Script 1:

Hàm hash là một hàm số dùng để chuyển đổi dữ liệu từ một kích thước bất kì sang một kích thước nhất định.

Hàm hash là một hàm một chiều, không thể nghịch đảo và có độ dài cố định vậy nên ta không thể suy ngược đầu vào của một giao dịch từ kết quả hash cũng như suy luận lượng thông tin đầu vào dựa vào độ dài của kết quả hash.

Kết quả của hàm Hash là duy nhất đối với một đầu vào nhất định. Do vậy, người ta dùng kết quả của hàm hash để kiểm tra đầu vào giao dịch có đúng không mà không cần tiết lộ dữ liệu.

Các thuật toán hash được sử dụng rộng rãi là MD5 và SHA256. Trong đó MD5 tạo ra giá trị băm 128 bit và SHA256 tạo ra giá trị băm là 256bit và trong thực tế thì hàm SHA256 được chứng minh là an toàn và được sử dụng rộng rãi hơn.

Trong Blockchain thì các giá trị đầu ra từ hàm hash được sử dụng làm các định danh duy nhất cho các Block. Hàm hash nhận các đầu vào là dữ liệu đã mã hóa của block đó chứa thông tin về các giao dịch, thông tin về thời gian block đó được tạo ra, giá trị hash của block trước đó,…

Vì block phía sau sử dụng lại giá trị hash của block phía trước, từ đó tạo thành một chuỗi liên kết trong Blockchain.

Bởi vì vậy nên khi ta thay đổi nội dung của một Block thì giá trị hash của tất cả Block nằm phía sau trong chuỗi cũng phải thay đổi theo để tạo thành một chuỗi hợp lệ. Nhờ tính chất này nên người ta đã tận dụng và tạo ra cơ chế đồng thuận trong Blockchain.

Cơ chế đồng thuận blockchain có thể được định nghĩa là một cơ chế mà qua đó các nút phân tán trong hệ thống đều đạt được sự đồng thuận.

Trong cấu trúc truyền thống, sự đồng thuận hiếm khi là vấn đề nhờ vào sự tồn tại của cơ quan trung ương. Trái lại, trong một hệ thống phân tán như blockchain, mỗi giao điểm vừa là máy chủ vừa là không gian lưu trữ dữ liệu. Vì vậy, mỗi giao điểm phải trao đổi thông tin với giao điểm khác để đạt được sự đồng thuận.

Có hai cơ chế đồng thuận được sử dụng rộng rãi trong Blockchain, đó là Proof of Work và Proof of Stake

* Proof of Work

PoW là thuật toán đồng thuận đầu tiên được tạo ra. Nó được sử dụng trên Bitcoin và nhiều đồng tiền điện tử khác. Thuật toán Proof of Work là một phần thiết yếu của quá trình đào coin.

Cách thức hoạt động đó là những người tham gia blockchain (được gọi là thợ đào) phải giải bài toán cần tính toán phức tạp để có thể thêm một khối vào blockchain.

Các thợ đào cần tìm được hệ số Nonce để giá trị hash của block thỏa một điều kiện nào đó đã được blockchain đặt ra, gọi là golden nonce. Giả sử blockchain yêu cầu giá trị hash của block phải được bắt đầu bằng 000, thợ đào cần tìm số Nonce để giá trị hash thỏa điều kiện đặt ra.

Đào coin dùng PoW liên quan đến nhiều nỗ lực băm, ở đây là tìm ra giá trị “golden nonce”, vì vậy khả năng tính toán càng lớn có nghĩa là thực hiện được nhiều phép thử hơn trên mỗi giây. Nói cách khác, thợ đào có tỷ lệ băm cao có cơ hội tốt hơn để tìm một lời giải hợp lệ cho khối tiếp theo.

Thuật toán đồng thuận PoW đảm bảo rằng các thợ đào chỉ có thể xác nhận một khối giao dịch mới và thêm nó vào blockchain nếu các nút phân tán của mạng đạt được sự đồng thuận và đồng ý rằng hàm băm khối được đưa ra bởi thợ đào là một bằng chứng công việc hợp lệ.

* Proof of Stake

PoS thay thế PoW bằng một cơ chế mà trong đó các khối được xác nhận theo tỷ lệ cổ phần của những người tham gia. Trình xác nhận hợp lệ của mỗi khối (cũng được gọi là thợ đúc tiền) được xác định bằng tỉ lệ cổ phần của đồng tiền điện tử chứ không phải bằng lượng công suất tính toán được phân bổ.

Mỗi hệ thống PoS có thể thực hiện thuật toán theo nhiều cách khác nhau, nhưng nói chung, Blockchain được bảo đảm bằng một quá trình bầu chọn giả ngẫu nhiên dựa trên việc xem xét tài sản của nút và độ tuổi của coin - cùng với một hệ số ngẫu nhiên.

Cơ chế đồng thuận đóng vai trò quan trọng trong việc duy trì tính toàn vẹn và bảo mật của mạng tiền điện tử. Chúng cung cấp phương tiện để các nút phân tán đạt được sự đồng thuận về phiên bản đúng của blockchain. Việc đồng thuận với trạng thái blockchain hiện tại là điều cần thiết cho một hệ thống kinh tế kỹ thuật số hoạt động đúng.

