Capítulo 10 BLOCKCHAIN

10 BLOCKCHAIN

Nuevo paradigma en seguridad de datos

JULIO MIRAVALLS

En 2008, Satoshi Nakamoto anunciaba la creación de una moneda digital, el Bitcoin. Esta nueva moneda no precisaba de las instituciones bancarias ni de los bancos centrales de ningún país, y permitía que las personas pudieran transferirse dinero unos a otros basándose únicamente en las claves criptográficas. La supuesta honestidad del mundo bancario se sustituía por la de toda una red verificadora, que seguiría unas reglas muy concretas.

Las implicaciones políticas, económicas y sociales del nuevo concepto, seguidas del carrusel de subidas, bajadas y especulaciones sobre el valor de una moneda global, no controlada por autoridad alguna y, por tanto, prácticamente anarquista, desviaron la atención del valor real de la tecnología subyacente, sobre la que se sustenta. La cadena de bloques. Un registro que contiene todas las transacciones efectuadas y que cualquier usuario de la red puede verificar, lo que se llamó una blockchain.

La tecnología que está detrás del Bitcoin, y varios centenares de criptomonedas diferentes, al ser aplicada al dinero, trata de resolver el problema de la confianza. Las divisas tradicionales se basan en la posesión de oro de los gobiernos, mientras que el bitcoin descansa su confianza en la resolución de problemas computacionales complejos. Además, tal y como ocurre con el dinero metálico, un Bitcoin no se puede usar simultáneamente en dos transacciones diferentes.

Cuando un *minero* observa una transacción, la incorpora a un bloque de datos, y si resuelve el desafío correspondiente (esencialmente, un *elliptic curve digital signature algorithm*, ECDSA), lo enlaza con bloques previos.

Eso es blockchain, archivos que tienen alguna información de otros archivos a los que van enlazados. Una tecnología con dos ingredientes esenciales: los bloques de información y la red de ordenadores, en cada uno de los cuales está toda la información. Esta no está repartida.

La tecnología blockchain se está extendiendo a otros campos en los que los conceptos de seguridad e identidad verificada tienen amplia trascendencia: certificación de documentos, acreditación de origen y trayectoria de productos (incluidos alimentos), compartición de recursos, o derechos de propiedad... Las posibles aplicaciones abren un inmenso abanico.

Tal como fue concebido, el bitcoin sólo puede alcanzar la cifra finita de 21 millones, lo que lo convierte en algo dudosamente útil si no está apreciado en relación con otros valores o divisas, ya sea el dólar, el patrón oro o el barril de petróleo. De hecho, aunque en determinados casos se pueda operar con criptomonedas, para comprar y vender bienes, o para turbias operaciones delictivas, el valor siempre se establece con referencia al cambio con una moneda *real*. Y lo mismo ocurre con las otras criptomonedas, aunque puedan estar mejor diseñadas, sin límites o con márgenes muchísimo más amplios.

Dejando a un lado esas veleidades monetaristas, la tecnología blockchain es un nuevo paradigma de acreditación de identidad de objetos, que no puede ser alterada de manera unilateral por un solo agente. Cualquier operación necesita la convalidación de la cadena. En un mundo orientado hacia lo digital, con la entrada en servicio de millones de objetos inteligentes que generan datos (IoT), control de productos que se mueven por todo el planeta y nuevos sistemas de gestión de actos financieros (productos fintech), digitalización de la sanidad e incluso difusión de información, la tecnología de cadena de bloques puede aportar la capacidad de identificación única e inalterable de un elemento de valor.

EL PAPEL DE ESPAÑA

La tecnología blockchain está siendo mejorada a velocidad acelerada, tratando de acomodarla a las necesidades del negocio. Supondrá seguramente una revolución en la economía mundial, provocando cambios en muchos casos imprevisibles.

