Introducción a *blockchain*

Blockchain y computación cuántica

CONTENIDO

Objetivos

- Conocer el uso y la definición de *blockchain*.
- Presentar los principales elementos de *blockchain*.
- Evidenciar el impacto que *blockchain* tiene en las empresas.
- Entender la importancia de *blockchain* en el entorno financiero.
- Comprender el origen y la evolución de *blockchain* repasando sus hitos más relevantes.

¿Qué es *blockchain*?

Es la tecnología que permite almacenar **transacciones** en un registro único de manera descentralizada.

Este registro de transacciones se almacena en todos los computadores que componen la red *blockchain*, haciendo de esta manera que la información sea accesible desde cualquier nodo de la red.

Las transacciones son agrupadas en **bloques** que quedan enlazados en forma de cadena mediante elementos criptográficos. Este mecanismo de enlazado criptográfico proporciona seguridad a la información, haciendo casi imposible alterar la información contenida en la cadena de bloques cuando la red *blockchain* cuenta con un gran número de nodos.

Todos los nodos mantienen una copia de la cadena de bloques.

Blockchain establece unas reglas bien definidas para que los **nodos** puedan procesar las transacciones y generar un nuevo bloque.

Los **nodos** que componen la red *blockchain* validan los nuevos bloques antes de ser incorporados a la cadena de bloques. Los bloques manipulados o con información incorrecta son desechados. Para poder validar las transacciones contenidas en los bloques, los nodos recorren la cadena de bloques y determinan si las transacciones son válidas, comprobando principalmente que la dirección de origen cuente con el saldo necesario para realizar cada transacción.

El tiempo que requiere *blockchain* en añadir un nuevo bloque a la cadena varía en función de la solución *blockchain*, en *bitcoin* se añade un bloque a la cadena aproximadamente cada 10 minutos.

La tecnología *blockchain* se basa en un conjunto de tecnologías predecesoras como las siguientes:

- La criptografía de clave pública
- Las redes P2P
- Las funciones *hash*
- Árbol de *Merkle*

La genialidad de *blockchain* radica en utilizar estas tecnologías existentes para crear una nueva tecnología que permite el intercambio de información de manera segura dentro de una red abierta sin la necesidad de intermediaros. La primera implementación de esta tecnología es *bitcoin*, que permite e intercambio de su criptomoneda sin la participación de entidades financieras.

El intercambio de información en una red abierta es posible gracias a la seguridad proporcionada por los mecanismos criptográficos incorporados en *blockchain*.

Inicialmente el termino *blockchain* estaba asociado al entorno financiero por su vinculación con las criptomonedas. Con la evolución de la tecnología su uso se extiende más allá del entorno financiero y actualmente un gran número de empresas de distintos sectores están explorando los beneficios que puede aportar esta tecnología a cada negocio.

Origen de *blockchain*

Antecedentes previos a la aparición de *blockchain*:

- *DigiCash* [1]. Fundada en 1990 por David Chaum creó una solución de pagos electrónicos llamada eCash, que fue comprada por varios bancos. Debido al bajo número de usuarios, *eCash* desaparece en 1998.
- Stuart Haber y W. Scott Stornetta presentan un artículo [2] en 1991 indicando distintas maneras de establecer un sellado de tiempo sobre un documento digital. En este artículo se indica cómo vincular las pruebas de los documentos para demostrar la fecha de creación de los mismos. En este artículo se establece un modelo de vinculación a modo de cadena donde se hace referencia al documento anterior, de manera similar al sistema de cadena de bloques de *blockchain*.
- *B-money* [3]. Es ideado por Wei Dai en 1998 quien presenta una solución de pagos electrónicos descentralizada basada en elementos criptográficos. Esta solución nunca se llegó a desarrollar, aunque su idea es muy similar a la desarrollada en *bitcoin*.

Blockchain fue concebido en 2008 mediante la publicación [4] de un documento llamado "*Bitcoin: a peer-to-peer electronic cash system*" por Satoshi Nakamoto, donde explica los principales conceptos y tecnologías que forman *bitcoin*.

En este documento, Satoshi hace referencia a un conjunto de tecnologías que proporcionan la funcionalidad necesaria para el desarrollo de *blockchain*.

