Cấu trúc Blockchain áp dụng công nghệ smart contract

1. Account

- Account là địa chỉ được tạo ra bởi ECDSA ( đối với ethereum).

- Địa chỉ được tạo ra bằng thuật toán sign publicKey và privateKey ngẫu nhiên, sau đó, được ghi ra file đi kèm password của người dùng nhập vào.

- Từ publicKey chúng ta có thể lấy được address của Account dạng bytes rồi chuyển qua hex string.

2. Database

- Database lưu trữ dự liệu về thông tin giao dịch, Pool chứa pending transaction, MerkelTree…. thường dùng LevelDb, MemoryDb hay Redis.

- Chỉ đơn giản các function: Add, Remove, Update, Delete

3. Network

- Chứa các Service về cách thức các Node kết nối đến với nhau, các thức tìm các node, bootnode

4. Protocol

- Chứa Service về download block, đồng bộ block, phản hồi yêu cầu từ các node khác trong mạng

5. Vm ( Virtual Matchine)

- Thành phần riêng biệt để chạy code smart contract. Dùng để complile code smart contract sang mã hex, validate code, execute code hex, lưu vào Db.

6. Core

7. Common

8. Consensus

- Chứa thuật toán đồng thuận về việc sinh ra block, ví dụ thuật toán DPOS hay POW

9. Rpc

- Http api server để client có thể tương tác với network thông qua rpc api

10. Cli

- dùng command line để tương tác với network

11. Wallet

- Quản lý các account có trong node hiện tại

12. Statistic

- Thống kê các thông số của network: Bao nhiêu node, bao nhiêu BP….

13. Cryptography

- Thuật toán liên quan đến mã hóa, sign address, verify dữ liệu, signature

14. Ledger

- Sổ cái, tại đây chứa các phương thức lưu trữ blockchain vào Db, validate block, validate transaction

Tiếp tục update chi tiết...