**Các thuật toán đồng thuận của công nghệ Blockchain**

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

Như đã đề cập trước đó, đây là thuật toán đồng thuận blockchain đầu tiên và được sử dụng lần đầu tiên bởi Bitcoin, loại tiền điện tử hàng đầu thị trường. Trong quá trình khai thác PoW, các thợ đào giải các câu đố toán học trong đó phức tạp đòi hỏi nhiều sức mạnh tính toán.

Người đầu tiên giải được câu đố sẽ tạo ra một khối và nhận phần thưởng cho khối đó. Cách để giải quyết nó về cơ bản là một “câu đố”, vì không có phương pháp nào khác ngoài trial and error.

Thuật toán PoW đảm bảo rằng các thợ đào chỉ có thể xác thực một khối giao dịch mới và thêm nó vào chuỗi nếu các nút phân phối của mạng đạt được sự đồng thuận và chấp nhận hàm băm (hash) được tìm thấy bởi thợ đào là hợp lệ.

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

Thuật toán đồng thuận này được tạo ra như là một sự thay thế cho PoW, và nhằm mục đích đạt được sự đồng thuận phân tán. Nó được sử dụng lần đầu tiên bởi Peercoin và được tạo ra vào năm 2011 sau khi được thảo luận trong một diễn đàn Bitcointalk cùng năm.

Quá trình hoạt động của nó khác rất nhiều so với các thuật toán trước đó. Thay vì yêu cầu những người khai thác chứng minh rằng mỗi giao dịch đều hợp lệ, Proof of Stake hay Proof of Participation (Bằng chứng Tham gia) yêu cầu một người đặt cược, hold hoặc chặn coin và xác thực quyền sở hữu của họ. Nói tóm lại, thuật toán này thay thế việc khai thác PoW chuyên sâu bằng một cơ chế trong đó các khối được xác nhận theo “sự tham gia” của những người liên quan.

Mặc dù có nhiều cách khác nhau trong đó người tạo khối mới được chọn để tránh tình trạng tập trung theo số lượng coin có thể bị khóa hoặc ‘đặt cược’, nói chung, blockchain được bảo mật bởi quy trình “chọn lọc ngẫu nhiên giả”, xem xét mức độ phong phú của nút và tuổi của các đồng coin cùng với một yếu tố ngẫu nhiên.

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

Bằng chứng ủy quyền cổ phần (DPoS) là một cơ chế đồng thuận rất nhanh và nổi tiếng bởi sự thực hiện của nó trong EOS, và thường được xem là dân chủ kỹ thuật số, nhờ hệ thống bỏ phiếu có trọng số của nó.

Cách thức hoạt động là người dùng bỏ phiếu cho “những người được ủy quyền” (delegates), người được trao quyền để kiếm lợi nhuận bằng cách chạy một nút đầy đủ. Trọng số phiếu bầu của bạn phụ thuộc vào sự tham gia hoặc việc chặn tiền của bạn.

Vì các delegate muốn nhận được càng nhiều phiếu càng tốt, họ liên tục được khuyến khích để tạo ra những thứ có giá trị cho cộng đồng, vì họ có khả năng nhận được thêm phiếu bầu để làm như vậy.

Phương pháp này được cho là hiệu quả hơn và bảo vệ người dùng khỏi các quy định không mong muốn. Tuy nhiên, người đề xuất lớn nhất của nó, EOS, đã phải chịu sự xuất hiện của những nhà phát triển ban đầu cáo buộc hệ thống bị tập trung hóa và không an toàn.

## **4. 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.

## **5. 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.

## **6. 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.

## **7. 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.

## **8. 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.

## **9. 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.

## **10. 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.

## **11. 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.

## **12. 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.