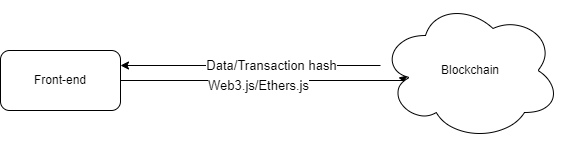
Phần 1: Lý thuyết

Câu 1:

Dapp được viết tắt của Decentralize Application là ứng dụng phi tập trung sử dụng Blockchain để vận hành và lưu trữ dữ liệu 1 cách phân tán thay vì sử dụng 1 Server tập trung dữ liệu tại 1 nơi.

Cách vận hành:

Fronte-end sử dụng thư viện Web3.js/Ethers.js để truy cập node trên mạng Blockchain, từ đó thông qua thư viện gọi đến Smart Contract có hàm cần sử dụng như 1 API ở Server tập trung

Câu 2:

Thuật toán ECDSA là thuật toán bất đối xứng

Chữ ký được biểu diễn bởi 1 cặp (r, s)

*Pha tạo chữ ký*:

* Tạo số ngẫu nhiên *k*
* Tính P = *k* × G (điểm sinh chọn tự đường cong Elliptic) → P(x, y) → r = x (của P)
* Ta có *z* (hash của message cần ký) → s ≡ *k-1*(*z* + dA × r ) (mod p)

→ Ta có cặp (r (publickey dùng làm address ví), s (privatekey))

*Pha xác thực chữ ký*:

Câu 3:

Mật mã đối xứng chỉ dùng 1 key để mã hóa và giải mã nhưng có tốc độ nhanh

Mật mã bất đối xứng dùng 2 key là 1 key dùng để mã hóa và 1 key dùng để giải mã trong đó 2 key nhân modulo lại với nhau sẽ bằng 1, tốc độ chậm

Câu 4:

Blockchain là 1 hệ thống database phân tán trong đó các dữ liệu được lưu ở dạng các block. Body của block chứa các transaction. Block được kết nối với nhau theo dạng linked list dưới dạng mã hóa SHA256. Mã hóa của một block bao gồm cả địa chỉ của block trước và body của chính nó nên khi một block được add vào, nó không thể thay đổi cũng như tái sắp xếp. Trong đó transaction sẽ chứa các data được truyền đi.

Mạng Blockchain bao gồm các node lưu bản sao của Blockchain cũng như để xác thực bản sao này là chính xác phải thông qua cơ chế đồng thuận.

Câu 7:

Blockchain thế hệ 2 có sử dụng Smart Contract trên hệ thống Virtual Machine

Có 3 loại blockchain:

* Public: cho phép mọi người có quyền đọc, ghi dữ liệu ở Blockchain
* Private: chỉ cho phép bạn đọc dữ liệu, không được gh
* Hybrid: Kết hợp 2 loại trên

Câu 8:

Smart Contract (hay Hợp đồng thông minh) là các chương trình chạy trên blockchain. Hợp đồng thông minh cũng giống như một hợp đồng kỹ thuật số bị bắt buộc thực hiện bởi một bộ quy tắc cụ thể. Các quy tắc này do bộ mã máy tính xác định trước mà tất cả các nút (node) trong mạng đều phải sao chép và thực thi các quy tắc đó.

Câu 9:

Hàm băm là giải thuật nhằm sinh ra các mã băm tương ứng với mỗi khối dữ liệu. Mã băm đóng vai gần như toàn vẹn thông tin để phân biệt các khối dữ liệu.

Câu 10:

* Phi tập trung: chỉ việc chuyển quyền kiểm soát và ra quyết định từ một thực thể tập trung (cá nhân, tổ chức hoặc nhóm) sang một mạng lưới phân tán
* Bất biến: một cái gì đó không thể thay đổi hay biến đổi được. Không người tham gia nào có thể làm giả giao dịch sau khi ai đó đã ghi lại giao dịch này vào sổ cái được chia sẻ.
* Đồng thuận: thiết lập các quy tắc về sự đồng thuận của người tham gia cho phép ghi lại các giao dịch. Bạn chỉ có thể ghi lại các giao dịch mới khi đa số người tham gia mạng lưới đồng thuận.

Câu 12:

Không ai quản lý các mạng Blockchain

Câu 13:

Câu 15: SHA256

Câu 16:

RSA là một hệ mã hóa bất đối xứng

Gồm cặp khóa (e, d) trong đó e là public key và d là private key

**Pha 1: Sinh khóa**

Mấu chốt cơ bản của việc sinh khóa trong RSA là tìm được bộ 3 số tự nhiên e, d và n sao cho:

med ≡ m mod n

Cụ thể, khóa của RSA được sinh như sau:

* Chọn 2 số nguyên tố p, q
* n = p × q
* Tính φ(n) = BCNN(p – 1, q - 1)
* Chọn e là số tự nhiên trong khoảng [1, φ(n)] sao cho ƯCLN(e, φ(n)) = 1 (nguyên tố cùng nhau)
* Tính d = e-1 (mod n) → ed ≡ 1 (mod n)

**Pha 2: Mã hóa**

C ≡ me (mod n)

**Pha 3: Giải mã**

m ≡ cd ≡ med ≡ m (mod n)

*Ví dụ*:

p = 5, q = 7

=> n = pq = 35

=> φ(n) = 24

=> e = 5, d = 29

Giả sử m = 32 → c = 325 % 35 = 2

m’ = 229 % 35 = 32 = m

Câu 17: Mạng Bitcoin không có máy chủ

Câu 18: Chữ ký số