Cơ chế đồng thuận

**Thuật toán đồng thuận Block chain là gì?**

* Thuật toán đồng thuận blockchain là một quy tắc hoặc cơ chế để các node tuân theo, nhằm đảm bảo các giao dịch được thực hiện trên blockchain là chính xác, minh bạch và giống nhau trên tất cả các node của mạng.

Cách hoạt động của cơ chế đồng thuận trên blockchain

Về bản chất, blockchain bao gồm nhiều node kết hợp lại tạo ra một mạng lưới. Để một giao dịch được ghi lại trên blockchain, nó phải được xác thực đồng thời bởi tất cả các node trên mạng lưới dựa trên cơ chế đồng thuận.

Trước tiên, cần hiểu rằng cấu trúc của blockchain bao gồm nhiều block (khối) liên kết với nhau và tạo thành một chain (chuỗi). Mỗi block sẽ chứa thông tin về mã băm (hash) của khối trước đó. Mã hash này được tạo ra dựa trên các thông tin đầu vào đã được xác định sẵn của một khối, bao gồm cả thông tin giao dịch đã được xác thực bởi node.

Khi người dùng thực hiện một giao dịch, các node sẽ dựa trên thuật toán đồng thuận của blockchain (như PoS, PoW, PoA…) để xác thực và ghi giao dịch vào khối mới trên blockchain. Sau đó, tất cả các node đều phải tải xuống thông tin về khối giao dịch mới được xác thực, để đảm bảo tính thống nhất và toàn vẹn dữ liệu trên mạng lưới.

Thuật toán đồng thuận cũng giúp việc thay đổi dữ liệu trên blockchain là không thể:

* Khi một block bị thay đổi dữ liệu thì mã hash của block cũng bị thay đổi theo.
* Chúng sẽ được so sánh với dữ liệu của khối khác để đảm bảo tính đúng đắn và phù hợp giữa mã hash của khối trước và sau nó.
* Nếu thấy có sự khác biệt, dữ liệu kia sẽ không được phép ghi vào blockchain.

**Các thuật toán đồng thuận blockchain phổ biến**

1. Proof of Work (PoW)

Proof of Work (PoW) hay bằng chứng công việc là cơ chế đồng thuận phi tập trung đầu tiên, được sử dụng để bảo mật blockchain Bitcoin.

PoW yêu cầu các node sử dụng sức mạnh tính toán của máy tính để giải các bài toán và tạo ra mã hash. Node đầu tiên giải bài toán và giành quyền xác thực giao dịch thì sẽ được nhận phần thưởng là đồng coin native của blockchain (ví dụ như BTC, ETH). Quá trình này được gọi là “mining” (đào coin), và node này được gọi là miner node (thợ đào).

Nếu một miner node giải bài toán, xác thực và ghi giao dịch lên khối mới, khối này sẽ được gửi tới tất cả các node khác trong mạng lưới. Khi có đủ số lượng node xác thực khối, chúng sẽ đạt được sự đồng thuận và giao dịch sẽ được xử lý.

Tuy nhiên, PoW sẽ có một số nhược điểm như:

* PoW sử dụng sức mạnh máy tính để bảo mật cho blockchain, do đó yêu cầu điện năng tiêu thụ lớn và chi phí đắt đỏ cho các phần cứng bắt buộc.
* Một block trên blockchain PoW cần nhiều thời gian hơn để được tạo ra và xác thực, khiến cho thuật toán này kém hiệu quả và tốn tài nguyên hơn các thuật toán đồng thuận khác.

1. Proof of Stake (PoS)

Proof of Stake (PoS) hay bằng chứng cổ phần, thay vì sử dụng sức mạnh máy tính, Proof of Stake yêu cầu các node tham gia xác thực giao dịch phải đặt cược (stake) một số lượng nhất định đồng coin native của blockchain để giành quyền tham gia xác thực và tạo khối.

Số token này nhằm đảm bảo các node hoạt động tốt, tức là nếu node đó offline quá lâu hoặc có những hành vi gian lận, số token đã stake có thể bị thu một phần hoặc mất toàn bộ tuỳ thuộc vào mức độ và quy định slashing (phạt).

Trong cơ chế PoS, node sẽ đóng vai trò là các validator thay vì miner như trong PoW.

Các validator trong mạng lưới PoS sẽ nhận được phí giao dịch làm phần thưởng. Khi một giao dịch diễn ra, các validator sẽ được chọn để xác thực giao dịch dựa trên số lượng token và thời gian stake.

