TRƯỜNG ĐẠI HỌC MỎ ĐỊA CHẤT

KHOA CÔNG NGHỆ THÔNG TIN

----------o0o----------

BÁO CÁO SINH HOẠT HỌC THUẬT

Đề tài: Cơ chế đồng thuận trong Blockchain.

Người báo cáo : Nguyễn Thu Hằng

Đơn vị : Bộ môn Tin học Kinh tế

Hà Nội, 12/ 2022

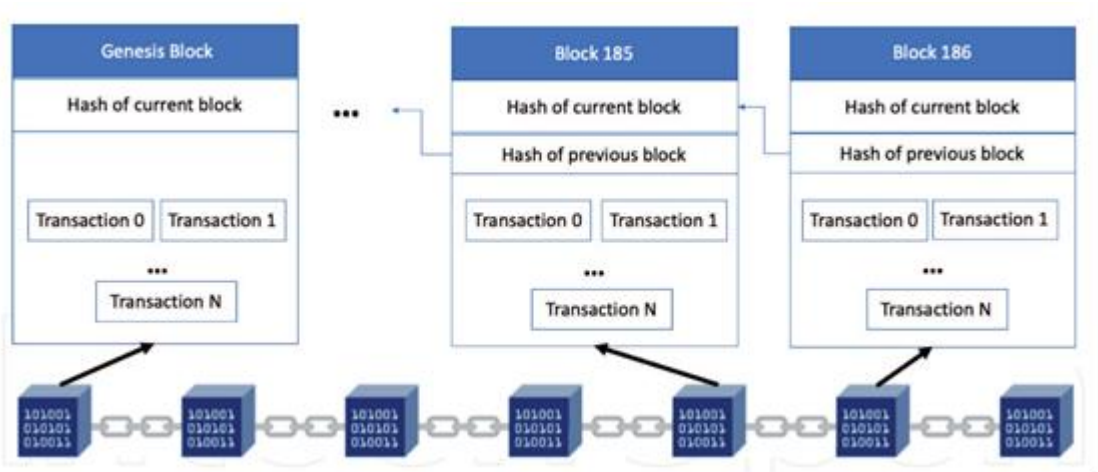
MỤC LỤC

1 BLOCKCHAIN

1.1 Khái niệm:

Thế giới đang trở nên ngày càng hiện đại, sự phát triển của khoa học đã làm thay đổi căn bản nền sản xuất thế giới. Cách mạng công nghiệp 4.0 xảy ra đã mang đến tác động to lớn cho sự phát triển của khoa học công nghệ tác động lên hệ thống chính trị thế giới, cùng với các công nghệ tự động hóa, trí tuệ nhân tạo. Công nghệ chuỗi khối cũng đã góp phần quan trọng xây dựng nền kinh tế số và được dự đoán sẽ dẫn dắt công nghệ tương lai.

Blockchain là một cơ sở dữ liệu phân cấp lưu trữ thông tin trong các khối (block) được liên kết với nhau bằng mã hóa và mở rộng theo thời gian để tạo thành một chuỗi (chain). Mỗi khối trong Blockchain sẽ được liên kết với khối trước đó, chứa thông tin về thời gian khởi tạo khối đó kèm một mã thời gian và dữ liệu giao dịch.



Hình 1-1: Kiến trúc của chuỗi dữ liệu trong mạng Blockchain [1]

Blockchain là một hệ thống cơ sở dữ liệu duy nhất được tạo ra, sao chép, đồng bộ hóa và duy trì bởi tất cả những người tham gia trong mạng phi tập trung. Blockchain hoạt động trong một mạng ngang hàng phi tập trung để xác thực và lưu trữ tất cả các giao dịch theo sự đồng thuận được tất cả các nút trong mạng đồng ý, không có bất kỳ cơ quan trung ương nào xác thực giao dịch (như với một bên trung gian [1]. Tất cả các giao dịch đã hoàn thành và được xác thực đều được ghi vào sổ cái phân tán theo cách có thể xác minh, an toàn, minh bạch và vĩnh viễn cùng với mốc thời gian và các chi tiết

[1] https://www.blockchain-council.org/

khác [2]. Do đó, việc trao đổi dữ liệu, tài sản hữu hình và vô hình giữa những người tham gia được ghi lại bằng kỹ thuật số. Mỗi bên liên quan sẽ lưu trữ một bản sao của sổ cái được đồng bộ hóa, giúp ngăn chặn một điểm lỗi trong hệ thống hoặc mất dữ liệu [3].

Hiểu đơn giản, Blockchain có thể được xem là một cuốn sổ cái điện tử được phân phối trên nhiều máy tính khác nhau, lưu trữ mọi thông tin giao dịch và đảm bảo các thông tin đó không thể bị thay đổi dưới bất kỳ hình thức nào.

Mọi thông tin được lưu trên cuốn sổ cái đó sẽ được xác nhận bởi hàng loạt máy tính được kết nối trong một mạng lưới chung. Sẽ không một cỗ máy nào có khả năng thay đổi, viết đè lên hay xóa dữ liệu trong cuốn sổ cái đó.

1.2 Cấu trúc của mỗi Block (Khối)

Mỗi block bao gồm 3 thành phần: Dữ liệu (Data), Mã hàm băm (Hash) và mã Hash của khối trước nó.

✓ Data: Các bản ghi dữ liệu đã được xác thực của các nút được bảo vệ bằng thuật toán mã hóa tùy thuộc vào từng blockchain.

✓ Hash: Mã hàm băm của của Block. Đây là chuỗi các ký tự và số được tạo một cách ngẫu nhiên và không giống nhau. Nó đại diện riêng cho block đó và được mã hoá bằng thuật toán mã hoá. Mã hash dùng để phát hiện sự thay đổi trong các khối.

✓ Previous Hash: Mã hàm băm của block trước đó. Nó dùng để các khối liền kề nhận biết khối nào trước, khối nào sau và nối với nhau.

