Chương 4
CÁC THUẬT TOÁN ĐỒNG THUẬN BLOCKCHAIN

4.1. THUẬT TOÁN ĐỒNG THUẬN

4.1.1. Khái niệm

Thuật toán đồng thuận blockchain là tập hợp các quy tắc và cơ chế mà các nút trong mạng blockchain sử dụng để xác nhận và thống nhất về tính hợp lệ của các giao dịch/khối mới, là cơ chế giúp đảm bảo tất cả các nút (nodes) trong mạng đồng ý với trạng thái hiện tại của sổ cái kỹ thuật số (ledger), từ đó đảm bảo tính toàn vẹn và độ tin cậy cũng như duy trì sự ổn định và an toàn cho hệ thống phân tán blockchain mà không cần đến bất kỳ một bên trung gian nào.

4.1.2. Cơ chế hoạt động của thuật toán đồng thuận

Cơ chế đồng thuận trong blockchain hoạt động dựa trên nguyên tắc đồng thuận giữa các nút (nodes) trong mạng. Mục tiêu chính là đảm bảo tất cả các nút đồng ý với trạng thái hiện tại của sổ cái (ledger) và xác nhận tính hợp lệ của các giao dịch mới trước khi chúng được thêm vào blockchain. Cách thức hoạt động của cơ chế đồng thuận gồm:

Bước 1. Gửi giao dịch: Khi một giao dịch được tạo ra, nó được gửi đến mạng blockchain.

Bước 2. Xác nhận giao dịch: Các nút trong mạng (miners hoặc validator) ghi nhận giao dịch và bắt đầu quá trình xác nhận. Hệ thống sẽ kiểm tra xem giao dịch có hợp lệ không. Chẳng hạn như người gửi có đủ số dư không, giao dịch có đúng định dạng không, ...

Bước 3. Thuật toán đồng thuận: Để đạt được đồng thuận giữa các nút trong mạng, một mạng blockchain sử dụng một thuật toán cụ thể. Mỗi blockchain có thể sử dụng một thuật toán khác nhau. Một số thuật toán thường sử dụng như:

- Bằng chứng công việc (PoW - Proof of Work)
- Bằng chứng cổ phần (PoS - Proof of Stake
- Bằng chứng ủy quyền cổ phần (DPoS - Delegated Proof-of-Stake)
- Bằng chứng về trọng số (PoWeight - Proof-of-Weight)
- Bằng chứng lịch sử (PoH - Proof of History)
- Bằng chứng về quyền hạn (PoA - Proof-of-Authority)
- Bằng chứng dung lượng (PoC - Proof of Capacity)

…

Bước 5. Thêm khối vào blockchain: Một khi giao dịch được xác nhận và đồng thuận, khối mới chứa giao dịch đó được thêm vào blockchain. Khối này liên kết với khối trước đó thông qua một chuỗi mã hash, tạo thành một chuỗi liên tục không thể thay đổi.

Bước 6. Cập nhật và phát tán: Sau khi khối mới được thêm vào, thông tin được cập nhật và phát tán đến tất cả các nút trong mạng. Điều này đảm bảo rằng mọi nút đều có bản sao giống nhau của blockchain, duy trì tính nhất quán và đảm bảo tính minh bạch.

4.1.3. Các yêu cầu của một thuật toán đồng thuận Blockchain

Thuật toán đồng thuận trong blockchain được sử dụng để xác nhận và thống nhất về tính hợp lệ của các giao dịch/khối mới. Thuật toán đồng thuận trong blockchain phải đáp ứng các yêu cầu cơ bản để đảm bảo mạng lưới hoạt động ổn định, bảo mật và hiệu quả. Do đó nó phải đạt được một số yêu cầu chính sau đây:

1. *Tính nhất quán (Consistency):* Tất cả các nút trong mạng phải đồng ý về trạng thái của blockchain. Dữ liệu trong blockchain phải nhất quán trên toàn bộ mạng lưới.

2. *Tính toàn vẹn (Integrity)*: Chỉ các giao dịch hợp lệ mới được thêm vào blockchain. Mỗi khối phải tuân thủ các quy tắc đã được định nghĩa bởi giao thức. Giao dịch không thể bị chỉnh sửa hoặc thêm lại sau khi đã được ghi vào blockchain.

3. *Tính phi tập trung (Decentralization):* Quy trình đồng thuận không phụ thuộc vào một thực thể trung tâm. Bất kỳ nút nào cũng có thể tham gia xác thực mà không cần xin phép. Điều này đảm bảo tính minh bạch và loại bỏ các rủi ro từ một điểm thất bại duy nhất (single point of failure).

4. *Khả năng chịu lỗi Byzantine (Byzantine Fault Tolerance - BFT):* Hệ thống phải hoạt động chính xác ngay cả khi một số nút trong mạng gặp lỗi hoặc có hành vi độc hại. Thuật toán đồng thuận cần có khả năng đối phó với các tấn công từ các nút không trung thực.

Vấn đề này xuất phát từ một tình huống trong quân đội thười la mã, tướng Byzantine chỉ quy một nhóm tướng lĩnh của quân đội, các tướng lĩnh này chỉ huy các đội quân đóng ở các vị trí khác nhau xung quanh một thành phố của kẻ thù. Họ giao tiếp với nhau thông qua người đưa tin, các tướng lĩnh phải đồng thuận về một kế hoạch chiến đấu chung. Tuy nhiên, một hoặc nhiều tướng lĩnh có thể là những kẻ phản bội, cố gắng gây nhầm lẫn cho những người khác về kế hoạch chung. Vấn đề đặt ra là tìm một thuật toán đảm bảo rằng các tướng lĩnh trung thành có thể đạt được sự đồng thuận.

5. *Tính bảo mật (Security):* Blockchain phải được bảo vệ khỏi các cuộc tấn công như:

- Double-spending: Chi tiêu một giao dịch hai lần,
- 51% Attack: Khi một thực thể kiểm soát hơn 50% sức mạnh mạng.

Thuật toán đồng thuận phải đảm bảo rằng không kẻ tấn công nào có thể sửa đổi chuỗi khối hoặc thay đổi trạng thái giao dịch.

6. *Hiệu suất (Performance):* Thuật toán đồng thuận phải có khả năng xử lý nhanh chóng và hiệu quả số lượng lớn giao dịch. Thời gian xác nhận giao dịch và tạo khối phải được tối ưu để đảm bảo trải nghiệm người dùng.

7. *Khả năng mở rộng (Scalability)*: Hệ thống cần hỗ trợ số lượng nút tham gia ngày càng lớn mà không ảnh hưởng đến hiệu suất. Blockchain phải xử lý khối lượng giao dịch tăng dần mà vẫn duy trì tốc độ và bảo mật.

8. *Tính công bằng (Fairness)*: Mỗi nút phải có cơ hội công bằng để tham gia vào quá trình xác thực và thêm khối mới. Các nút không nên bị loại trừ hoặc ưu ái dựa trên vị trí địa lý hoặc tài nguyên sở hữu (trừ khi được quy định rõ ràng như PoS).

9. *Tính không thể đảo ngược (Finality)*: Một khi giao dịch đã được xác nhận, nó không thể bị hoàn tác hoặc thay đổi. Điều này đảm bảo tính toàn vẹn và bảo mật của blockchain.

10. *Tiết kiệm năng lượng (Energy Efficiency)*: Đặc biệt quan trọng đối với các thuật toán đồng thuận thế hệ mới (PoS, PoC). Thuật toán nên giảm thiểu tiêu thụ năng lượng mà vẫn đảm bảo tính bảo mật và hiệu quả.

Như vậy: *Một thuật toán đồng thuận trong blockchain cần đảm bảo: tính nhất quán, bảo mật, phi tập trung, hiệu suất cao, khả năng mở rộng, và khả năng chịu lỗi Byzantine. Tùy thuộc vào ứng dụng và mục tiêu, các blockchain có thể ưu tiên một số yếu tố nhất định để tối ưu hóa hiệu quả hoạt động*.

4.2. HỆ THỐNG CHỊU LỖI BYZANTINE (BFT)

Cũng giống như hầu hết các hệ thống tính toán phân tán, những người tham gia mạng lưới tiền điện tử cần phải đồng ý về trạng thái hiện tại của blockchain, và đó là cái mà chúng ta gọi là sự đồng thuận. Tuy nhiên, việc đạt được sự đồng thuận trên mạng lưới phân tán một cách an toàn và đáng tin cậy không phải là một điều dễ dàng. Vậy thì làm thế nào một mạng lưới phân tán gồm các nút máy tính đạt được sự đồng thuận khi xử lý một quyết định, nếu một số các nút trong đó có khả năng là s không đáng tin? Đây là câu hỏi cơ bản của vấn đề được gọi là bài toán các vị tướng Byzantine, từ đó sinh ra khái niệm về hệ thống chịu lỗi Byzantine.

Bài toán các vị tướng Byzantine được các nhà khoa học máy tính Leslie Lamport, Robert Shostak và Marshall Pease đề xuất trong một bài báo khoa học mang tên "The Byzantine Generals Problem" vào năm 1982 [??]. Bài toán này mô tả vấn đề đạt được **sự đồng thuận** trong một hệ thống phân tán, ngay cả khi một số thành phần trong hệ thống không hoạt động đúng hoặc cố tình đưa ra thông tin sai lệch.

Bài toán được diễn đạt một cách ẩn dụ bằng tình huống của một đội quân Byzantine (quân đội đế quốc La Mã), tiến hành vây hãm một thành phố. Các vị tướng cần trao đổi để đạt được đến một thoả thuận về kế hoạch. Trong trường hợp đơn giản nhất, họ thoả thuận về việc nên **tấn công** hay **rút lui**.

Vấn đề tấn công hay rút lui không quan trọng mà là sự đồng thuận của tất cả các tướng, tức là, đồng thuận về một quyết định chung để cùng phối hợp thực hiện. Do đó, chúng ta có thể xem xét các mục tiêu sau:

- Mỗi tướng phải quyết định: tấn công hoặc rút lui (có hay không);
- Không thể thay đổi quyết định sau khi đưa ra;
- Tất cả tướng phải nhất trí về một quyết định giống nhau và tiến hành đồng bộ với nhau.

Các vấn đề liên lạc như đề cập ở trên liên quan đến thực tế là một tướng chỉ có thể giao tiếp với các tướng khác thông qua các thông điệp được chuyển đi bởi lính đưa tin. Vấn đề trọng tâm của bài toán các vị tướng Byzantine ở đây là các thông điệp có thể bị chậm, hủy hoặc mất. Ngoài ra, ngay cả khi thông điệp được gửi thành công, vẫn còn khả năng xảy ra một hoặc nhiều tướng có thể chọn thực hiện hành động gây hại và gửi đi một thông điệp sai để gây nhiễu tới các tướng khác, dẫn đến một thất bại hoàn toàn.

Nếu chúng ta áp dụng bài toán này vào trường hợp có sự xuất hiện của blockchain, mỗi tướng sẽ đại diện cho một nút mạng và các nút cần đạt được sự đồng thuận về trạng thái hiện tại của hệ thống. Nói cách khác, phần lớn những người tham gia trong một mạng lưới phân tán phải đồng ý và thực hiện cùng một hành động để tránh một thất bại hoàn toàn.

Cơ chế hoạt động của hệ thống chịu lỗi Byzantine

Cơ chế hoạt động của BFT là dựa trên sự đồng thuận và phân tách thông tin. Khi và chỉ khi các phần tử trong hệ thống đều đạt được sự đồng thuận thì một giao dịch hay một quyết định mới được thực hiện. Và để đạt được sự đồng thuận không phải là một câu chuyện dễ dàng. BFT phải sử dụng một số thuật toán phức tạp hơn, điều này nhằm đảm bảo tất cả các thành phần trong cùng một hệ thống sẽ thống nhất được thông tin chính xác nhất trước khi đưa ra kết quả cuối cùng.

Điểm quan trọng ở đây là sự phân tách thông tin trong hệ thống. Hệ thống không cần phải đạt được tất cả sự đồng thuận mà chỉ cần một phần nào đó là được. Mục đích của hành động này cũng nhằm ngăn chặn các sự gian lận của một số phần tử. Một khía cạnh quan trọng khác trong cơ chế hoạt động của BFT là việc phân bổ công việc và trách nhiệm cho các nút. Mỗi nút trong mạng lưới có thể được giao một phần công việc cụ thể để đảm bảo rằng không có nút nào có quyền kiểm soát quá nhiều thông tin hoặc ảnh hưởng quá lớn đến quyết định chung. Sự phân bổ này giúp giảm thiểu rủi ro từ các nút độc hại và đảm bảo rằng ngay cả khi một số nút bị chiếm quyền điều khiển.

