

Hiến pháp Cardano

MỞ ĐẦU

Chuỗi khối Cardano là một giao thức phần mềm cho phép phát triển các hợp đồng, ứng dụng và tài sản kỹ thuật số theo cách phi tập trung, không cần cấp phép.. Cardano, được đặt theo tên nhà toán học thế kỷ 16 Girolamo Cardano, được ra mắt tại Nhật Bản vào năm 2017. Ba nhà sáng lập tiên phong của nó là Input Output Hong Kong, Emurgo và Cardano Foundation đã chọn đánh giá ngang hàng làm phương pháp phát triển chuỗi khối nguồn mở an toàn, có thể mở rộng và phi tập trung.

Quản trị trên chuỗi ban đầu đã sử dụng các tham số trên chuỗi cũng như các quyết định ngoài chuỗi được đưa ra theo đa số phiếu bầu của những người sáng lập, những người nắm giữ bảy khóa gốc cho phép họ thực hiện các thay đổi đã thống nhất đối với giao thức. Những người sáng lập đã lấy ý kiến về sự phát triển của Cardano từ các nhà khoa học, chuyên gia học thuật, nhà phát triển và nhiều người khác, bao gồm cả những người nắm giữ ADA, loại tiền tệ bản địa của blockchain. Từ việc tạo ra sách trắng của Cardano, mục đích là phân quyền hoàn toàn việc quản trị.

Vào ngày __ tháng 9 năm 2024, một cột mốc quan trọng đã được hiện thực hóa khi chìa khóa nguồn gốc được chuyển giao cho các thành viên cộng đồng trên toàn thế giới, được bầu vào Ủy ban Hiến pháp đầu tiên của cộng đồng. Mục tiêu của Hiến pháp này là đặt ra một khuôn khổ quản trị nhằm giữ cho hệ sinh thái chuỗi khối Cardano tồn tại và phát triển cho các thế hệ mai sau.

Điều 1 - NGUYÊN TẮC

Phần 1

Những nguyên tắc này rất quan trọng đối với cộng đồng trong việc duy trì và phát triển chuỗi khối Cardano và các hành động quản trị được đề xuất sẽ được đánh giá theo chúng.

Hệ sinh thái blockchain Cardano có quyền tồn tại. Để nó phát triển mạnh, các hành động quản trị cần cố gắng cải thiện quy mô, hiệu quả và tốc độ giao dịch mà không ảnh hưởng quá mức đến an ninh và phân cấp.

Chi phí giao dịch trên Cardano Blockchain phải dựa trên mô hình định giá có thể truy cập và dự đoán được.

Chuỗi khối Cardano sẽ thúc đẩy khả năng tương tác với các giao thức chuỗi khối khác bao gồm chuỗi bên và chuỗi đối tác.

Cardano Blockchain sẽ luôn cố gắng để lưu giữ tất cả các giao dịch trên blockchain và thông tin trên chuỗi đi kèm của chúng.

Cardano Blockchain sẽ duy trì Kho bạc ADA được quản lý theo tài liệu này.

Cardano Blockchain sẽ thúc đẩy thiết kế, bộ nhớ và lưu trữ hiệu quả.

Chuỗi khối Cardano sẽ tiếp tục sử dụng ADA làm tiền tệ cơ bản.

Chuỗi khối Cardano sẽ không có hành động nào nhằm hạn chế nguồn cung ADA hiện tại là 45 tỷ token.

Chuỗi khối Cardano sẽ không thực hiện hành động nào nhằm loại bỏ quyền giữ ADA trong ví của chính họ theo cách không khóa mà không có sự đồng ý của chủ sở hữu ADA đó.

Trừ khi có thỏa thuận khác trong bản sửa đổi Hiến pháp này, chuỗi khối Cardano sẽ tiếp tục hoạt động thông qua cơ chế đồng thuận bằng chứng cổ phần, nhưng có thể hợp tác với các chuỗi hoạt động bằng bằng chứng công việc hoặc các cơ chế đồng thuận khác.

Phần 2

Cardano Blockchain sẽ hoạt động theo các Tám chấn bảo vệ Blockchain Cardano như được quy định trong Điều VII.. Cộng đồng Cardano có thể mã hóa các tám chấn bảo vệ Cardano Blockchain bằng kỹ thuật số.cái cho phép triển khai chúng trên blockchain bằng cách sử dụng các tập lệnh trên chuỗi hoặc quy tắc số cái tích hợp. Nếu có thể, việc triển khai trên chuỗi là mong muốn và được khuyến khích.

Trong trường hợp không nhất quán và giữa một lan can trong Hiến pháp này và Một Guardrail được lập trình và triển khai trên blockchain, phiên bản được triển khai trên blockchain sẽ được ưu tiên áp

dụng và Ủy ban Hiến pháp sẽ tìm cách giải quyết sự không nhất quán đó và thông qua hành động quản trị trên chuỗi.

Điều II - CỘNG ĐỒNG BLOCKCHAIN CARDANO

Phần 1

Không cần phải là thành viên chính thức để nắm giữ ADA hoặc tham gia vào hệ sinh thái Cardano Blockchain. Tất cả chủ sở hữu ADA đều là người thụ hưởng hệ sinh thái Cardano Blockchain.

Phần 2

Các thành viên của cộng đồng Cardano sở hữu ADA có quyền truy cập và tham gia vào quá trình ra quyết định trực tuyến của hệ sinh thái blockchain, trực tiếp hoặc thông qua việc bổ nhiệm các đại biểu theo Hiến pháp này, bao gồm cả việc bỏ phiếu theo Hiến pháp này..

Điều III - KHUNG QUẢN TRỊ

Phần 1

Hệ sinh thái Cardano Blockchain sẽ sử dụng mô hình quản trị trên chuỗi, phi tập trung để đưa ra quyết định về các thay đổi đối với chuỗi khối hoặc quản trị của nó, sử dụng, trong phạm vi có thể và có lợi, các hợp đồng "thông minh" có thể lập trình và các công cụ dựa trên chuỗi khối khác để hỗ trợ việc ra quyết định. và đảm bảo tính minh bạch. Việc bỏ phiếu trực tuyến cho các hoạt động quản trị sẽ tuân theo các quy trình được nêu trong Hiến pháp này.

Phần 2

Ba cơ quan quản trị đã được thành lập để tham gia bỏ phiếu trên Cardano Blockchain. Những người này bao gồm các Đại diện được ủy quyền (DReps), Người điều hành nhóm cổ phần (SPO) và Ủy ban Hiến pháp (CC). Hoạt động với tư cách là thành viên của nhiều nhóm trong số này sẽ thúc đẩy sự tập trung hóa và có thể dẫn đến xung đột lợi ích gây tổn hại cho blockchain. Do đó, các hành động quản trị được ưu tiên nhằm ngăn cản các bên giống nhau nắm giữ nhiều hơn một vị trí trong quản trị hoặc cho phép các bên tiết lộ những xung đột tiềm ẩn và tránh bỏ phiếu có khả năng xung đột.

DReps, SPO và thành viên Ủy ban Hiến pháp có thể là chủ sở hữu ADA cá nhân hoặc chủ sở hữu ADA đã tổ chức thành một nhóm.

Các SPO của DReps và các thành viên Ủy ban Hiến pháp nhất thiết sẽ phải chịu phí giao dịch để bỏ phiếu. Sẽ không vi hiến nếu cộng đồng bỏ phiếu yêu cầu hoàn trả các khoản phí đó hoặc đền bù cho thời gian đã bỏ ra để hoạt động với tư cách là DRep miễn là việc phân bổ cho việc đó được thực hiện trong phạm vi ngân sách được phê duyệt.

.

Phần 3

Các quyết định quản trị trên chuỗi sẽ được đưa ra thông qua quy trình ra quyết định tập thể, với các yêu cầu về ngưỡng đồng thuận cụ thể theo yêu cầu của Điều VII của Hiến pháp này, Các rào chắn của Cardano Blockchain. Tất cả các hành động quản trị trên chuỗi sẽ được biểu quyết theo các Guardrails đó.

Trừ khi được quy định trong Các rào cản tạm thời của Điều VII, mọi cuộc bỏ phiếu quản trị phải được hai trong ba cơ quan quản lý phê chuẩn, theo tỷ lệ phần trăm được quy định trong Hiến pháp này.

Phần 4

Một hình thức hành động quản trị đặc biệt tồn tại để đánh giá tình cảm của cộng đồng mà không cần cam kết thay đổi chuỗi Cardano. Những cái này "Tinfo" không có tác dụng trên chuỗi ngoài việc ghi lại kết quả của cuộc bỏ phiếu trên blockchain.

Phần 5

Bất kỳ hành động quản trị trên chuỗi nào được đề xuất đều phải yêu cầu định dạng được tiêu chuẩn hóa và dễ đọc, bao gồm URL và hàm băm được liên kết với nội dung ngoài chuỗi được ghi lại. Cơ sở lý luận sẽ được cung cấp để biện minh cho sự thay đổi được yêu cầu đối với chuỗi khối. Cơ sở lý

luận tối thiểu phải bao gồm tiêu đề, bản tóm tắt, lý do đưa ra đề xuất và các tài liệu hỗ trợ có liên quan.

Bất kỳ đề xuất hành động quản trị nào đạt đến giai đoạn quản trị trên chuỗi sẽ có nội dung giống hệt với phiên bản ngoài chuỗi cuối cùng của đề xuất hành động quản trị đó.

Các hành động quản trị “Khởi tạo Hard Fork” và “Thay đổi tham số giao thức” sẽ trải qua quá trình xem xét và giám sát kỹ thuật theo yêu cầu của Guardrails để đảm bảo rằng hành động quản trị đó không gây nguy hiểm cho tính bảo mật, chức năng hoặc hiệu suất của Cardano Blockchain. Các hành động quản trị trên chuỗi sẽ giải quyết tác động dự kiến của chúng đối với hệ sinh thái blockchain.

Phần 6

Cộng đồng Cardano dự kiến sẽ đề xuất, ít nhất là hàng năm, *(cũng không nhiều hơn trên cơ sở ____?)* ngân sách dành cho việc bảo trì liên tục và phát triển trong tương lai của Cardano Blockchain. Ngân sách sẽ được bỏ phiếu thông qua bỏ phiếu trực tuyến. Không được phép rút tiền từ kho bạc Cardano trừ khi ngân sách cho Cardano Blockchain có hiệu lực.

[Bất kỳ hành động quản trị nào yêu cầu ADA từ kho bạc Cardano Blockchain vượt quá [1.000.000] ADA sẽ yêu cầu phân bổ ADA như một phần của yêu cầu tài trợ đó để trang trải chi phí kiểm toán độc lập định kỳ và việc thực hiện các số liệu giám sát đối với việc sử dụng ADA đó.] [Các nghĩa vụ hợp đồng quản lý việc sử dụng ADA nhận được từ kho bạc Cardano Blockchain theo ngân sách Cardano vượt quá [1.000.000] sẽ bao gồm các điều khoản giải quyết tranh chấp.]?

Điều IV - ĐẠI DIỆN ĐƯỢC ỦY QUYỀN

Phần 1

Để tham gia bỏ phiếu trực tuyến, chủ sở hữu ADA phải đăng ký với tư cách là DRep để bỏ phiếu trực tiếp về các hoạt động quản trị hoặc ủy quyền quyền biểu quyết của họ cho các DRep đã đăng ký khác, những người sẽ thay mặt họ bỏ phiếu.