Redes P2P

Las redes *peer-to-peer* (P2P) surgen a principios de los 90 como un nuevo protocolo que permite compartir información de manera directa, mediante la comunicación entre pares.

El uso de esta nueva tecnología se hace popular en 1999 con el nacimiento de *Napster*, que proporcionaba un software que crea redes P2P para el intercambio de música y archivos. Esta red requería de un servidor central que proporciona el contenido.

Las redes P2P evolucionan hacia un modelo híbrido con la aparición del protocolo definido por *BitTorrent* en 2001, donde el intercambio de información no se realiza con un servidor central sino con los nodos de la red, aunque si se requiere de servidores de referencia para la gestión de las comunicaciones entre los nodos.

En 2001 con la aparición del protocolo desarrollado por Gnutella se consigue crear un sistema de intercambio de información soportado por una red P2P pura, donde todos los nodos actúan como clientes y como servidores, eliminando en cualquier caso la dependencia con servidores de referencia.

Blockchain utilizan la tecnología P2P para establecer las comunicaciones que permiten el intercambio de información entre los nodos que forman la red *blockchain*.

Criptografía de clave pública

La criptografía de clave pública o clave asimétrica es un componente esencial de la tecnología *blockchain*, este tipo de criptografía se compone de dos claves distintas denominadas pública y privada. Este par de claves permite firmar digitalmente el contenido de una transacción y asegurar que los datos de la transacción no han sido modificados.

En blockchain la criptografía asimétrica permite asegurar que la persona que firma digitalmente una transacción válida, es el propietario del par de claves.

Funciones *hash*

Las funciones hash son otro de los elementos fundamentales de *blockchain* y se usan de manera generalizada para ofrecer autenticidad de la información.

Una función *hash* es una función matemática que convierte unos datos de entrada en un valor de tamaño definido. La principal característica de estas funciones es que la misma entrada siempre devuelve el mismo valor de salida, pero cualquier modificación sobre la entrada devuelve un valor distinto *(figura 1)*.

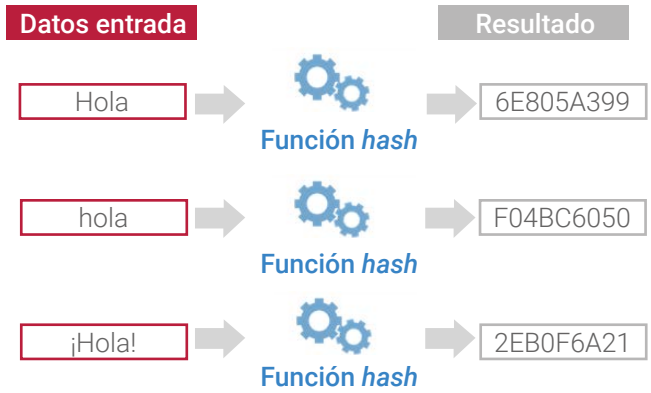

Figura 1. Funciones *hash*.

Las funciones *hash* se usan en *blockchain* para establecer identificadores de los bloques o de las transacciones.

Árbol de *Merkle*

Es una estructura en forma de árbol que hace referencia a un conjunto de datos. Las características de esta estructura hacen que las hojas del árbol contengan el hash de cada bloque de información referenciado. Los nodos permiten ir componiendo la información al hacer referencia a los hijos, mediante el *hash* resultante de la suma de los *hash* de los hijos referenciados *(figura 2)*.

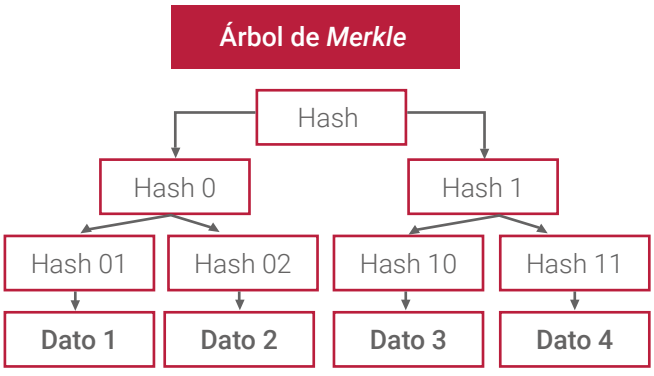

Figura 2. Árbol de *Merkle*.