BFT cung cấp một lớp bảo mật và độ tin cậy cao, do đó việc triển khai và duy trì các hệ thống chịu lỗi này có nhiều thách thức. Những thách thức này đòi hỏi sự cân nhắc kỹ lưỡng và sự phát triển liên tục để đảm bảo rằng các hệ thống BFT có thể đáp ứng được yêu cầu của môi trường hoạt động thực tế.

Mô hình BFT là một trong những nền tảng cốt lõi để xây dựng các hệ thống blockchain an toàn và phi tập trung. Nhiều dự án blockchain hiện đại đã tích hợp

hoặc phát triển các biến thể của mô hình này nhằm đảm bảo tính toàn vẹn, bảo mật và hiệu suất cao hơn.

Nói tóm lại, hệ thống chịu lỗi Byzantine là hệ thống có thể giải quyết được vấn đề của bài toán các vị tướng quân Byzantine. Điều này có nghĩa là hệ thống BFT có thể tiếp tục hoạt động ngay cả khi một số nút bị lỗi hoặc thực hiện hành động gây hại. Có nhiều giải pháp khả thi cho vấn đề của bài toán các vị tướng Byzantine. Do đó, có nhiều cách để xây dựng một hệ thống BFT. Tương tự như vậy, có nhiều cách khác nhau để một blockchain đạt được hệ thống chịu lỗi Byzantine và điều mà chúng ta có ở đây chính là các thuật toán đồng thuận. Trong các phần tiếp theo trình bày một số thuật toán đồng thuận đã được triển khai trong thực tế.

4.3. THUẬT TOÁN BẰNG CHỨNG CÔNG VIỆC

Thuật toán Bằng chứng công việc (Proof of Work - PoW), nguyên tắc chính của thuật toán này là các nút mạng phải giải một bài toán mật mã phức tạp để tìm ra một hàm băm hợp lệ thỏa mãn điều kiện đã cho. Nó đòi hỏi các nút phải mất chi phí tính toán (làm việc - work) rất lớn. Một số mạng sử dung thuật toán này như là Bitcoin, Ethereum 1.0, …

4.3.1. Lịch sử phát triển của thuật toán bằng chứng công việc

Vào năm 1999, trong [??] Markus Jakobsson và Ari Juels đề xuất sáng kiến Bằng chứng công việc, đánh dấu một bước ngoặt quan trọng trong lĩnh vực tiền điện tử. Đây là một cách thức mới để xác thực giao dịch trên mạng lưới blockchain phi tập trung. Ý tưởng ban đầu được thực hiện để xây dựng một hệ thống hoạt động trên nền tảng mạng P2P (peer to peer) vốn có. Jakobsson và Juels đã sử dụng kết hợp phương pháp băm (hashing) và Bằng chứng công việc để đạt được sự đồng thuận phi tập trung giữa các nút về thứ tự giao dịch. Hệ thống này được gọi là "Bằng chứng công việc". Ý tưởng này xuất phát từ mong muốn phi tập trung hóa quá trình xác thực giao dịch một cách tối đa. Điều này có nghĩa là mọi người tham gia đều có thể xác nhận giao dịch một cách hiệu quả mà không cần truy cập bất kỳ cơ sở dữ liệu trung tâm nào. Ý tưởng sau đó được tinh chỉnh và triển khai trên mạng Bitcoin. Trên mạng lưới Bitcoin, thợ đào cần giải một bài toán toán học phức tạp trước khi thêm giao dịch vào blockchain và nhận phần thưởng. Bài toán được thiết kế để tốn rất nhiều sức mạnh tính toán, khiến cho việc một cá nhân đơn độc kiểm soát quá trình đào coin trở nên khó khăn. Điều này ngăn chặn một cá nhân chiếm đa số sức mạnh băm và kiểm soát giao dịch.

4.3.2. Cơ chế hoạt động của PoW

Bước 1: Tạo khối mới

Một nút trong mạng (thợ đào - miner) chuẩn bị một khối mới để thêm vào blockchain. Khối mới chứa các thành phần chính:

- Danh sách các giao dịch hợp lệ đã được xác thực.
- Mã hash của khối trước để liên kết với khối trước đó trong chuỗi.

- Nonce: Một số ngẫu nhiên sẽ được tìm kiếm để giải bài toán băm.
- Thông tin metadata: Bao gồm thời gian khối và thông tin khác.

Bước 2: Giải bài toán băm

Mỗi thợ đào thực hiện hàng triệu phép tính băm để tìm giá trị nonce sao cho hàm băm của khối thỏa mãn yêu cầu độ khó (số lượng chữ số 0 nhất định ở đầu chuỗi băm).

Ví dụ: Nếu độ khó là 4, hàm băm phải có dạng 0000abcd1234ef....

Đây là bước tiêu tốn tài nguyên tính toán vì cần thử nhiều giá trị nonce cho đến khi tìm được kết quả đúng.

Bước 3: Phát tán kết quả

Thợ đào đầu tiên tìm được giá trị nonce hợp lệ sẽ gửi (broadcast) kết quả cho toàn bộ các nút trong mạng. Thông tin phát tán bao gồm:

- Dữ liệu của khối.
- Nonce đã tìm được.
- Kết quả hàm băm của khối.

Bước 4: Xác minh khối

Các nút khác trong mạng nhận thông tin và tiến hành kiểm tra tính hợp lệ của khối:

- Kiểm tra xem hàm băm có đúng định dạng yêu cầu (có đủ số chữ số 0 ở đầu) hay không.
- Kiểm tra tính đúng đắn của các giao dịch trong khối để đảm bảo không có gian lận như double-spending (chi tiêu hai lần).

Nếu khối hợp lệ, các nút sẽ thêm khối đó vào chuỗi blockchain của mình.

Bước 5: Thêm khối vào blockchain

Sau khi được xác minh, khối được thêm vào chuỗi blockchain. Chuỗi blockchain sẽ tiếp tục phát triển từ khối mới này như một phần mở rộng của chuỗi chính.

Bước 6: Nhận phần thưởng

Thợ đào giải thành công bài toán sẽ nhận được:

- Phần thưởng khối: Một lượng coin mới được sinh ra từ giao thức.

- Phí giao dịch: Tổng phí từ các giao dịch được chứa trong khối.

Bước 7: Điều chỉnh độ khó

Mạng blockchain tự động điều chỉnh độ khó để duy trì thời gian tạo khối trung bình ổn định.

Ví dụ: Trong mạng Bitcoin, độ khó được điều chỉnh sau mỗi 2016 khối (~2 tuần), nhằm duy trì thời gian tạo khối trung bình là 10 phút.

4.3.3. Cơ chế đồng thuận trong mạng Bitcoin

Bước 1: Tạo khối mới

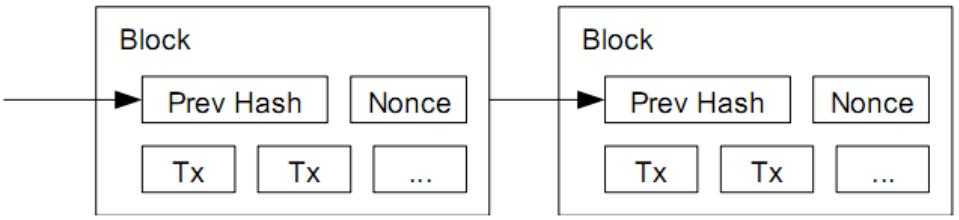
Sau khi xác thực giao dịch, một nút bitcoin sẽ thêm chúng vào danh sách giao dịch (memory pool) các giao dịch này chờ cho đến khi chúng được đưa vào để tạo thành một khối (block). Giả sử hiện tại (thời điểm viết giáo trình này) một nút X đã lắp ráp được một chuỗi lên đến khối 878.903. Nút X đang lắng nghe các giao dịch, cố gắng khai thác một khối mới và cũng lắng nghe các khối được các nút khác phát hiện. Khi nút của X đang khai thác thì nhận được khối 878.904 thông qua mạng bitcoin. Sự xuất hiện của khối này báo hiệu sự kết thúc của cuộc cạnh tranh cho khối 878.904 và sự bắt đầu của cuộc cạnh tranh để tạo ra khối 878.905.

Trong 10 phút trước đó, khi nút X đang tìm kiếm giải pháp cho khối 878.904, nó cũng đồng thời thu thập các giao dịch để chuẩn bị cho khối tiếp theo. Đến thời điểm này, nút đã thu thập được vài trăm giao dịch trong memory pool. Khi nhận được khối 878.904 và xác thực thành công, nút X sẽ so sánh các giao dịch trong khối đó với tất cả các giao dịch trong memory pool và loại bỏ những giao dịch đã được đưa vào khối 878.904. Những giao dịch còn lại trong memory pool là các giao dịch chưa được xác nhận và đang chờ được ghi vào một khối mới (khối thứ 878.905).

Nút X sẽ tạo một khối trống mới, khối thứ 878.905. Khối này được gọi là khối ứng viên (candidate block), vì nó chưa phải là khối hợp lệ do chưa có bằng chứng công việc hợp lệ. Khối này chỉ trở thành hợp lệ nếu thợ đào thành công trong việc tìm ra giải pháp cho thuật toán PoW.

Lưu ý giao dịch đầu tiên trong bất kỳ khối nào nó là một giao dịch đặc biệt, được gọi là giao dịch coinbase. Giao dịch này được tạo bởi nút X và chứa phần thưởng cho người sở hữu nút X nếu khai thác khối thành công. Nút X tạo giao dịch coinbase như một khoản thanh toán vào ví của người sở hữu X. Giao dịch này thực hiện chuyển đến địa chỉ ví của X số tiền bằng tiền thường (hiện tại là 3,125BTC) + phí giao dịch.

Khác với các giao dịch thông thường, giao dịch coinbase không sử dụng UTXO (đầu ra chưa được chi tiêu) làm đầu vào. Thay vào đó, nó chỉ có một đầu vào duy nhất, gọi là coinbase, tạo ra bitcoin từ "Nothing". Giao dịch coinbase có một đầu ra, là khoản thanh toán đến địa chỉ ví bitcoin của thợ đào.



Hình 4.1. Minh họa cấu trúc các khối trong blockchain

Tạo Block Header

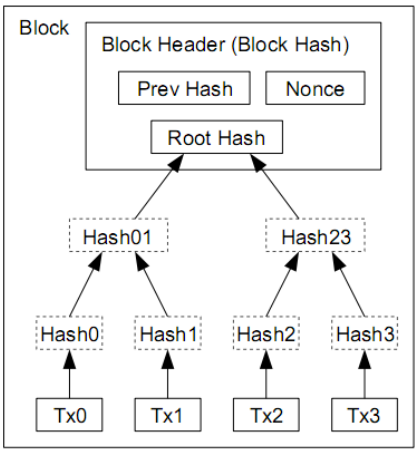
Một Block header không chứa giao dịch nào sẽ có kích thước 80 bytes. Gồm các trường thông tin:

Kích thước	Trường	Mô tả
4 bytes	Phiên bản (Version)	Số phiên bản dùng để theo dõi các bản nâng cấp phần mềm/giao thức.
32 bytes	Mã hash khối trước (Previous Block Hash)	Tham chiếu đến hash của khối trước đó (khối cha) trong chuỗi.
32 bytes	Gốc cây Merkle (Merkle root)	Mã hash của gốc cây Merkle chứa các giao dịch của toàn bộ khối
4 bytes	Dấu thời gian (Timestamp)	Thời gian tạo khối (tính bằng giây kể từ Unix Epoch).
4 bytes	Độ khó (Target)	Mục tiêu của thuật toán PoW cho khối này.
4 bytes	Nonce	Bộ đếm được sử dụng trong thuật toán PoW

Trường đầu tiên mô tả số phiên bản của khối được lưu trong 4 bytes, tại thời điểm khối 878.903 được khai thác, số phiên bản của khối là 0x2710e000. Mô tả mã hash của khối trước đó bằng 32 bytes, mã hash của khối trước của khối 878.903 là:

000000000000000001d043b2c9bd7f4bb4e41b1730381b87da0cae7b0343c2

Tiếp theo là 32 bytes mô tả mã hash của gốc cây Merkle. Cây Merkle là cây mô tả mã hash của các giao dịch trong khối. Cây Merkle được xây dựng như sau: lá của cây là các giao dịch, lưu ý giao dịch coinbase được liệt kê đầu tiên, tiếp theo là các giao dịch được thêm vào khối. Thực hiện tính mã hash của mỗi giao dịch (lá), được các nút cha của các lá, tiếp theo kết hợp 2 mã hash của 2 giao dịch liền kề để được mã hash char của 2 mã hash đó, cứ làm như vậy cho đến khi ta thu được mã hash của nút gốc. Xem mô tả cây Merkle trong hình 4.2 dưới đây.