Phần 2

Bất kỳ chủ sở hữu ADA nào cũng có tùy chọn đăng ký làm DRep. Bất kỳ chủ sở hữu ADA nào cũng được phép ủy quyền cổ phần biểu quyết của họ cho một hoặc nhiều DRep đã đăng ký, bao gồm cả chính họ. DReps có thể là cá nhân hoặc nhóm phối hợp. DReps có quyền bỏ phiếu trực tiếp cho các hành động quản trị trên chuỗi và đại diện cho những chủ sở hữu ADA ủy quyền quyền biểu quyết cho họ. Hệ thống bỏ phiếu này sẽ cung cấp một mô hình dân chủ linh hoạt trong đó chủ sở hữu ADA có thể lựa chọn liên mạch giữa các DReps, đăng ký làm DRep và thay đổi ủy quyền của họ bất cứ lúc nào.

Phần 3

DReps có thể chọn áp dụng các quy tắc ứng xử quản lý các hoạt động của họ với tư cách là DReps và công khai các quy tắc ứng xử đó. Tuy nhiên, các quy tắc ứng xử đó không bắt buộc phải rõ ràng và hy vọng rằng bất kỳ quy tắc ứng xử nào có thể được thông qua sẽ xem xét khả năng thực thi của nó trên toàn cầu. khu vực pháp lý cũng như các mục tiêu được nêu trong tài liệu này.

Phần 4

DReps sẽ có quyền hành động **BẰNG** kiểm tra quyền lực của Ủy ban Hiến pháp trong những trường hợp đặc biệt bằng cách bỏ phiếu về các hoạt động quản trị “Đề nghị bất tín nhiệm” và “Cập nhật ủy ban/ngưỡng”, như được mô tả trong tài liệu này..

Điều V - NGƯỜI ĐIỀU HÀNH CỔ PHẦN

Phần 1

Nhà điều hành nhóm cổ phần (SPO) là một cá nhân hoặc tổ chức chịu trách nhiệm vận hành nhóm cổ phần, tham gia vào cơ chế đồng thuận của Cardano Blockchain. SPO sẽ có vai trò cụ thể trong việc phê duyệt các hoạt động quản trị quan trọng trên chuỗi, đòi hỏi sự giám sát bổ sung và tính độc

lập, bỏ phiếu như được quy định trong Hiến pháp này. SPO sẽ tham gia vào quá trình khởi tạo hard fork với tư cách là người vận hành các nút tham gia vào cơ chế đồng thuận của Cardano Blockchain.

Phần 2

SPO sẽ có quyền hành động *BĂNG* kiểm tra quyền lực của Ủy ban Hiến pháp trong những trường hợp đặc biệt bằng cách bỏ phiếu về các hoạt động quản trị "Đề nghị bất tín nhiệm" và "Cập nhật ủy ban/ngưỡng", như được mô tả trong tài liệu này..

Điều VI - ỦY BAN Hiến Pháp

Phần 1

Một Ủy ban Hiến pháp sẽ được thành lập để đảm bảo rằng các hoạt động quản lý phù hợp với Hiến pháp này. Ủy ban Hiến pháp sẽ bao gồm chủ sở hữu của ADA chịu trách nhiệm đảm bảo rằng các hành động quản trị trên chuỗi trước khi ban hành trên chuỗi là hợp hiến. Ủy ban Hiến pháp sẽ bị giới hạn trong việc bỏ phiếu về tính hợp hiến của các hoạt động quản trị.

Phần 2

Ủy ban Hiến pháp sẽ được thành lập theo Hiến pháp này và các thành viên sẽ có nhiệm kỳ phù hợp với Hiến pháp này, với điều kiện là nhiệm kỳ không được ít hơn một năm trừ khi được chấp thuận khác bằng cách bỏ phiếu theo dây chuyền.. Để đảm bảo tính liên tục trong hoạt động của Ủy ban Hiến pháp, nhiệm kỳ của các thành viên Ủy ban Hiến pháp sẽ được thay đổi so le. Trong trường hợp kiến nghị bất tín nhiệm yêu cầu phải thay thế ngay các thành viên Ủy ban Hiến pháp thì ngày kết thúc của mỗi nhiệm kỳ sẽ được giữ nguyên đối với các thành viên mới, trừ khi có thỏa thuận khác.

Phần 3

Việc bầu chọn các thành viên vào Ủy ban Hiến pháp được thực hiện theo các yêu cầu của Điều lệ này.

Phần 4

Không có hành động quản trị nào, ngoại trừ "Động thái bất tín nhiệm" hoặc "Cập nhật ủy ban/ngưỡng hiến pháp" có thể được thực hiện trực tuyến trừ khi Ủy ban Hiến pháp trước tiên xác định và khẳng định thông qua hành động trực tuyến rằng đề xuất đó không vi phạm Hiến pháp này.

Ủy ban Hiến pháp luôn được coi là ở một trong hai trạng thái sau: trạng thái tín nhiệm hoặc trạng thái bất tín nhiệm. Trong tình trạng bất tín nhiệm, các thành viên của Ủy ban Hiến pháp thường trực khi đó phải được phục hồi hoặc thay thế bằng hành động quản trị "Cập nhật ủy ban/ngưỡng" trước khi bất kỳ hành động quản trị on-chain nào khác có thể được tiến hành.

Phần 5

Ủy ban Hiến pháp sẽ công bố từng quyết định. Khi bỏ phiếu chống lại một đề xuất, một thành viên sẽ đặt ra cơ sở cho quyết định của mình dựa trên các Điều khoản cụ thể của Hiến pháp này mâu thuẫn với một đề xuất nhất định.

Điều VII - TÀI BẢO VỆ BLOCKCHAIN

Phần 1

Để triển khai quản trị trên chuỗi Cardano Blockchain, cần phải thiết lập các biện pháp bảo vệ cho phép Cardano Blockchain tiếp tục hoạt động một cách an toàn và bền vững.

Các biện pháp bảo vệ này áp dụng cho môi trường mạng chính Cardano Blockchain Lớp 1. Chúng không nhằm mục đích áp dụng cho môi trường thử nghiệm hoặc cho các chuỗi khối khác sử dụng phần mềm Cardano Blockchain.

Không phải tất cả các tham số của Cardano Blockchain đều có thể được xem xét độc lập. Một số tham số tương tác với các cài đặt khác theo cách nội tại. Khi đã biết, những tương tác này sẽ được đề cập ở đây. Mặc dù các lan can hiện phản ánh hiện trạng hiểu biết kỹ thuật hiện tại nhưng Điều khoản này phải được coi như một tài liệu sống. Các cải tiến triển khai, mô phỏng mới hoặc kết quả đánh giá hiệu suất cho Cardano Blockchain có thể cho phép nói lỏng một số hạn chế trong các biện pháp bảo vệ này (hoặc, trong một số trường hợp, yêu cầu chúng phải được thắt chặt) theo thời gian thích hợp.

Các biện pháp bảo vệ bổ sung cũng có thể cần thiết khi các thông số giao thức mới được đưa vào chẳng hạn.

Các rào chắn được nêu trong Điều này có thể được sửa đổi theo hành động quản trị trên chuỗi đáp ứng ngưỡng biểu quyết hiện hành như được quy định trong Hiến pháp này. Bất kỳ sửa đổi nào như vậy đối với bất kỳ lan can nào sẽ yêu cầu và được coi là sửa đổi Hiến pháp.

Thuật ngữ và hướng dẫn

Nên/Không nên. Khi Điều này nói rằng một giá trị "không nên" được đặt dưới hoặc trên một giá trị nào đó, điều này có nghĩa rằng lan can là một khuyến nghị hoặc hướng dẫn và giá trị cụ thể có thể được đưa ra để thảo luận hoặc thay đổi bởi một nhóm chuyên gia phù hợp được công nhận bởi Cộng đồng Cardano dựa trên kinh nghiệm với hệ thống quản trị Cardano Blockchain hoặc hoạt động của Cardano Blockchain.

Phải/Không được. Khi Điều này nói rằng một giá trị "không được" được đặt dưới hoặc trên một số giá trị, điều này có nghĩa là lan can là một yêu cầu sẽ được thực thi bởi các quy tắc, loại sổ cái Cardano Blockchain hoặc các cơ chế tích hợp khác nếu có thể và rằng nếu không tuân theo có thể gây ra lỗi giao thức, vi phạm an ninh hoặc kết quả không mong muốn khác.

Điểm chuẩn. Đo điểm chuẩn đề cập đến việc đánh giá hiệu suất ở cấp độ hệ thống một cách cẩn thận được thiết kế để hiển thị trước rằng, chẳng hạn, 95% khối sẽ được phân tán trên mạng lưới các nút Cardano Blockchain toàn cầu trong khoảng thời gian 5 giây bắt buộc trong mọi trường hợp. Điều này có thể yêu cầu xây dựng các quy trình kiểm tra cụ thể và thực thi trên mạng thử nghiệm lớn gồm các nút Cardano, mô phỏng mạng Blockchain Cardano toàn cầu.

Phân tích hiệu suất. Phân tích hiệu suất đề cập đến việc dự đoán hiệu suất lý thuyết, điểm chuẩn thực nghiệm hoặc kết quả mô phỏng để dự đoán hoạt động thực tế của hệ thống. Ví dụ: kết quả hiệu suất thu được từ các thử nghiệm trong môi trường thử nghiệm được kiểm soát (chẳng hạn như tập hợp các trung tâm dữ liệu có thuộc tính mạng đã biết) có thể được ngoại suy để thông báo hành vi hiệu suất có thể xảy ra trong môi trường mạng Cardano Blockchain thực.

Mô phỏng. Mô phỏng đề cập đến việc thực thi tổng hợp được thiết kế để đưa ra các quyết định về hiệu suất/chức năng theo cách có thể lặp lại. Ví dụ: mô-đun Blockchain IOSim Cardano cho phép hoạt động của ngăn xếp mạng được mô phỏng theo cách có thể kiểm soát và lặp lại, cho phép phát hiện các vấn đề trước khi triển khai mã.

Giám sát hiệu suất. Giám sát hiệu suất liên quan đến việc đo lường hành vi thực tế của mạng Cardano Blockchain, chẳng hạn như bằng cách sử dụng đầu dò thời gian để đánh giá thời gian khứ hồi hoặc các khối kiểm tra để đánh giá tình trạng tổng thể của mạng. Nó bổ sung cho việc đo điểm chuẩn và phân tích hiệu suất bằng cách cung cấp thông tin về hoạt động thực tế của hệ thống mà không thể có được bằng cách sử dụng khối lượng công việc mô phỏng hoặc phân tích lý thuyết.

Hoàn nguyên các thay đổi. Khi giám sát hiệu suất cho thấy hành vi mạng thực tế sau một thay đổi không nhất quán với các yêu cầu về hiệu suất đối với Cardano Blockchain thì thay đổi đó phải được hoàn nguyên về trạng thái trước đó nếu có thể. Ví dụ: nếu kích thước khối được tăng từ 100KB lên 120KB và 95% khối không còn được phân tán trong vòng 5 giây thì phải thực hiện thay đổi để hoàn nguyên kích thước khối về 100KB. Nếu điều này là không thể thì phải thực hiện một hoặc nhiều thay đổi thay thế để đảm bảo đáp ứng các yêu cầu về hiệu suất.

