santelmo
business school

SIIN-6

BLOCKCHAIN EN LA CADENA ALIMENTARIA: ¿EVOLUCIÓN, REVOLUCIÓN O ILUSIÓN?

***BLOCKCHAIN* EN LA CADENA ALIMENTARIA: ¿EVOLUCIÓN, REVOLUCIÓN O ILUSIÓN?**

Nota técnica de la División de Investigación de San Telmo Business School, España. Preparada por el profesor Jose Antonio Boccherini Bogert, para su uso en clase, y no como ilustración de la gestión, adecuada o inadecuada, de una situación determinada.

AGRADECIMIENTOS

Las actividades de formación e investigación del FOODepartment se desarrollan gracias a las aportaciones económicas de las Empresas Miembros del Consejo Asesor de dicho departamento, compuesto en mayo de 2022 por: AECOC, AGROSEVILLA ACEITUNAS, ALIA CAPITAL PARTNERS, ALSEA EUROPA, ANGULAS AGUINAGA, ÁREAS, AZTI, BOLTON FOOD ESPAÑA, BONDUELLE IBÉRICA, CAJA RURAL DEL SUR, CAMPOFRÍO FOOD GROUP, CAPSA FOOD (Central Lechera Asturiana), CARREFOUR ESPAÑA, CASALBOR, COCA-COLA EUROPEAN PARTNERS, CORTEVA AGRISCIENCE, COVAP, COVIRAN, DEOLEO GLOBAL SAU, E-LECLERC, EL POZO ALIMENTACIÓN, EUROPASTRY, FIAB, FRULACT, GONZALEZ BYASS, GRUPO CALVO, GRUPO EBRO FOODS, GRUPO LACTALIS, GRUPO LUIS SIMÕES, GRUPO SOVENA, IFA RETAIL, LANDALUZ, MAHOU SAN MIGUEL, MAKRO, MERCADONA, NESTLÉ ESPAÑA, NUEVA PESCANOVA, OSBORNE Y CÍA., RABOBANK, SAT ROYAL, UNICA GROUP, WILLIAMS & HUMBERT Y ZYRCULAR FOODS S.L.

BLOCKCHAIN EN LA CADENA ALIMENTARIA: ¿EVOLUCIÓN, REVOLUCIÓN O ILUSIÓN?[1]

La tecnología *blockchain,* aparecida en 2009 como soporte tecnológico de la moneda virtual bitcóin, ha sido calificada en los últimos años como la gran revolución que cambiará la economía y muchos negocios. Marc Andreessen, cofundador de Netscape e inventor del primer navegador web, calificó a bitcóin en 2014 (y a su tecnología subyacente, *blockchain*) como el invento tecnológico más importante desde la creación de internet en 1993. *The Economist* definió *blockchain* como "*la gran cadena para estar seguro sobre las cosas*" [2], y afirmó que "*la tecnología que da soporte a bitcóin permite a personas que no se conocen ni confían entre sí construir un registro confiable, y esto tiene implicaciones mucho más allá de la criptomoneda*".

¿PARA QUÉ HACE FALTA UNA TECNOLOGÍA COMO *BLOCKCHAIN*? [3]

Según el documento original que lo describió[4], "*Bitcóin es un sistema de dinero electrónico entre particulares (peer-to-peer) que permite hacer pagos en línea entre ellos sin tener que pasar por una institución financiera*". Es decir, bitcóin permite hacer transacciones económicas sin la intervención de un "intermediario de confianza". La tecnología *blockchain* se inventó para dar soporte a esta moneda electrónica. ¿Por qué era necesaria?

---

[1] Nota técnica de la División de Investigación de San Telmo Business School, España. Preparada por el profesor Jose Antonio Boccherini Bogert, para su uso en clase, y no como ilustración de la gestión, adecuada o inadecuada, de una situación determinada.

[2] "The great chain of being sure about things", The Economist, 31 de octubre de 2015, https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things (consultado el 10 de febrero de 2019).

