

Blockchain actualmente es sinónimo de innovación y de estar a la última. En los últimos años 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. Otros se muestran más cautos y hablan de una burbuja de expectativas en torno a esta tecnología, que estaría a punto de estallar. Blockchain puede entrar en un largo invierno de entre cinco y diez años hasta ser capaz de demostrar su idoneidad y rentabilidad.

Blockchain, *cadena de bloques*, es uno de los términos *techie* más de moda de los últimos años. A pesar de ser un concepto intuitivamente difícil de entender, está muy presente en los discursos mediáticos y en las

agendas políticas, y se ha convertido en sinónimo de modernidad y de vanguardia tecnológica.

Algunos profetizan que llega para cambiarlo todo, como hizo internet en su día, y que, más allá de su aplicación en el campo financiero, pondrá cabeza abajo todos y cada uno de los sectores de actividad. Los usos previstos 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 nada queda fuera de su alcance.

Las expectativas que despierta esta tecnología son proporcionales a las inversiones que recibe: de acuerdo con McKinsey, en 2017 el capital riesgo dedicado a *startups* con productos o servicios blockchain ascendió a 1 000 millones de dólares. Por su parte, IBM ha gastado más de 200 millones de dólares en el desarrollo de aplicaciones de internet de las cosas (IoT) basadas en cadenas de bloques, y el sector financiero dirige anualmente hasta 1 700 millones a la experimentación en este campo.

Y, sin embargo, hay quien defiende que en la actualidad existe una burbuja de expectativas en torno a las cadenas de bloques que puede reventar en cualquier momento. Este punto de vista denuncia, entre otras cosas, la falta de iniciativas a gran escala basadas en esta tecnología que realmente pongan en evidencia su utilidad e importancia global. También se alega que todavía no aporta soluciones a problemas reales y que carece de propuestas sólidas de negocio. Finalmente, una barrera adicional a su difusión está relacionada con que técnicamente está muy verde aún.

Hoy en día, el valor práctico de blockchain se reduce a grandes rasgos a tres aspectos. El primero, la creación de aplicaciones de nicho para casos de uso en los que esta tecnología encaja a la perfección, principalmente, los que implican el uso de información para determinar la propiedad o la trazabilidad de algo.

Por otra parte, las cadenas de bloques sirven mejor a aquellos sectores de actividad que ya están estratégicamente orientados a la modernización. Aquí se convierte en una herramienta para digitalizar y simplificar procesos existentes. Un ejemplo podría ser el comercio internacional.

Finalmente, numerosas empresas se aferran a proyectos sobre blockchain como una forma de impulsar su imagen innovadora ante clientes e inversores, a menudo sin la intención real de crear aplicaciones comerciales.

Parece ser que hay bastante incertidumbre en torno a las cadenas de bloques. Podría no haber llegado todavía el momento de florecimiento de esta tecnología, aunque también cabe la posibilidad de que estemos llamando blockchain a lo que no lo es, dado que es un término atractivo de moda que “vende” innovación y modernidad.

No es blockchain todo lo que reluce

Antes de analizar el estado del arte de la cuestión, habría que aclarar qué es exactamente blockchain. Las cadenas de bloques son una tecnología de libro de registro digital descentralizado, lo que en inglés se conoce como *Distributed Ledger Technology* (DLT).

Un DLT es una base de datos que no está centralizada y que es gestionada por varios de los usuarios del sistema. Dentro de este tipo de sistemas está blockchain, que es un tipo de DLT con características propias, en concreto, que los registros van en unos bloques que forman una cadena. Cada bloque se cierra con un hash o código de seguridad que abre además el siguiente bloque.

Existen diversos tipos de libros descentralizados en función de su naturaleza y grado de apertura. El Foro Económico Mundial identifica tres distintos:

- *Sistemas compartidos privados bajo permiso.* Se trata de aquellos a los que solamente tiene acceso una lista cerrada de personas con potestad para leer o escribir en el sistema. Pueden tener uno o varios propietarios.
- *Sistemas compartidos públicos bajo permiso.* En este caso, aunque el acceso es restringido, todas las transacciones que tienen lugar en el sistema deben ser públicas, es decir, cualquiera las pueda consultar.
- *Sistemas compartidos públicos de acceso libre.* Es el sistema en el que se basan las criptomonedas como Bitcoin y el que generalmente se asocia con el término blockchain, y parte de que cualquiera puede acceder a él libremente con derecho a escribir y a leer todas las transacciones que allí se producen. No tiene un solo dueño, puesto que cada miembro posee una copia completa del libro de registro.

