**1.1 Cơ chế đồng thuận là gì?**

Consensus Mechanism ( Cơ chế đồng thuận ) là một cơ chế chịu lỗi được sử dụng trong các hệ thống máy tính và blockchain để đạt được thỏa thuận cần thiết về một giá trị dữ liệu hoặc một trạng thái duy nhất của mạng giữa các quy trình phân tán hoặc hệ thống đa tác nhân. Nó rất hữu ích trong việc lưu trữ hồ sơ, chứa tất cả những thứ khác đều có thể lưu trữ

Fault tolerance đề cập đến khả năng của một hệ thống (computer, network, cloud cluster,) có khả năng tiếp tục hoạt động mà không bị gián đoạn khi một hoặc nhiều thành phần của nó gặp sự cố. Mục tiêu của việc tạo ra một hệ thống chịu lỗi (fault-tolerant system) là ngăn chặn sự gián đoạn phát sinh từ một điểm thất bại duy nhất, đảm bảo tính sẵn sàng cao (high availability) và tính liên tục (business continuity) của các ứng dụng hoặc hệ thống thực hiện các nhiệm vụ quan trọng.

Ở các cấu trúc hệ thống truyền thống, luôn có cơ quan đầu não tập trung chịu trách nhiệm giải quyết các vấn đề xử lý và thống nhất thông tin. Tuy nhiên, với kiến trúc phân tán peer to peer của Blockchain thì cũng cần đảm bảo sự đồng thuận thống nhất trong luồng xử lý thông tin nhằm đảm bảo tính an toàn và bảo mật cho hệ thống không bị xung đột và mâu thuẫn.

Nói một cách đơn giản, sự đồng thuận là một cách năng động để đạt được thỏa thuận trong một nhóm. Trong khi bỏ phiếu chỉ giải quyết cho một nguyên tắc đa số mà không có bất kỳ suy nghĩ nào về cảm xúc và phúc lợi của người thiểu số, trong khi một sự đồng thuận đảm bảo rằng một thỏa thuận đạt được có thể đem lại lợi ích cho toàn bộ nhóm.

**1.2 Tại sao chúng ta cần luật đồng thuận?**

Trong một hệ thống blockchain mà không cần sự cho phép, kiểm tra tính danh, ai cũng có thể trở thành 1 node trong mạng lưới và chỉnh sửa,các giao dịch, bao gồm chúng trong 1 block mới. Khi đó, chúng ta có thể gọi các chỉnh sửa này là một fork, fork này bao gồm các giao dịch đã bị chỉnh sửa, khi đó mạng lưới của chúng ta có nhiều phiên bản khác nhau về thông tin của các giao dịch. Mục tiêu của consensus là để tránh những fork này và tất cả mọi người đều chấp nhật 1 phiên bản thật sự. Kể cả trong một blockchain mà các node được kiểm tra và cho phép, chọn lọc, chúng ta vẫn cần consensus bởi vì chúng ta cũng không chắc chắn 100% rằng các node này tin tưởng được.

Giải thích sâu hơn:

Ở các hệ thống tập trung, ví dụ hệ thông dữ liệu lưu trữ thông tin bằng lái ở một quốc gia. Một trung tâm quản lý tập turng được định danh để bảo trì và update dữ liệu như thêm/xóa/sửa tên của các chủ bằng lái xe. Điều này được thực hiện bởi một cơ quan trung ương, là cơ quan chịu trách nhiệm duy nhất trong việc duy trì hồ sơ thống nhất và hợp pháp

Các blockchains công khai hoạt động như các hệ thống phân quyền, tự điều chỉnh hoạt động trên quy mô toàn cầu mà không có bất kỳ cơ quan có thẩm quyền nào. Chúng liên quan đến sự đóng góp từ hàng trăm nghìn người tham gia, những người làm việc về xác minh và xác thực các giao dịch xảy ra trên blockchain và các hoạt động khai thác khối.

Trong trạng thái thay đổi động như vậy của blockchain, các sổ cái được chia sẻ công khai này cần một cơ chế hiệu quả, công bằng, thời gian thực, chức năng, đáng tin cậy và an toàn để đảm bảo rằng tất cả các giao dịch xảy ra trên mạng là chính thức và tất cả những người tham gia đồng ý với nhau về trạng thái của sổ cái. Nhiệm vụ quan trọng này được thực hiện bởi cơ chế đồng thuận, là một tập hợp các quy tắc quyết định sự đóng góp của những người tham gia khác nhau của blockchain.

**2.1 Byzantine**

Ok, hãy tưởng tượng rằng có một nhóm tướng Byzantine và họ muốn tấn công một thành phố. Họ đang phải đối mặt với hai vấn đề xung đột đầy khó khăn:

Các tướng lĩnh và quân đội của họ ở rất xa nhau nên quyền lực tập trung dưới một sự chỉ huy là không thể, khiến cho việc phối hợp tấn công trở nên rất khó khăn.

Thành phố có một đội quân khổng lồ và cách duy nhất để họ có thể giành chiến thắng là nếu tất cả cùng tấn công một lúc.