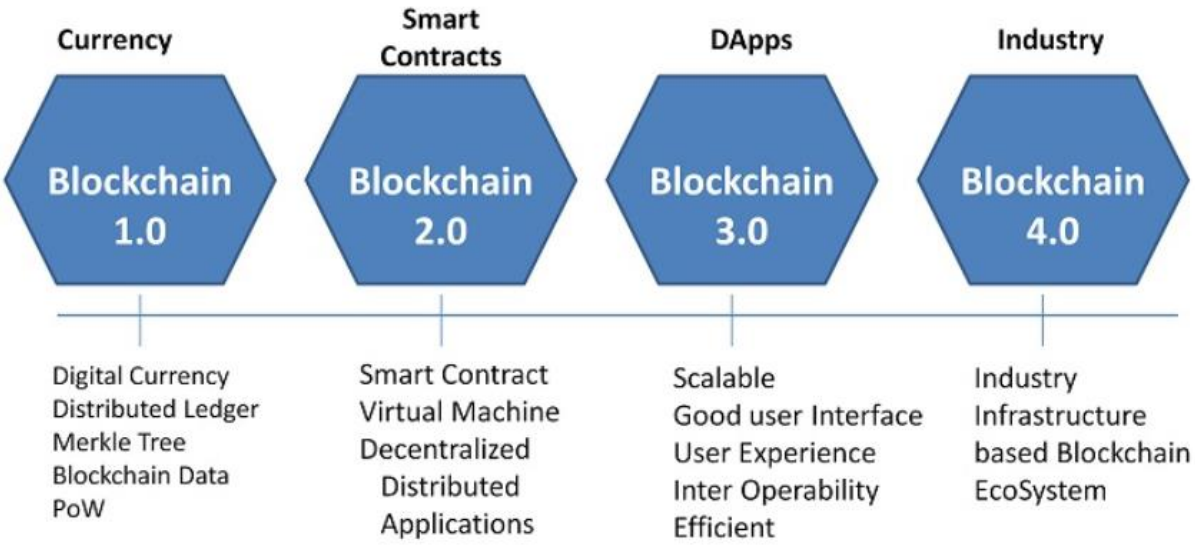
1.3 Các phiên bản công nghệ Blockchain

Công nghệ Blockchain trải qua 4 giai đoạn như hình Hình 1-2.

❖ Công nghệ Blockchain 1.0 - Tiền tệ

Đây là phiên bản đầu tiên của công nghệ blockchain. Nhờ áp dụng công nghệ sổ cái phân tán phi tập trung (Distributed Ledger Technology) mà các giao dịch được diễn ra trên Blockchain được xử lí nhanh chóng và minh bạch.

Ví dụ tiêu biểu cho phiên bản Blockchain 1.0 là Bitcoin, đồng tiền điện tử đầu tiên trên thế giới và đặt nền móng cho sự phát triển của thị trường Crypto.



Hình 1-2: Các phiên bản công nghệ Blockchain

❖ Công nghệ Blockchain 2.0 - Hợp đồng thông minh

Đây là phiên bản thứ 2 của công nghệ blockchain. Với hợp đồng thông minh (hay Smart Contract), giao dịch trên Blockchain sẽ được giảm mạnh các chi phí xác thực, chống gian lận, vận hành, đồng thời tăng tính minh bạch.

Phiên bản này loại bỏ hoàn toàn các yếu tố cảm tính hay đạo đức thường gặp khi làm việc với con người, ví dụ điển hình là Ethereum.

❖ Công nghệ Blockchain 3.0 - Ứng dụng phi tập trung

Ứng dụng phi tập trung (DApp - Decentralized Application) là các phần mềm được triển khai độc lập, không nằm trên một máy chủ duy nhất mà lưu trữ một cách phân tán trên các kho lưu trữ phi tập trung và có thể được viết bằng bất kỳ ngôn ngữ nào.

Hầu hết mã nguồn của Dapp đều chạy trên các mạng lưới ngang hàng (Peer-to-Peer), điều này ngược lại so với các ứng dụng truyền thống và chỉ chạy trên một hệ thống tập trung duy nhất.

❖ Công nghệ Blockchain 4.0 - Ứng dụng vào thực tiễn

Công nghệ Blockchain 4.0 là phiên bản Blockchain mới nhất hiện nay. Phiên bản này sẽ áp dụng tất cả những ứng dụng từ phiên 1 đến 3 vào nhiều lĩnh vực khác nhau trên thực tiễn:

✓ Ứng dụng trong sản xuất: Khi ứng dụng Blockchain vào sản xuất, Blockchain sẽ thay thế các thiết bị thông minh để cấp quyền quản lý hiệu quả, bao gồm: dõi quá trình tạo ra sản phẩm, quản lý thông tin giao dịch, chất lượng sản phẩm, vận chuyển và phân phối nó tới tay người dùng cuối,... nhằm gia tăng đáng kể năng suất cho các quy trình **quản lý chuỗi công ứng**. Đối với người tiêu dùng, họ có thể truy xuất ngược trở lại về lịch sử hình thành, vận chuyển của sản phẩm, để kiểm tra thông tin sản phẩm đó có phải hàng chính hãng hay không, từ đó tránh được những sản phẩm nhái, hàng giả trên thị trường.

✓ Ứng dụng Blockchain trong thương mại điện tử: Các vấn đề lớn nhất trong lĩnh vực thương mại điện tử là tính bảo mật, quản lý chuỗi cung ứng và quá trình vận chuyển hàng hoá đến người tiêu dùng, tạo nên nhiều rào cản giữa người tiêu dùng và nhà sản xuất. Tuy nhiên, Blockchain đã giúp giải quyết vấn đề đó bằng các hợp đồng thông minh (smart contract), tạo điều kiện cho các bên ký kết dễ dàng, tiết kiệm được chi phí nhờ lược bỏ được trung gian khi liên kết với các doanh nghiệp đa quốc gia.

✓ Ứng dụng của Blockchain trong y tế: Y tế là một lĩnh vực khá nhạy cảm với các số liệu, khi mà số liệu luôn có khoảng dao động được kiểm soát một cách chặt chẽ. Khi ứng dụng Blockchain trong y tế, tất cả các bên được ủy quyền đều có thể truy cập cùng một thông tin chính xác và được xác minh trong vài giây. Bệnh nhân có quyền kiểm soát dữ liệu của họ mọi lúc và có thể cấp cho người khác quyền truy cập theo yêu cầu, giảm nguy cơ bị lạm dụng và trộm cắp.

✓ Blockchain trong giáo dục: Ứng dụng Blockchain trong giáo dục giúp lưu trữ các dữ liệu về bảng điểm, quá trình đào tạo, kinh nghiệm giảng dạy & lịch sử của từng cá nhân, từ đó sẽ tránh được việc gian lận khi xin cấp học học bổng, thăng chức, hoặc khai gian về trình độ học vấn hay kinh nghiệm làm việc. Ngoài ra, với tính chất của hợp đồng thông minh, Blockchain còn cho phép tự động thực thi các điều khoản trong quy chế đào tạo và xử lý các trường hợp vi phạm,…Từ 30/06/2021, Bộ Giáo dục và Đào tạo đã chính thức vận hành **Hệ thống Tra cứu thông tin văn bằng chứng chỉ trên**

Blockchain do **TomoChain** bàn giao. Đây được xem là cột mốc đánh dấu cho sự công nhận của nhà nước đối với công nghệ Blockchain nói riêng và tiền điện tử nói chung.