Este mecanismo se utiliza en las redes P2P para verificar el contenido almacenado, gestionado o intercambiado entre los nodos de la red.

Blockchain utiliza el árbol de *Merkle* para gestionar la información que se almacena en *blockchain*.

En *bitcoin* esta estructura permite almacenar las transacciones recibidas por un a dirección. Esta estructura se consulta para validar si la dirección origen de una transacción dispone de suficiente saldo.

Evolución

La tecnología *blockchain* en sus primeros años evoluciona dentro del entorno de las criptomonedas. Tras el éxito de *bitcoin* que comienza a funcionar en enero de 2009, surgen distintas soluciones *blockchain* centradas en las criptomonedas como *litecoin* (2011), *tether* (2014), *navcoin* (2014), *bitcoin gold* (2017), *bitcoin chash* (2017) que intentan posicionarse como la divisa digital de referencia.

Durante los primeros años el termino *blockchain* estaba asociado únicamente a las criptomonedas. En 2014 Gartner incorpora las criptomonedas dentro del conjunto de tecnologías emergentes. Esta empresa dedicada al asesoramiento tecnológico pone las criptomonedas en el radar tecnológico de las empresas que asesora, generando una gran expectación sobre su evolución.

No será hasta **2015** con la aparición de *ethereum* cuando se considere *blockchain* como una tecnología de intercambio de valor con proyección para ofrecer soluciones más allá del entorno de las criptomonedas.

Ethereum añade a *blockchain* una nueva funcionalidad llamada *smart contract*, que permite establecer acuerdos entre dos o más participantes.

Los smart contracts son programas que se almacenan en *blockchain* y donde se establecen condiciones y reglas para modificar la información que guarda el smart contract, permitiendo incluso realizar otras transacciones.

Esta nueva funcionalidad permite ampliar el uso de *blockchain* incorporando lógica de negocio en los *smart* contracts.

Con los smart contracts se puede registrar la trazabilidad de un producto, crear juegos y apuestas o crear un sistema de financiación para proyectos.

Tras la incorporación de *smart contracts* en *Bockchain*, se abre un mundo de posibilidades para las empresas, que empiezan a usar *ethereum* como una herramienta que permite establecer nuevos modelos de negocio. Este nuevo planteamiento de *blockchain* hace que Gartner incorpore la tecnología *blockchain* en su gráfica de tecnologías emergentes en 2016.

Desde la aparición de *ethereum*, surgen un gran número de soluciones *blockchain* con el objetivo de mejorar el rendimiento que ofrece *ethereum* o establecer nuevas soluciones para las empresas, en el siguiente gráfico se muestran las soluciones *blockchain* más representativas *(figura 3)*.

En 2019 Gartner publica un gráfico *(figura 4)* sobre la tecnología *blockchain* donde incorpora el estado de esta tecnología en un gran conjunto de industrias. La evolución de *blockchain* es desigual en cada industria y con esta gráfica se muestra la importancia de conocer la evolución de *blockchain* en cada área.

La revolución de *blockchain*

La tecnología *blockchain* cuenta con el potencial para cambiar el mundo financiero actual, estableciendo un nuevo paradigma de intercambio de valor que reduce o elimina la intervención de instituciones financieras.

Tradicionalmente un traspaso de dinero de un banco a otro requiere de una operación de consolidación entre el banco origen y el banco destino, donde cada banco refleja la operación en su balance y actualiza su base de datos acorde a la operación consolidada. Con *blockchain* se realiza una transacción de criptomoneda sin la intervención de bancos o intermediarios y el tiempo requerido para completar la ejecución de la operación es mucho menor que el empleado utilizando la operativa de un banco, especialmente si se quiere realizar transacciones entre distintos países.

Figura 3. Cronograma de blockchain con criptomonedas.

