Tên: Nguyễn Đình Nhật Vinh

Lớp: 21SE3

MSV: 21IT253

**Câu 1**: Tìm hiểu về BlockChain

**Blockchain** là một công nghệ lưu trữ và truyền tải dữ liệu dưới dạng các khối (blocks) được liên kết với nhau bằng mã hóa, tạo thành một chuỗi liên tục (chain). Các đặc điểm chính của blockchain bao gồm:

1. **Phân tán và phi tập trung**: Dữ liệu được lưu trữ trên nhiều nút (nodes) khác nhau trong mạng, không phụ thuộc vào một trung tâm duy nhất, giúp giảm thiểu nguy cơ bị tấn công hoặc mất dữ liệu.
2. **Minh bạch và không thể thay đổi**: Mọi giao dịch đều được ghi lại công khai, không thể sửa đổi hay xóa bỏ sau khi được xác nhận.
3. **Bảo mật cao**: Các giao dịch và thông tin được mã hóa bằng các thuật toán mạnh mẽ, đảm bảo an toàn cho dữ liệu.

Blockchain thường được sử dụng trong nhiều lĩnh vực như:

* **Tài chính**: Tiền mã hóa (cryptocurrency) như Bitcoin, Ethereum.
* **Hợp đồng thông minh**: Thực hiện các giao dịch tự động theo điều kiện đã định trước.
* **Chuỗi cung ứng**: Theo dõi nguồn gốc và hành trình của hàng hóa.
* **Lưu trữ dữ liệu**: Xác thực tài liệu và danh tính số.

**Câu 2**: Mạng phân tán là gì

**Mạng phân tán** (distributed network) là một hệ thống mà trong đó các tài nguyên, dữ liệu hoặc nhiệm vụ được phân phối và xử lý trên nhiều nút (nodes) độc lập, thay vì tập trung vào một máy chủ duy nhất. Các nút trong mạng phân tán có thể là máy tính, máy chủ hoặc các thiết bị khác kết nối với nhau qua mạng.

**Đặc điểm của mạng phân tán:**

1. **Phi tập trung**: Không có một nút trung tâm nào kiểm soát toàn bộ hệ thống. Mỗi nút có vai trò độc lập và tự chủ.
2. **Khả năng mở rộng cao**: Hệ thống có thể dễ dàng mở rộng bằng cách thêm các nút mới mà không làm giảm hiệu suất tổng thể.
3. **Khả năng chịu lỗi tốt**: Nếu một số nút bị hỏng, các nút khác vẫn có thể hoạt động và duy trì hệ thống. Điều này giúp tăng độ tin cậy.
4. **Tính đồng nhất**: Các nút trong mạng có thể chia sẻ và đồng bộ hóa dữ liệu với nhau.

**Ưu điểm của mạng phân tán:**

* **Hiệu suất cao**: Nhiều nút có thể xử lý các nhiệm vụ cùng lúc, giảm tải cho từng nút cụ thể.
* **Độ bền**: Hệ thống vẫn hoạt động tốt ngay cả khi một số thành phần bị lỗi.
* **Tăng cường bảo mật**: Dữ liệu không tập trung vào một điểm duy nhất, khó bị tấn công hoặc đánh cắp.

**Ứng dụng của mạng phân tán:**

* **Blockchain**: Lưu trữ dữ liệu giao dịch trên nhiều nút, đảm bảo an toàn và minh bạch.
* **Lưu trữ đám mây phân tán**: Ví dụ như IPFS hoặc Storj, phân phối dữ liệu trên nhiều máy chủ.
* **Internet of Things (IoT)**: Các thiết bị IoT kết nối và chia sẻ dữ liệu với nhau.
* **Hệ thống tài chính**: Giao dịch phi tập trung trong tiền mã hóa

**Câu 3**: Tìm hiểu chuyên sâu về SHA 256

**SHA-256** (Secure Hash Algorithm 256-bit) là một thuật toán băm mật mã thuộc họ SHA-2, được phát triển bởi **Cơ quan An ninh Quốc gia Hoa Kỳ (NSA)** và công bố bởi Viện Tiêu chuẩn và Công nghệ Hoa Kỳ (NIST). SHA-256 được sử dụng rộng rãi trong bảo mật, đặc biệt là trong các hệ thống blockchain và chứng thực dữ liệu.

**Tính chất của SHA-256:**

1. **Hàm băm một chiều**:
   * Không thể đảo ngược (từ kết quả băm quay lại dữ liệu gốc).
   * Đảm bảo tính bảo mật cao.
2. **Đầu ra cố định**:
   * Bất kể dữ liệu đầu vào dài hay ngắn, đầu ra luôn là một chuỗi 256-bit (64 ký tự thập lục phân).
3. **Tính xác định**:
   * Cùng một đầu vào luôn cho ra một đầu ra duy nhất.
4. **Tính nhạy cảm với thay đổi**:
   * Một thay đổi nhỏ trong dữ liệu đầu vào sẽ tạo ra kết quả băm hoàn toàn khác biệt.
5. **Không đụng độ (collision)**:
   * Khả năng hai dữ liệu khác nhau cho ra cùng một giá trị băm rất thấp.

