ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

70/2018 12 de junio de 2018

*Ricardo Palomo-Zurdo**

«Blockchain»: la descentralización del poder y su aplicación en la defensa

«Blockchain»: la descentralización del poder y su aplicación en la defensa

Resumen

La tecnología *blockchain* promete ser la mayor revolución tecnológica global después de la aparición de Internet. Su singularidad radica en el concepto de descentralización y en la distribución entre los nodos de la red de las transacciones realizadas, desapareciendo el concepto de centralidad. Pero también, se caracteriza por su ingenioso sistema de encriptación, por la inmutabilidad de los registros y por sus virtudes de trazabilidad, lo que ha captado la atención en el ámbito militar, en particular en relación con el control de cadenas de suministros en el sector de la defensa, en materia de ciberseguridad en las comunicaciones y, también, en otros ámbitos aún en fase de experimentación, como la activación de sistemas de armamento.

Palabras clave

Blockchain, DLT, *smartcontract*, nodo, *token*, trazabilidad, ciberseguridad, descentralización, Internet del Valor, Alastria.

Blockchain: decentralization of power and its application in defense

Abstract

The blockchain technology promises to be the biggest global technological revolution after the appearance of the Internet. Its uniqueness lies in the concept of decentralization and in the distribution between the nodes of the network of transactions carried out, disappearing the concept of centralization. But also, it is characterized by its ingenious encryption system, by the immutability of the registers and by its traceability virtues, which has attracted attention in the military field, particularly in relation to the control of supply chains in the sector of defense, in terms of cybersecurity in communications and, also, in other areas still in the experimentation phase, such as the activation of weapons systems.

Keywords

Blockchain, DLT, smartcontract, node, token, traceability, cybersecurity, decentralization, Internet of Value, Alastria.

¿Qué es *blockchain*?

Esta es la pregunta habitual cuando se escucha por primera vez este enigmático anglicismo, pues aún no han transcurrido más de dos años desde que comenzara a popularizarse en determinados ámbitos empresariales, difundiéndose, de forma exponencial, hacia una creciente diversidad de entornos sociales, económicos e institucionales.

Blockchain (traducible como «cadena de bloques») es una tecnología que forma parte del ámbito de las denominadas tecnologías de registro distribuido o DLT (*Distributed Ledger Technologies*). Permite gestionar datos, órdenes, transacciones, activos y *tokens*[1], mediante un ingenioso sistema de registro distribuido —o descentralizado— que se anota en bloques de información que se encadenan secuencialmente creando una cadena de bloques o registros inmutable e inalterable, compartida colaborativamente entre todos los miembros de cada red de *blockchain*, y que son verificados por dichos miembros de la red, actuando como «nodos» de la misma. De esta forma, se crea un procedimiento de registro, que funciona mediante criptografía[2] consensual, en modo equivalente a un libro contable —en este caso digital—, del que hay tantas copias idénticas como miembros de la red.

El consenso criptográfico utilizado asegura que haya una única versión auditable e inmodificable de los datos almacenados y de cada movimiento o transacción, lo que introduce una suerte de descentralización del concepto de confianza, basada ahora en relaciones colaborativas P2P (*peer to peer*), que no requiere la existencia de una «autoridad central», como ha sido el denominador común hasta la fecha.

Al contrario que las tradicionales bases de datos centralizadas alojadas en una institución central o en sus servidores, mediante *blockchain* se puede crear una base de datos distribuida, descentralizada, compartida y replicada, que puede ser pública o privada, permisionada (accesible solo a los que son admitidos como miembros de la red, como ocurre con una *blockchain* privada o cerrada que pudiese crear, por ejemplo, un grupo empresarial, una organización gubernamental o una red de bases militares) o no permisionada (accesible libremente a cualquier usuario que desee hacerlo mediante la instalación del *software* libre apropiado).

[1] Más adelante se comenta el concepto de *token*, que puede entenderse, en este contexto, como una representación digital de un activo con valor propio.

[2] La criptografía experimentó un fuerte desarrollo durante la II GM por su vital aportación en las comunicaciones militares.

Los datos o transacciones registradas en el libro de registro o base de datos contable deben ser inmutables, auditables, gozar de protección criptográfica y estar dotados de un sistema de verificación de su veracidad; labor que realizan los denominados nodos validadores. Este procedimiento permite el registro de las distintas transacciones en una base descentralizada, facilitando el intercambio de información entre las partes en una manera eficiente, abierta y verificable[3].

Blockchain es conocido como el Internet del Valor —también el Internet de la confianza— frente al Internet de la información actual, dado que permite transferir valor o activos digitalizados entre los usuarios, frente a Internet clásico que permite solo enviar información o copias de activos. Un sencillo ejemplo puede ayudar a entender esta diferencia: actualmente se pueden enviar copias de una fotografía desde un dispositivo a todos los usuarios deseados, mientras que con *blockchain* se puede transmitir la propiedad de la fotografía a otro usuario. La misma idea funciona para infinidad de aplicaciones que actualmente se están desarrollando: transmisión de títulos de propiedad, de activos financieros, etc.