Mức độ nghiêm trọng. Các vấn đề ảnh hưởng đến mạng Blockchain Cardano được phân loại theo mức độ nghiêm trọng, trong đó:

Mức độ nghiêm trọng 1 là sự cố hoặc sự cố nghiêm trọng có tác động rất lớn đến bảo mật, hiệu suất hoặc chức năng của mạng Blockchain Cardano.

Mức độ nghiêm trọng 2 là một sự cố hoặc sự cố lớn có tác động đáng kể đến tính bảo mật, hiệu suất hoặc chức năng của mạng Blockchain Cardano.

Mức độ nghiêm trọng 3 là một sự cố hoặc sự cố nhỏ có tác động thấp đến tính bảo mật, hiệu suất hoặc chức năng của mạng Blockchain Cardano.

Yêu cầu về hiệu suất trong tương lai. Sự phát triển theo kế hoạch, chẳng hạn như cơ chế mới cho việc lưu trữ ngoài bộ nhớ, có thể ảnh hưởng đến việc phổ biến khối hoặc những thời điểm khác. Khi

thay đổi tham số, cần phải xem xét các yêu cầu về hiệu suất trong tương lai cũng như hoạt động hiện tại của Cardano Blockchain. Cho đến khi quá trình phát triển hoàn tất, các yêu cầu sẽ ở mức thận trọng; sau đó chúng có thể được thoải mái để giải thích cho hành vi tính thời gian thực tế.

Kiểm tra tự động ("Tập lệnh Guardrails")

Một hàm băm tập lệnh được liên kết với hàm băm hiện pháp khi một **Hiến pháp mới hoặc Tập lệnh bảo vệ** hoạt động quản lý được ban hành. Nó hoạt động như một biện pháp bảo vệ bổ sung cho các quy tắc và loại sổ cái, lọc các hành động quản trị không tuân thủ.

Tập lệnh lan can chỉ ảnh hưởng đến hai loại hành động quản trị:

Cập nhật thông số hành động và

Rút tiền kho bạc hành động.

Tập lệnh được thực thi khi một trong hai loại hành động quản trị này được gửi trực tuyến. Điều này tránh các tình huống, chẳng hạn như một tập lệnh sai có thể ngăn chuỗi thực hiện hành động Hard Fork, dẫn đến bế tắc. Có ba tình huống khác nhau áp dụng cho việc sử dụng tập lệnh.

Ký hiệu và giải thích

(y) Tập lệnh có thể được sử dụng để thực thi lan can.

(x) Không thể sử dụng tập lệnh để thực thi lan can.

(~ - lý do) Không thể sử dụng tập lệnh để thực thi lan can vì lý do đã đưa ra, nhưng những thay đổi sổ cái trong tương lai có thể kích hoạt điều này.

Các lan can có thể chồng lên nhau: trong trường hợp này, bộ lan can hạn chế nhất sẽ được áp dụng. Khi một tham số không được liệt kê rõ ràng trong tài liệu này thì tập lệnh **không được** cho phép bất kỳ thay đổi nào đối với tham số.

Ngược lại, khi một tham số được liệt kê rõ ràng trong tài liệu này nhưng không chỉ rõ các rào cản có thể kiểm tra thì tập lệnh **không được** áp đặt bất kỳ ràng buộc nào đối với những thay đổi đối với tham số.

2. HƯỚNG DẪN VÀ HƯỚNG DẪN VỀ CÁC HÀNH ĐỘNG CẬP NHẬT THAM SỐ GIAO THỨC

Dưới đây là các biện pháp bảo vệ và hướng dẫn để thay đổi cài đặt tham số giao thức có thể cập nhật thông qua hành động quản trị cập nhật tham số giao thức để Cardano Blockchain không bao giờ ở trạng thái không thể phục hồi do những thay đổi đó.

Lưu ý rằng có ít nhất năm nguồn tên tham số khác nhau và những nguồn này không phải lúc nào cũng nhất quán:

Tên được sử dụng trong tệp Genesis

Tên được sử dụng trong các hành động quản trị cập nhật tham số giao thức

Tên được sử dụng nội bộ trong quy tắc sổ cái

Tên được sử dụng trong đặc tả sổ cái chính thức

Tên sử dụng trong tài liệu nghiên cứu

Khi các tên tham số này khác nhau, Điều này sử dụng quy ước thứ hai.

Lan can

PARAM-01 (y) Bất kỳ tham số giao thức nào không được nêu tên rõ ràng trong tài liệu này **không được** được thay đổi bởi hành động quản trị cập nhật Thông số.

PARAM-02 (y) Trong trường hợp một tham số giao thức được liệt kê rõ ràng trong tài liệu này nhưng không có các bước bảo vệ có thể kiểm tra nào được chỉ định, thì tập lệnh các bước bảo vệ **không được** áp đặt bất kỳ ràng buộc nào đối với những thay đổi đối với tham số. Lan can có thể kiểm tra được thể hiện bằng (y).

2.1. Thông số giao thức quan trọng

Các tham số giao thức dưới đây rất quan trọng xét từ quan điểm bảo mật.

Các thông số quan trọng đối với hoạt động của Blockchain

kích thước cơ thể khối tối đa (*maxBlockBodySize*)
quy mô giao dịch tối đa (kích thước tối đaTxSize)
kích thước tiêu đề khối tối đa (kích thước *maxBlockHeader*)
kích thước tối đa của giá trị tài sản được tuần tự hóa (*maxValueSize*)
đơn vị bộ nhớ/thực thi tập lệnh tối đa trong một khối (*maxBlockExecutionUnits[bước/bộ nhớ]*)
hệ số phí tối thiểu (*txFeePerByte*)
hằng số phí tối thiểu (*txFeeFixed*)
phí tối thiểu mỗi byte cho các tập lệnh tham chiếu (*minPhíRefScriptCoinsPerByte*)
tiền gửi Lovelace tối thiểu cho mỗi byte UTxO được tuần tự hóa (*utxoCostPerByte*)
tiền gửi hành động quản trị (tiền gửi chính phủ)

Lan can

PARAM-03 (y) Các tham số giao thức quan trọng yêu cầu biểu quyết SPO bên cạnh biểu quyết DRep: SPO **phải** nói "có" với sự hỗ trợ chung của hơn 50% tổng số cổ phần sản xuất khối đang hoạt động. Điều này được thực thi bởi các rào chắn trên ngưỡng biểu quyết của nhóm cổ phần.

PARAM-04 (x) Ít nhất 3 tháng **nên** thường chuyển đổi giữa việc xuất bản đề xuất ngoài chuỗi để thay đổi một tham số giao thức quan trọng và gửi hành động quản trị trên chuỗi tương ứng. Lan can bảo vệ này có thể được nói lỏng trong trường hợp xảy ra sự cố mạng Mức độ nghiêm trọng 1 hoặc Mức độ nghiêm trọng 2 sau khi thảo luận và đánh giá kỹ thuật cẩn thận.

Các thông số quan trọng đối với hệ thống quản trị

chìa khóa ủy nhiệm Tiền gửi Lovelace (cổ phầnĐịa chỉtiền gửi)
đăng ký hồ bơi Tiền gửi Lovelace (cổ phầnPoolGửi tiền)
cắt giảm phần thưởng cố định tối thiểu cho các nhóm (phútPoolChi phí)
Số tiền gửi DRep (*dRepGửi tiền*)
quy mô tối thiểu của Ủy ban Hiến pháp (ủy banKích thước tối thiểu)
thời hạn nhiệm kỳ tối đa (tính theo thời điểm) đối với các thành viên Ủy ban Hiến pháp (ủy banMaxTermLimit)

Lan can

PARAM-05 (y) DRep **phải** bỏ phiếu "đồng ý" với sự ủng hộ chung của hơn 50% tổng số cổ phần bỏ phiếu đang hoạt động. Điều này được thực thi bởi các rào chắn trên ngưỡng biểu quyết DRep.

PARAM-06 (x) Ít nhất 3 tháng **nên** thường chuyển đổi giữa việc xuất bản đề xuất ngoài chuỗi để thay đổi một tham số quan trọng đối với hệ thống quản trị và việc gửi hành động quản trị trên chuỗi tương ứng. Lan can bảo vệ này có thể được nói lỏng trong trường hợp xảy ra sự cố mạng Mức độ nghiêm trọng 1 hoặc Mức độ nghiêm trọng 2 sau khi thảo luận và đánh giá kỹ thuật cẩn thận.

2.2. Thông số kinh tế

Mục tiêu tổng thể khi quản lý các thông số kinh tế là:

Kích hoạt tính bền vững kinh tế lâu dài cho hệ sinh thái Cardano Blockchain;
Đảm bảo rằng các nhóm cổ phần được khen thưởng thỏa đáng để duy trì Chuỗi khối Cardano;
Đảm bảo rằng chủ sở hữu ADA được thưởng xứng đáng khi sử dụng cổ phần theo cách mang tính xây dựng, bao gồm cả khi ủy quyền ADA cho việc sản xuất khối; Và Cân bằng các khuyến khích kinh tế cho các bên liên quan khác nhau của hệ sinh thái Cardano Blockchain, bao gồm nhưng không giới hạn ở Nhà điều hành nhóm cổ

phần, chủ sở hữu ADA, người dùng DeFi, người dùng cơ sở hạ tầng, nhà phát triển (ví dụ: DApps) và trung gian tài chính (ví dụ: sàn giao dịch).

Kích hoạt sự thay đổi

Những thay đổi đáng kể về giá trị tiền pháp định của ADA dẫn đến các vấn đề tiềm ẩn về bảo mật, hiệu suất hoặc chức năng.
Thay đổi về khối lượng hoặc loại giao dịch.
Yêu cầu hoặc đề xuất của cộng đồng.
Các tình huống khẩn cấp đòi hỏi phải thay đổi các thông số kinh tế.

Các chỉ số phản tác dụng

Những thay đổi đối với các thông số kinh tế không nên được thực hiện một cách cô lập. Họ cần tính đến:

Các yếu tố kinh tế bên ngoài.
Mối lo ngại về an ninh mạng.

Số liệu cốt lõi

Giá trị tiền pháp định của ADA dẫn đến các vấn đề tiềm ẩn về bảo mật, hiệu suất hoặc chức năng.
Khối lượng và loại giao dịch.
Số lượng và sức khỏe của stake pool.
Các yếu tố kinh tế bên ngoài.

Thay đổi các thông số kinh tế cụ thể

Phí giao dịch trên mỗi byte (txFeePerByte) và phí giao dịch cố định (txFeeFixed)

Xác định chi phí cho các giao dịch cơ bản trong Lovelace:

$\text{phí(tx)} = \text{txFeeFixed} + \text{txFeePerByte} \times \text{nBytes(tx)}$

Lưu ý

TFPB-01 (Và) *txFeePerByte* **không được** thấp hơn 30 (0,000030 ADA). Điều này bảo vệ chống lại các cuộc tấn công từ chối dịch vụ với chi phí thấp.

TFPB-02 (Và) *txFeePerByte* **không được** vượt quá 1.000 (0,001 ADA). Điều này đảm bảo rằng các giao dịch có thể được thanh toán.

TFPB-03 (Và) *txFeePerByte* **không được** hãy tiêu cực.

