Giới thiệu về hàm hash:

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 có chiều dài cố định và cũng 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. Định danh của một block được tính bằng cách lấy giá trị đầu ra của hàm hash nhận đầu vào là tổng của dữ liệu đã mã hóa của block đó và giá trị hash của block trước đó, từ đó ta tạo thành một chuỗi liên kết trong Blockchain.

Bởi vì đầu vào của hàm hash là nội dung của Block trước đó nên khi ta thay đổi nội dung của Block thì giá trị hash của tất cả Block trong chuỗi cũng phải thay đổi theo để tạo thành một chuỗi hợp lệ. Bởi vì tính chất này nên người ta đã tận dụng và tạo ra cơ chế đồng thuận trong Blockchain.

Consensus Mechanism

Thuật toán 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.

* Proof of work (PoW)

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

Mục đích: Đó là người dùng phải sử dụng tài nguyên (tiền điện, đầu tư phần cứng) của mình thì mới có thể xác thực dữ liệu vào blockchain (hay còn gọi là mine block) và nhận phần thưởng cho việc đó.

Thuật toán 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.