Hình 4.2. Cấu trúc cây Merkle

Dấu thời gian của nút được mô tả trong 4 bytes, được mã hóa dưới dạng thời gian epoch Unix, dựa trên số giây đã trôi qua kể từ nửa đêm ngày 1 tháng 1 năm 1970 theo giờ UTC/GMT. Độ khó (target) của thuật toán PoW được lưu trong 4 bytes và cuối cùng là số nonce, ban đầu được khởi tạo bằng 0. Sau khi tất cả các trường khác đã được điền đầy đủ, block header đã hoàn chỉnh và quá trình khai thác được bắt đầu. Mục tiêu lúc này là tìm một giá trị nonce sao cho hash của block header nhỏ hơn giá trị mục tiêu (target). Nút khai thác thực hiện bước 2.

Bước 2: Giải bài toán băm (khai thác)

Sau khi khối ứng viên được tạo bởi nút X, nó sẽ thực hiện khai thác khối này nhằm tìm ra lời giải cho thuật toán PoW để làm cho khối trở nên hợp lệ. Tức là lúc này này nút X phải đi tìm một giá trị nonce sao cho hash của block header nhỏ hơn giá trị mục tiêu.

Nói một cách đơn giản, khai thác là quá trình băm đi băm lại block header, với sự thay đổi một tham số duy nhất đó là số nonce cho đến khi giá trị mã hash kết quả thỏa mãn một mục tiêu cụ thể. Kết quả của hàm băm không thể được xác định trước, cũng như không thể tạo ra một mẫu có thể sinh ra một giá trị hash cụ thể. Tính chất này của hàm băm dẫn tới cách duy nhất là để tạo ra một kết quả hash khớp với mục tiêu thì chúng ta phải thử đi thử lại, thay đổi ngẫu nhiên đầu vào cho đến khi đạt được kết quả hash mong muốn xuất hiện.

Một thuật toán băm nhận dữ liệu đầu vào tùy ý và tạo ra một kết quả đầu ra có độ dài cố định. Thuật toán băm như vậy được gọi là **dấu vân tay số** của dữ liệu đầu vào. Đối với một đầu vào cụ thể, kết quả băm sẽ luôn giống nhau và có thể dễ dàng tính toán cũng như xác minh bởi bất kỳ ai sử dụng cùng thuật toán băm. Với thuật toán băm SHA256, đầu ra luôn có độ dài 256 bit, bất kể kích thước của dữ liệu đầu vào.

Trong mạng bitcoin sử dụng hàm băm SHA256 để tìm giá trị hash của Block header nhỏ hơn mục tiêu được thiết lập của mạng. Quá trình tìm giá trị nonce để tạo

ra hash của Block header thỏa mãn sẽ mất rất nhiều công sức. Do đó, nó được gọi là bằng chứng công việc (PoW).

Như vậy PoW là phải tạo ra một giá trị băm nhỏ hơn mục tiêu (target). Mục tiêu càng cao thì việc tìm một giá trị băm nhỏ hơn mục tiêu càng dễ dàng. Ngược lại, mục tiêu càng nhỏ thì việc tìm một giá trị băm nhỏ hơn mục tiêu càng khó khăn.

Bước 3: Phát tán kết quả

Khi giá trị nonce được tìm thấy và được ghi vào block header, nó tạo ra giá trị hash của block header này. Ngay lập tức, nút X truyền khối này đến tất cả các nút ngang hàng của nó. Các nút đó nhận khối, xác thực, và sau đó tiếp tục lan truyền khối mới này tới các nut khác. Khi khối được lan truyền khắp mạng lưới, mỗi nút thêm khối vào bản sao blockchain của riêng mình, tăng chiều cao khối mới là 878.905. Khi các nút khai thác nhận và xác thực khối này, chúng sẽ từ bỏ việc tìm kiếm khối ở cùng chiều cao và ngay lập tức bắt đầu tính toán khối tiếp theo trong chuỗi bằng cách sử dụng khối được tạo ra bởi nút X làm "khối cha". Các thợ đào đưa khối của nút X đào được vào blockchain của mình là đã "bỏ phiếu" cho khối của X và chuỗi mà nó mở rộng.

Bước 4: Xác minh khối

Khi khối mới tìm được một nút trong mạng tìm được số nonce sao cho hash của của block header thỏa mãn độ khó nó được lan truyền qua mạng, mỗi nút nhận được khối này sẽ thực hiện một loạt các kiểm tra để xác thực khối đó trước khi tiếp tục lan truyền đến các nút khác. Điều này đảm bảo rằng chỉ các khối hợp lệ mới được lan truyền trong mạng lưới.

Việc xác thực độc lập này đảm bảo rằng các thợ đào hành động trung thực thì các khối của họ sẽ được thêm vào blockchain, từ đó nhận được phần thưởng. Ngược lại, những thợ đào hành động không trung thực khối của họ sẽ bị từ chối và không chỉ mất phần thưởng mà còn lãng phí công sức và chi phí điện năng đã bỏ ra để tìm kiếm lời giải cho PoW mà không được bù đắp.

Khi một nút nhận được một khối mới, nó sẽ xác thực khối đó bằng cách kiểm tra dựa trên một danh sách các tiêu chí cần phải đáp ứng; nếu không, khối sẽ bị từ chối. Các tiêu chí này có thể được xem trong mã nguồn của **Bitcoin Core Client** qua các hàm CheckBlock và CheckBlockHeader, bao gồm:

- Cấu trúc dữ liệu của khối phải hợp lệ về mặt cú pháp.
- Hash của block header phải nhỏ hơn mục tiêu (đảm bảo PoW).
- Dấu thời gian của khối không được vượt quá hai giờ so với thời gian hiện tại.
- Kích thước của khối phải nằm trong giới hạn cho phép.
- Giao dịch đầu tiên (và chỉ giao dịch đầu tiên) phải là giao dịch coinbase.
- Tất cả các giao dịch trong khối phải hợp lệ.

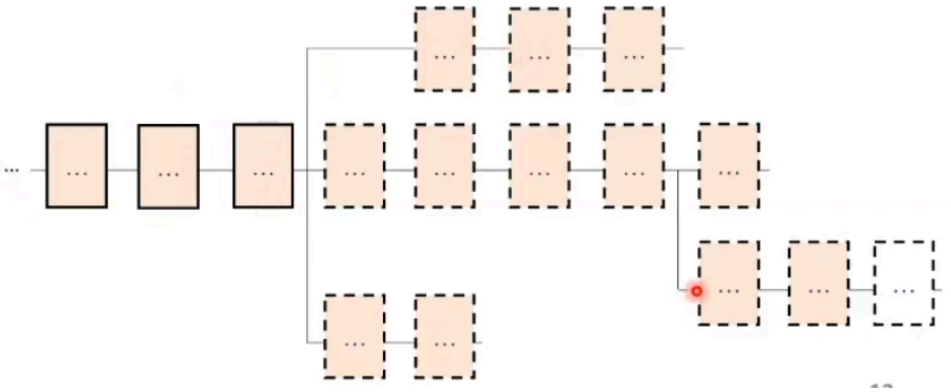
Việc xác thực độc lập mỗi khối mới bởi tất cả các nút trong mạng lưới đảm bảo rằng thợ đào không thể gian lận. Trong các phần trước, chúng ta đã thấy rằng thợ đào có quyền tạo một giao dịch để nhận phần thưởng bitcoin mới được tạo ra trong khối đồng thời thu phí giao dịch.

Vậy tại sao thợ đào không tự tạo cho mình một giao dịch với phần thưởng lên đến một nghìn bitcoin thay vì phần thưởng đúng quy định? Bởi vì mọi nút trong mạng đều xác thực các khối theo cùng một quy tắc chung. Một giao dịch coinbase không hợp lệ sẽ khiến toàn bộ khối trở nên không hợp lệ, dẫn đến khối đó sẽ bị từ chối và giao dịch sẽ không bao giờ được ghi vào sổ cái. Thợ đào buộc phải xây dựng một khối hoàn hảo dựa trên các quy tắc chung mà tất cả các nút tuân theo và khai thác khối đó với một lời giải PoW hợp lệ. Để làm được điều này, họ phải tiêu tốn rất nhiều điện năng trong quá trình khai thác. Nếu gian lận, tất cả công sức và chi phí điện năng sẽ bị lãng phí. Đó là lý do tại sao quá trình xác thực độc lập là một thành phần quan trọng trong cơ chế đồng thuận phi tập trung.

Bước 5: Thêm khối vào blockchain

Bước cuối cùng trong cơ chế đồng thuận phi tập trung của Bitcoin là lắp ráp các khối thành chuỗi và chọn chuỗi có tổng công sức PoW lớn nhất. Khi một nút đã xác thực thành công một khối mới, nó sẽ cố gắng lắp ráp vào một chuỗi bằng cách kết nối khối đó vào blockchain hiện có. Mỗi nút duy trì ba tập hợp khối chính:

1. Các khối được kết nối với chuỗi chính (main blockchain).
2. Các khối tạo thành các nhánh rẽ ra từ chuỗi chính (secondary chains).
3. Các khối không có "khối cha" đã biết trong các chuỗi hiện tại (orphans – khối mồ côi).



Hình 4.3. Minh họa các chuỗi khối trong một nút của mạng blockchain

Các khối không hợp lệ sẽ bị từ chối ngay khi chúng không đáp ứng một tiêu chí xác thực nào đó và do đó không được thêm vào bất kỳ chuỗi nào.

"Chuỗi chính" tại bất kỳ thời điểm nào là chuỗi khối hợp lệ có tổng công sức PoW tích lũy lớn nhất. Trong hầu hết các trường hợp, đây là chuỗi có nhiều khối nhất (dài nhất tính theo số khối), trừ khi có hai chuỗi dài bằng nhau nhưng một chuỗi có tổng công sức PoW lớn hơn. Chuỗi chính cũng có các nhánh chứa các khối "anh em" với các khối trên chuỗi chính. Những khối này hợp lệ nhưng không thuộc chuỗi

chính. Chúng được lưu giữ để tham chiếu trong tương lai, phòng trường hợp một trong các chuỗi nhánh được mở rộng và vượt qua chuỗi chính về tổng công sức PoW.

Khi một nút nhận được một khối mới, nó sẽ cố gắng chèn khối đó vào blockchain hiện có. Nút sẽ kiểm tra trường "previous block hash" của khối, là tham chiếu đến khối cha của nó. Sau đó, nút sẽ cố gắng tìm khối cha đó trong blockchain hiện tại.

Phần lớn khối cha sẽ là khối cuối cùng của chuỗi chính, nghĩa là khối mới sẽ được thêm vào chuỗi chính. Tuy nhiên, đôi khi, khối mới sẽ được thêm vào một chuỗi không phải là chuỗi chính. Trong trường hợp đó, nút sẽ gắn khối mới vào chuỗi phụ và so sánh tổng công sức PoW của chuỗi phụ đó với chuỗi chính. Nếu chuỗi phụ có tổng công sức PoW lớn hơn chuỗi chính, nút sẽ chuyển sang chuỗi phụ, nghĩa là nó sẽ chọn chuỗi phụ làm chuỗi chính mới và chuỗi chính cũ sẽ trở thành chuỗi phụ.

