**Anh/chị tìm hiểu các thuật toán đồng thuận sử dụng trong Blockchain hiện nay và trình bày ngắn gọn nguyên lý hoạt động của từng thuật toán.**

**Trả lời:**

Thuật toán đồng thuận là một cơ chế cho phép người dùng hoặc máy móc phối hợp hoạt động trong một thiết lập phi tập trung. Nó đảm bảo rằng tất cả các tác nhân trong hệ thống có thể đồng ý về một sự thật duy nhất, ngay cả khi một số tác nhân trong hệ thống thất bại. Nói cách khác, hệ thống phải có khả năng chịu lỗi.

Trong một thiết lập tập trung, chỉ có một thực thể duy nhất có quyền đối với hệ thống. Trong hầu hết các trường hợp, thực thể này có thể thực hiện các thay đổi khi họ muốn – không có một hệ thống quản trị phức tạp nào để đạt được sự đồng thuận giữa nhiều quản trị viên.

***Thuật toán đồng thuận Blockchain là gì?***

Thuật toán đồng thuật của blockchain là cơ chế đảm bảo các giao dịch được tạo ra trên blockchain là đúng đắn, trung thực và minh bạch. 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 đồng ý đồng thời bởi tất cả các node trên mạng lưới.

Nếu trong mạng lưới có một block bị thay đổi, dữ liệu này được so sánh với các dữ liệu của các khối khác. Nếu có sự khác biệt thì nó sẽ không cho phép dữ liệu ấy được ghi vào bên trong Blockchain. Đó là cách blockchain được thiết kế để chống lại sự thay đổi dữ liệu.

\* Các loại thuật toán đồng thuận:

1. Proof of Work

2. Proof of Stake

3. Delegated Proof of Stake (DPoS)

4. Proof of History (PoH)

5. Proof of Authority (PoA)

6. Proof of Contribution (PoC)

7. Byzantine Fault Tolerance (BFT)

Ngoài ra còn có: Proof of Location (PoL), Proof of Burn (PoB), Proof of Zero (PoZ), Proof of Weight (PoWeight), Direct Acyclic Graph Tangle (DAG),...

**Nguyên lý hoạt động của các thuật toán:**

**Proof of Work**

Proof of Work là thuật toán đồng thuận blockchain đầu tiên ra đời, thuật toán này được sử dụng bởi Bitcoin - đồng tiên mã hoá đầu tiên trên thế giới.

Proof of Work (PoW) hay còn gọi là bằng chứng công việc. Với cơ chế đồng thuận này, các node sẽ sử dụng sức mạnh máy tính để giải các bài toán tạo ra mã hash. Node đầu tiên giải bài toán, giành quyền xác thực giao dịch, sau đó sẽ được nhận phần thưởng là BTC. Quá trình này được gọi là “mining” (đào coin), trong đó các node đóng vai trò là các miners (thợ đào).

Khi một node giải bài toán và xác nhận giao dịch, giao dịch đó cũng sẽ được kiểm tra và xác nhận bởi tất cả các node khác trong mạng lưới. Nếu câu trả lời được thông qua, tất cả các node sẽ thêm giao dịch này vào blockchain, làm cho blockchain có thể dễ dàng xác minh và đồng bộ hoá.

Cách hoạt động của Proof of Work

Chính bởi vì việc sử dụng sức mạnh máy tính để bảo mật cho blockchain, Proof of Work yêu cầu một lượng tiêu thụ điện lớn cũng như chi phí khá đắt đỏ cho các phần cứng bắt buộc.

Thêm nữa, một block trên một blockchain Proof of Work cũng cần nhiều thời gian hơn để được tạo ra và xác thực, điều này làm cho thuật toán này kém hiệu quả và tốn tài nguyên (thậm chí là không thân thiện với môi trường) hơn các thuật toán đồng thuận khác.

Đây là cơ chế đồng thuận đầu tiên và gắn liền với Bitcoin (BTC), Ethereum (ETH),...

