

CIP-1694

Bước đầu tiên hướng tới Quản trị phi tập trung trên chuỗi

CIP	Trạng thái	Danh mục	Ngày tạo	Giấy phép
1694	Đã đề xuất	Sổ cái	18/11/2022	CC-BY-4.0

Đồng tác giả

- Jared Corduan <jared.corduan@iohk.io>
- Andre Knispel <andre.knispel@iohk.io>
- Matthias Benkort <matthias.benkort@cardanofoundation.org>
- Kevin Hammond <kevin.hammond@iohk.io>
- Charles Hoskinson <charles.hoskinson@iohk.io>
- Samuel Leathers <samuel.leathers@iohk.io>

Các phiên thảo luận

- Yêu cầu thay đổi số [380](#) của CIP
- Thảo luận cùng [Swarm](#) ngày 08/02/2023
- Thảo luận cùng [Charles Hoskinson](#) ngày 05/03/2023
- Thảo luận cùng [Richard McCrackn](#) ngày 06/03/2023
- Thảo luận cùng [Richard McCrackn](#) ngày 07/03/2023
- Thảo luận cùng [KtorZ](#) ngày 05/03/2023
- Thảo luận cùng [KtorZ](#) ngày 27/02/2023
- Thảo luận cùng [KtorZ](#) ngày 03/03/2023
- Thảo luận cùng [Danny Ribar](#) ngày 03/03/2023
- Thảo luận cùng [Digital Fortress](#) ngày 04/03/2023
- Thảo luận cùng [Swarm](#) ngày 16/02/2023

Tóm tắt

Chúng tôi đề xuất một bản sửa đổi hệ thống quản trị trên chuỗi của Cardano để hỗ trợ các yêu cầu mới cho Voltaire. Hỗ trợ quản trị chuyên biệt hiện tại cho cập nhật tham số giao thức và chứng chỉ MIR sẽ bị loại bỏ, và hai trường mới sẽ được thêm vào các phần thân giao dịch bình thường cho:

- hành động quản trị
- phiếu bầu

Bất kỳ người dùng Cardano nào cũng sẽ được phép nộp một **hành động quản trị**. Chúng tôi cũng giới thiệu ba cơ quan quản trị riêng biệt có các chức năng cụ thể trong khung quản trị mới này:

- một Ủy ban Hiến pháp
- một nhóm các đại diện được ủy quyền (sau đây gọi là DReps)
- các nhà vận hành pool uỷ thác (sau đây gọi là SPOs)

Mỗi hành động quản trị phải được ít nhất hai trong ba cơ quan quản trị này phê chuẩn bằng các phiếu bầu của họ trên chuỗi. Loại hành động và trạng thái của hệ thống quản trị sẽ quyết định cơ quan nào phải phê chuẩn nó.

Các hành động đã được phê chuẩn sau đó sẽ được thực hiện trên chuỗi, tuân theo một bộ quy tắc được xác định rõ ràng.

Cũng giống như các pool uỷ thác, bất kỳ chủ sở hữu ADA nào cũng có thể đăng ký trở thành một DRep và do đó chọn để đại diện cho chính họ và/hoặc người khác. Cũng giống như các pool uỷ thác, các chủ sở hữu ADA có thể, thay vào đó, ủy quyền quyền bầu cử của họ cho bất kỳ DRep nào khác. Quyền bầu cử sẽ dựa trên tổng số ADA được ủy quyền, tính theo số nguyên của Lovelace.

Do đó, khía cạnh quan trọng nhất của đề xuất này là khái niệm **"một Lovelace = một phiếu bầu"**.

Để biết danh sách những người đóng góp cho đề xuất này, hãy xem phần [Lời Cảm Ơn](#).

Động lực: tại sao cần có CIP này?