TFF-01 (Và) *txFeeFixed* **không được** thấp hơn 100.000 (0,1 ADA). Điều này bảo vệ chống lại các cuộc tấn công từ chối dịch vụ với chi phí thấp.

TFF-02 (Và) *txFeeFixed* **không được** vượt quá 10.000.000 (10 ADA). Điều này đảm bảo rằng các giao dịch có thể được thanh toán.

TFF-03 (Và) *txFeeFixed* **không được** hãy tiêu cực.

TFGEN-01 (x - "nên") Để duy trì mức độ bảo vệ nhất quán chống lại các cuộc tấn công từ chối dịch vụ, *txFeeFixed* Và *txFeePerByte* **nên** được điều chỉnh bất cứ khi nào giá Thực thi Plutus được điều chỉnh (executionUnitPrices[bước/bộ nhớ]).

TFGEN-02 (x - không thể định lượng được) Mọi thay đổi đối với *txFeeFixed* hoặc *txFeePerByte* **phải** xem xét tác động của việc giảm chi phí của một cuộc tấn công từ chối dịch vụ hoặc tăng phí giao dịch tối đa đến mức không thể thực hiện được giao dịch.

Chi phí UTxO mỗi byte (utxoCostPerByte)

Xác định chi phí lưu trữ trong UTxO:

Đặt ngưỡng tối thiểu trên ADA được giữ trong một UTxO duy nhất (tối thiểu ~ 1 ADA, có thể ≥ 50 ADA trong trường hợp xấu nhất).

Cung cấp khả năng bảo vệ chống lại cuộc tấn công từ chối dịch vụ với chi phí thấp trên bộ lưu trữ UTxO. Cuộc tấn công này đã được thực hiện trên các chuỗi khác; nó không phải là lý thuyết.

Khả năng bảo vệ DoS giảm theo bộ nhớ nút trống (tỷ lệ thuận với mức tăng trưởng UTxO).

Giúp giảm chi phí lưu trữ lâu dài.

Cung cấp động lực để trả lại UTxO khi không còn cần thiết.

Sẽ vượt quá đáng kể chi phí giao dịch tối thiểu (~0,15 ADA).

Lan can

UCPB-01 (Và) *utxoCostPerByte* **không được** thấp hơn 3.000 (0,003 ADA).

UCPB-02 (Và) *utxoCostPerByte* **không được** vượt quá 6.500 (0,0065 ADA).

UCPB-03 (Và) *utxoCostPerByte* **không được** bằng không.

UCPB-04 (Và) *utxoCostPerByte* **không được** hãy tiêu cực.

UCPB-05 (x - "nên") Thay đổi **nên** chiếm:

i) Chi phí tấn công có thể chấp nhận được. ii) Thời gian chấp nhận được cho một cuộc tấn công (giả định ít nhất một kỷ nguyên). iii) Cấu hình bộ nhớ có thể chấp nhận được đối với người dùng nút đầy đủ (giả định là 16GB đối với ví hoặc 24GB đối với nhóm cổ phần). iv) Kích thước của UTxO (tối thiểu ~ 200B mỗi UTxO, tối đa khoảng 10KB). v) Tổng mức sử dụng bộ nhớ của nút hiện tại.

Tiền gửi địa chỉ cổ phần (stakeAddressDeposit)

Đảm bảo rằng các địa chỉ cổ phần sẽ bị loại bỏ khi không còn cần thiết:

Giúp giảm chi phí lưu trữ lâu dài.

Giúp hạn chế chi phí CPU và bộ nhớ trong sổ cái.

Lý do đặt cọc là để khuyến khích tài nguyên bộ nhớ khan hiếm được trả lại khi không còn cần thiết nữa. Việc giảm số lượng địa chỉ cổ phần đang hoạt động cũng giúp giảm chi phí xử lý và bộ nhớ ở ranh giới kỷ nguyên khi tính toán ảnh chụp nhanh cổ phần.

Lan can

SAD-01 (Và) *cổ phầnĐịa chỉtiền gửi* **không được** thấp hơn 1.000.000 (1 ADA).

SAD-02 (Và) *cổ phầnĐịa chỉtiền gửi* **không được** vượt quá 5.000.000 (5 ADA).

SAD-03 (Và) *cổ phầnĐịa chỉtiền gửi* **không được** hãy tiêu cực.

Tiền gửi cổ phần (stakePoolDeposit)

Đảm bảo rằng nhà điều hành nhóm cổ phần sẽ ngừng hoạt động khi họ không còn cần thiết nữa:

Giúp giảm chi phí lưu trữ lâu dài.

Lý do đặt cọc là để khuyến khích tài nguyên bộ nhớ khan hiếm được trả lại khi không còn cần thiết nữa. Phần thưởng và tính toán ảnh chụp nhanh cổ phần cũng bị ảnh hưởng bởi số lượng nhóm cổ phần đang hoạt động.

Lan can

SPD-01 (Và) *cổ phầnPoolGửi tiền* **không được** thấp hơn 250.000.000 (250 ADA).

SPD-02 (Và) *cổ phầnPoolGửi tiền* **không được** vượt quá 500.000.000 (500 ADA).

SPD-03 (Và) *cổ phầnPoolGửi tiền* **không được** hãy tiêu cực.

Chi phí nhóm tối thiểu (minPoolCost)

Một phần của cơ chế khen thưởng:

Chi phí nhóm tối thiểu được chuyển đến địa chỉ phần thưởng nhóm trước khi bất kỳ phần thưởng ủy quyền nào được thanh toán.

Lan can

MPC-01 (Và) *phútPoolChi phí không được* hãy tiêu cực.

MPC-02 (Và) *phútPoolChi phí không được* vượt quá 500.000.000 (500 ADA).

MPC-03 (x - "nên") *phútPoolChi phí nên* được thiết lập phù hợp với chi phí kinh tế cho việc vận hành bể bơi.

_ *Cắt kho bạc (kho bạcCut)*

Một phần của cơ chế khen thưởng:

Phần cắt giảm kho bạc của việc mở rộng tiền tệ sẽ được chuyển vào kho bạc trước khi bất kỳ phần thưởng nhóm nào được thanh toán.

Có thể được đặt trong phạm vi 0,0-1,0 (0% -100%).

Lan can

TC-01 (Và) *kho bạcCắt không được* thấp hơn 0,1 (10%).

TC-02 (Và) *kho bạcCắt không được* vượt quá 0,3 (30%).

TC-03 (Và) *kho bạcCắt không được* hãy tiêu cực.

TC-04 (Và) *kho bạcCắt không được* vượt quá 1,0 (100%).

TC-05 (~ - không có quyền truy cập vào lịch sử thay đổi) *kho bạcCắt không được* được thay đổi nhiều lần trong bất kỳ khoảng thời gian 36 kỷ nguyên nào (khoảng 6 tháng).

Tỷ lệ mở rộng tiền tệ (Mở rộng tiền tệ)

Một phần của cơ chế khen thưởng:

Việc mở rộng tiền tệ kiểm soát lượng dự trữ được sử dụng để làm phần thưởng cho mỗi thời đại.

Quản lý sự bền vững lâu dài của Cardano.

Nguồn dự trữ dần cạn kiệt cho đến khi không có phần thưởng nào được cung cấp.

Lan can

ME-01 (Và) *tiền tệMở rộng không được* vượt quá 0.

ME-02 (Và) *tiền tệMở rộng không được* thấp hơn 0.

ME-03 (Và) *tiền tệMở rộng không được* hãy tiêu cực.

ME-04 (x - "nên") *tiền tệMở rộng không nên* có thể thay đổi nhiều hơn +/- 10% trong khoảng thời gian 73 kỷ bất kỳ (khoảng 12 tháng).

ME-05 (x - "nên") *tiền tệMở rộng không nên* được thay đổi nhiều lần trong bất kỳ khoảng thời gian 36 kỷ nguyên nào (khoảng 6 tháng).

Giá thực thi tập lệnh Plutus (executionUnitPrices[priceSteps/priceMemory])

Xác định phí thực thi tập lệnh Plutus:

Mang lại lợi ích kinh tế cho việc thực thi tập lệnh Plutus.

Cung cấp bảo mật chống lại các cuộc tấn công DoS chi phí thấp.

Lan can

EIUP-PS-01 (Và) *thực thiUnitPrices[priceSteps] không được* vượt quá 2.000/10.000.000.

EIUP-PS-02 (Và) *thực thiUnitPrices[priceSteps] không được* thấp hơn 500/10.000.000.

EIUP-PM-01 (Và) *thực thiUnitPrices[priceMemory] không được* vượt quá 2.000/10.000.

EIUP-PM-02 (Và) *thực thiUnitPrices[priceMemory] không được* thấp hơn 400/10.000.

EIUP-GEN-01 (x - "tương tự") Giá thực hiện **phải** được thiết lập sao cho:

- i) chi phí thực hiện giao dịch với các bước CPU tối đa tương tự như chi phí của giao dịch không phải tập lệnh có kích thước tối đa và
- ii) chi phí thực hiện một giao dịch với đơn vị bộ nhớ tối đa tương tự như chi phí của một giao dịch không phải tập lệnh có kích thước tối đa.

EIUP-GEN-02 (x - "nên") Giá thực hiện **nên** được điều chỉnh bất cứ khi nào phí giao dịch được điều chỉnh ($txFeeFixed/txFeePerByte$). Mục đích là để đảm bảo rằng độ trễ xử lý là tương tự đối với các giao dịch "đầy đủ", bất kể loại của chúng.

Điều này giúp đảm bảo đáp ứng các yêu cầu về thời gian khuếch tán/lan truyền khối.

Phí giao dịch trên mỗi byte cho tập lệnh tham chiếu ($minFeeRefScriptCoinsPerByte$)

Xác định chi phí cho việc sử dụng tập lệnh tham chiếu Plutus trong Lovelace.

Lan can

MFRS-01 (Và) $minPhíRefScriptCoinsPerByte$ **không được** vượt quá 1.000 (0,001 ADA).

Điều này đảm bảo rằng các giao dịch có thể được thanh toán.

MFRS-02 (Và) $minPhíRefScriptCoinsPerByte$ **không được** hãy tiêu cực.

MFRS-03 (x - "nên") Để duy trì mức độ bảo vệ nhất quán chống lại các cuộc tấn công từ chối dịch vụ, $minPhíRefScriptCoinsPerByte$ **nên** được điều chỉnh bất cứ khi nào giá Thực thi Plutus được điều chỉnh ($thực thiUnitPrices[bước/bộ nhớ]$) và bất cứ khi nào $txFeeFixed$ được điều chỉnh.

MFRS-04 (x - không thể định lượng được) Mọi thay đổi đối với $minPhíRefScriptCoinsPerByte$ **phải** xem xét ý nghĩa của việc giảm chi phí của một cuộc tấn công từ chối dịch vụ hoặc tăng phí giao dịch tối đa.

2.3. Thông số mạng

Mục tiêu tổng thể khi quản lý các tham số mạng Cardano Blockchain là:

Kết hợp dung lượng mạng Cardano Blockchain Lớp 1 có sẵn với nhu cầu lưu lượng hiện tại hoặc tương lai, bao gồm các giao dịch thanh toán, DApp lớp 1, quản lý sidechain và nhu cầu quản trị.

Cân bằng nhu cầu lưu lượng truy cập cho các nhóm người dùng khác nhau, bao gồm các giao dịch thanh toán, người tạo ra các Token Fungible/Non-Fungible, tập lệnh Plutus, nhà phát triển DeFi, Nhà điều hành nhóm cổ phần và giao dịch bỏ phiếu.