[3] Este apartado es una adaptación de la explicación contenida en el documento "¿What is blockchain technology?", *CB Insights*, 11 de septiembre de 2018. El documento puede descargarse en https://www.cbinsights.com/research/what-is-blockchain-technology/.

[4] Nakamoto,S., "Bitcoin: a Peer-to-Peer Electronic Cash System", 31 de octubre de 2008, https://bitcoin.org/bitcoin.pdf, consultado el 11 de febrero de 2018. Satoshi Nakamoto es un pseudónimo. El documento fue publicado en una lista de correos por un programador o grupo de programadores que operaban bajo ese pseudónimo y que permanecen anónimos hasta la fecha.

Imaginemos que, en el mundo del dinero físico, Mario quiere hacer un pago a Julia de un euro. Mario entrega la moneda a Julia y la transacción se completa, de forma segura. Tras la transacción, Mario ya no posee la moneda y ahora la posee Julia. Mario y Julia no necesitan de un intermediario que verifique la transacción. Mario ya no podría entregar esa misma moneda a Laura para hacer otro pago, porque ya no la tiene. No existe la posibilidad de hacer un pago doble con la misma moneda y se garantizan las condiciones que proporcionan valor a la divisa: se puede certificar su propiedad y sigue siendo un activo escaso.

Pero ¿qué pasaría si esa moneda no fuera física, sino digital? Mario podría enviar la moneda digital a Julia por correo electrónico (por ejemplo) para hacer el pago. Entonces, Julia debería tener esa moneda digital y Mario no debería seguir teniéndola. Pero ¿qué ocurre si Mario guarda una copia de esa moneda digital antes de enviársela a Julia y la utiliza posteriormente para pagar a otra persona? Porque, en definitiva, una moneda digital no es otra cosa que una secuencia de ceros y unos; es, por tanto, fácilmente copiable. Si no se encontrase una solución a este problema, las monedas virtuales carecerían de valor y utilidad.

Si Mario y Julia están en posesión de la misma secuencia de ceros y unos ¿cómo podemos saber quién es el legítimo propietario de la moneda? Una posible respuesta es utilizar un registro digital (un *ledger*, en inglés) en el que se apunten las transacciones y que de fe en todo momento de quién es el legítimo propietario. Así, si Mario hiciera un pago a Julia, se anotaría en el registro que esa moneda ahora pertenece a Julia y ya no pertenece a Mario.

Pero ¿quién gestiona ese registro? No puede ser Mario, porque podría borrar el apunte de la transacción para decir que él es todavía el propietario de la moneda. Por razones similares, tampoco puede ser Julia. Una solución podría ser utilizar a un intermediario, una tercera parte (llamémosle Leonardo), en la que tanto Mario como Julia confiaran, que apuntaría la transacción y mantendría actualizado el registro.

De alguna forma, esto es lo que ocurre hoy en día con la mayoría de los pagos que se realizan por transferencia bancaria. El dinero es un apunte contable y, por tanto, digital. Una transferencia es simplemente una transacción electrónica que resta un importe de la cuenta de la persona que paga y lo suma a la cuenta de la persona que cobra. La transacción la realiza una tercera parte de confianza (el banco) que da fe de que el saldo de ambas cuentas es correcto. Hoy en día, la mayoría de las personas en los países con sistemas bancarios desarrollados confían en ellos.

Pero Leonardo (el intermediario de confianza en el que confían Mario y Julia) podría empezar a cobrar una comisión por su labor que ni Julia ni Mario están dispuestos a pagar; o Mario podría chantajear a Leonardo para que borrase la transacción y recuperar así su moneda digital; o Leonardo podría no ser tan confiable y querer robar la moneda, añadiendo una transacción falsa al registro para proclamar que Mario le ha entregado la moneda.