✓ Ứng dụng của Blockchain trong nông nghiệp: Hiện nay, vấn đề về nguồn gốc xuất xứ và chất lượng được đặt lên hàng đầu trong lĩnh vực nông nghiệp. Việc ứng dụng Blockchain trong nông nghiệp với hệ thống sổ cái phân tán sẽ giúp các nhà bán lẻ và người tiêu dùng lưu trữ các thông tin giao dịch, quá trình lưu chuyển của sản phẩm từ nơi sản xuất đến các nhà bán lẻ và người dùng cuối. Bên cạnh đó, các dữ liệu trong suốt quá trình sản xuất và bán hàng cũng được lưu trữ và cập nhật liên tục trong Blockchain như quản lý chất lượng, quản lý tài chính, quản lý giá cả… Điều này giúp tăng tính minh bạch của sản phẩm và tạo được lòng tin của người tiêu dung.

✓ Ứng dụng Blockchain trong Ngân hàng & thanh toán: Như mình đã đề cập ở đầu bài viết, nhược điểm lớn nhất khi giao dịch trên ngân hàng là nguy cơ dữ liệu bị đe dọa, phí giao dịch và tồn tại trung gian thứ 3. Tính bảo mật và hợp đồng thông minh của Blockchain sẽ giúp bỏ qua trung gian thứ 3 và hạn chế các rủi ro về bảo mật cho khách hàng. Mọi người có thể truy cập và chuyển coin cho nhau ở bất kỳ đâu trên thế giới và với tốc độ tương đối nhanh và chi phí thấp. Việc này giúp cho người dân ở các quốc gia không có điều kiện tiếp cận với hệ thống ngân hàng cũng có thể giao dịch, chuyển tiền cho nhau.

Ngoài ra, Blockchain còn được ứng dụng vào nhiều lĩnh vực khác như: IoT - Internet of Things, Decentralized Storage, Từ thiện, Giải trí…

2 CƠ CHẾ ĐỒNG THUẬN (CONSENSUS MECHANISM)

2.1 Thuật toán đồng thuận Blockchain

Thuật toán blockchain là một phần quan trọng không thể thiếu của blockchain. Không chỉ đóng vai trò giữ bảo mật mạng lưới, các thuật toán này còn giúp các blockchain đảm bảo sự phi tập trung trong các hoạt động.

Thuật toán đồng thuật của blockchain là cơ chế đảm bảo các giao dịch được tạo ra trên blockchain là đúng đắn, trung thực và minh bạch. Về bản chất, blockchain bao gồm nhiều node kết hợp lại tạo ra một mạng lưới. Để một giao dịch được ghi lại trên blockchain, nó phải được đồng ý đồng thời bởi tất cả các node trên mạng lưới.

Thuật toán đồng thuận Blockchain là sự đồng ý xác thực thông tin trong bản ghi là chính xác của đa số các nút ở trong mạng lưới và cho phép ghi lại thông tin giao dịch vào trong Blockchain.

Nếu có sự thay đổi của một block trong mạng lưới. Dữ liệu này được so sánh với các dữ liệu của các khối khác. Nếu có sự khác biệt thì nó sẽ không cho phép dữ liệu ấy được ghi vào bên trong Blockchain. Đó là cách Blockchain được thiết kế để chống lại sự thay đổi dữ liệu.

Ví dụ: Trường hợp nếu có thay đổi trên 1 khối. Ở đây mình giả sử hacker tấn công và thay đổi thông tin trên khối A. Tại thời điểm đó:

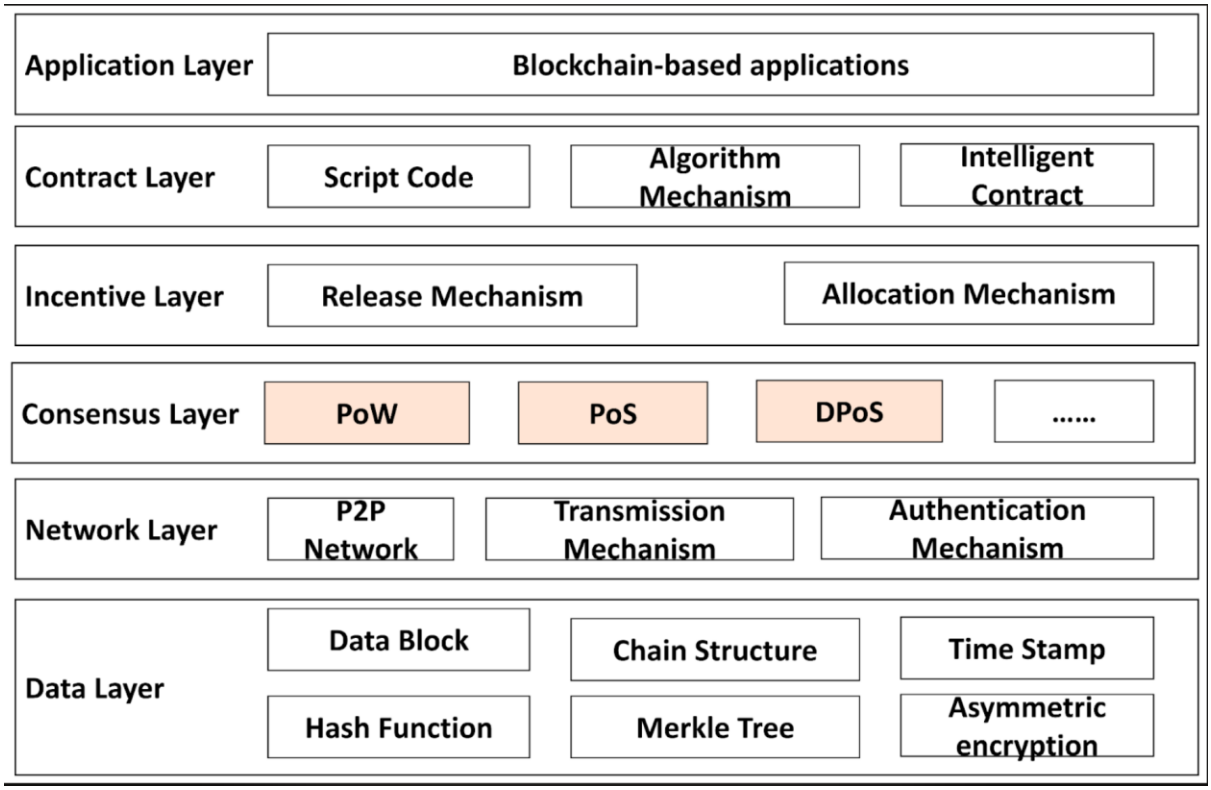
- Mã hash của khối A bị thay đổi.
- Hệ thống sẽ so sánh mã hash đó với với mã hash khối trước đó & phát hiện ra sai lệch.
- Như vậy hacker phải thay đổi hash của khối trước A. Hệ thống lại phát hiện ra sai lệch ở khối A-1. Hacker phải tiếp tục thay đổi hash của khối A-2.
- Như vậy để thay đổi được giao dịch thì hacker phải thay đổi tất cả các khối vì cơ chế đồng thuận.