Để thực hiện sự phối hợp thành công, đội quân bên trái lâu đài sẽ gửi một sứ giả đến đội quân bên phải lâu đài với một thông điệp có nội dung “HÃY TẤN CÔNG THỨ TƯ”. Tuy nhiên, giả sử các đội quân ở bên phải không chuẩn bị cho cuộc tấn công và nói, “KHÔNG. TẤN CÔNG NGÀY THỨ SÁU ”và gửi lại sứ giả đi xuyên qua thành địch và trở lại đội quân bên trái.

Đây là nơi chúng ta phải đối mặt với một vấn đề.

Một số điều có thể xảy ra với người đưa tin ko may mắn. Anh ta có thể bị bắt, bị xâm phạm, bị giết và bị thay thế bằng một sứ giả khác bởi thành phố địch. Điều này sẽ dẫn đến việc quân đội nhận được thông tin giả mạo, có thể dẫn đến một cuộc tấn công và thất bại khi không phối hợp.

Điều này cũng có tham chiếu rõ ràng đến blockchain. Chuỗi là một mạng lưới khổng lồ; làm thế nào bạn có thể tin tưởng họ? Nếu bạn đang gửi cho ai đó 4 Ether từ ví của mình, làm thế nào bạn biết chắc rằng ai đó trong mạng sẽ không giả mạo nó và thay đổi 4 thành 40 Ether?

Những gì các vị tướng này cần, là một cơ chế đồng thuận có thể đảm bảo rằng quân đội của họ có thể thực sự tấn công như một đơn vị bất chấp tất cả những trở ngại này.

Bây giờ chúng ta sẽ xem xét danh sách các cơ chế đồng thuận có thể giải quyết vấn đề của các Tướng Byzantine.

**2.2 PoW (BITCOIN, LITECOIN)**

Satoshi Nakamoto, người tạo ra Bitcoin, đã có thể giải quyết vấn đề bằng cách phát minh ra giao thức bằng chứng công việc.

Trước tiên, hãy xem nó hoạt động như thế nào trong bối cảnh vấn đề của các Tướng Byzantine.

Giả sử quân bên trái muốn gửi một thông báo gọi là "ATTACK MONDAY" cho quân bên phải, họ sẽ làm theo các bước nhất định.

Đầu tiên, họ sẽ thêm một “nonce” vào văn bản gốc. Số nonce có thể là bất kỳ giá trị thập lục phân ngẫu nhiên nào.

Sau đó, họ băm văn bản được nối với một nonce và xem kết quả. Giả sử, nói theo giả thuyết, quân đội đã quyết định chỉ chia sẻ các thông điệp, khi băm, đưa ra kết quả bắt đầu bằng 5 số 0.

Nếu các điều kiện băm được thỏa mãn, họ sẽ gửi tin nhắn cùng với hàm băm của tin nhắn. Nếu không, thì họ sẽ tiếp tục thay đổi giá trị của nonce một cách ngẫu nhiên cho đến khi họ nhận được kết quả mong muốn. Hành động này cực kỳ tẻ nhạt, tốn thời gian và cần nhiều sức mạnh tính toán.

Nếu người đưa tin bị thành phố bắt và tin nhắn bị giả mạo, theo thuộc tính hàm băm, bản thân hàm băm sẽ bị thay đổi đáng kể. Nếu các tướng ở phía bên phải, thấy rằng thông báo băm không bắt đầu với số lượng 0 cần thiết thì họ có thể đơn giản dừng lại cuộc tấn công giả mạo.

Tuy nhiên, có thể có một kẽ hở.

Không có hàm băm nào là 100% không có va chạm. Vì vậy, điều gì sẽ xảy ra nếu thành phố nhận được thông điệp, giả mạo nó và sau đó thay đổi nonce theo đó cho đến khi họ nhận được kết quả mong muốn có số 0 cần thiết? Việc này sẽ vô cùng tốn thời gian nhưng vẫn có thể thực hiện được. Để chống lại điều này, các vị tướng sẽ sử dụng sức mạnh theo số lượng.

Giả sử thay vì chỉ có một tướng bên trái gửi tin nhắn cho một tướng bên phải thì có 3 tướng bên trái phải gửi tin nhắn cho những người bên phải. Để làm điều đó, họ có thể tạo thông điệp của riêng mình và sau đó băm thông báo tích lũy và sau đó thêm nonce vào hàm băm kết quả và băm lại. Lần này, họ muốn một tin nhắn bắt đầu bằng sáu số 0.

Rõ ràng, điều này sẽ cực kỳ tốn thời gian, nhưng lần này, nếu người đưa tin bị thành phố bắt, khoảng thời gian mà họ sẽ mất để giả mạo thông báo tích lũy và sau đó tìm nonce tương ứng cho hàm băm sẽ là vô hạn. hơn. Nó thậm chí có thể mất nhiều năm. Vì vậy, ví dụ. Nếu thay vì một sứ giả, các tướng cử nhiều sứ giả, vào thời điểm thành phố thậm chí còn đang trong quá trình tính toán, họ sẽ bị tấn công và phá hủy.

Các tướng bên phải có nó khá dễ dàng. Tất cả những gì họ phải làm là thêm vào tin nhắn với số nonce chính xác sẽ được cấp cho họ, băm chúng và xem liệu băm có khớp hay không. Việc băm một chuỗi rất dễ thực hiện. Về bản chất, đó là quy trình đằng sau bằng chứng công việc.