Nếu nhận được một khối hợp lệ nhưng không tìm thấy khối cha trong các chuỗi hiện có, khối đó được coi là khối mồ côi (orphan). Các khối mồ côi sẽ được lưu trữ trong bộ nhớ tạm của các khối mồ côi, nơi chúng sẽ ở lại cho đến khi khối cha được nhận. Khi khối cha được nhận và liên kết vào các chuỗi hiện có, khối mồ côi có thể được lấy ra khỏi bộ nhớ tạm (orphan pool) và liên kết với khối cha, trở thành một phần của chuỗi. Các khối mồ côi thường xuất hiện khi hai khối được khai thác gần như đồng thời và được nhận theo thứ tự ngược lại (khối con trước khối cha).

Bằng cách chọn chuỗi hợp lệ có tổng công sức PoW tích lũy lớn nhất, tất cả các nút cuối cùng đạt được sự đồng thuận trên toàn mạng lưới. Những khác biệt tạm thời giữa các chuỗi sẽ được giải quyết khi công sức tính toán được bổ sung, mở rộng một trong các chuỗi khả dĩ.

Khi thợ đào khai thác một khối mới và mở rộng chuỗi, khối mới đó chính là lá phiếu biểu quyết của họ.

Bước 6: Nhận phần thưởng

Để tạo giao dịch coinbase, nút X trước tiên tính tổng số phí giao dịch bằng cách cộng tất cả các đầu vào và đầu ra của các giao dịch được thêm vào khối. Phí giao dịch được tính theo công thức:

Tổng phí = Tổng (Đầu vào) - Tổng (Đầu ra)

Tiếp theo, nút X tính phần thưởng chính xác cho khối mới. Ban đầu phần thưởng được thiết lập là 50BTC khi khai thác được một khối mới, sau mỗi 210.000 khối thì phần thưởng sẽ giảm đi một nửa. Như vậy với việc đào được khối thứ 878.905 thì nút X sẽ nhận được phần thưởng là 3,125BTC.

Số lần giảm một nửa tối đa được phép là 64, vì vậy nếu vượt quá 64 lần giảm, phần thưởng sẽ bị đặt về 0. Khi đó thợ đào chỉ nhận được phí giao dịch khi đào được khối mới.

Bước 7: Điều chỉnh độ khó

Khi tạo ra một khối mời, nhiệm vụ của các nút là tìm ra số nonce để làm cho hash của block header nhỏ hơn mục tiêu. Với độ khó hiện tại trên mạng Bitcoin, thợ đào phải thử hàng hàng triệu tỷ lần trước khi tìm được một nonce để tạo ra giá trị hash của block header đủ nhỏ để thỏa mãn mục tiêu. Chúng ta có thể thấy, việc tăng độ khó thêm 1 bit sẽ làm tăng không gian tìm kiếm lời giải tăng gấp đôi.

Trung bình, mạng lưới cần thực hiện hơn 1.8 septa-hashes (tức hàng nghìn tỷ tỷ tỷ phép tính băm) mỗi giây để tìm ra khối tiếp theo. Điều này có vẻ là một nhiệm vụ bất khả thi, nhưng may mắn thay, mạng lưới hiện có sức mạnh xử lý lên đến 3 exa-hashes mỗi giây (EH/s, tương đương 3 tỷ tỷ phép tính băm mỗi giây), cho phép tìm ra một khối trong khoảng 10 phút trung bình.

Như chúng ta đã thấy, mục tiêu quyết định độ khó và do đó ảnh hưởng đến thời gian tìm ra giải pháp cho thuật toán PoW. Điều này dẫn đến các câu hỏi hiển nhiên: Tại sao độ khó cần được điều chỉnh, ai điều chỉnh nó và điều chỉnh như thế nào?

Các khối của Bitcoin được tạo ra trung bình mỗi 10 phút. Đây được coi như "nhịp đập" của hệ thống Bitcoin, hỗ trợ tần suất phát hành tiền tệ và tốc độ xử lý giao dịch. Tần suất này cần phải được duy trì ổn định không chỉ trong ngắn hạn mà còn trong suốt hàng thập kỷ. Trong khoảng thời gian dài đó, công suất tính toán dự kiến sẽ tiếp tục tăng với tốc độ nhanh chóng. Hơn nữa, số lượng người tham gia khai thác và hệ thống máy tính họ sử dụng cũng sẽ liên tục thay đổi. Để giữ thời gian tạo khối ở mức trung bình 10 phút**,** độ khó khai thác phải được điều chỉnh để bù đắp cho những thay đổi này.

Với mạng Bitcoin, việc điều chỉnh độ khó (retargeting) diễn ra một cách tự động và độc lập trên mỗi nút mạng. Cứ sau 2,016 khối, tất cả các nút sẽ điều chỉnh lại PoW. Phương trình điều chỉnh đo thời gian thực tế cần để tìm ra 2,016 khối cuối cùng và so sánh với thời gian mong đợi là 20,160 phút. Tỷ lệ giữa thời gian thực tế và thời gian mong đợi được tính toán, và từ đó thực hiện điều chỉnh mục tiêu (tăng hoặc giảm) một cách tương ứng.

- Nếu mạng lưới tìm ra các khối nhanh hơn 10 phút/khối, độ khó sẽ tăng lên (giá trị mục tiêu giảm xuống).
- Nếu tốc độ tìm khối chậm hơn mong đợi, độ khó sẽ giảm xuống (giá trị mục tiêu tăng lên).

Công thức điều chỉnh có thể được tóm tắt như sau:

$$Target_{new} = Target_{current} \times \left(\frac{Số\ phút\ thực\ tế\ đào\ 2016\ khối}{20160\ (phút)}\right)$$

Để tránh sự biến động quá lớn trong độ khó, việc điều chỉnh độ khó phải nhỏ hơn hoặc bằng hệ số 4 cho mỗi chu kỳ điều chỉnh. Nếu cần điều chỉnh mục tiêu vượt quá hệ số 4, thì nó sẽ bị giới hạn ở mức hệ số 4 và không cao hơn.

Bất kỳ sự điều chỉnh thêm nào sẽ được thực hiện trong chu kỳ điều chỉnh tiếp theo, vì sự mất cân bằng sẽ tiếp tục tồn tại qua 2,016 khối tiếp theo. Do đó, sự chênh lệch lớn giữa sức mạnh tính toán và độ khó có thể cần đến vài chu kỳ 2,016 khối để được cân bằng hoàn toàn.

Độ khó của việc khai thác một khối bitcoin được thiết lập sao cho toàn bộ mạng lưới mất khoảng 10 phút để xử lý một khối, dựa trên thời gian khai thác 2,016 khối trước đó và được điều chỉnh sau mỗi 2,016 khối. Điều này đạt được bằng cách giảm hoặc tăng mục tiêu.

Lưu ý rằng mục tiêu (target) không phụ thuộc vào số lượng giao dịch hoặc giá trị của các giao dịch. Điều này có nghĩa là lượng sức mạnh tính toán, và do đó lượng điện năng tiêu tốn để bảo vệ mạng lưới Bitcoin, hoàn toàn độc lập với số lượng giao dịch.

4.3.4. Ưu nhược điểm của thuật toán đồng thuận PoW

4.3.4.1. Ưu điểm của PoW

- **Bảo mật cao**: PoW yêu cầu các thợ đào phải giải các bài toán mật mã rất khó, nhưng dễ dàng kiểm tra. Việc thay đổi dữ liệu trong một khối sẽ làm thay đổi toàn bộ chuỗi băm liên kết, khiến kẻ tấn công phải giải lại toàn bộ chuỗi, điều này đòi hỏi sức mạnh tính toán cực kỳ lớn. Tấn công 51% là lý thuyết có thể xảy ra nhưng thực tế rất khó khăn với các mạng lưới lớn như Bitcoin.

- **Tính phi tập trung:** PoW giúp đảm bảo rằng không có thực thể trung tâm nào kiểm soát mạng lưới. Bất kỳ ai có thiết bị tính toán đều có thể tham gia mạng lưới và trở thành thợ đào mà không cần sự cho phép từ một bên thứ ba.

- **Chống gian lận và double-spending**: PoW đảm bảo rằng các giao dịch không thể bị ghi đè hoặc sửa đổi sau khi đã được thêm vào blockchain. Ngăn chặn hành vi chi tiêu hai lần (double-spending) vì các giao dịch đã được xác nhận trở thành một phần vĩnh viễn của chuỗi khối.

- **Khả năng bất biến và minh bạch:** Một khi dữ liệu được ghi vào blockchain thông qua PoW, nó gần như không thể thay đổi hoặc bị xóa. Blockchain PoW công khai tất cả các khối, cho phép người dùng kiểm tra và xác minh một cách minh bạch.

- **Đơn giản trong cơ chế hoạt động:** PoW chỉ yêu cầu việc giải các phép tính băm mật mã (trong mạng Bitcoin là SHA-256), giúp các nút tham gia có thể dễ dàng kiểm tra tính hợp lệ mà không cần cơ chế phức tạp.

4.3.4.2. Nhược điểm của PoW

- **Tiêu tốn năng lượng:** Việc giải bài toán băm đòi hỏi sức mạnh tính toán khổng lồ và tiêu tốn rất nhiều điện năng.

- **Yêu cầu phần cứng mạnh:** Các thợ đào cần sử dụng các thiết bị chuyên dụng như ASIC để cạnh tranh trong việc tìm giá trị nonce, khiến chi phí đầu tư phần cứng rất cao. Người dùng thông thường khó tham gia khai thác do không đủ điều kiện phần cứng và tài nguyên, dẫn đến sự tập trung vào các mỏ đào lớn (mining pools).

- Khả năng tập trung hóa: Các mỏ đào lớn có thể tập trung sức mạnh tính toán và chi phối mạng. Các pool đào (mining pools) – nơi nhiều thợ đào hợp tác để chia sẻ phần thưởng – có thể làm giảm tính phi tập trung của mạng. Các mỏ đào lớn có thể chiếm phần lớn sức mạnh tính toán, gây nguy cơ tập trung hóa.

- Tốc độ xử lý giao dịch thấp: Do thời gian tạo khối cố định (trung bình 10 phút/khối trong Bitcoin), số lượng giao dịch có thể xử lý trong một giây (TPS) bị giới hạn. Bitcoin chỉ có thể xử lý khoảng 7 giao dịch/giây (TPS), trong khi các hệ thống thanh toán tập trung như Visa có thể xử lý hàng chục nghìn giao dịch mỗi giây.

4.4. THUẬT TOÁN BẰNG CHỨNG CỔ PHẦN (POS)

- Bằng chứng cổ phần (PoS - Proof of Stake), thay vì sử dụng sức mạnh tính toán như PoW, PoS chọn người xác thực (validators) dựa trên số lượng coin (token) họ đặt cọc trong mạng lưới. Người nắm giữ nhiều coin hơn (hoặc đặt cọc lâu hơn) có cơ hội cao hơn để được chọn tạo khối mới. Một số mạng sử dung thuật toán này như là Ethereum 2.0, Cardano, Solana, Algorand, …

4.4.1. Lịch sử phát triển của thuật toán bằng chứng cổ phần

Một trong những vấn đề chính mà chúng ta cần quan tâm đến các giao thức của các blockchain dựa trên PoW là năng lượng cần thiết để thực thi chúng. Hiên nay lương điện tiêu thụ để duy trì mạng blockchain Bitcoin có thể so sánh với một quốc gia nhỏ. Thực trạng này đã thúc đẩy việc nghiên cứu các giao thức blockchain thay thế, nhằm loại bỏ sự phụ thuộc vào PoW bằng cách thay thế nó bằng một cơ chế khác hiệu quả hơn về năng lượng nhưng vẫn cung cấp các đảm bảo tương tự [??].

Khái niệm về PoS đã được thảo luận rộng rãi trên diễn đàn Bitcoin.
Các thiết kế blockchain dựa trên bằng chứng cổ phần đã được nghiên cứu một cách chính thức bởi Bentov và cộng sự, cả khi kết hợp với bằng chứng công việc (PoW) và khi PoS là cơ chế duy nhất cho một giao thức blockchain [5]. Mặc dù Bentov và cộng sự đã chỉ ra rằng các giao thức của họ an toàn trước một số loại tấn công nhất định, nhưng họ không cung cấp một mô hình chính thức để phân tích các giao thức dựa trên PoS hoặc các chứng minh bảo mật dựa trên các định nghĩa chính xác. Nhiều giao thức blockchain dựa trên PoS đã được đề xuất (và triển khai) cho một số loại tiền điện tử, tuy nhiên vì dựa trên các lập luận bảo mật có tính chất kinh nghiệm, các loại tiền điện tử này thường được phát hiện có những thiếu sót từ góc độ bảo mật.

