Cuadernos de divulgación PUE

La revolución del *blockchain*

Pablo Rodríguez Canfranc
José Ramón Granger Alemany
Carlos Guallarte Nuez

Programa Universitat-Empresa UAB

La revolución de *blockchain*

La revolución de *blockchain*

Pablo Rodríguez Canfranc
José Ramón Granger Alemany
Carlos Guallarte Nuez

© del texto: Pablo Rodríguez Canfranc, José Ramón Granger Alemany,
Carlos Guallarte Nuez
© de esta edición: Servei de Publicacions de la UAB

Edición:
Servei de Publicacions
Universitat Autònoma de Barcelona
Edifici A. 08193 Bellaterra (Cerdanyola del Vallès). Spain
Tel. 93 581 10 22
sp@uab.cat
https://publicacions.uab.cat

ISBN (digital): 978-84-10202-39-9

Este libro está publicado con una licencia Creative Commons CC-BY-NC-ND.
El titular de la obra autoriza a utilizar los contenidos siempre que se reconozca
la autoría. No se permite hacer un uso comercial, ni la generación
de obras derivadas.

SUMARIO

INTRODUCCIÓN

> «La primera generación de la revolución digital nos trajo el internet de la información. La segunda generación —alimentada por la tecnología *blockchain*— nos está trayendo el internet del valor: una nueva plataforma para remodelar el mundo de los negocios y transformar para bien el antiguo orden de los asuntos humanos.»
>
> Don y Alex Tapscott, *Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business and the World.*

> «Tiene matemáticas. Tiene informática. Tiene criptografía. Tiene económicas. Tiene filosofía política y social. Fue esta [*blockchain*] la comunidad por la que inmediatamente me sentí atraído.»
>
> Vitalik Buterin. Fundador de Ethereum.

A menudo la aparición de *blockchain* es comparada con el nacimiento de internet. En ambos casos, la base está en el avance de tecnologías clave junto con el desarrollo de nuevas arquitecturas abiertas y en el hecho de que son estructuras descentralizadas que se hacen más fuertes en la medida en que son utilizadas por un número cada vez mayor de usuarios. Tanto internet como *blockchain* se basan en un protocolo abierto e interoperable sobre el que empresas y particulares pueden desarrollar servicios y aplicaciones. La información

se almacena en una cadena de bloques, o *blockchain*, cuyo fin es evitar su modificación una vez que el dato ha sido publicado. Los bloques ordenan la información temporalmente enlazando cada bloque con el anterior.

Blockchain promete eliminar intermediarios en las relaciones entre los usuarios de la red y reforzar su poder, quitándoselo a las entidades e instituciones que lo han ejercido tradicionalmente. Es algo que ya hizo el primer internet, y que se intensificó con la llegada de los medios sociales hacia el año 2009: alterar las relaciones entre las marcas y los consumidores, reconvertir sectores enteros, como las industrias culturales, o replantear el papel de los medios de comunicación, entre otros ejemplos. Se trata de la llegada de un tsunami que lo trastoca todo.

La próxima evolución de internet se basará en las cadenas de bloques, de acuerdo con los expertos. La web futura ya no funcionará sobre plataformas digitales de servicios como hasta ahora, sino sobre *blockchain*, que garantizará las relaciones directas sin intermediación de los usuarios, y traerá la llegada de un internet más democrático, vaticinan los más optimistas. La Web 3 promete el advenimiento de un internet en manos de los individuos, en que las organizaciones y las grandes empresas tecnológicas no podrán imponer su poder. En esta versión de la red de redes toda la confianza habrá sido depositada en la propia filosofía de la tecnología subyacente, es decir, en las características intrínsecas de las cadenas de bloques, que garantizan el marco de relaciones entre los usuarios.

Este monográfico presenta una introducción a la tecnología *blockchain*, su filosofía y sus orígenes, sus principales aplicaciones sociales y económicas, y sus posibilidades de evolución en los próximos años.

De esta manera, en primer lugar, se expone el funcionamiento de la tecnología DLT (*Distributed Ledger Technology*), los distintos conceptos que incluye, y los diferentes tipos de redes *blockchain* que existen en la actualidad.

A continuación, se trata brevemente el fenómeno de las criptodivisas como la primera aplicación de las tecnologías basadas en cadenas de bloques, cuya popularidad ha ido creciendo desde mediados de la década pasada hasta el momento actual, en que las sucesivas pérdidas de valor de las principales divisas las colocan ante un futuro incierto.

El siguiente capítulo presenta el papel que puede desempeñar *blockchain* en la operativa de la empresa, a través de conceptos como los contratos inteligentes, para, a continuación, describir aplicaciones concretas en sectores específicos de actividad.

El penúltimo epígrafe plantea el estado de desarrollo de esta tecnología en España, que es impulsada por la asociación Alastria, y los programas institucionales para su difusión y crecimiento, tanto desde la Comisión Europea como desde la Administración española. Finalmente, se esbozan las probables sendas de evolución del *blockchain* y su convergencia con otras tecnologías de vanguardia, como la inteligencia artificial o el internet de las cosas (IoT).

1. ¿QUÉ SON LAS CADENAS DE BLOQUES?

La tecnología de contabilidad distribuida (*Distributed Ledger Technology*)

En este planeta ya conectado, la importancia de las transacciones digitales va en aumento, y aspectos como la integridad y la trazabilidad de la información, o la transparencia en su manipulación, son cruciales para asegurar la confianza en las redes de comunicaciones, el canal por donde fluye toda esa información. La tecnología *blockchain* proporciona a las redes una capa adicional que permite garantizar, no ya que el intercambio de información sea seguro o fiable, sino la atribución con certeza absoluta de la autoría de la información. Las cadenas de bloques certificarán el contenido o el bien que se genera y se transmite; qué persona, entidad, institución o dispositivo generó o envió qué; desde dónde, cómo y cuándo. Al aplicar *blockchain* en el entorno corporativo, estamos hablando de diseñar redes de confianza sobre las que se construyen las relaciones empresariales.

Blockchain es, hoy en día, un sinónimo de innovación y de vanguardia tecnológica. Con el cambio de década, ha abandonado los laboratorios y ha permeado en el mundo de la empresa, en los medios de comunicación generalistas y hasta en los discursos políticos. Hay profetas tecnológicos que auguran que traerá consigo una revolución equivalente a la llegada de internet. Algunos advierten que llega para trastocarlo todo y que, más allá de su aplicación en el campo financiero, pondrá patas arriba todos y cada uno de los sectores de actividad económica. Los usos y aplicaciones se suceden de

forma vertiginosa: *blockchain* en la educación, en la Administración Pública, en la logística, en las cadenas de suministro, en la gestión de los derechos de autor, en el periodismo... Aparentemente pocas actividades quedan fuera de su alcance.

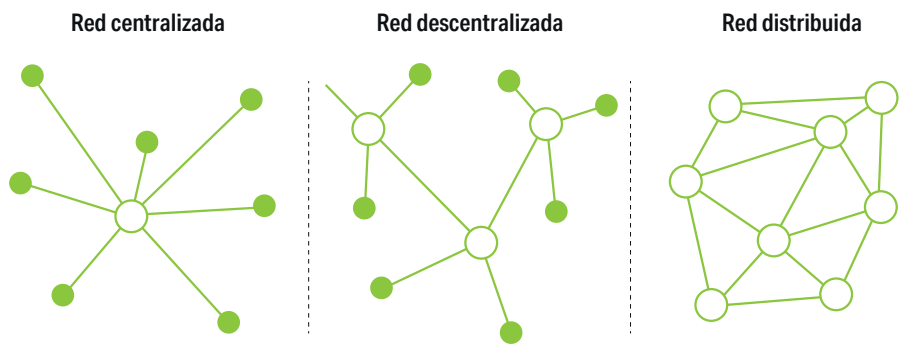
Uno de los desafíos a los que se enfrenta la difusión de la tecnología *blockchain* es lograr que se comprenda su utilidad y su potencial en el seno de una organización. En realidad, no es otra cosa que una tecnología que permite tener un sistema de registros distribuido a través de la red —es decir, no encerrado en una base de datos centralizada—, que permite que todos los usuarios participantes en el sistema puedan ver las transacciones que tienen lugar en el mismo. La privacidad es completa, pues todas las transacciones son fiables, están autentificadas y se pueden verificar en cualquier momento. Adicionalmente, las cadenas de bloques permiten realizar contratos inteligentes, es decir, transacciones o hitos que quedan registrados de forma automática, sin intervención humana, una vez que se produce cierta condición especificada de antemano.

Con frecuencia se asocia *blockchain* a un libro de contabilidad o registro distribuido. Algo que en inglés se conoce como *Distributed Ledger Technology* (DLT), cuya poco afortunada traducción es «tecnología de libro mayor distribuido», hace referencia a la infraestructura y los protocolos de comunicación que permiten que distintos ordenadores separados geográficamente propongan y validen transacciones, actualizando de forma sincronizada los registros de estas. *Blockchain* es un tipo específico de DLT en el que las transacciones (ya sean de criptomonedas, unidades de cuenta o de mera información) son almacenadas en bloques sellados criptográficamente y unidos unos a otros formando una cadena. Este punto constituye un factor de seguridad determinante, dado que, aunque consiguieras quebrar el sello de un bloque para alterar la información que contiene, tendrías que cambiar todos los de los bloques sucesivos para poder completar la operación.

A menudo, se identifican las cadenas de bloques con la DLT, pero no son sinónimos, pues hay DLT que no son *blockchain*. Igual que

todos los Kleenex son pañuelos de papel, pero no todos los pañuelos de papel son Kleenex. Para que una DLT sea *blockchain*, tiene que cumplir la condición de que los registros sean ordenados en bloques y que se unan unos a otros mediante un *hash* o sello criptográfico.

La red distribuida tiene ciertas ventajas frente a las redes centralizadas o descentralizadas, pues la tecnología que permite compartir la información con todos los usuarios de la red es independiente de los nodos que la conforman. Es decir, la red no tiene una estructura jerárquica y no existe una ruta predefinida para conectar dos puntos del sistema. Además, es posible incorporar nuevos nodos o eliminar nodos existentes sin influir en su funcionamiento. Las diferencias se aprecian mejor gráficamente:



Fuente: Blockchain Intelligence.

Tipos de redes DLT

Los sistemas basados en la tecnología de contabilidad distribuida (DLT) pueden ser de tres tipos: públicos, privados o de consorcio. A los públicos puede acceder todo el mundo y convertirse en un nodo autorizado de la red, y en ellos existe un método establecido para que los usuarios se pongan de acuerdo para validar las nuevas

operaciones o transacciones que son añadidas, que suele ser el denominado *Proof of Work* (PoW) o el conocido como *Proof of Stake* (PoS). Por su parte, a los privados solamente se accede mediante autorización y tienen unas autoridades que hacen cumplir las normas a los usuarios de la red. Finalmente, las DLT de consorcio están gobernadas por una serie de nodos que son independientes unos de otros —es decir, constituyen una estructura descentralizada—, pero que ejercen un control mutuo.

Además de lo anterior, las DLT pueden ser *permisionadas o cerradas*, cuando requieren de una autorización para operar en ellas, y *no permisionadas*, cuando son de libre acceso.

En consecuencia, las DLT pueden ser clasificadas en distintas categorías atendiendo a una serie de dimensiones:[1]

- ¿Quién puede acceder?
- ¿Qué tipo de permisos son necesarios para operar en ella?
- ¿Qué tipo de criptografía utiliza?
- ¿Qué tipo de consenso utiliza?
- ¿Qué forma tiene la red (centralizada, distribuida o descentralizada)?
- ¿Quién decide la prioridad en el cierre de bloques?
- ¿Quién paga la infraestructura y los costes de computación?
- ¿Qué algoritmos son utilizados y qué comportamiento presentan?

Si combinamos las dos primeras cuestiones de la lista, aparecen cuatro tipos de DLT.

Una DLT pública y no permisionada. Son sistemas a los que todo el mundo puede acceder libremente, y realizar operaciones en ellos sin tener que recibir permiso, incluyendo la participación en los mecanismos de consenso y en la verificación de transacciones. Este tipo de DLT es el único que realmente puede considerarse una *block-*

1. Engineering. *Blockchain. Unchaining business through the Blockchain.*

chain pura, como bitcoin o ethereum, pues reúne las cuatro características inherentes a las cadenas de bloques: seguridad, transparencia, descentralización e inmutabilidad.

Una DLT pública y permisionada. En estas redes todo el mundo puede acceder y leer la información contenida, pero se necesita autorización y permisos para realizar otras operaciones, como, por ejemplo, añadir nuevos registros. Un ejemplo de esta categoría podría ser un sistema de garantía de calidad o de la denominación de origen de un determinado producto, que sería accesible para el consumidor, quien puede leer la información que avala la mercancía, pero en el que solamente los agentes autorizados implicados en la cadena de producción y distribución pueden añadir registros de información, como podría ser un cambio de estado en el proceso de conservación.

Una DLT privada y no permisionada. En este caso, solo pueden realizar operaciones un número limitado de usuarios del sistema, pero no requieren permisos especiales para hacerlo. Sería el tipo de red utilizada en el seno de una organización, cerrada al exterior, pero accesible por los miembros de esta.

Una DLT privada y permisionada. Este último tipo tiene el acceso reservado para determinados usuarios o grupos, que, además, requieren de autorizaciones específicas para realizar operaciones en el sistema.

De esta forma, dependiendo del uso que se le quiera dar a una DLT, será conveniente adoptar formatos más o menos abiertos. Así, las podemos encontrar absolutamente colaborativas y abiertas a todo usuario que quiera participar, como lo son las que dan soporte a las criptomonedas, y, en el otro extremo, totalmente restringidas al uso de agentes concretos que tengan autorización expresa para operar en ellas, como la que crearía una empresa para su uso interno.