Quá trình tìm kiếm nonce cho mục tiêu băm thích hợp sẽ vô cùng khó khăn và tốn thời gian.

Tuy nhiên, quá trình kiểm tra kết quả để xem không có sơ suất nào được thực hiện rất đơn giản.

Vì vậy, nếu chúng ta muốn tóm tắt cách Proof Of Work Protocol hoạt động với blockchain.

Các thợ mỏ giải quyết các câu đố mật mã để “khai thác” một khối để thêm vào blockchain.

Quá trình này đòi hỏi một lượng lớn năng lượng và sử dụng tính toán. Các câu đố đã được thiết kế theo cách gây khó khăn và đánh thuế hệ thống. Miners thay đổi value hash liên tục nhằm tìm ra con số đúng và hợp lệ trên block header. Con số hash value đúng gọi là số nonce. (Tìm số nonce)

Khi một người khai thác giải được câu đố, họ đưa khối của mình lên mạng để xác minh.

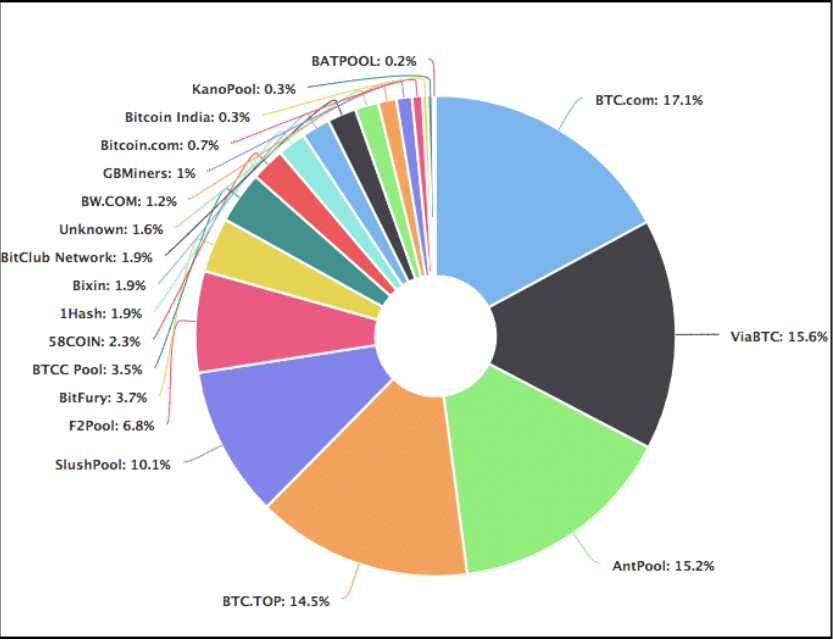
Xác minh xem khối có thuộc chuỗi hay không là một quá trình cực kỳ đơn giản.

Cơ chế proof-of-work chắc chắn đã trả lời rất nhiều câu hỏi khi giải quyết vấn đề Byzantine General’s Problem, nhưng rất tiếc có một số vấn đề với Proof-of-work.

Đầu tiên và quan trọng nhất, chứng minh công việc là một quá trình cực kỳ kém hiệu quả vì lượng sức mạnh và năng lượng mà nó ngốn hết.

Những người và tổ chức có đủ khả năng mua ASIC nhanh hơn và mạnh hơn thường có cơ hội khai thác tốt hơn những người khác.

Do đó, bitcoin không được phi tập trung như mong muốn. Hãy kiểm tra biểu đồ phân phối tốc độ băm:



Như bạn có thể thấy, ~ 65% hashrate được chia riêng cho 5 nhóm khai thác!

Về mặt lý thuyết, các nhóm khai thác lớn này có thể đơn giản hợp tác với nhau và tung ra 51% trên mạng bitcoin.

Mặc dù công nghệ blockchain đã nhận được sự quan tâm đáng kể từ cộng đồng khoa học máy tính và kinh tế, việc sử dụng các phương pháp lý thuyết trò chơi trong công nghệ này còn hạn chế. Trong phần này, chúng ta trình bày các công trình gần đây và có liên quan nhất sử dụng lý thuyết trò chơi trong công nghệ blockchain.

**2.3 Game Theory**

Lý thuyết trò chơi trong validation người A có quyền chọn trung thực hay gian lận, nếu chọn gian lận có thể gây hại cho chính bản thân mình khi đa số người dùng khác trung thực. Từ đó, có thể dễ dàng phát hiện ra một vài cá nhân đang đi ngược lại với số đông nhằm mục đích phá hoại.

**2.4 PoS (ETHEREUM)**

Một miner nắm 2% tổng lượng tiền thì chỉ có thể validate tối đa 2% tổng lượng giao dịch có giá trị tương ứng => Nhược điểm: tích trữ, hạn chế chi tiêu, đồng tiền không vận động giảm giá trị.

Ethereum sắp có kế hoạch chuyển từ Proof of Work (POW) sang Proof of Stake (POS).

Bằng chứng về cổ phần sẽ làm cho toàn bộ quá trình khai thác trở nên ảo hóa và thay thế các thợ đào bằng các trình xác thực.

Đây là cách quy trình sẽ hoạt động:

Người xác nhận sẽ phải khóa một số tiền của họ dưới dạng tiền cược.