**Proof of Stake**

Proof of Stake (PoS), hay còn gọi là bằng chứng cổ phần, là cơ chế thuật toán đồng thuận phổ biến nhất hiện nay, được sử dụng đầu tiên bởi Ethereum. 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 native token của blockchain để giành quyền tham gia xác thực và tạo khối.

Thường các blockchain sử dụng Proof of Stake sẽ yêu cầu một số lượng token tối thiểu để được tham gia làm validator.

Ví dụ, để trở thành validator của Ethereum, người dùng sẽ phải stake ít nhất 32 ETH (khoảng 33 nghìn USD tại thời điểm viết bài). Số token này được đặt cọc để 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.

Validator node trong mạng lưới Proof of Stake sẽ nhận được phí giao dịch làm phần thưởng. Khi một giao dịch giao dịch diễn ra, các validator sẽ được chọn ngẫu nhiên để xác thực giao dịch, số lượng token stake càng nhiều tỉ lệ được chọn cũng sẽ tăng tương ứng.

Với các hoạt động trên, Proof of Stake là thuật toán tiết kiệm chi phí, thân thiện với môi trường hơn Proof of Work. Để trở thành một validator node cũng đơn giản hơn và không phải sử dụng các thiết bị phần cứng quá “khủng”.

Proof of Stake được đánh giá là ưu việt hơn Proof Of Work và đang rất thịnh hành với rất nhiều blockchain sử dụng như Cosmos (ATOM), Binance Coin (BNB), Ontology (ONT),...

**Delegated Proof of Stake (DPoS)**

Delegated Proof of Stake (DPoS), hay còn gọi là bằng chứng uỷ quyền cổ phần, là phiên bản phát triển của Proof of Stake.

Thay vì chọn validator ngẫu nhiên như PoS, token holders sẽ chọn một số các node chuyên nghiệp để các node này vận hành mạng, bù lại, token holders sẽ được chia sẻ một phần phần thưởng cho công việc duy trì an ninh cho mạng. Trong mỗi block, số lượng delegators được chọn để xác thực giao dịch là giới hạn và ngẫu nhiên.

Ngoài ra, Delegated Proof of Stake có số lượng validator có giới hạn, thường giao động từ 10 - 100, so với PoS nguyên bản, DPoS được đánh giá là nhanh hơn và hiệu suất tốt hơn.

DPoS giúp đảm bảo sự trung thực và công bằng bằng việc thực hiện các hoạt động bỏ phiếu liên tục và cũng liên tục xáo trộn trong hệ thống, để đảm bảo những người được chọn là trung thực và có trách nhiệm.

**Proof of History (PoH)**

Proof of History, hay còn gọi là bằng chứng lịch sử, là thuật toán đồng thuận khá mới được giới thiệu bởi Solana. Thay vì xét theo logic, PoH sử dụng timeline giao dịch làm tài liệu tham khảo. Vì vậy, các validator node của mạng Solana có thể tạo các block tiếp theo mà không cần phải phối hợp với toàn bộ mạng lưới.

Về cơ bản, Proof of History không tính toán output từ dữ liệu input, thay vào đó PoH sử dụng một tính năng để sử dụng các output đã có trước đó làm input. Cơ chế này được xây dựng để giải quyết vấn đề về thời gian trong các mạng phi tập trung ở nơi không có cùng mốc thời gian.

**Proof of Authority (PoA)**

Proof of Authority, hay còn gọi là bằng chứng uỷ quyền, là thuật toán đồng thuận dựa trên danh tiếng. Khác với PoS, những validators làm nhiệm vụ xác thực khối sẽ không được chọn dựa trên số coin họ nắm giữ mà sẽ dựa trên chính danh tiếng của mình.

Lượng validator của mạng lưới được giới hạn, giúp cho Proof of Authority trở thành một mô hình có khả năng mở rộng. Trong đó, các giao dịch được xác thực bởi các validator đã được chọn lọc và phê duyệt, đây cũng chính là những người điều tiết hệ thống.

PoA đề cao giá trị danh tính, tức là những người được chọn là các validator đáng tin cậy, điều này giúp cho một vài công ty và doanh nghiệp có thể ứng dụng thuật toán này. Không chỉ vậy, thuật toán đồng thuật PoA có thể được coi là một lựa chọn giá trị cho các ứng dụng trong ngành hậu cần, chuỗi cung ứng.

