Câu hỏi ôn tập môn BlockChain

1. **Bitcoin là gì? Trình bày đặc điểm chính và các thuật toán đồng thuận của bitcoin**

Khái niệm:

- Bitcoin là một loại tiền kỹ thuật số, được sử dụng và phân phối điện tử.
- Bitcoin là một mạng ngang hàng phi tập trung, không một cá nhân hay một tổ chức nào kiểm soát nó.
- Bitcoin không thể được in ra và số lượng của chúng rất hạn chế – chỉ có 21 triệu bitcoin có thể được tạo ra.

Đặc điểm:

- Phi tập trung
- Ẩn danh
- Minh bạch
- Nhanh chóng
- Không thể trả lại

Cơ chế đồng thuận:

- Đồng thuận là sự đồng ý của cả mạng lưới.
- Cơ chế đồng thuận là một phương pháp tạo ra sự quyết định đồng thuận.
- Có rất nhiều cơ chế đồng thuận. Nhưng có 2 cơ chế đồng thuận được sử dụng nhiều nhất hiện nay đó là Proof of Work và Proof of Stake
- PoW (Proof of work) là một cơ chế đồng thuận sử dụng cho Bitcoin.

2. **ETH là gì? Trình bày đặc điểm chính và các thuật toán đồng thuận của ETH**
3. **Cây merkle root là gì? Trình bày các tạo cây.**

Khái niệm:

Cây Merkle (Merkle Tree) là một cấu trúc dữ liệu được sử dụng trong các ứng dụng khoa học máy tính. Trong bitcoin và các loại tiền mã hóa khác, cây Merkle phục vụ để mã hóa dữ liệu blockchain hiệu quả và an toàn hơn. Chúng cũng được gọi là **cây băm nhị phân**

Cách tạo cây:

Mỗi giao dịch được băm, sau đó mỗi cặp giao dịch được nối và băm với nhau, và cứ như vậy cho đến khi có một hàm băm cho toàn bộ khối. (Nếu có số lượng giao dịch lẻ, một giao dịch được nhân đôi và hàm băm của nó được nối với chính nó.)

4. Số nonce trong bitcoin, cách sử dụng số nonce

Khái niệm:

Nonce (số chỉ được sử dụng một lần) là số cho phép một nút (mining node) có quyền xuất bản khối.

Cách sử dụng:

Khai thác thành công một khối đòi hỏi một người khai thác phải là người đầu tiên đoán ra số nonce, đó là một chuỗi số ngẫu nhiên. Số này được thêm vào nội dung băm của khối, và sau đó được thử lại. Nếu hàm băm đáp ứng các yêu cầu được đặt ra trong mục tiêu, thì khối được thêm vào blockchain. Đi qua các giải pháp để đoán nonce được gọi là bằng chứng công việc (POW) và người khai thác có thể tìm thấy giá trị được trao khối và trả bằng coin.

5. Trình bày thuật toán đồng thuận PoW, ưu và nhược điểm của PoW

Trong PoW, mỗi nút của mạng sẽ tính toán giá trị băm của tiêu đề khối. Các tiêu đề khối chứa một nonce và thợ mỏ sẽ thay đổi nonce thường xuyên để có được giá trị băm khác nhau. Sự đồng thuận yêu cầu giá trị được tính phải bằng hoặc nhỏ hơn một giá trị nhất định

Sau khi tìm được số nonce phù hợp. Nút sẽ công bố khối tới các nút khác và tất cả các nút khác cùng nhau xác định tính chính xác của giá trị băm. Giả sử có một nút muốn thay đổi, giả mạo khối vừa đến. Thì mã hash sẽ thay đổi khiến mạng lưới từ chối khối mới này.

Ưu điểm:

- PoW giải quyết tốt vấn đề đồng thuận.
- Đơn giản thực hiện.