Tipos de *blockchain*

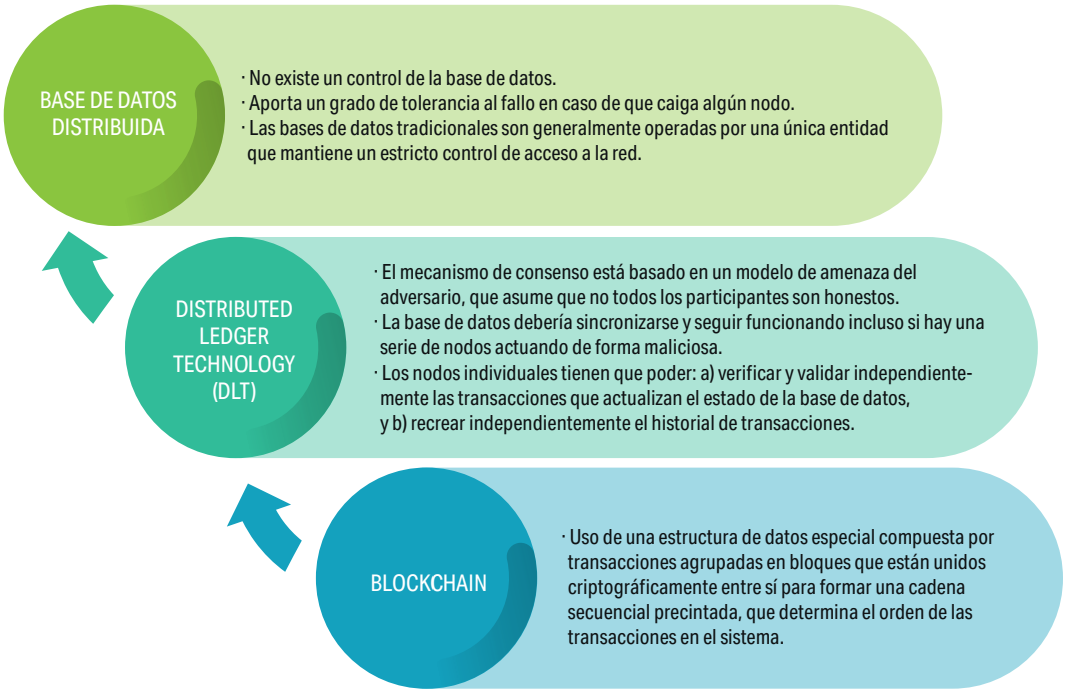
Grado de descentralización	PÚBLICA		CONSORCIO		PRIVADA
Gestión	Gestión no centralizada		Múltiples organizaciones		Una sola entidad
Acceso	Permisionada	No permisionada	Permisionada	No permisionada	Permisionada
	Lectura abierta / validación de transacciones abierta	Lectura abierta / validación de transacciones permisionada	Lectura permisionada o abierta / validación de transacciones permisionada	Lectura abierta / validación de transacciones abierta	Lectura y validación de transacciones permisionada
Participantes	Anónimos / pseudoanónimos	Anónimos / pseudoanónimos	Identificados	Normalmente identificados	Identificados
Validación basada en protocolo de consenso	Abierta a cualquier miembro de la red	Abierta a cualquier miembro de la red sujeta a ciertas condiciones	Por participantes preautorizados (de las organizaciones implicadas)	Depende del protocolo de consenso elegido por la plataforma	Por participantes preautorizados (de una sola organización)
Velocidad de validación	Lenta	Más rápida	Rápida	Rápida	Rápida
Grado de privacidad de los usuarios	Ninguno	Ninguno	Adaptado a las necesidades de los participantes	Adaptado a las necesidades de los participantes	Adaptado a las necesidades de los participantes
Poder computacional requerido/consumo energético	Alto. Dependiente del mecanismo de validación	Intermedio. Dependiente del mecanismo de validación	Menor	Menor	Menor
Cuotas de transacción	Sí	Sí	Opcional — dependiendo de las reglas del *blockchain*	Opcional — dependiendo de las reglas del *blockchain*	Opcional — dependiendo de las reglas del *blockchain*
Escalabilidad	Baja	Algo mayor	Mayor	Mayor	Mayor
Ejemplos	Proof of Work (Bitcoin)	Proof of Stake (Ethereum)	*Blockchains* desarrolladas en Hyperledger Frabric. *Blockchains* permisionadas construidas en Ethereum	Fasta Track Trade	*Blockchains* privadas construidas en Ethereum

Fuente: Ganne, E. (2018). *Can Blockchain revolutionize international trade?* World Trade Organization. Elaboración propia.

Cómo funcionan las cadenas de bloques

Como ha quedado expuesto más arriba, una *blockchain* es un tipo específico de DLT en su versión más abierta. Para ayudar a entender esta tecnología, a menudo se la asocia con un libro de contabilidad abierto a ser utilizado por cualquier persona, en el que cada registro está unido al inmediatamente anterior y al posterior mediante un sello criptográfico, formando, de esta manera, una cadena. Esto implica, por una parte, la inmutabilidad del sistema, pues para alterar la información contenida en un bloque tendríamos que alterar todos los precedentes, y, por la otra, garantiza la trazabilidad de la información contenida en el *blockchain*, dado que la secuencia de bloques establece un registro cronológico de las operaciones realizadas al ser cada nuevo elemento añadido al precedente en el tiempo.

Relación entre bases de datos distribuidas, DLT y *blockchains*



Fuente: World Economic Forum (2019). *White Paper. Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction.*

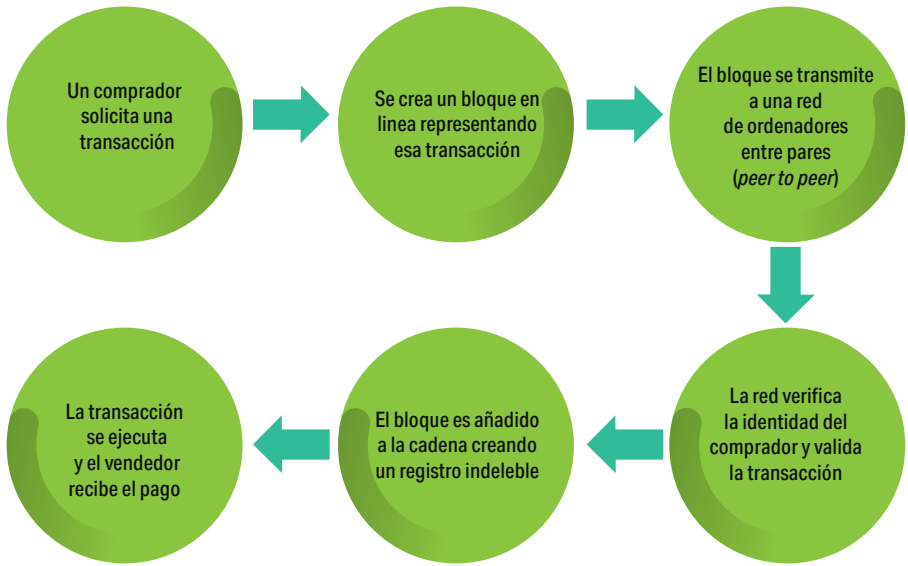
Uno de los rasgos que más destacan los defensores de esta tecnología es su seguridad, que reposa sobre la criptografía y sobre su carácter descentralizado. El primer elemento está constituido por algoritmos criptográficos que sellan cada bloque, uniéndolo al siguiente. Además de esto, en las *blockchain* puras completamente distribuidas, cada usuario del sistema tiene una copia completa del sistema, por lo que sería muy difícil que fuese alterado por uno de ellos sin que el resto se dé cuenta. De ahí que siempre se asocie las cadenas de bloques con la transparencia, porque, a diferencia de otros tipos de bases de datos más tradicionales de gestión centralizada, en ellas todos los miembros del sistema conocen el estado de la red en cada momento. Esto último implica que la figura del consenso es la que rige el funcionamiento y el crecimiento de la *blockchain*. Cada usuario o nodo del sistema aprueba toda nueva transacción añadida a este, y puede detectar si se ha quebrantado en algún momento alguno de los bloques de información de la cadena.

Otra garantía de seguridad de las cadenas de bloques es la elevada capacidad de computación que sería necesaria para alterar fraudulentamente alguno de los bloques sin que el resto de los usuarios se percate de ello. Siempre se ha considerado este factor como una barrera que hace imposible cometer un delito en *blockchain*, como podría ser, por ejemplo, realizar una compra que quede registrada en la cadena, y luego alterar secretamente el bloque correspondiente para borrar la transacción y que figure de nuevo en nuestro poder el dinero entregado. Si bien esto es algo imposible de realizar en redes muy grandes, como puede ser el bitcoin, por la cantidad de poder de computación que haría falta para alterar toda la cadena de bloques que sigue al que queremos cambiar, es un delito que se ha llevado a cabo en una *blockchain* más pequeña, como es ethereum.

En términos prácticos, una operación en *blockchain* presentaría, a grandes rasgos, el flujo reflejado en el gráfico siguiente. Cuando un usuario de la red desea realizar una operación (por

ejemplo, comprar bitcoins) lo solicita al sistema, e inmediatamente se crea un bloque específico para ella. El nuevo bloque se transmite a todos los usuarios de la red, que, como se ha mencionado más arriba, cuentan con una copia en tiempo real de toda la cadena de bloques. Cuando la identidad del comprador es verificada y la operación queda validada, el bloque al que está asociada se une a la cadena por medio de un *hash* o sello criptográfico. En ese momento, la operación se ejecuta (el vendedor le transfiere los bitcoins y recibe el pago por ellos).

Cómo funciona una transacción en *blockchain*



Fuente: elaboración propia.

Estos sistemas se caracterizan por una serie de cualidades, que, de alguna forma, los definen: seguridad, transparencia, descentralización e inmutabilidad. En el sistema puro de cadena de bloques, es el conjunto de usuarios el que garantiza el correcto funcionamiento de la red, mediante unos mecanismos que veremos más adelante.

La tecnología como garantía frente a la ausencia de intermediación

La revista *The Economist* llegó a definir *blockchain* como la «máquina de la confianza»,[2] dado que nos permite realizar transacciones con otros participantes en la red a los que no conocemos de nada, confiando ciegamente para ello en las herramientas criptográficas y matemáticas del sistema, y en el funcionamiento correcto del protocolo de consenso.

Solamente una certeza absoluta del público en su seguridad garantizará su expansión y supervivencia. Pero, como indica Vitalik Buterin, cofundador de Ethereum, esto implica una contradicción: «se supone que la mayor ventaja de la tecnología *blockchain* es que es más segura, pero a la gente le cuesta confiar en nuevas tecnologías, y esta paradoja no puede ser evitada».

Blockchain supone un cambio de paradigma en el ámbito de las relaciones comerciales, que, generalmente, se basan en la confianza. Tradicionalmente, las transacciones se asientan sobre agentes intermediarios que, de algún modo, garantizan que todo se va a hacer de forma correcta. Entidades financieras, abogados, notarios o agencias de certificación, a modo de ejemplo, son figuras que otorgan confianza a las relaciones comerciales de todo tipo. Otro elemento que aporta fiabilidad a la operación es conocer bien al interlocutor en la transacción y poder confiar en su honradez.

La confianza es un fenómeno social complejo, que se basa en la interrelación de aspectos individuales de las personas (psicológicos, actitudinales, informacionales) y aspectos del sistema en el que se desenvuelven (económicos, legales, tecnológicos y sociales). Conlleva varias dimensiones, si las relaciones son entre actores sociales (confianza interpersonal), entre actores e instituciones (confianza institucional) o entre instituciones y actores sociales que confían (la confianza como expectativa compartida). En ellas, la infraestructu-

2. https://www.economist.com/leaders/2015/10/31/the-trust-machine

ra institucional define la naturaleza y la fortaleza de las relaciones de confianza entre los distintos actores. En suma, la confianza hace referencia a las expectativas que se forja el que confía sobre la persona en la que deposita su confianza, en relación con la ocurrencia de acciones o eventos futuros que conllevan un riesgo para aquel que confía. Implica elementos tanto cognitivos como emocionales, pero es diferente de la fe ciega.

El reto que plantean las cadenas de bloques es poder realizar transacciones entre perfectos desconocidos, sin ningún tipo de intermediación que garantice que no se produzca un posible fraude. La confianza se ha trasladado de la figura del intermediario, que en el nuevo escenario desaparece, a la tecnología y el proceso automático de validación de la red. Sobre este particular, hay opiniones enfrentadas. Para algunos estudiosos del fenómeno, el *blockchain* implica la desaparición de la confianza, puesto que el sistema ya no la necesita; para otros, en cambio, la confianza sigue existiendo, aunque ya no en las contrapartidas de la relación (los demás usuarios de la red), sino en los elementos de la cadena de bloques (protocolo de consenso, mineros, nodos...).[3]

Un ejemplo claro de esto son las criptomonedas, que, a diferencia de las divisas tradicionales, carecen de una entidad u organismo —como un banco central—, que respalde su legalidad en los mercados financieros. En el caso de las criptodivisas, esta garantía la aporta la propia filosofía de la tecnología de las cadenas de bloques.

Minería, *hash*, tókenes y protocolos de consenso

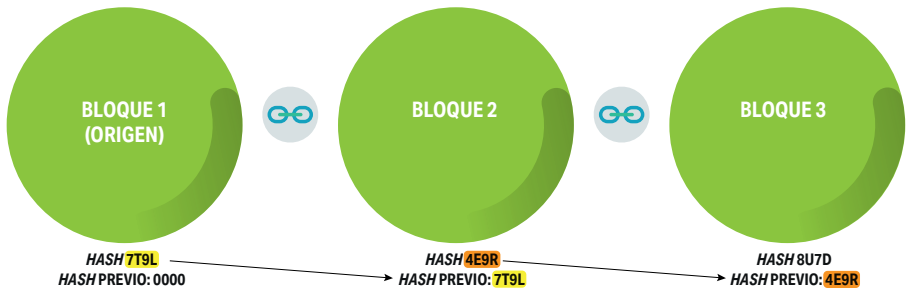
La aireada inquebrantabilidad de las redes *blockchain* reposa en dos elementos de vital importancia: cada bloque del sistema está asociado a una huella digital criptográfica única, y es necesario que

3. Becker, M. y Bodó, B. (2021). *Trust in blockchain-based systems.* Internet Policy Review, 10(2).

exista un protocolo de consenso que consiga que todos los nodos de la red estén de acuerdo sobre la veracidad del historial que todos comparten.

Estas huellas digitales se denominan *hash*, y son creadas por los mineros de *blockchain*, unas figuras esenciales dentro del sistema. Los mineros son poderosos ordenadores que trabajan a cambio de criptomonedas. Cada *hash* es una fórmula matemática única que concentra en pocos caracteres gran cantidad de información. Sirven para sellar un bloque y para unirlo con el bloque siguiente, dado que este contiene el *hash* del anterior. De esta forma, no es posible alterar la información contenida en un bloque —un pago, por ejemplo— sin cambiar toda la cadena.

Esquema del funcionamiento de *blockchain*



Fuente: elaboración propia.

Cuando se añade un nuevo bloque a la cadena, todos los nodos de la red verifican que el *hash* corresponde al bloque en cuestión, y, automáticamente, actualizan sus copias de la *blockchain*, pues todos guardan una copia de toda la cadena. Esta miríada de nodos constituye un «único punto de verdad» (*Single Point of Truth*), porque hace posible preservar la integridad de los datos, permitiendo que cualquier actualización legítima procedente de uno de los nodos la reciban automáticamente a la misma vez el resto de los participantes. Si alguien intentase alterar un registro de forma retroactiva, ten-

dría que cambiar el *hash* de ese bloque y de todos los siguientes que van unidos, pero los bloques que intente añadir entrarían en conflicto con los existentes, y los nodos rechazarían la operación.

La validación de las transacciones y los nuevos bloques en una *blockchain* se realiza mediante el protocolo de consenso, que no es otra cosa que una forma de retribuir a los mineros que realizan esta función, incentivándolos a que trabajen de una forma honesta y leal. Uno de los más extendidos —es el que utiliza bitcoin— es el denominado *Proof of Work* (prueba de trabajo), que implica que cada bloque nuevo que se crea en la cadena debe ser resuelto por los mineros mediante un cálculo matemático. Para ello, realizan millones de intentos y utilizan una inmensa capacidad computacional, con el consiguiente gasto de energía que ello conlleva. Cuando un minero resuelve el puzle matemático, la transacción y el bloque son validados por el resto, y puede ser añadido a la cadena.

Existen otros protocolos de consenso; uno de los más conocidos es el *Proof of Stake* (prueba de participación), que en 2022 fue adoptado por la red *blockchain* Ethereum. En este caso, no hay competición entre mineros. Cada usuario debe aportar una cantidad de tókenes (unidades de cuenta en *blockchain*) para poder tener la oportunidad de participar en la validación del nuevo bloque. En el PoS, el sistema elige al azar a un usuario para validar la nueva transacción, y recibirá la recompensa si lo hace. La ventaja de este sistema es que, al haber solamente un validador (frente a la competición de mineros del PoW), el poder computacional necesario y el gasto energético son notablemente inferiores.

