En cadenas de bloques blockchain como Bitcoin, toda la "base de datos" de todas las transacciones entre direcciones se almacena en bloques encadenados entre sí. Este registro o libro mayor se distribuye a todos los nodos de la red

La blockchain es una estructura de datos matriz muy grande que permite buscar información como "cuánto Bitcoin" tiene una dirección y qué transacciones se realizaron en el bloque "1.476.203"

Los algoritmos hash y las estructuras de almacenamiento de datos permiten que la red almacene datos y recupere información valiosa rápidamente.

La belleza de Bitcoin es el uso de la criptografía 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.

En los siguientes artículos se explica el funcionamiento básico de la Tabla Hash de la blockchain de Bitcoin:
https://medium.com/@quantalysus/education-series-hash-tables-and-hash-algorithms-5ec0d3f30a2d

https://inleo.io/@leonordomonol/p-np-the-dangling-blackhole-under-crypto

https://www.reddit.com/r/AskComputerScience/comments/1c8z2iv/if_p_was_proved_to_equal_np_would_there_still_be/

https://www.youtube.com/watch?v=YIc6MNfv5iQ

El siguiente vídeo explica, más generalmente, la base como Estructura de Datos de Merkle Tree de Web3 o la Web Descentralizada (P2P)
https://www.youtube.com/watch?v=YIc6MNfv5iQ

Utilizando estas referencias o cualquier otra fuente que el alumno quiera utilizar, explicar de forma resumida la estructura de datos y algoritmos para realizar operaciones básicas en la Blockchain de Bitcoin

Estructura de Datos y Algoritmos en la Blockchain de Bitcoin

La blockchain de Bitcoin es una estructura de datos distribuida diseñada para almacenar transacciones de manera transparente y segura. Su diseño combina varias estructuras de datos y algoritmos clave:

Estructura de Datos en la Blockchain

Bloques:

Cada bloque contiene:

Lista de transacciones.
Un puntero hash al bloque anterior.
Datos adicionales como timestamp y nonce (para la prueba de trabajo).
Esto crea una cadena inmutable, ya que cualquier alteración en un bloque invalida los siguientes.

Árbol de Merkle:

Los datos de las transacciones dentro de un bloque se organizan en un árbol de Merkle.
Este permite verificar eficientemente la existencia de una transacción específica en el bloque, sin necesidad de revisar toda la cadena.

Tabla Hash:

Se utiliza para almacenar direcciones y claves asociadas, facilitando la búsqueda rápida de información como saldos y transacciones previas.

Algoritmos Clave

SHA-256:

Genera hashes únicos para los bloques y transacciones, asegurando integridad.
Este algoritmo permite que incluso un pequeño cambio en los datos genere un hash completamente diferente.

Prueba de Trabajo (Proof of Work):

Resuelve un problema criptográfico complejo para añadir nuevos bloques a la cadena.
Esto garantiza que añadir un bloque requiera recursos computacionales significativos, dificultando ataques.

Distribución P2P:

Cada nodo de la red mantiene una copia de la blockchain.
Los algoritmos de consenso, como el de Bitcoin (Proof of Work), aseguran que todos los nodos estén sincronizados y acuerden el estado de la cadena.

Implicaciones de P vs NP en Blockchain

La seguridad de la blockchain, como la de Bitcoin, se basa en que resolver problemas criptográficos (como el encontrar claves privadas) es significativamente más difícil que verificar su solución. Si P = NP fuera demostrado, la seguridad basada en criptografía podría verse comprometida, ya que estos problemas difíciles serían resolubles tan rápido como se verifican.

Proyecto interesante basado en la blockchain:
Votaciones democracia participativa.
El blockchain también es útil para sistemas de votación, resolviendo problemas como la falta de transparencia y la manipulación de resultados. Un caso práctico sería una plataforma de votaciones descentralizada basada en blockchain:

Estructura de Datos Aplicada:
Los votos se registran como transacciones en bloques, asegurando inmutabilidad.
Un árbol de Merkle permite verificar la validez de un voto rápidamente.

Operaciones Clave:
Emisión de votos:
Los ciudadanos emiten votos a través de claves privadas, registrándose en la cadena.
Auditoría:
Cualquier votante o entidad puede verificar los resultados sin acceso a datos personales.
Transparencia:
La cadena completa está disponible públicamente, mostrando el conteo en tiempo real.

La Plataforma como Follow My Vote y Democracy earth están diseñadas para procesos democráticos más seguros.
Estas soluciones eliminan intermediarios y reducen costos logísticos.

https://followmyvote.com/
https://democracy.earth/