Es decir, ¿qué ocurre si Mario y Julia no quieren pagar comisiones al intermediario, o no se fían de él? Una posible solución sería distribuir copias del registro a todos sus amigos,

descentralizando la confianza. Como el registro es digital, todas las copias deberían sincronizarse y cualquier nueva transacción debería actualizarse en todas ellas de forma simultánea. Si una mayoría simple de los participantes manifiestan que la transacción es válida (es decir, que Mario es el legítimo propietario de la moneda con la que quiere pagar a Julia), se aprueba y se añade al registro.

Esto es lo que se conoce como un registro distribuido (*distributed ledger*, en inglés). Si Mario o Julia quisieran falsificar una transacción, tendrían que chantajear a la mayoría de los participantes o modificar la mayoría de las copias del registro, lo cual es mucho más difícil de hacer. Y Leonardo solo tiene una de las copias del registro; si la modificase para intentar robar la moneda, dejaría de ser igual a las demás copias y se detectaría la falsificación.

Cuantas más "partes de confianza" mantengan una copia del registro, más seguro y fiable será. El sistema, por tanto, permite construir confianza entre partes que no se conocen y que no son necesariamente fiables a título individual. Si más de la mitad de los participantes son honestos y fiables, la seguridad es absoluta. Pero incluso aunque no lo fueran, sería difícil que a todos les interesara falsificar el registro de la misma manera de tal forma que una falsificación fuera consistente en la mayoría de las copias y se diera por válida.

En el ejemplo anterior los participantes que guardaban una copia del registro eran "amigos" y, por tanto, relativamente fiables. Pero en bitcóin, el registro es totalmente público y cualquiera puede participar y mantener una copia. Por tanto, hay un riesgo mayor de participantes malintencionados y transacciones falsas.

La solución que ofrece bitcóin es recompensar a los participantes honestos y castigar a los malintencionados. Algunos participantes de la red de bitcóin (que se denominan "mineros") reciben incentivos para hacer el "trabajo sucio" de garantizar la integridad del registro. Cuando se añade una nueva transacción, los mineros compiten para encajar la transacción en la estructura del registro, resolviendo para ello un puzle matemático deliberadamente complejo que requiere un esfuerzo de computación enorme. El primero que resuelve el problema recibe, tras la comprobación de al menos el 51% de los mineros restantes, una recompensa en bitcoines. Dada la cotización que han llegado a alcanzar los bitcoines, esto supone un gran incentivo. De esta manera, se desincentiva a los falsificadores, porque grabar una transacción falsa exigiría un esfuerzo de computación ingente, un gasto enorme de electricidad y, por tanto, mucho dinero (bastante más del que se obtendría con la falsificación). Pero incluso si la red de bitcoines pudiera ser falsificada de forma asumible, el resultado sería el mayor desincentivo: el valor de la moneda acabaría cayendo en picado, con lo que la posible recompensa de los falsificadores se desvanecería.

¿QUÉ ES LA TECNOLOGÍA *BLOCKCHAIN*?

Blockchain (cadena de bloques), la tecnología que da soporte a bitcóin, tiene potencialmente muchas aplicaciones además de la criptomoneda. Permite crear

registros digitales de información (transacciones, eventos, contratos, etc.), distribuidos y descentralizados, seguros e inmutables, sin que para ello deba existir un intermediario o una autoridad central que certifique que la información registrada es fiable:

- **¿Qué se puede registrar en una cadena de bloques?:** cualquier información, pero está especialmente pensada para registrar transacciones entre dos o más partes (por ejemplo, un pago entre personas), contratos (por ejemplo, una compraventa de una casa), eventos (por ejemplo, la salida de un camión cargado con una determinada mercancía de un almacén) y otras informaciones similares. Cada pieza de información (transacción, evento, …) se graba en lo que se denomina un bloque.
- **Distribuido y descentralizado**: el registro no se almacena en ningún ordenador central, sino que se distribuye entre los ordenadores de la red, guardándose múltiples copias de este. No hay un propietario único. De esta forma, aumenta la seguridad porque si ocurriese una catástrofe no se perdería la información y, al mismo tiempo, se dificulta la alteración porque cualquier pirata que quisiera cambiar un solo dato del registro tendría que hacerlo en todas las copias distribuidas por la red.
- **Un registro seguro e inmutable***:* la tecnología *blockchain* ofrece un nivel de seguridad altísimo de que la información que se graba en ella no se puede modificar, alterar ni falsificar una vez grabada. El Anexo 1 presenta una explicación más detallada de los dos mecanismos principales con los que se consigue esta seguridad.
- **La confianza en que la información introducida es correcta y no ha sido alterada no se alcanza por la existencia de una autoridad central (un intermediario) que de fe de ello***.* Los registros habituales (por ejemplo, los registros notariales o los registros de la propiedad) están avalados por una autoridad central (el notario o el registro) que garantiza que la información es fiable y no ha sido alterada. Con la tecnología *blockchain*, la fiabilidad se obtiene por consenso entre los nodos de la red; cuando la mayoría de los nodos certifican que las comprobaciones de integridad son correctas. Es decir, la fiabilidad se alcanza sin que sea necesaria la existencia de un intermediario certificador de confianza, y se logra entre nodos que ni se conocen ni confían necesariamente entre sí.

En resumen, y esto es lo potencialmente revolucionario de la tecnología, una cadena de bloques permite a partes que no se conocen y no confían entre ellas, ponerse de acuerdo y alcanzar un consenso sobre una historia digital, sin necesidad de intermediarios.

CADENAS DE BLOQUES PÚBLICAS Y PRIVADAS

Las cadenas de bloques pueden configurarse de diferentes maneras. Así, según sea el acceso a los datos, se clasifican en cadenas públicas o privadas, y según los permisos, en cadenas con permisos o cadenas sin permisos:

- Cadenas públicas*:* cualquiera puede unirse a la red y acceder a la información —si bien, parte, o toda la información, puede estar cifrada y requerir que el propietario de la información facilite una clave para poder descifrarla y leerla. La red no es propiedad de nadie y reside en servidores públicos de una red (de forma similar a internet).
- Cadenas privadas*:* funcionan sobre una red privada de servidores y el propietario de la red decide a quien da acceso a la misma.
- Cadenas sin permisos*:* cualquier persona o entidad con acceso a la red (según sea pública o privada) puede crear nuevos bloques y procesar transacciones. Estas cadenas necesitan *tókenes nativos* (por ejemplo, una moneda virtual como bitcóin) que incentiven a los participantes a mantener la integridad de la cadena y proporcionen la seguridad necesaria (véase la explicación anterior en este documento).
- Cadenas con permisos*:* sólo una lista de participantes autorizados, con identidades conocidas, pueden añadir bloques y procesar transacciones. Generalmente, estas cadenas no requieren el uso de *tókenes* nativos para incentivar su integridad.

Combinando estas características pueden obtenerse cuatro tipos genéricos de cadenas de bloques:

- Cadenas públicas sin permisos*:* son las que más mecanismos de seguridad exigen, por su naturaleza. Están gobernadas por mecanismos complejos lo que las hace, en principio, poco escalables. Bitcóin es un ejemplo de cadena de bloques pública sin permisos.
- Cadenas públicas con permisos*:* son más seguras que las cadenas sin permisos y su escalabilidad es media.
- Cadenas privadas sin permisos*:* su naturaleza privada las hace, en principio, más seguras y, por tanto, necesitan mecanismos de seguridad menos complejos; son más escalables.
- Cadenas privadas con permisos*:* es el modelo más escalable de todos.