El problema del modelo PoW es el inmenso consumo de energía que implica. Según cálculos del Cambridge Center for Alternative Finance, la red bitcoin en solitario utiliza tanta cantidad de energía como países como Malasia o Suecia.[4]

Un último concepto asociado a la tecnología de las cadenas de blo-

4. Marquit, M. (2022). *Proof of Work vs. Proof of Stake: Why the Difference Matters for Ethereum Investors en Next Advisor.*

ques es el de token. Un token (palabra que significa *ficha* en inglés) es una unidad de valor basada en criptografía y emitida por una entidad privada en una *blockchain*. Por ejemplo, los bitcoins son tókenes. Sin embargo, no todos los tókenes son criptomonedas, dado que también pueden servir para otorgar un derecho, para pagar por un trabajo o por ceder unos datos, como incentivo, como puerta de entrada a unos servicios extra o a una mejor experiencia de usuario.[5]

Un token servirá para aquel fin que la persona u organización que lo haya creado decida. A grandes rasgos, se pueden distinguir tres tipos:

- Aquellos utilizados como pago o como divisa, como los que forman parte de Bitcoin o Ethereum. Se trata de medios de pago alternativos a los de las instituciones financieras tradicionales.
- Tókenes de seguridad, equidad o inversión, que implican participación en empresas y los derechos asociados de codeterminación.
- Tókenes de utilidad, que cumplen la función de dar acceso a productos y servicios. Son como vales virtuales que equivalen a productos o servicios futuros de una empresa u organización.

Cuando *blockchain* deja de ser inexpugnable

A pesar de que *blockchain* se presenta como una tecnología absolutamente segura, que mantiene las transacciones que tienen lugar en su seno a salvo de *hackers* y ciberdelincuentes, la experiencia ha demostrado que las cadenas de bloques no son del todo inquebrantables y que, en ocasiones, pueden ser objeto de ataques y robos.

En mayo de 2018, la empresa de intercambio de criptomonedas

5. BBVA (2023). *Qué es un «token» y para qué sirve.*

Binance anunció públicamente que había sufrido un ciberataque que supuso la pérdida de 7.000 bitcoins valorados en 40 millones de dólares. Los *hackers* lo consiguieron a través del *phishing* (ciberdelito basado en la suplantación de identidad) y del uso de virus informáticos. Otro ejemplo es el de la plataforma de *blockchain* Komodo, que en 2019 fue atacada por un virus *backdoor*, que permitió al delincuente que lo desarrolló acceder a los datos de encriptación de la empresa. Los responsables tuvieron que extraer los datos y el dinero de sus clientes y trasladarlos a una plataforma más segura.

Un estudio realizado por la compañía de software especializada en seguridad informática McAfee identifica cuatro vectores concretos de posibles ataques a las cadenas de bloques: *phishing*, *malware*, vulnerabilidades de implementación y tecnología.[6]

A través del *phishing*, el delincuente se hace con las claves de identidad del usuario, generalmente con la intención de obtener lucro de ello robando criptodivisas. Un claro ejemplo de esto es el robo que sufrieron de sus monederos los usuarios de la criptomoneda IOTA, a finales de 2017, que casi alcanzó globalmente la cifra de cuatro millones de dólares.

Los programas malignos o *malware* también afectan de lleno a *blockchain*, como hemos visto anteriormente con el caso del criptohackeo. Igualmente, los delincuentes utilizan la modalidad de *ransomware* o secuestro de los sistemas de criptomonedas, para exigir un rescate por la liberación de la información.

Un tercer problema viene asociado con las propias vulnerabilidades técnicas de las *blockchain*, que han dado lugar a ataques de denegación del servicio (DoS), robo de monedas y exposición de la información confidencial.

Finalmente, aparecen las vulnerabilidades relacionadas con las reglas de funcionamiento de *blockchain*. Uno de estos riesgos es la denominada regla del 51 %, algo que se quedaba en el terreno de la teoría hasta que lo sufrió la red Ethereum Classic en 2019. Básicamente,

6. McAfee (2018). *Informe sobre amenazas contra blockchain.*

consiste en alterar el funcionamiento de una criptodivisa para poder gastar el mismo dinero repetidas veces. En este caso concreto, los delincuentes cambiaron una cantidad de moneda de Ethereum por dinero real, para después reescribir el *blockchain* como si la operación no hubiese tenido lugar, con lo que seguían disponiendo de las criptomonedas que habían gastado. Para poder cometer este ciberdelito, es necesario acumular el 51 % de todo el poder computacional que sostiene la red. Esto es algo casi imposible de realizar con bitcoin, dado lo extendida que está esta criptodivisa y la inmensa cantidad de nodos que tiene su estructura *blockchain*, pero es factible con otras criptodivisas que tienen redes mucho más pequeñas.

Sin entrar en excesivos tecnicismos, el minero que ha conseguido la mayoría del poder para minar criptomonedas en el sistema tiene en sus manos la posibilidad de engañar a los demás, creando rápidamente una versión alternativa de la *blockchain* en la que los pagos que ha realizado nunca han tenido lugar. Esta nueva versión se conoce en el argot como *fork*, y el poder computacional del delincuente la convierte en la autorizada, sin que el resto de los participantes se percaten del fraude.

Los responsables de Ethereum Classic descubrieron que algo raro había pasado en su sistema cuando vieron que alguien había hecho cambios en la *blockchain*. Las primeras estimaciones arrojaban una estafa de 460.000 dólares, pero más adelante esa cifra superó el millón, realizada a lo largo de quince transacciones distintas.

2. LOS ORÍGENES: BITCOIN Y LAS CRIPTODIVISAS

Nace la moneda electrónica

Sin duda, el paradigma de *blockchain* es bitcoin, una divisa electrónica que no está respaldada por ningún organismo ni banco central, y en la que el cumplimiento de sus principios y reglas de funcionamiento está garantizado por la red de los propios usuarios de la moneda, que rechazan cualquier operación que infrinja las normas, como en toda cadena de bloques pura.

Bitcoin se dio a conocer en 2008, al estallar la crisis financiera, cuando, en un artículo publicado en internet, alguien que decía llamarse Satoshi Nakamoto (probablemente un seudónimo de una persona o de un grupo de personas) describió y preconizó la llegada de un nuevo formato de dinero electrónico o informático, el bitcoin, que podía transferirse sin pasar por entidades financieras.[7]

No obstante, ya habían existido intentos de impulsar el uso de criptomonedas con anterioridad, que, sin embargo, no habían conseguido trascender la esfera de las comunidades especializadas en la criptografía. Los antepasados de bitcoin fueron desarrollados por ciberpunks, o activistas de internet, que defendían el uso de tecnologías criptográficas que garantizaban la privacidad como una forma de provocar un cambio social y político. En suma, intentaban promover sistemas de intercambio financiero directo entre pares (*peer-to-peer*), que escapasen del control del sistema bancario.

7. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

De alguna forma, el bitcoin llegó en el momento oportuno para arraigar y crecer, pues la crisis financiera supuso un duro golpe para las entidades bancarias de todo el mundo, que perdieron gran parte de la credibilidad y la confianza del público. Las criptodivisas, en cambio, aparecían como una alternativa independiente de los poderes económicos, como habían soñado los colectivos radicales ciberpunk. El modelo propuesto por el informe de Nakamoto se basaba en un sistema monetario independiente, sin una autoridad central, y en el que los propios usuarios eran los encargados de validar las transacciones. La seguridad del sistema, en vez de un banco central, reposaba sobre una sólida tecnología criptográfica que evitaba que se produjeran fraudes y estafas en las operaciones allí realizadas. Adicionalmente, se trataba de una solución que permitía combinar la transparencia —todas las transacciones son públicas y son conocidas por todos los usuarios— con la privacidad, pues los participantes del sistema pueden mantener el anonimato.

Durante los cinco años siguientes a la publicación del manifiesto de Satoshi Nakamoto, el bitcoin fue casi un sinónimo de *blockchain*, ambos términos eran prácticamente una identidad. En 2013, un programador de 19 años llamado Vitalik Buterin publica su proyecto para desarrollar un nuevo sistema *blockchain*, que facilitaría la creación de aplicaciones descentralizadas. Se trataba de la red Ethereum, que, lanzada en 2015, constituye el segundo gran hito en la historia de las cadenas de bloques. Una de las ventajas que ofrecía el nuevo proyecto era incluir en Ethereum un lenguaje de programación que pudiese ser utilizado por desarrolladores para crear sus propias aplicaciones sobre la red.

Una de las innovaciones que introdujo Ethereum fue el concepto de contratos inteligentes (*smart contracts*), unos programas informáticos que se autoejecutan cuando tienen lugar determinadas condiciones previamente establecidas. Se trata de una verdadera revolución para las relaciones comerciales, pues garantizan el cumplimiento de los compromisos entre partes, sin retrasos y sin posibilidad de que se produzcan fraudes.

El número de criptomonedas que existen es inmenso y crece año tras año. En 2022, Funcas[8] calculaba que había más de 21.000 criptomonedas distintas, siendo las más conocidas las siguientes: bitcoin (BTC), ether de Ethereum (ETH), dogecoin (DOGE), binance coin (BNB), ripple (XRP), lumens (XLM) y litecoin (LTC). De todas formas, las dos más relevantes, bitcoin y ether, representaban a finales de dicho año cerca del 60 % de la capitalización total del mercado.

El valor de estas divisas está principalmente determinado por las fuerzas del mercado, es decir, por la relación entre la oferta y la demanda. Otros factores que pueden influir en el valor de una criptodivisa son su utilidad, seguridad y adopción. Por ejemplo, si una criptomoneda es ampliamente reconocida como medio de pago, es posible que valga más que otras que no estén tan extendidas. De la misma manera, tendrá más valor una moneda con un amplio historial de seguridad que otra de la que se conoce que haya sufrido ataques y hackeos.

Uno de los principales problemas que afectan a las criptomonedas como bitcoin y ether es la elevada volatilidad de su valor. Esto implica que existe una gran incertidumbre sobre sus variaciones, tanto positivas como negativas, lo que dificulta que puedan ser utilizadas como medio de cambio con otras divisas u otros tipos de activos. Es por ello que ha surgido una categoría de criptomonedas que experimentan muy pocas variaciones en el corto plazo, denominadas *stablecoins*.

Las *stablecoins* constituyen un tipo específico de criptodivisa que ofrecen a los inversores potenciales una estabilidad de precio, ya sea porque están respaldadas por activos específicos, ya sea porque su propio algoritmo gestiona la oferta y la demanda para evitar grandes fluctuaciones. La mayor parte de ellas tiene su valor asociado a una moneda *fiat*, como puede ser el dólar. La primera surgió en 2014, y en un principio era utilizada para la compra de criptodivisas en plataformas que no aceptaban el intercambio con dinero *fiat*. Progresivamente, su abanico de usos se ha ido ampliando, y ahora las *stable-*

8. https://www.funcas.es/odf/hay-muchas-criptomonedas/

coins se utilizan en diversos servicios financieros ofrecidos sobre *blockchain*, como pueden ser las plataformas de préstamo.

Rasgos de las *stablecoins*

	Stablecoins	**Criptodivisas tradicionales**
Volatilidad	Extremadamente baja	Puede resultar elevada
Política monetaria	Similar al dinero *fiat* o a activos como los metales preciosos	Determinada por el protocolo *blockchain*
Propiedades	Medio de cambio, unidad de cuenta y stock de valor	Diversos. Por ejemplo, Bitcoin se percibe como stock de valor, mientras que otras pueden ser vistas como medio de cambio
Respaldo de activos	Respaldadas por activos o por algoritmos	No está respaldada por ningún activo ni metal
Grado de autoridad	La mayoría de las *stablecoins* están controladas por una entidad central	La mayoría de las criptodivisas persigue la descentralización

Fuente: cointelegraph.com.

El invierno de las criptomonedas

A pesar de que tradicionalmente había sido un mercado boyante, 2022 supuso un año negro para las criptodivisas, que vieron como su valor caía sensiblemente respecto al año anterior. La capitalización máxima la alcanzó en noviembre de 2021, y fue cercana a los 3 billones de dólares; en el mismo mes de 2022, el mercado de criptodivisas había caído al nivel de los 800.000 millones de dólares, es decir, una reducción en torno al 73 %.[9]

9. Coinmarketcap. Total Cryptocurrency market cap. https://coinmarketcap.com/charts/

El popular bitcoin fue la criptodivisa que más determinó el desplome del mercado global. Su capitalización pasó de los 1,27 billones de dólares en noviembre de 2021 a los 350.000 millones de dólares en el mismo mes de 2022. El precio máximo del bitcoin se alcanzó el 9 de noviembre de 2021, llegando a los 67.550 dólares, cifra que se redujo a los 18.500 dólares el mismo día de 2022.

Este hundimiento estuvo provocado por varias causas. En primer lugar, por la subida de los tipos de interés asociada a la inflación que había supuesto la crisis económica. En segundo lugar, debido a la prohibición de minar e intercambiar criptomonedas en países como China o Rusia. En tercer lugar, los inversores prefirieron vender activos de riesgo como las criptomonedas ante la incertidumbre económica, lo que provocó el desplome de sus precios.

Estos profundos desplomes causaron sucesos como el de la *stablecoin* LUNA, del proyecto *blockchain* Terra, que perdió el 99 % de su valor en mayo de 2022. Se trata de la mayor caída experimentada por cualquier criptomoneda en toda la historia.

La complejidad y volatilidad de los mercados de criptoactivos causan no poca preocupación a los poderes públicos, de forma que empieza a surgir una legislación específica para este sector. Los sucesos acaecidos en los pasados años han puesto aún más de manifiesto la necesidad de imponer principios básicos a la emisión y negociación de estos activos de base tecnológica. En este sentido, en abril de 2023, el Parlamento Europeo aprobó el Reglamento de Mercados de Criptoactivos[10] (también conocido como MiCA, por sus siglas en inglés), que supone la primera norma europea sobre criptomonedas y productos relacionados. La medida entró en vigor en julio de 2023, y empezará a aplicarse entre mediados de 2024 y 2025.

MiCA afecta a las personas físicas y jurídicas que participan en la emisión, oferta al público y admisión a cotización de criptoactivos, así como en la prestación de varios servicios relacionados con los

10. Parlamento Europeo (2023). *Crypto-assets: green light to new rules for tracing transfers in the EU*. Press Releases.

criptoactivos dentro del espacio de la Unión Europea. Sin embargo, la norma no contempla la aplicación a los criptoactivos que ya se encuentran regulados por la legislación vigente sobre servicios financieros, como pueden ser los *security tokens*.

Los principales temas tratados por este texto normativo son:

- Requisitos de transparencia y divulgación en el marco de la emisión, oferta pública y admisión a negociación de criptoactivos en plataformas de negociación.
- Autorización y supervisión de los prestadores de servicios de criptoactivos y emisores de tókenes referenciados a activos o tókenes *e-money* .
- Requisitos de protección de los poseedores de criptoactivos y de los clientes de los proveedores de servicios de criptoactivos.
- Requisitos relativos a la prevención de las operaciones con información privilegiada, la divulgación ilícita de información privilegiada y la manipulación del mercado.

3. *BLOCKCHAIN* COMO UNA SOLUCIÓN PARA LA EMPRESA

Una fuente de valor para el negocio

Más allá de las criptodivisas, existe un campo abonado para que florezcan nuevas e innovadoras aplicaciones de *blockchain*. Cualquier actividad o sector que repose sobre la gestión de las relaciones entre múltiples partes puede beneficiarse de esta tecnología.