Script 2:

Hiện nay người ta sử dụng các loại tiền tệ như tiền giấy, tiền xu, vàng bạc và tiền điện tử. Các loại tiền trên đều được sử dụng phổ biến và khá quen thuộc với chúng ta, trừ tiền điện tử mới trở nên phổ biến gần đây. Vậy tiền điện tử là gì?

Tiền điện tử được tạo thành từ những bit số hay còn được gọi là tiền đã được số hóa. Tiền điện tử chỉ hoạt động trong môi trường điện tử dùng để thanh toán chi phí. Để thực hiện được các giao dịch, người dùng phải dựa trên 3 yếu tố: Internet, mạng máy tính và các phương tiện điện tử của tổ chức phát hành.

Tiền điện tử không hiện hữu như một vật chất mà tồn tại vô hình thông qua môi trường điện tử. Chúng được lưu trữ trên: Internet, điện thoại, thông tin và các thẻ thanh toán điện tử khác. Điều này đồng nghĩa với việc người dùng không thể cầm nắm số tiền của mình được.

Bên cạnh đó, tiền điện tử có thể hiểu là phương thức thanh toán thông qua chữ ký bảo mật. Cũng như tiền giấy, tiền điện tử là công cụ dùng để giao dịch, tích lũy giá trị. Tiền điện tử có thể chuyển đổi thành tiền giấy theo yêu cầu của chủ sở hữu.

Tiền điện tử được chia làm 3 loại như sau:

* Tiền số pháp định: Là tiền điện tử được Chính phủ công nhận. Chúng được lưu trữ trong thẻ ATM, tài khoản ngân hàng, ví điện tử,… Tiền pháp định có giá trị ngang hàng với tiền mặt.
* Tiền ảo: Là tiền điện tử được phát hành và kiểm soát bởi các tổ chức, doanh nghiệp. Tiền ảo không được Chính phủ công nhận. Chúng chỉ hoạt động trong một môi trường ảo phục vụ những mục đích nhất định.
* Tiền mã hóa: Đây là tập hợp con của đồng tiền. Tiền mã hóa dựa trên nền tảng kỹ thuật số không bị chi phối bởi Chính phủ. Ưu điểm của dòng tiền này là tính bảo mật cao, không qua trung gian nên đảm bảo được an toàn.

**Coin là gì?**

Coin là một dạng tiền kỹ thuật số, được tạo ra bởi kỹ thuật mã hóa, lưu trữ giá trị theo thời gian.

Về cơ bản, Coin tương đương với tiền tệ. Bitcoin là một ví dụ điển hình nhất, Bitcoin dựa trên [công nghệ Blockchain](https://cryptoviet.com/blockchain-la-gi) mang tính công khai và phân tán với một sổ cái chung, trên đó tất cả giao dịch được công khai một cách minh bạch. Blockchain đảm bảo tính minh bạch và giảm thiểu gian lận.

Coin có đặc điểm tương tự như tiền tệ : chúng có thể được phân loại, có thể phân chia, được chấp nhận, di động, bền vững và có nguồn cung hữu hạn. Hấu hết những người tham gia thị trường Crypto đều nghĩ rằng Crypto tương lai sẽ thay thế tiền tệ.

**Token là gì?**

Token là tài sản kỹ thuật số do các dự án phát hành, thực hiện các chức năng tương tự như Coin, nhưng khác biệt chính là nó cho phép những người nắm giữ các Token này tham gia vào mạng lưới hệ thống.

Token thể hiện chức năng của tài sản kỹ thuật số, đại diện cho phần vốn của công ty, cho phép truy cập vào chức năng của dự án và nhiều hơn thế nữa.

Token đại diện cho một loại tài sản hay một ứng dụng, do đó Security và Utility là 2 dạng phân biệt lẫn nhau của Token. Security Token được thiết kế chia sẻ tài sản của công ty, trong khi đó Utility Token có một số trường hợp để sử dụng bên trong dự án đó.

+ Security token hay còn gọi với tên gọi khác là token chứng khoán. Chúng được xem như là một dạng cổ phiếu điện tử.

+ Utility token là một loại token tiện ích. Chứng được sinh ra theo mục đích và tính năng riêng theo mong muốn của người phát hành.

Ta có ba cách để phân biệt Coin và Token.

### Về định nghĩa

* Coin là đồng tiền ảo có thể hoạt động một cách riêng lẻ.
* Token là đồng tiền ảo phải dựa trên nền tảng của một loại tiền ảo khác để hoạt động. Ví dụ nền tảng Ethereum có thể dùng để xây dựng các loại token.

### Về mặt tính năng:

* Coin được tạo ra với mục đích sử dụng như một loại tiền tệ, một đơn vị lưu trữ giá trị và để giao dịch.
* Token thì có mục đích sử dụng rộng hơn Coin. Token có thể là nhiên liệu cho một mạng lưới hoạt động hay là đơn vị trao đổi trong một ứng dụng.

### Về mặt kỹ thuật:

* Một loại coin cần phải được phát triển ví lưu trữ riêng. Phí giao dịch sẽ được trừ thẳng vào coin đó.
* Token thì có thể lưu trữ cùng một ví được phát triển riêng cho nền tảng gốc. Phí giao dịch phải trả theo quy định của nền tảng gốc.