- [Mục tiêu](#)
- [Thiết kế hiện tại](#)
- [Những thiếu sót của thiết kế quản trị Shelley](#)
- [Ngoài phạm vi](#)

Mục tiêu

Chúng ta đang hướng tới kỷ nguyên Voltaire, đặt nền tảng cho việc ra quyết định phi tập trung. CIP này mô tả một cơ chế quản trị trên chuỗi sẽ hỗ trợ giai đoạn Voltaire của Cardano. CIP xây dựng và mở rộng kế hoạch quản trị Cardano ban đầu dựa trên một số lượng cố định các khóa quản trị. Nó nhằm mục đích cung cấp một bước đầu tiên vừa có giá trị vừa quan trọng, đồng thời cũng khả thi về mặt kỹ thuật trong tương lai gần như một phần của hệ thống quản trị Voltaire được đề xuất. Nó cũng tìm cách hoạt động như một điểm khởi đầu cho đầu vào liên tục của cộng đồng, bao gồm cả các cài đặt ngưỡng phù hợp và các cài đặt trên chuỗi khác. Các đề xuất tiếp theo có thể điều chỉnh và mở rộng đề xuất này để đáp ứng nhu cầu quản trị mới nổi.

Thiết kế cơ chế quản trị hiện tại

Cơ chế quản trị Cardano trên chuỗi được giới thiệu trong kỷ nguyên sổ cái Shelley có khả năng:

1. sửa đổi các giá trị của các tham số giao thức (bao gồm cả việc khởi tạo "hard fork")
2. chuyển ADA ra khỏi quỹ dự trữ và kho bạc (và cũng di chuyển ADA giữa quỹ dự trữ và kho bạc)

Trong kế hoạch hiện tại, các hành động quản trị được khởi tạo bởi các giao dịch đặc biệt yêu cầu ủy quyền Quorum-Many từ các khóa quản trị (5 trong số 7 trên mạng chính)

Cardano). Các trường trong thân giao dịch cung cấp chi tiết về hành động quản trị được đề xuất: hoặc i) thay đổi tham số giao thức; hoặc ii) khởi tạo chuyển tiền. Mỗi giao dịch có thể kích hoạt cả hai loại hành động quản trị, và một hành động duy nhất có thể có nhiều hơn một hiệu ứng (ví dụ: thay đổi hai hoặc nhiều tham số giao thức).

- Cập nhật tham số giao thức sử dụng trường giao dịch số 6 của thân giao dịch.
- Việc di chuyển kho bạc và dự trữ sử dụng các chứng chỉ Di chuyển Phần thưởng Tức thời (viết tắt là MIR).

Các hành động quản trị được ủy quyền đúng cách được áp dụng trên ranh giới epoch (mà chúng **được ban hành**).

Hard Fork

Một trong những tham số giao thức đủ quan trọng để xứng đáng được chú ý đặc biệt: thay đổi phiên bản giao thức chính cho phép Cardano ban hành các hard fork được kiểm soát. Do đó, loại cập nhật tham số giao thức này có trạng thái đặc biệt, vì các Pool uỷ thác phải nâng cấp các nốt mạng của họ để có thể hỗ trợ phiên bản giao thức mới sau khi hard fork được ban hành.

Những thiếu sót của thiết kế quản trị Shelley

Thiết kế quản trị Shelley nhằm mục đích cung cấp một cách tiếp cận quản trị đơn giản, chuyển tiếp. Đề xuất này nhằm giải quyết một số thiếu sót của thiết kế đó khi chúng tôi chuyển sang Voltaire.

1. Thiết kế quản trị Shelley không có chỗ cho sự tham gia tích cực trên chuỗi của người nắm giữ ADA. Mặc dù những thay đổi đối với giao thức thường là kết quả của các cuộc thảo luận với các nhân tố cộng đồng được lựa chọn, nhưng quá trình này hiện do các thực thể sáng lập điều khiển chủ yếu. Đảm bảo rằng mọi người có thể bày tỏ quan ngại của mình là điều công bằng và đôi khi có thể bị coi là tùy tiện.
2. Việc di chuyển tiền từ kho bạc là một chủ đề quan trọng và nhạy cảm. Tuy nhiên, chúng có thể khó theo dõi. Điều quan trọng là phải có thêm tính minh bạch và nhiều lớp kiểm soát hơn đối với các hoạt động di chuyển tiền này.
3. Mặc dù cần được các SPO xử lý đặc biệt, nhưng hard fork không được phân biệt với các thay đổi tham số giao thức khác.
4. Cuối cùng, mặc dù hiện có một tầm nhìn chung về Cardano được các thực thể sáng lập và nhiều thành viên cộng đồng chia sẻ, nhưng không có tài liệu được xác định rõ ràng ghi lại các nguyên tắc hướng dẫn này. Thật hợp lý khi tận dụng blockchain Cardano để ghi lại tinh thần Cardano chung theo cách không thể thay đổi, dưới dạng Hiến pháp Cardano chính thức.