Nhược điểm:

- Tiêu tốn năng lượng điện và cuộc chạy đua phần cứng
- Tiềm ẩn nguy cơ tấn công 51%
- Đào rất chậm

6. Trình bày thuật toán đồng thuận PoS, ưu và nhược điểm của PoS

- PoS (Proof of stake) là một giải pháp tiết kiệm năng lượng cho PoW. Các thợ mỏ (người xác thực) trong PoS phải chứng minh quyền sở hữu số lượng tiền tệ. Người ta tin rằng những người có nhiều tiền hơn sẽ ít có khả năng tấn công mạng.
- Người xác thực thực ra không được chọn một cách ngẫu nhiên trên mạng. Để trở thành một Người xác thực thì người này phải bỏ một khoản tiền vào mạng lưới. Khoản tiền này gọi là Stake
- Khoản tiền này sẽ bị hệ thống thực hiện lock. Kích thước của stake quyết định cơ hội được chọn làm người tạo ra khối mới của Người xác thực.
- Ngoài cổ phần, thì tỉ lệ được chọn còn phụ thuộc vào khoảng thời gian mà cổ phần được giữ. (tuổi của đồng tiền)
- Trong PoS. Nếu một node được chọn làm người xác thực khối mới. Node này phải kiểm tra tất cả các giao dịch là hợp lệ.
- Khi mọi thứ kiểm tra xong. Node này phải ký tên vào block và thêm nó vào chuỗi. Phần thưởng cho node này là phí giao dịch của các giao dịch trong block.
- Stake được khóa lại lúc đầu. Khi có gian lận. Toàn bộ số tiền mà node dùng để stake bị khóa lúc đầu sẽ mất.
- Để đảm bảo thì số tiền dùng để Stake lớn hơn chi phí giao dịch.
- Nếu một node dừng làm người xác thực, số tiền ban đầu và số tiền họ kiếm được sẽ được hoàn trả sau khi mạng lưới xác thực node này không gian lận.
- Có một thực tế là người đặt nhiều Stake hơn sẽ được chọn thường xuyên hơn. Kiếm được nhiều tiền hơn. Coin age (tuổi của coin) được đưa ra để giải quyết vấn đề này.
- Một vấn đề tiềm ẩn khác là khi mạng chọn người xác thực tiếp theo nhưng anh ta không bật lên để làm công việc của mình. Đơn giản chỉ cần chọn nhiều người xác thực để dự phòng.

Ưu điểm:

- Xử lý giao dịch nhanh chóng.
- Ngược lại với PoW, PoS không gây hại đến môi trường.
- Không dễ bị chính quyền tấn công: không cần lượng điện năng khổng lồ.
- Có thể được thực hiện trên các thiết bị nhỏ hơn

Nhược điểm:

- Người giàu thì càng giàu.
- Không phụ thuộc yếu tố bên ngoài.

7. Sự khác biệt giữa PoW và PoS

Đối với PoW người dùng cần phải có máy đào, internet… họ làm việc và tạo ra lợi nhuận, PoS thể hiện sự giàu có, người dùng sử dụng coin của họ để tạo ra lợi nhuận.

8. Các hình thức tấn công vào mạng Bitcoin, ETH.

9. Double spending là gì? Cách phòng chống

- Khi tôi thực hiện giao dịch 100 Bitcoin. Giao dịch này được xác nhận và ví tiền bị trừ 100 bitcoin.
- Tuy nhiên Miner có thể không công khai block của mình và tạo một blockchains con không được khai báo
- Với sức mạnh tính toán tương đương 51% toàn bộ mạng lưới máy đào, Miner định tấn công có thể tạo ra một chuỗi khối dài hơn. Sau khi tạo ra chuỗi khối dài hơn, người này sẽ công bố với mạng lưới.

Cách phòng chống:

Các nhà điều hành ví giữ liên kết mạnh mẽ với các nút đào để truyền các giao dịch một cách trực tiếp – do đó một giao dịch khác sử dụng cùng một đầu ra với ý định gian lận không thể được đưa vào mạng lưới.