Kích hoạt sự thay đổi

Những thay đổi đối với tham số mạng có thể được kích hoạt bởi:

Những thay đổi được đo lường về nhu cầu giao thông trong khoảng thời gian 2 kỷ nguyên (10 ngày).

Dự kiến những thay đổi về nhu cầu giao thông.

Yêu cầu của cộng đồng.

Các chỉ số phân tác dụng

Những thay đổi có thể cần phải được hủy bỏ và/hoặc không nên được thực hiện trong trường hợp:

Độ trễ lan truyền khối quá mức.

Nhóm cổ phần không thể xử lý lưu lượng truy cập.

Tập lệnh không thể hoàn thành quá trình thực thi.

Số liệu cốt lõi

Tất cả các quyết định về thay đổi tham số phải được thông báo bởi:

- Cấu hình độ trễ lan truyền khối.
- Lưu lượng truy cập (kích thước khối theo thời gian).
- Khối lượng tập lệnh (kích thước của tập lệnh và đơn vị thực thi).
- Điểm chuẩn chi phí thực thi tập lệnh.
- Chặn các tiêu chuẩn về độ trễ/khuếch tán lan truyền.

Cần có kết quả đo điểm chuẩn chi tiết để xác nhận tác động của bất kỳ thay đổi nào đối với hiệu suất hoặc hành vi của mạng chính trước khi ban hành. Tác động của các kết hợp giao dịch khác nhau phải được phân tích, bao gồm các giao dịch thông thường, tập lệnh Plutus và hành động quản trị.

Lan can

MANG-01 (x - "nên") Không có tham số mạng riêng lẻ **nên** thay đổi nhiều hơn một lần trong hai kỳ nguyên.

MANG-02 (x - "nên") Chỉ có một tham số mạng **nên** được thay đổi theo từng kỳ nguyên trừ khi chúng có mối tương quan trực tiếp, ví dụ: giới hạn đơn vị bộ nhớ trên mỗi giao dịch và mỗi khối.

Những thay đổi đối với các thông số mạng cụ thể

Kích thước khối ($maxBlockBodySize$)

Kích thước tối đa của một khối, tính bằng Byte.

Lan can

MBBS-01 (Và) $maxBlockBodySize$ **không được** vượt quá 122.880 Byte (120KB).

MBBS-02 (Và) $maxBlockBodySize$ **không được** thấp hơn 24.576 Byte (24KB).

MBBS-03 (x - "trường hợp ngoại lệ") $maxBlockBodySize$ **không được** bị giảm đi, trừ những trường hợp đặc biệt khi có vấn đề tiềm ẩn về bảo mật, hiệu suất hoặc chức năng.

MBBS-04 (~ - không có quyền truy cập vào các giá trị tham số hiện có) $maxBlockBodySize$ **phải** đủ lớn để bao gồm ít nhất một giao dịch (nghĩa là, $maxBlockBodySize$ **phải** ít nhất là *kích thước tối đaTxSize*).

MBBS-05 (x - "nên") $maxBlockBodySize$ **nên** được thay đổi tối đa 10.240 Byte (10KB) mỗi kỳ nguyên (5 ngày) và tốt nhất là 8.192 Byte (8KB) trở xuống mỗi kỳ nguyên.

MBBS-06 (x - "nên") Kích thước khối **không nên** tạo ra một chuyển đi khứ hồi Giao thức điều khiển truyền dẫn (TCP) bổ sung. Bất kỳ sự gia tăng nào vượt quá mức này đều phải được hỗ trợ bằng phân tích hiệu suất, mô phỏng và đo điểm chuẩn.

MBBS-07 (x - "không thể định lượng") Tác động của bất kỳ thay đổi nào đối với $maxBlockBodySize$ **phải** được xác nhận bằng điểm chuẩn/mô phỏng chi tiết và không vượt quá yêu cầu về quỹ thời gian khuếch tán/truyền khối, như được mô tả dưới đây. Bất kỳ sự gia tăng nào đến $maxBlockBodySize$ cũng phải xem xét các yêu cầu trong tương lai đối với việc thực thi tập lệnh Plutus ($maxBlockExecutionUnits[bước]$) so với mục tiêu khuếch tán tổng khối là 3 giây với tốc độ truyền khối 95% trong vòng 5 giây. Giới hạn về kích thước khối tối đa có thể được tăng lên trong tương lai nếu điều này được hỗ trợ bởi kết quả đo điểm chuẩn và giám sát.

Kích thước giao dịch ($maxTxSize$)

Kích thước tối đa của một giao dịch, tính bằng Byte.

Lan can

MTS-01 (Và) *kích thước tối đaTxSize* **không được** vượt quá 32.768 Byte (32KB).

MTS-02 (Và) *kích thước tối đaTxSize* **không được** hãy tiêu cực.

MTS-03 (~ - không có quyền truy cập vào các giá trị tham số hiện có) *kích thước tối đaTxSize* **không được** được giảm đi.

MTS-04 (~ - không có quyền truy cập vào các giá trị tham số hiện có) *kích thước tối đaTxSize* **không được** quá $maxBlockBodySize$.

MTS-05 (x - "nên") *kích thước tối đaTxSize* **không nên** được tăng hơn 2.560 Byte (2,5KB) trong bất kỳ kỳ nguyên nào và tốt nhất là **nên** được tăng thêm 2.048 Byte (2KB) hoặc ít hơn mỗi kỳ nguyên.

MTS-06 (x - "nên") *kích thước tối đaTxSize* **không nên** vượt quá 1/4 kích thước khối.

Giới hạn đơn vị bộ nhớ (*maxBlockExecutionUnits[memory]*, *maxTxExecutionUnits[memory]*)

Giới hạn về số lượng đơn vị bộ nhớ tối đa mà tập lệnh Plutus có thể sử dụng, trên mỗi giao dịch hoặc trên mỗi khối.

Lưu ý

MTEU-M-01 (Và) *maxTxExecutionUnits[bộ nhớ]* **không được** vượt quá 40.000.000 đơn vị.

MTEU-M-02 (Và) *maxTxExecutionUnits[bộ nhớ]* **không được** hãy tiêu cực.

MTEU-M-03 (~ - không có quyền truy cập vào các giá trị tham số hiện có) *maxTxExecutionUnits[bộ nhớ]* **không được** được giảm đi.

MTEU-M-04 (x - "nên") *maxTxExecutionUnits[bộ nhớ]* **không nên** được tăng lên hơn 2.500.000 đơn vị ở bất kỳ thời điểm nào.

MBEU-M-01 (Và) *maxBlockExecutionUnits[bộ nhớ]* **không được** vượt quá 120.000.000 đơn vị.

MBEU-M-02 (Và) *maxBlockExecutionUnits[bộ nhớ]* **không được** hãy tiêu cực.

MBEU-M-03 (x - "nên") *maxBlockExecutionUnits[bộ nhớ]* **không nên** được thay đổi (tăng hoặc giảm) hơn 10.000.000 đơn vị ở bất kỳ thời điểm nào.

MBEU-M-04 (x - không thể định lượng) Tác động của bất kỳ thay đổi nào đối với *maxBlockExecutionUnits[bộ nhớ]* **phải** được xác nhận bằng điểm chuẩn/mô phỏng chi tiết và không vượt quá yêu cầu về quỹ thời gian khuếch tán/truyền bá, cũng như bị ảnh hưởng bởi *maxBlockExecutionUnits[bước]*. Bất kỳ sự gia tăng nào **phải** cũng xem xét các yêu cầu trong tương lai đã được thống nhất trước đó đối với tổng kích thước khối (*maxBlockBodySize*) được đo dựa trên mục tiêu khuếch tán tổng khối trong 3 giây với mức truyền khối 95% trong vòng 5 giây. Những cải tiến về hiệu suất của Plutus trong tương lai có thể cho phép tăng giới hạn trên mỗi khối nhưng phải được cân bằng với các giới hạn khuếch tán tổng thể như được chỉ định trong câu trước và các yêu cầu trong tương lai.

TÔI-M-01 (~ - không có quyền truy cập vào các giá trị tham số hiện có) *maxBlockExecutionUnits[bộ nhớ]* **không được** ít hơn *maxTxExecutionUnits[bộ nhớ]*.

Giới hạn đơn vị CPU (*maxBlockExecutionUnits[steps]*, *maxTxExecutionUnits[steps]*)

Giới hạn về số bước CPU tối đa mà tập lệnh Plutus có thể sử dụng, trên mỗi giao dịch hoặc trên mỗi khối.

Lưu ý

MTEU-S-01 (Và) *maxTxExecutionUnits[bước]* **không được** vượt quá 15.000.000.000 (15 tỷ) đơn vị.

MTEU-S-02 (Và) *maxTxExecutionUnits[bước]* **không được** hãy tiêu cực.

MTEU-S-03 (~ - không có quyền truy cập vào các giá trị tham số hiện có) *maxTxExecutionUnits[bước]* **không được** được giảm đi.

MTEU-S-04 (x - "nên") *maxTxExecutionUnits[bước]* **không nên** được tăng hơn 500.000.000 (500M) đơn vị trong bất kỳ kỳ nguyên nào (5 ngày).

MBEU-S-01 (Và) *maxBlockExecutionUnits[bước]* **không được** vượt quá 40.000.000.000 (40 tỷ) đơn vị.

MBEU-S-02 (Và) *maxBlockExecutionUnits[bước]* **không được** hãy tiêu cực.

MBEU-S-03 (x - "nên") *maxBlockExecutionUnits[bước]* **không nên** được thay đổi (tăng hoặc giảm) hơn 2.000.000.000 (2Bn) đơn vị trong bất kỳ kỳ nguyên nào (5 ngày).

MBEU-S-04 (x - không thể định lượng) Tác động của sự thay đổi đối với *maxBlockExecutionUnits[bước]* **phải** được xác nhận bằng điểm chuẩn/mô phỏng chi tiết và không vượt quá yêu cầu về ngân sách thời gian khuếch tán/truyền khối, cũng như bị ảnh hưởng bởi *maxBlockExecutionUnits[bộ nhớ]*. Bất kỳ sự gia tăng nào **phải** cũng xem xét các yêu cầu trong tương lai được xác định trước đó đối với tổng kích thước khối (*maxBlockBodySize*) được đo dựa trên mục tiêu khuếch tán tổng khối trong 3 giây với mức truyền khối 95% trong vòng 5 giây. Những cải tiến về hiệu suất của Plutus trong tương lai có thể cho phép tăng giới hạn trên mỗi khối, nhưng **phải** được cân bằng với các giới hạn khuếch tán tổng thể như đã nêu trong câu trước và các yêu cầu trong tương lai.

MY-S-01 (~ - không có quyền truy cập vào các giá trị tham số hiện có) *maxBlockExecutionUnits[bước]* **không được** ít hơn *maxTxExecutionUnits[bước]*.

Kích thước tiêu đề khối (*maxBlockHeaderSize*)

Kích thước của tiêu đề khối.

Ghi chú: Việc tăng kích thước tiêu đề khối có thể ảnh hưởng đến kích thước khối tổng thể (*maxBlockBodySize*).

Lưu ý

MBHS-01 (Và) *kích thước maxBlockHeader không được* vượt quá 5.000 Byte.