En un planeta cada vez más conectado, el protagonismo de las transacciones digitales es mayor día a día, y existen temas como la integridad y la trazabilidad de la información, o la transparencia en su manipulación, que resultan fundamentales para garantizar esa confianza en las redes de comunicaciones, el canal por donde fluye toda esa información. La tecnología *blockchain* proporcionará a las redes ese estrato añadido que permite que el intercambio de información sea completamente seguro y fiable, y conocer con toda certeza la autoría de esta. Las cadenas de bloques pueden certificar el contenido o el bien que se genera y se transmite; qué persona, entidad, institución o dispositivo creó o envío qué; desde dónde, cómo y cuándo. Al aplicar la tecnología *blockchain* en el entorno corporativo, apostamos por el diseño de redes de confianza sobre las que se construyen las relaciones empresariales.

A muy grandes rasgos, se puede resumir que el caso de uso ideal de *blockchain* será uno que plantee algunas o todas las siguientes necesidades:

- Un repositorio de información compartido entre todas las partes implicadas.

- Más de una de las partes genera transacciones que requieren modificar los registros compartidos.
- No existe una confianza mutua entre los miembros de la red que realizan las transacciones.
- Existen uno o varios mediadores en el sistema que garantizan la confianza en el mismo.
- La dependencia o interacción de las transacciones es generada por las distintas entidades participantes.

El Foro Económico Mundial llevó a cabo un estudio de campo basado en entrevistas a ejecutivos del sector privado y a altos cargos de las Administraciones públicas, con el fin de definir cuáles son los motores de valor de las cadenas de bloques para las organizaciones.[11] Las conclusiones del ejercicio le han permitido diseñar un marco de valor de esta tecnología, que parte de tres dimensiones específicas de transformación del negocio: la mejora de la rentabilidad y de la calidad; el aumento de la transparencia en las operaciones, y, por último, la reinvención de los productos y procesos.

11. WEF (2019). *Building Value with Blockchain Technology: How to Evaluate Blockchain's Benefits.*

Marco de valor de *blockchain*

Dimensiones clave	Mejorando la rentabilidad y la calidad				Aumentando la transparencia entre partes		Reinventando productos y procesos	
Capacidades	**Automatización:** una red autovalidadora + contratos inteligentes permiten la autoejecución de las reglas de negocio		**Control:** control en el nivel de dato individual, máxima flexibilidad sobre qué dato se comparte y cómo		**Distribuida:** ninguna única entidad es propietaria de los datos, consenso aplicado a las transacciones y acceso compartido sin un punto de fallo central		**DAx (Decentralized Autonomus x):** las reglas transparentes predefinidas implican que nuevas iniciativas se pueden crear, aportando nuevos productos / servicios mediante un modelo descentralizado	
	Trazabilidad completa: se conoce la procedencia y el historial completo de cada nuevo dato añadido		**Seguridad:** los datos pueden ser encriptados y segregados al nivel de dato elemental impulsando la seguridad general de los datos		**Visión holística:** misma fuente de verdad; todos los usuarios ven la misma información a la que tienen acceso		**Identidad aumentada:** una combinación de capacidades con avances en identidad digital incrementan la seguridad y la confianza en la gestión de los datos personales del cliente	
	Velocidad / eficiencia: permite una transferencia de datos más rápida, agilizando tareas para optimizar la eficiencia de procesos, especialmente donde han desaparecido los intermediarios		**Evidencia de alteraciones:** las matemáticas y criptografía subyacentes permiten a los usuarios autorizados verificar que los datos no han sido alterados				**Tokenización y activos digitales:** los objetos físicos con una representación digital única verificada permiten garantizar su titularidad, su gestión y transferencia	
Generadores de valor	Auditabilidad	Cumplimiento	Gestión de datos	Seguridad de datos	Compartir datos	Resiliencia	Autenticación	Gestión de identidad
	Titularidad	Pagos	Automatización de procesos	Reconciliación	Transparencia	Confianza	Creación de marcadores digitales	Nuevos y mejorados productos y servicios
		Estandarización	Seguimiento y rastreo				Nuevas y ampliadas alianzas	

Fuente: WEF (2019). *Building Value with Blockchain Technology: How to Evaluate Blockchain's Benefits.*

La primera dimensión es la relacionada con la rentabilidad y la calidad en el negocio, y parte de los siguientes elementos para generar valor:

- Auditabilidad, pues *blockchain* permite registrar las transacciones realizadas en tiempo real y facilita su seguimiento y supervisión.
- Cumplimiento de las normativas, al facilitar la fluidez de los distintos procesos administrativos y garantizar la veracidad de todos los datos ofrecidos por la empresa.
- Gestión de los datos. Esta tecnología certifica la procedencia de los datos y su integridad —dado que no se puede alterar o falsificar—, y favorece su agregación y gestión, al poder ser compartidos por todas las partes implicadas en tiempo real.
- Seguridad de la información, gracias al sellado criptográfico de los bloques de la cadena.
- Titularidad. *Blockchain* permite conocer en todo momento la titularidad tanto de bienes físicos como de activos digitales.
- Pagos, por la capacidad de esta tecnología de mantener el registro de todo tipo de transacciones de forma automática.
- Automatización de procesos al aplicar algoritmos que ejecutan acciones sin intervención humana, como en el caso de los contratos inteligentes.
- Reconciliación. Las cadenas de bloques apoyan el ahorro de costes al reducir errores, la información duplicada o la existencia de desencuentros en la información que tienen distintas partes.
- Estandarización. Cuando varias organizaciones trabajan juntas en una red *blockchain* comparten lógica y flujos de negocio al compartir el acceso a los mismos datos, algo muy interesante en el caso de la integración vertical de sectores de actividad económica.
- Seguimiento y rastreo, una función que permite gestionar en tiempo real toda la cadena de valor de la empresa.

La segunda dimensión estratégica de las cadenas de bloques para la empresa, la transparencia entre partes, se articula en los siguientes elementos:

- Datos compartidos. Gracias a esta tecnología, los socios comerciales o partes de un negocio pueden compartir información en tiempo real, no solo asumiendo que es verídica, sino también conociendo su origen e historial de modificaciones.
- Resiliencia, pues mantener la información de la empresa en una red distribuida reduce los riesgos de daño y pérdida que conlleva un sistema centralizado y aislado.
- Transparencia, dado que todas las partes implicadas pueden acceder a los datos en tiempo real.
- Confianza, otorgada por el elevado nivel de seguridad de la información almacenada en una cadena de bloques.

Por último, la dimensión de reinvención de productos y procesos gira en torno a las siguientes propuestas de valor del *blockchain*:

- Autenticación. Mediante algoritmos criptográficos, se puede autenticar a un mismo usuario en distintas redes, aumentando la confianza en las redes y en los participantes.
- Gestión de la identidad. Las cadenas de bloques garantizan la identidad de los usuarios, simplificando la identificación de los distintos actores implicados en un proceso de negocio.
- Creación de mercado. *Blockchain* aumenta la confianza en los productos y servicios en los mercados digitales, incrementando las oportunidades de mercado.
- Nuevos y mejores productos y servicios digitales originados por las posibilidades que ofrece esta tecnología.
- Nuevas alianzas derivadas del aumento en la confianza en la información que otorgan las cadenas de bloques.

La utilidad real de esta tecnología

Durante la última mitad de la década pasada, *blockchain* conoció la explosión de una burbuja de expectativas, que, al desinflarse, trajo consigo cierta decepción sobre su potencial. La popularidad que habían adquirido entonces las criptomonedas —y en concreto bitcoin— presentaba las cadenas de bloques como la nueva revolución tecnológica que iba a trastocarlo todo. No obstante, su penetración en la economía resultó mucho más pausada de lo esperado, y esto generó una suerte de escepticismo sobre su utilidad real.

A medida que nos adentramos en la presente década, *blockchain* va mostrando cada vez más aplicaciones que pueden ayudar a optimizar el funcionamiento de las organizaciones y de los negocios. He aquí una serie de campos de aplicación de esta tecnología que ofrecen una muestra de su utilidad.

Facilitar los pagos. Los acelera, elimina intermediarios, incrementa la transparencia y disminuye los costes asociados a las transacciones. Se trata de un tema de especial relevancia en el caso de las remesas, dado que la tecnología de cadenas de bloques puede conseguir que la transferencia se adelante más incluso que las llevadas a cabo por medio de servicios como PayPal o TransferWise, que tardan días. También implicaría una reducción de costes, que el Banco Mundial estima que suponen de media un 6,5 %.[12]

Los pagos entre empresas podrían transformarse en transacciones en tiempo real, gracias a la tecnología *blockchain*. Una estimación postula que, en 2024, el 9,7 % de todos los pagos entre negocios se llevará a cabo por medio de *blockchain*, y, de hecho, agentes del sector como Visa y JPMorgan ya están desarrollando soluciones en este terreno.[13] Dentro del comercio minorista, también existen ini-

12. GlobalData (2021). *Blockchain. GDTMT-TR-S317.*
13. Insider Intelligence (2021). *Blockchain in Payments: A Grounded Look at the Emerging Use Cases for Blockchain in Payments with Real Potential.*

ciativas al respecto. Por ejemplo, Visa, Mastercard y PayPal tienen ya en marcha criptoprogramas de tarjetas de débito.

Las cadenas de suministro internacionales. Dada la complejidad de las relaciones entre los agentes que intervienen en el comercio internacional, la digitalización de las cadenas de suministro internacionales por medio de soluciones *blockchain* permite conocer en tiempo real la localización y el estado de las mercancías, aportando trazabilidad, eficiencia y transparencia al proceso logístico. La generación de ecosistemas fiables de intercambio de información entre los actores que intervienen provee a todos ellos de una visibilidad completa de situación, y los dota de mucha más flexibilidad y capacidad de reacción frente a los posibles incidentes que pueden tener lugar fuera del perímetro de acción de cada empresa (roturas de stock, retrasos en las operaciones portuarias, conflictos sociales o bélicos en ciertas zonas geográficas, etc.).

Compartir datos. La fiabilidad y seguridad de las cadenas de bloques para el tratamiento de la información las convierten en el canal ideal para compartir datos entre organizaciones, un tema que a menudo puede verse limitado por la falta de confianza mutua o de interoperabilidad de los sistemas informáticos. Un caso especialmente destacable es el cuidado de la salud, en que el hecho de poder compartir con absoluta seguridad entre centros sanitarios o entre facultativos de distintas especialidades los datos médicos de los pacientes, que son especialmente sensibles, es algo que impulsa la eficacia del sistema.

Servicios jurídicos y eficacia administrativa. La inmutabilidad de la información almacenada en una red de bloques garantiza el registro seguro y la custodia de evidencias electrónicas. En esta categoría de aplicaciones existen buenos ejemplos en los que *blockchain* se utiliza para salvaguardar la propiedad intelectual y la gestión de marcas, tanto mediante la creación de evidencias irrefutables, que permiten ser verificadas por terceros y con las que los propietarios legítimos puedan ejercer sus derechos sobre los activos protegidos, como en la implementación de las liquidaciones o pago de *royalties*

originados por el uso autorizado de estos, mediante contratos inteligentes (*smart contracts*). Igualmente, se muestran de mucha utilidad en el seguimiento de contratos, la trazabilidad de información confidencial o para dotar de transparencia a servicios tales como canales de denuncias, portales de transparencia o adjudicaciones públicas, entre otros.

Servicios financieros. Como ya se ha descrito anteriormente, uno de los usos más extendidos del *blockchain* es en las criptodivisas, que son la base de una nueva generación de servicios financieros digitales, bautizada como *fintech*. Dentro de todo este nuevo escenario, destacan las finanzas descentralizadas, comúnmente conocidas como *DeFi*, que constituyen una forma experimental de actividad financiera que no depende de intermediarios financieros centrales —como corretajes, plataformas de intercambio o bancos— para ofrecer instrumentos financieros tradicionales y que, en cambio, utilizan para ello contratos inteligentes basados en la tecnología de las cadenas de bloques.

Tókenes no fungibles. Los *non-fungible tokens* (NFT) son certificados de autenticidad de activos digitales. Aunque todavía no está muy claro su potencial, pueden desempeñar un papel importante en el mercado del arte o del intercambio de piezas únicas de internet, como, por ejemplo, el primer tuit publicado en Twitter, que fue vendido como NFT por 2,9 millones de dólares en marzo de 2021.[14]

Identidad digital descentralizada. Se entiende por identidad digital el conjunto de toda la información de un usuario de internet (como, por ejemplo, su documento de identidad, carné de conducir, certificados académicos o registros sanitarios, entre otros) que se encuentra digitalizada. Al aplicar *blockchain* en este campo, se garantiza, a través de la tecnología, que dicha información digital es veraz y que ha sido generada y certificada por un emisor válido.

14. Vega, G. (2021). «El primer tuit de la historia, vendido por 2,9 millones de dólares», en *El País*. 23 de marzo.

España ha sido pionera en este terreno, pues en enero de 2021 se estableció el marco de referencia para la gestión de identidades descentralizadas (DID) con tecnología *blockchain*, que constituyó el primer estándar oficial desarrollado en el mundo sobre este tema. Su gran ventaja es que son los individuos, y no terceras partes, quienes crean y gestionan la identidad, gracias a la descentralización de las cadenas de bloques.[15]

También la Comisión Europea apuesta por la implementación de este concepto como base de la futura identidad digital europea. Esta identidad será la base para nuevos servicios no solo de autenticación e identificación de los ciudadanos ante las administraciones públicas y empresas privadas, sino también de intercambio seguro de datos personales entre organizaciones para simplificar procesos de *onboarding* digital, ofrecer servicios personalizados o agilizar ciertos trámites administrativos (liquidación de tributos, atestaciones, poderes de representación, etc.).[16]

Procedencia. Las cadenas de bloques permiten garantizar el nivel de calidad de los bienes y servicios, su autenticidad, en el caso de objetos de lujo o con denominación de origen, y si cumplen con los requisitos sanitarios o medioambientales que pregona su vendedor. En España ya hay grandes empresas que aplican esta tecnología. Por ejemplo, las Bodegas Emilio Moro han implementado el *blockchain* para proporcionar toda la información acerca de la parcela de viñedo de procedencia de la uva, así como los datos relativos a su recorrido y sus circunstancias para acreditar que cumple las exigencias de control y certificación de producto que requiere la obtención del sello Denominación de Origen Ribera del Duero.[17] Igualmente, en el ámbito del jamón serrano, Navidul, empresa perteneciente a Cam-

15. Felguera, E. (2021). «España aprueba el primer estándar mundial sobre identidad digital descentralizada en *Blockchain*», en *Think Big*.
16. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en
17. Quirós, F. (2020). «Aplican *blockchain* para certificar la Denominación de Origen de vinos». Cointelegraph.

pofrío Food Group, utiliza *blockchain* para ofrecer, a través de una aplicación de lectura de códigos QR en el teléfono móvil, la información veraz, completa e inmutable suministrada por todos los proveedores que participan en la producción de cada pieza, como, por ejemplo, la alimentación del cerdo, dónde se ha curado su peso o la fecha de consumo preferente.[18]

El contrato inteligente y la automatización de acciones

Una de las funcionalidades especialmente interesantes para el negocio y, en general, las relaciones entre organizaciones es el contrato inteligente (*smart contract*). A pesar de su nombre, no son exactamente contratos ni conllevan el uso de tecnologías de inteligencia artificial. El código, en este caso, no tiene por qué ser un contrato legal, puede ser simplemente una programación sin implicaciones contractuales.

Realmente se trata de programas informáticos que se autoejecutan sin la intervención de terceros cuando tiene lugar una condición previamente establecida, siguiendo una estructura lógica del tipo: «si... entonces...» (por ejemplo, «si se entregan los bienes X, entonces se libera el pago de fondos»). El concepto de contrato inteligente fue creado por el criptógrafo Nick Szabo en 1994, y fue introducido en *blockchain* por Ethereum en 2015. Hoy en día, muchas cadenas de bloques ofrecen este tipo de servicio, y en ellas asumen las propiedades de la infraestructura subyacente, como la descentralización o la resistencia a la manipulación.

