras clave: *DLT,* registros distribuidos, *bitcoin,* criptoactivos, criptografía, innovación, tecnología.

Códigos JEL: O31, O33.

TECNOLOGÍA DE REGISTROS DISTRIBUIDOS *(DLT):* UNA INTRODUCCIÓN

Este artículo ha sido elaborado por José Luis Romero Ugarte, de la Dirección General de Operaciones, Mercados y Sistemas de Pago[1].

Introducción

Un registro distribuido (en adelante, *DLT*[2]) es 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. Aunque el ejemplo más conocido de aplicación de esta tecnología son los criptoactivos (singularmente, el *bitcoin),* en los últimos años ha proliferado el número de iniciativas en el sector financiero, en particular en aquellos ámbitos en los que existen procesos complejos en los que intervienen numerosos actores *(v. g.,* la negociación y la poscontratación de valores o la financiación del comercio exterior). Estos casos presentan diferencias significativas con los criptoactivos en la complejidad del mecanismo de consenso o en las características de los participantes, que los hacen más fácilmente implementables. De este modo, el uso de registros distribuidos se está configurando como una herramienta que podría contribuir a reducir costes y a incrementar la trazabilidad, la transparencia y, en algunas circunstancias, la velocidad de esos procesos.

No obstante, los *DLT* no están exentos de riesgos y limitaciones más allá de los vinculados a los propios productos para los que se están empleando *(v. g.,* criptoactivos). Así, a día de hoy los registros distribuidos no son suficientemente escalables, su robustez y resiliencia no están suficientemente probadas, no han resuelto completamente el problema de la necesaria confianza de los participantes y no son interoperables entre sí ni con las infraestructuras tradicionales. Además, su funcionamiento plantea retos de naturaleza legal *(v. g.,* firmeza de las transacciones), su sistema de gobernanza no siempre es adecuado y, en algunos casos, su operativa conlleva un coste medioambiental muy elevado.

El uso de los *DLT* por el sector financiero también plantea retos para las autoridades, dado que algunas aplicaciones pueden llevar a la desintermediación de determinadas actividades y afectar a la integridad del sistema financiero, de modo que no resulta sencillo definir claramente las responsabilidades y no existe un marco supervisor adecuado. Aunque el uso de esta tecnología es limitado a día de hoy, es conveniente profundizar en el conocimiento de sus posibilidades e implicaciones, a fin de poder valorar los proyectos que vayan surgiendo y ante la perspectiva de que su uso pueda seguir creciendo a medio plazo.

¿Qué es un *DLT?*

Un registro distribuido es, fundamentalmente, una base de datos descentralizada y única que gestionan varios participantes. 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. 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,

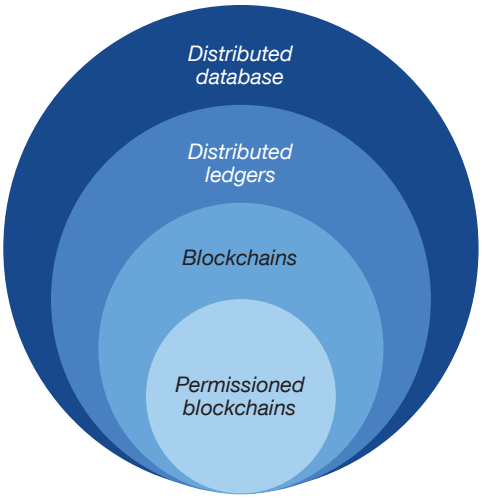
1 El autor agradece los comentarios de Juan Ayuso, Carlos Conesa, José Manuel Marqués, Ana Fernández, Sergio Gorjón y Esther Barruetabeña.

2 En inglés, *Distributed Ledger Technology.*

DLT Y *BLOCKCHAIN* SON EJEMPLOS DE BASES DE DATOS

ESQUEMA 1

Básicamente, *DLT* es un caso particular de base de datos distribuida, caracterizada por su proceso de validación consensuado. Al mismo tiempo, la tecnología *blockchain* constituye una alternativa a la hora de almacenar la información de sistemas basados en *DLT,* agrupando las transacciones por bloques en orden secuencial. Por último, dentro del *blockchain* podemos distinguir dos categorías, en función de si el acceso resulta abierto o restringido.