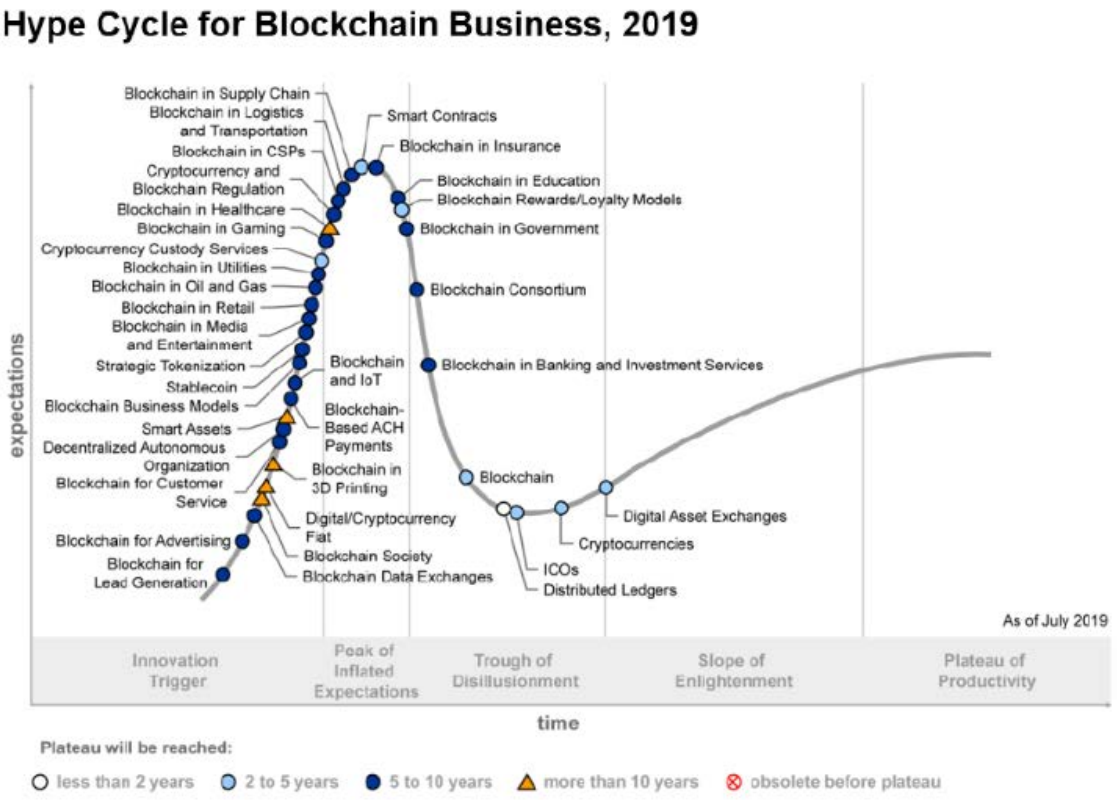

Figura 4. Gráfico Gartner 2019 [5].

Blockchain ha conseguido agitar los cimientos del mundo financiero, poniendo a prueba un sistema basado en la supervisión y el control realizado por bancos centrales y gobiernos.

¿DÓNDE SE PUEDE UTILIZAR *BLOCKCHAIN*?

La tecnología *blockchain* no solo se aplica al sector financiero, el interés que genera en otros sectores se debe a la capacidad de proporcionar un entorno seguro para el intercambio de información.

A medida que la tecnología ha ido evolucionando y el conocimiento sobre la tecnología se ha extendido, ha aumentado el interés de empresas y gobiernos por conocer las posibilidades que ofrece la tecnología *blockchain* en otros sectores como; el industrial, el sector sanitario, el manufacturero y en general **cualquier sector donde la colaboración con distintos participantes sea clave para el desarrollo del negocio**.

El interés que suscita *blockchain* se debe al potencial que ofrece para definir nuevos modelos de negocio y por la capacidad de mejorar algunos de los procesos de negocio que utilizan las empresas actualmente.

¿QUÉ SE PUEDE CONSEGUIR CON *BLOCKCHAIN*?

En el sector financiero se ha utilizado *blockchain* para realizar pagos internacionales mucho más rápidos y baratos. *blockchain* permite generar una red donde se gestionan las operaciones de cambio de divisa entre los participantes de la red, minimizando la necesidad de acudir a una casa de cambio de divisa que repercute en un aumento de costes de las operaciones.