Es tecnología digital. No se basa en disponer de sistemas sofisticados de producción de bienes físicos, materias primas o una cadena de suministros, ni en poseer equipos informáticos extraordinariamente potentes, sino, fundamentalmente, en las matemáticas que se usan *(backed by math)*. En la capacidad de imaginar posibles aplicaciones y un conocimiento sólido para desarrollar la programación adecuada a tales fines. Es un entorno en el que el punto de partida no concede ventajas particulares a ningún país, ni a ningún grupo de trabajo, más allá de la capacidad para contratar talento y gente ya experimentada en este terreno.

Cualquier persona o grupo de trabajo puede identificar un objetivo de posible aplicación, lanzar su proyecto y desarrollarlo, aprovechando las ventajas de un ecosistema global de computación, almacenamiento y herramientas en la nube (IA incluida) sin necesidad de un invertir un gran capital.

Blockchain es, por tanto, una oportunidad para países que gocen de un buen sistema educativo e investigador. Una inversión en talento que desarrolle las técnicas criptográficas, basadas en la teoría de números, la geometría algebraica (curvas elípticas) y los procesos aleatorios llevaría a España a las fronteras de esta tecnología. •

CON DATOS EN LA MANO

#10 Blockchain

ANDRÉS VALDÉS

Nuestro mundo se basa en el intercambio seguro de bienes, servicios e información que atraviesa complejas estructuras con multitud de nodos en su viaje hasta llegar al destinatario. Las transferencias se producen en las condiciones acordadas, en un entorno donde los actores no tienen *a priori* motivos para confiar en los demás. Todo esto hace que el intermediario sea el actor más relevante y mejor informado en cada sector. En finanzas, logística, administración pública y otras actividades de intercambio; los peajes, tiempos de espera e incluso la posición dominante del supervisor han sido interpretados por los participantes como condiciones obligatorias para trabajar con garantías. Aceptar el papel y el precio del operador central es clave para mantener el sistema activo y confiable.

La irrupción de las tecnologías de registro distribuido (DLT en sus siglas en inglés), también denominadas blockchain por la popularidad de la cadena de bloques que hace funcionar la criptpomoneda Bitcoin, desafía, virtualmente, el papel de los intermediarios. En esencia, una blockchain garantiza el intercambio de códigos únicos de criptografía –una criptomoneda, en este caso- mediante un sistema de contabilidad que recompensa a los propios usuarios por registrar los movimientos y verificar que la base de datos no es manipulada. Pocos años después de nacer en un foro de criptografía como una alternativa experimental al dinero[1], Bitcoin era una divisa cuya unidad ya se cambiaba a unos 10.000 dólares[2] y con la que se podían comprar todo tipo de bienes físicos. Sin embargo, las criptomonedas se revelan como los árboles que ocultan el bosque: la verdadera disrupción no es el dinero virtual sino el sistema de registro que la hace posible.

La propia OCDE considera que intermediarios como entidades financieras, industrias de transformación e incluso administraciones pueden gobernar los mercados, aplicar tarifas excesivas y ralentizar la actividad económica y todo ello sin ser necesariamente confiables[3]. Desde la aparición de los registros distribuidos, muchos agentes económicos se preguntan para qué necesitan un fedatario si la propia transacción es un protocolo que ofrece suficientes garantías de cumplimiento para todas las partes.

Según el Banco Mundial, una tecnología de registro distribuido tiene dos componentes imprescindibles: la capacidad de almacenar, registrar e intercambiar información digital entre varios usuarios sin intermediación central y un sistema para garantizar que no se produce ningún doble gasto, de forma que los recursos (criptomonedas u otros archivos encriptados) no se envían a varios participantes a la vez[4]. A partir de esta definición, y dadas las dificultades para consolidarse como alternativa financiera que han mostrado las criptomonedas, las blockchain han ingresado en los departamentos de I+D como una tecnología versátil que ofrece seguridad, velocidad y ahorro de costes. Las aplicaciones más directas de esta tecnología están en finanzas, logística, identidad digital y gobernanza. (Fig. 1)

Las entidades financieras, en especial los bancos, son los negocios más afectados por el desarrollo de las tecnologías de registro distribuido. Si bien su papel puede perder relevancia si se produce un cambio de paradigma financiero, hoy por hoy las alternativas carecen de recursos y alcance necesario para amenazar a las entidades tradicionales. En cambio, esta tecnología ofrece oportunidades que el sector ha abrazado de forma temprana. Se estima que la introducción de blockchains sólo en la gestión de activo y pasivo y