FUENTE: *Global blockchain benchmarking study,* Cambridge Centre for Alternative Finance.

conforme a unas reglas o procedimientos aceptados por todos[3]. Normalmente, los *DLT* se implementan mediante una *blockchain* o cadena de bloques, que es un tipo de base de datos (véase esquema 1) 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.

El primer ejemplo que conocemos de aplicación práctica de la tecnología se remonta a 2008, cuando una o varias personas, bajo el seudónimo de Satoshi Nakamoto, publicaron un documento[4] que esboza el funcionamiento de la primera «criptomoneda»: el *bitcoin.* Basándose en la tecnología *blockchain*, el documento aportaba una solución criptográfica para transferir este criptoactivo entre partes que no necesitaban conocerse ni contar con un tercero de confianza. Desde entonces, la experimentación con esta tecnología y sus potenciales aplicaciones no han cesado, tanto por parte de entidades financieras, empresas tecnológicas y desarrolladores como por parte de bancos centrales y otras autoridades, tratando de buscar un sistema seguro, escalable y adaptado a las necesidades del sector financiero.

En función de cómo sea el acceso de participantes a la red, suelen distinguirse las redes públicas de las privadas. La diferencia entre ambas radica en la existencia o no de un sistema de permisos para participar en la red, de lo que se derivan asimismo diferencias en los protocolos de consenso utilizados.

Una red pública o de acceso no restringido es completamente abierta, es decir, cualquiera puede participar. Se caracteriza, además, por requerir un sistema de incentivos que permita sumar participantes a la red que validen las transacciones. Bitcoin es a día de hoy

3 Dichos procedimientos permiten asegurar a todas las partes que las anotaciones no son el resultado de una operación fraudulenta.

4 S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* octubre de 2008.

la mayor red pública en producción, utilizando la remuneración en criptoactivos como incentivo para realizar las validaciones (esto es, los validadores reciben *bitcoins* como recompensa de las tareas que conlleva, en este caso, la validación). Las redes públicas plantean dos dificultades principales: la primera de ellas es que para alcanzar el consenso (por ejemplo, en el caso de Bitcoin) se solicita que los potenciales validadores resuelvan complejas pruebas de trabajo criptográfico (minado) que requieren el empleo de gran poder de computación; la segunda dificultad es cómo mantener la privacidad de las transacciones.

En contraste, para participar en una red privada[5] es necesaria una invitación y/o el cumplimiento de una serie de requisitos de acceso, siendo habitual que los participantes se conozcan entre sí. Este tipo de redes permite a los operadores de la red restringir el acceso a participantes en los que se confía en cierta medida, así como la asignación de roles diferenciados a los participantes[6], lo que *a priori* permitiría aligerar los requisitos de validación de un registro, mejorando la escalabilidad y limitando posibles problemas de seguridad. En el tránsito de una red pública a una red privada se pone de manifiesto cómo el anonimato y la desintermediación de la red implican un coste en términos de eficiencia. En consecuencia, la mayoría de los proyectos que están desarrollando las entidades financieras se basan en redes privadas.

¿Cómo funciona la tecnología *DLT?*

La tecnología *DLT* es fundamentalmente resultado de combinar tres tecnologías que ya existían con anterioridad (véase esquema 2):

— *Redes P2P:* en estos modelos, cada participante de la red (nodo) actúa al mismo tiempo como cliente y como servidor, aportando y consumiendo recursos. Esta tecnología se popularizó en 1999, con el lanzamiento de Napster, *software* que, básicamente, permitía a sus usuarios compartir música.

— *Criptografía:* concretamente, la criptografía asimétrica[7], que permite el intercambio seguro de información entre dos partes. Mediante su uso, se consigue autentificar al remitente, garantizar la integridad del contenido del mensaje e impedir mediante el cifrado que un tercero pueda acceder a la información en caso de que lograse interceptarlo.

— *Algoritmos de consenso:* permiten que diversos participantes, que pueden no conocerse ni confiar los unos en los otros, se pongan de acuerdo para añadir nuevas entradas al registro. Existen distintos mecanismos para alcanzar este consenso, es decir, garantizar que los registros de todos los participantes de la red son idénticos y que no se producen fraudes ni duplicidades. El más popular es el denominado *Proof of work,* coloquialmente conocido como «proceso de minado», que implica la resolución de problemas computacionales complejos para la validación y creación de cada nuevo bloque de la cadena. Este mecanismo, generalizado por Bitcoin, conlleva un gran consumo de energía para la validación de las transacciones (algunas estimaciones hablan de un consumo anual de 71,12 TWh, similar al de Chile, si bien no existen datos

