**Họ và Tên: Nguyễn Văn Phi – VNPT Gia Lai**

**Tổng quan về các thuật toán đồng thuận**

Trái tim của blockchain chính là thuật toán đồng thuận ( consensus ). Các thuật toán đồng thuận đơn giản là những cơ chế được sử dụng trong các hệ thống máy tính phân tán nhằm đạt được thỏa thuận về một giá trị dữ liệu hoặc một trạng thái duy nhất của mạng giữa các máy trong hệ thống.

**1.Proof of Work**

**Ưu điểm**

* Đã chạy từ 2009 và vẫn hoạt động tốt đến tận bây giờ

**Nhược điểm**

* Chậm
* Tốn nhiều năng lượng

**Được sử dụng**

* Bitcoin, Ethereum, Litecoin, Dogecoin etc.

**Type :** Đồng thuận cạnh tranh (Competitive consensus) .

**Giải thích**

Đây là thuật toán đồng thuận đầu tiên được đưa vào một blockchain bởi Satoshi Nakamoto nhằm tạo ra một thuật toán đồng thuận phi tập trung nhằm giải quyết vấn đề double-spend. PoW không phải là một ý tưởng mới thế nhưng Satoshi kết hợp nó với mới một số khái niệm khác như: cryptographic signatures, merkle chains, và P2P networks vào hệt thống phân tán với ứng dụng là Bitcoin.

Cách thức hoạt động đó là những người tham gia blockchain (được gọi là miner) phải giải bài toán cần tính toán phức tạp để có thể thêm một khối vào blockchain.Mục đích của việc này 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 . Chính vì thế nếu cố gắng gian lận sẽ dẫn đến tài nguyên sử dụng để mine sẽ lãng phí do đó tự làm hại chính mình .

Hơn nữa độ khó của bài toán dành cho miner cũng thay đổi theo thời gian để đảm bảo thời gian để tạo một block luôn khoảng 10 phút. Đôi khi sẽ có nhiều hơn một miner mine ra các block .Trong trường hợp đó sẽ chọn một trong các chuỗi dài nhất làm chuỗi chính .Tóm lại miner chiến thắng chính là người giải được bài toán nhanh nhất và duy trì lâu nhất chính vì thế là đáng tin tưởng nhất.Vì vậy Bitcoin an toàn miễn là có hơn 50% miner trung thực trong mạng.

**2. Proof of Stake**

**Ưu điểm**

* Tiết kiệm năng lượng
* Tốn nhiều chi phí để tấn công hơn

**Nhược điểm**

* nothing-at-stake problem

**Được sử dụng**

* Ethereum 2.0, Peercoin, Nxt.

**Type:** Đồng thuận cạnh tranh (Competitive consensus) .

**Giải thích**

Proof of Stake được tạo ra như một giải pháp cho các vấn đề của Proof of Work như tiết kiệm năng lượng hơn.Ở đây thay vì chạy đua trong cuộc đua sử dụng phần cứng mạnh để tính toán rồi đóng block thì ở đây xác suất đc đóng block đựa vào số lượng cổ phần mà người đó nắm giữ.Ví dụ bạn nắm 10% số lượng coin thì xác suất để đc mine block tiếp theo là 10%.

Đối với Bitcoin việc khai thác đòi hỏi rất nhiều sức mạnh tính toán để chạy các thuật toán mã hóa khác nhau.Cùng một thời điểm lại có rất nhiều miner chạy chương trình tính toán đó chính vì thế nó cần một lượng điện rất lớn để một block đc sinh ra. Một số liệu thống kê vào 2015 cho thấy một transaction Bitcoin cần một lượng điện cần thiết có thể cung cấp cho 1.57 hộ gia đình mỗi ngày. Vì thế vấn đề về điện là vấn đề lớn đối với PoW mà PoS có thể giải quyết được.

Về tính an toàn nếu bạn cố gắng tấn công thì chính bạn sẽ làm mất tiền mà bạn stake. Ở đây mất tiền nghĩa là giá trị của token của blockchain này sẽ bị mất giá vì mọi người không tin vào nó nữa điều đó đồng nghĩa với giá trị mà bạn stake cũng về 0. Không giống như POW bạn chỉ tốn tiền điện còn máy thì bạn vẫn còn. Còn một vấn đề nữa đó là **nothing at stake** là một lỗ hổng bảo mật xảy ra khi xảy ra fork trên chuỗi. Vì việc mining không tốn nhiều chi phí như PoW nên chiến thuật sẽ là mining ở cả 2 branch khi xảy ra fork và chi tiêu ở 1 nhánh sau đó mining ở nhánh còn lại với như vậy sẽ xảy ra **double spend**. Có nhiều cách giải quyết vấn đề này được đề cập trong phần đọc thêm. Ví dụ, một trong những giải pháp là trừng phạt những người miner như có hành động gian lận như vậy.