Un elemento esencial de *blockchain* es que permite que usuarios que no confían plenamente unos en otros pueden mantener un consenso sobre la existencia, el estado y la evolución de una serie de factores compartidos; es decir, la propia red actúa como fedatario introduciendo sistemas de confianza entre desconocidos. Desde un punto de vista técnico, este sistema basado en la confianza y el consenso se construye a partir de una red global de ordenadores que gestionan una gigantesca base de datos[4].

Actualmente hay varias redes de *blockchain* funcionando mundialmente, algo así como diversos sistemas operativos. Por ejemplo, *bitcoin*, la famosa criptomoneda, que se configura como la primera aplicación efectiva y mundialmente difundida de *blockchain*, es una de ellas. Otra de las más destacadas es Ethereum[5], que está formada por miles de nodos distribuidos por todo el mundo y que forman una plataforma sobre la que se pueden mover o desarrollar muchas aplicaciones concretas, dada su versatilidad,

---

[3] WORKIE, H. y JAIN, K., «Distributed ledger technology: implications of blockchain for the securities industry», Journal of Securities Operations & Custody, V. 9, n.º 4, 2017, pp. 437-355.

[4] PREUKSCHAT, A. (Coord.), «Blockchain: La revolución industrial de internet», Grupo Planeta, Madrid, España, 2017, pp. 23-27.

[5] En palabras de Vitalik Buterin, creador de Ethereum: *A Blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong crypto-economically secured guarantee that programs running on the chain will continue to execute in exactly the way that the Blockchain protocol specifies.*

siendo especialmente útil para el desarrollo de los llamados *Smart contracts*, contando con el protocolo ERC-20 para la creación e intercambio de *tokens*. De hecho, la variante Quorum de esta red es la que está implantando en España el Consorcio ALASTRIA, de carácter nacional, semipúblico o público requiriendo la identificación de los participantes y multisectorial en el que participan empresas de todo tipo y sector, desde pequeñas *start-up* a la mayoría de las empresas del IBEX 35, consultoras, reconocidos despachos de abogados y diversas universidades e instituciones privadas y públicas[6].

¿Cómo funciona *blockchain*?

Para explicar de forma resumida el funcionamiento de *blockchain*, en primer lugar, hay que conocer los principales elementos que la integran. Así, los principales componentes de un sistema *blockchain* son los siguientes:

- Las cadenas de bloques donde se anotan las transacciones que se realizan en la red. Los bloques están enlazados secuencialmente entre sí, mediante funciones *hash* (resúmenes criptográficos), formando una cadena. Cada bloque tiene una determinada capacidad máxima y viene a ser como una página de un libro contable, prácticamente infinito, y en el que todo lo que se ha escrito ya no puede borrarse o alterarse, lo que le confiere inmutabilidad plena[7].
- Los nodos, que son simplemente ordenadores que almacenan la copia del libro contable, es decir, almacenan la cadena de bloques. Para configurarse como nodo, el ordenador debe contar con el software correspondiente y, en caso de ser una red permisionada, con los permisos pertinentes[8].
- Las carteras digitales o *wallets*, que son meras aplicaciones o *interfaces* a través de las cuales los usuarios hacen las transacciones y gestionan su identidad digital (ID) para poder operar. Es una simple app que puede descargarse en el dispositivo del

[6] El consorcio ALASTRIA cuenta con más de 220 asociados en mayo de 2018. Puede verse detalle de sus funciones, integrantes y comisiones en www.alastria.io.

[7] PILKINGTON, M., «Blockchain Technology: Principles and Applications» en Research Handbook on Digital Transformations, editado por Olleros X., Zhegu, M., Elgar, E., 2016. SSRN: https://ssrn.com/abstract=2662660.

[8] Por ejemplo, pueden verse las instrucciones de configuración de un nodo del citado consorcio ALASTRIA —una vez que ha sido permisionado— en https://github.com/alastria/alastria-node.

usuario y mediante la cual se dispone de la clave privada y la clave pública con las que cada usuario podrá operar.

Por otro lado, también existen los llamados mineros, especialmente en las redes de criptomonedas, que son ordenadores que autorizan que se vayan añadiendo bloques a la cadena y, para ello, deben resolver un problema matemático siguiendo un protocolo de consenso. Por ese esfuerzo (que supone tener gran capacidad de computación y utilizar mucha energía) reciben recompensas en moneda digital que proceden tanto de nuevas monedas, que se crean al minar la transacción, como de las comisiones que abonan aquellos que ordenan las transacciones. En las criptomonedas la minería puede utilizar principalmente sistemas de prueba de trabajo (*Proof of Work o PoW*) o de prueba de participación (*Proof of Stake*)[9].

El funcionamiento de una transacción común en *blockchain* comienza con el envío de un activo digital desde una cartera digital o *wallet* a otra cartera de otro usuario. Esta transacción debe ser visada por diversos nodos y agrupada con otras transacciones para, seguidamente, ser tomada por los mineros como un trabajo que tienen que resolver a cambio de una recompensa. Los mineros eligen un conjunto de transacciones que puede ser distinto para cada grupo de mineros; y compiten entre sí por conseguir lo que se denomina un valor (*nonce*) que resuelve el acertijo o reto matemático que autoriza al minero que lo resuelve (lógicamente de forma mecanizada mediante su capacidad computacional) a proponer su bloque con las transacciones que dicho bloque contiene, para ser agregado a la cadena de bloques. Este bloque propuesto incluye también la identificación y *hash* del bloque anterior estableciéndose así la linealidad de la cadena.