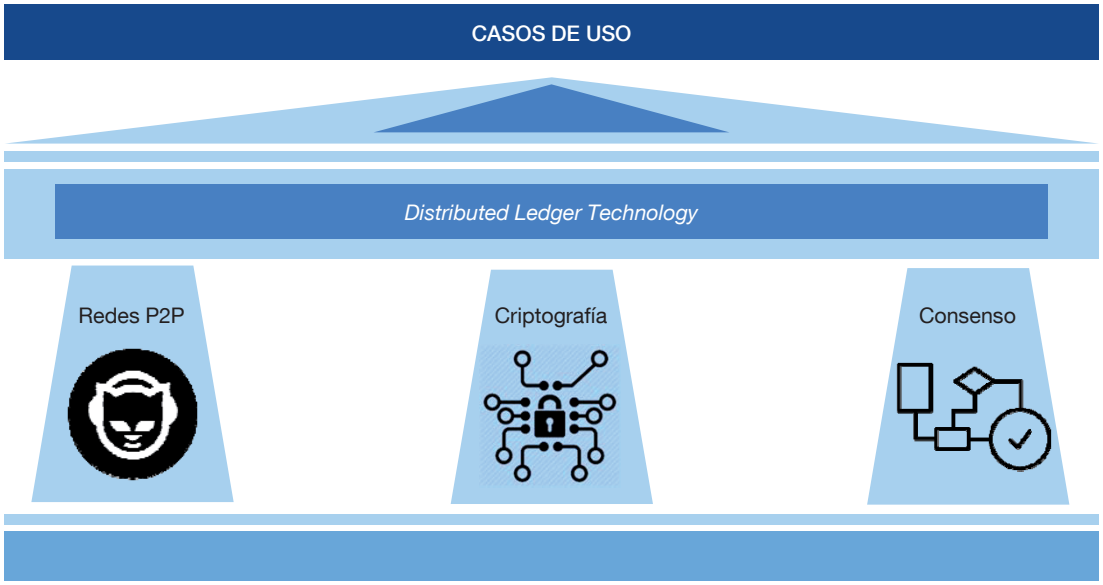
5 Este tipo de redes se conoce habitualmente como redes «privadas», «permisionadas» o «cerradas», de manera indistinta.

6 En algunos proyectos, la asignación de roles permite limitar el número de nodos que validan transacciones.

7 Cada usuario tiene una pareja de claves, una pública y una privada. La pública puede entregarse a cualquiera, que puede utilizarla para cifrar un mensaje, que únicamente podrá descifrarse mediante la clave privada correspondiente. Del mismo modo, un mensaje cifrado con una clave privada solamente podrá ser descifrado utilizando la clave pública correspondiente.

DLT COMBINA TRES TECNOLOGÍAS ANTERIORES ESQUEMA 2

La tecnología *DLT* es fundamentalmente resultado de combinar tres tecnologías que ya existían con anterioridad: redes P2P, criptografía y algoritmos de consenso.



FUENTE: Elaboración propia.

precisos al respecto) e implica unos tiempos de proceso elevados, lo que ha llevado a buscar otros mecanismos más eficientes *(v. g., Proof of stake*[8]).

El almacenamiento, mantenimiento y actualización de registros en la *DLT* (véase esquema 3) constituyen el núcleo de la tecnología. La responsabilidad de la actualización de los registros está distribuida entre los nodos, que pueden estar ubicados en distintos entornos, instituciones o jurisdicciones. Por ello, es frecuente que los cambios en el registro no estén actualizados simultáneamente en todos los nodos y se produzcan tiempos de espera hasta que todas las versiones se sincronicen.

Si bien cada uno de los participantes en una *DLT* constituye un nodo, no necesariamente todos los nodos participantes en la red cumplen las mismas funciones. Así, pueden constituir meros puntos de acceso a la red para la entrada de datos, almacenar registros, dar el consentimiento a transacciones o actuar como nodos jerárquicamente superiores cuya aprobación sea condición necesaria para el registro definitivo de una transacción. Los distintos roles dependen de las particularidades de cada una de las redes, pudiendo cada nodo adoptar más de uno al mismo tiempo.