Hình 2-1: Thuật toán Blockchain khi thông tin thay đổi trên 1 khối trong chuỗi.

Nếu trong mạng lưới có một block bị thay đổi, dữ liệu này được so sánh với các dữ liệu của các khối khác. Nếu có sự khác biệt thì nó sẽ không cho phép dữ liệu ấy được ghi vào bên trong Blockchain. Đó là cách blockchain được thiết kế để chống lại sự thay đổi dữ liệu.

Thuật toán đồng thuận cũng là một phần không thể thiếu của một blockchain, đóng vai trò cốt lõi giữ các blockchain hoạt động một cách phi tập trung và bảo mật. Ở thời điểm ban đầu, cơ chế đồng thuận Proof of Work của Bitcoin là lựa chọn chính của các

developer, tuy nhiên tới thời điểm hiện tại, đã có rất nhiều cơ chế đồng thuận khác nhau. Trong đó, phổ biến nhất là Proof of Stake.

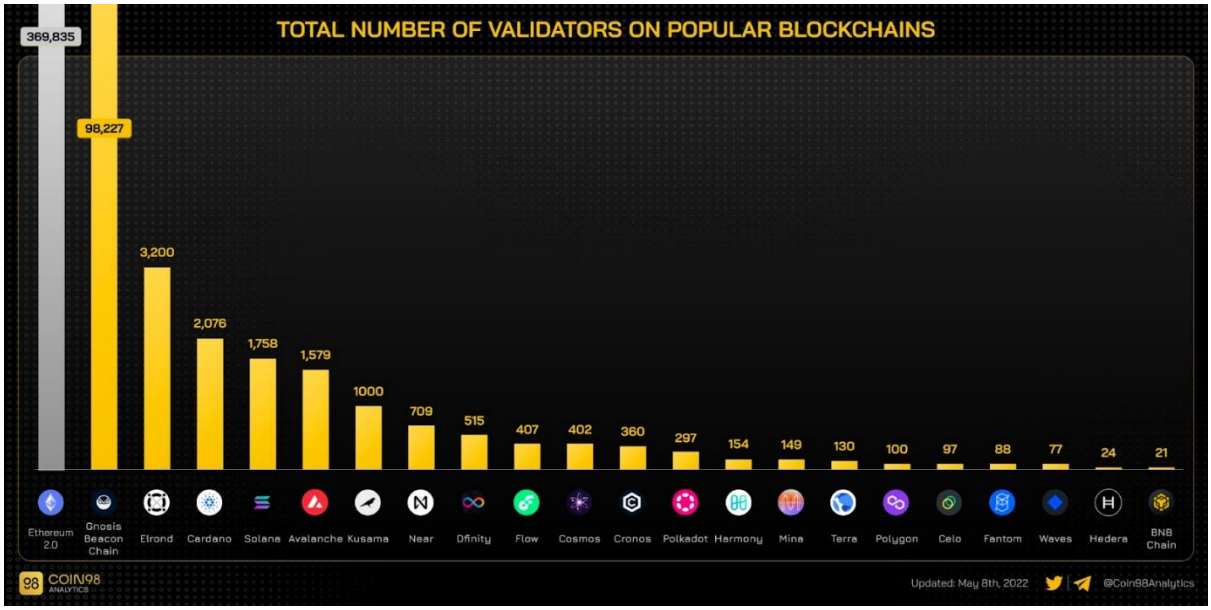


Hình 2-2: Kiến trúc mạng Blockchain[1]

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

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

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



Hình 2-3: Số lượng validator trên các blockchain phổ biến (không tính Bitcoin)[2]

Cơ chế đồng thuận được biết đến chính là một trong đặc tính quan trọng ảnh hưởng khả năng mở rộng và tính an toàn của mỗi nền tảng tiền mã hóa. Cơ chế này tồn tại nhằm ngăn chặn vấn đề chi tiêu 2 lần trên Blockchain (double spending). Xét từ góc độ đầu tư, cơ chế đồng thuận là một trong những tiêu chí quan trọng khi lựa chọn bất kỳ đồng tiền mã hóa nào.

Cơ chế đồng thuận là một cơ chế chịu lỗi được sử dụng trong các hệ thống máy tính và chuỗi khối để đạt được thỏa thuận mong muốn về một giá trị dữ liệu hoặc một trạng thái duy nhất của mạng giữa các qui trình phân bổ hoặc hệ thống đa tác nhân. Nó rất hữu ích trong việc lưu trữ hồ sơ so với các cơ chế khác.

Nội dung về Cơ chế đồng thuận:

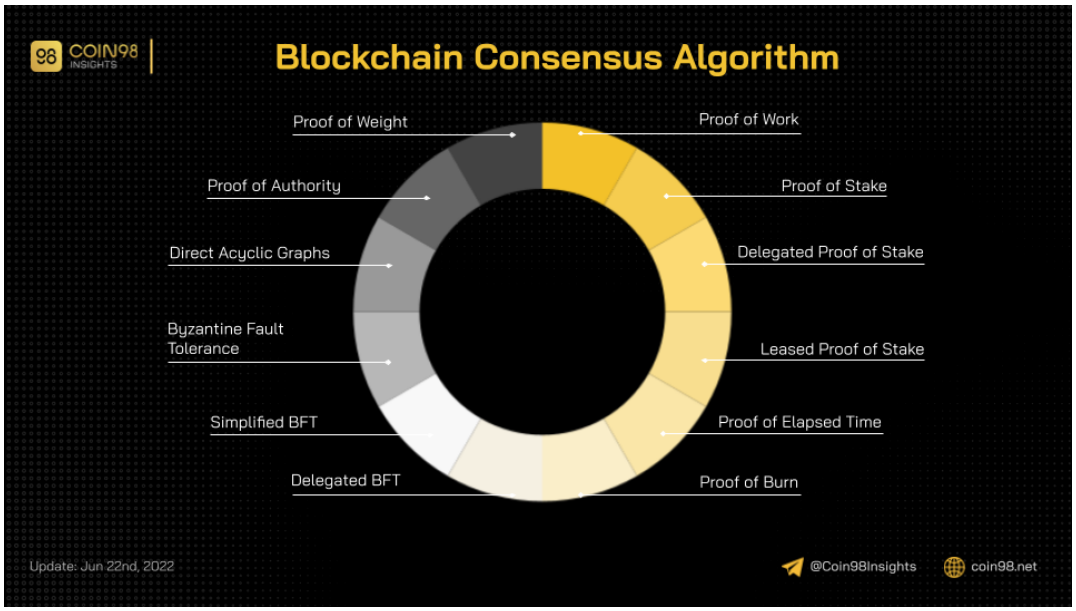
Trong bất kì hệ thống tập trung nào, ta có thể kể đến như cơ sở dữ liệu chứa thông tin chính về giấy phép lái xe ở một quốc gia, quản trị viên trung tâm có quyền duy trì và cập nhật cơ sở dữ liệu. Các công việc cập nhật như thêm, xóa, cập nhật tên của những người đủ điều kiện cho một số giấy phép nhất định được thực hiện bởi một cơ quan trung ương chịu trách nhiệm duy trì hồ sơ gốc.