10. Trình bày về phân loại mạng BlockChain

Permissionless là các nền tảng phi tập trung và được mở để tham gia mà không cần người dùng yêu cầu quyền truy cập hay còn gọi là Public blockchain

Bất cứ ai có thể tham gia mạng, tham gia vào quá trình xác minh khối để tạo ra sự đồng thuận hoặc tạo ra các hợp đồng thông minh.

Ứng dụng:

- Ứng dụng công chứng, chứng minh quyền sở hữu
- Công nghiệp năng lượng

Permissioned là một nên tảng phi tập trung yêu cầu người muốn tham gia phải được phép của tổ chức sáng lập mạng lưới

Trong Permissioned blockchain, chỉ một nhóm người dùng mới có quyền xác thực các giao dịch, khối.

Các Permissioned blockchain có thể được thiết lập để mọi người có thể đọc chúng, nhưng chỉ các thành viên được chọn mới có thể ghi lại các giao dịch trên chúng

Ứng dụng:

- Ngân hàng
- Chuỗi cung ứng
- Bảo hiểm chăm sóc sức khỏe

Public Blockchain cho phép bất cứ ai có quyền tham gia vào quy trình xác định khối nào được thêm vào chuỗi

Bất cứ ai cũng có thể giao dịch trong mạng Blockchain. Các giao dịch phảiđược thực hiện miễn là chúng hợp lệ.

Bất kỳ ai cũng có thể truy cập và đọc các giao dịch bằng cách sử dụng block explorer. Giao dịch là minh bạch nhưng ẩn danh.

Private BlockChain: Ngườidùng chỉ được quyền đọc dữ liệu, không có quyền ghi vì điều này thuộc về bên tổ chức thứ ba tuyệt đối tin cậy.

Bên thứ ba toàn quyền quyết định mọi thay đổi trên Blockchain. Vì đây là một Private Blockchain, nên thời gian xác nhận giao dịch khá nhanh vì chỉ cần một lượng nhỏ thiết bị tham gia xác thực giao dịch.

Consortium blockchain: Là một loại blockchain Permissioned

Thay vì cho phép bất kỳ người nào có kết nối internet tham gia vào quá trình xác minh giao dịch hoặc chỉ cho phép một công ty có toàn quyền kiểm soát, một số nút được chọn được xác định trước.

Cung cấp nhiều lợi ích tương tự private blockchain - hiệu quả và sự riêng tư giao dịch, mà không cần hợp nhất quyền lựcvới chỉ một công ty.

Consortium blockchain có nhiều lợi thế giống với một private blockchain, nhưng hoạt động dưới sự lãnh đạo của một nhóm thay vì mộtthực thể duy nhất.

11. **Public key được sử dụng trong BlockChain như thế nào?**
    - Tạo địa chỉ.
    - Xác minh chữ ký số.

12. **Private key được sử dụng trong BlockChain như thế nào?**

- Tạo chữ ký số, ký vào giao.
- Bảo mật tài khoản.

13. **BlockChain là gì? Các thành phần chính được sử dụng trong BlockChain?**

Khái niệm:

Blockchain là một sổ cái kỹ thuật số bất biến, bảo mật, chống giả mạo và được chia sẻ, lưu trữ phân tán; trong đó ghi lại lịch sử giao dịch tài sản giữa các thành viên trong mạng ngang hàng (Peer to Peer Network).

Thành phần công nghệ:

- Sổ cái số chia sẻ (shared digital Ledgers)
- Transactions (giao dịch)
- Lý thuyết mã hóa
  - Hàm băm (hash function)
  - Mật mã hóa khóa bất đối xứng (Asymmetric - Key Cryptography): Public and Private Keys
- Blocks
- Chaining Blocks

14. **Node là gì? Phân loại các node?**

Có hai loại node:

- Full node :Các máy tính lưu trữ dữ liệu blockchain, truyền dữ liệu đến các nút khác và đảm bảo các khối mới được thêm vào hợp lệ.
- Lightweight node :không cần lưu trữ bản sao đầy đủ của blockchain và chúng thường chuyển dữ liệu của chúng đến các full node để được xử lý

Bất kỳ nút nào cũng có thể đề xuất các giao dịch mới và các giao dịch được đề xuất này được truyền đi giữa các nút cho đến khi chúng được thêm vào một khối.