**Cách SHA-256 hoạt động:**

SHA-256 thực hiện quá trình băm dữ liệu thông qua các bước chính:

1. **Bước 1: Tiền xử lý**
   * **Bổ sung bit (Padding)**: Dữ liệu đầu vào được bổ sung thêm một số bit để chiều dài trở thành bội số của 512.
   * **Bổ sung chiều dài**: Thêm 64 bit cuối để biểu diễn chiều dài ban đầu của dữ liệu.
2. **Bước 2: Chia dữ liệu thành khối**
   * Dữ liệu được chia thành các khối 512-bit để xử lý.
3. **Bước 3: Khởi tạo giá trị băm ban đầu (IV)**
   * Sử dụng 8 hằng số 32-bit được xác định trước.
4. **Bước 4: Xử lý từng khối dữ liệu**
   * Thực hiện 64 vòng lặp (rounds) với mỗi khối, sử dụng các hằng số và hàm logic như XOR, AND, OR, cùng với các phép quay và dịch bit.
5. **Bước 5: Kết hợp giá trị**
   * Sau khi xử lý toàn bộ các khối, giá trị băm cuối cùng được ghép lại từ 8 giá trị 32-bit thành chuỗi 256-bit.

**Ứng dụng của SHA-256:**

1. **Blockchain**:
   * Dùng để tạo mã băm của các khối trong chuỗi khối.
   * Đảm bảo tính toàn vẹn của dữ liệu giao dịch.
2. **Chữ ký số và chứng chỉ số**:
   * Tạo mã băm của tài liệu để ký số hoặc xác thực tài liệu.
3. **Xác thực mật khẩu**:
   * Băm mật khẩu người dùng trước khi lưu trữ.
4. **Hệ thống kiểm tra tính toàn vẹn dữ liệu**:
   * So sánh mã băm của dữ liệu trước và sau khi truyền tải để phát hiện thay đổi.

**Ưu điểm của SHA-256:**

* Tính bảo mật cao và chống lại các tấn công phổ biến như tấn công đụng độ (collision) và tấn công tiền hình ảnh (preimage attack).
* Được tiêu chuẩn hóa và sử dụng rộng rãi trong nhiều ứng dụng bảo mật.

**Nhược điểm:**

* **Tốc độ chậm**: So với một số thuật toán băm khác, SHA-256 có tốc độ xử lý chậm hơn.
* **Kích thước đầu ra lớn**: Với 256-bit, SHA-256 có thể không tối ưu trong một số hệ thống yêu cầu lưu trữ hạn chế.

**Câu 4**: Tìm hiểu về cách lưu dữ liệu trên nền tảng BlockChain

**Lưu trữ dữ liệu trên nền tảng Blockchain** là một quá trình mà dữ liệu được ghi và duy trì trong các khối (blocks) trên một chuỗi liên kết phi tập trung. Phương pháp này không chỉ đảm bảo tính toàn vẹn và minh bạch của dữ liệu mà còn giúp bảo mật và chống lại các hành vi gian lận hoặc giả mạo.

**Cách lưu trữ dữ liệu trên Blockchain**

Dữ liệu được lưu trữ trên blockchain qua các bước cơ bản sau:

1. **Ghi dữ liệu vào khối (block):**
   * Dữ liệu được tổ chức thành các giao dịch (transactions) hoặc bản ghi (records).
   * Mỗi khối có một kích thước giới hạn (ví dụ: Bitcoin là 1MB).
2. **Liên kết các khối với nhau:**
   * Mỗi khối chứa một giá trị băm (hash) đại diện cho nội dung của nó và giá trị băm của khối trước đó.
   * Điều này tạo ra một chuỗi khối không thể thay đổi: nếu một khối bị chỉnh sửa, toàn bộ chuỗi sẽ không hợp lệ.
3. **Phân phối dữ liệu trên mạng phân tán:**
   * Blockchain là một mạng lưới phi tập trung, nơi dữ liệu được lưu trữ trên nhiều nút (nodes).
   * Mọi nút đều có một bản sao đầy đủ của chuỗi khối, đảm bảo tính đồng nhất và toàn vẹn.
4. **Xác thực và thêm khối mới:**
   * Trước khi dữ liệu được thêm vào blockchain, mạng phải xác thực thông qua các thuật toán đồng thuận (consensus), ví dụ như Proof of Work (PoW) hoặc Proof of Stake (PoS).

**Loại dữ liệu được lưu trữ trên Blockchain**

1. **Dữ liệu giao dịch:**
   * Ghi nhận thông tin về các giao dịch, ví dụ: địa chỉ ví, số tiền chuyển, thời gian thực hiện (Bitcoin, Ethereum).
2. **Dữ liệu hợp đồng thông minh:**
   * Lưu trữ các điều khoản và logic của hợp đồng thông minh.
3. **Tài liệu hoặc tệp:**
   * Lưu trữ hash của tài liệu hoặc tệp để đảm bảo tính toàn vẹn, thay vì lưu toàn bộ tệp trên blockchain.
4. **Danh tính số:**
   * Xác thực danh tính cá nhân hoặc doanh nghiệp.
5. **Chuỗi cung ứng:**
   * Theo dõi nguồn gốc và hành trình của sản phẩm.

**Cơ chế lưu trữ dữ liệu:**

Blockchain lưu trữ dữ liệu chủ yếu thông qua hai cách chính:

1. **On-chain (Trên chuỗi):**
   * Dữ liệu được lưu trữ trực tiếp trong các khối của blockchain.
   * Ưu điểm: Tính toàn vẹn và bảo mật cao.
   * Nhược điểm: Kích thước khối có giới hạn, chi phí lưu trữ cao.
2. **Off-chain (Ngoài chuỗi):**
   * Chỉ lưu giá trị băm hoặc liên kết đến dữ liệu thực trên blockchain, trong khi dữ liệu thực được lưu trữ ở các hệ thống bên ngoài (ví dụ: IPFS, hệ thống lưu trữ đám mây).
   * Ưu điểm: Giảm tải cho blockchain, lưu trữ dữ liệu lớn hơn.
   * Nhược điểm: Phụ thuộc vào hệ thống bên ngoài.