

I. Blockchain là gì

- . Công nghệ lưu trữ với các chuỗi khối tham chiếu lùi với nhau
- . Block có
 - . Metadata : ngày đào, số block, tham chiếu tới block trước đó
 - . Transaction : dữ liệu được thay đổi ntn trong block đó
- . Tính chất
 - . Immutability (không thể thay đổi dữ liệu)
 - . Decentralization (Ai cũng có thể lưu trữ block)

II. Bitcoin và Ethereum

- . Bitcoin
 - . Ứng dụng trong lưu trữ và vận chuyển tiền tệ
 - . Proof of work : người đầu tiên đào được 1 khối và ghi lên blockchain thì BTC mới sẽ được sinh ra để thưởng cho người đào
 - . Tổng cung 21tr (giúp giảm lạm phát)
 - > phức tạp, ít người dùng
- . Ethereum
 - . Ethereum Virtual Machine (EVM) chạy trên blockchain
 - . Dễ dùng, hỗ trợ smartcontract , không sửa được source code sau khi deploy

III. Cryptographic Hash

- . Là fingerprint để xác định một giao dịch
- . Mã sẽ thay đổi khi dữ liệu trong block thay đổi

IV. Wallet

- . Do bên thứ 3 tạo ra để quản lý các địa chỉ ví
- . Có thể gen ra trùng private key nhưng rất khó

V. Blockchain Address

- . Địa chỉ sử dụng để gửi và nhận tài sản trên blockchain
- . Privatekey --> Public key (128 ký tự) --> Publickey (64 ký tự) --> Address (lấy 42 ký tự cuối thêm 0x ở đầu)
- . Gồm
 - . EOA
 - . Contract Address

VI. Blockchain Transactions

- . Bất kỳ hành động nào thay đổi trên blockchain đều được gọi là Transactions
 - . Gửi nhận tiền
 - . Deploy smartcontract
 - . Gọi hàm trong smartcontract thay đổi giá trị trong block
- . Transaction gồm
 - . Địa chỉ from (người gửi) và to (người nhận)
 - . Gas và gas price
 - . Value (giá trị chuyển)
 - . Data được mã hóa thành chuỗi ký tự random
- . Vòng đời Transaction
 - . Build một Transaction gồm các trường dữ liệu

- . Dùng Privatekey để sign Transaction đó
- . send Transaction đó lên blockchain
- . Chờ verify (từ validator node hoặc minner node)
- . Nếu Transaction đã ghi lên blockchain sẽ trả về Transaction receipt

VII.Smart contract

- . Là các ứng dụng chạy trên blockchain thông qua EVM
- . Ưu điểm
 - . Code không thể thay đổi sau khi deploy
 - . Không bị quản lý bởi tổ chức/chính phủ
 - . Không cần sever
 - . Lưu chuyển tiền tệ dễ dàng
- . Nhược điểm
 - . Mắc vì cần trả tiền gas cho minner hay validator node
 - . Chậm
 - . Khả năng lưu trữ bị giới hạn do tốn chi phí
 - . smartcontract không gọi được API bên ngoài (đã được hỗ dẫn)
- . Build smartcontract
 - . Viết bằng solidity, Rush, Haskell, Viper
 - . Compile code thành EVM bytecode
 - . Gửi Transaction contract creation + EVM bytecode lên blockchain
 - . Chờ Transaction được đào
- . Giao tiếp smartcontract
 - . tạo Transaction để gọi hàm tới smartcontract
 - . trong hàm smartcontract có thể gọi hàm của smartcontract khác

VIII.Gas

- . Gas là phí giao dịch khi gửi 1 Transaction cần trả
- . trả cho minner hoặc validator node - người ghi block có chứa Transaction đó lên blockchain
- . người gửi Transaction là người trả dựa trên người sign Privatekey
- . trả bằng native token - ethereum
- . Gas phụ thuộc độ phức tạp của Transaction
- . Gas = tổng gas * gas private
- . Gas tính toán không xài hết thì gas dư sẽ được trả ngược về tài khoản
- >Wallet sẽ thực hiện tính gas

IX.Phỏng vấn Blockchain

- . Ethereum smartcontract là các ứng dụng nhỏ chạy trên blockchain Ethereum qua EVM
- . Điều đặc biệt nhất của smartcontract là sau khi deploy sẽ không thể sửa đổi source code
- . Có thể gọi 1 smartcontract bằng 1 smartcontract khác
- . smartcontract không thể gọi 1 API từ bên ngoài, chỉ lấy thông tin từ oracel chainlink gửi vào blockchain thông qua internal Transaction
- . smartcontract không lưu nhiều dữ liệu
- . Solidity, Rust, Viper, Haskell dùng để dev smartcontract, sau đó gen ra EVM bytecode

- . Có thể code nhiều smartcontract trong 1 file, chỉ cần định nghĩa contract nhiều lần trong file solidity
- . Solidity là static (cần định nghĩa kiểu dữ liệu trước khi xài)
- . Để xem và dữ liệu blockchain dựa trên block explore
- . ABI là Application Binary Interface
 - . sinh ra sau khi compile smartcontract.
 - . Là signature của smartcontract, chứa thông tin về thông số nhận vào và dữ liệu trả ra của hàm
 - . Dùng bởi các thư viện của bên thứ 3 để giao tiếp với smartcontract