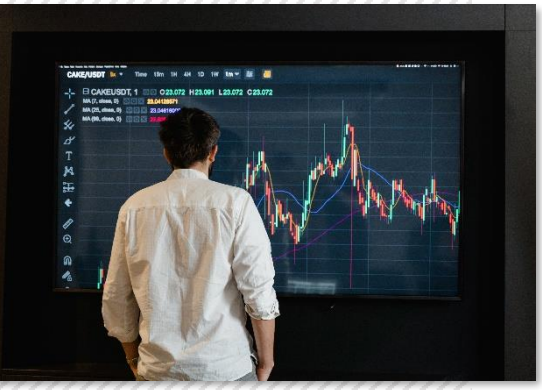
Seguridad y transparencia gracias a la tecnología Blockchain

La criptografía y la capacidad de transmitir y almacenar datos a gran escala han hecho posible la aparición de tecnologías de registros distribuidos (DLT), es decir, de bases de datos con copias idénticas que se actualizan de forma sincronizada y consensuada y que se encuentran distribuidas entre los participantes de la red. La principal característica de esta tecnología es que es inmutable, la información se guarda sin que pueda ser alterada, y los datos se gestionan y se comparten de manera segura. Uno de los máximos exponentes de las DLT es la tecnología **Blockchain** o cadena de bloques.



Si echamos la vista atrás, en los inicios de internet, los servicios eran caros y centralizados física y jerárquicamente. Con la llegada del *Cloud*, computación en la nube, se produce la descentralización física, pero no jerárquica de la red y se abarata considerablemente su acceso. Es con la tecnología **Blockchain** cuando se produce la descentralización total, tanto física como jerárquica, puesto que todos los usuarios tienen poder de decisión y de acción sobre la red.

Hoy en día, no existe una única definición oficial de Blockchain debido a la novedad del concepto y a la disparidad de consideraciones. A continuación, apuntamos algunas ideas que destacan las diferentes propiedades que significan esta tecnología. Así, podemos precisar que **Blockchain** es:

- Un registro distribuido de datos integrable y programable.
- Una base de datos distribuida y segura que se puede aplicar a todo tipo de transacciones, no necesariamente económicas.

- Un conjunto de tecnologías que permiten la transferencia de un activo, sin intervención de terceros.
- Una base de datos distribuida entre los nodos participantes en la red.

Para comprender mejor las propiedades que definen esta tecnología debemos conocer cómo funciona. El funcionamiento de **Blockchain** requiere de un Genesis block, que es el primer bloque de la cadena en el cual se establecen las reglas que determinarán cómo se consigue y se mantiene el consenso de la red. Este protocolo de consenso es el que regula la generación de bloques y la validación de las transacciones y se consigue de muchas maneras diferentes gracias a los algoritmos. Por ejemplo, el algoritmo de consenso de Bitcoin y Ethereum, dos exponentes de **Blockchain**, es el *Proof of Work*.

A partir de ahí, ya se empiezan a realizar las transacciones que se irán almacenando en los bloques. Para ello, debe haber varios usuarios (**nodos**) que se encarguen de verificarlas y cuando se llega a un número determinado de transacciones se valida o sella (**mina**) el bloque, es decir, se cierra. En realidad, el minado de bloques consiste en la realización de cálculos complejos que requieren tiempo y consumo de electricidad. Este sellado es un registro permanente que no puede ser modificado, sólo es posible ir incorporando nueva información a la cadena. Cuando se mina un bloque, este se añade a la cadena. Los nodos mineros que consiguen subir un bloque reciben una recompensa en forma de criptomonedas (tanto por el bloque como por las transacciones contenidas en el mismo).

En el proceso de la cadena de bloques se eliminan los intermediarios puesto que, como vemos, se descentraliza toda la gestión en los diferentes usuarios. La responsabilidad ya no recae en un único tercero que certifica la información, sino que está distribuida en múltiples nodos independientes e iguales entre sí que no necesariamente se conocen entre ellos. Su sincronización facilita la irreversibilidad de las transacciones y evita el fraude. Además, la cadena de bloques protege la privacidad de los usuarios y permite controlar la

trazabilidad de los movimientos. Así, el nivel de seguridad es extremadamente alto dado que los datos están codificados mediante criptografía.

Cuáles son, entonces, las principales ventajas del uso de la tecnología **Blockchain**:

- Procesos optimizados porque se suprime la intervención de terceros.
- Altos niveles de transparencia.
- Alta auditabilidad puesto que se tiene toda la historia en la cadena.
- Red siempre activa ya que solo necesita de un nodo para funcionar.
- Sin necesidad de *backups* porque todos los registros están en todos los nodos de la red.
- Alta seguridad contra ataques gracias a la criptografía.

El uso más extendido del **Blockchain** son las criptodivisas como Bitcoin o Ethereum, pero el sistema está preparado para operar otro tipo de transacciones. Así pues, sus aplicaciones son ilimitadas y pueden realizarse en sectores tan diferentes como el registro de propiedades, pagos en el mundo real, *carsharing*, almacenamiento en la nube, identidad digital, música, seguridad social y sanidad, gestión de autorías, cadena de suministros de productos o procesos electorales. Como se puede ver, la versatilidad de esta tecnología es enorme. Una de sus aplicaciones emergentes más relevantes es la que se conoce como "contratos inteligentes" o *smart contracts*. Consisten en la capacidad para confiar en una red distribuida la confirmación que un contrato de cualquier tipo ha sido cumplido sin revelar ningún tipo de información confidencial.

La tecnología **Blockchain** está en constante evolución, pero permanece intacta su implicación con los valores de confianza y transparencia que la caracterizan. Los niveles de democracia y objetividad a los cuales se puede llegar son ingentes ya que el poder se reparte entre todos los usuarios y no se puede mentir sobre eventos pasados o presentes. Será necesario observar cómo se produce esta evolución y estudiar las posibles aplicaciones, integraciones o creación de soluciones dirigidas a nuevos sectores operativos.