

## Tema 7 & 8

Blockchain de Bitcoin es una estructura de datos matriz muy grande que almacena todas las transacciones entre direcciones en bloques encadenados entre sí. Este registro se distribuye a todos los nodos de la red y permite buscar información como cuánto Bitcoin tiene una dirección y qué transacciones se realizaron en un bloque específico.

La recuperación de información valiosa es gracias a los algoritmos hash y las estructuras de almacenamiento de datos. Además, la criptografía como vimos en un ejemplo de temas anteriores, se utiliza para generar direcciones y claves privadas. Conocer la clave privada de una dirección aplicada al algoritmo hash de Bitcoin permite al usuario acceder a la dirección y utilizar el protocolo para enviar y recibir Bitcoin una manera segura para las transacciones y el seguimiento de la moneda. La estructura de datos utilizada en la blockchain de Bitcoin es una Tabla Hash.

En resumen, la blockchain de Bitcoin utiliza una combinación de algoritmos hash, estructuras de almacenamiento de datos y criptografía para permitir operaciones básicas como buscar información, almacenar datos y enviar y recibir Bitcoin.

Para mayor información ver los siguientes artículos:

- Education Series: Hash Tables and Hash Algorithms – <https://medium.com/@quantalysis/education-series-hash-tables-and-hash-algorithms-5ec0d3f30a2d>
- If  $P = NP$ , Does Bitcoin Fall Apart? – <https://medium.com/predict/if-p-np-does-bitcoin-fall-apart-21534c16ab97>