1 *Bitcoin*. Wikipedia, 2020

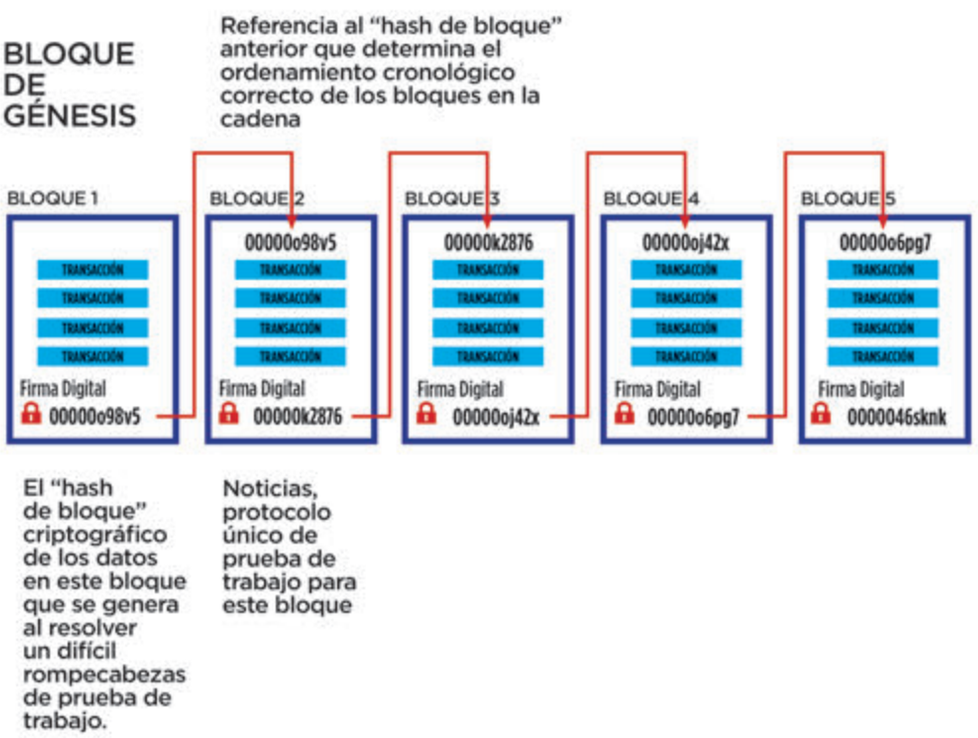
2 *Bitcoin's Price History.* Investopedia, 2019

3 *Blockchain Primer.* OCDE, 2018

4 *Distributed Ledger Technology (DLT) and Blockchain.* Banco Mundial, 2017

Fig. 1 **REGISTRO DE DATOS CON CRIPTOGRAFÍA EN UNA BLOCKCHAIN**

La escritura de transacciones requiere resolver una clave. El agente que la desbloquea añade los nuevos datos al bloque, que incluye una refrencia al anterior para mantener el orden cronológico de la cadena.



Fuente: Banco Mundial, 2017

compliance podría reducir los costes de sus departamentos en más de un 70%[5].

En Europa, algunos gobiernos ya han comenzado a usar blockchain para ofrecer un mejor servicio a los ciudadanos. Algunos ejemplos de estas iniciativas incluyen un sistema de votación local en Suiza, un registro de propiedad inmobiliaria en Suecia, el ensayo de una base de datos de historiales médicos distribuida en Estonia o un archivo de expedientes académicos vía blockchain en Chipre[6].

El sector logístico es uno de los que más pueden beneficiarse de la prometedora subtecnología blockchain de contratos inteligentes o *smart contracts*. Los procesos de transmisión de fondos o información sujetos a condiciones que contienen los contratos pueden, al ser concebidos como unidades criptográficas inalterables naturales del registro, automatizarse para imprimir un ritmo algorítmico en la cadena de distribución y simplificar tareas complejas como supervisión de entregas, paso de aduanas o trazabilidad de productos[7].