**3. Delegated Proof-of-Stake**

**Ưu điểm**

* Tiết kiệm năng lượng
* Nhanh

**Nhược điểm**

* Tập trung.
* Những người tham gia stake nhiều có thể tự bỏ phiếu để trở thành validator.

**Được sử dụng**

* BitShares, Steemit, EOS, Lisk, Ark

**Type :** Đồng thuận hợp tác (Collaborative consensus) .

**Giải thích**

Trong DPoS các stake holders sẽ bầu ra các ng chứng nhận (**witnesses**) để thay họ mining block. Tiến trình này sẽ nhanh hơn một chút so với PoS. Ví dụ trong EOS, hệ thống sẽ bao gồm 21 người sẽ được chọn làm người chứng nhận ( witnesses ) và sẽ luôn giữ số lượng đó vì thế nếu 1 người cố gian lận hay có vấn đề sẽ lập cho người khác vào thay thế ngay. Những witnesses này cũng sẽ đc trả một khoản fee (tùy vào stake holders quyết định) trong việc tạo block.

Thông thường witnesses sẽ tạo ra một block trong một thời điểm và theo chiến lược **round robin**. Nếu một witnesses ko tạo đc block trong turn của mình thì các stake holders sẽ vote cho witnesses khác làm việc hiệu quả hơn.

DPoS , các miner không phải cạnh tranh nhau giống như PoW hay PoS vì thế mà tốc độ sẽ nhanh hơn rất nhiều .Ví dụ EOS chỉ tốn 0.5s cho một block !

**4. Proof-of-Authority**

**Ưu điểm**

* Tiết kiệm năng lượng
* Nhanh

**Nhược điểm**

* Không phân tán. Có thể sử dụng trong cách blockchain public nhưng thường được dùng trong các blockchain private và permissioned blockchains.

**Được sử dụng**

* POA.Network, Ethereum Kovan testnet, VeChain

**Type :** Đồng thuận hợp tác (Collaborative consensus) .

**Giải thích**

Trong các mạng sử dụng PoA các giao dịch, block sẽ được xác thực bởi các tài khoản được approved được gọi là **validators**. Validators chạy phần mềm giúp họ đẩy các transaction bào block, quá trình này là hoàn toàn tự động.

Sẽ có 3 điều kiện chính để trở thành validator :

* Identity phải được verified on-chain, với khả năng kiểm tra chéo các thông tin đó trên publicly available domain.
* Các điều kiện trở thành validators phải khó đạt được. ( ví dụ các node muốn là thành validator thì phải đc cấp license )
* Phải có sự thống nhất hoàn toàn trong việc kiểm tra và thiết lập một authority

Với các validator cần phải có một động lực để giữ vị trí mà họ đã đạt được. Bằng cách gán reputation với identity, validator được khuyến khích duy trì quá trình giao dịch, vì họ không muốn mất reputation, vì vậy mất vai trò của validator khó kiếm được.

**5. Proof-of-Weight**

**Ưu điểm**

* Tiết kiệm năng lượng
* Tùy biến và khả năng mở rộng cao.

**Nhược điểm**

* khó setup lợi nhuận dành cho người tham gia hệ thống

**Được sử dụng**

* Algorand

**Type :** Đồng thuận cạnh tranh (Competitive consensus) .

**Giải thích**

Proof of Weight là một thuật toán đồng thuận base theo thuật toán đồng thuận Algorand . Ý tưởng của nó cũng giống PoS đó là cũng dựa vào số lượng token nắm dữ trong mạng sẽ tương đương với phần trăm xác suất tạo đc ra block tiếp theo cơ chế tính của hệ thống PoWeight kèm với một vài giá trị khác được sử dụng. Một số triển khai khác là Proof of Reputation và Proof of Space .