Un reciente informe de Forrester, citado por la revista Fortune, habla del uso excesivo del término blockchain por parte de las empresas, como fenómeno de moda que es. De hecho, muchas de ellas empaquetan servicios ya existentes bajo esa categoría, intentando parecer más innovadoras. El estudio alerta de que *“las redes que están operativas o en desarrollo varían notablemente, y, frecuentemente, carecen de características que para muchos son componentes esenciales de blockchain”*.

Las predicciones de Forrester también avisan de la llegada de un posible *“invierno blockchain”*, a pesar de que se siga invirtiendo e investigando en esta tecnología.

Se acerca el invierno

El efecto transformador de blockchain en la economía puede no estar tan cerca como lo venden los profetas más optimistas. La hiperinflación de expectativas sobre esta tecnología pasa por alto que todavía quedan muchos temas que resolver, principalmente relacionados con la escalabilidad de las soluciones desarrolladas, la interoperabilidad con distintos sistemas, y el marco regulatorio, que no suele mantener el paso rápido de la innovación, pero que debe establecer una legislación específica en torno a este fenómeno.

Frente a estos factores, que podríamos denominar institucionales y de oferta, también desde la perspectiva de la demanda el florecimiento de esta tecnología requiere crear aplicaciones de las cadenas de bloques que solucionen necesidades reales de mercado y que impliquen una rentabilidad económica.

La Organización Mundial del Comercio, basándose en la famosa curva de Gartner, que establece el periodo de maduración de una tecnología, retrasa al menos diez años la llegada de un blockchain realmente extendido a todos los ámbitos y económicamente rentable.



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

Como muestra la gráfica anterior, estamos en una época de *“exuberancia irracional”* en la que abundan los proyectos piloto con blockchain y las pruebas de concepto, pero que arroja muy pocos casos de éxito. A partir de 2022 este modelo predice la llegada de grandes inversiones a largo plazo en esta tecnología y la sucesión de experiencias exitosas. Pero no será hasta después de 2027 en que veremos crecer con vigor el valor de negocio de las cadenas de bloques.

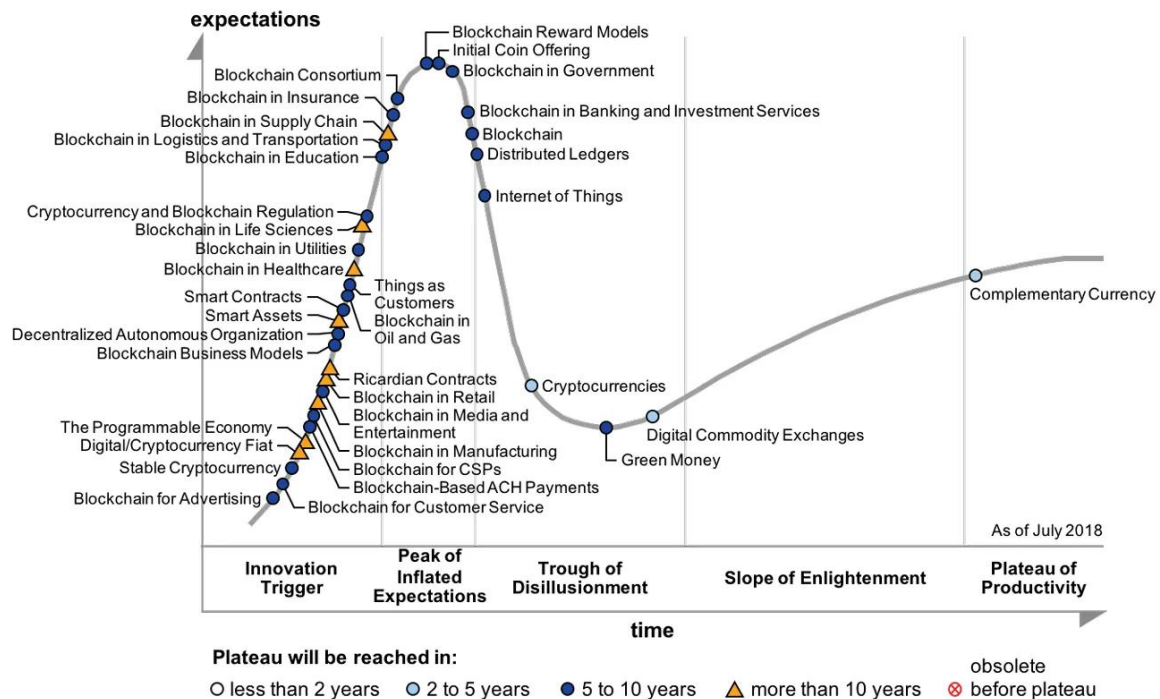
La fatiga de blockchain

En una reciente nota de prensa, la consultora Gartner habla de la *“fatiga de blockchain”* aplicada a la cadena de suministro. Se trata de una innovación que ya se han planteado grandes empresas, como, por ejemplo, Carrefour.