Todas las cadenas de bloques están distribuidas, es decir, se ejecutan en ordenadores que ofrecen voluntariamente personas de todo el mundo; por lo que no hay una base de datos central que pueda atacarse. Un potencial atacante debería tener al menos el 51% de la red para intentar conseguir su objetivo. Por ejemplo, en la *blockchain* de *bitcoin*, cada diez minutos, todas las transacciones realizadas se comprueban, ordenan y almacenan en un bloque que se une al bloque anterior, creándose así una cadena. Si se quiere robar un *bitcoin* hay que reescribir toda la cadena de bloques a la vista de todos, lo que es prácticamente imposible.

[9] Hay incluso minería en la nube (*Cloud Minning*) pues los usuarios pueden alquilar capacidad de minado durante un tiempo sin tener equipos propios.

El sistema de encriptación es esencial en *blockchain*. En 1976, Whitfield Diffie y Martin Hellman crearon el algoritmo que lleva su nombre, con el que proponían romper las claves encriptadas en dos claves, de modo que hubiese una pública y otra privada. Con la pública se puede encriptar un mensaje, pero para desencriptarlo es necesaria la clave privada. Estos autores, junto con Ralf Merkle, creador de los Árboles de Merkle, y Ron Rivest, Adi Shamir y Leonard Adleman, creadores del algoritmo RSA que permite el cifrado y descifrado de mensajes[10], constituyen el grupo de los creadores de la criptografía de clave pública.

Para realizar modificaciones fraudulentas sobre las operaciones se requeriría lanzar un ataque informático simultáneo a las diversas bases de datos. Si por ejemplo se intentara modificar el contenido dentro de uno de los bloques, el resto de los dispositivos de la red responderían al instante, corroborando que el dato alterado no coincide con el resto y revirtiéndolo al original. De este modo, se mantiene un registro saneado sobre las operaciones en redes de criptomonedas y evitar problemas como el doble gasto[11] u otras acciones que resulten malintencionadas.

¿Cómo se aplica la tecnología *blockchain*?

Dado que cada nodo de la red almacena una copia de la cadena de bloques, que no hay intermediarios ni jerarquía entre ellos; todos son iguales y ninguno es el dueño exclusivo de la cadena ni tiene ascendencia jerárquica sobre el resto. Todos pueden ver qué hay en la cadena y cualquier intento de alteración es inmediatamente descubierto, por lo que el diseño resultante es inalterable y transparente.

Esta característica de sistema distribuido, frente a los modelos habituales de sistemas centralizados, es lo que puede cambiar muchos modelos de negocio en el ámbito económico[12], pero también muchos modelos de gestión y de organización institucional; por lo que va a resultar especialmente trascendente durante los próximos años. De algún modo, esto podría parecer una amenaza al perder el Estado posibles parcelas de control o no poder acceder a la información que discurre en estas redes.

[10] Para probar la fuerza de su código, publicaron una prueba para los lectores de una revista que consistía en descifrar un mensaje a cambio de 100 dólares. Nadie lo consiguió hasta mediados de los años 90, cuando a Derek Atkins, Michael Graff, Arjen k. Lenstra y Paul C. Leyland se les ocurrió utilizar la capacidad computacional de ordenadores de personas diferentes, alrededor del mundo, para resolver el problema.

[11] Consistente en la utilización de una misma unidad de moneda digital dos veces.

[12] LERIDA, J. y MORA, J.J., «La economía de *blockchain*: los negocios de la nueva web», Kolokium, 2016.

Por primera vez en la historia, el desarrollo de la tecnología permite la participación global de usuarios privados e institucionales de todo el mundo sobre un mismo tablero de juego. Además, el sistema criptográfico de doble cable, público y privado, con el que opera *blockchain* aporta una seguridad a las transacciones de la que carece el actual modelo convencional de Internet. De algún modo, *blockchain* surge como una solución a los graves problemas de la vulnerabilidad de Internet, con posibilidad de aplicación frente a los problemas de ciberseguridad, y como un medio de transferir órdenes y transacciones de modo indescifrable por terceros ajenos. No en vano, las primeras aplicaciones reales de esta tecnología se han realizado en el ámbito financiero, como es el caso de las criptomonedas[13] y también en transferencias bancarias con dinero fiduciario, pero igualmente se puede aplicar en el ámbito de las comunicaciones militares como se trata posteriormente.

La distribución frente a la centralización puede alterar considerablemente los arraigados sistemas tradicionales centralizados a los que estamos acostumbrados (registro de propiedad, registro civil, expedientes médicos, titulaciones académicas, etc.). Es una tecnología que va más allá de lo que actualmente se considera una revolución socio-digital, como es el caso, por ejemplo, de las conocidas plataformas Uber, Airbnb, Amazon, las agencias de viajes *on line* y los populares portales de compraventa o de intercambio de productos o servicios, pues estos son simplemente modelos que se fundamentan en la sustitución de la cadena de intermediación, por una única intermediación centralizada entre oferentes y demandantes y en la recopilación de datos de sus usuarios. *Blockchain* implica desintermediación real, y por ello, estos pujantes negocios de la era digital pueden verse obligados a cambiar en los próximos años al ser posible un contacto más directo entre usuarios de una red de *blockchain*. En ello jugarán un papel destacado los denominados *smart contracts*.