Una de las aplicaciones que aparecen como más prometedoras en relación con el uso de *DLT* son los contratos inteligentes[9]. Básicamente, estos contratos se basan en un código o protocolo informático que facilita la verificación y la ejecución del acuerdo subyacente de forma automatizada, sin necesidad de intermediarios. Un ejemplo ilustrativo sería el pago de un cupón de una emisión de deuda, de manera que el comprador se garantiza que,

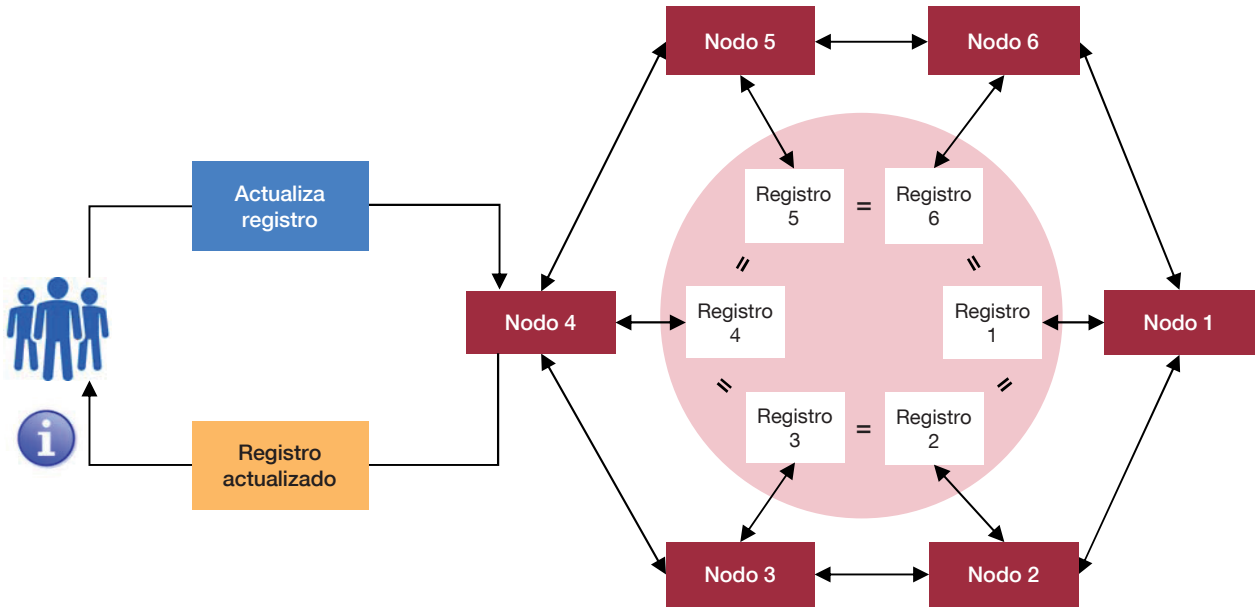
8 En lugar de minado se asigna la validación a un nodo en concreto. El criterio más habitual para seleccionarlo es en función del número de criptoactivos asociado a cada nodo de la red. Adicionalmente, pueden establecerse incentivos y penalizaciones para asegurar que el nodo realiza de modo adecuado la validación.

9 En inglés, *Smart Contracts.*

PROCESO DE ACTUALIZACIÓN DE UN *DLT* ESQUEMA 3

El presente esquema muestra, de manera muy simplificada, los principales pasos de la actualización de un registro distribuido:

a) Para iniciar la actualización del registro, mediante el uso de herramientas criptográficas, un agente firma digitalmente una transacción y la envía a la red a través de uno de los nodos, solicitando su procesamiento.
b) Recibida la solicitud, otros nodos verifican la identidad del solicitante y validan la transacción de acuerdo con el mecanismo de consenso correspondiente, confirmando que el solicitante cuenta con las credenciales necesarias para actualizar el registro (y saldo suficiente, según el caso).
c) Una vez que la transacción ha sido validada por los nodos, se actualizan los registros de cada uno de ellos.



FUENTE: Elaboración propia.

llegado el vencimiento previamente establecido, el contrato se autoejecutará transfiriendo al comprador el importe correspondiente, calculado de acuerdo con las condiciones prefijadas.

¿Para qué sirve?

La tecnología *DLT* cuenta con potencial en muy distintos ámbitos, si bien destaca principalmente en aquellos en los que participan múltiples actores y no existe confianza entre las partes[10]. En la actualidad, están proliferando multitud de proyectos, algunos de ellos meros ensayos, que no implican necesariamente que esta tecnología resulte óptima para los procesos objeto del experimento.