Una particularidad de los *smart contracts* es que pueden nutrirse de información externa, provista por fuentes ajenas a las partes implicadas, que actúa como catalizador de una acción concreta a emprender. Estos puentes entre *blockchain* y el mundo exterior se

18. Financial Food (2021). *Navidul estrena las primeras paletas ibéricas con tecnología blockchain.*

conocen como oráculos (*oracles*). A modo de ejemplo, un contrato inteligente de seguros puede recibir datos relativos a la temperatura en el interior de un contenedor refrigerado, de forma que, si el sensor detecta una subida por encima de cierto nivel, el contrato se ejecuta automáticamente, y podría liberar pagos al asegurado o enviar una inspección para ver qué ocurre. Es por ello que los contratos inteligentes suelen combinar *blockchain* con otras tecnologías, como puede ser el internet de las cosas.

Un campo de aplicación del *blockchain* y los contratos inteligentes es la financiación del comercio internacional. En el caso de las pymes, el proceso puede ralentizarse y complicarse por la necesidad de las entidades financieras de validar la información asociada a la operación. Los *smart contracts* permiten la necesidad de confianza entre las partes, dado que las acciones se ejecutan automáticamente cuando las circunstancias se producen. Por ejemplo, la plataforma we.trade está integrada por doce bancos europeos y tiene por objeto conectar a compradores, vendedores y entidades financieras a través de contratos inteligentes sobre *blockchain*.[19] Reduce notablemente el riesgo del crédito al asegurar que hasta que una parte no lleva a cabo sus obligaciones establecidas en el contrato, este no autoriza automáticamente los pagos.

Otro ejemplo puede ser su utilización en la gestión de la cadena de suministro, cuando esta está integrada por numerosos proveedores. En ellas, el estatus y la localización del bien va cambiando en cada fase de producción, y con los *smart contracts* todos los participantes en la cadena pueden rastrearla, y, además, automatizar acciones rutinarias y los pagos, evitando retrasos debidos a la comunicación a través de documentos.

También en el sector inmobiliario, los contratos inteligentes pueden acelerar las transferencias de titularidad en las ventas de activos, de forma que estos pueden cambiar el propietario de un inmueble automáticamente una vez que el vendedor realiza el pago.

19. https://www.ibm.com/blog/we-trade-provides-intelligent-trading-solution/

La empresa Propy realizó en 2017 la primera transacción de inmuebles mediante *smart contract*, en concreto, un apartamento en Ucrania.

4. CASOS DE USO DE LA TECNOLOGÍA DE CADENA DE BLOQUES

Después de un lento despegue, el *blockchain* va paulatinamente llegando a numerosos sectores del tejido productivo en forma de aplicaciones y casos de uso. Como hemos podido ver, su utilidad estuvo inicialmente relacionada con las criptomonedas, pero sus ventajas desde el punto de vista de la seguridad y de la trazabilidad de las transacciones hacen de ella una solución ideal para cualquier tipo de actividad basada en un ecosistema de interrelaciones de distintas partes. Cada vez aparecen más casos de uso de esta tecnología, pero se pueden resaltar los siguientes como los más relevantes en la actualidad.

Gestión de las cadenas de suministro

Se trata de uno de los ejemplos más citados por expertos y analistas de esta tecnología. La internacionalización y globalización de las cadenas de suministro, unidas a las tensiones en el escenario geopolítico que han tenido lugar en los últimos años, exigen tener un control total de la cadena de suministro para garantizar la continuidad de las operaciones, especialmente en el caso de las grandes cadenas intercontinentales.

Blockchain supone una solución de seguridad —gracias a su inmutabilidad—, además de una herramienta de transparencia para garantizar la supervisión de cada activo a lo largo de todo el recorrido (productos finales, lotes o componentes y partes por separado). Un buen caso de uso de gestión de la trazabilidad de equipos es el de

la empresa brasileña Vivo, la operadora local del grupo Telefónica, que desde 2018 gestiona el equipamiento doméstico del cliente (rúters y descodificadores) desde que los componentes llegan a la fábrica donde se ensamblan hasta la activación del equipo por el instalador en el domicilio. En la actualidad, esta solución gestiona once millones de equipos anualmente, incluyendo en la cadena a más de cincuenta agentes, entre almacenes propios y de terceros, subcontratas de distribución o los más de 18.000 instaladores.[20]

Industria alimentaria y denominación de origen

Una variante del ejemplo anterior es la aplicación de *blockchain* a la cadena de producción agroalimentaria, de forma que queden acreditados todos los insumos incorporados en un producto dado, y, además, se data sin posibilidad de ser cuestionada cada etapa en el proceso de elaboración. De este modo, la producción agroalimentaria puede ser trazada y el consumidor recibe todo tipo de garantías sobre el origen del producto, los procesos de fabricación, los diferentes medios de transporte hasta el punto de venta o sus componentes. Esto resulta muy relevante cuando se trata de productos *premium* o exclusivos, ya sea por su origen (denominaciones de origen o zonas geográficas protegidas), por su composición (productos ecológicos o artesanales) o por cualquier otra característica (series limitadas, bienes de lujo, etc.).

Otra aplicación de este tipo de trazabilidad acreditada se basa en ofrecer garantías de las condiciones de conservación de un producto —por ejemplo, alimentos frescos, congelados o productos farmacéuticos—, para los que la temperatura u otras condiciones como la humedad o la luminosidad deben mantenerse dentro de unos umbrales determinados durante todas las fases del transporte y el almacenamiento desde la fábrica hasta el punto de venta.

20. https://www.blockchaineconomia.es/telefonica-lanza-su-blockchain-en-brasil/

Este tipo de trazabilidad a través de *blockchain* ya se aplica en la pesca del atún. La plataforma de Code Contract ofrece la posibilidad de integrarse en los sistemas de las compañías pesqueras para poder coordinar desde un solo lugar las diferentes fases del proceso —desde la captura del pez hasta su descarga portuaria— sin necesidad de modificar aspectos técnicos en su metodología existente, con lo que facilita la interoperabilidad de los corresponsables de la cadena, que pueden compartir todos los documentos de una forma rápida y segura. Las empresas atuneras Albacora y Pevasa forman parte de este proyecto.[21]

Titularidad de la propiedad intelectual

Una cadena de bloques puede registrar —y convertir en inmutable— cualquier tipo de archivo, no solamente contenido multimedia (vídeo o audio) o documentos ofimáticos (texto, pdf, hojas de cálculo...), sino también archivos comprimidos que contengan, por ejemplo, el código de un programa informático. Es por ello que *blockchain* es una plataforma idónea para acreditar la integridad del contenido digital, y permitir en todo momento verificar qué está registrado previamente, la persona que lo registró y la huella digital de los cambios que pueda haber sufrido, por ejemplo, el traspaso de los derechos asociados. De alguna forma, esta tecnología asume la función del notario, pues certifica la titularidad de la propiedad intelectual.

De forma similar, su utilidad se extiende a otras situaciones, como puede ser garantizar la trazabilidad de información confidencial y detectar posibles fugas, la recogida y verificación de evidencias digitales, o, en el marco de la comunicación, certificar el origen y la autenticidad de una noticia en los medios digitales o en un boletín informativo.

21. https://alastria.io/trazabilidad-y-automatizacion-de-la-cadena-de-suministro-pesquera/

Certificación de obras de arte

Esta tecnología puede ayudar a combatir el fraude en el mercado del arte, gracias a que aporta trazabilidad y transparencia a las obras. Por una parte, la creación de registros distribuidos ofrece evidentes ventajas en materia de protección y registro, y como medio de prueba, ya sea en la fase de registro o en los tribunales. Por la otra, prescinde de intermediarios, pues es el propio artista quien registra su obra y sigue su trazabilidad en su ciclo de vida.

Ya existen experiencias en este sentido, como es el caso de la empresa DigitArt, que utiliza los certificados Pukkart y que ha creado para los diferentes operadores del mercado del arte un entorno para registrar de forma totalmente segura y fiable la autoría, propiedad y trazabilidad de las obras, tanto plásticas como digitales. De esta forma, se emite un certificado digital, haciendo uso de *blockchain*, y un certificado impreso tradicional, pero reforzado con los mecanismos propios de la tecnología de las cadenas de bloques.

Formación y titulaciones profesionales

La posibilidad de acreditar con cadenas de bloques títulos educativos y credenciales profesionales es una forma de asegurar que la información presentada en un currículum es absolutamente cierta. Se puede convertir en la solución idónea para las agencias de colocación y los departamentos de recursos humanos de las empresas, pues permite acceder de forma rápida a todo el historial académico de un candidato y confiar en su veracidad. Cualquiera puede verificar que la información no ha sido manipulada ni alterada, sin tener que acudir a la institución que emitió el título o la credencial para validarlo. Estas funciones no son aplicables solo al campo de la educación y la formación, sino también a cualquier sector en el que un dato concreto deba ser acreditado y verificado por terceros.

Existe una aplicación específica en el sector del deporte, en el que resulta crucial poder verificar que los datos deportivos son au-

ténticos, para que no haya errores o fraude en los logros de los deportistas. En este sentido, el servicio SportChain permite a los usuarios autogestionar sus atestados de credenciales deportivas como tarjetas verificables en formato digital mediante un monedero criptográfico en su teléfono móvil. Las credenciales son firmadas por la organización deportiva o quien corresponda, como si fuera una declaración jurada, y se utiliza un *blockchain* para hacer posible la verificación de dicha credencial.[22]

Un gobierno digital y abierto

Los sistemas descentralizados de información almacenada en bloques pueden traer consigo ventajas evidentes para el funcionamiento del sector público, en concreto, al reducir el coste económico, el tiempo de ejecución y la complejidad de los intercambios de información, tanto dentro de la propia Administración y sus distintos departamentos como entre esta y las empresas y los ciudadanos. Por otra parte, la desintermediación que supone el uso de este tipo de tecnologías puede contribuir en la disminución de la carga burocrática, actuar contra el poder discrecional que ostentan determinados cargos y evitar la posibilidad de que ese poder los lleve a incurrir en prácticas de corrupción.

Las cadenas de bloques fomentan la transparencia en la información pública y su auditabilidad, contribuyendo al objetivo de desarrollar un gobierno abierto. Por último, el uso de algoritmos para el mantenimiento de registros públicos les quita ese monopolio a los poderes públicos, y puede reforzar la confianza de ciudadanos y empresas en el sector público.

En España, el Gobierno de Aragón fue pionero en este campo, pues utiliza tecnología *blockchain* para controlar el proceso de licitación de obras públicas a través de una plataforma electrónica que

22. https://alastria.io/sportchain-servicio-que-pretende-aportar-transparencia-seguridad-y-eficiencia-a-la-industria-del-deporte/

facilita el registro distribuido de ofertas y evaluación automatizada de estas en procedimientos de contratación pública electrónica.

Más recientemente, el Ayuntamiento de Las Rozas (Madrid) puso en marcha una solución basada en *blockchain* para dotar de una mayor seguridad y trazabilidad a los procesos de contratación de proveedores que está llevando a cabo el consistorio.

Por su parte, a mediados de 2019, el Departamento de Políticas Digitales y Administración Pública de la Generalitat de Catalunya lanzó la Estrategia *Blockchain* de Catalunya, un ambicioso plan que tiene por objeto desplegar esta tecnología en distintos ámbitos de la Administración. El programa de actuaciones de la Estrategia *Blockchain* de Cataluña se estructura en torno a seis grandes ejes que se mencionan a continuación.[23]

- Administración: mejorar los servicios públicos mediante la adopción de las tecnologías *blockchain* y DLT.
- Promoción: posicionar Cataluña como referencia en *blockchain* y DLT dentro del mapa tecnológico internacional y difundir las oportunidades y el impacto que genera su despliegue.
- Innovación: impulsar la investigación y la innovación mediante los centros de investigación y tecnológicos, y desarrollar entornos de innovación para su adopción en distintos sectores productivos.
- Ecosistema: potenciar una nueva industria en torno a la tecnología *blockchain* y DLT y dinamizar la demanda de servicios y soluciones asociados a sectores verticales prioritarios.
- Talento: generar, retener y atraer talento, tanto tecnológico como emprendedor, con los conocimientos y las capacidades necesarias para el desarrollo de esta nueva industria.

23. https://smartcatalonia.gencat.cat/ca/projectes/tecnologies/detalls/article/estrategia-blockchain-de-catalunya

- Regulación: analizar las implicaciones que tiene la regulación sobre el despliegue de esta tecnología y también cómo se regulan las aplicaciones que utilizan.

Impulsando los videojuegos

Los juegos digitales, ya desde hace tiempo, no son actividades solitarias acotadas al entorno del ordenador personal —como en los años 80 y 90—, sino experiencias compartidas con otros, asociadas a un ecosistema de jugadores en red. Un videojuego *blockchain* es aquel que tiene lugar —completamente o en parte— sobre una cadena de bloques. La actividad del juego aparece como el conjunto de transacciones realizadas entre los nodos de la red, y cada jugador se convierte en un nodo de esta.

De esta forma, las cadenas aportan dos formas de valor a los juegos: por un lado, ofrecen la posibilidad de intercambiar activos digitales entre los distintos juegos, y por el otro, permiten realizar trueques de dichos activos entre los jugadores. En otras palabras, se trata de transformar al usuario pasivo del juego tradicional —que se limita a seguir las normas de una estructura cerrada— en una suerte de propietario de elementos digitales (armas, tierras, unidades monetarias, avatares...) que tienen un valor dentro del ecosistema de los juegos, y que pueden ser enajenados.

El *blockchain* puede empoderar al jugador y mejorar sustancialmente su experiencia en el juego. Por una parte, se trata de una herramienta para garantizar la propiedad de los activos digitales de cada jugador, y en su caso, certificar su transacción. Pero, por la otra, también es eficaz para evitar que nadie realice trampas en las partidas y para que el juego funcione como se espera, sin cambios imprevistos, puesto que la transparencia que otorga esta tecnología impide en gran medida la manipulación. Por último, diferentes videojuegos creados sobre una misma *blockchain* pueden establecer conexiones entre sí de otra forma imposibles de realizar. Esto permite, por ejemplo, que un jugador que ha terminado un juego co-

mience a jugar en una secuela de este o en otro similar, conservando todas las características y los activos digitales que ha ganado en el primero.

Dentro de la nueva generación de videojuegos *blockchain* destaca Decentraland, un mundo digital en el que los usuarios pueden comprar parcelas con la criptomoneda MANA. La ciudad tiene 90.000 parcelas que miden diez metros cuadrados, en las que los jugadores pueden edificar todo lo que quieran.

Periodismo y medios de comunicación

La caída de los ingresos publicitarios y la dificultad para monetizar una oferta en línea de información han obligado a los medios de comunicación a buscar desesperadamente nuevas fuentes de financiación. Después de más de dos décadas de ensayos, todavía no se perfila en el horizonte un único modelo de negocio universal, como los que existieron antaño. Cada cierto tiempo surgen nuevos formatos, nuevos canales de comunicación y nuevas formas de ofrecer el contenido, pero no parecen proponer un sistema de ingresos sólido. Y los medios que todavía se aferran a soportes tradicionales, como el papel, aún tienen una tarea de reinvención importante por delante.

La tecnología de la cadena de bloques puede tener sus aplicaciones dentro del periodismo digital. A grandes rasgos, se pueden plantear los siguientes casos posibles: micropagos a través de *blockchain* para apoyar pequeñas publicaciones, criptomonedas para financiar proyectos periodísticos y el trabajo de los periodistas, o, también, plataformas de noticias sobre *blockchain*.