Sau đó, họ sẽ bắt đầu xác thực các khối. Có nghĩa là, khi họ phát hiện ra một khối mà họ nghĩ có thể được thêm vào chuỗi, họ sẽ xác nhận nó bằng cách đặt cược vào nó.

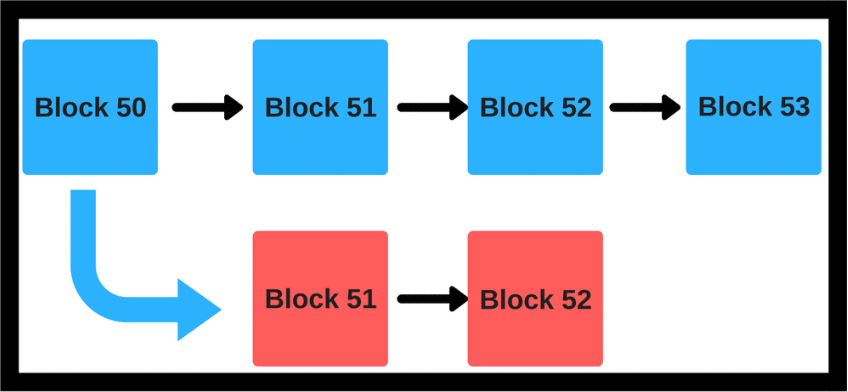
Nếu khối được thêm vào, thì những người xác nhận sẽ nhận được phần thưởng tương ứng với số tiền đặt cược của họ.

Như bạn có thể thấy, giao thức POS thân thiện với tài nguyên hơn rất nhiều so với POW. Trong POW, bạn CẦN lãng phí nhiều tài nguyên để đi cùng với giao thức, về cơ bản đó là lãng phí tài nguyên vì lợi ích của việc lãng phí tài nguyên.

\* Rào cản lớn nhất đối với bằng chứng cổ phần

Các nhà phát triển Ethereum luôn có kế hoạch cuối cùng chuyển sang bằng chứng cổ phần, đó luôn là kế hoạch của họ. Tuy nhiên, trước khi họ có thể làm như vậy, họ phải giải quyết một trong những sai sót lớn nhất của bằng chứng cổ phần (POS).

Hãy xem xét kịch bản này trong giây lát:



Giả sử chúng ta có một tình huống như trên. Có một chuỗi chính màu xanh lam và một chuỗi màu đỏ phân loại các nhánh từ chính chuỗi chính. Có gì để ngăn một thợ đào độc hại khai thác trên các khối màu đỏ và buộc một hardfork?

Trong hệ thống bằng chứng công việc (POW), rủi ro này có thể được giảm thiểu.

Giả sử người khai thác độc hại Alice muốn khai thác trên chuỗi màu đỏ. Ngay cả khi cô ấy dành tất cả sức mạnh băm của mình cho nó, cô ấy sẽ không có bất kỳ người khai thác nào khác tham gia cùng cô ấy trên chuỗi mới. Mọi người khác vẫn sẽ tiếp tục khai thác trên chuỗi màu xanh lam, vì khai thác trên chuỗi dài hơn sẽ có lợi hơn và không có rủi ro.

Bây giờ hãy nhớ rằng, POW là nguồn tài nguyên vô cùng đắt đỏ.

Không có nghĩa lý gì nếu một người khai thác lãng phí quá nhiều tài nguyên vào một khối sẽ bị mạng từ chối. Do đó, việc chia tách chuỗi được tránh trong hệ thống bằng chứng công việc vì số tiền mà kẻ tấn công sẽ phải lãng phí.

Tuy nhiên, mọi thứ có vẻ hơi khác khi bạn mang máy POS vào.

Nếu bạn là người xác thực, thì bạn có thể chỉ cần đặt tiền của mình vào cả chuỗi màu đỏ và chuỗi màu xanh lam mà không sợ bị ảnh hưởng gì cả. Bất kể điều gì xảy ra, bạn sẽ luôn chiến thắng và không có gì để mất, bất chấp hành động của bạn có thể ác ý đến mức nào.

\* Đây được gọi là vấn đề “Nothing at Stake”.

Để kết hợp hệ thống đồng thuận POS, tiền điện tử cần giải quyết vấn đề này và Ethereum sẽ thực hiện điều này theo một cách rất thú vị bằng cách điều chỉnh giao thức Casper của họ.

Casper là giao thức POS mà Ethereum đã chọn để sử dụng. Trong khi có cả một nhóm bận rộn tạo ra nó, Vlad Zamfir thường được coi là "Gương mặt của Casper".

\* Vậy Casper khác với các giao thức Proof of Stake khác như thế nào?

Casper đã thực hiện một quy trình mà họ có thể trừng phạt tất cả các phần tử độc hại. Đây là cách POS dưới Casper sẽ hoạt động:

Người xác nhận đặt cược một phần trong số Ethers của họ dưới dạng tiền cược.

Sau đó, họ sẽ bắt đầu xác thực các khối. Có nghĩa là, khi họ phát hiện ra một khối mà họ nghĩ có thể được thêm vào chuỗi, họ sẽ xác nhận nó bằng cách đặt cược vào nó.