Fuera del sector financiero se puede plantear una red *blockchain* donde se almacenen las revisiones de un vehículo. Utilizando un smart contract se puede almacenar todas las revisiones que se realizan a un vehículo, indicando incluso las operaciones realizadas en cada taller. De esta manera cualquier persona puede comprobar la actividad que ha tenido un coche en el taller.

Las apuestas son otro de los usos principales de *blockchain*. Los smart contracts permiten crear un sistema de apuestas, donde cualquier usuario puede apostar enviando una cantidad de criptomoneda. Cuando la apuesta se resuelve, el ganador recibe la cantidad correspondiente de criptomonedas que son enviadas directamente por el smart contract.

El sector de la distribución, puede utilizar un smart contract para almacenar la trazabilidad de un producto, desde que se crea hasta que se vende, permitiendo a los participantes disponer de información en tiempo real de la fase en la que se encuentra el producto.

El futuro de *blockchain*

La inversión en *blockchain* crece de manera notable cada año y las previsiones [6] presentadas antes de la irrupción de la pandemia del COVID-19, indicaban que el mercado de *blockchain* llegaría a 15 900 millones de dólares en 2023.

El crecimiento del mercado depende en buena medida de la evolución de la tecnología *blockchain*. Esta tecnología se encuentra en una fase donde ha de demostrar sus verdaderas capacidades, desterrando falsas expectativas y evidenciando los logros y avances realizados por las empresas y organismos que apuestan por el desarrollo de la tecnología *blockchain.*

Retos

La evolución de *blockchain* ha sido enorme en un periodo de tiempo muy corto, pero la adopción de esta tecnología de manera general depende de la capacidad que tenga la propia tecnología y a comunidad que promueve la tecnología para hacer frente a los siguientes retos:

Legal y regulatorio

Blockchain genera un nuevo orden que no se ajusta a las leyes y al marco regulatorio actual. Este supone uno de los grandes retos que organismos y gobiernos deben resolver para facilitar la adopción y desarrollo de la tecnología en ciertas áreas, para que empresas, ciudadanos, notarios, abogados y jueces cuenten con un marco jurídico adaptado al entorno tecnológico actual.

Un ejemplo de colaboración multisectorial a favor de desarrollo de *blockchain* es Alastria [7]. Esta organización donde participan las principales empresas del país cuenta con representantes de los principales sectores, prestando especial atención a los asuntos legales y regulatorios. Uno de sus principales objetivos es el desarrollo de un sistema de Identidad Digital que cumple con los requisitos establecidos por la Unión Europea para el tratamiento de datos personales e información sensible.

Tecnológico

La tecnología *blockchain* es relativamente nueva y ha de resolver dos grandes restricciones tecnológicas que en muchos casos frenan a las empresas a apostar por la tecnología *blockchain*, según se recoge en la encuesta realizada por Cambridge Centre for Alternative Finance, donde se identifican como principales retos tecnológicos los siguientes:

- **Escalabilidad:** las primeras soluciones *blockchain* estaban muy limitadas para ofrecer escalabilidad, pero las últimas soluciones *blockchain* ofrecen una mayor capacidad de escalado, aunque en algunos casos lo hacen disminuyendo la descentralización.
- **Desempeño:** la capacidad para procesar mayor número de transacciones ha sido uno de los principales motivos para el desarrollo de nuevas soluciones *blockchain*. En este sentido se ha avanzado considerablemente en los últimos años. Por ejemplo, el *blockchain* NEO es capaz de procesar entre 1000 y 10 000 transacciones por segundo [8], lo que supone un gran avance comparado con la media de menos de 5 transacciones por segundo de bitcoin o las 15 transacciones por segundo de *ethereum* con el algoritmo de consenso de PoW.

Interoperabilidad

Este reto hace referencia a la capacidad de establecer comunicación entre distintos *blockchain* y en menor medida a capacidad de comunicar *blockchain* con otros sistemas.

Blockchain es una tecnología diseñada para procesar transacciones en un entorno aislado de otros sistemas o fuentes de información. Este funcionamiento puede condicionar la capacidad de vincular el comportamiento de un *blockchain* con información del exterior o de otro *blockchain*.