Para 2023, el 90% de las iniciativas emprendidas en este campo corren el riesgo de quedar estancadas. Alex Pradhan, analista de Gartner atribuye esta fatiga a factores como la propia falta de madurez de esta tecnología o la falta de estándares, pero también al hecho de que no se comprende bien cómo mejorar la cadena de suministro con blockchain, lo que a menudo lleva a concebir iniciativas demasiado ambiciosas.

Pero esta *fatiga* de las cadenas, que presumiblemente retrasará sobremanera su adopción en la logística, también está presente en el resto de los sectores objeto de asumir las cadenas de bloques. La curva de Gartner relativa a blockchain lo retrata muy gráficamente.

Hype Cycle for Blockchain Business, 2018



gartner.com/SmarterWithGartner

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Gartner

La mayoría de las aplicaciones no llegarán hasta la rentabilidad, aquí denominada meseta de la productividad, hasta dentro de cinco o diez años, y alguna –entre las que se encuentra el uso en cadenas de suministro- más de diez. La mayoría de aplicaciones de blockchain está ascendiendo hacia el pico de las expectativas infladas, mientras que ya hay unas cuantas cayendo en la “*sima de la desilusión*”, en concreto, las criptomonedas y el blockchain como servicio fintech.

La consultora McKinsey, por su parte, califica blockchain como una tecnología que está en su infancia y que actualmente no puede ir más allá de la fase inicial de lanzamiento y creación de prototipos, dentro de su curva de crecimiento. Por ahora no parece claro que vaya a pasar en breve a la siguiente, en la que la demanda comienza a crecer, el mercado se expande y la tecnología efectivamente despegar.

Los servicios financieros arrastraron el blockchain inicial entre 2012 y 2015, tras la popularidad que adquirieron las criptomonedas y, en concreto, Bitcoin. Las perspectivas de aplicaciones relacionadas con las finanzas, el comercio y la contratación, atrajeron cuantiosas inversiones, que fueron a parar a *startups* y a consorcios, con el objeto de impulsar la investigación y la innovación en este campo.

Las posibilidades de las cadenas de bloque se extendieron a otros sectores, como los seguros, la administración pública o las cadenas de suministro, entre muchos otros. Aunque a finales de 2016 las

expectativas en torno a esta tecnología eran muy prometedoras, un año más tarde comenzaron a surgir dudas sobre su grado de madurez e incluso sobre si es la solución idónea para las necesidades de las empresas.

El caso es que han sido invertidos miles de millones de dólares en investigación y desarrollo de las cadenas de bloques, pero son escasos los casos de éxito desde el punto de vista del negocio y de la rentabilidad económica.

Es bueno que reviente la burbuja

La inflación de expectativas sobre el blockchain ha llegado hasta tal punto que, en los seminarios y encuentros sobre el tema, parece que los ponentes están pidiendo perdón por lo que esta tecnología no ha sido capaz de conseguir. Así lo comenta por lo menos James Ovenden, redactor del medio digital *Innovation Enterprise*.

También reflexiona este experto sobre por qué es positivo que estalle la burbuja de expectativas que existe actualmente sobre las cadenas de bloques, y por qué no es tan malo que lleguemos a un periodo de cierta decepción sobre el particular.

En primer lugar, porque permitirá a los desarrolladores concebir soluciones reales a problemas reales, sin la presión que le impone la moda a la empresa de ser innovadora y de hacer gala de la tecnología más vanguardista, sin tomar en consideración su posible utilidad y rentabilidad. La verdadera difusión llegará cuando se multipliquen los casos exitosos de uso.

Asociado a lo anterior, cuando acabe la especulación sobre blockchain y empecemos a ver aplicaciones de negocio reales, las autoridades podrán elaborar una legislación adecuada. Hasta ahora, la evolución tecnológica es mucho más rápido que la capacidad de legislar. En el caso de las cadenas de bloques, al no existir demasiados casos prácticos de uso comercial, resulta extremadamente complejo establecer un acervo normativo al respecto.