Nếu khối được thêm vào, thì những người xác nhận sẽ nhận được phần thưởng tương ứng với số tiền đặt cược của họ.

Tuy nhiên, nếu người xác thực hành động theo cách ác ý và cố gắng làm “không có gì bị đe dọa”, họ sẽ ngay lập tức bị khiển trách và tất cả số tiền đặt cọc của họ sẽ bị cắt.

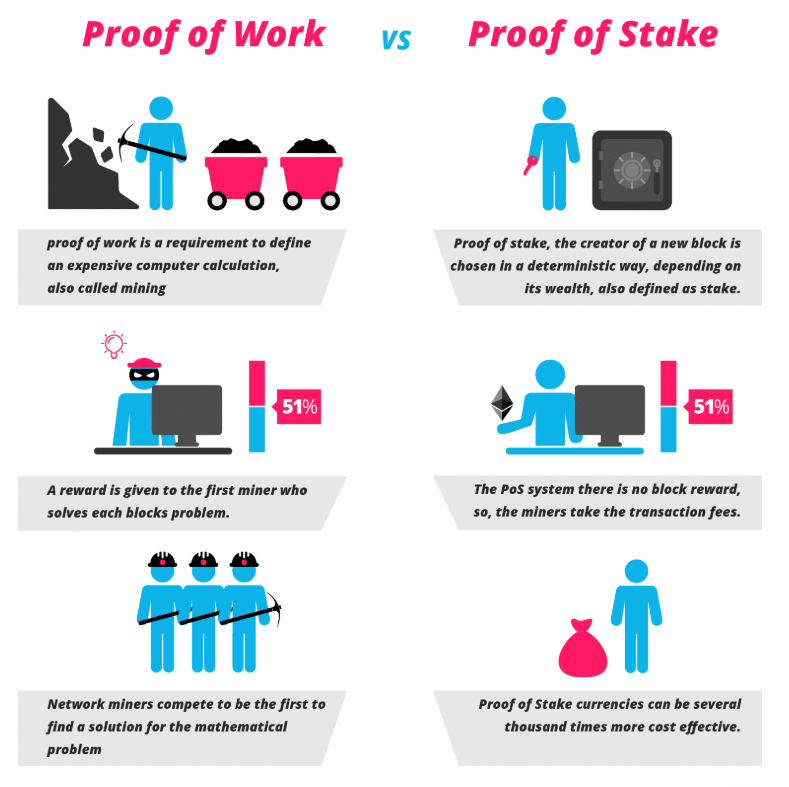
Như bạn có thể thấy, Casper được chỉ định làm việc trong một hệ thống không đáng tin cậy và có khả năng Chịu lỗi Byzantine nhiều hơn.

Bất kỳ ai hành động theo cách độc hại / Byzantine sẽ bị trừng phạt ngay lập tức bằng cách cắt cổ phần của họ. Đây là nơi nó khác với hầu hết các giao thức POS khác. Các phần tử độc hại có cái gì đó để mất nên không thể có chuyện không có gì bị đe dọa.

Việc triển khai Casper và Proof Of Stake một cách hoàn hảo sẽ rất quan trọng nếu Ethereum có kế hoạch mở rộng quy mô.

Tiền điện tử đáng chú ý sử dụng giao thức này: Ethereum (trong tương lai gần)

**2.5 Compare PoW vs PoW**



**2.6 Delegated proof-of-stake algorithm (DPoS): EOS**

Bây giờ chúng ta đến với một dạng Proof Of Stake thú vị được gọi là DPOS hoặc Proof Of Stake được ủy quyền. EOS đang sử dụng cơ chế đồng thuận này để mở rộng quy mô lên đến hàng triệu giao dịch mỗi giây.

Thứ nhất, bất kỳ ai nắm giữ token trên blockchain được tích hợp trong phần mềm EOS đều có thể chọn nhà sản xuất khối thông qua hệ thống bỏ phiếu phê duyệt liên tục. Bất kỳ ai cũng có thể tham gia vào cuộc bầu cử nhà sản xuất khối và họ sẽ có cơ hội tạo ra các khối tỷ lệ thuận với tổng số phiếu bầu mà họ nhận được so với tất cả các nhà sản xuất khác.

Làm thế nào nó hoạt động?

Các khối được sản xuất theo vòng 21.

Vào đầu mỗi vòng, 21 nhà sản xuất khối được chọn. Top 20 được chọn tự động trong khi người thứ 21 được chọn tỷ lệ thuận với số phiếu bầu của họ so với các nhà sản xuất khác.

Các nhà sản xuất sau đó được xáo trộn xung quanh bằng cách sử dụng một số giả ngẫu nhiên có được từ thời gian khối. Điều này được thực hiện để đảm bảo rằng sự kết nối cân bằng với tất cả các nhà sản xuất khác được duy trì.

Để đảm bảo duy trì quá trình sản xuất khối thường xuyên và thời gian khối được giữ ở mức 3 giây, các nhà sản xuất sẽ bị trừng phạt vì không tham gia bằng cách loại bỏ khỏi sự xem xét. Một nhà sản xuất phải sản xuất ít nhất một khối mỗi 24 giờ để được xem xét.