Ý tưởng về PoS lần đầu tiên được đề xuất trên diễn đàn Bitcointalk vào năm 2011 bởi một số nhà phát triển trong cộng đồng Bitcoin như QuantumMechanic. Mục tiêu ban đầu của PoS là làm giảm thiểu tiêu tốn năng lượng do khai thác PoW và tạo ra một hệ thống đồng thuận không phụ thuộc vào sức mạnh tính toán. Tuy nhiên, vào thời điểm đó, ý tưởng này chỉ mới ở mức lý thuyết và chưa được triển khai thực tế. Lần đầu tiên PoS được áp dụng trong mạng blockchain Peercoin (PPC). Đây là mạng blockchain do Sunny King và Scott Nadal phát triển lần năm 2012. Peercoin sử dụng một cơ chế hybrid (kết hợp) giữa PoW và PoS để đảm bảo bảo mật ban đầu và dần chuyển sang PoS hoàn toàn. Năm 2014 mạng blockchain Blackcoin ra đời và là blockchain đầu tiên chuyển hoàn toàn sang PoS mà không sử dụng PoW sau khối khởi tạo (genesis block). Giai đoạn 2015-2018 sự ra đời của mạng

blockchain Ethereum do Vitalik Buterin phát triển. Năm 2015, Ethereum ra mắt như một blockchain PoW nhưng đã lên kế hoạch chuyển đổi sang PoS ngay từ những phiên bản đầu tiên. Năm 2017, Ethereum giới thiệu kế hoạch nâng cấp Casper, một thuật toán PoS nhằm thay thế cơ chế PoW trong mạng Ethereum và cũng trong năm 2017 ra đời của mạng blockchain Cardano, Cardano được phát triển bởi Charles Hoskinson, người đồng sáng lập Ethereum. Đây là mạng blockchain sử dụng PoS ngay từ đầu với thuật toán đồng thuận Ouroboros, được thiết kế để tăng cường bảo mật và hiệu suất mà vẫn tiết kiệm năng lượng. Năm 2022 mạng Ethereum chính thức chuyển hoàn toàn từ PoW sang PoS với sự kiện "The Merge". Đây là cột mốc quan trọng, biến Ethereum trở thành mạng PoS lớn nhất thế giới. Với việc chuyển sang PoS đã làm giảm hơn 99% lượng năng lượng tiêu thụ của mạng lưới. Mở đường cho các nâng cấp khác như sharding để tăng khả năng mở rộng. Giải đoạn 2020 đến nay là giai đoạn bùng nổ của các blockchain PoS hiện đại. Các blockchain mới như Polkadot, Tezos, Solana, Avalanche đã áp dụng các biến thể của PoS ngay từ đầu, mang lại tốc độ xử lý nhanh và phí giao dịch thấp. Các nền tảng PoS hiện đại kết hợp các tính năng như Bằng chứng cổ phần được ủy quyền (Delegated Proof of Stake - DPoS), Bằng chứng lịch sử (Proof of History - PoH) để tăng hiệu suất mà vẫn đảm bảo tính phi tập trung và bảo mật.

4.4.2. Cơ chế hoạt động của PoS

Bước 1: Đặt cọc tài sản (Staking)

Người dùng muốn trở thành validator phải đặt cọc một số lượng coin nhất định vào mạng blockchain. Số coin này đóng vai trò như một cam kết và "thế chấp" để tham gia quá trình xác thực.

Tùy vào mạng lưới, số lượng coin đặt cọc yêu cầu có thể khác nhau (ví dụ: Ethereum 2.0 yêu cầu 32 ETH).

Bước 2: Chọn người xác thực khối (Validator Selection)

Hệ thống chọn validator để xác thực khối mới dựa trên các tiêu chí sau:

- Số lượng coin đặt cọc: Validator có nhiều coin đặt cọc hơn có xác suất được chọn cao hơn.
- Thời gian đặt cọc: Validator đặt cọc càng lâu có khả năng được chọn càng lớn.
- Ngẫu nhiên hóa: Một số giao thức PoS áp dụng yếu tố ngẫu nhiên để đảm bảo tính công bằng trong việc lựa chọn.

Bước 3: Xác thực giao dịch và tạo khối (Block Creation)

Validator được chọn sẽ xác minh các giao dịch trong khối mới và đảm bảo rằng tất cả các giao dịch hợp lệ, không vi phạm quy tắc mạng lưới (ví dụ: không có giao dịch chi tiêu hai lần). Nếu tất cả các điều kiện đều hợp lệ, validator sẽ thêm khối mới vào blockchain và phát broadcast khối đó đến các nút khác trong mạng.

Bước 4: Xác nhận và đồng thuận (Consensus Verification)

Các nút khác trong mạng sẽ kiểm tra và xác nhận khối mới. Nếu khối được xác nhận là hợp lệ, khối sẽ được thêm vào blockchain chính thức.

Bước 5: Nhận phần thưởng và phí giao dịch (Reward Distribution)

Validator tạo khối thành công sẽ nhận được phần thưởng là tổng phí giao dịch từ các giao dịch trong khối va tùy vào giao thức, validator có thể nhận thêm coin mới sinh ra.

Bước 6: Cơ chế phạt (Slashing)

Nếu một validator cố tình tạo khối sai hoặc gửi dữ liệu không hợp lệ, họ sẽ bị phạt thông qua cơ chế slashing. Validator tạo khối sai hoặc gửi dữ liệu không hợp lệ sẽ mất một phần hoặc toàn bộ số coin đặt cọc, có thể bị loại khỏi quá trình tham gia xác thực trong một khoảng thời gian. Điều này giúp đảm bảo rằng các validator sẽ luôn hành xử trung thực để tránh mất tài sản.

4.4.3. Cơ chế đồng thuận của mạng Cardano

Cardano là một nền tảng blockchain công khai được xây dựng dựa trên nghiên cứu học thuật và phương pháp luận khoa học. Nó được tạo ra để giải quyết các hạn chế của Bitcoin và Ethereum 1.0 về khả năng mở rộng, khả năng tương tác và tính bền vững. Cardano được Charles Hoskinson bắt đầu phát triển vào năm 2015, ông là một trong những người đồng sáng lập của Ethereum. Công nghệ cốt lõi của Cardano là sử dụng giao thức đồng thuận PoS tiên tiến được gọi là Ouroboros và được công bố năm 2017. Nó được phát triển bằng ngôn ngữ lập trình Haskell, một ngôn ngữ lập trình cho phép Cardano đạt được tính bảo mật và ổn định cao. Ouroboros là tên một biểu tượng cổ đại một con rắn tự ăn đuôi của chính nó, tượng trưng cho sự tái tạo và tuần hoàn vĩnh cửu. Cơ chế đồng thuận Ouroboros cho phép mạng Cardano đạt được sự đồng thuận một cách an toàn và hiệu quả về trạng thái của sổ cái phân tán. Ouroboros đã được phát triển qua 5 phiên bản.

- Phiên bản thứ nhất (Ouroboros Classic): Đây là phiên bản đầu tiên của Ouroboros, được công bố vào năm 2017. Nó là một trong những thuật toán PoS đầu tiên được nghiên cứu và chứng minh lý thuyết về tính bảo mật và khả năng phân tán. Ouroboros Classic thiết lập cơ chế đồng thuận bằng cách chia mạng thành các chu kỳ thời gian (epochs) và các slot nhỏ hơn (slots), trong đó các "slot leaders" được chọn ngẫu nhiên từ những người sở hữu cổ phần ADA (stakeholders). Ouroboros Classic mở rộng khả năng của blockchain mà không cần đến PoW, tiết kiệm năng lượng.

- Phiên bản thứ 2 (Ouroboros Praos): Phiên bản này được phát triển như một bản nâng cấp của Ouroboros Classic và được công bố vào năm 2018. Ouroboros Praos cải thiện tính bảo mật của hệ thống bằng cách sử dụng một mô hình ngẫu nhiên khởi tạo trong mỗi chu kỳ thời gian (epoch). Các slot leaders được chọn không chỉ dựa trên cổ phần mà còn theo một yếu tố ngẫu nhiên thêm, giúp hệ thống trở nên bảo mật hơn đối với các cuộc tấn công mạng. Ouroboros Praos cải thiện tính bảo mật và khả năng chống lại các cuộc tấn công Sybil và các mối đe dọa từ các kẻ tấn công với nhiều cổ phần.

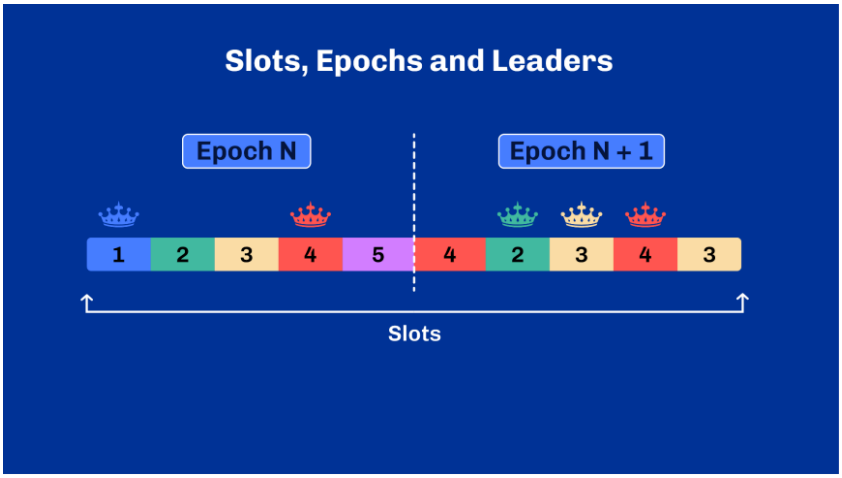
- Phiên bản thứ 3 (Ouroboros BFT (Byzantine Fault Tolerant)): Phiên bản này được ra mắt vào năm 2019 và là một cải tiến quan trọng của Ouroboros Praos, nhằm tăng cường khả năng kháng lỗi và nâng cao hiệu suất. Ouroboros BFT áp dụng các kỹ thuật Byzantine Fault Tolerance (BFT), giúp hệ thống duy trì sự đồng thuận ngay cả khi có sự hiện diện của một số nút không trung thực hoặc không hoạt động. Điều này cho phép mạng vẫn tiếp tục hoạt động bình thường ngay cả khi một số nút bị lỗi hoặc bị tấn công. Ouroboros BFT bảo mật cao hơn, khả năng phục hồi lỗi mạnh mẽ, và giảm thiểu thời gian hoàn thành các giao dịch.

Phiên bản thứ 4 (Ouroboros Omega): Đây là phiên bản tiếp theo, được nghiên cứu và phát triển sau Ouroboros BFT, với mục tiêu tối ưu hóa tính bảo mật và khả năng mở rộng hơn nữa. Ouroboros Omega được thiết kế để tăng cường khả năng mở rộng của Cardano, đặc biệt là trong các trường hợp sử dụng quy mô lớn. Phiên bản này có thể hỗ trợ các mạng lưới lớn hơn mà vẫn duy trì hiệu quả trong việc đồng thuận và tiết kiệm năng lượng. Ouroboros Omega tối ưu hóa tính bảo mật và khả năng mở rộng, giúp Cardano có thể xử lý các giao dịch với tần suất cao mà không làm giảm hiệu suất.

Phiên bản thứ 5 (Ouroboros Chronos): Là phiên bản tiếp theo của Ouroboros Omega, với một số thay đổi và cải tiến nhỏ nhưng quan trọng. Ouroboros Chronos tập trung vào việc cải thiện khả năng mở rộng và đồng thuận trong các tình huống sử dụng thực tế, đồng thời duy trì tính bảo mật của mạng.

4.4.3.1. Một số khái niệm chính của Ouroboros

- **Epoch (Kỷ nguyên):** Thời gian được chia thành các epoch, mỗi epoch kéo dài một khoảng thời gian nhất định, trong mạng Cardano là 5 ngày.
- **Slot (Khe thời gian):** Mỗi epoch được chia thành các slot ngắn hơn. Trong mạng Cardano mỗi slot là một giây, như vậy trong một Epoch sẽ có 432.000 slots.
- **Slot leader (Người đứng đầu khe thời gian):** Trong mỗi slot, một nút mạng i được chọn ngẫu nhiên với xác xuất $p_i = \frac{s_i}{\sum_{j=1}^{n} s_j}$ để trở thành slot leader. Slot leader có trách nhiệm (quyền) tạo ra một khối mới. Trong đó n là số nút trong mạng, s_i số ADA mà nút mạng thứ i stake.



