**CÁC THUẬT TOÁN ĐỒNG THUẬN BLOCKCHAIN**

1. **Delegated Proof-of-Stake**

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 !

**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.

1. **Proof-of-Authority**

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.

#### 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.

1. **Proof-of-Weight**

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.

#### 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

1. **Proof of Reputation**

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

#### Ưu điểm

* Tốt với private, permissoned networks

#### Nhược điểm

* Chỉ dùng được trong private, permissoned networks

1. **Proof of Elapsed Time**

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.

#### 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

1. **Byzantine Tolerance to Delegated Failure (dBFT)**

Byzantine Tolerance to Delegated Failure (dBFT) là một cái tên thanh lịch và xuất sắc cho một giải pháp để đạt được sự đồng thuận cuối cùng trong những điều kiện nhất định. Điều kiện thực sự đơn giản: miễn là có ít hơn 1/3 các nút là các tác nhân xấu, nó có thể đạt được sự đồng thuận cuối cùng và khi đó mọi người sẽ hạnh phúc.

dBFT đảm bảo rằng nếu bạn đạt được sự đồng thuận, bạn không thể đạt được một sự đồng thuận khác sau này. Miễn là các tác nhân xấu ít hơn 1/3, thì mọi thứ đều ổn.

Thuật toán được đề xuất bởi NEO, và từ đó nó đã phát triển các ứng dụng phi tập trung theo cơ chế này.

1. **Proof of Activity (PoA)**

Khái niệm này lần đầu tiên được giới thiệu vào năm 2012 như là một sự thay thế cho Proof of Stake. Proof of Activity (Bằng chứng hoạt động) về cơ bản là một cấu trúc thay thế cho Bitcoin và là sự pha trộn của hai trong số các cơ chế đồng thuận phổ biến nhất: Proof of Work và Proof of Stake. Proof of Activity nhằm hạn chế những lo ngại về sự kết thúc trong quá trình khai thác Bitcoin khi hết sạch 21 triệu coin tồn tại và bổ sung Proof of Work để giúp ngăn chặn cuộc tấn công 51%.

Cơ chế này hoạt động bằng cách bắt đầu với Proof of Work, nơi các thợ đào về cơ bản giải một câu đố mật mã và nhận phần thưởng nếu họ thành công. Sự khác biệt nằm ở chỗ các khối được khai thác chỉ là các tiêu đề và địa chỉ phần thưởng khai thác, thay vì chứa các giao dịch.

Hai trong số các loại tiền phổ biến nhất sử dụng nó là Decred (DCR) và Espers (ESP).

1. **Proof of Burn (PoB)**

Proof of Burn (Bằng chứng đốt cháy) tương đương với khái niệm rằng sẽ là bất khả thi để ai đó xóa dữ liệu khỏi blockchain. Vì vậy, khái niệm này là để “đốt” coin. Nó bao gồm việc cung cấp bằng chứng rằng một số đồng tiền đã bị đốt trong quá trình gửi giao dịch đến một địa chỉ không thể sử dụng.

Phương pháp này chỉ hoạt động với các đồng tiền được trích xuất từ các loại tiền mã hóa của Proof of Work. Người dùng sẽ cố gắng đốt nhiều coin nhất để nhận được phần thưởng. Hầu hết thời gian thử nghiệm đốt cháy đã được giới thiệu để làm chậm các đồng tiền khác phá hủy giá trị của một đồng tiền.

Quá trình lựa chọn được cho là ngẫu nhiên, nhưng đồng thời, người ta cũng nói rằng người dùng đốt càng nhiều coin, cơ hội để họ được chọn để trích xuất khối tiếp theo sẽ càng lớn. Điều này có phần giống với quy trình Bitcoin, nơi đầu tư nằm ở sức mạnh tính toán cần được cải thiện để có được hash rate tốt hơn.

Slimcoin (SLM) là ví dụ tuyệt vời của thuật toán này. Đồng thời TGCoin hay Coin thế hệ thứ ba, cũng sử dụng thuật toán này. Tuy nhiên, loại tiền bổ trợ cho Counterparty, một phần mở rộng của phần mềm Bitcoin có chức năng coin màu, đã được phân phối thông qua quy trình thử nghiệm đốt cháy. Người tham gia đã phải gửi Bitcoin đến một địa chỉ không đáng tin cậy và nhận lại token Counterparty.

1. **Proof of Capacity (PoC)**

Proof of Capacity (Bằng chứng năng lực) là một cơ chế đồng thuận sử dụng một quá trình gọi là truy tìm (tracing). Với Proof of Work, các thợ đào sử dụng điện toán để đưa ra giải pháp chính xác; tuy nhiên, với Proof of Capacity, các giải pháp trước đây được lưu trữ trong các kho kỹ thuật số (như ổ đĩa cứng). Quá trình này được gọi là truy tìm.

Sau khi một bộ lưu trữ đã được đưa ra (có nghĩa là nó đã được lấp đầy bằng các giải pháp), bạn có thể tham gia vào quá trình tạo khối.

Bất cứ ai có giải pháp nhanh nhất cho câu đố của một khối (mới), có thể tạo ra khối mới. Bạn càng có nhiều dung lượng lưu trữ, bạn càng có thể lưu trữ nhiều giải pháp, và cơ hội tạo khối càng lớn.

Burstcoin là loại tiền đầu tiên giới thiệu khái niệm này. Các ví dụ khác là Chia và SpaceMint.