[2] https://coin98.net/thuat-toan-dong-thuan-blockchain-la-gi

Các chuỗi khối công khai hoạt động giống như các hệ thống phân cấp, tự điều chỉnh trên qui mô toàn cầu mà không có bất kì cơ quan ủy quyền nào. Chúng liên quan đến sự đóng góp của hàng trăm ngàn người tham gia, những người làm việc xác minh và xác thực các giao dịch diễn ra trên chuỗi khối và trên các hoạt động khai thác khối.

Trong trạng thái thay đổi linh hoạt của chuỗi khối, các sổ cái được chia sẻ công khai này cần một cơ chế hiệu quả, công bằng, thực tế, thiết thực, đáng tin cậy và an toàn để đảm bảo rằng tất cả các giao dịch diễn ra trên mạng là chính thống và tất cả những người tham gia đồng ý về tình trạng của sổ cái. Nhiệm vụ cực kì quan trọng này được thực hiện bởi cơ chế đồng thuận, là một bộ qui tắc quyết định sự đóng góp của những người tham gia khác nhau trên nền tảng chuỗi khối.

Có nhiều loại thuật toán về cơ chế đồng thuận khác nhau hoạt động trên các nguyên tắc khác nhau.



Hình 2-4 : Các thuật toán đồng thuận blockchain nổi tiếng [1]

2.2 Các cơ chế đồng thuận phổ biến:

2.2.1 Proof-of-work (PoW) – Minh chứng làm việc:

Proof of Work là thuật toán đồng thuận blockchain đầu tiên ra đời, thuật toán này được sử dụng bởi Bitcoin - đồng tiên mã hoá đầu tiên trên thế giới.

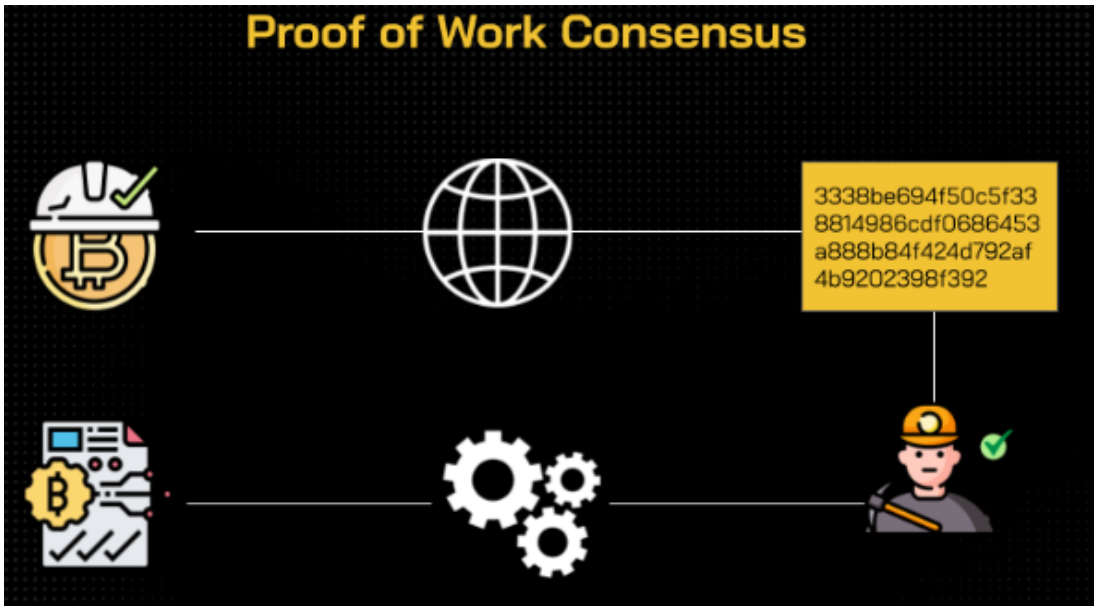
Proof of Work (PoW) hay còn gọi là bằng chứng công việc. Với cơ chế đồng thuận này, các node sẽ sử dụng sức mạnh máy tính để giải các bài toán tạo ra mã hash. Node đầu tiên giải bài toán, giành quyền xác thực giao dịch, sau đó sẽ được nhận phần thưởng là BTC. Quá trình này được gọi là "mining" (đào coin), trong đó các node đóng vai trò là các miners (thợ đào).

Khi một node giải bài toán và xác nhận giao dịch, giao dịch đó cũng sẽ được kiểm tra và xác nhận bởi tất cả các node khác trong mạng lưới. Nếu câu trả lời được thông qua, tất cả các node sẽ thêm giao dịch này vào blockchain, làm cho blockchain có thể dễ dàng xác minh và đồng bộ hoá.

Chính bởi vì việc sử dụng sức mạnh máy tính để bảo mật cho blockchain, Proof of Work yêu cầu một lượng tiêu thụ điện lớn cũng như chi phí khá đắt đỏ cho các phần cứng bắt buộc.

Thêm nữa, một block trên một blockchain Proof of Work cũng cần nhiều thời gian hơn để được tạo ra và xác thực, điều này làm cho thuật toán này kém hiệu quả và tốn tài nguyên (thậm chí là không thân thiện với môi trường) hơn các thuật toán đồng thuận khác.

Đây là cơ chế đồng thuận đầu tiên và gắn liền với Bitcoin (BTC), Ethereum (ETH)....