Existen algunas soluciones como los oráculos, sistemas de alertas y plataformas de interconexión de *blockchain* que permiten conectar la información de un *blockchain* con otras fuentes de información.

Este tipo de soluciones son utilizadas por los *smart contracts* para por ejemplo conocer el ganador de una apuesta deportiva. Ejemplo, se programa un *smart contract* que permite gestionar apuestas sobre los partidos de tenis, este *smart contract* se despliega en *ethereum* y cualquier persona que disponga de una cuenta y saldo puede realizar una apuesta enviando una transacción al *smart contract*. Este *smart contract* por sí mismo no tiene mecanismos para resolver la apuesta y transferir los ETH (criptomoneda de *ethereum*) correspondientes al ganador. Necesita la información de un sistema externo para poder resolver la apuesta. En este caso, se puede utilizar un oráculo para que proporcione el ganador del partido, de manera que el *smart contract* de apuestas pueda resolver la apuesta y enviar al ganador la cantidad de ETH que le corresponde.

Otro de los retos de interoperabilidad, aparece con la necesidad de interconectar dos *blockchain* diferentes utilizados por dos empresas que deciden colaborar intercambiando información. En este caso se están desarrollando soluciones que permiten interconectar distintos *blockchain* como Hyperledger.

Estandarización

La estandarización es otro de los retos para conseguir avanzar en la interoperabilidad de *blockchain*. Los principales *blockchain* enfocados al entorno empresarial, proporcionan mecanismos para facilitar el acceso y la estandarización de la información. En la actualidad las soluciones *blockchain* más importantes cuentan con interfaces que proporcionan un formato estándar para la conexión de sistemas y aplicaciones.

Resumen

En este tema se ha presentado la tecnología *blockchain* y se han repasado las tecnologías que han hecho posible crear *bitcoin*.

Bitcoin marca un hito en el mundo financiero estableciendo nuevos modelos de negocio. El verdadero éxito de *bitcoin* es demostrar que la tecnología *blockchain* funciona y lo demuestra con una solución que permite la gestión de dinero electrónico desde 2009 sin que se hayan detectado fallos en el funcionamiento de *blockchain*.

Blockchain es una tecnología muy nueva, poco más de 10 años, y tiene bastantes retos que frenan la adopción de la tecnología por parte de las empresas. Actualmente, *blockchain* se encuentra en un momento decisivo, en el que tiene que demostrar su verdadera utilidad, al mismo tiempo que va superando los retos. Solo si evoluciona favorablemente podrá considerarse una tecnología disruptiva que es capaz de revolucionar cualquier sector mediante el intercambio de información en entornos colaborativos.

Bibliografía

[1] (1996). "*DigiCash´s Ecash*™ to be Issued by Deutsche Bank". [En línea] Disponible en: https://www.chaum.com/ecash/articles/1996/05-07-96%20-%20DigiCash_s%20Ecash%E2%84%A2%20to%20be%20Issued%20by%20Deutsche%20Bank.pdf

[2] S. Haber and W. Scott Stornetta. (1991). "*How To Time-Stamp a Digital Documen*". [Online]. Available: https://www.anf.es/pdf/Haber_Stornetta.pdf

[3] D. Wei. "B-Money". [En línea] Disponible en: http://www.weidai.com/bmoney.txt

[4] S. Nakamoto. (2008). "*Bitcoin: A peer-to-peer electronic cash system*". [En línea] Disponible en: https://bitcoin.org/bitcoin.pdf

[5] Gartner. (2019). Gráfico [En línea] Disponible en: https://www.gartner.com/en/newsroom/press-releases/2019-09-12-gartner-2019-hype-cycle-for-blockchain-business-shows

[6] (2019, Agoust, 8). "*New IDC Spending Guide Sees Strong Growth in Blockchain Solutions Leading to $15.9 Billion Market in 2023*". [En línea] Disponible en: https://www.idc.com/getdoc.jsp?containerId=prUS45429719

[7] Alastria [En línea] Disponible en: https://alastria.io/

[8] "Neo White Paper". [En línea] Disponible en: https://docs.neo.org/docs/en-us/basic/whitepaper.html