Để có những ưu điểm trên, PoA phải đánh đổi bằng sự phi tập trung, hi sinh sự phi tập trung để đổi lấy hiệu suất và khả năng mở rộng, hay nói cách khác, mô hình này chỉ làm các hệ thống tập trung trở nên hiệu quả hơn.

PoA được đề xuất lần đầu tiên bởi cựu CTO của Etherueum, Gavin Wood vào năm 2017, sau đó được sử dụng bởi Binance Smart Chain (BNB Chain) và các exchange chain khác như HECO, OKExChain, Gatechain, Cronos…

**Proof of Contribution (PoC)**

Proof of Contribution (tạm dịch là bằng chứng cống hiến) giám sát hành động của tất cả validator trong mạng lưới và xếp hạng các validator đó dựa theo đóng góp của họ - một cơ chế khá tương đồng với hệ thống tín dụng xã hội. Sự uy tín của một người dùng được đánh giá dựa trên số lượng token đã stake và các giao dịch trong lịch sử.

Trước khi tham gia vào mạng lưới, người dùng sẽ phải stake một khoản tiền gọi là security deposit. Sau khi hoàn thành các công việc tính toán, các node có các kết quả được xác thực sẽ được thưởng phí giao dịch và staked token từ các node không có kết quả chính xác.

**Byzantine Fault Tolerance (BFT)**

Byzantine Fault Tolerance (hay Hệ thống chịu lỗi Byzantine - BFT) là hệ thống có thể giải quyết được vấn đề của bài toán Byzantine. Điều này có nghĩa là hệ thống BFT có thể tiếp tục hoạt động ngay cả khi một số node bị lỗi hoặc thực hiện hành động gây hại cho mạng chung.

Thuật toán này cho phép những người thực hiện xác minh quản lý mỗi trạng thái của một chuỗi, đồng thời chia sẻ các thông điệp với một chuỗi khác, để có được những bản ghi giao dịch chính xác và đảm bảo sự trung thực.

Một số dự án sử dụng thuật toán này: NEO (NEO), Ripple (XRP), Stellar (XLM)...

**\*Thuật toán đồng thuận và tiền mã hóa**

Với tiền mã hóa, số dư của người dùng được ghi lại trong cơ sở dữ liệu – tức blockchain. Mọi người (hay chính xác hơn là mọi node) phải duy trì một bản sao cơ sở dữ liệu giống hệt nhau. Nếu không, thông tin sẽ bị xung đột. Từ đó, mạng lưới tiền mã hoá sẽ bị phá vỡ.

Mật mã khóa công khai đảm bảo rằng người dùng không thể tiêu tiền của nhau. Nhưng vẫn cần phải có một nguồn xác thực duy nhất để những người tham gia mạng lưới có thể xác định xem tiền đã được chi chưa.

Điểm chung tiên quyết là khi người dùng (trình xác thực) muốn thêm khối, họ phải stake một giá trị gì đó. Việc stake một giá trị khiến cho trình xác thực có xu hướng hành động trung thực. Nếu họ gian lận, họ sẽ mất những thứ họ đã stake. Những thứ có thể stake bao gồm sức mạnh tính toán, tiền mã hóa hoặc thậm chí danh tiếng.

Tại sao người dùng lại muốn mạo hiểm nguồn lực của chính họ? Bởi vì việc này mang đến cho họ cơ hội nhận phần thưởng. Phần thưởng thường là tiền mã hóa gốc của giao thức và được tạo thành từ các khoản phí do người dùng khác trả, các đơn vị tiền mã hóa mới được tạo hoặc cả hai.

Điều cuối cùng chúng ta cần là sự minh bạch. Chúng ta cần khả năng phát hiện khi ai đó đang gian lận. Lý tưởng nhất là họ phải tốn kém chi phí để sản xuất các khối, nhưng lại rất rẻ để bất kỳ ai muốn xác thực chúng. Điều này đảm bảo rằng các trình xác thực được người dùng thường xuyên kiểm tra.