Hệ thống DPOS không trải qua một đợt fork vì thay vì cạnh tranh để tìm ra các khối, thay vào đó, các nhà sản xuất sẽ phải hợp tác. Trong trường hợp có fork, sự đồng thuận sẽ tự động chuyển sang chuỗi dài nhất.

Xác nhận giao dịch trong DPOS?

Một blockchain DPOS thường có 100% sự tham gia của nhà sản xuất khối. Một giao dịch thường được xác nhận trong vòng 1,5 giây kể từ thời điểm phát sóng bởi độ chắc chắn 99,9%. Để có sự chắc chắn tuyệt đối về tính hợp lệ của một giao dịch, một nút chỉ cần đợi 15/21 (tức là 2/3 đa số) nhà sản xuất đi đến thống nhất.

Vậy điều gì sẽ xảy ra trong trường hợp fork do sơ suất hoặc có ý đồ xấu?

Theo mặc định, tất cả các nút sẽ không chuyển sang một nhánh không bao gồm bất kỳ khối nào chưa được hoàn thiện bởi 15/21 nhà sản xuất. Điều này sẽ đúng bất kể độ dài chuỗi. Mỗi khối phải đạt được sự chấp thuận 15/21 để được coi là một phần của chuỗi.

Do thời gian tạo khối ngắn nên có thể cảnh báo các nút về việc chúng nằm trong chuỗi chính hay chuỗi phụ trong vòng 9 giây. Lý do tại sao điều đó rất đơn giản. Hãy nhớ rằng, thời gian trung bình trôi qua giữa mỗi khối là 3 giây.

Nếu một nút bỏ lỡ 2 khối liên tiếp, có 95% khả năng chúng nằm trong một nhánh nhỏ.

Nếu một nút bỏ lỡ 3 khối, thì có 99% khả năng chúng nằm trên một chuỗi thiểu số.

What is TAPOS?

Transaction As Proof Of Stake or TAPOS is a feature of the EOS software

Mọi giao dịch trong hệ thống bắt buộc phải có mã băm của tiêu đề khối gần đây. Điều này thực hiện như sau:

Ngăn chặn phát lại giao dịch trên các chuỗi khác nhau.

Báo hiệu cho mạng rằng người dùng và cổ phần của họ đang ở một nhánh cụ thể.

Điều này ngăn trình xác thực hành động có hại trên các chuỗi khác.

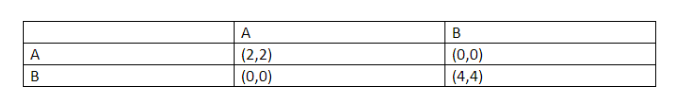
Ok, vậy nghe có vẻ khá hấp dẫn.

Bạn có một giao thức Proof-of-stake nhanh chóng và hiệu quả.

\*Where is the catch?

DPOS có thể fail với co-ordiation game theory

Co-ordination game theory là gì?



Bây giờ, nếu bạn nhìn thấy ma trận này, có hai Nash Equilibria: (A, A) và (B, B), độ lệch so với một trong hai trạng thái sẽ không có lợi cho chúng. Ý tưởng của trò chơi này là làm thế nào bạn có thể thuyết phục mọi người đi từ (A, A) đến (B, B)? Nếu có một nhóm nhỏ người tham gia thì điều đó tương đối đơn giản, bạn có thể điều phối đơn giản qua điện thoại hoặc email. Nhưng, điều này thay đổi khi chúng ta đang nói về một nhóm người khổng lồ.

Sự khác biệt cơ bản giữa tình thế tiến thoái lưỡng nan của tù nhân và vấn đề phối hợp là trong tình thế tiến thoái lưỡng nan của tù nhân, cả hai người chơi đều phải chọn (B, B) vì đó là lựa chọn có lợi nhất mặc dù (A, A) là giải pháp tốt hơn về mặt đạo đức . Trong vấn đề Phối hợp, nó không phải là về đạo đức hay sự đền đáp, nó là về động cơ thúc đẩy một người đi từ trạng thái này sang trạng thái khác. Tại sao một nhóm lớn người phải thay đổi cách họ làm việc?

Trò chơi phối hợp thất bại khi chỉ có thiểu số trong nhóm thay đổi trạng thái của họ còn đa số thì không và ngược lại, sẽ thành công khi đa số trong nhóm thay đổi trạng thái của họ. Hãy xem điều đó với một ví dụ.

Giả sử chúng ta muốn thay đổi ngôn ngữ thành ngôn ngữ dựa trên ký hiệu. Ví dụ:

Câu gốc: "Cho tôi số của bạn?"

Tuyên bố mới: “#?”

Nếu chỉ bạn nói bằng ngôn ngữ này thì sẽ là một thất bại vì đa số sẽ không hiểu bạn đang nói gì và bạn sẽ bị xa lánh khỏi các cuộc trò chuyện, tức là phần thưởng dành cho bạn rất thấp và bạn không có động lực để thay đổi.

Tuy nhiên, nếu phần lớn xã hội của bạn chuyển sang ngôn ngữ này và sử dụng nó độc quyền, bạn sẽ phải thay đổi ngôn ngữ của mình nếu không bạn sẽ không bao giờ có thể hòa nhập. Lúc này, động cơ để bạn tham gia là rất cao.

