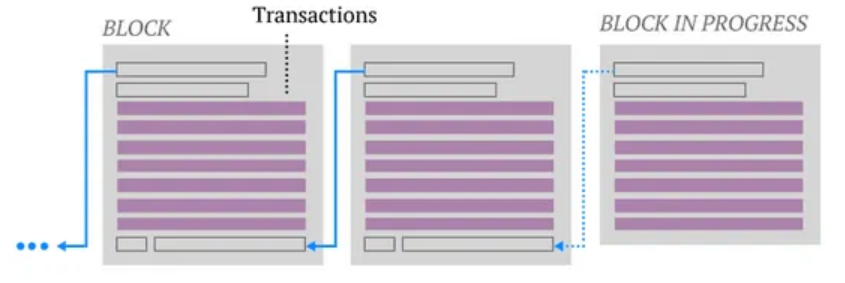
Blockchain

**La blockchain es una tecnología que permite crear un** [**libro de contabilidad (ledger) distribuida**](https://academy.bit2me.com/que-es-ledger-distribuido-libro-mayor/) **en una red de ordenadores sin necesidad de contar con un servidor o base de datos central. La actualización y manejo del mismo solo se puede realizar en consenso con todas las partes que forman la red (nodos).**

* **Bloques: conjunto de transacciones confirmadas e información adicional que se ha incluido en la cadena de bloques.**

**Sus componentes son:**

* + **Número de bloque**
  + **Hash bloque anterior**
  + **Timestamp: Marca de tiempo que determina el momento exacto en que se ha minado y validado el bloque.**
  + **Nonce: Número aleatorio.**
  + **Paquete de transacciones: Su tamaño depende de la blockchain específica. En Bitcoin es 1Mb, y en Ethereum depende de la cantidad de la cantidad de “gas”.**
  + **Hash final**

****

* **Nodos: ordenador/chip conectado a la red blockchain.**

**Hay tres tipos de nodos:**

* + **Nodos completos: Nodos que implementan el** [**software que almacena y distribuye una copia actualizada en tiempo real de la cadena de bloques**](https://bitcoin.org/en/es/descargar)**.**
    - **Nodos mineros: Ejecutan software de minería para realizar las Proof of Work (PoW). Por ejemplo. en la blockchain de Bitcoin.**
    - **Nodos validadores: Se encargan de las Proof of Stake (PoS). Por ejemplo, en la blockchain de Ethereum.**
    - **Nodos de autoridad: Se encargan de las Proof of Authority (PoA). Por ejemplo, en las blockchains privadas.**
    - **Nodos maestros: Estabilizan y protegen todo el ecosistema y pueden ofrecer servicios como transacciones privadas, transacciones instantáneas, gestión y financiación de tesorería, y votación de gobernanza.**
  + **Nodos ligeros o de luz: No descargan la blockchain de manera completa, si no que prefieren recibir la información a través de terceros.**

**Son utilizados por personas que se dedican básicamente a realizar o recibir transacciones en su vida cotidiana utilizando esta plataforma como medio de pago (exchanges).**

* **Wallets:**
  + **Full Wallets/Clients: Pertenecen a nodos completos.**
  + **Lightweight Wallets: Pertenecen a nodos ligeros.**
    - **Hot Wallet**
      * **Web**
      * **Desktop**
      * **App**
    - **Cold Wallet**
      * **Hardware**
      * **Paper**
* **Minería/Validación:**
  + **Proof of Work (PoW): Se usa en Bitcoin y en Ethereum.**
  + **Proof of Stake (PoS).**
  + **Proof of Authority (PoA).**
* **Cuentas/Addresses:**
  + **Cuentas de propiedad externa: Son direcciones con una wallet asociada.**
  + **Smart Contracts: Aparecieron en la red de Ethereum. Es un tipo especial de instrucciones que es almacenada en la** [**blockchain**](https://academy.bit2me.com/que-es-la-aleatoriedad-en-blockchain/)**. Y que además tiene la capacidad de autoejecutar acciones de acuerdo a una serie de parámetros ya programados. Todo esto de forma inmutable, transparente y completamente segura.**
* **Estado de la blockchain: Conjunto del estado de las cuentas.**
* **Estado de cuentas:**
  + **Balance: Cantidad de ethers que contiene.**
  + **Storage: Variables globales de la cuenta. En las cuentas de propiedad externa es un string vacío.**
  + **Nonce**
* **Interacciones con la Blockchain:**
  + **Lecturas: No consumen el estado de la blockchain. No se firman y no consumen gas.**
  + **Transacciones(escritura): Modifican el estado de la blockchain. Se firma con clave privada y consumen gas.**
* **Tokens: Son unidades de valor.**
  + **Tokens Fungibles: Aquellos que se pueden sustituir indistintamente.** 
    - **ICO: Criptomonedas. Este tipo de token está relacionado con el entorno blockchain que tiene detrás (bitcoins en la red Bitcoin, ethers en Ethereum…)**
    - **Utility Tokens (ITO): Es lo que se conoce popularmente como tokens. Tienen utilidad dentro de un entorno concreto de smart contracts. Ejemplo en la vida real: los billetes del monopoly.**

**Sigue el estándar ERC-20.**

* + - **Security Token: Relacionado con acciones o participaciones en un negocio.**

**Sigue el estándar ERC-1400.**

* + **Tokens No Fungibles (NFTs): Aquellos que NO se pueden sustituir indistintamente. Es decir, aquellos tokens que representan objetos, activos, o servicios de la vida real que tienen una identidad propia insustituible. Ejemplo en la vida real: La versión original de una obra de arte. Siguen el estándar ERC-721.**
* **Exchange: Es como una casa de cambio. Permite cambiar dinero fiat (real) a criptomonedas y almacenarlas en una wallet. Algunos exchanges tienen su propia wallet. Pueden ser online o físicos. Ejemplos: Binance, Bit2me (online, con wallet incluida), Bitcoin ATM (físico, sin wallet).**
* **Estándares**
  + **ERC-20**
  + **ERC-1400**
  + **ERC-721**
  + **ERC-165: Permite comprobar si un smart contract implementa una interfaz (contiene una serie de funciones) con el fin de utilizar delegatecall(). (ver Contract9.sol)**