Hình 2-5: Cơ chế đồng thuận Proof of Work

Ưu điểm: Là giao thức đầu tiên, Proof-of-work (PoW) đã chứng minh khả năng phục hồi của nó trước các cuộc tấn công nội bộ và bên ngoài.

Nhược điểm: Proof-of-work (PoW) bị chỉ trích vì nhiều lý do. Proof-of-work (PoW) tiêu thụ nhiều năng lượng, với một số ước tính chỉ ra năng lượng mạng Bitcoin tiêu thụ ở cùng cấp độ với 159 quốc gia. Các nhà phê bình của Bitcoin như Andrew Tayo đã chỉ ra rằng phần lớn năng lượng này bị lãng phí, vì chỉ có một thợ mỏ cuối cùng có thể khai thác từng khối (được chấp nhận), bất kể có bao nhiêu người tham gia cuộc đua đến đó trước.

Bitcoin hiện nay chủ yếu được khai thác bằng cách sử dụng ASIC (vi mạch dành riêng cho giải mã thuật toán đào), vì vậy khai thác mỏ bị chi phối bởi các tổ chức lớn như Bitmain, có thể đủ khả năng phần cứng cần thiết để khai thác ở quy mô lớn. Điều này tập trung sức mạnh khai thác vào tay của một số ít, dẫn đến việc một số người trong cộng đồng gọi Bitcoin là một loại tiền tệ tập trung. Mặc dù một số đồng tiền mã hóa như Vertcoin cố gắng duy trì việc chống lại-ASIC bằng các thuật toán thay đổi thường xuyên, nó là một thách thức lớn ở phía trước với các nhà sản xuất ASIC.

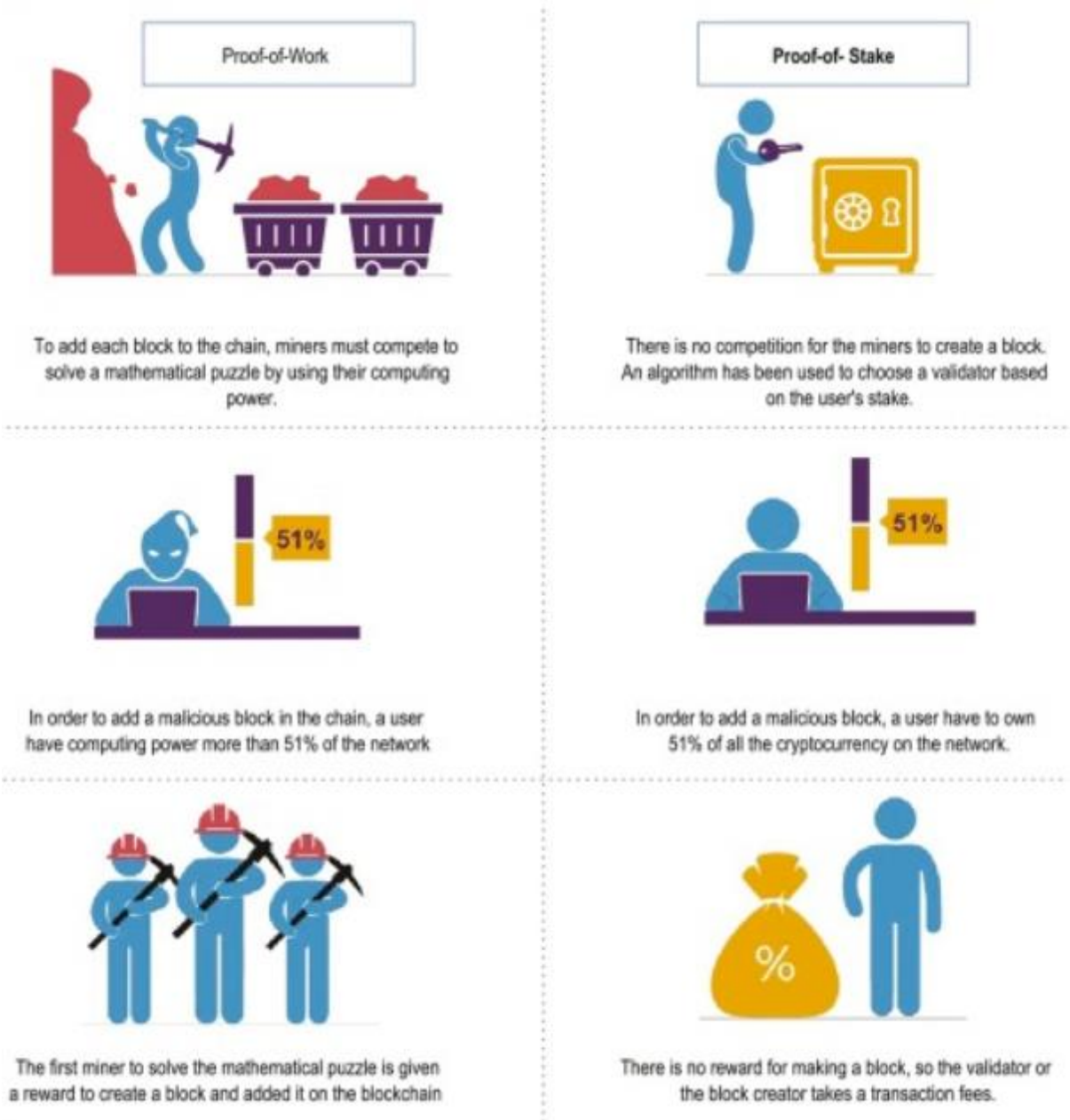
2.2.2 Proof-of-stake (PoS) – Minh chứng cổ phần:

Proof of Stake (PoS), hay còn gọi là bằng chứng cổ phần, là cơ chế thuật toán đồng thuận phổ biến nhất hiện nay, được sử dụng đầu tiên bởi Ethereum. Thay vì sử dụng sức mạnh máy tính, Proof of Stake yêu cầu các node tham gia xác thực giao dịch phải ký gửi (stake) một số lượng nhất định native token của blockchain để giành quyền tham gia xác thực và tạo khối.

Thường các blockchain sử dụng Proof of Stake sẽ yêu cầu một số lượng token tối thiểu để được tham gia làm validator. Ví dụ, để trở thành validator của Ethereum, người dùng sẽ phải stake ít nhất 32 ETH (khoảng 33 nghìn USD tại thời điểm viết bài). Số token này được đặt cọc để đảm bảo các node hoạt động tốt, tức là nếu node đó offline quá lâu hoặc có những hành vi gian lận, số token đã stake có thể bị thu một phần hoặc mất toàn bộ tuỳ thuộc vào mức độ.