MBHS-02 (Và) *kích thước maxBlockHeader không được* hãy tiêu cực.

MBHS-03 (x - "tiêu đề hợp lệ lớn nhất" có thể thay đổi) *kích thước maxBlockHeader phải* đủ lớn cho tiêu đề hợp lệ lớn nhất.

MBHS-04 (x - "nên") *kích thước maxBlockHeader nên* thường chỉ được tăng lên nếu giao thức thay đổi.

MBHS-05 (x - "nên") *kích thước maxBlockHeader nên* nằm trong cửa sổ tắc nghẽn ban đầu của TCP (3 hoặc 10 MTU).

2.4. Thông số kỹ thuật/bảo mật

Mục tiêu tổng thể khi quản lý các thông số kỹ thuật/bảo mật là:

Đảm bảo tính bảo mật của mạng Cardano về mặt phân cấp, bảo vệ chống lại các cuộc tấn công Sybil và 51% cũng như bảo vệ chống lại các cuộc tấn công từ chối dịch vụ.

Cho phép thay đổi ngôn ngữ Plutus.

Kích hoạt sự thay đổi

Thay đổi về số lượng SPO đang hoạt động.

Thay đổi ngôn ngữ Plutus.

Các mối đe dọa an ninh.

Yêu cầu của cộng đồng.

Các chỉ số phản tác dụng

Những lo ngại về kinh tế, ví dụ: khi thay đổi số lượng cổ phần.

Số liệu cốt lõi

Số lượng cổ phần.

Mức độ phân cấp.

Thay đổi các thông số kỹ thuật/bảo mật cụ thể

Số lượng cổ phần mục tiêu (stakePoolTargetNum)

Đặt số lượng mục tiêu của nhóm cổ phần:

Số lượng nhóm dự kiến khi mạng ở trạng thái cân bằng.

Chủ yếu là một tham số bảo mật, đảm bảo phân cấp theo phân chia/sao chép nhóm.

Có hiệu quả kinh tế cũng như hiệu quả an ninh; tư vấn kinh tế cũng được yêu cầu khi thay đổi thông số này.

Những thay đổi lớn trong thông số này sẽ gây ra các sự kiện tái phân bổ hàng loạt.

Lưu ý

SPTN-01 (Và) *stakePoolTargetNum không được* thấp hơn 250.

SPTN-02 (Và) *stakePoolTargetNum không được* vượt quá 2.000.

SPTN-03 (Và) *stakePoolTargetNum không được* hãy tiêu cực.

SPTN-04 (Và) *stakePoolTargetNum* **không được** bằng không.

Yếu tố ảnh hưởng cam kết (poolPledgeInfluence)

Kích hoạt cơ chế bảo vệ cam kết:

Cung cấp sự bảo vệ chống lại cuộc tấn công Sybil.

Giá trị cao hơn sẽ thưởng cho các nhóm có nhiều cam kết hơn và trừng phạt các nhóm có ít cam kết hơn.

Có hiệu quả kinh tế cũng như hiệu quả kỹ thuật; tư vấn kinh tế cũng được yêu cầu.

Có thể được đặt trong phạm vi 0,0-vô cực.

Lan can

PPI-01 (Và) *poolPledge* **Ảnh hưởng không được** thấp hơn 0,1.

PPI-02 (Và) *poolPledge* **Ảnh hưởng không được** vượt quá 1,0.

PPI-03 (Và) *poolPledge* **Ảnh hưởng không được** hãy tiêu cực.

PPI-04 (x - "nên") *poolPledge* **Ảnh hưởng không nên** thay đổi nhiều hơn +/- 10% trong bất kỳ khoảng thời gian 18 kỷ nguyên nào (khoảng 3 tháng).

Cửa sổ nghỉ hưu của nhóm (poolRetireMaxEpoch)

Xác định số lượng thông báo kỷ nguyên tối đa mà một nhóm có thể đưa ra khi lập kế hoạch ngừng hoạt động.

Lan can

PRME-01 (Và) *poolRetireMaxEpoch* **không được** hãy tiêu cực.

PRME-02 (x - "nên") *poolRetireMaxEpoch* **không nên** thấp hơn 1.

Tỷ lệ tài sản thế chấp (Tỷ lệ tài sản thế chấp)

Xác định số lượng tài sản thế chấp phải được cung cấp khi thực thi tập lệnh Plutus theo tỷ lệ phần trăm của chi phí thực hiện thông thường:

Tài sản thế chấp là tài sản bổ sung cho các khoản thanh toán phí.

Nếu tập lệnh không thực thi được thì tài sản thế chấp sẽ bị mất.

Tài sản thế chấp không bao giờ bị mất nếu tập lệnh thực thi thành công.

Cung cấp khả năng bảo mật chống lại các cuộc tấn công chi phí thấp bằng cách làm cho việc thực thi các tập lệnh bị lỗi trở nên tốn kém hơn thay vì ít tốn kém hơn.

Lan can

CP-01 (Và) *phần trăm tài sản thế chấp* **không được** thấp hơn 100.

CP-02 (Và) *phần trăm tài sản thế chấp* **không được** vượt quá 200.

CP-03 (Và) *phần trăm tài sản thế chấp* **không được** hãy tiêu cực.

CP-04 (Và) *phần trăm tài sản thế chấp* **không được** bằng không.

Số lượng đầu vào tài sản thế chấp tối đa (maxColonynousInputs)

Xác định số lượng đầu vào tối đa có thể được sử dụng làm tài sản thế chấp khi thực thi tập lệnh Plutus.

Lan can

MCI-01 (Và) *maxTài sản thế chấpĐầu vào* **không được** thấp hơn 1.

Giới hạn về kích thước được xê-ri hóa của Giá trị trong mỗi đầu ra.

Lan can

MVS-01 (Và) *maxValueSize* **không được** vượt quá 12.288 Byte (12KB).

MVS-02 (Và) *maxValueSize* **không được** hãy tiêu cực.

MVS-03 (~ - không có quyền truy cập vào các giá trị tham số hiện có) *maxValueSize* **phải** ít hơn *kích thước tối đaTxSize* .

MVS-04 (~ - không có quyền truy cập vào các giá trị tham số hiện có) *maxValueSize* **không được** được giảm bớt.

MVS-05 (x - "đầu ra hợp lý" có thể được giải thích) *maxValueSize* **phải** đủ lớn để cho phép các đầu ra hợp lý (ví dụ: mọi đầu ra trên chuỗi hiện có hoặc các đầu ra dự đoán có thể được tạo ra bởi các quy tắc số cái mới).

Mô hình chi phí Plutus (costModels)

Xác định chi phí cơ bản cho từng nguyên thủy Plutus theo đơn vị CPU và bộ nhớ:

Tổng cộng có khoảng 150 thông số vi mô riêng biệt.

Mô hình chi phí được xác định cho từng phiên bản ngôn ngữ Plutus. Phiên bản ngôn ngữ mới có thể giới thiệu các tham số vi mô bổ sung hoặc loại bỏ các tham số vi mô hiện có.

Lan can

PCM-01 (x - không thể định lượng được) *Mô hình chi phí* giá trị **phải** được thiết lập bằng cách so sánh điểm chuẩn trên kiến trúc tham chiếu.

PCM-02 (x - phiên bản nguyên thủy và ngôn ngữ không được giới thiệu trong giao dịch) *mô hình chi phí phải* được cập nhật nếu phiên bản gốc mới được giới thiệu hoặc phiên bản ngôn ngữ Plutus mới được thêm vào.

PCM-03 (~ - không có quyền truy cập vào *Mô hình chi phí Plutus* thông số) *Mô hình chi phí* giá trị **không nên** hãy tiêu cực.

PCM-04 (~ - không có quyền truy cập vào *Mô hình chi phí Plutus* thông số) A *mô hình chi phí phải* được cung cấp cho từng phiên bản ngôn ngữ Plutus mà giao thức hỗ trợ.

2.5. Thông số quản trị

Mục tiêu tổng thể khi quản lý các tham số quản trị là:

Đảm bảo ổn định quản lý.

Duy trì một hình thức quản trị mang tính đại diện như được nêu ở đây..

Kích hoạt sự thay đổi

Những thay đổi về tham số quản trị có thể được kích hoạt bởi:

Yêu cầu của cộng đồng.

Yêu cầu quy định.

Kết quả quản trị bất ngờ hoặc không mong muốn.

Bước vào trạng thái mất tự tin.

Các chỉ số phản tác dụng

Những thay đổi có thể cần phải được hủy bỏ và/hoặc không nên được thực hiện trong trường hợp:

Những tác động không mong đợi đến quản trị.

Tải Lốp 1 quá mức do bỏ phiếu trên chuỗi hoặc số lượng hành động quản trị quá nhiều.

Số liệu cốt lõi

Tất cả các quyết định về thay đổi tham số phải được thông báo bởi:

Mức độ tham gia quản trị

Các hành vi và mô hình quản trị.

Những cân nhắc về mặt quy định.

Niềm tin vào hệ thống quản lý.

Hiệu quả của hệ thống quản trị trong việc quản lý những thay đổi cần thiết.

Thay đổi các thông số quản trị cụ thể

Tiền gửi cho các hành động quản trị (govDeposit)

Khoản tiền gửi được tính khi gửi hành động quản trị:

Giúp hạn chế số lượng hành động được gửi.

Lan can

GD-01 (Và) *tiền gửi chính phủ không được* hãy tiêu cực.

GD-02 (Và) *tiền gửi chính phủ không được* thấp hơn 1.000.000 (1 ADA).

GD-03 (Và) *tiền gửi chính phủ không được* vượt quá 10.000.000.000.000 (10 triệu ADA).

GD-04 (x - “nên”) *tiền gửi chính phủ nên* được điều chỉnh phù hợp với những thay đổi của tiền pháp định.

Gửi tiền cho DReps (dRepDeposit)

Khoản tiền gửi được tính khi đăng ký DRep:

Giúp hạn chế số lượng DReps hoạt động.

Lan can

DRD-01 (Và) *dRepGửi tiền không được* hãy tiêu cực.

DRD-02 (Và) *dRepGửi tiền không được* thấp hơn 1.000.000 (1 ADA).

DRD-03 (Và) *dRepGửi tiền không được* vượt quá 100.000.000.000 (100.000 ADA).

DRD-04 (x - “nên”) *dRepGửi tiền nên* được điều chỉnh phù hợp với những thay đổi của tiền pháp định.

Khoảng thời gian hoạt động DRep (dRepActivity)

Khoảng thời gian (tính theo toàn bộ số kỷ nguyên) sau đó DRep được coi là không hoạt động vì mục đích tính toán phiếu bầu, nếu chúng không bỏ phiếu cho bất kỳ đề xuất nào.

Lan can

DRA-01 (Và) *dRepHoạt động không được* thấp hơn 13 kỷ nguyên (2 tháng).

DRA-02 (Và) *dRepHoạt động không được* vượt quá 37 kỷ nguyên (6 tháng).

DRA-03 (Và) *dRepHoạt động không được* hãy tiêu cực.

DRA-04 (~ - không có quyền truy cập vào các giá trị tham số hiện có) *dRepHoạt động phải* lớn hơn govHành độngTrộn đời .

DRA-05 (x - “nên”) *dRepHoạt động nên* được tính bằng con người (2 tháng, v.v.).