Además, la existencia de tantos usuarios como copias de los bloques de transacciones que forman el registro y su actualización simultánea confieren a las

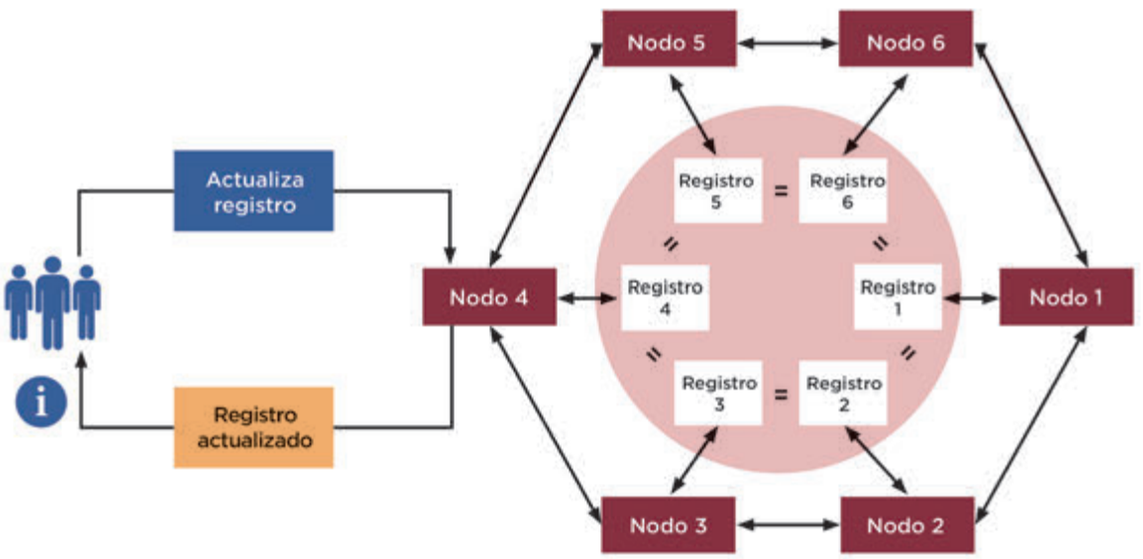
5 *Banking on Blockchain. A Value Analysis for Investment Banks.* Accenture, 2017

6 *Blockchain in Trade Finance and Supply Chain.* European Union Blockchain Observatory and Forum, 2019

7 *Blockchain for Government and Public Services.* European Union Blockchain Observatory and Forum, 2018

Fig. 2 **PROCESO DE ACTUALIZACIÓN DE UN REGISTRO DISTRIBUIDO**

El agente firma la transacción, la envía a la red a través de uno de los nodos y pide su procesamiento. Otros nodos verifican la identidad del solicitante y validan la transacción, confirmando que el peticionario tiene las credenciales necesarias para actualizar el registro. Una vez validada la operación por los nodos, se actualizan los registros de cada uno de ellos.



Fuente: Banco de España, 2018

blockchain mayores garantías de transparencia y seguridad que las bases de datos que tienen un único administrador. Cualquier intento de manipulación necesita alterar toda la red, lo que resulta inabarcable porque sería necesario invertir más recursos que los que se pretende conseguir. Especialmente si el atacante pretende vulnerar registros distribuidos de gran tamaño[8]. (Fig. 2)

Las tecnologías blockchain se desarrollan con cadencias irregulares, por lo que su penetración empresarial es todavía escasa a pesar de que los años de mayor interés se concentraron a finales de la pasada década debido a la atención generada por las criptomonedas. Con los registros distribuidos desvinculados de las divisas, los analistas estiman que las inversiones ganen concreción e intensidad progresivamente. La capitalización global de la investigación en blockchain durante 2019 fue de 3.000 millones de dólares, pero su valor añadido podría ser de 360.000 millones en 2026[9].