Validator node trong mạng lưới Proof of Stake sẽ nhận được phí giao dịch làm phần thưởng. Khi một giao dịch giao dịch diễn ra, các validator sẽ được chọn ngẫu nhiên để xác thực giao dịch, số lượng token stake càng nhiều tỉ lệ được chọn cũng sẽ tăng tương ứng.

Với các hoạt động trên, Proof of Stake là thuật toán tiết kiệm chi phí, thân thiện với môi trường hơn Proof of Work. Để trở thành một validator node cũng đơn giản hơn và không phải sử dụng các thiết bị phần cứng quá "khủng".



Hình 2-6: So sánh cơ chế đồng thuận Proof-of-work và Proof-of-State

Proof-of-stake (PoS) lần đầu tiên được hình thành như một cách để tránh những vấn đề cố hữu với Proof-of-work (PoW), chẳng hạn như tiêu thụ năng lượng. Trong mô hình PoS, những người nắm giữ những đồng coin có thể đặt cược chúng vào khả năng khối tiếp theo là chính xác. Nếu có, họ nhận được phần thưởng. Nếu ai đó đặt cược những đồng coin vào một khối mà khối đó có chứa các giao dịch gian lận, họ sẽ bị 'phạt' giá trị cổ phần (phần cược) của họ.

Ưu điểm: Proof-of-stake (PoS) tiêu thụ ít năng lượng hơn Proof-of-work (PoW). Proof-of-stake (PoS) cũng tích cực trừng phạt gian lận, ngăn chặn hành vi lừa đảo giữa các người xác nhận.

Nhược điểm: Khi các nút xác nhận không đóng góp sức mạnh tính toán – được gọi là vấn đề "không có cổ phần" – có nguy cơ tăng lên đó là PoS Blockchains có thể thấy nhiều nhánh hơn PoW. Ngoài ra, Proof-of-stake (PoS) ủng hộ những người có nhiều đồng coin nhất, đồng thời thúc đẩy tập quyền vì những người nắm giữ giàu có hơn có thể đặt cược nhiều hơn. Đối với PoS coin NXT, nó đã được chứng minh được rằng làm thế nào một người nắm cổ phần có thể tăng vững chắc số cổ phần của họ đến mức họ sẽ sở hữu hơn 90% số đồng coin.

Sự chấp nhận: Các dự án sử dụng thuật toán PoS thuần túy là Reddcoin, Decred và NavCoin. Các vấn đề với thuật toán PoW là những gì đã khiến Ethereum phải rời khỏi PoW thuần túy và áp dụng Casper (một giao thức hỗn hợp PoW / PoS).

2.2.3 Delegated PoS (dPoS) – PoS được ủy quyền:

Delegated Proof of Stake (DPoS), hay còn gọi là bằng chứng uỷ quyền cổ phần, là phiên bản phát triển của Proof of Stake. PoS được ủy quyền được phát minh bởi Daniel Larimer, đồng sáng lập của Steem và CTO của EOS, cả hai đều sử dụng dPoS. Ở đây, mạng lưới sẽ bầu cho 'Nhân Chứng', người đạt được sự đồng thuận để thêm khối tiếp theo. Tương tự như mô hình PoS chuẩn, trọng số biểu quyết của người tham gia mạng được xác định bằng số lượng token (mã thông báo) mạng mà họ nắm giữ.

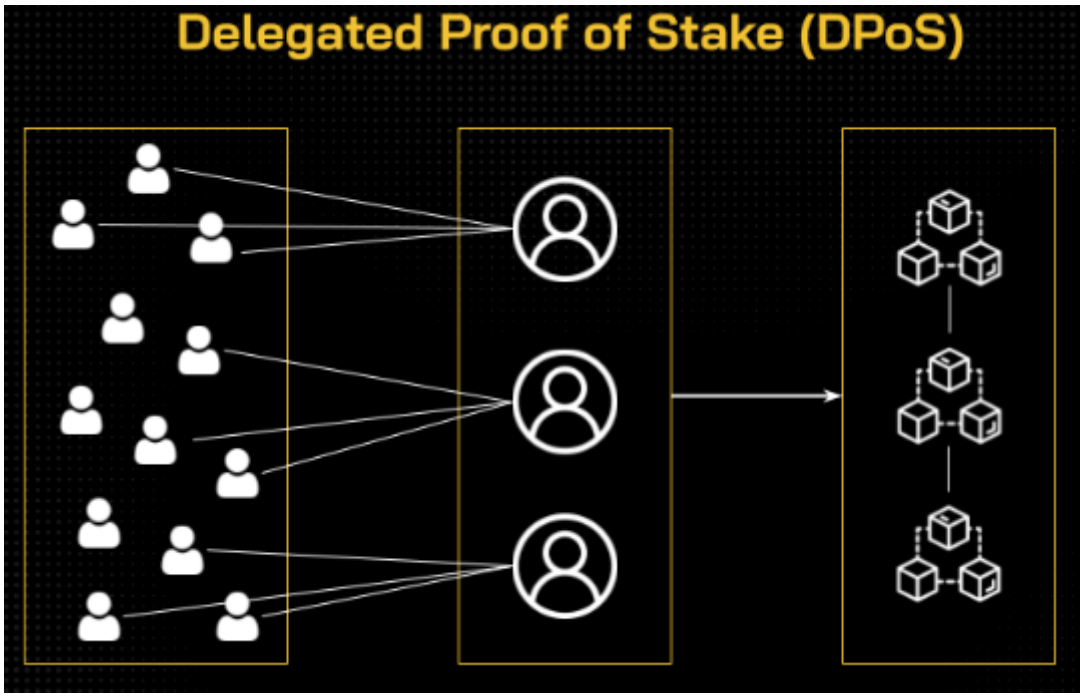
Thay vì chọn validator ngẫu nhiên như PoS, token holders sẽ chọn một số các node chuyên nghiệp để các node này vận hành mạng, bù lại, token holders sẽ được chia

sẻ một phần phần thưởng cho công việc duy trì an ninh cho mạng. Trong mỗi block, số lượng delegators được chọn để xác thực giao dịch là giới hạn và ngẫu nhiên.

Ngoài ra, Delegated Proof of Stake có số lượng validator có giới hạn, thường giao động từ 10 - 100, so với PoS nguyên bản, DPoS được đánh giá là nhanh hơn và hiệu suất tốt hơn.

DPoS giúp đảm bảo sự trung thực và công bằng bằng việc thực hiện các hoạt động bỏ phiếu liên tục và cũng liên tục xáo trộn trong hệ thống, để đảm bảo những người được chọn là trung thực và có trách nhiệm.

