**Học viên: Hồ Hữu Thanh Liêm**

**Đề bài:** Anh/chị hãy 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.

**BÀI LÀM**

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.

Thuật toán đồng thuận cũng là một phần không thể thiếu của một blockchain, đóng vai trò cốt lõi giữ các blockchain hoạt động một cách phi tập trung và bảo mật. Ở thời điểm ban đầu, cơ chế đồng thuận Proof of Work của Bitcoin là lựa chọn chính của các developer, tuy nhiên tới thời điểm hiện tại, đã có rất nhiều cơ chế đồng thuận khác nhau. Trong đó, phổ biến nhất là Proof of Stake.

Các blockchain cần thuật toán đồng thuận bởi vì đây chính là cơ chế tạo dựng và duy trì sự phi tập trung ngang hàng của mạng lưới. Thay vì một vài cá nhân hay tổ chức kiểm soát toàn bộ hệ thống, blockchain cho phép ai cũng có thể tham gia mạng lưới bằng cách trở thành một node.

Cơ chế đồng thuận cũng là lớp bảo vệ vững chắc của blockchain khỏi việc thay đổi dữ liệu cũng như chống lại các giao dịch gian lận của hacker, nhờ có cơ chế đồng thuận, một giao dịch sẽ luôn được xác thực bởi các node trong mạng lưới một cách ngang hàng.

Nếu các cơ chế đồng thuận luôn ổn định, vững chắc và an toàn, sẽ không có một bên nào có thể khai thác hay tấn công vào blockchain. Càng có nhiều node/validator, blockchain đó càng trở nên bảo mật và phi tập trung. Điều này đồng nghĩa với việc Bitcoin và Ethereum là 2 blockchain an toàn nhất cho tới hiện tại.

Các thuật toán đồng thuận Blockchain phổ biến hiện nay:

1. **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.

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.

1. **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),...

1. **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.

Một số dự án sử dụng cơ chế này là: Cosmos (ATOM), EOS (EOS), Tron (TRX)...

1. **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.

1. **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…

1. **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.

1. **Proof of Reputation (PoR)**

Proof of Reputation (tạm dịch bằng chứng danh tiếng), là phiên bản nâng cấp của Proof of Contribution. Tiến trình hoạt động của PoR tương đồng với PoC, điểm khác biệt là ở cách chọn validator. Trong khi ai cũng có thể trở thành 1 node của một blockchain PoC, PoR yêu cầu một quy trình chọn lọc khắt khe hơn.

Để được trở thành một validator trên blockchain PoR, danh tiếng của người dùng phải lớn tới mức việc có các hoạt động gian lận trên blockchain ngay lập tức có thể huỷ hoại danh tiếng.

Do đó, các validator của mạng lưới thường là công ty. Đây là khái niệm tương đối trừu tượng vì hầu hết các công ty tham gia vào hệ thống nếu gian lận sẽ bị ảnh hưởng đến danh tiếng, những công ty lớn sẽ thiệt hại nhiều hơn.

Dự án tiêu biểu sử dụng thuật toán PoR là GoChain Coin (GO).

1. **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)...

1. **Các thuật toán đồng thuận khác**

Hiện tại đã xuất hiện rất nhiều cơ chế đồng thuận khác nhau, phục vụ cả nhu cầu công cộng và riêng tư. Còn một vài cái tên khác có thể kể đến như Proof of Location (PoL), Proof of Burn (PoB), Proof of Zero (PoZ), Proof of Weight (PoWeight), Direct Acyclic Graph Tangle (DAG),...

Các thuật toán blockchain này khá khó để thay đổi, do đó người ta thường nghĩ tới việc tạo ra một cơ chế mới. Những blockchain mới hơn với những cơ chế đồng thuận mới hơn sẽ đem đến sự phát triển không ngừng của blockchain trong tương lai.

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

Thuật toán đồng thuận của Bblockchain 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 thuật toán đồng thuận blockchain**

1. **Proof-of-Work (PoW)**

[Proof of Work](https://coin98.net/proof-of-work-pow) (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](https://coin98.net/dao-coin-la-gi)), 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.

**Nhược điểm:**

* Yêu cầu một lượng tiêu thụ điện lớn cũng và chi phí khá đắt đỏ cho các phần cứng bắt buộc.
* 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.

**2. Proof of Stake (PoS)**

[Proof of Stake](https://coin98.net/proof-of-stake-la-gi)(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.

Proof of Stake giúp **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)](https://coin98.net/cosmos-network-atom), [Binance Coin (BNB)](https://coin98.net/binance-coin-bnb), [Ontology (ONT)](https://coin98.net/ontology-ont),…

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

### ****3. Delegated Proof of Stake (DPoS)****

**Delegated Proof of Stake (DPoS)** 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.

Một số dự án sử dụng cơ chế này là: Cosmos (ATOM), [EOS (EOS)](https://coin98.net/eos), [Tron (TRX)](https://coin98.net/tron-trx)…

### ****4. Proof of History (PoH)****

[Proof of History](https://coin98.net/proof-of-history-poh-la-gi), hay còn gọi là bằng chứng lịch sử, là thuật toán đồng thuận khá mới được giới thiệu bởi [Solana](https://coin98.net/solana-sol). 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.

### ****5. Proof of Authority (PoA)****

[Proof of Authority](https://coin98.net/proof-of-authority-poa-la-gi), 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…

### ****6. 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.

### ****7. Proof of Reputation (PoR)****

Proof of Reputation (tạm dịch bằng chứng danh tiếng), là phiên bản nâng cấp của Proof of Contribution. Tiến trình hoạt động của PoR tương đồng với PoC, điểm khác biệt là ở cách chọn validator. Trong khi ai cũng có thể trở thành 1 node của một blockchain PoC, PoR yêu cầu một quy trình chọn lọc khắt khe hơn.

Để được trở thành một validator trên blockchain PoR, danh tiếng của người dùng phải lớn tới mức việc có các hoạt động gian lận trên blockchain ngay lập tức có thể huỷ hoại danh tiếng.

Do đó, các validator của mạng lưới thường là công ty. Đây là khái niệm tương đối trừu tượng vì hầu hết các công ty tham gia vào hệ thống nếu gian lận sẽ bị ảnh hưởng đến danh tiếng, những công ty lớn sẽ thiệt hại nhiều hơn.

Dự án tiêu biểu sử dụng thuật toán PoR là [GoChain Coin (GO)](https://coin98.net/gochain-coin-go).

### ****8. Byzantine Fault Tolerance (BFT)****

[Byzantine Fault Tolerance](https://coin98.net/byzantine-la-gi) (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)](https://coin98.net/neo), [Ripple (XRP)](https://coin98.net/ripple-xrp), [Stellar (XLM)](https://coin98.net/stellar-xlm)…

### ****Các thuật toán đồng thuận khác****

Hiện tại đã xuất hiện rất nhiều cơ chế đồng thuận khác nhau, phục vụ cả nhu cầu công cộng và riêng tư. Còn một vài cái tên khác có thể kể đến như Proof of Location (PoL), Proof of Burn (PoB), Proof of Zero (PoZ), Proof of Weight (PoWeight), [Direct Acyclic Graph Tangle](https://coin98.net/directed-acyclic-graph-dag-la-gi) (DAG),…