Hình 4.3. Minh họa các khái niệm epoch, slot, Slot leader

- **Stake (Cổ phần):** Các chủ sở hữu ADA có thể "stake" (đặt cược) token của họ để tham gia vào quá trình đồng thuận. Khả năng một nút được chọn làm slot leader tỷ lệ thuận với số lượng ADA mà nó đã stake hoặc được ủy quyền stake.

4.4.3.2. Cách Ouroboros hoạt động

Bước 1. Stake pool (Nhóm cổ phần): Người dùng có thể stake ADA của họ trực tiếp hoặc ủy quyền cho các stake pool. Stake pool là các nút vận hành bởi các nhà điều hành pool, họ chịu trách nhiệm duy trì hoạt động của nút và nhận phần thưởng thay mặt cho những người ủy quyền.

Bước 2. Lựa chọn slot leader: Vào đầu mỗi epoch, một quá trình lựa chọn ngẫu nhiên diễn ra để xác định slot leader cho mỗi slot trong epoch đó. Xác suất một node được chọn phụ thuộc vào tổng số ADA được stake cho node đó hoặc stake pool mà nó vận hành.

Bước 3. Tạo khối: Slot leader được chọn có quyền tạo một khối mới trong slot của mình. Khối này chứa các giao dịch đã được xác minh. Một giao dịch Cardano bao gồm các thành phần sau:

Đầu vào (Inputs): Bao gồm các UTXO hiện có mà người gửi muốn chi tiêu. Mỗi đầu vào chỉ định một UTXO cụ thể từ các giao dịch trước đó.

Đầu ra (Outputs): Bao gồm các UTXO mới được tạo ra bởi giao dịch. Mỗi đầu ra chỉ định một địa chỉ nhận và một giá trị ADA được chuyển đến địa chỉ đó. Ngoài ra, nó có thể chứa data script.

Phí giao dịch (Transaction Fee): Một khoản phí nhỏ được trả cho mạng để xử lý giao dịch. Phí này được tính toán dựa trên kích thước của giao dịch và độ tắc nghẽn của mạng.

Chữ ký (Witness): Chữ ký số của người gửi được sử dụng để xác minh tính hợp lệ của giao dịch và đảm bảo rằng chỉ người sở hữu khóa riêng tư tương ứng mới có thể chi tiêu các UTXO đầu vào.

Bước 4. Xác nhận khối và động thuận: Slot leader phát tán khối mới được tạo tới các nút trong mạng. Các nút trong mạng xác minh tính hợp lệ của khối được tạo bởi slot leader.

Một giao dịch hợp lệ trong Cardano là giao dịch đáp ứng các điều kiện sau:

Tính hợp lệ của đầu vào: Tất cả các UTXO đầu vào phải tồn tại và chưa được chi tiêu. Người gửi phải chứng minh quyền sở hữu của mình đối với các UTXO này bằng cách cung cấp chữ ký số hợp lệ.

Tính hợp lệ của đầu ra: Tổng giá trị của các đầu ra cộng với phí giao dịch phải nhỏ hơn hoặc bằng tổng giá trị của các đầu vào. Điều này đảm bảo rằng không có ADA mới được tạo ra từ không khí.

Kiểm tra Script (nếu có): Nếu bất kỳ UTXO đầu ra nào chứa data script, script đó phải được thực thi thành công. Điều này đảm bảo rằng các điều kiện được quy định trong script được đáp ứng.

Chữ ký hợp lệ: Tất cả các chữ ký được cung cấp phải hợp lệ và tương ứng với các khóa riêng tư của người gửi.

Kiểm tra Tuân thủ Giao thức: Nút kiểm tra xem khối có tuân thủ các quy tắc của giao thức Ouroboros hay không, ví dụ như: số lượng giao dịch tối đa trong một khối, kích thước khối tối đa, thông tin metadata của khối.

Đồng thuận: Nếu khối vượt qua tất cả các kiểm tra trên, nút sẽ coi nó là hợp lệ và thêm nó vào bản sao cục bộ của blockchain. Quá trình này được lặp lại bởi tất cả các nút trong mạng, tạo ra sự đồng thuận về trạng thái của blockchain.

Sau khi được xác thực bởi phần lớn các nút, khối mới sẽ được chính thức thêm vào blockchain, kéo dài chuỗi và ghi lại vĩnh viễn các giao dịch trong khối đó.

Bước 5. Nhận phần thưởng: Các slot leader và các stake pool nhận được phần thưởng ADA cho việc tạo và xác nhận khối. Phần thưởng này được chia sẻ với những người đã ủy quyền stake cho pool.

4.4.4. Ưu nhược điểm của của PoS

4.4.4.1. Ưu điểm của PoS

- Tiết kiệm năng lượng: Một trong những ưu điểm lớn nhất của PoS là nó tiêu tốn ít năng lượng hơn so với PoW. PoW yêu cầu các thợ đào giải các bài toán tính toán phức tạp, tiêu tốn năng lượng rất lớn. Ngược lại, PoS không yêu cầu tính toán phức tạp mà thay vào đó, lựa chọn người tạo khối (validator) dựa trên cổ phần

họ nắm giữ. Điều này làm cho PoS trở thành một lựa chọn bền vững và thân thiện với môi trường.

- Khả năng mở rộng cao: PoS có thể xử lý giao dịch nhanh hơn và hiệu quả hơn khi số lượng người tham gia tăng lên, do không yêu cầu các bài toán tính toán phức tạp. Điều này giúp cải thiện khả năng mở rộng của blockchain, làm cho PoS trở thành một lựa chọn tốt cho các mạng lưới blockchain với khối lượng giao dịch lớn.

- Chi phí thấp: Việc không cần đến phần cứng mạnh mẽ như trong PoW giúp giảm chi phí tham gia mạng cho các validator. Điều này khiến PoS dễ tiếp cận hơn đối với nhiều người tham gia và có thể làm giảm sự tập trung vào một nhóm nhỏ các thợ đào hoặc nhà đầu tư.

- An toàn và bảo mật: PoS có cơ chế bảo mật mạnh mẽ, vì các validator cần đặt cược tài sản của mình (stake) để tham gia vào việc tạo khối và xác minh giao dịch. Nếu validator hành động không trung thực, họ sẽ mất một phần hoặc toàn bộ tài sản đã đặt cược. Điều này giúp giảm thiểu các cuộc tấn công vào mạng, vì chi phí tấn công mạng PoS sẽ tốn kém và khó thực hiện.

- Khả năng kháng tấn công 51%: Trong PoS, để chiếm ưu thế trong mạng và thực hiện một cuộc tấn công 51% (tức là kiểm soát hơn 50% sức mạnh đồng thuận), kẻ tấn công cần phải sở hữu hơn 50% tổng số cổ phần của mạng. Điều này cực kỳ khó thực hiện và đắt đỏ, đặc biệt trong các mạng lưới PoS lớn.

4.4.4.2. Nhược điểm của PoS

- Tập trung hóa (Centralization): Một trong những vấn đề lớn nhất của PoS là sự tập trung vào những người sở hữu nhiều cổ phần. Những người sở hữu lượng lớn token có nhiều cơ hội hơn để trở thành các validator và tạo ra khối, dẫn đến việc mạng có thể trở nên tập trung vào một số ít cá nhân hoặc tổ chức có tài sản lớn. Điều này có thể làm giảm tính phân quyền của mạng blockchain, mục tiêu chính của các hệ thống như Bitcoin.

- Người giàu càng giàu hơn: Trong PoS, những người sở hữu nhiều token có cơ hội cao hơn để kiếm phần thưởng từ việc xác minh giao dịch và tạo khối. Điều này có thể dẫn đến sự gia tăng sự giàu có của các nhà đầu tư lớn và làm giảm cơ hội cho những người tham gia nhỏ lẻ. Đây là một vấn đề tiềm ẩn trong việc duy trì sự công bằng trong mạng blockchain.

- Tính hgẫu nhiên và rủi ro lựa chọn Validator: Mặc dù PoS có cơ chế ngẫu nhiên để chọn các validator, nhưng việc lựa chọn người tạo khối dựa trên cổ phần có thể dẫn đến việc một số người tham gia không được lựa chọn trong một thời gian dài, điều này có thể làm giảm động lực tham gia. Hơn nữa, một số phương pháp lựa chọn validator có thể dẫn đến những quyết định không công bằng hoặc có sự thiên lệch.

- Cần lượng cổ phần lớn để tham gia: Để có cơ hội trở thành một validator và tạo ra khối, người tham gia cần phải có một lượng cổ phần đáng kể. Điều này có thể tạo ra một rào cản đối với những người mới tham gia hoặc những người có tài sản nhỏ hơn. Một số mạng PoS yêu cầu người tham gia phải đặt cược một số lượng

token lớn để tham gia vào quá trình đồng thuận, điều này có thể khiến cho mạng lưới bị hạn chế về số lượng người tham gia.

- Rủi ro phân mảnh và tấn công: PoS có thể đối mặt với các vấn đề về phân mảnh mạng, đặc biệt nếu không có đủ sự bổ công bằng về cổ phần. Nếu có quá ít validator hoặc nếu quá nhiều cổ phần được tập trung vào một số ít người, có thể gây ra các vấn đề về sự đồng thuận và hiệu quả của mạng. Hơn nữa, PoS cũng có thể gặp phải các cuộc tấn công Sybil, nơi kẻ tấn công tạo ra nhiều nút giả để tăng cổ phần của mình và có thể làm thay đổi quá trình đồng thuận.

4.5. CÁC BIẾN THỂ CỦA THUẬT TOÁN BẰNG CHỨNG CỔ PHẦN

4.5.1. Thuật toán Bằng chứng ủy quyền cổ phần (DPoS)

- Bằng chứng ủy quyền cổ phần (DPoS - Delegated Proof-of-Stake) là một biến thể của PoS trong đó người dùng ủy quyền quyền xác thực của mình cho một nhóm đại diện (Delegates). Các đại diện được lựa chọn thông qua cơ chế bỏ phiếu, với quyền biểu quyết tỷ lệ thuận với lượng coin mà người dùng nắm giữ. Một số mạng sử dung thuật toán này như là EOS, TRON, Tezos, …

4.5.1.1. Cơ chế hoạt động của DPoS

Bỏ phiếu: Những người nắm giữ token sử dụng cổ phần của họ để bỏ phiếu cho các đại biểu mà họ tin tưởng. Số lượng phiếu bầu của mỗi người tỷ lệ thuận với số lượng token mà họ nắm giữ.

Lựa chọn Đại biểu: Một số lượng nhất định các đại biểu được bầu chọn dựa trên số phiếu bầu mà họ nhận được. Số lượng này được xác định bởi giao thức của blockchain.

Xác thực và tạo khối: Các đại biểu được bầu chọn sẽ luân phiên nhau xác thực giao dịch và tạo ra các khối mới. Thứ tự này thường được xác định bởi một lịch trình được xác định trước hoặc một thuật toán ngẫu nhiên.

Phần thưởng: Các đại biểu nhận được phần thưởng cho việc tạo ra các khối mới. Phần thưởng này có thể được chia sẻ với những người đã bỏ phiếu cho họ, tùy thuộc vào cách giao thức được thiết lập.

4.5.1.2. Ưu điểm của DPoS

Khả năng mở rộng: DPoS có khả năng xử lý số lượng giao dịch lớn hơn so với PoS truyền thống do số lượng người xác thực được giới hạn.

Tốc độ giao dịch nhanh: Thời gian tạo khối thường nhanh hơn so với PoS, dẫn đến tốc độ giao dịch nhanh hơn.

Hiệu quả năng lượng: Tương tự như PoS, DPoS tiết kiệm năng lượng hơn so với Bằng chứng công việc (PoW) như Bitcoin.

4.5.1.3. Nhược điểm của DPoS

Tập trung hóa: Do số lượng đại biểu được giới hạn, DPoS có thể dẫn đến sự tập trung quyền lực vào một nhóm nhỏ người, làm giảm tính phi tập trung của blockchain.