Ngoài phạm vi

Các chủ đề sau được coi là ngoài phạm vi của CIP này.

Nội dung của hiến pháp

CIP này chỉ tập trung vào các cơ chế trên chuỗi. Các điều khoản của hiến pháp ban đầu là cực kỳ quan trọng, cũng như bất kỳ quy trình nào cho phép sửa đổi nó. Những điều này xứng đáng được thảo luận riêng biệt và tập trung.

Thành viên của Ủy ban Hiến pháp

Đây là một vấn đề ngoài chuỗi.

Các vấn đề pháp lý

Bất kỳ việc thực thi pháp lý tiềm năng nào đối với giao thức Cardano hoặc Hiến pháp Cardano đều hoàn toàn nằm ngoài phạm vi của CIP này.

Các tiêu chuẩn ngoài chuỗi cho các hành động quản trị

Cộng đồng Cardano phải suy nghĩ sâu sắc về các tiêu chuẩn và quy trình chính xác để xử lý việc tạo ra các hành động quản trị được chỉ định trong CIP này. Đặc biệt, vai trò của Dự án Catalyst trong việc tạo ra các hành động rút tiền kho bạc hoàn toàn nằm ngoài phạm vi của CIP này.

Sở hữu và ủy quyền ADA

Cách thức bất kỳ công ty tư nhân, tổ chức công cộng hoặc tư nhân, cá nhân, v.v. lựa chọn nắm giữ hoặc ủy quyền ADA của họ, bao gồm cả việc ủy quyền cho các Pool ủy thác hoặc DRep, nằm ngoài phạm vi của CIP này.

Đặc tả kỹ thuật

[Hiến pháp Cardano](#)

[Ủy ban Hiến pháp](#)

- [Trạng thái Bất tín nhiệm](#)
- [Các khóa Ủy ban Hiến pháp](#)
- [Thay thế Ủy ban Hiến pháp](#)
- [Quy mô của Ủy ban Hiến pháp](#)
- [Nhiệm kỳ](#)
- [Tập lệnh rào chắn](#)

[Đại diện được ủy quyền \(DRep\)](#)

- [Các tùy chọn bỏ phiếu được xác định trước](#)
- [DRep đã đăng ký](#)
- [Phân phối cổ phần mới cho DRep](#)
- [Khuyến khích người nắm giữ ADA ủy quyền cổ phần bỏ phiếu](#)

- [Khuyến khích DRep](#)

[Các hành động quản trị](#)

- [Phê chuẩn](#)
 - [Yêu cầu](#)
 - [Giới hạn](#)
- [Thực thi](#)
- [Vòng đời](#)
- [Nội dung](#)
- [Các nhóm tham số giao thức](#)

[Bỏ phiếu](#)

- [Trang thái quản trị](#)
- [Thay đổi ảnh chụp cổ phần](#)
- [Định nghĩa liên quan đến cổ phần bỏ phiếu](#)

Hiến pháp Cardano

Hiến pháp Cardano là một tài liệu văn bản định nghĩa các giá trị chung và nguyên tắc hướng dẫn của Cardano. Tại giai đoạn này, Hiến pháp là một tài liệu thông tin nắm bắt rõ ràng các giá trị cốt lõi của Cardano và đảm bảo tính bền vững lâu dài của nó. Ở giai đoạn sau, chúng ta có thể hình dung Hiến pháp có thể phát triển thành một bộ quy tắc dựa trên hợp đồng thông minh điều khiển toàn bộ khuôn khổ quản trị. Tuy nhiên, hiện tại, Hiến pháp sẽ vẫn là một tài liệu ngoài chuỗi có giá trị bám được ghi lại trên chuỗi. Như đã thảo luận ở trên, Hiến pháp chưa được xác định và nội dung của nó nằm ngoài phạm vi của CIP này.