APLICACIONES DE *BLOCKCHAIN* MÁS ALLÁ DE BITCÓIN

Por sus características, la tecnología *blockchain* tiene aplicaciones potenciales más allá de las criptomonedas. Es sobre todo una tecnología de desintermediación, que permite a partes que no se conocen y que no necesariamente confían entre sí construir registros de eventos fiables y seguros. Además, un uso generalizado de una cadena de bloques en un sector establecería una infraestructura informática común entre todos los participantes que permitiría agilizar los intercambios de información, evitando los típicos problemas de intercambios de datos entre sistemas incompatibles. Algunas de sus posibles aplicaciones —la lista es meramente ilustrativa, no exhaustiva— son:

- Contratos inteligentes*:* contratos que permiten la ejecución de sus cláusulas de forma automática (por ejemplo, el pago de la compensación prevista en un seguro) sin intervención humana.
- Servicios financieros*:* pueden agilizar el procesamiento de las transacciones, especialmente pagos y transferencias interbancarias, reduciendo sus costes.
- Registros de la propiedad y notarías*:* se podrían construir registros públicos, fiables e inmutables, sin la necesidad de autoridades de verificación y certificación.
- Gestión y comercialización de servicios basados en propiedad intelectual*:* las cadenas de bloques podrían utilizarse para crear un registro público, permanente y transparente para poder hacer un seguimiento del uso y los pagos a creadores de contenidos (por ejemplo, músicos), que podría dar a dichos creadores más control sobre la distribución de sus obras, permitiéndoles incluso la comercialización directa sin necesidad de intermediarios.
- Creación de *marketplaces:* de igual manera, las cadenas de bloques podrían utilizarse para crear mercados abiertos de comercialización de bienes y servicios, de forma directa entre sus miembros, sin la necesidad de intermediarios.

BLOCKCHAIN **EN LA CADENA ALIMENTARIA**

Hasta la fecha, la aplicación de *blockchain* por la que se está apostando de forma más decidida en la cadena alimentaria está relacionada con la mejora de la eficiencia, la transparencia y la trazabilidad de la cadena de aprovisionamiento de productos e ingredientes alimentarios.

Los consumidores de alimentos en todo el mundo son cada vez más exigentes con los productos que consumen; esperan que los productores y detallistas den respuesta a un conjunto de demandas y requisitos cada más completo y complejo:

- Conocer el origen de los productos y cómo se han producido (mostrando una preferencia creciente por los productos locales).
- Garantías de que el producto y sus ingredientes han sido producidos y comercializados a lo largo de la cadena bajo condiciones de comercio justo, evitando situaciones de explotación —infantil o laboral—, maltrato animal y respetando el medio ambiente.
- Garantías sanitarias y de seguridad alimentaria.
- En el caso de los productos orgánicos y biológicos, seguridad de que no se han utilizado pesticidas u otros ingredientes y aditivos no ecológicos o modificados genéticamente.

Sin embargo, los consumidores no disponen de un mecanismo fiable para comprobar el cumplimiento de esos requisitos. Con frecuencia, las certificaciones alimentarias se han demostrado falsas o fraudulentas; resulta difícil conocer los detalles de la cadena de aprovisionamiento y si las etiquetas son incorrectas o incompletas.

Conscientes de estas demandas, los detallistas, fabricantes y productores de alimentos han redoblado los esfuerzos para ganar la confianza de los consumidores. Pero al mismo tiempo, la globalización del comercio de alimentos está generando cadenas de aprovisionamiento cada vez más complejas. Una pizza vendida en un establecimiento de EE.UU. puede tener ingredientes de muchos países y de varios continentes. También una pizza comercializada por una cadena de restaurantes con la misma receta puede tener diferentes proveedores para cada ingrediente, en función de la zona de comercialización o producción o de la época del año. Ante una alerta de seguridad alimentaria (por ejemplo, una infección por la bacteria E. Coli) es muy complicado averiguar de forma rápida y fiable su origen concreto e identificar qué productos están realmente afectados, lo cual obliga a los productores a realizar retiradas masivas de productos, en lugar de retiradas selectivas, con el consiguiente impacto en costes que ello supone.

Ante esta situación, ¿podría la tecnología *blockchain* proporcionar una solución?