Si bien el principal impulso de la tecnología *DLT* ha venido por sus aplicaciones como soporte para el intercambio de criptoactivos, su potencial transformador es mayor. En los últimos años, tanto desde la industria financiera como por parte de algunas autoridades, se han iniciado múltiples proyectos para experimentar con esta tecnología en distintos ámbitos. A continuación se presentan, de modo no exhaustivo, los principales casos de uso que se están estudiando en la actualidad.

Algunos de los proyectos más prometedores se están desarrollando en el ámbito de los pagos, concretamente, en relación con las transferencias de fondos internacionales. Este tipo de iniciativas permite incrementar la velocidad de puesta a disposición de los fondos,

10 Una discusión sobre los casos en los que, en la actualidad, puede tener lógica usar la tecnología de registros distribuidos puede encontrarse en:
— Wüst y Gervais (2017).
— World Economic Forum (2018).

dotar a la operativa de mayor transparencia, así como reducir sensiblemente los costes asociados. Algunas soluciones permiten el intercambio de fondos de manera rápida y eficiente, lo que, además de las ventajas para los usuarios, mediante la realización de la operativa de manera instantánea, supone la reducción de los riesgos de compensación y de fraude, así como menores necesidades de liquidez.

Por otro lado, los proyectos más destacados en los que han participado bancos centrales, también en el ámbito de los pagos, han consistido en pruebas de concepto orientadas a la realización de pagos interbancarios. Dichos proyectos han identificado fortalezas y debilidades en el uso de esta tecnología para las infraestructuras financieras y, aunque estas experiencias se valoran como positivas, no se han observado ventajas globales frente a los actuales sistemas centralizados de pagos interbancarios. Sin embargo, existen alternativas que en un futuro podrían resultar interesantes, como la comunicación entre distintos sistemas de pagos nacionales o la introducción de otro tipo de activos como valores en los mismos registros, añadiendo funcionalidades al sistema.

En el ámbito de la negociación y de la poscontratación de valores, la tecnología *DLT* posibilitaría la creación de una base digital común, donde se registrarían la propiedad de los valores y la custodia de activos, y que sería compartida entre aquellos autorizados a acceder. Existe, por tanto, potencial para lograr acelerar la liquidación de las operaciones financieras, reducir el número de intermediarios[11] y hacer que el proceso de conciliación sea más eficiente. Distintos actores dentro del mercado de valores, tanto del sector privado como autoridades, han llevado a cabo proyectos con el fin de investigar las posibilidades de la tecnología.

El ámbito del comercio internacional se caracteriza por la intervención de multitud de actores, así como por la gran cantidad de documentación, por lo que los procesos tienden a ser complejos y no siempre plenamente transparentes, y pueden dilatarse en el tiempo, siendo otro de los ámbitos donde la tecnología *DLT* encuentra un potencial caso de aplicación. Sobre este caso de uso, una entidad española ha realizado un piloto que ha puesto de manifiesto la posibilidad de mejorar la eficiencia del proceso, así como de dotarlo de trazabilidad en todo momento. Adicionalmente, mediante el uso de la tecnología, la operación queda validada y registrada de modo transparente y seguro para todas las partes.

Otro de los ámbitos en los que están surgiendo proyectos basados en la tecnología *DLT* es el área de cumplimiento regulatorio, conocido como *regtech.* Mediante el uso de la tecnología, se busca optimizar el modo en el que satisfacer los requerimientos regulatorios *(v. g.,* obligaciones de reporte, transparencia, gestión de riesgos, control del blanqueo de capitales y financiación del terrorismo, etc.). Algunos de los aspectos que potencialmente se podrían mejorar serían la calidad de la información, así como reducir los costes de los procesos, dotar de flexibilidad y posibilitar su externalización.

Finalmente, ante la generalización del proceso de digitalización de la sociedad, se hace necesario reforzar los mecanismos para identificar de manera no presencial, precisa y eficiente a los individuos que interactúan en dicho entorno. Se trata, en definitiva, de garantizar la confianza de los usuarios en los entornos digitales, lo que resulta relevante en todos los sectores, incluido el financiero. Algunos proyectos basados en la tecnología *DLT* ofrecen precisamente una solución de gestión de identidades sobre la que se podría construir un ecosistema digital con muy variadas funcionalidades.

11 Estos serían las entidades de contrapartida central, los depositarios centrales de valores, los *brokers,* los custodios, los miembros compensadores y las entidades gestoras y liquidadoras.