Por regiones y considerando el número de *start-ups* dedicadas a tecnologías blockchain, EE UU y China se reparten a partes iguales el 60% del ecosistema. La salida de Reino Unido de la Unión Europea supone la pérdida de casi la mitad de la contribución del continente, donde Alemania, Francia, Estonia y Suecia agrupan las mayores concentraciones de empresas especializadas. Otros actores globales de relevancia son Singapur, Japón y Corea del Sur. (Fig. 3)

España queda fuera de esta fotografía realizada por el Centro Común de Investigación de la UE. La adopción de esta tecnología es embrionaria y las iniciativas más visibles relacionadas con estas tecnologías quedan restringidas a la banca, a algunas comunidades autónomas y a agrupaciones empresariales. De esta forma, BBVA fue una de las primeras entidades en explorar el potencial de los registros distribuidos al sumarse al consorcio internacional R3 para desarrollo de una blockchain privada[10]. Santander, Caixabank y Bankia también han invertido en *start-ups* o investigado aplicaciones en sus departamentos de transformación digital[11].

8 *Blockchain Primer.* OCDE, 2018

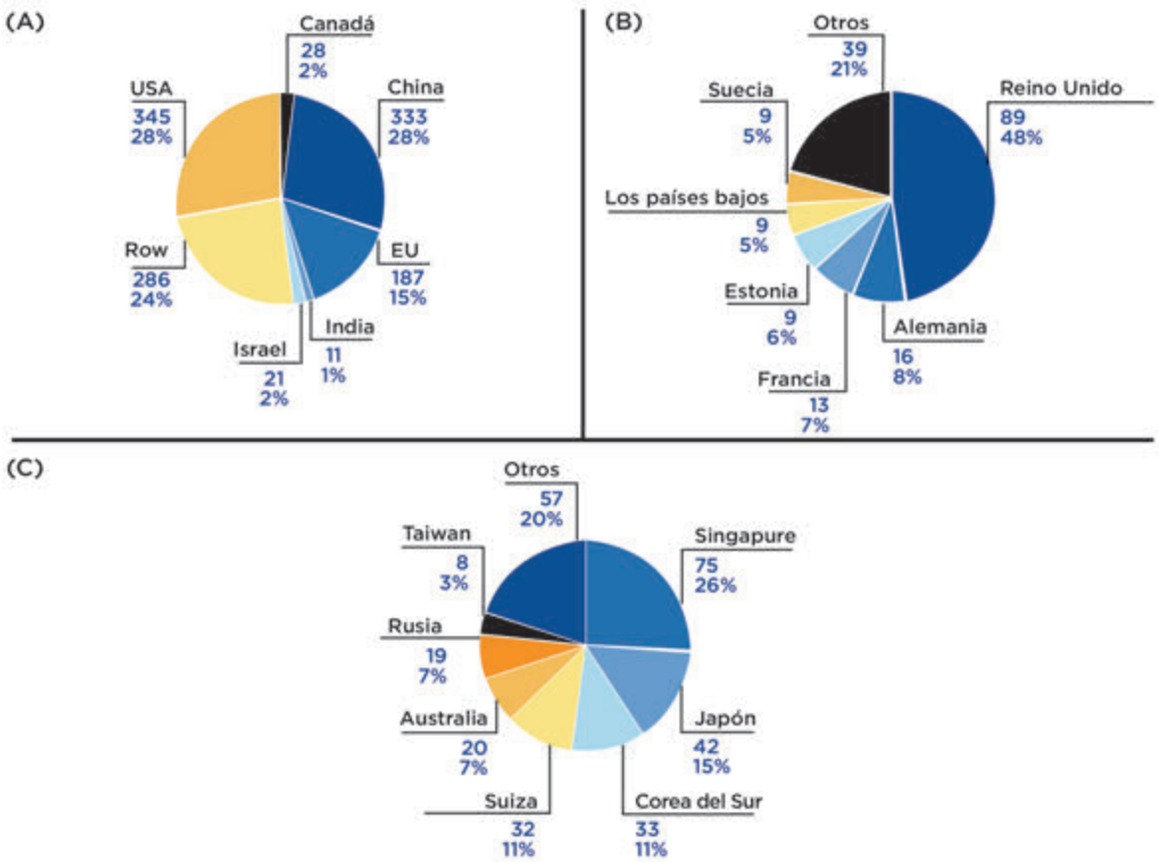
9 *Blockchain Now And Tomorrow.* Centro Común de Investigación, CE, 2019