En septiembre de 2018, tras experimentar problemas de contaminación en lechugas en la primavera de ese año, Walmart anunció que exigiría a sus proveedores de lechuga y espinacas que grabaran información detallada sobre sus productos en una *blockchain* desarrollada por IBM —por aquel entonces estaba en pruebas y se lanzó comercialmente un mes después con el nombre de *Food Trust*. Ello le permitiría obtener información individualizada de cada bolsa de espinacas y de cada lechuga.

Por las mismas fechas, Albert Heijn, la empresa holandesa de supermercados anunció que empezaría a utilizar *blockchain* para hacer que la cadena de producción de zumo de naranja fuera más transparente, en colaboración con su proveedor Refresco. Para garantizar la sostenibilidad del producto de marca propia de la cadena, los clientes podrían escanear un código QR en el envase de zumo que les facilitaría información detallada sobre la ruta de producción y manipulación de extremo a extremo, desde Brasil a los Países Bajos. El sistema almacenaría las certificaciones de calidad y sostenibilidad de los productores, así como información sobre las frutas mismas, incluido el período de cosecha y la intensidad de dulzura[5].

En noviembre, el minorista multinacional Carrefour anunció que usaría la solución *Food Trust* de IBM para rastrear pollos de corral en España y Francia, y que en 2022 ampliaría su uso para realizar el seguimiento de todas las marcas propias de Carrefour en el mundo. Al mismo tiempo, en Suiza, Gustav Gerig AG reveló que usaría la cadena de bloques de Ethereum para rastrear el atún. Y el gobierno de Corea del Sur anunció que comenzaría a rastrear la carne de res en enero de 2019; por su parte, la cadena

[5] Fuente: "Gigante holandés de supermercados adopta *blockchain* para hacer transparente la producción del zumo de naranja", *Cointelegaph,* https://es.cointelegraph.com/news/dutch-supermarket-giant-adopts-blockchain-to-make-orange-juice-production-transparent, consultado el 11 de febrero de 2019.

estadounidense de restaurantes de ensaladas Sweetgreen anunció que dedicaría parte de los 200 millones de dólares conseguidos en una ampliación de capital a desarrollar un sistema de rastreo de sus ingredientes basado en *blockchain*[6].

Para facilitar la adopción de la tecnología blockchain a los actores de la cadena alimentaria, IBM lanzó en octubre de 2018 la plataforma *Food Trust*, una cadena de bloques privada (es decir, propiedad de IBM y gestionada por esta empresa en sus servidores) que detallistas, fabricantes y proveedores podían utilizar para gestionar la trazabilidad y la transparencia en sus cadenas de aprovisionamiento. La plataforma incluía tres módulos:

- Trazabilidad: que permite rastrear de forma segura la ubicación y el estado de los alimentos, desde la granja hasta la tienda. Según IBM, los clientes de la plataforma pueden realizar la trazabilidad completa, desde la tienda a la granja en solo 2,2 segundos, siempre que los datos estén disponibles.
- Certificaciones: que permite a los usuarios subir, gestionar y compartir sus certificaciones y registros de inspección y calidad.
- Entrada y acceso a datos: que permite subir a la plataforma datos de los alimentos y compartirlos solo con los socios que necesiten conocerlos.

Según IBM, "*sus datos le pertenecen. Los datos son propiedad de la organización o compañía registrada que fuera propietaria de los datos antes de que se cargaran a IBM Food Trust. Los usuarios pueden establecer permisos que rigen qué datos se pueden ver y quién los puede ver […] Los datos cargados por un tercero son propiedad del propietario original.*" [7]

El uso de la plataforma de IBM se factura según un esquema de pago por uso y en su escalón más barato, para empresas pequeñas de menos de 50 millones de dólares, puede utilizarse a partir de 96,50 euros al mes.

En otro tipo de aplicación para la cadena alimentaria, las cuatro empresas de materias primas alimentarias más grandes del mundo (Archer Daniels Midland, Bunge, Cargill y Louis Dreyfus) se asociaron para digitalizar el comercio internacional de granos mediante el uso de tecnologías de *blockchain* e inteligencia artificial. El objetivo inicial era conseguir mayor eficiencia y reducir costes, automatizando los procesos de ejecución posventa de granos y oleaginosas, que se basaban en contratos en papel, facturas y pagos manuales que exigían un proceso muy costoso.