De confiar en las personas a hacerlo en la tecnología

La confianza es un elemento indispensable en el funcionamiento de la economía y de la sociedad. Bruce Schneier, en su libro *Liar's and Outlier*, identifica cuatro categorías de confianza. Las dos primeras, sobre todo aplicables en comunidades pequeñas, son la moral y la reputación de las personas. Después vendría la seguridad institucional, cuyas normas y leyes obligan a los miembros de la sociedad a cumplir sus compromisos con sus conciudadanos, y, finalmente, los sistemas de seguridad, que pueden ir desde un cerrojo o una verja, hasta una auditoría de cuentas.

El problema es que blockchain traslada la confianza en las personas e instituciones a la tecnología. De acuerdo con su forma de funcionar, ya no importa quién está al otro lado de la red y lo fiable que pueda ser; tampoco hace falta un control centralizado de las transacciones que se realicen en el sistema, ni una regulación del mismo. La filosofía que rige en las cadenas de bloques hace que solamente debamos confiar en la criptografía, los protocolos, el *software*, los ordenadores y la red.

Pero, como apunta Schneier, a veces es peor confiar en la tecnología que confiar en las personas:

“Si tu monedero de bitc oin es hackeado, pierdes todo tu dinero. Si te olvidas de las credenciales de acceso, pierdes todo tu dinero. Si hay un fallo en el c odigo de tu contrato inteligente, pierdes todo tu dinero. Si alguien consigue hackear la seguridad de blockchain, pierdes todo tu dinero”.

¿Qué es mejor? ¿Confiar en un sistema legal humano -como hemos hecho toda la vida- o en un código informático que ni entendemos ni podemos auditar?

¿Son las cadenas de bloques la solución idónea?

Dejando de lado la necesidad de parecer innovadoras y *techies*, las empresas deben evaluar seriamente hasta qué punto las cadenas de bloques pueden resultar adecuadas para satisfacer sus necesidades.

La Organización Mundial del Comercio establece un razonamiento interesante en este sentido, que permite saber si blockchain es realmente la solución requerida para solventar un problema.

En primer lugar, debemos preguntarnos si nuestra necesidad de negocio se soluciona quitando de en medio a los intermediarios, bien porque acelere los procesos, bien porque abarate los costes de producción o distribución. En caso afirmativo, blockchain puede ser una opción deseable.

Otro punto importante es que blockchain funciona mejor cuando se basa en activos “nativos digitales”, es decir, unidades de valor o de cuenta perfectamente representables en formato digital. Resulta fácil en este entorno manejar *tokens* o criptomonedas, pero es más complejo hacerlo con la gestión de bienes físicos.

Blockchain crea registros inmutables, pero, ¿es eso deseable en el caso de todos los activos que queramos gestionar con dicha tecnología? En las ocasiones en las que el poder eliminar información es un asunto crítico (por ejemplo, porque resulte redundante o poder quedar obsoleta), blockchain no es la mejor opción tecnológica.

Por otro lado, si un activo digital requiere de distintas fuentes para garantizar su fiabilidad en cada momento, a lo mejor almacenarlo en la cadena de bloques no es la solución óptima. Algo similar ocurre cuando en un determinado proyecto existe la necesidad de contar con intermediarios o terceras personas que validen o supervisen las transacciones, por ejemplo, para garantizar que cumplen aspectos legales. Un caso podrían ser los sectores estrictamente regulados, cuya operativa está sometida a un control férreo por parte de las autoridades o de auditores externos.

El tiempo es otro factor decisivo a la hora de elegir tecnología. Un proceso de negocio que requiere cerrar transacciones en milisegundos no puede ser soportado por las blockchains actuales que emplean entre dos y diez minutos en procesar la información. No obstante, el acelerado ritmo de innovación actual permite predecir que esta velocidad mejorará pronto.

En principio, la Organización Mundial del Comercio en su informe desaconseja utilizar tecnología de libro de registro digital descentralizado para almacenar información no relacionada con transacciones, porque guardar allí datos privados puede entrar en conflicto con la legislación vigente sobre protección de la información y, más en concreto, con el Reglamento General de Protección de Datos europeo.

Blockchain es una opción adecuada cuando los distintos miembros de la red registran transacciones en la misma, si no es así, probablemente otra solución tecnológica resulte más idónea. Igualmente, si las partes que intervienen se conocen entre sí y confían unos en otros tampoco parece necesario recurrir a las cadenas de bloques.

Entonces, ¿cuándo hace falta blockchain?

A grandes rasgos, se puede resumir que el caso de uso ideal de blockchain será aquel que presente 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 entre transacciones es generada por las distintas entidades participantes.

Imagen de [Ricardo Esquivel](#) en [Pexels](#)