Ủy ban Hiến pháp

Chúng tôi định nghĩa một Ủy ban Hiến pháp đại diện cho một tập hợp các cá nhân hoặc thực thể (mỗi cá nhân hoặc thực thể được liên kết với một chứng chỉ Ed25519 hoặc tập lệnh gốc hoặc tập lệnh Plutus) có trách nhiệm tập thể đảm bảo rằng **Hiến pháp được tôn trọng**.

Mặc dù **không thể được thi hành trên chuỗi**, nhưng Ủy ban Hiến pháp chỉ được cho phép bỏ phiếu về tính hợp hiến của các hành động quản trị (do đó đảm bảo tính bền vững lâu dài của blockchain) và nên được thay thế (thông qua hành động Bất tín nhiệm) nếu họ vượt quá ranh giới này. Nói cách khác, có một hợp đồng xã hội giữa Ủy ban Hiến pháp và các tác nhân của mạng lưới. Mặc dù Ủy ban Hiến pháp có thể từ chối một số hành động quản trị (bằng cách bỏ phiếu 'Chống' cho hành động đó), nhưng họ chỉ nên làm như vậy khi các hành động quản trị đó xung đột với Hiến pháp.

Ví dụ: nếu chúng ta xem xét quy tắc Hiến pháp giả định "Mạng lưới Cardano phải luôn có thể tạo ra các khối mới", thì một hành động quản trị sẽ giảm kích thước khối tối đa xuống 0 sẽ là vi hiến, và do đó có thể không được Ủy ban Hiến pháp phê chuẩn. Tuy nhiên, quy tắc

không chỉ định kích thước khối tối đa nhỏ nhất được chấp nhận, vì vậy Ủy ban Hiến pháp sẽ cần xác định số này và bỏ phiếu tương ứng.

Trạng thái Bất tín nhiệm

Ủy ban Hiến pháp được coi là ở một trong hai trạng thái sau tại mọi thời điểm:

1. trạng thái Bình thường (tức là trạng thái Tín nhiệm)
2. trạng thái Bất tín nhiệm

Trong trạng thái Bất tín nhiệm, ủy ban hiện tại không còn có thể tham gia vào các hành động quản trị và phải được thay thế trước khi bất kỳ hành động quản trị nào có thể được phê chuẩn (xem bên dưới).

Các khóa Ủy ban Hiến pháp

Ủy ban Hiến pháp sẽ sử dụng thiết lập khóa nóng và lạnh, tương tự như cơ chế "chứng chỉ ủy quyền khởi tạo" hiện có.

Thay thế Ủy ban Hiến pháp

Ủy ban Hiến pháp có thể bị thay thế thông qua một hành động quản trị cụ thể ("Cập nhật ủy ban", được mô tả bên dưới) yêu cầu sự chấp thuận của cả SPO và DRep. Ngưỡng phê chuẩn có thể khác nhau tùy thuộc vào việc quản trị ở trạng thái bình thường hay trạng thái Bất tín nhiệm. Ủy ban Hiến pháp mới về nguyên tắc có thể giống hệt hoặc chòng chéo một phần với ủy ban cũ, miễn là hành động được phê chuẩn đúng cách. Điều này có thể xảy ra, ví dụ, nếu cử tri có niềm tin chung vào toàn bộ hoặc một phần của ủy ban và muốn gia hạn nhiệm kỳ của họ.