[6] Fuente: "Desde Corea del Sur a IBM Food Trust: cómo se utiliza *blockchain* en la industria alimentaria", *Cointelegaph,* https://es.cointelegraph.com/news/from-south-korea-to-ibm-food-trust-how-blockchain-is-used-in-the-food-industry, consultado el 11 de febrero de 2019.

[7] Fuente: IBM, https://www.ibm.com/es-es/blockchain/solutions/food-trust, consultado el 11 de febrero de 2019.

DUDAS E INCERTIDUMBRES: ¿SE HARÁN REALIDAD LAS PROMESAS?

La tecnología *blockchain* y sus posibles aplicaciones han generado en los últimos años una gran expectación, no exenta a veces de exageración y de un bombo publicitario excesivo. Un signo de esta expectación y del potencial que se anticipaba eran las grandes inversiones que se estaban realizando: en 2017, la financiación de fondos de capital riesgo para *start-ups* de *blockchain* ascendió a 1.000 millones de dólares[8].

A pesar de la expectación, algunos críticos señalaban que la tecnología, en ocasiones, se estaba "sobrevendiendo" y que aún era excesivamente inmadura.

Por ejemplo, algunas voces habían criticado el proyecto de Walmart para gestionar la trazabilidad de las lechugas sobre la *blockchain* de IBM. Un artículo de *The New York Times* recogía las siguientes afirmaciones[9]:

- *"Algunos críticos se preguntan hasta qué punto la tecnología blockchain es diferente de las viejas bases de datos online de toda la vida".*
- *"No soy capaz de entender de qué manera hacer este proyecto sobre blockchain lo convierte en mágico".*
- *"Creo que es sobre todo una acción de relaciones públicas para que estas empresas puedan venderse a sí mismas como los líderes del blockchain".*
- *"Se supone que las cadenas de bloques hacen posible mantener bases de datos actualizadas sin que una autoridad central se encargue de ello. Pero los datos de la cadena que quiere utilizar Walmart se almacenan en ordenadores de la nube de IBM, para ser utilizados por Walmart. Eso genera dudas sobre si el uso de una tecnología de base de datos distribuida como blockchain es ni siquiera necesaria".*
- *"La idea es buena pero la ejecución parece equivocada. IBM ha elegido una nueva tecnología que no necesita intermediarios y se ha establecido a sí misma como intermediario".*
- *"Una cadena de bloques puede capturar y registrar el registro digital de una caja de espinacas. Pero no puede garantizar que alguien no haya abierto la caja y haya cambiado las espinacas, sustituyéndolas por rúcula o por drogas ilegales".*

Con un escepticismo similar, la consultora McKinsey apuntaba algunas dudas y precauciones (aunque reconocía avances en algunas áreas) [10]:

[8] Fuente: Carson, B, Romanelli, G, Walsh. P y Zhumaev, A.; "Blockchain beyond the hype: What is the strategic business value?", *McKinsey Digital*, 19 de junio de 2018, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value, consultado el 11 de febrero de 2019.

[9] Fuente: "From Farm to Blockchain: Walmart Tracks Its Lettuce", *The New York Times*, 24 de septiembre de 2018, https://www.nytimes.com/2018/09/24/business/walmart-blockchain-lettuce.html, consultado el 11 de febrero de 2019.

[10] Fuente: Higginson, M, Nadeau M. C. y Rajgopal K; "Blockchain's Occam Problem", *McKinsey*, enero de 2019.