Un proyecto pionero en este campo fue Civil, pero sus creadores, The Civil Media Company, lo cerraron en 2020. Sin embargo, han surgido otras plataformas de periodismo basadas en la tecnología *blockchain*, como Popula, Publiq o la holandesa Publicism.

Protección del medio ambiente

ClimateTrade es una plataforma web que hace uso de *blockchain* para lograr que empresas y consumidores puedan encontrar el lugar donde compensar su huella de carbono y también invertir en productos financieros verdes para impulsar aquellas tecnologías y los proyectos disruptivos que tienen como objetivo mitigar el cambio climático.

Básicamente, consiste en un ecosistema que une a los desarrolladores de proyectos de mitigación con empresas y consumidores sin intermediarios. Los inversores conocen de forma rápida y completa el destino de su dinero y obtienen toda la información sobre el proyecto. Según los responsables de la iniciativa, el valor añadido es la descentralización del mercado de carbono, que permitirá a las empresas poder compensar sus emisiones un 30 % más barato de una forma totalmente transparente y, a los individuos, participar en este mercado, algo que resultaba antes inaccesible para ellos.

Las aplicaciones de esta tecnología son inimaginables y trascienden los límites de sectores y actividades concretas. A modo de ejemplo de su potencial, un informe de GlobalData sugiere toda una batería de aplicaciones a sumarse a las descritas anteriormente en este capítulo.[24]

Sector aeroespacial y defensa

- Gestión de la cadena de suministro: mejorar la planificación y el suministro de armamento y componentes.
- Gestión de operaciones en el campo de batalla: asegurar las operaciones de comando y control.
- Enjambres de drones: mejorar la toma de decisiones en un enjambre.

24. GlobalData (2021). *Blockchain. GDTMT-TR-S317.*

Textil y moda

- Cadena de suministro sostenible: dirigirse al consumidor concienciado.
- Autenticidad: proteger la propiedad intelectual y evitar las falsificaciones de productos.
- Trazabilidad de regalías: gestionar las licencias de los diseños y marcas registradas, y rastrear el pago de regalías.

Automoción

- Micropagos: realizar el pago basado en el uso efectivo de vehículos.
- Viajes compartidos descentralizados: deshacerse de los intermediarios.
- P2P Marketplace: crear mercados de confianza de coches usados y piezas.

Banca y pagos

- Pagos transfronterizos: reducir el número de intermediarios y acelerar las transferencias, los pagos y las remesas.
- Gestión de identidad: simplificar el proceso de «conozca a su cliente».
- Liquidación de valores: quitar intermediarios y acelerar las liquidaciones.

Construcción

- Contratos inteligentes: eliminar intermediarios, ahorrar tiempo y resolver de disputas.
- Procedencia: aportar la certificación de materiales y diseños para cumplir con los niveles de calidad.
- Modelado de la información de los edificios: crear un rastro de auditoría del proceso de diseño.

Consumidor

- Procedencia: saber la fuente o el origen sostenible.
- Pagos y micropagos: realizar el pago basado en el consumo.
- Gestión de inventarios: crear un sistema de gestión proactivo.

Servicio de comida

- Procedencia: conocer la trazabilidad, fuente u origen sostenible.
- Seguridad alimentaria: rastrear el inventario fraudulento o contaminado.
- Comida sobrante: rastrear partidas de comida sobrante desde la recogida hasta la donación.

Cuidado de la salud

- Gestión de datos: habilitar a los individuos para que controlen sus informes médicos digitales.
- Trazabilidad de medicamentos: prevenir la falsificación y la caducidad de medicinas.
- Compartir datos: mejorar y agilizar el intercambio de datos clínicos o de los pacientes.

Seguros

- Gestión de partes: facilitar el procesado de los partes de forma transparente.
- Registros: realizar la trazabilidad de la propiedad de elementos de gran valor y garantías.
- Seguros P2P: seleccionar el fondo de seguros y compartir el riesgo.

Minería

- Trazabilidad de activos: realizar la trazabilidad de materiales en la cadena de valor de la minería.
- Procedencia del mineral: resolver problemas relacionados con el origen de los minerales.
- Comercio de materias primas: utilizar contratos inteligentes para automatizar los procesos manuales.

Medicina

- Monitorización remota de pacientes: asegurar y proteger los datos recogidos por dispositivos IoT.
- Trazabilidad de la cadena de suministro: realizar la trazabilidad de dispositivos médicos acabados y de partes dentro de las facturas de materiales.
- Desarrollo de productos: gestionar los documentos del registro maestro del dispositivo y el archivo de historial de diseño.

Petróleo y gas

- Gestión de la cadena de suministro: realizar la trazabilidad de materiales en bruto y productos para el control de calidad.
- Trazabilidad de la huella de carbono: regular y reportar la trazabilidad de sustancias.
- Gestión de flotas: monitorizar las métricas y la localización de las flotas.

Empaquetado

- Empaquetado sostenible: realizar la trazabilidad y el rastro de materiales a lo largo de la cadena de valor.

- Autenticidad: resolver las preocupaciones del consumidor en relación con la autenticidad y el origen de los productos.
- Empaquetado inteligente: prevenir la falsificación de productos y favorecer el uso de los materiales más adecuados para envolver cada producto.

Farmacia

- Pruebas clínicas: mejorar la calidad y fiabilidad de los datos de pruebas clínicas.
- Trazabilidad de las cadenas de valor: reducir el fraude y la falsificación de medicamentos.
- Gestión de inventarios: gestionar las cantidades en inventario para prevenir picos de demanda.

Energía

- Comercio de energía P2P(*peer-to-peer*): vender la energía sobrante.
- Financiación medioambiental: gestionar el comercio de créditos de carbono y certificados de energía renovable.
- Gestión de la carga de vehículos eléctricos: usar contratos inteligentes para pagar directamente por la energía utilizada.

Comercio minorista

- Autenticidad: proteger la propiedad intelectual y prevenir la falsificación de productos.
- Procedencia de productos: garantizar la seguridad alimentaria y dirigirse a los consumidores concienciados.
- Programas de fidelización inteligentes: usar contratos inteligentes para automatizar los beneficios.

Deporte

- Tókenes para fans: implicar a los fans en la toma de decisiones de los clubes.
- Coleccionables digitales: facilitar la compra y venta de recuerdos de los partidos y de los equipos participantes.
- Sistemas de venta de entradas: prevenir la falsificación de entradas.

Tecnología, medios y telecomunicaciones

- Almacenaje de datos P2P (*peer-to-peer*): permitir que cualquiera pueda almacenar, retirar y albergar información digital.
- Redes sociales: proteger los datos de los usuarios y darles el control sobre su información.
- Trazabilidad de regalías, propiedad intelectual y derechos de autor: licenciar marcas registradas y realizar la trazabilidad de los pagos de regalías.

Viajes y turismo

- Servicios de identificación: reducir los tiempos de registro (*check-in*) con identidades de viajero conocidas.
- Reembolso: realizar el reembolso automático a través de contratos inteligentes por retrasos de los vuelos o extravío de equipajes.
- *Marketplaces* de contratación P2P (*peer-to-peer*): conectar a los consumidores directamente con los proveedores de productos o servicios.

5. EL *BLOCKCHAIN* EN ESPAÑA

El impulso institucional de la Comisión Europea

La Comisión Europea apuesta por *blockchain* como una tecnología que tiene el potencial de revolucionar cómo compartimos la información y cómo llevamos a cabo transacciones digitales, gracias a que genera una confianza en los datos de forma inédita hasta ahora. De esta forma, la Unión Europea tiene en marcha una estrategia relacionada con las cadenas de bloques, que persigue favorecer su implementación a partir de una infraestructura regulatoria basada en los valores y los ideales europeos. El estándar *blockchain* europeo deberá incluir los siguientes principios:

- Sostenibilidad medioambiental y eficiencia energética.
- Protección de datos y privacidad.
- Consonancia con la política comunitaria de identidad digital.
- Ciberseguridad.
- Interoperabilidad con los sistemas dentro y fuera de la Unión Europea.

Una de las primeras acciones emprendidas es la implementación de la European Blockchain Services Infrastructure (EBSI), una red en la que participan los 27 estados miembros, el Reino Unido, Liechtenstein y Noruega, cuyo objetivo es la prestación de servicios públicos transfronterizos en el ámbito de la Unión Europea.[25]

25. https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure

En la primera etapa del proyecto, se han seleccionado los siguientes cuatro casos de uso:

- *European Self-Sovereign Identity Framework* (*ESSIF*), iniciativa orientada a la implementación de una capacidad genérica de identidad autónomamente gestionada, que permita a los ciudadanos crear y controlar su propia identidad de forma transfronteriza, sin tener que confiar en autoridades centralizadas.
- *Diplomas*, una línea de trabajo que persigue devolver a los ciudadanos el control de la gestión de sus credenciales educativas, con lo que se reducirán de forma significativa los costes de verificación y se incrementará la confianza en su autenticidad.
- *Notarización*, cuya finalidad es aprovechar la potencia de *blockchain* para crear pistas digitales confiables de auditoría, automatizar las comprobaciones de cumplimiento en procesos donde las fechas resultan sensibles y certificar la integridad de los datos.
- *Intercambio fiable de datos*, destinado a fomentar el empleo de las cadenas de bloques para intercambiar con garantías determinados datos entre las aduanas y las autoridades tributarias competentes.

En el marco de EBSI, la Comisión Europea ha puesto en marcha una iniciativa para la creación de un *sandbox* regulatorio o espacio de prueba para casos innovadores de aplicación de *blockchain* y, en general, de las tecnologías de contabilidad distribuida (DLT). El *sandbox* europeo de *Blockchain* pretende ser un canal de diálogo entre los reguladores y los innovadores tanto del sector público como del privado, en el que los nuevos desarrollos de esta tecnología son probados y validados en un entorno seguro antes de su salida al mercado.

Dentro del ámbito de la legislación, uno de los hitos más relevantes fue la aprobación, en abril de 2023, de una nueva regulación para

los mercados de criptoactivos, conocida como el reglamento MiCA (*Markets in Crypto Assets*). En concreto, la normativa pretende regular la emisión, la oferta al público y la negociación de criptoactivos, a los que dota de una definición común y específica.

El programa Europa Digital es el marco en el que se engloban actualmente la mayor parte de las iniciativas innovadoras de la Comisión Europea. El programa proporciona financiación estratégica para responder a los grandes retos y apoya la creación y el desarrollo de expertos digitales cualificados.

Entre las iniciativas recientes, se puede destacar CHAISE, financiada por el programa Erasmus, que constituye una alianza de habilidades sectoriales para desarrollar un enfoque estratégico sobre la generación de habilidades de *blockchain* para Europa, así como ofrecer nuevas soluciones de capacitación para el futuro, con el fin de abordar la escasez de habilidades en este campo y prepararse para responder a las necesidades futuras de la fuerza laboral europea en relación con el aprovechamiento de oportunidades derivadas del uso de las cadenas de bloques (https://chaise-blockchainskills.eu/es/).

Una de las principales preocupaciones de la Comisión Europea es interactuar con el sector privado, el mundo académico y la comunidad *blockchain*, para lo cual utiliza la Asociación Internacional de Aplicaciones de Blockchain de Confianza (INATBA), una asociación público-privada diseñada para promover el ecosistema *blockchain* en Europa. INATBA promueve la interoperabilidad de las tecnologías *blockchain* y el buen gobierno, y actúa como interlocutor de gobiernos y organismos internacionales.

Otra herramienta importante de coordinación entre organismos es el European Blockchain Observatory and Forum, que facilita el diálogo entre los tomadores de decisiones, los líderes de opinión y la comunidad *blockchain*. Es un proyecto piloto financiado por el Parlamento Europeo con el objetivo de reunir experiencia para identificar y monitorear iniciativas y tendencias de *blockchain* a nivel mundial para crear una fuente completa y disponible públicamente de

conocimiento que apoye el ecosistema de *blockchain* dentro de la Unión Europea y que mejore la comprensión de esa tecnología, sus aplicaciones y los ecosistemas en los que pueden ser especialmente relevantes.[26]

Según la página web del observatorio, entre sus objetivos se encuentran: «trazar un mapa de iniciativas clave en Europa y fuera de ella; supervisar la evolución, analizar las tendencias y abordar las nuevas cuestiones; servir como un centro de conocimiento global en *blockchain*; crear un foro atractivo y transparente para compartir información y opiniones de expertos; promover a los actores europeos, fomentando al mismo tiempo el compromiso con la comunidad mundial de cadenas de bloques; representar una gran oportunidad de comunicación para que Europa exponga su visión y ambición en la escena internacional; inspirar acciones comunes basadas en casos de uso específicos; formular recomendaciones sobre el papel que podría desempeñar la Unión Europea en la aceleración de la innovación y la adopción de cadenas de bloques.»

El observatorio cuenta con su propia página web (https://www.eublockchainforum.eu/) e interactúa con la comunidad de diferentes maneras: talleres, un mapa interactivo de *blockchain*, grupos de trabajo, informes y un foro en línea.

Avance relativo del *blockchain* en España

Entre los temas previos necesarios para el desarrollo de las cadenas de bloques, se puede mencionar el lanzamiento del 5G como infraestructura de telecomunicaciones con innovaciones tecnológicas que facilitan el lanzamiento y el desarrollo de nuevos servicios. El Plan Nacional 5G para el período 2018-2020 ya mencionaba como princi-

26. https://digital-strategy.ec.europa.eu/es/policies/eu-blockchain-observatory-and-forum

pales aplicaciones de las nuevas infraestructuras las comunicaciones ultrafiables y de baja latencia, en torno a 1 milisegundo (ms) frente a 20-30 ms propios de las redes 4G. Y las considera especialmente apropiadas para nuevas aplicaciones que tienen requerimientos específicos. Entre estas aplicaciones innovadoras, se menciona el vehículo conectado o el vehículo autónomo, servicios de telemedicina, sistemas de seguridad y control en tiempo real y la fabricación inteligente.

También menciona ese plan las comunicaciones masivas tipo máquina a máquina (M2M). «Se incrementará la capacidad para gestionar una gran cantidad de conexiones simultáneas, lo que permitirá, entre otras cosas, el despliegue masivo de sensores, el internet de las cosas (*Internet of Things*, IoT) y el crecimiento de los servicios de *big data*.»[27]

En España, las empresas y otras organizaciones han empezado a comprender la importancia que *blockchain* puede tener para optimizar los diferentes procesos digitales de negocio, y esto ha comenzado a manifestarse por medio de la inversión en esta tecnología, como parte de las distintas iniciativas de digitalización. Las cadenas de bloques se consolidan como la línea de innovación corporativa susceptible de añadir un estrato de integridad y trazabilidad necesario para cualquier estrategia centrada en el dato.

El ecosistema *blockchain* español presenta un dinamismo relevante, y su desarrollo se encuentra en un estadio intermedio al ser comparado con los de otras naciones de Europa. En un estudio publicado en 2020, la consultora PwC predijo que en 2030 *blockchain* será responsable de haber provocado un aumento del PIB español de 24.000 millones de dólares, y de la creación de un total de 227.000 puestos de trabajo.[28]

El observatorio y foro de Blockchain de la Unión Europea clasifican el grado de desarrollo de cada estado miembro en función de

27. https://avancedigital.mineco.gob.es/5G/Documents/plan_nacional_5g.pdf
28. PwC (2020). *Time for trust. The trillion-dollar reasons to rethink blockchain.*

dos variables: el grado de madurez del ecosistema *blockchain* y el avance de la legislación existente sobre esta tecnología.