Los *smart contracts*, traducibles como contratos inteligentes, no gozan de tal inteligencia, sino que se crean mediante líneas de código que configuran programas informáticos que incorporan instrucciones para ejecutar las cláusulas preestablecidas en los mismos de forma automática y programada siempre y cuando se cumplan las condiciones establecidas en el mismo. Por ejemplo, un *smart contract* puede activar un

[13] La primera aplicación real de la tecnología *blockchain* se realizó con la conocida criptomoneda bitcoin, originada con la publicación, en el año 2008, del ya famoso documento firmado por Satoshi Nakamoto (pseudónimo de una identidad real aún desconocida) titulado «*Bitcoin: A Peer-to-Peer Electronic Cash System*» que puede verse en: https://bitcoin.org/bitcoin.pdf.

determinado armamento o un sistema de defensa o seguridad cuando se cumplen los escenarios de amenaza que han sido programados o las autorizaciones pertinentes, sin que requiera autorización humana o la existencia de una entidad centralizada que active tales sistemas.

Las posibilidades de aplicación de *blockchain* y de instrumentos como los *smart contracts* y la *tokenización* de activos, permiten vislumbrar infinidad de aplicaciones que tomarán forma durante los próximos años[14].

Actualmente, la tecnología *blockchain* se está aplicando, ensayando o visionando en los siguientes ámbitos:

Criptomonedas y sistemas de pago, el ámbito pionero de desarrollo de *blockchain*, al encontrar la solución para transferir valor sin que una unidad digital se pueda gastar dos veces, dado que se registra cada transacción una única vez y de forma inalterable, por lo que cada unidad monetaria digital se transfiere entre usuarios con la única intermediación de los llamados *exchanges* u otros especialistas en criptomonedas (mediante *apps* y *wallets*) sin necesidad de intermediarios financieros o de sistemas de compensación y liquidación de operaciones, de forma ágil y prácticamente inmediata, condenando al olvido la conocida expresión de «fecha valor» de las transferencias bancarias tradicionales.

Mercados de valores, como por ejemplo el sistema *blockchain* que utiliza el NASDAQ que es el índice de bolsa de las empresas tecnológicas de EE. UU. En cierto modo, los actuales sistemas centralizados de las bolsas de valores podrán ser replanteados en su concepción y funcionamiento.

Gestión de identidades, siendo este uno de los campos más atractivos en el momento actual, dado que las ID de *blockchain* pronto reemplazarán a los clásicos usuarios y contraseñas y a la firma digital. Cada usuario almacenará los datos que considere dentro de su identidad digital y abrirá solo aquella parcela de datos que desee a un tercero, por ejemplo, a una compañía de suministro de energía, que únicamente podrá acceder a los datos que precise o que pueda solicitar según la regulación legal. A este respecto, se podrán garantizar los sistemas de voto electrónico, pues con *blockchain* cada persona solo podrá votar una vez, lo que podría reforzar los sistemas democráticos y participativos con un gran ahorro de costes.

[14] HILEMAN, G. y RAUCHS, M., «Global Blockchain Benchmarking Study», 2017. En SSRN: http://dx.doi.org/10.2139/ssrn.3040224.

Sistemas de seguridad y de autorizaciones, pues se pueden crear contratos inteligentes que funcionen como cerraduras o permisos inteligentes que solo confieran acceso o disponibilidad a los usuarios autorizados.

Aplicaciones militares y de inteligencia, pues pueden establecerse sistemas de mensajerías seguros e indescifrables, o programar el bloqueo o desbloqueo automático de sistemas de armamento sin depender de un operador central que podría ser vulnerable a un ataque cibernético o a la destrucción física. También se pueden elaborar *smart contracts* para la ejecución de órdenes de intervención de efectivos de combate en función de escenarios preestablecidos, o la activación de sistemas de evacuación, el uso de vehículos militares, etc.

Mercados de suministros, como los de energía o materias primas. Así, por ejemplo, usuarios particulares pueden generar electricidad con energías renovables en su propio domicilio y vender sus excedentes sin intermediarios.

Explotación de propiedad intelectual, dado que, por ejemplo, un escritor, un músico o un periodista puede conceder directamente licencias de uso de sus obras y recibir la contraprestación sin intermediarios.

Contratos de prestación de servicios e intercambios de la economía colaborativa, por ejemplo, para viviendas o para coches compartidos. Por ejemplo, un vehículo alquilado en *renting* no autorizaría su propia apertura o movilidad si el usuario no estuviese al corriente de pago de las cuotas. Esto, unido a los sistemas de geolocalización y de conducción autónoma revolucionará los sistemas de movilidad. De hecho, si el vehículo fuese autoconducible, él mismo regresaría autónomamente a su empresa o base si el cliente no ha cumplido sus obligaciones contractuales.