15. **EVM trong Ethereum là gì , cách hoạt động của EVM.**
16. **Trình bày về Casper trong Ethereum là gì? Casper được sử dụng như thế nào trong Ethereum.**
17. **Khối epoch là gì, nó được sử dụng trong Ethereum như thế nào.**
18. **Trình bày về Slash trong Ethereum.**

19. Địa chỉ của bitcoin là gì, cách tạo ra địa chỉ.

Địa chỉ Ví Bitcoin hay gọi tắt là địa chỉ Bitcoin chính là cái địa chỉ để người khác có thể chuyển Bitcoin cho bạn

Cách tạo địa chỉ: Băm PublicKey.

20. Sổ cái trong mạng bitcoin là gì? Nêu cách lưu trữ sổ cái và các đặc điểm của sổ cái trong mạng blockchain.

Sổ cái là một tập hợp các giao dịch.

Sổ cái blockchain sẽ được sao chép và lưu trữ phân tán tại các nút (node) trong hệ thống blockchain.

Các giao dịch mới được gửi đến một nút, sau đó sẽ thông báo tới phần còn lại của mạng là có một giao dịch mới đã đến.

Một nút sẽ lưu giao dịch mới này trong một khối và hoàn thành phương thức đồng thuận cần thiết của hệ thống

Khối mới này sẽ được phân phối trên toàn hệ thống và tất cả các sổ cái sẽ được cập nhật để bao gồm giao dịch mới

21. Các chức năng của một nút trong mạng Bitcoin. Mô tả chi tiết của từng chức năng

22. Các hạn chế của Blockchain

- Người dùng độc hại
  - Trong blockchain, người dùng hoàn toàn ẩn danh và thực hiện các giao dịch qua địa chỉ được sinh ra từ khóa công khai. Những người dùng cố ý phá hoại mạng lưới là ẩn danh.
  - Từ chối truyền các khối đến các nút khác, về cơ bản làm gián đoạn việc phân phối thông tin
  - Tạo chuỗi thay thế chuỗi chính thức của mạng lưới khi người dùng có đủ sức mạnh khả năng tính toán.
- Vấn đề về sử dụng tài nguyên năng lượng
  - Với thuật toán đồng thuận proof of work, quá trình tìm ra khối mới tốn nhiều năng lượng điện.
  - Khi kích cỡ của blockchain lớn, quá trình sinh ra một full node sẽ tốn nhiều băng thông

- Thời gian xử lý giao dịch chậm với public blockchain
  - Quá trình xác nhận giao dịch cũng như xác nhận các khối trở nên chậm chạp khi mạng lưới có kích cỡ lớn.
- Mức độ an toàn phụ thuộc vào kích cỡ mạng lưới
  - Blockchain có mức độ an toàn cao khi có kích cỡ mạng lưới lớn.
  - Ngược lại, nếu kích cỡ mạng lưới blockchain thì mạng lưới dễ dàng bị thực hiện các cuộc tấn công 51%
- Khai thác ích kỷ
  - Những nút khai thác ích kỷ thực hiện khai thác nhưng không truyền đi các nhánh họ đã khai thác được và các nhánh riêng sẽ được công khai khi thỏa mãn một số điều kiện.
  - Do tính chất thừa nhận chuỗi dài nhất là chuỗi chính thức nên khi chuỗi riêng của các nút khai thác ích kỷ được công khai thì các nút khai thác sẽ rời bỏ nhánh chính thức ngắn hơn .

23. Mining là gì, trình bày quá trình mining và xác nhận khối trong mạng Bitcoin