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



Hình 2-7: Cơ chế đồng thuận DPoS

Ưu điểm: PoS được ủy quyền làm giảm thời gian tạo khối, vì càng ít bên tham gia vào một sự đồng thuận từ đó tăng tốc độ ra quyết định. Bằng cách tránh sử dụng ASIC, nó khuyến khích phân cấp – nhưng với một số cảnh báo, như được nêu ra dưới đây.

Khuyết điểm: Việc sử dụng ‘Nhân Chứng’ có nghĩa là sự phân cấp hoàn toàn không bao giờ đạt được. Xem xét sự khác biệt giữa một nền dân chủ đầy đủ – tất cả các công dân bỏ phiếu cho tất cả các vấn đề – và một nền dân chủ đại diện, nơi các đại biểu được bầu để đại diện cho cử tri.

Vitalik Buterin (người sáng lập Ethereum) đã viết một lời chỉ trích về PoS được ủy quyền, mô tả cách thức giao thức đồng thuận này có thể dẫn đến chế độ phân biệt giai cấp, với các cử tri có ảnh hưởng hình thành các nhóm, chúng có thể kết thúc chung cuộc trong một cuộc tấn công nguy hiểm. Larimer đã phản ứng phòng thủ mạnh mẽ với bài đăng trên blog của riêng ông có tiêu đề "Giới hạn về quản trị kinh tế mật mã":

"Vitalik đang tìm kiếm một hộp đen kinh tế – mã hóa giả định rằng các chủ thể không thể dựa vào việc bỏ phiếu cho dù qua hình thức cổ phần (phân biệt giai cấp) hoặc bởi cá nhân (dân chủ)."

Larimer kết luận với quan điểm của ông rằng sự đồng thuận là vai trò của mạng lưới, và rằng "mỗi cộng đồng có thể có định nghĩa riêng về "đúng và sai", chỉ có thể được đo bằng một cuộc thăm dò ý kiến chủ quan của các thành viên cộng đồng".

2.2.4 Proof of History (PoH)

Proof of History, hay còn gọi là bằng chứng lịch sử, là thuật toán đồng thuận khá mới được giới thiệu bởi Solana. Thay vì xét theo logic, PoH sử dụng timeline giao dịch làm tài liệu tham khảo. Vì vậy, các validator node của mạng Solana có thể tạo các block tiếp theo mà không cần phải phối hợp với toàn bộ mạng lưới.

Về cơ bản, Proof of History không tính toán output từ dữ liệu input, thay vào đó PoH sử dụng một tính năng để sử dụng các output đã có trước đó làm input. Cơ chế này được xây dựng để giải quyết vấn đề về thời gian trong các mạng phi tập trung ở nơi không có cùng mốc thời gian.

2.2.5 Proof of Authority (PoA)

Proof of Authority, hay còn gọi là bằng chứng uỷ quyền, là thuật toán đồng thuận dựa trên danh tiếng. Khác với PoS, những validators làm nhiệm vụ xác thực khối sẽ không được chọn dựa trên số coin họ nắm giữ mà sẽ dựa trên chính danh tiếng của mình.

Lượng validator của mạng lưới được giới hạn, giúp cho Proof of Authority trở thành một mô hình có khả năng mở rộng. Trong đó, các giao dịch được xác thực bởi các validator đã được chọn lọc và phê duyệt, đây cũng chính là những người điều tiết hệ thống.

PoA đề cao giá trị danh tính, tức là những người được chọn là các validator đáng tin cậy, điều này giúp cho một vài công ty và doanh nghiệp có thể ứng dụng thuật toán này. Không chỉ vậy, thuật toán đồng thuật PoA có thể được coi là một lựa chọn giá trị cho các ứng dụng trong ngành hậu cần, chuỗi cung ứng.

Để có những ưu điểm trên, PoA phải đánh đổi bằng sự phi tập trung, hi sinh sự phi tập trung để đổi lấy hiệu suất và khả năng mở rộng, hay nói cách khác, mô hình này chỉ làm các hệ thống tập trung trở nên hiệu quả hơn.

PoA được đề xuất lần đầu tiên bởi cựu CTO của Etherueum, Gavin Wood vào năm 2017, sau đó được sử dụng bởi Binance Smart Chain (BNB Chain) và các exchange chain khác như HECO, OKExChain, Gatechain, Cronos…

2.2.6 Proof of Contribution (PoC)

Proof of Contribution (tạm dịch là bằng chứng cống hiến) giám sát hành động của tất cả validator trong mạng lưới và xếp hạng các validator đó dựa theo đóng góp của họ - một cơ chế khá tương đồng với hệ thống tín dụng xã hội. Sự uy tín của một người dùng được đánh giá dựa trên số lượng token đã stake và các giao dịch trong lịch sử.

Trước khi tham gia vào mạng lưới, người dùng sẽ phải stake một khoản tiền gọi là security deposit. Sau khi hoàn thành các công việc tính toán, các node có các kết quả được xác thực sẽ được thưởng phí giao dịch và staked token từ các node không có kết quả chính xác.

2.2.7 Proof of Reputation (PoR)

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

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

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

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

2.2.8 Byzentin Fault Tolerance (BFT)

Byzantine Fault Tolerance (hay Hệ thống chịu lỗi Byzantine - BFT) là hệ thống có thể giải quyết được vấn đề của bài toán Byzantine. Điều này có nghĩa là hệ thống BFT có thể tiếp tục hoạt động ngay cả khi một số node bị lỗi hoặc thực hiện hành động gây hại cho mạng chung.

Thuật toán này cho phép những người thực hiện xác minh quản lý mỗi trạng thái của một chuỗi, đồng thời chia sẻ các thông điệp với một chuỗi khác, để có được những bản ghi giao dịch chính xác và đảm bảo sự trung thực.

Một số dự án sử dụng thuật toán này: NEO (NEO), Ripple (XRP), Stellar (XLM)...

2.2.9 Các thuật toán đồng thuận khác

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

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

TÀI LIỆU THAM KHẢO

[1] Y. Chen, “Blockchain tokens and the potential democratization of entrepreneurship and innovation,” *Business Horizons*, vol. 61, no. 4, pp. 567–575, Jul. 2018, doi: 10.1016/j.bushor.2018.03.006.

[2] C. Holotescu, V. Holotescu, and T. Holotescu, “Understanding Blockchain Technology and how to get involved,” 2018, doi: 10.13140/RG.2.2.25185.33126/1.

[3] Y. Chang, E. Iakovou, and W. Shi, “Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities,” *International Journal of Production Research*, vol. 58, no. 7, pp. 2082–2099, Apr. 2020, doi: 10.1080/00207543.2019.1651946.