Hệ thống DPOS có thể sử dụng lý thuyết trò chơi phối hợp để gây bất lợi cho nó. Có thể xảy ra một tình huống trong đó một tình huống nhất định được các nhà sản xuất khối ưu tiên không phù hợp với phần còn lại của các nút.

Giả sử các nút chính muốn chuyển chuỗi từ trạng thái A sang trạng thái B. Đó có thể là một nhiệm vụ rất khó khăn đối với họ để giúp toàn bộ chuỗi thực hiện cùng một quá trình chuyển đổi cùng với chúng, đặc biệt nếu các nút khác trái ngược với trạng thái B.

Chỉ có thời gian mới trả lời được liệu EOS có thể tích hợp DPOS đúng cách và hoàn hảo hay không.

Tiền điện tử đáng chú ý sử dụng giao thức này: EOS

**2.7 Byzantine Fault Tolerance?**

Byzantine Fault Tolerance (BFT) là tính năng của mạng phân tán để đạt được sự đồng thuận (thỏa thuận về cùng giá trị) ngay cả khi một số nút trong mạng không phản hồi hoặc phản hồi với thông tin không chính xác. Mục tiêu của cơ chế BFT là bảo vệ chống lại các lỗi hệ thống bằng cách sử dụng việc ra quyết định tập thể (cả - nút đúng và nút bị lỗi) nhằm mục đích giảm ảnh hưởng của các nút bị lỗi. BFT có nguồn gốc từ Byzantine Generals ’Problem.

**2.7 pBFT: Zilliqa, Hyperledger Fabric, Tendermint**

Đồng thuận theo quy tắc đa số (tổng số node trả về cùng kết quả phải lớn hơn tổng số node lỗi trong hệ thống) (node lỗi là node không trả về cùng kết quả)

Một hệ thống Byzantine Fault Tolerant thực tế có thể hoạt động với điều kiện số lượng tối đa các nút độc hại không được lớn hơn hoặc bằng một phần ba tổng số các nút trong hệ thống.

Các nút chính có hể được thay thế nếu đủ điều kiện khi có nút chính khác bị lỗi

Các vòng đồng thuận pBFT được chia thành 4 giai đoạn (tham khảo hình ảnh bên dưới):

Máy khách gửi một yêu cầu đến nút chính (lãnh đạo).

Nút chính (đầu tàu) phát yêu cầu đến tất cả các nút phụ (dự phòng).

Các nút (chính và phụ) thực hiện dịch vụ được yêu cầu và sau đó gửi lại phản hồi cho khách hàng.

Yêu cầu được phục vụ thành công khi máy khách nhận được phản hồi ‘**m + 1**’ từ các nút khác nhau trong mạng với cùng kết quả, trong đó m là số lượng nút bị lỗi tối đa được phép.

**2.8 dBFT: NEO**

Thoạt nhìn, cơ chế đồng thuận dBFT tương tự như Proof-of-Stake được ủy quyền dPOS. Sử dụng quy trình bỏ phiếu, chủ sở hữu mã thông báo NEO có quyền bỏ phiếu cho các đại biểu. Điều này không phụ thuộc vào số lượng tiền tệ mà họ sở hữu.

Bất kỳ ai cũng có thể trở thành đại biểu, miễn là người đó đáp ứng các yêu cầu. Điều này có nghĩa là kết nối internet đáng tin cậy, thiết bị phù hợp, danh tính đã được xác thực và 1.000 GAS. GAS là phần thưởng mà người dùng nhận được cho hoạt động của họ trên mạng. Từ các đại biểu, một diễn giả (speaker) được chọn ngẫu nhiên.

Người nói xây dựng một khối mới từ các giao dịch đang chờ được xác thực. Sau đó, diễn giả gửi đề xuất đến các đại biểu được bầu. Họ dự kiến ​​sẽ theo dõi tất cả các giao dịch và ghi lại chúng trên mạng.

Các đại biểu có thể tự do chia sẻ và so sánh đề xuất mà họ đã nhận được để kiểm tra độ chính xác của dữ liệu, cũng như tính trung thực của speaker. Khối được thêm vào blockchain nếu hơn 2/3 số đại biểu đạt được sự đồng thuận và xác nhận nó.

Bỏ phiếu trong mạng NEO là một quá trình diễn ra trong thời gian thực.

**2.9 PoA: NEO**

Kết hợp trung gian PoW và PoS. Lúc đầu PoW sau khi miner tìm ra block mới thì chọn ra validator để thực hiện xác nhận PoS. Phần thưởng chia cho miner và validator. PoA khắc phụ nhược điểm cả 2 cũng như kết hợp ưu điểm cả 2.

**2.10 LPoS: WAVES**

Cho vay token để tăng Stake trong PoS từ đó tăng cơ hội validate để nhận fees. Các WAVES đã cho thuê bị khóa trong tài khoản người dùng và không thể chuyển nhượng hoặc giao dịch. Tuy nhiên, các token vẫn nằm trong sự kiểm soát hoàn toàn của chủ tài khoản và hợp đồng thuê có thể bị hủy bất cứ lúc nào

**2.11 PoC (bộ nhớ): BURSTCOIN**

Bằng chứng về năng lực cho phép các thiết bị khai thác (nút) trên mạng blockchain có khả năng sử dụng không gian trống trên ổ cứng của chúng để khai thác các loại tiền điện tử có sẵn. Thay vì liên tục thay đổi các số nonce trong tiêu đề khối và băm lặp lại cho giá trị giải pháp, POC hoạt động bằng cách lưu trữ danh sách các giải pháp khả thi trên ổ cứng của thiết bị khai thác ngay cả trước khi hoạt động khai thác bắt đầu.

