Blockchain

**INTRODUCCION**

Blockchain significa cadena de bloques nació como actor secundario en la revolucióndel bitcoin, ya que se trata de la tecnología o el sistema de codificación de la informaciónque está por detrás de la moneda virtual y que sustenta toda su estructura.Blockchain es una tecnología que permite la transferencia de datos digitales con unacodificación muy sofisticada y de una manera completamente segura. Sería como el libro deasientos de contabilidad de una empresa en donde se registran todas las entradas y salidas dedinero; en este caso hablamos de un libro de acontecimientos digitales.Está compuesto por el código de computadora compartida y bases de datos que permiten alas partes a participar en Machine-to-Machine el comercio de la moneda, es decir permite lacreación, la autenticación, la secuenciación, sellado de tiempo, la replicación y la finalizaciónde una transacción Bitcoin.Esta transferencia no requiere de un intermediario centralizado que identifique y certifiquela información, sino que está distribuida en múltiples nodos independientes entre sí que laregistran y la validan sin necesidad de que haya confianza entre ellos. Una vez introducida, lainformación no puede ser borrada, solo se podrán añadir nuevos registros, y no serálegitimada a menos que la mayoría de ellos se pongan de acuerdo para hacerlo.El blockchain, como su nombre indica, es una cadena de bloques, cada uno de esos bloquescontiene la información codificada de una transacción en la red en la cual cada bloque portael paquete de transacciones y dos códigos, uno que indica cuál es el bloque que lo precede yotro para el bloque que le sigue, es decir, que están entrelazados o encadenados por lo que sellaman códigos o apuntadores hash, dentro de esta también está el minado que realizanlos nodos, es decir, el proceso de validación de la información. En este proceso de minado ocomprobación, cuando hay dos bloques que apuntan al mismo bloque previo, sencillamentegana el primero en ser desencriptado por la mayoría de los nodos, es decir, que la mayoría de puntos de la red deben ponerse de acuerdo para validar la información.

**Qué es el blockchain?**

Entre otras cosas, es una de las palabras de moda en los últimos tiempos. La cadena de bloques es también un concepto que **plantea una enorme revolución** no solo en nuestra economía, sino en todo tipo de ámbitos.

Entender lo que es esa cadena de bloques no es tan difícil, y dado que cada vez se utiliza más este concepto hemos querido hacer una especie de **curso rápido de introducción al blockchain**, para explicar qué es, cómo funciona y cuál es esa revolución que plantea la cadena de bloques.

¿Qué es entonces la cadena de bloques? Pues un gigantesco libro de cuentas en los que los registros (los bloques) están enlazados y cifrados para proteger la seguridad y privacidad de las transacciones. Es, en otras palabras, **una base de datos distribuida y segura** (gracias al cifrado) que se puede aplicar a todo tipo de transacciones que no tienen por qué ser necesariamente económicas.

Esa cadena de bloques tiene un requisito importante: **debe haber varios usuarios (nodos) que se encarguen de verificar esas transacciones** para validarlas y que así el bloque correspondiente a esa transacción (en cada bloque hay un gran número de transacciones que eso sí, [es variable](https://blockchain.info/charts/n-transactions-per-block)) se registre en ese gigantesco libro de cuentas.

Ese minado de bloques consiste en la realización de una serie de complejos cálculos que requieren tiempo y (cada vez más) electricidad, pero cuando el proceso esos bloques **quedan registrados de forma permanente en esa cadena de bloques**, y no pueden ser modificados sin que se alteren todos los bloques que están enlazados con él, una operación que además necesitaría que la mayoría de los nodos la validasen.

**La cadena de bloques más allá de la economía**

Aunque la cadena de bloques está íntimamente relacionada con las nuevas criptodivisas o criptomonedas, es lógico preguntarse si este sistema sería válido para otro tipo de transacciones, y **la respuesta es un rotundo sí**.

De hecho eso es lo que está intentando lograr desde sus inicios **la plataforma Ethereum**, que tiene su propia cadena de bloques (podéis echarle un vistazo en sitios como [Etherscan.io](https://etherscan.io/)) y su propia moneda, llamada Ether. A diferencia de bitcoin, las transacciones aquí son los contratos inteligentes —[los programadores aman este concepto](https://www.xataka.com/empresas-y-economia/por-que-los-programadores-amamos-ethereum)—, que pueden ser más o menos complejos y que permiten definir todo tipo de transacciones.

Al igual que ocurre con bitcoin, lo bueno de esas transacciones es que se mantendrán en la cadena de bloques, inalterables y accesibles durante toda la vida de esa cadena de bloques. Si nos vamos al extremo, **Ethereum podría sustituir básicamente a cualquier intermediario**, sustituyendo productos y servicios que dependen de terceros para estar totalmente descentralizados.

Por supuesto esta es solo una de las alternativas que se han originado con la cadena de bloques como protagonista, y **de hecho hay muchas ideas**que tratan de explotar las bondades de una tecnología que tiene un alcance virtualmente ilimitado. Veamos algunos ejemplos:

* **Consorcio R3**: las propias entidades financieras que muchos tratan de [reemplazar con bitcoin o Ethereum](https://www.xataka.com/seguridad/como-ethereum-esta-disputando-el-papel-de-criptomoneda-mas-segura-sobre-blockchain-a-bitcoin) han creado el [consorcio R3](https://www.r3.com/) para averiguar cómo aprovechar la cadena de bloques en los sistemas financieros tradicionales. Uno de los primeros problemas de la aplicación de este esquema es el anonimato que proporciona el diseño de la cadena de bloques, algo que han resuelto con el llamado "libro de contabilidad autorizado" ('permissioned ledger'), una variante muy peculiar de la cadena de bloques de bitcoin, por ejemplo, que sí que identifica a los usuarios que añaden bloques y que hace que las transacciones del sistema solo puedan consultarse por ciertas partes.
* **Registro de propiedades**: el gobierno japonés [ha iniciado un proyecto](https://www.cryptocoinsnews.com/japan-place-entire-property-registry-blockchain/)para unificar todo el registro de propiedades urbanas y rústicas con tecnología de cadena de bloques, lo que permitiría contar con una base de datos abierta en la que se pudieran consultar los datos de las 230 millones de fincas y 50 millones de edificios que se estima existen en el país asiático. En Dubai [están planeando](https://www.cryptocoinsnews.com/100-dubai-put-entire-land-registry-blockchain/) algo muy parecido.
* **Pagos en el mundo real**: una startup llamada [TenX](https://www.tenx.tech/) ha creado una tarjeta prepago que se puede recargar con distintas criptodivisas para luego pagar con ella en cualquier sitio como si esa tarjeta tuviera dinero convencional, sin importar si ese establecimiento acepta o no este tipo de monedas virtuales.
* **Carsharing**: la empresa EY, subsidiaria de Ernst & Young Global Ltd está desarrollando un sistema basado en la cadena de bloques que permite a empresas o grupos de personas acceder a un servicio para compartir coches de forma sencilla. El llamado [Tesseract](http://www.ey.com/gl/en/newsroom/news-releases/news-ey-advancing-future-of-transportation-with-launch-of-blockchain-based-integrated-mobility-platform) permitiría registrar quién es el propietario del vehículo, el usuario de ese vehículo y generar los costes basados en el seguro y otras transacciones en este tipo de servicios.
* **Almacenamiento en la nube**: normalmente los servicios de almacenamiento están centralizados en un proveedor específico, pero la empresa [Storj](https://storj.io/) quiere descentralizar este servicio para mejorar la seguridad y reducir la dependencia de ese proveedor de almacenamiento.
* **Identidad digital**: los últimos y gigantescos fallos de seguridad y robos de datos han hecho que la gestión de nuestras identidades se convierta en un problema muy real. La cadena de bloques podría proporcionar un sistema único para lograr validar identidades de forma irrefutable, segura e inmutable. Hay [muchas empresas](https://letstalkpayments.com/22-companies-leveraging-blockchain-for-identity-management-and-authentication/) desarrollando servicios en este ámbito, y todas ellas creen que aplicar la tecnología de la cadena de bloques para este propósito es una solución óptima.
* **Música**: aunque hay críticas [que afirman](http://www.hypebot.com/hypebot/2017/08/why-you-cant-put-the-music-industry-on-a-blockchain-excerpt.html) que esta opción no tiene validez, [hay quien afirma](https://techcrunch.com/2016/10/08/how-blockchain-can-change-the-music-industry/) que la distribución musical podría sufrir toda una revolución si se lograra implantar un sistema basado en la cadena de bloques para gestionar su reproducción, distribución y disfrute. [La mismísima Spotify](https://www.xataka.com/empresas-y-economia/spotify-si-que-cree-en-blockchain-asi-funciona-mediachain-la-empresa-que-acaba-de-comprar) está apostando fuerte por su propia cadena de bloques.
* **Servicios públicos/gubernamentales**: otro de los ámbitos más interesantes de la aplicación de la cadena de bloques es en los servicios públicos que podrían presumir así de una transparencia absoluta. Las áreas de actividad son múltiples: desde la gestión de licencias, transacciones, eventos, movimiento de recursos y pagos, gestión de propiedades hasta la gestión de identidades. De hecho el [robo masivo de datos en Equifax](https://www.xataka.com/seguridad/como-el-de-equifax-se-ha-convertido-en-el-mayor-robo-de-datos-personales-de-la-historia) han hecho que algunos [propongan la sustitución](https://www.bloomberg.com/news/articles/2017-10-09/want-to-ditch-social-security-numbers-try-blockchain) de los números de la seguridad social en Estados Unidos con un sistema basado en la cadena de bloques. Hay [iniciativas](http://www.ibtimes.co.uk/decentralised-government-project-bitnation-offers-refugees-blockchain-ids-bitcoin-debit-cards-1526547) incluso para "descentralizar el gobierno", y [Bitnation](https://bitnation.co/) es una de esos proyectos que tratan de llamarnos convertirnos en "ciudadanos del mundo".
* **Seguridad social y sanidad**: aunque se podría englobar dentro de los servicios públicos mencionados, la sanidad pública [podría sufrir una verdadera revolución](https://www.technologyreview.com/s/608821/who-will-build-the-health-care-blockchain/) con un sistema de cadena de bloques que sirviera para registrar todo tipo de historiales médicos y resolver uno de los problemas clásicos de la gestión de la sanidad.
* **Gestión de autorías**: aunque relacionado con lo mencionado para el mundo de la música, [Ascribe](https://www.ascribe.io/) es una plataforma que trata de ayudar a creadores y artistas a atribuirse la autoría de sus trabajos a través de la cadena de bloques. Hay otras muchas plataformas en este ámbito ([Bitproof](https://bitproof.io/), [Blockai](https://blockai.com/), [Stampery](https://stampery.com/), por ejemplo) que entre otras cosas permiten generar tiendas en las que se puedan comprar trabajos originales de una forma segura y sencilla.

Son tan solo algunos ejemplos de la aplicación de la cadena de bloques a todo tipo de ámbitos, pero hay muchísimos más: la versatilidad de esta tecnología es tan enorme que **es difícil pensar en un área que no pueda ser transformada** por esta idea.

**Bibliografía:**

https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda

https://es.scribd.com/document/378017017/Ensayo-Blockchain