**6. Proof of Reputation**

**Ưu điểm**

* Tốt với private, permissoned networks

**Nhược điểm**

* Chỉ dùng được trong private, permissoned networks

**Được sử dụng**

* GoChain

**Type :** Đồng thuận hợp tác (Collaborative consensus) .

**Giải thích**

Khá tương đồng với Proof of Authority

Tư tưởng của proof of Reputation (PoR) là dựa vào uy tín của các bên tham gia để giữ cho mạng an toàn. Một bên tham gia xác thực block phải là đủ uy tín để nếu họ cố tình gian lận thì uy tín của họ sẽ bị ảnh hưởng. 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 nhưng công ty lớn sẽ thiệt hại nhiều hơn.

Khi một công ty chứng minh được danh tiếng và vượt qua các bước xác mình lúc này sẽ được chọn để kí và xác thực block giống như Proof of Authority

**7. Proof of Elapsed Time**

**Ưu điểm**

* Tính công bằng : Chi phí tham gia thấp. Vì vậy, nhiều người có thể tham gia dễ dàng, do đó là phi tập trung.
* Tính xác thực : Dễ dàng check leader được bầu một cách hợp pháp đối với tất cả người tham gia.
* Tính đầu tư : Chi phí controlling quá trình bầu leader tỷ lệ thuận với giá trị thu được từ nó.

**Nhược điểm**

* Không phù hợp với public blockchain

**Được sử dụng**

* HyperLedger Sawtooth

**Type :** Đồng thuận cạnh tranh (Competitive consensus) .

**Giải thích**

PoET là một thuật toán đồng thuận thường được sử dụng trong permissioned blockchain networks để quyết định quyền khai thác hoặc người chiến thắng trong việc mining block. permissioned blockchain networks là những mạng yêu cầu bất kỳ người tham gia nào cũng phải đăng kí identify trước khi họ được phép tham gia. Dựa trên nguyên tắc random trong đó mọi node đều có khả năng là người chiến thắng như nhau, cơ chế PoET dựa trên việc lan truyền cơ hội chiến thắng một cách công bằng trên số lượng node tham gia mạng là lớn nhất có thể.

Hoạt động của thuật toán PoET như sau. Mỗi validator trong mạng được yêu cầu chờ trong khoảng thời gian được chọn ngẫu nhiên từ một hàm được gọi là ( trusted function ) và node đầu tiên hoàn thành thời gian chờ được chỉ định sẽ được chọn là leader. Mỗi nút trong mạng blockchain tạo ra một thời gian chờ ngẫu nhiên và chuyển sang chế độ sleep trong khoảng thời gian được chỉ định đó. Người thức dậy đầu tiên - nghĩa là người có thời gian chờ đợi ngắn nhất - thức dậy và commit một khối mới vào blockchain, broadcasing các thông tin cần thiết đến toàn bộ mạng. Quá trình tương tự lặp lại để tạo ra block tiếp theo .

Cơ chế đồng thuận mạng PoET cần đảm bảo hai yếu tố quan trọng. Đầu tiên, rằng các node tham gia thực sự phải chọn một thời gian thực sự ngẫu nhiên. Hai là người chiến thắng thực sự đã hoàn thành thời gian chờ đợi.

Khái niệm PoET được phát minh vào đầu năm 2016 bởi Intel, gã khổng lồ sản xuất chip nổi tiếng. Họ cung cấp một high tech tool để giải quyết vấn đề computing của "random leader election".

Cơ chế này cho phép các ứng dụng thực thi trusted code trong môi trường được bảo vệ và điều này đảm bảo rằng cả hai yêu cầu cho việc chọn ngẫu nhiên thời gian chờ cho tất cả các node tham gia và hoàn thành đúng thời gian chờ của người tham gia.

Cơ chế thực thi trusted code trong một môi trường an toàn cũng đảm bảo các nhu cầu thiết yếu khác của mạng. Nó đảm bảo rằng trusted code thực sự chạy trong môi trường an toàn và không bị thay đổi bởi bất kỳ người tham gia bên ngoài nào. Nó cũng đảm bảo rằng các kết quả có thể kiểm chứng được bởi những người tham gia và các thực thể bên ngoài, do đó tăng cường tính minh bạch của sự đồng thuận mạng.

PoET kiểm soát chi phí của quy trình đồng thuận này và duy trì tốc độ nhanh để chi phí vẫn tỷ lệ thuận với giá trị thu được từ quy trình, một yêu cầu chính để cryptocurrency economy tiếp tục phát triển./