**2.12 PoI: NEM**

Bằng chứng quan trọng, càng giao dịch nhiều thì cơ hội được xác nhận nhiều hơn.

**2.13 PoAuthority**

ĐỊnh danh tính ngoài đời thực để thực hiện việc xác thực các transaction

**2.14 PoB: SLIMCOIN**

Proof of burn (POB) là một thuật toán đồng thuận thay thế cố gắng giải quyết vấn đề tiêu thụ năng lượng cao của hệ thống POW.

POB thường được gọi là hệ thống POW không lãng phí năng lượng. Nó hoạt động trên nguyên tắc cho phép các thợ mỏ “đốt” các token tiền ảo. Sau đó, họ được cấp quyền viết các khối tương ứng với số tiền bị cháy.

Iain Stewart, người phát minh ra thuật toán POB, sử dụng một phép tương tự để mô tả thuật toán: các đồng tiền bị cháy giống như các giàn khai thác. Tương tự như vậy, một người khai thác đốt tiền của họ để mua một giàn khai thác ảo cung cấp cho họ sức mạnh để khai thác các khối. Người khai thác càng đốt nhiều coin thì "giàn" khai thác ảo của họ sẽ càng lớn.

Để đốt tiền, các thợ đào gửi chúng đến một địa chỉ không thể chi tiêu có thể xác minh được. Quá trình này không tiêu tốn nhiều tài nguyên (ngoài số tiền đã đốt) và đảm bảo rằng mạng vẫn hoạt động và nhanh nhẹn. Tùy thuộc vào việc triển khai, các thợ đào được phép đốt tiền bản địa hoặc tiền tệ của một chuỗi thay thế, chẳng hạn như Bitcoin. Đổi lại, họ nhận được phần thưởng bằng mã thông báo tiền tệ bản địa của blockchain.

Bạn có thể gửi các giao dịch đến mạng sẽ đốt các đồng tiền điện tử của riêng bạn. Những người tham gia khác có thể khai thác / ghi trên đầu khối của bạn và bạn cũng có thể lấy các giao dịch của những người tham gia khác để thêm họ vào khối của bạn. Về cơ bản, tất cả hoạt động đốt này giữ cho mạng hoạt động nhanh và những người tham gia được thưởng cho các hoạt động của họ (cả đốt tiền của chính họ và đốt tiền của người khác).

Để ngăn chặn khả năng có những lợi thế không công bằng cho những người chấp nhận sớm, hệ thống POB đã triển khai một cơ chế thúc đẩy việc đốt các đồng tiền mã hóa định kỳ để duy trì sức mạnh khai thác. Sức mạnh của các đồng tiền bị cháy "phân rã" hoặc giảm một phần mỗi khi một khối mới được khai thác. Điều này thúc đẩy hoạt động thường xuyên của các thợ đào, thay vì đầu tư một lần, sớm. Để duy trì lợi thế cạnh tranh, các thợ đào cũng có thể cần đầu tư định kỳ vào thiết bị tốt hơn khi công nghệ tiến bộ.

**2.15 PoET**

Xổ số công bằng cho ngủ thời gian random khi vẫn dựa vào PoW

POET là một thuật toán cơ chế đồng thuận thường được sử dụng trên các mạng blockchain được cấp phép để quyết định quyền khai thác hoặc người chiến thắng khối trên mạng. Các mạng blockchain được phép là những mạng yêu cầu bất kỳ người tham gia tiềm năng nào phải xác định danh tính bản thân trước khi họ được phép tham gia. Dựa trên nguyên tắc của một hệ thống xổ số công bằng trong đó mọi nút đơn lẻ đều có khả năng là người chiến thắng như nhau, cơ chế POET dựa trên việc chia đều cơ hội chiến thắng cho số lượng người tham gia mạng lớn nhất có thể.

Hoạt động của thuật toán POET như sau. Mỗi nút tham gia trong mạng được yêu cầu đợi trong một khoảng thời gian được chọn ngẫu nhiên và nút đầu tiên hoàn thành thời gian chờ được chỉ định sẽ thắng khối mới. Mỗi nút trong mạng blockchain tạo ra thời gian chờ ngẫu nhiên và chuyển sang chế độ ngủ trong khoảng thời gian được chỉ định đó. Người thức dậy đầu tiên - tức là người có thời gian chờ ngắn nhất - thức dậy và cam kết một khối mới cho chuỗi khối, phát thông tin cần thiết cho toàn bộ mạng ngang hàng. Quá trình tương tự sau đó lặp lại để phát hiện ra khối tiếp theo .

Cơ chế đồng thuận mạng POET cần đảm bảo hai yếu tố quan trọng. Đầu tiên, các nút tham gia thực sự chọn thời gian thực sự là ngẫu nhiên và không phải là khoảng thời gian ngắn hơn do những người tham gia cố ý chọn để giành chiến thắng và hai, người chiến thắng đã thực sự hoàn thành thời gian chờ đợi.