Registros y servicios de notaría, pues gracias a que *blockchain* es un gran registro distribuido (todos los nodos tienen copia) al que muchas partes pueden acceder desde cualquier lugar del mundo, resulta muy útil para registro de documentos, actas, activos, derechos de autor, registros de nacimiento, de divorcios, de defunciones, registros de propiedad, registro de vehículos, expedientes médicos, componentes de medicamentos, etc. También se pueden registrar obras de arte para evitar falsificaciones, diamantes, y hasta denominaciones de origen que gozarían así de una trazabilidad contrastable e inalterable. Una aplicación clave será en las cadenas de suministros y, en particular, en las que contengan componentes sensibles como en la industria de defensa.

Autentificación de aportaciones, tanto para recursos de financiación empresarial en forma de bonos o acciones u otros títulos o activos (como es el caso de las operaciones de ICOs —*Initial Currency Offer*—)[15], o bien, fondos para proyectos solidarios o de caridad. Así, por ejemplo, con esta tecnología se puede comprobar que los donativos llegan directamente a las personas o instituciones que tienen que recibirlas sin el peligro de su mala administración por parte de intermediarios privados o de un gobierno, pues puede introducirse *smart contracts* que invaliden el uso de los fondos si no se cumple la secuencia de condiciones garantistas exigidas para ello.

Autentificación de títulos, como es caso de los títulos académicos y las actividades de formación, pero también de la vida laboral o de los puestos ocupados. Una vez registrados en la *blockchain* por parte de la institución emisora de los títulos o certificadora de los puestos ocupados queda almacenado en la red y es inalterable e infalsificable.

Trazabilidad de mercancías y cadena de suministros: Se puede añadir una huella digital a cada mercancía para conocer cómo se transforma o qué fases de producción o del recorrido ha realizado. Así, se puede seguir el recorrido de una mercancía por todo el mundo, conocer quién la ha manipulado, etc. Muchas empresas de supermercados y del sector textil están ya trabajando en este ámbito. Con la llegada del Internet de las Cosas (IoT) se podrá conectar un *smart contract* con sensores y GPS para que así se realice un pago al proveedor en cuanto llegue la mercancía al destino, lo cual cambia radicalmente los actuales sistemas de crédito documentario que hacían residir la confianza de las transacciones en la existencia de bancos intermediarios. Este campo es uno de los de interés prioritario en el ámbito de la logística militar y aprovisionamientos y, en particular, en suministros de componentes de equipamiento militar.

Más aún, *blockchain* puede luchar contra la corrupción pues, a través de *smart contracts* se puede establecer la máxima desviación de un presupuesto o actuación, las fechas de pago, las cláusulas de resolución o de indemnización y todo ello quedaría registrado.

Como puede verse, pueden ser innumerables las aplicaciones de *blockchain* en el ámbito social, político e institucional. En el ámbito económico se ha llegado a originar el

[15] SEBASTIÁN, J., «El asombroso fenómeno de las ICOs», BBVA Rs, Editorial Deusto, Nueva York, 2017.

concepto de «*tokenización* de la economía» o *tokenomics*, especialmente trascendente desde el punto de vista de la capacidad de *blockchain* para transmitir valor y activos digitales. Concretamente, a partir del año 2016, comenzó la popularización de la palabra *token*, traducible o entendible como «ficha, vale o resguardo» en español, también asimilable a «pieza» o «unidad». Por ejemplo, una ficha o un «vale» o cupón para utilizar en una máquina, como una de lavado de automóviles, serían un *token* «físico»; mientras que un *token* digital sería un código criptográfico que permite representar un determinado importe, valor, el derecho a ese mismo lavado e incluso un activo de forma digital.

Este concepto permite hablar de la virtualización o digitalización de todo tipo de activos, e incluso de la partición de diversos *tokens* de un único activo real o físico («moléculas de *token*») o de un derecho o activo financiero digitalmente representado.

¿Qué cambios de paradigmas introduce *blockchain*?

Blockchain y el desarrollo de los *smart contracts* aportan admirables o inquietantes novedades para la sociedad, pues permite la desintermediación y la descentralización[16] y eso cambiará paradigmas muy asentados hasta ahora.

La tecnología que ha hecho posible esta forma de distribución aporta confianza (por haber tantos fedatarios como operadores de la red), seguridad y, también, transparencia; frente al notorio riesgo actual al que están sometidos los sistemas centralizados que pueden ser *hackeados*, o que pueden sufrir suplantación de identidad. La actual replicación de servidores o el almacenamiento en la nube (*cloudcomputing*) seguirán siendo vulnerables a ciberataques.

Blockchain va a cambiar el paradigma de la necesidad de elementos centralizadores, del rol de los intermediarios y de la tradicional necesidad de compilar registros en un mismo lugar físico o virtual, lo cual puede ser percibido como una amenaza, pero también, como una oportunidad.

La centralización ha sido el modelo característico de muchas interacciones humanas desde su propio origen, como lo fueron los primeros mercados de trueque y luego de compra-venta, o como lo son ahora los mercados financieros o los centros comerciales.

[16] ATZORI, M., «Blockchain Technology and Decentralized Governance: Is the State Still Necessary?», 2015. En SSRN: https://ssrn.com/abstract=2709713.II.

La novedad que ha supuesto el estreno de las tecnologías distribuidas como *blockchain*, de la mano de las criptomonedas aparecidas a partir del año 2008, está configurando un panorama disruptivo e innovador, para muchos fascinante, pero también controvertido e inquietante, dado que, en su planteamiento más trascendente, puede percibirse como el albor de un sistema alternativo o sustitutivo del tradicional.