Quy mô của Ủy ban Hiến pháp

Không giống như thiết kế quản trị của Shelley, quy mô của Ủy ban Hiến pháp không cố định và có thể là bất kỳ số không âm nào. Quy mô này có thể thay đổi bất cứ khi nào một ủy ban mới được bầu ("Cập nhật Ủy ban"). Tương tự như vậy, ngưỡng ủy ban (tỷ lệ phiếu Thuận của ủy ban cần thiết để phê chuẩn các hành động quản trị) không cố định và cũng có thể thay đổi theo hành động quản trị. Điều này mang lại sự linh hoạt hơn cho thành phần của ủy ban. Đặc biệt, có thể bầu một **ủy ban trống** nếu cộng đồng muốn bãi bỏ hoàn toàn Ủy ban Hiến pháp. Lưu ý rằng điều này khác với trạng thái Bất tín nhiệm, và vẫn cấu thành một hệ thống quản trị có khả năng ban hành các đề xuất.

Sẽ có một tham số giao thức mới cho kích thước tối thiểu của ủy ban, chính nó là một số không âm được gọi là tham số *committeeMinSize*.

Nhiệm kỳ

Mỗi Ủy ban Hiến pháp mới được bầu sẽ có một nhiệm kỳ. Nhiệm kỳ của mỗi thành viên cho phép áp dụng chế độ luân phiên, chẳng hạn như một phần ba ủy ban hết hạn mỗi năm. Các

thành viên mãn nhiệm sẽ không còn được bỏ phiếu nữa. Thành viên cũng có thể tự nguyện từ chức sớm, điều này sẽ được đánh dấu trên chuỗi là thành viên mãn nhiệm.

Nếu số lượng thành viên ủy ban đang tại nhiệm mà bị giảm xuống dưới quy mô tối thiểu của ủy ban, Ủy ban Hiến pháp sẽ không thể phê chuẩn các hành động quản trị. Điều này có nghĩa là chỉ những hành động quản trị không yêu cầu bỏ phiếu từ Ủy ban Hiến pháp thì vẫn có thể được phê chuẩn.

Ví dụ, một ủy ban có quy mô năm thành viên với ngưỡng là 60%, trong khi quy mô tối thiểu của ủy ban là ba thành viên, và hai thành viên đã bị miễn nhiệm, thì ủy ban này vẫn có thể thông qua các hành động quản trị nếu hai thành viên đang tại nhiệm bỏ phiếu Thuận. Tuy nhiên, nếu có thêm một thành viên nữa bị miễn nhiệm, thì Ủy ban Hiến pháp đó sẽ không thể phê chuẩn bất kỳ hành động quản trị nào nữa.

Nhiệm kỳ tối đa là một tham số giao thức quản trị, được chỉ định là số kỷ nguyên. Trong trạng thái Bất tín nhiệm, không có hành động nào có thể được phê chuẩn, vì vậy ủy ban nên lập kế hoạch thay thế riêng nếu muốn tránh gián đoạn.

Tập lệnh rào chắn

Trong khi hiến pháp là một tài liệu không chính thức, ngoài chuỗi, cũng sẽ có một tập lệnh tùy chọn có thể thực thi một số hướng dẫn. Tập lệnh này có tác dụng bổ sung cho Ủy ban Hiến pháp bằng cách hạn chế một số loại đề xuất. Ví dụ: nếu cộng đồng muốn có một số quy tắc cứng rắn đối với kho bạc không thể vi phạm, một tập lệnh thực thi các quy tắc này có thể được bỏ phiếu là Tập lệnh Rào chắn.

Tập lệnh Rào chắn chỉ áp dụng cho các đề xuất **Cập nhật tham số giao thức** và **Rút tiền kho bạc**.

Đại diện được ủy quyền (DRep)

Cảnh báo: DRep trong CIP-1694 không nên bị nhầm lẫn với DRep của Project Catalyst.

Các tùy chọn bỏ phiếu được xác định trước

Để tham gia quản trị, một chứng chỉ cổ phần phải được ủy quyền cho một DRep. Những người nắm giữ ADA thường sẽ ủy quyền quyền bỏ phiếu của họ cho một DRep đã đăng ký để thay mặt họ tham gia bỏ phiếu. Ngoài ra, có hai tùy chọn bỏ phiếu được xác định trước:

- **Abstain:**

Nếu một người nắm giữ ADA ủy quyền cho tùy chọn Abstain, thì cổ phần hoạt động của họ được đánh dấu là **không tham gia vào quản trị**.