Khả năng bị thao túng: Nếu một nhóm người nắm giữ một lượng lớn token có thể kiểm soát quá trình bầu chọn và bầu ra các đại biểu thân cận với họ, họ có thể thao túng mạng lưới.

4.5.2. Thuật toán Bằng chứng trọng số (PoWeight)

Bằng chứng về trọng số (Proof of Weight - PoWeight) là một cơ chế đồng thuận được sử dụng trong công nghệ blockchain để bảo mật mạng lưới và xác thực giao dịch. Không giống như PoW truyền thống, dựa trên việc giải các câu đố mật mã phức tạp, PoWeight dựa trên sự đồng thuận của nó vào số lượng "trọng lượng" hoặc cổ phần mà những người tham gia nắm giữ trong mạng lưới. Trọng lượng này thường tương quan với số lượng token hoặc tài sản do người tham gia kiểm soát, ảnh hưởng đến khả năng tạo khối mới và xác thực giao dịch của họ.

PoWeight được ra mắt vào năm 2017 như một thuật toán đồng thuận trên nền tảng blockchain Filecoin và là bản nâng cấp lớn của cơ chế PoS nhằm mục đích loại bỏ bản chất thiên vị của PoS. PoWeight không phải là một thuật toán đồng thuận duy nhất. Thay vào đó, nó là một thuật ngữ chung cho toàn bộ một loạt các thuật toán đồng thuận phần lớn dựa trên mô hình đồng thuận Algorand do các nhà nghiên cứu tại Phòng thí nghiệm Khoa học máy tính và Trí tuệ nhân tạo MIT phát triển, trong đó Algorand là một giao thức xác nhận giao dịch rất nhanh.

4.5.2.1. Cơ chế hoạt động của PoWeight

Xác định trọng số: Người tham gia được chỉ định trọng số dựa trên số lượng token hoặc tài sản họ nắm giữ và sẵn sàng khóa làm tài sản thế chấp. Người tham gia có trọng số càng lớn thì họ càng có nhiều ảnh hưởng trong mạng lưới.

Tạo và xác thực khối: Những người tham gia có trọng số đáng kể có thể đề xuất các khối mới để thêm vào blockchain. Cơ hội được chọn để tạo khối của họ tỷ lệ thuận với trọng số của họ. Những người tham gia mạng khác xác thực các khối được đề xuất. Vì quy trình này dựa trên trọng số chứ không phải công việc tính toán, nên nó tập trung vào việc xác minh tính hợp pháp dựa trên cổ phần của người tham gia.

Đạt được sự đồng thuận: Khi một khối được đề xuất và xác thực, nó sẽ được thêm vào blockchain nếu nó đáp ứng các quy tắc đồng thuận của mạng. Hệ thống đạt được sự đồng thuận dựa trên trọng số của những người tham gia vào quá trình tạo và xác thực khối.

Phần thưởng và khuyến khích: Những người tham gia tạo và xác thực khối thành công sẽ được thưởng token hoặc phí. Phần thưởng thường tỷ lệ thuận với trọng lượng họ nắm giữ, khuyến khích họ hành động trung thực và tham gia tích cực.

4.5.2.2. Ưu điểm của PoWeight

Khả năng mở rộng: Ưu điểm chính của cơ chế đồng thuận bằng chứng trọng số là nó có khả năng tùy chỉnh cao và có khả năng mở rộng cho nhiều người dùng.

Hệ thống Bằng chứng trọng số cho phép tạo ra các ủy ban bao gồm những người dùng mạng ngẫu nhiên được chỉ định 'trọng số' theo giao thức đồng thuận.

Bảo mật: PoWeight cũng cung cấp một số mức độ tập trung giúp duy trì mạng lưới phi tập trung toàn diện và an toàn.

Rủi ro phân nhánh: Cơ chế bằng chứng trọng số cố gắng đạt được sự đồng thuận mà không có bất kỳ rủi ro phân nhánh mới nào vì nó xem xét giá trị có trọng số tương đối dựa trên bất kỳ yếu tố có trọng số nào chứ không chỉ dựa trên số tiền mà nút nắm giữ.

Giảm mức tiêu thụ năng lượng: Không giống như PoW, đòi hỏi sức mạnh tính toán và năng lượng đáng kể, PoWeight dựa vào tiền cược thay vì các phép tính mở rộng, dẫn đến mức tiêu thụ năng lượng thấp hơn.

Chi phí vận hành thấp hơn: Với nhu cầu năng lượng và nhu cầu tính toán giảm, việc vận hành và duy trì mạng blockchain theo PoWeight thường tiết kiệm chi phí hơn.

Phần thưởng dựa trên cổ phần: Người tham gia được thưởng dựa trên số lượng trọng số hoặc cổ phần họ nắm giữ. Động lực tài chính này khuyến khích sự tham gia tích cực và trung thực, vì cá nhân có lợi ích kinh tế trực tiếp trong việc duy trì tính toàn vẹn của mạng lưới.

4.5.2.2. Một số nhược điểm của PoWeight

Thiết lập và quản lý: Việc triển khai PoWeight đòi hỏi phải thiết kế và quản lý cẩn thận việc phân phối tiền cược và tính toán trọng lượng. Điều này có thể phức tạp và có thể yêu cầu các hệ thống tinh vi để xử lý tiền cược và trọng lượng một cách chính xác.

Phân phối Token: Việc phân phối token hoặc tài sản ban đầu có thể ảnh hưởng đến tính công bằng của cơ chế đồng thuận. Nếu việc phân bổ ban đầu không đồng đều, có thể dẫn đến sự bất bình đẳng trong việc kiểm soát và ảnh hưởng của mạng lưới.

Rủi ro về Staking: Tính bảo mật của mạng phụ thuộc vào giá trị kinh tế của các stake do người tham gia nắm giữ. Trong trường hợp cực đoan, nếu một phần đáng kể stake của mạng bị xâm phạm hoặc bị đánh cắp, điều này có thể ảnh hưởng đến tính bảo mật của mạng.

Thách thức pháp lý: Bối cảnh pháp lý cho PoWeight và các cơ chế tương tự vẫn đang trong quá trình phát triển. Sự không chắc chắn về mặt pháp lý và các vấn đề tuân thủ có thể gây ra thách thức cho việc áp dụng và vận hành.

Tải mạng: Mặc dù PoWeight cải thiện khả năng mở rộng so với PoW, nhưng nó vẫn có thể gặp phải các vấn đề về khả năng mở rộng khi khối lượng giao dịch hoặc quy mô mạng cực lớn, tùy thuộc vào cách triển khai.

4.5.3 Một số thuật toán khác.

4.5.3.1. Thuật toán PoH

Bằng chứng lịch sử (PoH - Proof of History) là một cơ chế đồng thuận kết hợp với các thuật toán khác (thường là PoS) để tăng tốc độ xác nhận giao dịch trong mạng blockchain. PoH tạo ra một chuỗi thời gian mã hóa, cho phép các nút xác minh thứ tự các sự kiện (giao dịch) một cách độc lập mà không cần đồng bộ hóa thời gian với nhau, thời gian và thứ tự các giao dịch được ghi lại trước khi đưa vào khối. Một số mạng sử dung thuật toán này như là Solana một nền tảng blockchain hiệu suất cao, Pipelined blockchain.

PoH là một cơ chế đồng thuận được phát triển bởi Anatoly Yakovenko, người sáng lập Solana Labs. Ý tưởng cốt lõi của PoH là thứ tự của các sự kiện trong mạng Blockchain cũng quan trọng như chính các sự kiện đó, và khả năng chứng minh được thứ tự này là yếu tố cần thiết để duy trì tính toàn vẹn của mạng.

Để đạt được điều này, PoH sử dụng một Hàm trì hoãn có thể xác minh (Verifiable Delay Function - VDF) để tạo ra một dấu thời gian (timestamp) cho mỗi khối trong Blockchain. VDF được thiết kế để khó bị thao túng, nhờ tính "kháng trì hoãn" và "kháng bộ nhớ," khiến cho các kẻ tấn công không dễ dàng thao túng các dấu thời gian. Dấu thời gian do VDF tạo ra được tích hợp vào mỗi khối trên Blockchain, cung cấp một bản ghi thứ tự giao dịch bất biến và có thể xác minh được. Nhờ PoH, Solana đạt được khả năng chốt giao dịch nhanh (fast finality), nghĩa là khi một khối được thêm vào Blockchain, nó được xem như đã hoàn tất và không thể bị thay đổi.

PoH chủ yếu được sử dụng trong mạng Blockchain Solana, với thiết kế xử lý được hàng nghìn giao dịch mỗi giây. PoH giúp giảm thiểu yêu cầu về lưu trữ và băng thông để duy trì mạng Blockchain, đồng thời cải thiện hiệu quả và tốc độ của hệ thống, trong khi vẫn đảm bảo tính bảo mật và khả năng xác minh giao dịch.

Cách hoạt động của PoH

1. Ghi Dấu Thời Gian Mật Mã (Cryptographic Timestamping)

PoH sử dụng một hàm băm có tính liên tiếp và kháng tiền hình ảnh (pre-image resistant). Hàm băm này nhận một đầu vào (bao gồm trạng thái hiện tại của Blockchain và một seed ngẫu nhiên) và tạo ra một đầu ra duy nhất, không thể đảo ngược, gọi là hash. Hash này là dấu thời gian có thể xác minh được.

2. Tạo chuỗi hash (Generating a Hash Chain)

Solana tạo ra một chuỗi hash bằng cách áp dụng hàm băm liên tục lên đầu ra của hash trước đó. Mỗi bước trong chuỗi đại diện cho một "tick" (nhịp thời gian), với số lượng hash được tính toán biểu thị khoảng thời gian đã trôi qua. Kết quả là một bản ghi thời gian liên tục, có thể xác minh được, dùng để sắp xếp các giao dịch.

3. Ghi nhận giao dịch

Khi một giao dịch được thực hiện, nó được gắn với hash gần nhất trong chuỗi PoH. Các validator (người xác thực) kiểm tra tính hợp lệ và thời gian của giao dịch bằng cách đảm bảo rằng nó tham chiếu đến một hash trong chuỗi PoH hiện tại.

4. Đồng thuận

Các giao dịch được gắn dấu thời gian bởi PoH sau đó được xử lý thông qua cơ chế đồng thuận dựa trên Proof of Stake (PoS), cụ thể là Tower BFT trong mạng Solana. Các validator đặt cọc token SOL để tham gia, nhận phần thưởng khi bảo vệ mạng và xác nhận giao dịch. Nhờ sự hỗ trợ từ cơ chế ghi thời gian của PoH, Tower BFT đạt được đồng thuận nhanh chóng, cho phép Solana xử lý hàng nghìn giao dịch mỗi giây.

5. Hàm trì hoãn có thể xác minh (VDF)

VDF đảm bảo rằng các nhà sản xuất khối phải đi qua nó để có quyền tạo khối. Solana kết hợp hash của dữ liệu từ trạng thái đã được tạo trước đó trong chuỗi giao dịch, tạo ra dấu thời gian có thể xác minh được mà không thể tái tạo hoặc thay đổi.

Ưu điểm của PoH

- Khả năng mở rộng cao: PoH cho phép Solana xử lý hàng chục nghìn giao dịch mỗi giây.
- Độ trễ thấp: Thời gian chờ giao dịch được giảm thiểu đáng kể nhờ khả năng xác minh nhanh chóng.
- Bảo mật cao: Chuỗi hash liên tục đảm bảo rằng thứ tự giao dịch không thể bị thao túng.
- Hiệu quả năng lượng: Không yêu cầu các phép tính phức tạp hoặc tiêu tốn năng lượng như trong PoW.
- Loại bỏ đồng hồ tập trung: PoH tích hợp thời gian trực tiếp vào Blockchain, loại bỏ nhu cầu về một hệ thống đồng hồ tập trung.

Nhược điểm của PoH

- Yêu cầu phần cứng Cao: Do cần xử lý khối lượng lớn dữ liệu, các nút phải có phần cứng mạnh mẽ, có thể làm giảm tính phi tập trung.
- Tập trung hóa: Các yêu cầu về hiệu suất phần cứng có thể dẫn đến sự tập trung hóa trong số ít các node lớn.
- Phức tạp kỹ thuật: Việc triển khai PoH đòi hỏi sự tích hợp chặt chẽ giữa phần cứng và phần mềm, tăng độ phức tạp vận hành.