Por lo que respecta a las criptomonedas, el hecho de que una moneda no sea emitida por un Estado soberano, que esté respaldada por una autoridad monetaria a modo de banco central y que su volumen en circulación no pueda ser controlado; resulta claramente un desafío al orden monetario establecido.

Blockchain es, sin duda alguna, una gran oportunidad de avance tecnológico con aportación de valor a la humanidad, aunque pueda verse como una amenaza en algunos contextos. La clave es la adaptación y asimilación del cambio, como ocurrió con el coche frente al caballo o con la artillería frente a las lanzas.

Ahora se puede dar por finalizada la era industrial con el asentamiento de la nueva era digital. La nueva tecnología que va a obrar el siguiente cambio es *blockchain*, unida a otras expresiones cada día más comunes, como IoT, inteligencia artificial, robotización, big data, industria 4.0, realidad virtual y aumentada, etc.

Es cierto que la revolución *blockchain* se ha gestado, con cierto aire subversivo[17] y en un clima de desconfianza de la población, durante la mayor crisis financiera internacional conocida, utilizando Internet como medio propagador del primer «alzamiento criptomonetario», *bitcoin*, para ampliarse en los próximos años a todo tipo de actividades económicas y sociales, entrando ya en una fase de legalidad y progreso ordenado con aplicaciones realistas y cooperadoras con el logro de la eficiencia. Las criptomonedas han roto paradigmas en la teoría del dinero, al tiempo que se erigen como símbolo del *empoderamiento* financiero para la parte más romántica e idealista de sus usuarios, un símbolo de democratización financiera frente a las devaluaciones unilaterales o al cerco a su movilidad (el «corralito»). Otros, menos sensibles al llamado «criptoanarquismo», simplemente aprovechan su existencia con ánimo especulativo.

La «tokenización» antes indicada permitirá globalizar el trueque digital y movilizar cualquier tipo de activo como medio de pago o de transferencia de valor o propiedad como partidas de nacimiento, títulos de propiedad, grados académicos, informes

[17] BBVA Research, «De Alan Turing al "ciberpunk": la historia de *Blockchain*»; (https://www.bbva.com/es/historia-origen-*blockchain*-bitcoin/); 2017.

financieros, procedimientos médicos, demandas de seguros, votos, origen de los alimentos y cualquier otra cosa que pueda codificarse.

Ponto habrá miles de millones de cosas inteligentes interconectadas que percibirán, responderán, se comunicarán, comprarán su propia electricidad y compartirán información importante, e incluso, protegerán el medio ambiente y cuidarán de la salud de los usuarios; y este Internet de todo necesita un registro de todo[18].

La novedad de *blockchain*, su ingenio operativo, pero también la dificultad o resistencia por asimilar el concepto de sistemas distribuidos desconcierta a los reguladores y actores institucionales, pero despierta el interés del público, como lo hizo internet en sus orígenes. La resistencia al cambio no pasaría de una maniobra táctica.

Es lógico que los sistemas institucionales y los gobiernos miren con recelo la entrada en escena de sistemas distribuidos que amenazan los tradicionales sistemas centralizados y que arañen el «oligopolio» del control de los resortes del Estado. Así en el ámbito de las criptomonedas es frecuente tildarlas como sistema de evasión fiscal y canal de operaciones ilícitas, por razón de su anonimidad; aunque procede no olvidar que hasta ahora la abultada economía sumergida y la economía delictiva han funcionado durante décadas en todo el mundo y con moneda de curso legal, preferentemente las más fuertes y reputadas: el dólar y el euro.

La tecnología *blockchain* en el contexto de la seguridad nacional: aplicaciones, riesgos y amenazas

En diciembre de 2017, Donald Trump firmó la Ley de Defensa de EE. UU. (aprobada en septiembre) en la que se incluía aplicar *blockchain* para la ciberseguridad militar, contemplando, tanto aplicaciones ofensivas como defensivas. Su aplicación se considera estratégica para aumentar la seguridad frente a ataques cibernéticos, por lo que planteaba un plazo de 6 meses para tener resultados del estudio de estos sistemas.

En un interesante documento publicado por la reconocida Fundación para la Defensa de las Democracias[19], en Washington, se recoge que un riesgo importante para la

[18] TAPSCOTT, D. y TAPSCOTT, A., «Blockchain Revolution», Penguin Publisher Group, Nueva York, 2016, pp. 27-29.

[19] HSIEM, M. y RAVICH, S., «Leveraging Blockchain Technology to Protect the National Security Industrial Base», Foundation for Defense of Democracies, 2017, http://www.defenddemocracy.org/media-hit/samantha-ravich-leveraging-*blockchain*-technology-to-protect-the-national-security-industria/.

seguridad nacional es la vulnerabilidad en las cadenas de suministro de equipamientos mediante introducción de *hardware* malicioso que, en un momento dado, pueda alterar su correcto funcionamiento.

Figura 1: Tecnología *blockchain*. Fuente: cryptoconsulting.info.