1. **Proof of Elapsed time (PoET)**

Proof of Elapsed time (Bằng chứng về thời gian đã trôi qua) là một thuật toán cơ chế đồng thuận thường được sử dụng trong các mạng blockchain được ủy quyền để quyết định quyền khai thác hoặc người chiến thắng trong mạng lưới. Các mạng blockchain được ủy quyền là các mạng lưới yêu cầu bất kỳ người tham gia tiềm năng nào phải được xác định trước khi họ có thể tham gia. Dựa trên nguyên tắc của một hệ thống xổ số công bằng trong đó mỗi nút có khả năng là người chiến thắng như nhau, cơ chế PoET dựa trên cơ hội phân phối công bằng cơ hội chiến thắng giữa số lượng người tham gia mạng lớn nhất có thể.

Về cơ bản, quy trình làm việc tương tự như cơ chế đồng thuận theo sau bởi thuật toán Proof of Work (PoW), nhưng không có mức tiêu thụ năng lượng cao. Ví dụ rõ nhất của giao thức này là Hyperledger Sawtooth, một nền tảng blockchain cấp doanh nghiệp và được ủy quyền.

1. **Thuật toán đồng thuận Obelisk**

Obelisk là một thuật toán đồng thuận đầy hứa hẹn nhằm loại bỏ những thiếu sót của thuật toán Proof of Work (PoW) và Proof of Stake (PoS), giúp duy trì trạng thái blockchain trong mạng lưới phân tán với sức mạnh tính toán tối thiểu, và không cần phải tham gia. Nó làm giảm nhu cầu khai thác, cải thiện đáng kể tốc độ giao dịch và cung cấp khả năng bảo mật với sự cải thiện.

Obelisk cố gắng khắc phục các vấn đề của PoW và PoS bằng cách phân phối sự ảnh hưởng trong mạng lưới theo một khái niệm có tên là “mạng lưới tin cậy”, trong đó mật độ của mạng lưới của một node sẽ xác định ảnh hưởng của nó trong chuỗi. Trường hợp điển hình nhất của thuật toán đồng thuận này được tìm thấy trong dự án có tên là SkyCoin.

1. **Proof of Assignment (PoA)**

Proof of Assignment (Bằng chứng chuyển nhượng) là một cơ chế đồng thuận của kỷ nguyên mới, trong đó đòi hỏi ít năng lượng hơn và có thể chạy trên phần cứng low-end. Cơ chế hoạt động PoA cho phép các ứng dụng Internet of Things (IoT) hàng ngày được sử dụng cho các khả năng khai thác cơ bản có dung lượng hạn chế. Với sức mạnh xử lý của chúng, các thiết bị tương thích với IoT có thể được sử dụng để khai thác tiền điện tử.

Tuy nhiên, do bộ nhớ và khả năng xử lý trên các thiết bị này bị hạn chế, sự đóng góp của chúng cho việc khai thác vẫn còn nhỏ. Cơ chế hoạt động của thuật toán PoA tạo điều kiện cho kiểu khai thác “nhẹ nhàng” này. Ví dụ đáng chú ý nhất là trong blockchain IOTW.

1. **Proof of Checkpoint (PoC)**

Proof of Checkpoint là một hệ thống kết hợp sử dụng bất kỳ hệ thống Proof of Stake nào với một hệ thống Proof of Work. Ý tưởng của khái niệm này là để giảm thiểu các cuộc tấn công vào hệ thống Proof of Stake. Tuy nhiên, nó vẫn phải chịu một cuộc tấn công vào một nút đã bị ngắt kết nối trong một thời gian dài và đến lượt nó, có thể được sử dụng để cung cấp thông tin sai lệch về blockchain.

Mỗi khối trong hệ thống Proof of Stake đều yêu cầu loại bỏ khối Proof of Work. Mỗi khối Proof of Work không chứa các giao dịch và được liên kết trực tiếp với cả mạng Proof of Work và mạng Proof of Participation.

1. **Proof of Formulation (PoF)**

Thuật toán đồng thuận mới được đề xuất bởi nền tảng FLETA của Hàn Quốc có tên là Proof Formulation (PoF), trong đó nó cố gắng giải quyết các thiếu sót của PoW (chi tiêu năng lượng), PoS (lỗi bảo mật) và dPoS (tính tập trung) bằng cách kết hợp từng cơ chế trong một cơ chế đồng thuận duy nhất .

Trong Proof of Formulation (PoF), việc khai thác và tạo khối được thực hiện khác so với các nền tảng blockchain hiện có. Các formulator (bộ định dạng) đóng vai trò là bộ tạo khối trên nền tảng FLETA. Các nhà quan sát cho phép xác nhận theo thời gian thực mà các khối được tạo và tránh double spending. Các formulator đóng vai trò là xương sống của thuật toán PoF. Thuật toán PoF khác với PoW ở chỗ nó không đòi hỏi sức mạnh tính toán khổng lồ và cũng khác với DPoS, nơi chỉ các “delegate” được bầu mới có thể tham gia khai thác.

Do thời gian khối ngắn, chỉ 0,5 giây, khai thác có tốc độ cao, chỉ có 4 giây cho mỗi khối. Ngoài ra, trong hệ sinh thái khai thác FLETA, các khối được xác nhận ngay lập tức thông qua các Observer Nodes (Các nút quan sát). Trong số 5 nút quan sát, 3 trong số chúng nên xác nhận các khối ngay sau khi tạo chúng, cho phép các khối lan rộng một cách nhanh chóng.