De esta forma, el desarrollo del marco legislativo se clasifica en tres niveles:

1. No existe legislación específica en el país hasta el momento que regule los criptoactivos.
2. Existe cierto compromiso con las cadenas de bloques a través de una legislación más amplia, pero que hace referencia a los criptoactivos, o estudios o proyectos piloto sobre *blockchain* impulsados por el gobierno.
3. Existe una legislación específica sobre *blockchain* o los criptoactivos, y el gobierno ha anunciado una estrategia nacional al respecto.

Paralelamente, la madurez del ecosistema *blockchain* también presenta tres estadios, clasificados en función de tres variables: presencia de un ecosistema local de negocios o *startups*; existencia de un número significativo de iniciativas de educación formal o investigación académica relacionadas con *blockchain*, y número significativo de comunidades de usuarios en torno al *blockchain* o los criptoactivos. Así surge la siguiente clasificación:

1. Países donde se da uno o ninguno de los tres factores.
2. Países donde se dan por lo menos dos de los tres factores.
3. Países donde se dan los tres factores.

El resultado de combinar estos dos parámetros es una matriz 3x3 en cuyas celdas se van clasificando los distintos países en función de su grado de desarrollo *blockchain*, que constituye una forma muy visual e intuitiva de comparar los resultados nacionales.

Madurez del ecosistema	Madurez regulatoria: Nivel I	Madurez regulatoria: Nivel II	Madurez regulatoria: Nivel III
Nivel I		Lituania Países Bajos Eslovenia	Chipre Reino Unido Estonia Suiza Francia Malta
Nivel II	Bélgica Eslovaquia Dinamarca Suecia Irlanda	Austria Liechtenstein Finlandia Letonia Italia España Portugal	Alemania Luxemburgo
Nivel III	Croacia República Checa Grecia Hungría Rumanía Noruega	Polonia Bulgaria	

Fuente: EU *Blockchain* Observatory and Forum (2022) *EU Blockchain Ecosystem latest developments - Version2022*.

Como queda patente en el gráfico del Observatorio Blockchain de la Unión Europea, nuestro país ocupa una posición intermedia entre los países de Europa en cuanto al desarrollo y despliegue de esta tecnología, situándose en el segundo nivel tanto en términos de madurez del ecosistema como en el de la regulación. En concreto, compartimos el mismo grado de avance en esta materia con naciones como Austria, Finlandia, Letonia, Italia y Portugal.

El informe destaca el interés tanto de la Administración como del tejido empresarial español por las cadenas de bloques, y fija el año 2018 como el momento clave en el que comienza con fuerza su despliegue. Específicamente, menciona cómo las iniciativas comenzaron a florecer en el sector privado, sobre todo en los sectores de la banca, la energía y la logística. En 2022, existían más de 200 compañías dedicadas a *blockchain* en España, y establece que el 2,3 % de la población muestra interés por esta tecnología.[29]

Uno de los aspectos más destacables del ecosistema *blockchain* español es la oferta de formación que ha surgido en torno a esta tecnología en el ámbito de la educación superior. De esta manera, tanto las universidades como los centros de formación y las escuelas de negocios ofrecen programas académicos que cubren un amplio abanico de temas —incluyendo algunos de nicho—, entre los que se incluyen los contratos inteligentes, la figura de la organización autónoma descentralizada o DAO, criptografía, regulación y fiscalidad o política monetaria.

Como ejemplo de lo anterior, se pueden destacar las siguientes titulaciones disponibles en diversos centros universitarios:

- Universidad de Alcalá: Máster de formación permanente en Blockchain, Smart Contracts, y Criptoeconomía.
- IEBS Digital School: Máster en Blockchain y Fintech.
- Universitat de Barcelona: Global Master's in Blockchain Technologies.
- EU Business School/Universidad Católica de Murcia/University of Roehampton: MBA in Blockchain Management.
- Universidad del País Vasco: Máster propio en bitcoin y tecnología blockchain.

29. EU Blockchain Observatory and Forum (2022). *EU Blockchain Ecosystem latest developments - Version2022.*

- Universidad Europea de Madrid: Postgrado de experto universitario en Fintech.
- Universidad Cardenal Herrera (CEU): Certificate in Fintech and Cryptoactive.

El apoyo y la difusión en España

El ecosistema del *blockchain* y de las tecnologías DLT crece a paso firme en nuestro país gracias al impulso que recibe por parte de los poderes públicos y la iniciativa privada, desde distintos frentes.

En 2020 y como respuesta a la crisis sanitaria, el Gobierno de España puso en marcha la Agenda España Digital, una hoja de ruta para la transformación digital del país para aprovechar plenamente las nuevas tecnologías y lograr un crecimiento económico más intenso y sostenido, rico en empleo de calidad, con mayor productividad y que contribuyera a la cohesión social y territorial. España Digital 2026 es la actualización de la estrategia, que incorpora dos nuevos ejes transversales referidos a los Proyectos Estratégicos para la Recuperación y Transformación Económica (PERTE) y a la iniciativa RETECH, una red de proyectos estratégicos emblemáticos transformadores en el área digital propuestos por las comunidades autónomas. A finales de 2022, el Gobierno anunció los once primeros proyectos emblemáticos de transformación digital seleccionados dentro del programa RETECH, y entre ellos figuraba la propuesta Infraestructura para Red Española de Blockchain, o la construcción de una red tecnológica de ámbito nacional basada en la tecnología de las cadenas de bloques. Estará coordinada por la Comunidad de Madrid y participarán Asturias y las Islas Canarias.[30]

Desde el punto de vista normativo, la Ley 11/2021, de lucha contra el fraude fiscal, contempla por primera vez la tributación de las criptodivisas, a las que denomina «moneda virtual». En concreto,

30. https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2022/141222-programa-retech-proyectos.aspx

se establecen obligaciones de suministro de información a la Administración tributaria referidas a la tenencia y operativa (adquisición, transmisión, permuta, transferencia, cobros y pagos) de monedas virtuales, y, además, se incluyen en la declaración de bienes y derechos en el extranjero.[31]

Por otro lado, España fue pionera en la creación del primer estándar mundial de identidad digital descentralizada vía *blockchain*. La Asociación Española de Normalización, UNE, publicó en 2020 la Norma UNE 71307-1 Tecnologías Habilitadoras Digitales. Modelo de Gestión de Identidades Descentralizadas sobre *Blockchain* y otras Tecnologías de Registros Distribuidos. Parte 1: Marco de referencia. Se trata del primer estándar mundial sobre gestión de identidades digitales descentralizadas, basado en *blockchain* y las tecnologías de registro distribuido (DLT), lo que supone todo un hito para nuestro país. La Norma española UNE 71307-1 contempla una serie de conceptos y procesos básicos de gestión descentralizada de la identidad, con el propósito de que los sistemas tecnológicos que los soporten puedan cumplir con los pertinentes requisitos empresariales, contractuales y regulatorios. En concreto, la nueva normativa define un marco de referencia genérico para la emisión, la administración y el uso descentralizados de aquellos atributos que faciliten la identificación de personas u organizaciones, permitiendo la creación y el control de la propia identidad digital de forma autogestionada, sin la necesidad de recurrir a autoridades centralizadas.

Otro gran hito español es la creación de un *sandbox* —incluido en la Ley para la transformación digital del sector financiero aprobada en 2020—, que no es otra cosa que un espacio de pruebas controlado y no desregulado que identifica nuevos proyectos *fintech* para mejorar la prestación de servicios financieros, con unos protocolos de supervisión que conocerán todas las partes implicadas. Este espacio de pruebas no persigue probar ideas, sino proyectos en fase de ma-

31. https://www.boe.es/boe/dias/2021/07/10/pdfs/BOE-A-2021-11473.pdf

durez, que hagan uso de una tecnología ya preparada para probarse en el mercado con clientes reales.

En suma, se trata de garantizar que los productos innovadores de empresas digitales no causen perjuicios no esperados en el mercado financiero o en los activos de los inversores. Un *sandbox* es un espacio de pruebas regulatorio en el que las *fintech* e *insurtech* (seguros) que se encuentran en estados iniciales de proyectos innovadores pueden emprender su actividad, bien bajo la modalidad de exención, para las que podrían situarse bajo el paraguas regulador con la normativa actual, bien bajo la modalidad de no sujeción, para quienes aún no están expresamente regulados precisamente por su carácter innovador. El *sandbox* financiero español presentó su primera convocatoria en 2021, y a ella se presentaron 67 empresas. Desde entonces y hasta 2023 ha cerrado cinco cohortes.

Sin duda, el mayor apoyo que ha recibido la difusión de *blockchain* en nuestro país ha sido la creación en 2017 de Alastria, un consorcio destinado a impulsar el uso de esta tecnología por parte del tejido productivo. Se trata de una red de más de 500 socios entre grandes empresas, pymes, *startups*, entidades del sector público, asociaciones y académicos de las universidades y las escuelas, como son las universidades y las escuelas de negocios. Alastria actúa como *hub* de conexión entre los diferentes actores, facilitando espacios para la participación y la cocreación de plataformas, recursos, estándares y guías relacionadas con las tecnologías DLT.

6. TENDENCIAS DE FUTURO

La tecnología basada en las cadenas de bloques va penetrando con paso firme en cada vez más sectores del tejido productivo. Aunque en principio parecía acotada a los criptoactivos, sus prestaciones en términos de seguridad y de trazabilidad de las transacciones la convierten en una potencial aplicación para cualquier actividad que implique un esquema de relaciones entre distintas partes. Como se ha explicado anteriormente, una de las ventajas más destacables de *blockchain* es la transparencia, puesto que toda la información es compartida por todos los usuarios de la red, pero también es crucial la descentralización física que conlleva, ya que elimina el riesgo de que al fallar un nodo crítico —por ejemplo, al sufrir un ciberataque— se venga abajo todo el sistema.

No obstante, la adopción masiva de esta tecnología llevará su tiempo. La consultora Gartner, en su informe sobre las expectativas de *blockchain* de julio de 2022, subrayaba que todavía no ha aparecido una «aplicación estrella» (*killer app*) que pueda garantizar que se alcance una masa crítica de usuarios.[32] Con todo, Gartner reconoce que estamos asistiendo a mejoras graduales en el uso de las cadenas de bloques. Por ejemplo, menciona aplicaciones corporativas en sectores como el mantenimiento de aeronaves o la seguridad alimentaria, que hacen uso de tókenes que representan activos del mundo físico y que son gestionados por contratos inteligentes.

La curva de Gartner es una herramienta que expone gráficamente el grado de implantación de una tecnología dada, y el tiempo previsto para que alcance la denominada «meseta de la productivi-

32. Litan, A. (2022) *Gartner Hype Cycle for Blockchain and Web 3, 2022.*

dad», es decir, una rentabilidad real en el mercado. El modelo aplicado a *blockchain* en julio de 2022 situaba tres aplicaciones en la «rampa de la consolidación», que es la fase previa a la rentabilidad. En el caso de las criptodivisas y de los monederos *blockchain*, el periodo para llegar a la meseta de la productividad sería inferior a dos años, mientras que las aplicaciones descentralizadas tardarían entre dos y cinco años.

Igualmente, la curva de Gartner establece un periodo de entre dos y cinco años para temas como los contratos inteligentes, las plataformas *blockchain* o los tókenes no fungibles (NFT), pero, en otros casos, se espera que la llegada de su rentabilidad se retrase hasta entre cinco y diez años, como es el caso de la tokenización de actividades o la gestión descentralizada de la identidad.

La evolución futura de la tecnología es incierta, aunque el momento actual ya permite predecir una serie de tendencias que pueden cobrar importancia, como el *blockchain* como servicio, los tókenes no fungibles (*Non Fungible Tokens*), la Web 3 o la convergencia con otras tecnologías, como el internet de las cosas (IoT) o la inteligencia artificial.

Blockchain como servicio (BaaS)

El concepto «como servicio», muy extendido en tiempos recientes, hace alusión a distintas modalidades de contratación de servicios informáticos por parte de empresas a terceros, e implica que la corporación cliente deja de administrarlos por su cuenta, y los delega en un proveedor especializado. La modalidad más conocida y extendida es la de *software* como servicio (*Software-as-a-Service*), puesto que es ampliamente usado por las compañías, pero también por particulares, por ejemplo, cuando hacemos uso de recursos de almacenamiento en red «como Google Drive o Dropbox —y de herramientas, como el correo electrónico— Gmail» o una *suite* de trabajo en línea como Office 365 de Microsoft.

Algo más complejo es el concepto de infraestructura como servicio (*Infrastructure-as-a-Service*), en el que el cliente paga por disponer de los recursos —servidores, espacio de almacenamiento— y se encarga de la gestión y administración de su infraestructura, como ocurre con Amazon Web Services (AWS) o Microsoft Azure. Finalmente, en la plataforma como servicio (*Platform-as-a-Service*), lo que se ofrece es una plataforma para el desarrollo de aplicaciones de la cual el cliente no tiene control sobre la gestión o el mantenimiento. Un ejemplo de esto es Google App Engine, en la que los desarrolladores pueden crear sus aplicaciones en Java o Python.

En el campo de las cadenas de bloques, ha aparecido el *blockchain-as-a-service* (BaaS), el *blockchain* como servicio, una opción que ofrece a cualquier empresa o institución la capacidad de disponer de soluciones basadas en registros distribuidos sin la necesidad de realizar costosas inversiones en desarrollos tecnológicos propios. Se trata de un planteamiento que podría contribuir a extender la adopción de las cadenas de bloques y normalizar su uso entre las organizaciones.

La idea de *blockchain* como un servicio para ser ofrecido por un proveedor a terceras personas es algo relativamente reciente, pero ya se han sumado a ello algunos de los grandes nombres del sector, como Microsoft, Amazon o IBM. Estimaciones realizadas por *Fortune* calculan que el subsector de BaaS alcanzará un valor global de mercado en 2027 de 23.200 millones de euros, un crecimiento significativo, teniendo en cuenta que en 2019 la cifra no alcanzaba los 2.000 millones de euros.[33]

Esta modalidad ofrece prestaciones en la nube para que las organizaciones usuarias desarrollen sus propias soluciones digitales basadas en esta tecnología. El proveedor es el encargado de instalar, mantener y almacenar las redes de cadenas de bloques de sus clientes, ofreciendo toda la tecnología necesaria a cambio de una cuota.

33. De Meijer, C. R. W. (2020). *Blockchain-as-a-service and SMEs: great opportunities* en *Finextra.*

De esta forma, el usuario no tiene que preocuparse de desarrollar la infraestructura informática para soportar su red, y se desentiende de temas como la actualización de los sistemas o la política y las estrategias de ciberseguridad.

Uno de los obstáculos para la adopción de las tecnologías de registro distribuido es la complejidad técnica que conllevan —tanto en la definición de un proyecto como en la instalación y el mantenimiento—, y, también, la inversión que requiere, no solo en sistemas, sino también en consumo energético y en garantizar que se dispone del inmenso ancho de banda necesario para su funcionamiento. El BaaS es una solución a estas cuestiones, y puede estimular el despegue a gran escala de esta tecnología entre las empresas y las instituciones.

Tókenes no fungibles

Los denominados tókenes no fungibles (del término inglés *non-fungible tokens* - NFT) son certificados de autenticidad de activos digitales registrados en cadenas de bloques. A pesar de su reciente burbuja de popularidad, todavía no queda muy clara su utilidad más allá del campo del arte o del intercambio de piezas únicas de internet.

Para comprender este concepto, baste saber que puede constituir un token no fungible una imagen, un gráfico, un vídeo, música o cualquier otro contenido de naturaleza digital sobre el que alguien quiera ejercer posesión. El elemento en cuestión queda registrado mediante un contrato inteligente que le asigna un número único, y, de esta forma, queda así identificado y diferenciado de posibles réplicas. El registro contiene los datos del propietario y del creador, lo que permite preservar por igual los derechos de autor.