Por ello, se adivina un importante potencial de transformación de los sistemas de verificación de aprovisionamientos mediante tecnología *blockchain*, dada la capacidad de introducir sistemas de trazabilidad, estableciendo la procedencia de cada procesador, circuito o componente. De este modo, se podría registrar cada iteración de diseño de un circuito; y los fabricantes de componentes que se utilizasen en sistemas de defensa podrían registrar y compartir la veracidad de cada modelo, al tiempo que los distribuidores podrían registrar la venta de los componentes a los integradores de sistemas quienes, a su vez, podrían registrar la asignación de esos componentes a, por ejemplo, aviones de combate o misiles concretos[20].

Esto sería también muy útil cuando se trata de renovar componentes electrónicos que dejan de fabricarse, pero que se necesitan para sistemas de armamentos con vida útil de más de 25 años, dado que habría así un incentivo para la búsqueda de piezas contrastadamente originales y evitaría las restricciones que habitualmente se aplican

[20] BARNAS, N., «Blockchains in National Defense. Trustworthy Systems in a Trustless World», 2016, https://es.scribd.com/document/367972252/*Blockchain*s-in-National-Defense-Trustworthy-Systems-in-a-Trustless-World-by-Neil-b-Barnas-Major-Usaf.

cuando se trata de reemplazar componentes cuya procedencia no pueda establecerse correctamente. De esta forma se puede afrontar la debilidad actual de las instituciones responsables de defensa en la gestión de las adquisiciones de componentes a miles de proveedores globales, muchos de los cuales son de mínima dimensión y tienen sistemas de seguridad y control poco rigurosos susceptibles de sabotajes.

Cualquier cambio no programado en una cadena de suministros, en cualquier configuración, por pequeña que sea, se podría detectar instantáneamente evitando el problema actual de la incapacidad para controlar los miles o millones de componentes, uno a uno, que pueden integrar, por ejemplo, un sistema de armamento sofisticado.

El Departamento de Defensa estadounidense planteó la necesidad crítica de contar con un sistema de mensajes y transacciones seguro, accesible a través de un navegador web o una aplicación nativa independiente. En este sentido, la conocida agencia norteamericana DARPA[21] ha buscado propuestas que sean capaces de crear mensajes, transferirlos y recibirlos usando una red de mensajería descentralizada. Esto es especial relevante para áreas como el de armamento nuclear o satélites militares.

Bajo la dirección de Timothy Booher, actual responsable del programa *blockchain* de DARPA se han gestionado contratos como el adjudicado a la compañía Galois por su aplicación *Blockchain Guardtime Keyless Signature Infraestructure (KSI)* que puede detectar amenazas diseñadas para permanecer ocultas en las redes.

[21] Acrónimo de: Defense Advanced Research Projects Agency. https://www.darpa.mil/.

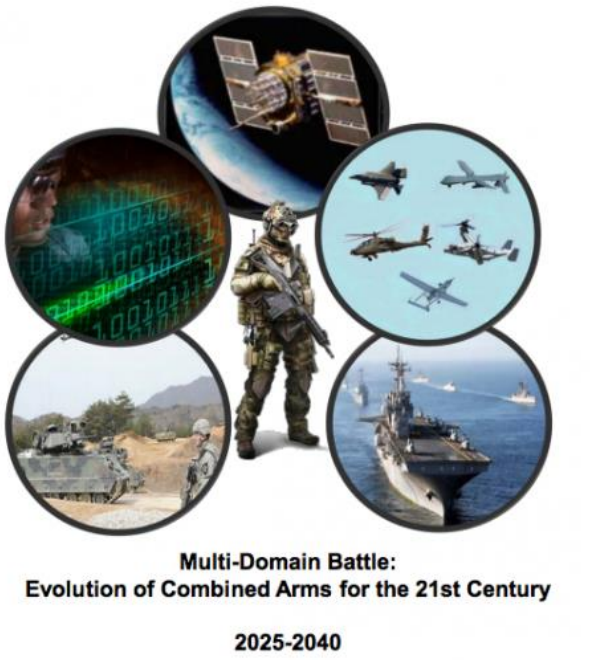

Figura 2: Ámbito múltiple de operaciones: evolución de armas combinadas para el s. XXI (2025-2040). Fuente: https://www.zerohedge.com/news/2017-10-17/us-army-preparing-decades-hybrid-wars.

Por su parte, la Agencia de Comunicaciones e Información de la OTAN está evaluando propuestas en áreas de aplicación de tecnología *blockchain* relacionadas con logística militar, adquisiciones, Internet de las cosas y otras aplicaciones de interés militar.

En el marco de la Agencia Europea de Defensa, *blockchain* se ha introducido en la Agenda de Investigación Cibernética Estratégica, dada su capacidad de cifrado y su robustez en materia de seguridad de la información, autenticación e integridad de los datos. Se aprecia ya la futura aplicación en materia de soporte logístico y en la creación de sistemas de interconexión para los dispositivos dotados de IoT.

La escalada de los ataques cibernéticos puede hacer inservible el mejor sistema de armamento, por lo que contar con sistemas criptográficos cuya manipulación sea imposible (o simplemente obvia) al alinear a los nodos honestos frente a los deshonestos supone la inatacabilidad o la hipotética necesidad de incurrir en enormes costes para un potencial adversario que desee manipular la red.