Ngưỡng hành động quản trị DRep và SPO (dRepVotingThresholds[...], poolVotingThresholds[...])

Ngưỡng đối với cổ phần biểu quyết đang hoạt động được yêu cầu để phê chuẩn một loại hành động quản trị cụ thể của DReps hoặc SPO:

Đảm bảo tính hợp pháp của hành động.

Các tham số ngưỡng được liệt kê dưới đây:

dRepVotingNgưỡng :

dvtỦy banKhông cóSự tự tin

Ủy ban dvtBình thường

dvtHardForkKhởi tạo

dvtMotionKhông có sự tự tin

dvtPPEkinh tếGroup

dvtPPGovGroup

dvtPPMạngNhóm

dvtPPNhóm kỹ thuật
dvtKho bạcRút tiền
dvtUpdateToHiến pháp

poolVotingNgưỡng :

Ủy ban pvtKhông có sự tự tin
Ủy ban pvtBình thường
pvtHardForkKhởi tạo
pvtMotionKhông Tự tin
pvtPPSecurityGroup

Lan can

VT-GEN-01 (y) Tất cả các ngưỡng **phải** lớn hơn 50% và nhỏ hơn hoặc bằng 100%.

VT-GEN-02 (y) Các ngưỡng thông số kinh tế, mạng lưới và kỹ thuật **phải** nằm trong khoảng 51%-75%.

VT-GEN-03 (y) Ngưỡng tham số quản trị **phải** nằm trong khoảng 75%-90%.

VT-HF-01 (Và) **Cái nĩa cứng** ngưỡng hành động **phải** nằm trong khoảng 51%-80%.

VT-CON-01 (Và) **Hành động kịch bản của Hiến pháp hoặc lan can mới** ngưỡng **phải** nằm trong khoảng 65%-90%.

VT-CC-01 (Và) **Cập nhật hành động của Ủy ban Hiến pháp** ngưỡng **phải** nằm trong khoảng 51%-90%.

VT-NC-01 (Và) **Không có sự tự tin** ngưỡng hành động **phải** nằm trong khoảng 51%-75%.

Hành động quản trị trọn đời (govActionLifetime)

Khoảng thời gian mà sau đó một hành động quản trị sẽ hết hiệu lực nếu nó không được ban hành:

Như một số lượng lớn các kỷ nguyên.

Lan can

GAL-01 (Và) *govHành độngTrọn đời* **không được** thấp hơn 1 kỷ nguyên (5 ngày).

GAL-03 (x - "nên") *govHành độngTrọn đời* **không nên** thấp hơn 2 kỷ nguyên (10 ngày).

GAL-02 (Và) *govHành độngTrọn đời* **không được** vượt quá 15 kỷ nguyên (75 ngày).

GAL-04 (x - "nên") *govHành độngTrọn đời* **nên** được điều chỉnh về mặt con người (ví dụ: 30 ngày, hai tuần) để có đủ thời gian cho việc bỏ phiếu, v.v., diễn ra.

GAL-05 (~ - không có quyền truy cập vào các giá trị tham số hiện có) *govHành độngTrọn đời* **phải** ít hơn *dRepHoạt động* .

Nhiệm kỳ tối đa của Ủy ban Hiến pháp (ủy banMaxTermLimit)

Giới hạn về nhiệm kỳ tối đa mà một thành viên ủy ban có thể phục vụ.

Lan can

CMTL-01 (Và) *ủy banMaxTermLimit* **không được** bằng không.

CMTL-02 (Và) *ủy banMaxTermLimit* **không được** hãy tiêu cực.

CMTL-03 (Và) *ủy banMaxTermLimit* **không được** thấp hơn 18 kỷ nguyên (90 ngày hoặc khoảng 3 tháng).

CMTL-04 (Và) *ủy banMaxTermLimit* **không được** vượt quá 293 kỷ nguyên (khoảng 4 năm).

CMTL-05 (x - "nên") *ủy banMaxTermLimit* **không nên** vượt quá 220 kỷ nguyên (khoảng 3 năm).

Quy mô tối thiểu của Ủy ban Hiến pháp (committeeMinSize)

Số lượng thành viên ít nhất có thể được đưa vào Ủy ban Hiến pháp sau hành động quản lý nhằm thay đổi Ủy ban Hiến pháp.

Lan can

CMS-01 (Và) *ủy banKích thước tối thiểu* **không được** hãy tiêu cực.

CMS-02 (Và) *ủy banKích thước tối thiểu* **không được** thấp hơn 3.

CMS-03 (Và) *ủy banKích thước tối thiểu* **không được** vượt quá 10.

2.6. Giám sát và đảo ngược các thay đổi tham số

Một kỷ nguyên bao gồm 5 ngày theo lịch. Tất cả các thay đổi tham số mạng **phải** được theo dõi cẩn thận không dưới 2 đợt (10 ngày):

Thay đổi **phải** được hoàn nguyên càng sớm càng tốt nếu độ trễ truyền khối vượt quá 4,5 giây đối với hơn 5% khối trong bất kỳ cửa sổ cuộn 6 giờ nào.

Tất cả các thay đổi tham số khác phải được theo dõi cẩn thận để phát hiện bất kỳ tác động bất lợi nào đến hiệu suất, bảo mật hoặc chức năng. Nếu quan sát thấy những ảnh hưởng như vậy thì cần thực hiện các hành động thích hợp, bao gồm cả việc quay trở lại các thông số trước đó.

Một kế hoạch đảo ngược/khôi phục cụ thể **phải là** được tạo ra cho mỗi thay đổi tham số. Kế hoạch này phải bao gồm:

Những tham số nào cần thay đổi và theo cách nào để trở về trạng thái trước đó (hoặc trạng thái tương tự).

Làm thế nào để khôi phục mạng trong trường hợp có sự cố nghiêm trọng.

Kế hoạch này **nhận** được tuân theo nếu quan sát thấy có vấn đề sau khi thay đổi thông số. Lưu ý rằng không phải tất cả các thay đổi đều có thể được hoàn nguyên. Phải cẩn thận hơn khi thực hiện thay đổi các thông số này.

2.7. Các thông số giao thức không thể cập nhật

Một số tham số giao thức cơ bản không thể thay đổi được bằng hành động quản trị Cập nhật tham số giao thức. Các tham số này chỉ có thể được thay đổi trong tệp Genesis mới như một phần của hard fork. Không cần thiết phải cung cấp các biện pháp bảo vệ cụ thể khi cập nhật các thông số này.

3. CÁC QUY ĐỊNH VÀ HƯỚNG DẪN VỀ HOẠT ĐỘNG RÚT KHO BÀ

Rút tiền kho bạc các hành động chỉ định đích đến và số tiền rút từ kho bạc Cardano.

Lan can

KHO BẤU-01 (x) DRep **phải** xác định giới hạn thay đổi ròng cho số dư của Kho bạc Cardano trong mỗi khoảng thời gian.

KHO BẤU-02 (x) Ngân sách cho Kho bạc Cardano **không được** vượt quá giới hạn thay đổi ròng đối với số dư của Kho bạc Cardano trong một khoảng thời gian.

KHO BẤU-03 (x) Ngân sách cho Kho bạc Cardano **phải** được mệnh giá bằng ADA.

KHO BẤU-04 (x) Rút tiền kho bạc **không được** được phê chuẩn cho đến khi có ngân sách Cardano được cộng đồng phê duyệt, sau đó có hiệu lực theo hành động quản trị trên chuỗi trước đó đã được DReps đồng ý với ngưỡng lớn hơn 50% cổ phần biểu quyết đang hoạt động.

4. CÁC HƯỚNG DẪN VÀ HƯỚNG DẪN VỀ CÁC HÀNH ĐỘNG KHỞI ĐỘNG Hard Fork

các **bắt đầu hard fork** hành động yêu cầu cả phiên bản giao thức chính mới và phiên bản giao thức phụ mới phải được chỉ định:

Là số nguyên dương.

Là kết quả của một hard fork, các tham số giao thức có thể cập nhật mới có thể được đưa ra. Các lan can có thể được xác định cho các tham số này, các tham số này sẽ có hiệu lực sau đợt hard fork. Các tham số giao thức có thể cập nhật hiện tại cũng có thể không được dùng nữa bởi hard fork, trong trường hợp đó, các biện pháp bảo vệ trở nên lỗi thời đối với tất cả các thay đổi trong tương lai.

Lan can

HARDFORK-01 (~ - không có quyền truy cập vào các giá trị tham số hiện có) Phiên bản giao thức chính **phải** giống hoặc lớn hơn phiên bản chính sẽ được ban hành ngay trước thay đổi này. Nếu phiên bản giao thức chính lớn hơn thì phiên bản giao thức phụ **phải** bằng không.

HARDFORK-02 (~ - không có quyền truy cập vào các giá trị tham số hiện có) Phiên bản giao thức phụ **phải** không kém hơn phiên bản nhỏ sẽ được ban hành ngay trước khi có thay đổi này.

HARDFORK-03 (~ - không có quyền truy cập vào các giá trị tham số hiện có) ít nhất một trong các phiên bản giao thức (chính hoặc phụ hoặc cả hai) **phải** thay đổi.

HARDFORK-04 (x) Ít nhất 85% tổng số cổ phần theo số cổ phần đang hoạt động **nên** đã nâng cấp lên phiên bản nút Cardano có khả năng xử lý các quy tắc liên quan đến phiên bản giao thức mới.

HARDFORK-05 (x) Bất kỳ tham số giao thức có thể cập nhật mới nào được giới thiệu bằng hard fork **phải** được bao gồm trong Điều này và các lan can phù hợp được xác định cho các thông số đó.

HARDFORK-06 (x) Cài đặt cho bất kỳ tham số giao thức mới nào được giới thiệu bằng hard fork **phải** được đưa vào tệp Genesis thích hợp.

HARDFORK-07 (x) Mọi tham số giao thức không được dùng nữa **phải** được nêu rõ trong Điều này.

HARDFORK-08 (~ - không có quyền truy cập vào *Mô hình chi phí Plutus* thông số) Phiên bản Plutus mới **phải** được hỗ trợ bởi một phiên bản cụ thể *Mô hình chi phí Plutus* bao gồm từng nguyên thủy có sẵn trong phiên bản Plutus mới.

5. CÁC QUY ĐỊNH VÀ HƯỚNG DẪN CẬP NHẬT CÁC HÀNH ĐỘNG CỦA ỦY BAN Hiến Pháp HOẶC NGƯỠNG CHỨNG

Cập nhật Ủy ban Hiến pháp hoặc Ngưỡng các hành động quản trị có thể thay đổi quy mô, thành phần hoặc ngưỡng bỏ phiếu bắt buộc đối với Ủy ban Hiến pháp.

Lan can

CẬP NHẬT-CC-01 (x) **Cập nhật Ủy ban Hiến pháp và/hoặc ngưỡng và/hoặc thời hạn** hành động quản trị **không được** được phê chuẩn cho đến khi chủ sở hữu ADA phê chuẩn Hiến pháp cuối cùng thông qua hành động quản trị trên chuỗi.

6. CÁC ĐIỀU KHOẢN VÀ HƯỚNG DẪN VỀ HIỆP PHÁP MỚI HOẶC CÁC HÀNH ĐỘNG KÍCH bản GUARDRAILS

Các hành động của tập lệnh Guardrails hoặc hiến pháp mới thay đổi hàm băm của hiến pháp trên chuỗi và tập lệnh Guardrails liên quan.