4.5.3.2. Thuật toán Bằng chứng thẩm quyền (PoA)

Bằng chứng thẩm quyền **(**Proof of Authority - PoA) là một thuật toán đồng thuận dựa trên uy tín, cung cấp giải pháp khả thi và hiệu quả cho các mạng lưới blockchain, đặc biệt là các mạng lưới blockchain riêng tư (private blockchain). Thuật ngữ này được đề xuất vào năm 2017 bởi Gavin Wood, đồng sáng lập và cựu CTO của Ethereum.

Thuật toán đồng thuận PoA tận dụng giá trị của danh tính, thay vì để các node xác thực đặt cược tiền mã hóa (như trong PoS), họ đặt cược uy tín của chính mình. Do đó, các blockchain PoA được bảo vệ bởi các node xác thực được chọn lựa cẩn thận và được xem là các thực thể đáng tin cậy.

Thuật toán đồng thuận PoA rất linh hoạt và được coi là một lựa chọn giá trị cho các ứng dụng trong lĩnh vực hậu cần. Đối với chuỗi cung ứng, chẳng hạn, PoA được xem là một giải pháp hiệu quả và hợp lý. Mô hình PoA cho phép các doanh nghiệp duy trì tính riêng tư của mình trong khi vẫn tận dụng được những lợi ích của công nghệ blockchain.

Microsoft Azure là một ví dụ khác về một công ty áp dụng PoA. Nền tảng Azure cung cấp các giải pháp cho các mạng riêng tư mà không yêu cầu một loại tiền tệ nội bộ, chẳng hạn như "gas" trong ether, vì quá trình khai thác là không cần thiết.

PoA là một hệ thống có khả năng mở rộng cao vì nó dựa vào số lượng nhỏ các validator. Hệ thống này được điều hành bởi những người tham gia đã được phê duyệt trước, chịu trách nhiệm xác minh các khối và giao dịch. Một số mạng sử dung thuật toán này như là Binance Smart Chain, VeChain, Microsoft Azure Blockchain, …

Cách hoạt động của PoA

PoA là một cơ chế đồng thuận dựa vào việc xác thực các giao dịch blockchain bởi các thực thể được ủy quyền. So với PoS, PoA được thiết kế để cung cấp một giải pháp mở rộng và hiệu quả hơn cho việc xây dựng các mạng blockchain riêng tư.

Xác thực dựa trên danh tính: Không giống như PoW và PoS phụ thuộc vào năng lực tính toán hoặc số lượng tiền đặt cọc, PoA sử dụng danh tính của các validator làm điều kiện xác thực chính. Đây là một cơ chế đồng thuận hiệu quả, nhấn mạnh vào sự tin cậy và công nhận danh tiếng.

Lựa chọn Validator: Validator hay "authority" phải có danh tính rõ ràng và được xác minh bởi toàn bộ mạng lưới. Khi nhận được đề xuất giao dịch mới, tất cả các validator sẽ độc lập xác minh giao dịch dựa trên các quy tắc của mạng. Nếu đa số đồng ý, giao dịch sẽ được thêm vào khối mới.

Xác thực khối: Một thuật toán đồng thuận như chọn ngẫu nhiên có trọng số hoặc vòng tuần tự được sử dụng để chọn validator tạo khối. Sau khi khối được tạo, nó sẽ được phát đến tất cả các node trong mạng. Các nút sẽ kiểm tra tính hợp lệ của khối, bao gồm các giao dịch và liên kết với khối trước đó. Khi đa số đồng thuận, khối sẽ được thêm vào blockchain.

Ưu điểm của PoA

- Hiệu quả: Không yêu cầu khai thác (mining) tiêu tốn năng lượng như PoW hay đặt cọc vốn lớn như PoS.
- Tốc độ: Quá trình xác thực nhanh, độ trễ thấp do danh sách validator cố định.

- Bảo mật: Danh tiếng và danh tính rõ ràng của validator giúp chống lại các cuộc tấn công Sybil và các hoạt động độc hại khác.
- Quản trị: Thích hợp cho các mạng blockchain riêng hoặc liên minh, nơi quản trị tập trung là cần thiết.
- Khả năng mở rộng: Dễ dàng mở rộng do không bị giới hạn bởi tài nguyên như PoW hoặc PoS.

Nhược điểm của PoA

- Tập trung hóa: Validator là những thực thể được chọn trước, dẫn đến lo ngại về khả năng cấu kết hoặc tập trung quyền lực.
- Giới hạn phân quyền: PoA không đạt mức độ phân quyền cao như PoW hay PoS.
- Rủi ro tấn công Validator: Nếu một thực thể độc hại kiểm soát được đa số validator, mạng có thể bị xâm phạm.

4.5.3.3. Thuật toán PoC

- Bằng chứng dung lượng (PoC - Proof of Capacity) là một thuật toán đồng thuận trong blockchain, dựa trên dung lượng lưu trữ ổ cứng thay vì sức mạnh tính toán hoặc tài sản đặt cọc. Trong PoC, người tham gia sử dụng dung lượng lưu trữ để khai thác và xác thực giao dịch. PoC còn được gọi là Bằng chứng không gian (Proof of Space) hoặc Bằng chứng lưu trữ (Proof of Storage). Một số mạng sử dung thuật toán này như là Burstcoin, Chia Network, Signum, …

Trong PoC, các thợ đào sử dụng dung lượng ổ cứng của họ để giải quyết các bài toán toán học và tạo ra các khối mới. Dung lượng lưu trữ càng lớn, cơ hội của thợ đào để tạo ra một khối mới càng cao. Khác với PoW, nơi các thợ đào phải giải quyết các bài toán toán học phức tạp, PoC sử dụng một thuật toán băm đơn giản hơn, yêu cầu ít năng lực tính toán hơn. Điều này giúp PoC dễ tiếp cận hơn với các thợ đào quy mô nhỏ, những người không có điều kiện sở hữu các thiết bị khai thác đắt tiền.

Những điểm chính của PoC:

1. Dung lượng lưu trữ

Trong PoC, dung lượng lưu trữ là tài nguyên quan trọng nhất. Thợ đào càng có nhiều không gian lưu trữ, họ càng có cơ hội cao hơn để tạo ra các khối mới. Tuy nhiên, điều này không có nghĩa là cần phải sở hữu dung lượng lớn để tham gia mạng lưới. Ngay cả với một dung lượng nhỏ, thợ đào vẫn có thể nhận được phần thưởng.

2. Quá trình "plotting"

Plotting là quá trình tính toán trước các hàm băm để tăng tốc độ khai thác. Thợ đào sử dụng không gian lưu trữ của mình để tạo ra các tệp plot chứa tất cả các hàm băm cần thiết cho việc khai thác. Các tệp này sau đó được sử dụng để khai thác các

khối mới. Quá trình plotting có thể mất nhiều thời gian và tài nguyên, nhưng một khi hoàn thành, việc khai thác sẽ trở nên nhanh chóng và hiệu quả hơn.

3. Khai thác (Mining)

Khai thác trong PoC liên quan đến việc đọc tệp plot và tìm kiếm câu trả lời chính xác cho bài toán toán học. Khi câu trả lời chính xác được tìm thấy, thợ đào có thể tạo ra một khối mới và nhận phần thưởng. Khai thác trong PoC tiêu tốn ít năng lượng hơn so với PoW, giúp nó trở thành một giải pháp bền vững hơn.

4. Phần thưởng

Các thợ đào trong PoC nhận được phần thưởng khi tạo ra các khối mới. Phần thưởng thường ở dạng tiền mã hóa. Số lượng phần thưởng phụ thuộc vào kích thước của khối và giá trị thị trường hiện tại của loại tiền mã hóa đó.

Ưu điểm của PoC:

- Bền vững và thân thiện với môi trường: PoC tiêu tốn ít năng lượng hơn, góp phần giảm tác động tiêu cực đến môi trường.
- Dễ tiếp cận: Không yêu cầu thiết bị khai thác đắt tiền, cho phép nhiều người tham gia hơn.
- Hỗ trợ thợ đào nhỏ: Ngay cả những người có dung lượng lưu trữ hạn chế cũng có thể tham gia và nhận phần thưởng.

PoC là một giải pháp thay thế bền vững và dễ tiếp cận hơn so với các thuật toán đồng thuận truyền thống. Bằng cách sử dụng dung lượng lưu trữ làm tài nguyên chính, PoC góp phần xây dựng một mạng lưới blockchain hiệu quả về năng lượng và thân thiện với môi trường. Khi ngành công nghiệp blockchain tiếp tục phát triển, chúng ta có thể kỳ vọng nhiều thuật toán đồng thuận sáng tạo như PoC sẽ ra đời.

4.6. Câu hỏi và bài tập

1 Thuật toán đồng thuận blockchain là gì, và vai trò của nó trong việc duy trì tính an toàn và ổn định của hệ thống phân tán?
2 Nêu các bước chính trong cơ chế hoạt động của một thuật toán đồng thuận blockchain.
3 Tại sao tính phi tập trung (decentralization) lại là yêu cầu quan trọng đối với một thuật toán đồng thuận?
4 Mô tả bài toán các vị tướng Byzantine và sự liên quan của nó đến hệ thống chịu lỗi Byzantine (BFT).
5 So sánh các ưu, nhược điểm của thuật toán Proof of Work (PoW) và Proof of Stake (PoS).
6 Giải thích cách hoạt động của thuật toán Proof of History (PoH) trong mạng Solana và vai trò của nó trong việc tăng tốc độ xử lý giao dịch.
7 Thuật toán Proof of Authority (PoA) hoạt động như thế nào, và tại sao nó phù hợp với các mạng blockchain riêng tư (private blockchain)?
8 Mô tả cơ chế chọn Slot Leader trong thuật toán Ouroboros của Cardano.

9 Thuật toán Proof of Capacity (PoC) giúp giảm tiêu thụ năng lượng như thế nào, và nó khác gì so với PoW?

10 Bằng chứng ủy quyền cổ phần (DPoS) giải quyết vấn đề tập trung hóa như thế nào so với PoS?

11 Hãy giải thích cách hệ thống chịu lỗi Byzantine (BFT) đảm bảo tính ổn định của mạng lưới blockchain ngay cả khi một số nút không trung thực.

12 Một thợ đào sử dụng thuật toán PoC có 5 TB dung lượng lưu trữ, trong khi người khác có 10 TB. Tính xác suất tương đối của mỗi người trong việc tạo khối mới.

13 Lập bảng so sánh ưu, nhược điểm của PoW, PoS và PoC. Đề xuất tình huống ứng dụng phù hợp cho từng thuật toán.

14 Mô phỏng cách tạo và xác thực khối bằng thuật toán PoW. Mô tả các bước từ tạo khối ứng viên đến xác nhận khối hợp lệ.

15 Nếu bạn phải xây dựng một blockchain cho một ứng dụng tài chính với yêu cầu cao về tốc độ và bảo mật, bạn sẽ chọn thuật toán nào trong số PoW, PoS, PoH hoặc PoA? Giải thích lý do.

Tài liệu tham khảo

[1] Andreas M. Antonopoulos, “Mastering Bitcoin”, Second edition, Oreilly (2017).

[2] Andreas M. Antonopoulos, Dr. Gavin Wood, “MasteringEthereum, Building Smart Contracts and DApps”, Oreilly (2019).

[3] The Byzantine Generals Problem, Leslie Lamport, Robert Shostak, and Marshall Pease, SRI International (1982).

[4] Markus Jakobsson, Proofs of work and bread pudding protocols (extended abstract), Information Sciences Research Center, Bell Labs, Murray Hili, New Jersey 07974, www.bell-Iabs.com/user (1999).

[5] Iddo Bentov, Charles Lee, Alex Mizrahi, and Meni Rosenfeld. Proof of activity: Extending bitcoin’s proof of work via proof of stake [extended abstract]y. SIGMETRICS Performance Evaluation Review, 42(3):34–37, 2014

[6] Aggelos Kiayias, Alexander Russell, Bernardo David, Roman Oliynykov, Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol, July 20, 2019

[7] https://www.lcx.com/proof-of-authority-explained/

[8] https://academy.cardanofoundation.org/cbca

[9] https://ocw.mit.edu/courses/15-s12-blockchain-and-money-fall-018/pages/lecture-slides/

[10] https://iohk.io/en/research/library/papers/ouroboros-a-provably-secure-proof-of-stake-blockchain-protocol/