En el ámbito de las comunicaciones militares, *blockchain*, al contar con protocolos P2P con la contribución de todos los nodos de la red, en el caso de que se produjese un ataque que interrumpiese el funcionamiento de Internet o las comunicaciones inalámbricas o mediante satélite, se podría incluso enviar mensajes de *blockchain* mediante canales alternativos, como radio de alta frecuencia, fax o incluso mediante

transmisión manual de impresiones de código de barras. La inexistencia de un nodo central permite funcionar a la red aunque cayese una considerable proporción de los nodos que la integran; asegurando además, mediante el mecanismo de consenso, que los mensajes no válidos generados por el agresor son ignorados.

Desde otro punto de vista, podría ser posible distribuir la red *blockchain* sobre bases militares nacionales con capacidad informática suficiente para alojar los servidores *blockchain*. De esta forma, habría una copia local del libro mayor en caso de problemas de red, y se distribuiría de modo que no hubiese puntos centrales vulnerables.

La conocida compañía aeroespacial Lockheed Martin ha sido la primera contratista de defensa del pentágono que ha incorporado *blockchain* en sus estrategias de desarrollo. Junto con la compañía Guardtime Federal, están realizando demostraciones sobre la capacidad de mantener la integridad de los datos y repeler las amenazas cibernéticas, además de desarrollar *software* más seguro para la gestión de riesgos de las cadenas de suministro. También colabora con la compañía ForAllSecure, ganadora del *DARPA Cyber Grand Challenge* y trabajan sobre el concepto de *Cyber Aware Systems*.

Conclusiones

La economía y la sociedad están en permanente evolución. La historia de la humanidad es testigo de periodos en los que diversos avances tecnológicos aceleraron los cambios desde su más remoto pasado. Muchas invenciones y avances tecnológicos han sido el propulsor de cambios sociales y económicos trascendentes para la especie humana.

La época actual asiste a una revolución tecnológica sin precedentes, potenciada por una convergencia o acoplamiento de tecnologías diversas; y por la coincidencia en el tiempo de diversos desarrollos tecnológicos que, ahora, empiezan a unirse entre sí para crear cosas inimaginables hasta hace pocos años, incluso para los más visionarios.

En este contexto, la irrupción de los sistemas encriptados de cadenas de bloques (*blockchain*) y las nuevas tecnologías denominadas «distribuidas» (DLT), prometen cambiar radicalmente muchos modelos de negocio y de gestión institucional al romper con los modelos centralizados de gestión, al tiempo que transformarán la economía, la sociedad y las instituciones, pero también puede reconfigurar, considerablemente, diversos campos relacionados con la defensa.

Los beneficios y las aplicaciones reales en el ámbito de las comunicaciones y la lucha contra las amenazas cibernéticas probablemente no se verán hasta el año 2025, pero el interés despertado es ya considerable. En este sentido, la agencia norteamericana DARPA ha aportado financiación para un proyecto de desarrollo de sistemas de mensajería para las Fuerzas Armadas estadounidenses que sean seguras y no *hackeables*[22], que incluye las comunicaciones entre las tropas desplegadas y el cuartel general. La idea básica es descentralizar los mensajes separando su origen de su transmisión.

También resulta de gran interés la posibilidad de descentralizar parte de la infraestructura de soporte o *back-office* mediante la aplicación de *smart contracts* que puedan ser inmediatamente enviados o recibidos.

El control y conocimiento de la veracidad de los componentes de las cadenas de suministro de las que se proveen los sistemas de defensa se considera actualmente esencial y prioritario, por lo que *blockchain* puede ser una relevante aportación.

La tecnología digital es vulnerable a los ataques cibernéticos y al uso fraudulento de los datos, pudiendo dañar seriamente la privacidad de las personas y la seguridad de las instituciones, por lo que apremia poner en marcha soluciones tecnológicas de alcance como es *blockchain*.

En este sentido, en el ámbito de la defensa nacional en España, puede ser de interés comenzar con el conocimiento y la posterior investigación de las potencialidades de *blockchain*, así como hacer un seguimiento de sus avances en otros países. También se puede motivar la creación de grupos de expertos en esta materia que puedan interactuar y extrapolar al ámbito militar las aplicaciones que se están comenzando a desarrollar en el ámbito civil; pudiendo aprovechar la infraestructura nacional ya iniciada con el consorcio Alastria, más arriba citado.

Sin duda alguna, *blockchain* es una tecnología que no va a poder ignorarse en los próximos años y que puede aportar soluciones a la vulnerabilidad de muchos sistemas de defensa.

Al igual que cambian los modelos de negocio y de gestión empresarial con, la defensa se verá obligada a convivir con una sociedad «blockchainizada» que supone romper el

[22] https://www.prnewswire.com/news-releases/itamco-to-develop-*blockchain*-based-secure-messaging-app-for-us-military-300464063.html.

paradigma tradicional del control centralizado y su reemplazamiento por modelos de organización de base distribuida, descentralizada y geodeslocalizada.

*Ricardo Palomo-Zurdo**
Catedrático de Economía Financiera
Universidad CEU San Pablo

* Mi agradecimiento al equipo de Alastria y de la Fundación para la Innovación Financiera y la Economía Digital (FIFED) por sus valoraciones previas sobre esta publicación, en particular a Carlos Pastor Matut.