Lan can

HIẾN PHÁP MỚI-01 (x) A **Hiến pháp mới hoặc tập lệnh Guardrails** hành động quản trị **phải** được gửi để xác định bất kỳ biện pháp bảo vệ cần thiết nào cho các tham số mới được giới thiệu thông qua hành động quản trị Hard Fork.

7. Rào chắn và HƯỚNG DẪN VỀ CÁC HÀNH ĐỘNG KHÔNG BÍ MẬT

Không có sự tự tin hành động báo hiệu tình trạng không tin tưởng vào hệ thống quản trị. Không có rào chắn nào được áp đặt trên **Không có sự tự tin** hành động.

Lan can

Không có

8. RÀ SOÁT VÀ HƯỚNG DẪN VỀ CÁC HÀNH ĐỘNG THÔNG TIN

Thông tin các hành động không được thực hiện trên chuỗi. Không có rào chắn nào được áp đặt trên **Thông tin** hành động.

Lan can

Không có

9. RÀO CẢN TRONG GIAI ĐOẠN TẠM THỜI

Giai đoạn tạm thời

Giai đoạn tạm thời bắt đầu với Hard-Fork Chang vào tháng 9 __ năm 2024 và kết thúc sau khi Hiến pháp cuối cùng được cộng đồng phê chuẩn được ban hành trực tuyến. Trong suốt Giai đoạn tạm thời, các yếu tố kích hoạt được thực thi theo hiến pháp và kỹ thuật sẽ dần dần bật các tính năng quản trị..

Triển khai kỹ thuật trong giai đoạn tạm thời:

Hard Fork Chang đã kích hoạt ba hành động quản trị ban đầu do Đề xuất cải tiến Cardano (CIP) 1694 đề xuất và cho phép thiết lập khuôn khổ quản trị đại diện. Những hành động này là **"Thông tin"** , **"Bắt đầu hard fork"** , Và **"Thay đổi tham số giao thức"** hành động.

Những người nắm giữ ADA có thể đăng ký và ủy quyền cho DReps ngay sau hard fork Chang nhưng việc bỏ phiếu DRep sẽ không có sẵn, ngoại trừ trên **"Thông tin"** hành động. Điều này đảm bảo rằng chủ sở hữu ADA có đủ thời gian để chọn đoàn biểu quyết của họ. SPO có thể bỏ phiếu như được mô tả trong CIP-1694.

"Bắt đầu hard fork" Và **"Thay đổi tham số giao thức"** các hành động cũng sẽ được Ủy ban Hiến pháp phê chuẩn.

Những người nắm giữ ADA sẽ có thể rút phần thưởng đặt cược của họ như bình thường.

Một hard fork tiếp theo, được Ủy ban Hiến pháp và SPO phê chuẩn, ngay sau Hard Fork Chang, sẽ cho phép bốn hành động quản trị CIP-1694 còn lại:

"Rút tiền từ kho bạc" ,
"Chuyển động bất tin" ,
"Cập nhật ủy ban hiến pháp và/hoặc ngưỡng và/hoặc điều khoản" , Và
"Hiến pháp mới hoặc kích bản lan can" .

Tại thời điểm này, tính năng bỏ phiếu DRep sẽ được kích hoạt và phần thưởng đặt cược chỉ có thể được rút nếu chủ sở hữu ADA đã ủy quyền phiếu bầu của họ (bao gồm cho chính họ và các tùy chọn bỏ phiếu Trắng/Không tin cậy được xác định trước).

Lan can

TẠM THỜI-01 (x) Cung cấp đủ thời gian để DReps đăng ký và vận động cũng như để chủ sở hữu ADA chọn các phái đoàn bỏ phiếu ban đầu của họ, ít nhất 18 kỷ nguyên (90 ngày hoặc khoảng 3 tháng) **phải** trôi qua sau hard fork Chang trước khi hard fork tiếp theo có thể được phê chuẩn. Sau khi đợt hard fork tiếp theo được thực hiện, việc bỏ phiếu DRep có thể diễn ra như được mô tả trong CIP-1694.

TẠM THỜI-02 (x) Rút tiền kho bạc **không được** được phê duyệt cho đến khi có ngân sách Hệ sinh thái Blockchain Cardano được cộng đồng phê duyệt và sau đó có hiệu lực theo hành động quản trị trên chuỗi trước đó.

TẠM THỜI-03 (x) Rút tiền kho bạc **phải** nhất quán với (các) ngân sách của hệ sinh thái Cardano Blockchain đã được cộng đồng phê duyệt.

TẠM THỜI-04 (x) Người nắm giữ ADA **phải** đã phê chuẩn Hiến pháp cuối cùng như quy định tại Điều II này trước khi phê chuẩn bất kỳ đề xuất nào khác **"hiến pháp mới"** , **"cập nhật ủy ban hiến pháp và/hoặc ngưỡng và/hoặc điều khoản"** , Và **"động thái bất tín"** các hoạt động quản trị.

TẠM THỜI-05 (x) **"Kích bản lan can mới"** các hành động phù hợp với Hiến pháp tạm thời có thể được phê chuẩn trong thời gian tạm thời, miễn là bản thân Hiến pháp tạm thời không bị thay đổi.

10. DANH SÁCH NHÓM THAM SỐ GIAO THỨC

Các tham số giao thức được nhóm theo loại, cho phép đặt các ngưỡng khác nhau cho mỗi nhóm.

Nhóm mạng bao gồm:

kích thước cơ thể khối tối đa (`maxBlockBodySize`)

quy mô giao dịch tối đa (kích thước tối đa `TxSize`)

kích thước tiêu đề khối tối đa (kích thước `maxBlockHeader`)

kích thước tối đa của giá trị tài sản được tuần tự hóa (`maxValueSize`)

đơn vị thực thi tập lệnh tối đa trong một giao dịch (`maxTxExecutionUnits[bước]`)

đơn vị thực thi tập lệnh tối đa trong một khối (`maxBlockExecutionUnits[bước]`)

số lượng đầu vào tài sản đảm bảo tối đa (*maxTài sản thể chấpĐầu vào*)

Nhóm kinh tế gồm có:

hệ số phí tối thiểu (*txFeePerByte*)
hằng số phí tối thiểu (*txFeeFixed*)
phí tối thiểu mỗi byte cho các tập lệnh tham chiếu (*minPhíRefScriptCoinsPerByte*)
chìa khóa ủy nhiệm Tiền gửi Lovelace (cổ phầnĐịa chỉ tiền gửi)
đăng ký hồ bơi Tiền gửi Lovelace (cổ phầnPoolGửi tiền)
mở rộng tiền tệ (tiền tệMở rộng)
mở rộng kho bạc (kho bạcCất)
cắt giảm phần thưởng cố định tối thiểu cho các nhóm (phútPoolChi phí)
tiền gửi Lovelace tối thiểu cho mỗi byte UTxO được tuân tự hóa (*utxoCostPerByte*)
giá các đơn vị thực thi Plutus (thực thiUnitPrices[priceSteps/priceMemory])

Nhóm kỹ thuật bao gồm:

ảnh hưởng của cam kết pool (*poolPledgeẢnh hưởng*)
kỷ nguyên nghỉ hưu tối đa của nhóm (*poolRetireMaxEpoch*)
số lượng hồ bơi mong muốn (*stakePoolTargetNum*)
Mô hình chi phí thực hiện Plutus (chi phíMô hình)
tỷ lệ tài sản thể chấp cần thiết cho các tập lệnh (phần trăm tài sản thể chấp)

Nhóm quản trị bao gồm tất cả các tham số giao thức mới được giới thiệu trong CIP-1694:

ngưỡng biểu quyết quản trị (*dRepVotingThresholds[...], poolVotingThresholds[...]*)
hành động quản trị thời gian tồn tại tối đa trong các kỷ nguyên (*govHành độngTron đời*)
tiền gửi hành động quản trị (chính phủHành độngGửi tiền)
Số tiền gửi DRep (*dRepGửi tiền*)
Thời gian hoạt động DRep trong các kỷ nguyên (*dRepHoạt động*)
quy mô ủy ban hiến pháp tối thiểu (ủy banKích thước tối thiểu)
thời hạn nhiệm kỳ tối đa (tính theo thời điểm) đối với các thành viên ủy ban hiến pháp (ủy banMaxTermLimit)

Điều VIII - SỬA ĐỔI

Trừ khi có quy định khác ở đây, các sửa đổi Hiến pháp này sẽ được cơ quan quản lý có thẩm quyền phê duyệt bằng hành động quản trị trực tuyến với ngưỡng không ít hơn 67% số cổ phần bỏ phiếu đang hoạt động khi đó.

Các thay đổi đối với Guardrails có thể được thực hiện bằng hành động quản trị trên chuỗi đáp ứng ngưỡng đa số cổ phần đang hoạt động của các SPO bỏ phiếu..

ĐIỀU IX - GIẢI QUYẾT TRANH CHẤP

Giải quyết tranh chấp theo cách tiết kiệm chi phí là rất quan trọng đối với hệ sinh thái Cardano Blockchain. Ủy ban giải quyết tranh chấp sẽ được thành lập (trong vòng chín mươi (90) ngày?) sau khi phê chuẩn Điều lệ, bao gồm DReps, SPO và các thành viên của Ủy ban Hiến pháp, với mục tiêu nghiên cứu các phương pháp giải quyết tranh chấp trên chuỗi và ngoài chuỗi phù hợp cho blockchain và đưa ra một khuôn khổ giải quyết tranh chấp cho những tranh chấp phù hợp để giải quyết trên chuỗi hoặc với các thủ tục ngoài chuỗi đã được thống nhất.. Trong vòng một (1) năm (?) sau khi phê chuẩn Hiến pháp này trên chuỗi , MỘT việc sửa đổi Hiến pháp sẽ được đề xuất để quản lý việc giải

quyết tranh chấp. Nếu không có khuôn khổ như vậy được phê chuẩn, việc rút tiền kho bạc cho Catalyst hoặc cho các cá nhân hoặc công ty đang tìm kiếm nguồn vốn để phát triển trên blockchain phải cung cấp chi tiết về các cơ chế giải quyết tranh chấp đã được thống nhất như một phần trong đề xuất của họ. Tính đầy đủ của điều này sẽ được đánh giá bởi những người bỏ phiếu cho các đề xuất đó và sẽ là yếu tố chính quyết định liệu nguồn tài trợ có được cung cấp hay không. .

Hiến pháp này tìm cách khuyến khích các thành viên của cộng đồng blockchain Cardano tham gia vào quản trị. Để tạo điều kiện thuận lợi cho việc này, người ta thống nhất rằng SPO, DReps, thành viên Ủy ban Hiến pháp và thành viên Ủy ban Giải quyết Tranh chấp cũng như những người khác tham gia quản trị sẽ được miễn trách nhiệm pháp lý và kiện tụng đối với các hành động được thực hiện trong quá trình thực hiện nhiệm vụ thông thường của họ. Quyền miễn trừ này sẽ không được áp dụng nếu hành động của các thành viên đó được xác định là nằm ngoài quá trình và phạm vi nhiệm vụ thông thường của họ hoặc được xác định là vi phạm luật hình sự trong khu vực tài phán hiện hành. Chỉ không đồng ý với phiếu bầu của những cá nhân đó không đủ cơ sở để khởi kiện.