Tác động của việc ủy quyền cho Abstain trên chuỗi là cổ phần được ủy quyền sẽ không được coi là một phần của cổ phần bỏ phiếu đang hoạt động. Tuy nhiên, cổ

phần sẽ được coi là đã đăng ký với mục đích nhận các khoản tiền thưởng được mô tả trong [Tiền thưởng cho người nắm giữ ADA](#) ủy thác cổ phần bỏ phiếu.

- **No Confident:**

Nếu một người nắm giữ ADA ủy quyền cho tùy chọn **No Confident**, thì cổ phần của họ được tính là phiếu “Thuận” cho mọi hành động Bất tín nhiệm, và phiếu “Chống” cho mọi hành động khác. Cổ phần được ủy quyền sẽ được coi là một phần của cổ phần bỏ phiếu hoạt động. Nó cũng đóng vai trò là một thước đo trực tiếp về sự Tín nhiệm của người nắm giữ ADA đối với Ủy ban Hiến pháp.

Lưu ý: Các tùy chọn bỏ phiếu được xác định trước không bỏ phiếu bên trong các giao dịch, hành vi của chúng được tính đến ở cấp giao thức. Tùy chọn Abstain có thể được chọn vì nhiều lý do, bao gồm cả mong muốn không tham gia vào hệ thống quản trị.

Lưu ý nữa: Bất kỳ người nắm giữ ADA nào cũng có thể tự đăng ký làm DRep và ủy quyền cho chính họ nếu họ muốn tham gia tích cực vào việc bỏ phiếu.

DRep đã đăng ký

Trong Voltaire, thông tin xác thực cổ phần hiện tại sẽ có thể ủy thác cổ phần của họ cho DReps cho mục đích bỏ phiếu, ngoài việc ủy quyền hiện tại cho các pool uỷ thác để sản xuất khối. Ủy quyền DRep sẽ mô phỏng các cơ chế ủy quyền cổ phiếu hiện có (thông qua chứng chỉ trên chuỗi). Tương tự như vậy, đăng ký DRep sẽ mô phỏng các cơ chế đăng ký cổ phần hiện có. Ngoài ra, các DRep đã đăng ký sẽ cần phải bỏ phiếu thường xuyên để vẫn được coi là hoạt động. Cụ thể, nếu một DRep không nộp bất kỳ phiếu bầu nào cho các hành động quản trị *drepActivity* trong nhiều epoch, thì DRep được coi là không hoạt động, trong đó *drepActivity* là một tham số giao thức mới. Các DRep không hoạt động sẽ không được tính vào cổ phần bỏ phiếu đang hoạt động nữa, và có thể hoạt động trở lại với tham số *drepActivity* trong nhiều epoch bằng cách bỏ phiếu cho bất kỳ hành động quản trị nào, hoặc nộp chứng chỉ cập nhật DRep. Lý do đánh dấu DRep là không hoạt động là để các DRep ngừng tham gia nhưng vẫn có cổ phần được ủy quyền cho họ, cuối cùng không rời khỏi hệ thống ở trạng thái không có hành động quản trị nào có thể thông qua.

DRep đã đăng ký được xác định bằng một chứng chỉ có thể là:

- Một khóa xác minh (Ed25519)
- Một tập lệnh gốc hoặc tập lệnh Plutus

Bản mã hoá băm blake2b-224 của một chứng chỉ DRep được chuỗi hoá được gọi là ID DRep.

Các loại chứng chỉ mới sau đây sẽ được thêm vào cho DRep: Chứng chỉ đăng ký DRep, Chứng chỉ miễn nhiệm DRep và chứng chỉ ủy quyền bỏ phiếu.