Oportunidades que ofrece la adopción de la tecnología

La tecnología *DLT* tiene potencial para mejorar el diseño y, en particular, la eficiencia de algunos mercados en aspectos como:

— Eliminación de los costes de mensajería y disminución de los costes de *back-office,* al reducir la necesidad de reconciliación entre partes por estar toda la información unificada en un solo registro compartido, con copias sincronizadas.

— Reducción de la complejidad de las transacciones y mayor trazabilidad y transparencia.

— Mayor velocidad de proceso en algunos casos de uso o circunstancias y, en consecuencia, mejoras en la gestión de liquidez.

En particular, la trazabilidad del dato es un requisito fundamental de cualquier sistema de registro, permitiendo que una entidad legitimada pueda verificar el histórico de transacciones. Frente a otros sistemas tradicionales, donde dicha trazabilidad no siempre es posible en todo momento y para todos los participantes, se trata de una de las características más ventajosas de la tecnología *DLT.* Dicha trazabilidad, adicionalmente, tiene implicaciones en materia de *KYC (Know Your Customer),* así como de prevención del blanqueo de capitales y financiación del terrorismo.

La trazabilidad está ligada a la inmutabilidad de las transacciones, que implica que, una vez registradas, no se pueden modificar. Esta característica es crucial para garantizar la integridad del dato y la seguridad[12]. La combinación de estas dos características convierte el sistema en transparente y seguro para sus participantes, que en cualquier momento pueden acceder y consultar los registros, con la confianza de que se trata de registros fiables, que no pueden alterarse en el tiempo, y la certeza de que las restantes entidades que participan en la operativa tienen exactamente la misma información.

Adicionalmente, la tecnología *DLT* permite, dependiendo del tipo de registro o transacción, distintos niveles de privacidad. No resulta sencillo alcanzar un equilibrio entre privacidad y transparencia: a mayor información disponible para el validador, menor es la privacidad de la red. Por su propia naturaleza, los procesos que se apoyan en tecnología *DLT* compartirán más información que los sistemas centralizados tradicionales. Si bien en algunos modelos todos los nodos tienen una copia del registro completo y visibilidad total sobre las transacciones, en sus aplicaciones al sector financiero, según los intereses de los participantes, el acceso a la información puede estar restringido. De esta manera, a las ventajas de trazabilidad e inmutabilidad de las transacciones se les añade la posibilidad de que en cada momento cada uno de los participantes comparta solo aquella información que desea compartir, mediante encriptación, el uso de canales u otras tecnologías. Si bien la privacidad puede alcanzarse en un sistema o red pública, tendrá implicaciones en términos de eficiencia.

Limitaciones

Al mismo tiempo, la tecnología *DLT* presenta algunas limitaciones, en ocasiones fruto de su falta de madurez. A continuación se identifican las limitaciones propias de la tecnología, al margen de las vinculadas a las particularidades de cada caso de uso, como los

12 En junio de 2016, la red pública Ethereum sufrió un ataque con el robo de criptoactivos por valor de unos 70 millones de dólares. Los participantes en la red, tras una votación, acordaron retrotraer el fraude y devolver los fondos. Esta actuación, si bien solventó el fraude, pone en duda la inmutabilidad de las transacciones sobre tecnología *DLT.*

criptoactivos o la emisión de moneda digital soberana, que no son objeto de análisis en este artículo.

Actualmente, la escalabilidad en el número de transacciones y su velocidad de registro presentan importantes limitaciones. Esto es así, especialmente, para el caso de redes públicas basadas en *blockchain,* por tres motivos: el número de transacciones registradas en cada bloque suele estar limitado, los bloques deben procesarse de manera secuencial y el mecanismo de consenso es complejo. En consecuencia, el sistema se puede congestionar dejando un número de transacciones a la espera. Si bien mejora para redes privadas, su eficiencia en este ámbito se mantiene muy por debajo de las prestaciones que ofrecen a día de hoy otros sistemas centralizados[13].

Todavía existen dudas acerca de la verdadera robustez y resiliencia de las plataformas *DLT,* dado que la tecnología aún no está lo suficientemente probada. Por otra parte, a día de hoy, no existe un marco regulatorio apropiado que dé la suficiente cobertura legal a las anotaciones que se producen en el registro distribuido. Por ejemplo, en el ámbito de los pagos, no está establecido en qué momento una transacción es firme. En el futuro, las soluciones basadas en la tecnología *DLT* necesitarán cumplir con el marco regulatorio, que variará según al área de cada aplicación. Esto supondrá un reto por su naturaleza distribuida y porque probablemente operará de manera transfronteriza para optimizar su potencial.