10 *R3: La apuesta de los bancos por la tecnología Blockchain.* BBVA, 2016

11 *La banca española explora el potencial del 'blockchain'.* Expansión, 2018

Fig. 3 **START-UPS DE BLOCKCHAIN**

Distribución por empresas creadas entre 2009 y 2018 en A) actores internacionales más relevantes B) UE C) resto del mundo.



Fuente: VentureSource – Dow Jones, 2018

En los últimos años, han surgido también iniciativas privadas para impulsar el conocimiento y la adopción de estas tecnologías. Una de las de mayor crecimiento y alcance es Alastria, que suma 471 socios con mayoría de pymes y administraciones[12]. A escala territorial, Aragón y Cataluña son las comunidades con más iniciativa. El Gobierno de Aragón ha implementado registros distribuidos para tramitar licitaciones públicas mientras que la Generalitat catalana ha presentado recientemente su Estrategia Blockchain a fin de facilitar el desarrollo público y privado de estas soluciones[13].

Como se observa en el gráfico, los registros distribuidos sólo presentan un desarrollo maduro en el sector de la minería e intercambio de criptodivisas, pero su aplicación a cadenas de distribución y operaciones financieras está cerca de ser necesaria para el mercado. (Fig. 4)

Según CB Insights, los proyectos de blockchain públicas relacionados con identidad digital, organizaciones descentralizadas o mercado de datos se encuentran en una fase muy experimental. Cabe esperar por tanto que durante los próximos años el sector continúe copado por las criptomonedas y el sector privado.

Los registros distribuidos plantean desafíos más allá de la competencia e incluso la relevancia empresarial. Son sistemas robustos pero no infalibles y han revelado brechas de seguridad, especialmente en la operación mediante firma y sello personal de los usuarios. Además, la dificultad de ganar la masa crítica necesaria para ser viables compromete su desarrollo más allá del ámbito privado. Por otra parte, la percepción de esta tecnología como una amenaza al orden económico-financiero tradicional puede generar legisla-

12 *Memoria de actividades. Junio 2018 – Junio 2019.* Alastria, 2019

13 *Tecnología 'blockchain': un nuevo concepto a dominar.* Harvard Deusto, 2019

ciones restrictivas que desincentiven la participación, como ya ha ocurrido en algunos países asiáticos[14].

Un problema adicional, y que suele pasar desapercibido, es el impacto medioambiental que generan las blockchain. La energía necesaria para almacenar y añadir nuevos bloques a los registros demandan cantidades ingentes de electricidad. Sólo la minería que desencripta cada nuevo bloque en Blockchain, el registro distribuido de Bitcoin, consume una proporción de energía similar a la de Dinamarca[15]. Tampoco se han resuelto aspectos técnicos como la sobrecarga de los sistemas más grandes en número de participantes, por lo que su estabilidad no está del todo garantizada[16].

Los registros distribuidos tienen muchas etapas que consolidar antes de convertirse en un elemento fundamental de la nueva revolución industrial en ciernes. No obstante, el interés que generan en el sector público y privado y la complementariedad que presentan con otras tecnologías primordiales de esta transformación como la Inteligencia Artificial o el Internet de las Cosas prometen compensar las dificultades y hacerla imprescindible en los años venideros. •

14 *Blockchain. Investment Insight.* Morgan Stanley, 2018

15 idem

16 *Blockchain Now And Tomorrow.* Centro Común de Investigación, CE, 2019

Fig. 4 **TENDENCIAS EMERGENTES EN TECNOLOGÍAS BLOCKCHAIN. GRADO DE MADUREZ DE APLICACIONES DE REGISTRO DISTRIBUIDO**

Fuente: CB Insights, 2019