

LAB01 - BLOCKCHAIN

Danh sách thành viên:

1. 22C11002 - Ngô Minh Đức
2. 22C11030 - Đặng Văn Hiền
3. 22C11035 - Đặng Trung Kiên

1. Cấu Trúc Dự Án:

Dự án được chia làm hai package là package main và package blockchain

Trong đó:

- package main có trách nhiệm tạo blockchain, thêm giao dịch và in ra màn hình.
- package blockchain có trách nhiệm định nghĩa cấu trúc Transaction, Block, Blockchain và một số các hàm tạo Block, tính Hash và một số các hàm tính toán và quản lý các Block và Blockchain

2. Cấu Trúc Dữ Liệu

- Transaction:

- + Data: Dãy byte chứa dữ liệu của giao dịch.

- Block:

- + Timestamp: Thời điểm tạo block theo định dạng Unix timestamp.
- + Transactions: Danh sách con trỏ đến các đối tượng Transaction.
- + PrevBlockHash: Dãy byte đại diện cho hash của block trước đó.
- + MerkleRoot: Dãy byte đại diện cho Merkle root của các giao dịch trong block.
- + Hash: Dãy byte đại diện cho hash của block hiện tại.

- Blockchain:

- + blocks: chứa con trỏ đến các đối tượng Block.

3. Nhận Xét về Thiết Kế và Thực Hiện

- Blockchain được hiện thực thông qua cấu trúc danh sách liên kết với con trỏ đến các block.
- Giao dịch được biểu diễn dưới dạng dãy byte, tạo linh hoạt cho việc sử dụng nhiều loại dữ liệu.
- Cây Merkle được hiện thực một cách hiệu quả để tính toán Merkle root cho việc xác minh giao dịch.

4. Hoạt Động của Hệ Thống

- Khởi Tạo: Blockchain được khởi tạo với một block genesis.
- Thêm Giao Dịch: Giao dịch được thêm vào blockchain, tạo ra các block mới.
- In Blockchain: Toàn bộ blockchain được in ra màn hình, hiển thị chi tiết từng block và các giao dịch của nó.

5. Thách Thức Trong Quá Trình Thực Hiện

- Lựa Chọn Cấu Trúc Dữ Liệu: Quyết định về biểu diễn của giao dịch và đảm bảo tính tương thích với cấu trúc cây Merkle.

Quản Lý Con Trỏ: Quản lý đúng con trỏ để tránh rò rỉ bộ nhớ và đảm bảo liên kết chính xác giữa các block.

6. Bài Học Học Được

- Khái Niệm Mật Mã: Hiểu rõ hơn về việc áp dụng mã hóa hash trong blockchain.

- Xử Lý Con Trỏ: Kỹ năng cải thiện trong việc quản lý con trỏ trong Go, đặc biệt là trong cấu trúc danh sách liên kết.

- Thiết Kế Modul: Sự quan trọng của việc có một cấu trúc dự án modul và có tổ chức để dễ bảo trì hơn.

7. Tham Khảo

- <https://go.dev/doc/>
- <https://viblo.asia/p/tuong-tac-voi-smartcontract-tren-blockchain-voi-go-phan-1-1Je5EjD4KnL>
- <https://academy.binance.com/vi/articles/double-spending-explained>
- <https://academy.binance.com/vi/articles/what-is-public-key-cryptography>