En el ámbito de la ciberseguridad, hay que empezar señalando que la naturaleza distribuida de la tecnología hace que no existan puntos únicos de compromiso y mejore la resiliencia, así como que el uso de la criptografía incrementa la seguridad. Pero existen otros riesgos, como la pérdida de la clave privada, que podría facilitar a los atacantes copias completas de la base de datos, así como la posibilidad de que la concentración de los procesos de validación en la red *(i. e.,* «ataques del 51 %») pudieran permitir fraudes mediante doble gasto o incluso revertir transacciones.

Otra debilidad del estado actual de esta tecnología radica en la falta de interoperabilidad de los registros *DLT,* tanto entre sí (por la falta de estandarización) como con las infraestructuras tradicionales. Lograr esta interoperabilidad supondrá costes que tendría que soportar la industria de manera coordinada.

Los sistemas de gobernanza no siempre resultan suficientemente eficientes, transparentes y responsables. Los modelos varían de una plataforma a otra, desde un sistema completamente descentralizado donde es necesario alcanzar el consenso para llevar a cabo cualquier cambio en los protocolos o funciones del sistema, tradicionalmente utilizados en las redes públicas, hasta redes privadas con estructuras más centralizadas. El sistema de gobernanza elegido será crítico para garantizar una gestión adecuada de los riesgos y, en definitiva, para mantener la estabilidad y la seguridad del sistema.

Finalmente, hay que incluir en esta lista el elevado coste medioambiental derivado del uso de los denominados *Proof of work* (en redes públicas), que conlleva elevados consumos de poder de computación y un importante coste energético, si bien existen

13 A título de ejemplo, el número de transacciones máximas por segundo que permite Bitcoin son 7, la red pública de Ethereum permite hasta 23 y Quorum (protocolo desarrollado a partir del código de Ethereum, pero de carácter privado) presume de poder alcanzar cientos de transacciones por segundo. El número de transacciones por segundo que admiten los esquemas de tarjetas de pago se sitúa en el entorno de las 50.000.

otros algoritmos de consenso, principalmente en redes privadas, que no tienen esta limitación[14].

Retos para las autoridades

La tecnología *DLT* engloba distintos diseños sobre los que en la actualidad se está experimentando. Cada diseño cuenta con su propia arquitectura, pudiéndose identificar cuestiones inherentes a la tecnología con carácter general y otras particularidades de cada una de las plataformas. Además de las diferencias entre redes públicas y privadas, uno de los aspectos que más varían entre redes es el trato de la privacidad de las transacciones, que prácticamente se aborda de manera diferente en cada uno de los proyectos. Todos estos aspectos por definir plantean nuevos retos para las autoridades.

La arquitectura de los sistemas *DLT* puede llevar a la desintermediación de determinadas funciones en algunas entidades, lo que podría alterar la competencia en los mercados financieros, dejando fuera a algunos de los actores tradicionales pero, al mismo tiempo, permitiendo la entrada de nuevos participantes que actualmente no se encuentran cubiertos por el marco regulatorio. Ante este potencial nuevo escenario, sería necesario proceder a una nueva definición de responsabilidades de las infraestructuras y de los actores en la prestación de servicios financieros.

Garantizar la seguridad y la integridad de las transacciones, en un sentido amplio, es fundamental para la estabilidad del sistema financiero. En este sentido, no existe en la actualidad un marco supervisor ni de vigilancia que permita el control de los sistemas basados en *DLT* por las autoridades del modo que sí existe para las infraestructuras críticas. Al mismo tiempo, se da la circunstancia de que el diseño y el mantenimiento de las plataformas no corresponden, por lo general, a la entidad que las utiliza, por lo que existe el riesgo de perder el control sobre la infraestructura. En este sentido, resulta difícil prever posibles incidentes ante la inmadurez de la tecnología y anticipar actuaciones en caso de incidentes.