Với cách hoạt động trên, Proof of Stake là thuật toán tiết kiệm chi phí, thân thiện với môi trường hơn Proof of Work.

1. Delegated Proof of Stake (DPoS)

Delegated Proof of Stake (DPoS) hay bằng chứng uỷ quyền cổ phần, là thuật toán đồng thuận được phát triển từ Proof of Stake.

Thay vì trở thành validator, DPoS cho phép người nắm giữ token (holder) stake token và chọn một người đại diện (delegator) để uỷ quyền xác thực giao dịch, duy trì bảo mật cho blockchain. Đổi lại, holder sẽ được chia sẻ phần thưởng từ việc gián tiếp vận hành mạng lưới.

Thông thường, delegator sẽ được chọn dựa trên danh tiếng (chứ không phải tài sản) của họ và có số lượng giới hạn khoảng 20-100 delegator trên mỗi block.

So với PoS, DPoS được đánh giá là nhanh hơn và hiệu suất tốt hơn. DPoS giúp đảm bảo sự minh bạch, công bằng và đáng tin cậy thông qua việc liên tục thực hiện các hoạt động bỏ phiếu và xáo trộn trong hệ thống, nhằm đảm bảo những delegator được chọn là trung thực và có trách nhiệm.

1. Proof of Authority (PoA)

Proof of Authority (PoA) hay bằng chứng uỷ quyền là thuật toán đồng thuận dựa trên danh tiếng, phát triển dựa trên Proof of Stake.

Thay vì stake coin, validator stake “uy tín” của mình để được tham gia vào mạng lưới node xác thực giao dịch và khối của blockchain, đồng thời đóng vai trò như là những người vận hành của hệ thống.

PoA đề cao giá trị danh tính, tức là những người được chọn để trở thành validator phải thật sự đáng tin cậy. Điều này khiến cho các blockchain PoA phải đối mặt với sự đánh đổi giữa tính phi tập trung và khả năng mở rộng:

Vì tính chất chỉ lựa chọn những người uy tín và có danh tiếng, blockchain PoA thường có ít validator node, dẫn đến việc ít phi tập trung hơn so với những thuật toán đồng thuận khác.

PoA có số lượng validator giới hạn, giúp giảm thời gian xác nhận giao dịch, tăng thông lượng và khả năng mở rộng cho mạng lưới.

Nói cách khác, thuật toán đồng thuận PoA sẽ phù hợp hơn với các hệ thống tập trung.

**Nguyên lý hoạt động: Quy tắc sổ cái**

Mỗi nút trong blockchain đều đang lưu giữ một bản sao của sổ kế toán. Do vậy mỗi nút đều biết số dư tài khoản của bạn là bao nhiêu. Hệ thống blockchain không hề theo dõi số dư tài khoản mà nó chỉ ghi lại mỗi giao dịch được yêu cầu.

Sổ cái trên thực tế không theo dõi số dư, nó chỉ theo dõi mọi giao dịch được phát đi trong mạng lưới Bitcoin. Để biết số dư trên ví điện tử của bạn, bạn cần xác thực và xác nhận tất cả các giao dịch đã diễn ra trên mạng lưới mà có liên quan tới ví điện tử của bạn.

Các nút sẽ kiểm tra tất cả các giao dịch trước đó có liên quan đến ví tiền điện tử bạn sử dụng để gửi Bitcoin thông qua các tham chiếu lịch sử giao dịch. Để đơn giản hóa và tăng tốc quá trình xác minh, một bản ghi đặc biệt sẽ lưu trữ số Bitcoin chưa được dùng sẽ được các nút mạng lưu giữ. Nhờ cơ chế kiểm tra này nên các ví tiền điện tử tránh được tình trạng chi tiêu đúp giao dịch.

Như vậy sở hữu Bitcoin có nghĩa là có các giao dịch được lưu trong sổ kế toán liên hệ đến địa chỉ ví của bạn mà chưa được sử dụng làm giao dịch đầu vào.

Tất cả mã nguồn để thực hiện các giao dịch trên mạng lưới Bitcoin đều là nguồn mở, điều này có nghĩa là bất kỳ ai có máy tính xách tay và kết nối internet đều có thể tham gia vào mạng lưới và thực hiện giao dịch.

Tuy nhiên, nếu có bất kỳ lỗi lầm nào trong mã nguồn được sử dụng để phát thông báo yêu cầu giao dịch, các Bitcoin liên quan sẽ bị mất vĩnh viễn.