El año 2021 tuvo lugar la explosión de los NFT, que comenzó con la subasta de la imagen en formato GIF de Nyan Cat, el gato volador, por más de 500.000 dólares. La primera referencia al respecto se

atribuye al artista Kevin McCoy con su obra *Quantum*, aunque quizás el ejemplo más notorio sea el del artista Beeple, cuyo collage digital se subastó el 11 de marzo de dicho año por 69 millones de dólares en la emblemática casa Christie's. También la NBA, la liga de baloncesto americana, llegó a subastar vídeos con las mejores jugadas, que alcanzaron precios que superan los 100.000 dólares.

Dos años después de esta fiebre, los NFT ya no ocupan titulares y parecen relegados al olvido, aunque quién sabe si serán el inicio de una aplicación de futuro de *blockchain*, más allá de su utilidad dentro del coleccionismo.

El *blockchain* de las cosas

La expresión internet de las cosas (IoT) fue utilizada por primera vez en 1999 por Kevin Ashton, del MIT, y hace alusión a la conexión de distintos objetos o dispositivos electrónicos o eléctricos a las redes. Estos pueden ser cualquier cosa susceptible de generar información y enviarla a través de internet, desde sensores y cámaras hasta *wearables*, termostatos, termómetros, altavoces inteligentes o instrumental para medir la calidad del aire de una ciudad, por poner unos pocos ejemplos. De acuerdo con IoT Analytics, a finales de 2021 había en el mundo 12,2 mil millones de dispositivos IoT, un 8 % más que en 2020. El informe de 2022 calculaba que esa cifra iba a crecer ese año un 18 %, hasta los 14,4 mil millones, impulsada por la superación de la crisis de los microchips.[34]

Una de las ventajas de incorporar *blockchain* al internet de las cosas es que afecta positivamente a la privacidad y la fiabilidad de la red. Las cadenas de bloques son capaces de efectuar el seguimiento de miles de millones de dispositivos conectados, permitiendo gestionar las transacciones y la coordinación entre ellos, con el consiguiente ahorro de costes.

34. IoT Analytics (2022). *State of IoT 2022*.

Igualmente, pueden mantener un registro inmutable de la historia de los distintos dispositivos inteligentes presentes en una red IoT, haciendo que funcionen sin la necesidad de que sean controlados por una autoridad central. *Blockchain* puede conseguir que la comunicación entre los distintos objetos y dispositivos sea segura y confiable, al igual que hace al registrar las transacciones que se producen en el marco de una criptodivisa.

Actualmente, los dispositivos conectados al internet de las cosas son altamente vulnerables ante los ciberataques. En 2019, un *malware* llamado Silex se propagó por las redes rápidamente borrando el *firmware* de cámaras de vigilancia, cerraduras, bombillas, termostatos, enrutadores, *webcams* y en general todos los productos conectados en el hogar o la oficina. En unas pocas horas, Silex fue capaz de neutralizar más de 4.000 elementos del internet de las cosas. Cuantos más objetos tenemos conectados en nuestras vidas, más vulnerables nos hacen. En general, la mayoría de estos dispositivos no cuentan con los estándares de autentificación necesarios para proteger adecuadamente los datos de los usuarios.

La tecnología *blockchain* puede reforzar los aspectos relativos a la seguridad del IoT. En primer lugar, es capaz de tener identificados y autentificados los dispositivos conectados. En el caso de los sensores, puede llevar un seguimiento de los datos y las mediciones realizadas y protegerlos frente a la manipulación. Además, puede garantizar de forma automática la transmisión de datos entre dispositivos, sin necesidad de que intervengan terceras personas para hacerlo.

Un aspecto importante es el de la resiliencia que las cadenas de bloques pueden otorgar a una red. En una *blockchain*, cada nodo guarda una copia completa de todas las transacciones que han tenido lugar en la red. De esta manera, ante un ataque que destruya parte de la red, toda la información sigue estando segura en los nodos supervivientes, algo que, aplicado al internet de las cosas, garantiza la fortaleza del sistema. Esto, no obstante, plantea unas necesidades de capacidad de procesado y de almacenamiento de información muy superiores.

Maridaje con la inteligencia artificial

No cabe duda de que una de las alianzas más prometedoras es aquella entre *blockchain* y la inteligencia artificial, la tecnología estrella por excelencia. De esta fusión surge el concepto de sistema descentralizado de inteligencia artificial, que es aquel que permite que el usuario procese la información a través de distintos dispositivos, encontrando soluciones a los problemas que un sistema centralizado no encuentra. Las cadenas de bloques tienen la capacidad para registrar todos los datos y las variables que influyen en la decisión tomada por un sistema inteligente basado en el aprendizaje automático (*machine learning*), haciendo posible rastrear cómo y por qué ha tomado tal decisión.

Uno de los grandes problemas que plantea la inteligencia artificial actual es que, a menudo, sus programadores y gestores no son capaces de explicar el proceso que ha seguido el algoritmo para llegar a una conclusión. Por ejemplo, el Hospital Mount Sinai de Nueva York utilizaba un programa basado en el aprendizaje profundo que ayudaba a los médicos a predecir enfermedades. Deep Patient —ese era su nombre— se nutría de una base de datos de 700.000 pacientes para aprender sobre dolencias, síntomas y hábitos, y, de hecho, demostró una gran eficacia para diagnosticar anticipadamente desórdenes mentales como la esquizofrenia, algo muy difícil de realizar para los psiquiatras. El problema es que nadie conseguía explicar cómo lo hacía, para poder aprender de él. *Blockchain* puede aportar trazabilidad al funcionamiento del algoritmo para identificar qué datos utiliza y cómo los utiliza a la hora de elaborar los patrones que guían su toma de decisiones.

Las ventajas de concatenar ambas tecnologías se pueden resumir en una serie de características que afloran de la unión:[35]

35. Turing. *The Future of AI and Blockchain Technology & How It Complements Each Other?*

- Fuente transparente de datos: el aprendizaje automático necesita alimentarse de grandes cantidades de datos para formarse, y el uso de *blockchain* para ello aporta transparencia y trazabilidad para conocer en todo momento el origen de la información utilizada.
- Sistema autónomo: las cadenas de bloques garantizan que la operativa de la inteligencia artificial no se concentra en un solo servidor, y que todo el proceso se realiza sin supervisión de manera descentralizada.
- Protección de la privacidad: las técnicas criptográficas refuerzan la privacidad a lo largo de la red que soporta el entrenamiento y las operaciones que realizan los algoritmos de IA.
- Poder de computación distribuido: *blockchain* ayuda a distribuir eficientemente la inmensa cantidad de capacidad de computación que requiere el funcionamiento de la inteligencia artificial.
- Seguridad: la inteligencia artificial puede optimizar el funcionamiento de los contratos inteligentes que se ejecutan a través de cadenas de bloques, reforzando su seguridad.
- Eficiencia lectora: las limitaciones de almacenamiento de información con frecuencia reducen la rapidez de respuesta de *blockchain*, pero la inteligencia artificial puede hacer más fluidos los procesos.
- Autenticidad: *blockchain* puede avalar la integridad y autenticidad de los datos que nutren a los algoritmos de aprendizaje automático.
- Escalabilidad: cuando una organización amplíe el uso de datos externos para alimentar sus sistemas de inteligencia artificial, *blockchain* contribuirá a hacer escalable el modelo, creando una economía de datos fiable y transparente.
- Automatización: el tándem entre inteligencia artificial y *blockchain* elimina las fricciones de los procesos y aumenta la transparencia, impulsando la automatización de las operaciones.

La Web 3: la evolución de internet

La nueva web que viene ya no correrá sobre plataformas digitales de servicios, sino sobre cadenas de bloques, que permitirán las relaciones directas entre usuarios sin intermediarios, y, según vaticinan algunos, traerá consigo la llegada de un internet más democrático. La denominada Web 3 asegura que el próximo internet estará en manos de las personas y las organizaciones, por lo que las grandes empresas tecnológicas no podrán imponer su poder como hacen ahora. En teoría, las características intrínsecas de *blockchain* garantizan un marco de relaciones entre usuarios en que estos mantienen el control y no existen intermediarios.

Uno de los principales cambios que llegarán con la nueva web es el principio filosófico sobre el que reposa la confianza de los usuarios. Hasta ahora los agentes que concurren en un medio como internet realizan sus intercambios del tipo que sean —información, bienes, servicios, monetarios...— con otros agentes, depositando su confianza en una figura o institución que garantiza esos intercambios. Las cadenas de bloques trasladan dicha confianza desde el agente que certifica que se van a cumplir las reglas del juego hasta la propia tecnología *blockchain*, que es la que se responsabilizará de la seguridad del sistema, evitando la intermediación.

Gavin Wood, el creador de la criptodivisa *ether* (ETH), inventó el término Web 3 en 2014, y resume su esencia en una frase sintética: «menor confianza, mayor verdad». Para él, la confianza constituye básicamente fe, la creencia ciega de que el mundo va a funcionar, pero sin una evidencia real o un argumento racional que lo justifique. En sus propias palabras: «la confianza implica que estás depositando algún tipo de autoridad en otra persona, o en alguna organización, y ellos pueden hacer uso de esta autoridad de una forma arbitraria». Y concluye: «queremos más verdad, a lo que realmente me refiero es a una razón de más peso para creer que nuestras expectativas se cumplirán».[36]

36. Edelman, G. (2021). *The Father of Web 3 Wants You to Trust Less* en *Wired*.

Una de las bases de *blockchain* son los tókenes o unidades de cuenta digitales, que se utilizan como soporte de las relaciones entre los diferentes agentes que intervienen en la red. De esta manera, tanto nuestra información personal —de la que ahora se benefician empresas como Facebook o Google— como otros activos digitales de nuestra propiedad, representados por tókenes, están registrados y protegidos en bloques de *blockchain*. Por lo tanto, cualquier operación que hagamos con ellos quedará igualmente registrada y protegida por la cadena de bloques de posibles alteraciones o manipulaciones.

A diferencia de lo que ocurre actualmente, los usuarios de la Web 3 son los dueños de sus datos personales, y son ellos y solo ellos los que deciden cuáles son necesarios compartir con los servicios de internet, tanto de los que definen su identidad como de los que son generados a través de las interacciones de las redes. En el futuro, todos ellos quedarán protegidos en *wallets* o monederos digitales personales y anónimos.

La gran esperanza es que la Web 3 transforme el marco de relaciones en internet, eliminando el papel de las plataformas, los servidores y la centralización de autorizaciones en la gestión de la información que circula por la red y de los flujos de valor que se generan entre los distintos agentes. La idea es que el usuario pueda navegar por un internet más libre y participativo, en el que todas las personas tengan un protagonismo específico y en el que sus manifestaciones digitales no constituyan materia prima para alimentar algoritmos que supongan la manipulación comercial o ideológica.

BIBLIOGRAFÍA

BBVA (2018). «¿Cuál es la diferencia entre una DLT y 'blockchain'?». Disponible en: https://www.bbva.com/es/innovacion/diferencia-dlt-blockchain/

BBVA (2023). «¿Qué es un 'token' y para qué se puede utilizar?». Disponible en: https://www.bbva.com/es/innovacion/que-es-un-token-y-para-que-sirve/

Becker, M., y Bodó, B. (2021). «Trust in blockchain-based systems». Internet Policy Review, 10(2).

BOE (2021). «Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, de transposición de la Directiva (UE) 2016/1164, del Consejo, de 12 de julio de 2016, por la que se establecen normas contra las prácticas de elusión fiscal que inciden directamente en el funcionamiento del mercado interior, de modificación de diversas normas tributarias y en materia de regulación del juego».

De Meijer, C. R. W. (2020). «Blockchain-as-a-service and SMEs: great opportunities» en *Finextra*.

Edelman, G. (2021) «The Father of Web 3 Wants You to Trust Less», en *Wired*. Disponible en: https://www.wired.com/story/web3-gavin-wood-interview/

Engineering. «Blockchain. Unchaining business through the Blockchain».

EU Blockchain Observatory and Forum (2022). «EU Blockchain Ecosystem latest developments - Version2022».

European Parliament (2022). «Intellectual Property Rights and Distributed Ledger Technology with a focus on art NFTs and tokenized art».

Ganne, E. (2018). «Can Blockchain revolutionize international trade?». World Trade Organization.

GlobalData (2021). «Blockchain. GDTMT-TR-S317».

Insider Intelligence (2021). «Blockchain in Payments: A Grounded Look at the Emerging Use Cases for Blockchain in Payments with Real Potential».

IoT Analytics (2022). «State of IoT 2022».

Litan, A. (2022). «Gartner Hype Cycle for Blockchain and Web 3, 2022». Gartner. Nota de prensa. Disponible en: https://www.gartner.com/en/newsroom/press-releases/2022-08-30-metaverse-web3-and-crypto-separating-blockchain-hype-from-reality

Marquit, M. (2022). «Proof of Work vs. Proof of Stake: Why the Difference Matters for Ethereum Investors» en *Next Advisor*.

McAfee (2018). «Informe sobre amenazas contra blockchain». McAfee. Disponible en: https://lopdcumplimiento.es/biblioteca/ENS%20Medidas%20Seguridad/Informes%20McAfee/Informe%20de%20McAfee%20sobre%20amenazas%20contra%20blockhain.pdf

Nakamoto, S. (2008). «Bitcoin: A Peer-to-Peer Electronic Cash System». Disponible en: https://bitcoin.org/bitcoin.pdf

PwC (2020). «Time for trust. The trillion-dollar reasons to rethink blockchain». PWC. Disponible en: https://www.pwc.com.cy/en/issues/assets/blockchain-time-for-trust.pdf

Turing. «The Future of AI and Blockchain Technology & How It Complements Each Other?»- en Turing. Disponible en: https://www.turing.com/kb/how-blockchain-and-ai-complement-each-other

Wiles, J. (2022). «¿Qué es la Web 3?». Gartner.

World Economic Forum (2019). «White Paper. Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction».

— (2019). «Building Value with Blockchain Technology: How to Evaluate Blockchain's Benefits».

Dentro de la ola actual de transformación digital, la tecnología *blockchain* se erige como una de las principales palancas de cambio. Aunque generalmente se la asocia al ámbito de las criptomonedas, su campo de acción trasciende las finanzas y su utilidad potencial alcanza prácticamente cualquier sector de actividad productiva. En cuestión de tiempo, el uso de las cadenas de bloques se extenderá a todo el espectro socioeconómico: desde la banca hasta la Administración pública, desde los contratos de alquiler o la gestión energética hasta las reservas turísticas. Al igual que ocurre con el protocolo TCP/IP, cuyo funcionamiento desconocemos, pero que rige todos nuestros movimientos por internet, los usuarios no «veremos» las *blockchains*, pero disfrutaremos de servicios cada vez más seguros y eficientes basados en ellas.

La filosofía de *blockchain* parte de que es un sistema que almacena la información en cadenas de bloques con el fin de evitar su modificación una vez publicado el dato. Los bloques ordenan la información temporalmente enlazando cada bloque con el anterior de forma que, para cambiar un dato cualquiera, habría que alterar todos los bloques precedentes; de ahí la poderosa seguridad que ofrece.

En un internet tan grande y diverso como el actual, las redes descentralizadas como *blockchain* serán la próxima base tecnológica del ciberespacio, puesto que permiten que los dispositivos inteligentes se comuniquen entre ellos mejor y más rápido.

Cuadernos de divulgación PUE

ISBN: 978-84-10202-39-9