Adicionalmente, desde la perspectiva del banco central preocupan además otros aspectos, como la protección al usuario de servicios bancarios, el blanqueo de capitales y la financiación del terrorismo, la seguridad y la eficiencia de los sistemas de pago, la integridad del sistema financiero y el ejercicio de la supervisión y la vigilancia. Ante el carácter transversal de la tecnología, cuya importancia trasciende los servicios financieros y que podría encontrar aplicación en otros sectores de la economía y de la sociedad, la Comisión Europea ha tomado medidas para poner en marcha la creación del Observatorio y Foro de la cadena de bloques de la UE, dentro de las medidas presentadas dentro del «Plan de acción en materia de tecnología financiera: por un sector financiero europeo más competitivo e innovador». Entre otras medidas, tratará de desarrollar la gobernanza y los estándares para la tecnología, habiendo entrado en funcionamiento en febrero de 2018, por un período de dos años.

En el ámbito del Eurosistema se ha creado una red de expertos de bancos centrales, en la que participa Banco de España. Su objetivo es compartir conocimientos e información,

14 Si bien no contamos en la actualidad con datos fiables sobre el consumo de electricidad en redes que utilizan este tipo de algoritmos de consenso, como Bitcoin, sí que podemos afirmar que los denominados «mineros» afrontan una estructura de costes muy flexible.
Frente a unos costes fijos principalmente de *hardware* poco significativos, los costes flexibles de mantenimiento de equipos (principalmente, de refrigeración), y más concretamente el consumo de energía eléctrica, son los más elevados, pudiendo desincentivar esta actividad, y el motivo por el que la mayoría de nodos se encuentran situados en países donde el consumo de energía eléctrica es comparativamente barato. La estimación del consumo de energía de la red resulta tremendamente complejo sin contar con la colaboración de los mineros, dado que depende de variables como el tipo de equipos utilizados.

así como lograr un mejor entendimiento de las oportunidades y retos que plantea el uso de la tecnología *DLT,* centrándose en particular en el ámbito de los pagos y de las infraestructuras del mercado.

Conclusiones

La tecnología *DLT* surge como una combinación de varias innovaciones previas y se ha popularizado partir de la aparición de Bitcoin. No obstante, es importante señalar que Bitcoin es solo una aplicación singular de esta tecnología, cuyo alcance potencial es mucho mayor.

Por sus características intrínsecas, los ámbitos en los que las posibilidades de éxito de esta tecnología parecen más elevadas son los que reúnen los siguientes rasgos: se trabaja (o puede resultar eficiente trabajar) sobre registros compartidos por múltiples participantes, donde varios de ellos pueden modificar dicho registro pero existe un cierto grado de desconfianza o intereses contrapuestos entre ellos.

A día de hoy, la tecnología se encuentra en un estado todavía incipiente para su implementación efectiva en procesos productivos relacionados con la prestación de servicios financieros, lo que recomienda (y augura) una mayor experimentación por parte del sector. En paralelo, las características de los sistemas basados en *DLT,* su potencial y sus posibles implicaciones para el sistema financiero hacen conveniente que las autoridades lleven a cabo un seguimiento continuo de los desarrollos que se vayan produciendo en el mercado.

16.10.2018.

BIBLIOGRAFÍA

BANK FOR INTERNATIONAL SETTLEMENTS (20107). *Distributed ledger technology in payment, clearing and settlement.*

CITI GLOBAL PERSPECTIVES & SOLUTIONS (2018). *Bank of the future: The ABCs of Digital Disruption in Finance.*

FINANCIAL INDUSTRY REGULATORY AUTHORITY (2017). *Report on Distributed Ledger Technology.*

HILEMAN, G., y M. RAUCHS (2017). *Global Blockchain Benchmarking Study,* Cambridge Centre for Alternative Finance.

MILLS, D., K. WANG, B. MALONE, A. RAVI, J. MARQUARDT, C. CHEN, A. BADEV, T. BREZINSKI, L. FAHY, K. LIAO, V. KARGENIAN, M. ELLITHORPE, W. NG y M. BAIRD (2017). «Distributed ledger technology in payments, clearing and settlement», *Journal of Financial Market Infrastructures,* 6(2/3), pp. 207-249.

NAKAMOTO, S. (2008). «Bitcoin: A Peer-to-Peer Electronic Cash System».

WORLD BANK GROUP (2017). *Distributed Ledger Technology (DLT) and Blockchain.*

WORLD ECONOMIC FORUM (2018). *Blockchain Beyond the Hype. A Practical Framework for Business Leaders.*

WÜST, K., y A. GERVAIS (2017). *Do you need a Blockchain?,* Department of Computer Science, ETH Zürich, Suiza.