- *"Blockchain aún tiene que convertirse en el generador de cambios en las reglas del juego que algunos esperan. Una clave para extraer valor del uso de esta tecnología es utilizarla solo cuando es la solución más simple disponible".*
- *"A pesar de la cantidad de tiempo y dinero que ya se ha invertido, se han conseguido pocos resultados sustanciales".*
- *"Blockchain es una tecnología que está aún en su infancia, y que es todavía relativamente inestable, cara y compleja. Además, no está regulada".*
- *"La lógica de blockchain es que la información se comparta, lo cual requiere cooperación entre empresas y un gran esfuerzo para estandarizar datos y sistemas. Y entonces aparece la paradoja de la "coopetición"[11]: pocas empresas tienen suficiente motivación para liderar el desarrollo de una infraestructura que beneficiará a la industria en su totalidad".*
- *"Hay una sensación creciente de que blockchain es una solución aún poco entendida (y un poco tosca) en busca de un problema que resolver".*

¿Es la tecnología *blockchain* realmente tan revolucionaria como sus primeros defensores han anunciado? ¿Es, por el contrario, una tecnología simplemente interesante, que ayudará a mejorar algunos procesos de negocio, pero sin llegar a provocar una revolución?, ¿o es simplemente una ilusión que, al igual que muchas otras tecnologías que han despertado expectativas similares a lo largo de la historia, se desvanecerá con el tiempo y quedará relegada a unas pocas aplicaciones de nicho?

[11] Neologismo que hace referencia a la colaboración entre diferentes actores económicos que son además competidores.

ANEXO 1
MECANISMOS DE SEGURIDAD DE *BLOCKCHAIN*

La tecnología *blockchain* utiliza dos mecanismos para proteger la seguridad y la inmutabilidad de la información:

a) las técnicas criptográficas más avanzadas para codificar la información[12].

b) La cadena de bloques: cada bloque se **enlaza** con el anterior formando una cadena. Cuando se añade un bloque nuevo al registro, se almacena un código en el mismo, junto con la información y la fecha de la transacción. Este código, que se denomina *hash*, se genera automáticamente a partir del contenido del bloque anterior mediante un algoritmo establecido (y conocido por todos los nodos de la red) y depende del texto completo de dicho bloque. El *hash* tiene la propiedad de que, si se modificase un solo carácter del bloque precedente, el código que se generaría sería completamente distinto. De la misma manera, el bloque anterior se enlazó cuando se creó a su bloque precedente mediante otro *hash*; y así sucesivamente, formando la cadena que da nombre a la tecnología.

   Para entender de qué manera este mecanismo protege la inmutabilidad de la información, imaginemos que un pirata informático quiere alterar un registro (por ejemplo, el que contiene la compraventa de una determinada vivienda, cambiando el nombre del propietario), y modifica para ello el bloque que contiene esa información. Por la característica del *hash* descrita anteriormente, el código del bloque alterado ya no sería igual al que se almacenó en el bloque siguiente cuando se creó (el enlace que forma la cadena), y al hacerse una comprobación de integridad, se detectaría la inconsistencia descubriéndose fácilmente la manipulación. Por tanto, el pirata que quisiera modificar el contrato de compraventa tendría que modificar también el bloque siguiente, guardando en él el nuevo código *hash*. Pero entonces el código del siguiente bloque también cambiaría, al haberse modificado; y así, sucesivamente. Es decir, si el pirata quisiera modificar un bloque, tendría que cambiar toda la cadena de bloques, entera para que volviera a cuadrar, y tendría que hacerlo en todas las copias de la cadena de bloques distribuidas por toda la red… Esa acción sería excesivamente compleja y requeriría un esfuerzo de computación inmenso y un coste (por ejemplo, en electricidad) enorme, lo cual hace la alteración impracticable e inviable económicamente[13].

[12] No obstante, esta característica no es realmente diferencial de *blockchain*: la misma seguridad criptográfica se puede incorporar a cualquier base de datos.

[13] El siguiente dato permite hacerse una idea del nivel de esfuerzo necesario: el consumo de electricidad anual para la operación de la *blockchain* que da soporte al bitcóin equivale al consumo anual total de Irlanda.