Chứng chỉ đăng ký DRep

Chứng chỉ đăng ký DRep bao gồm:

- Một ID DRep
- Một khoản tiền đặt cọc
- Một móc neo tùy chọn

Một móc neo là một cặp gồm:

- Một URL đến nội dung tải JSON của siêu dữ liệu
- Một mã băm của nội dung URL của siêu dữ liệu

Cấu trúc và định dạng của siêu dữ liệu này cố ý được để mở trong CIP này. Các quy tắc trên chuỗi sẽ không kiểm tra URL hoặc mã băm. Tuy nhiên, các ứng dụng khách nên thực hiện các kiểm tra hợp lý thông thường khi lấy nội dung từ URL được cung cấp.

Chứng chỉ mãn nhiệm DRep

Chứng chỉ mãn nhiệm DRep bao gồm:

- Một ID DRep

Lưu ý rằng một DRep sẽ bị mãn nhiệm ngay lập tức khi chuỗi chấp nhận chứng chỉ mãn nhiệm và khoản tiền đặt cọc được trả lại như một phần của giao dịch nộp chứng chỉ mãn nhiệm (giống như cách mà khoản đặt cọc đăng ký chứng chỉ cổ phần được trả lại).

Chứng chỉ ủy quyền bỏ phiếu

Chứng chỉ ủy quyền bỏ phiếu bao gồm:

- ID DRep mà cổ phần nên được ủy thác
- Chứng chỉ cổ phần cho người ủy thác

Lưu ý: Việc ủy thác DRep luôn ánh xạ một chứng chỉ cổ phần vào một chứng chỉ DRep. Điều này có nghĩa là một DRep không thể ủy thác cổ phần bỏ phiếu cho một DRep khác.

Các cơ chế ủy quyền chứng chỉ

Cơ chế ủy quyền (tức là chữ ký nào được yêu cầu để đăng ký, mãn nhiệm hoặc ủy quyền) mô phỏng theo cơ chế ủy quyền chứng chỉ cổ phần hiện có.

Phân phối cổ phần mới cho DRep

Ngoài phân phối theo từng chứng chỉ cổ phần và phân phối theo từng Pool ủy thác hiện có, sổ cái giờ đây cũng sẽ xác định phân phối cổ phần cho từng DRep. Phân phối này sẽ xác định mỗi phiếu bầu từ một DRep được hỗ trợ bởi bao nhiêu cổ phần.

Cảnh báo: Không giống như phân phối được sử dụng để sản xuất khối, chúng tôi sẽ luôn sử dụng phiên bản mới nhất của phân phối cổ phần cho mỗi DRep như được đưa ra trên ranh giới epoch.

Điều này có nghĩa là đối với bất kỳ chủ đề nào mà người bỏ phiếu cá nhân quan tâm sâu sắc, họ có thời gian để ủy quyền cho chính mình với tư cách là một DRep và bỏ phiếu trực tiếp. Tuy nhiên, điều đó có nghĩa là có thể có sự khác biệt giữa cổ phần được sử dụng để sản xuất khối và cổ phần được sử dụng để bỏ phiếu trong bất kỳ epoch nào.

Khuyến khích người nắm giữ ADA ủy quyền cổ phần bỏ phiếu

Sẽ có một giai đoạn khởi động ngắn mà trong đó phần thưởng vẫn sẽ được chi trả cho việc ủy thác cổ phần, v.v. và có thể được rút ra bất kỳ lúc nào. Sau giai đoạn này, mặc dù sẽ vẫn tiếp tục được kiếm được phần thưởng cho việc ủy quyền sản xuất khối, v.v., các tài khoản phần thưởng sẽ **bị chặn, không được rút bất kỳ phần thưởng nào**, trừ khi thông tin xác thực cổ phần liên quan của họ cũng được ủy quyền cho DRep hoặc ủy quyền cho các tùy chọn bỏ phiếu được xác định trước. Điều này giúp đảm bảo sự tham gia cao, và do đó đảm bảo tính hợp pháp.

Lưu ý: Mặc dù phần thưởng không thể được rút, nhưng chúng không bị mất đi. Chỉ khi một chứng chỉ cổ phần đã ủy quyền (bao gồm cả ủy quyền cho tùy chọn bỏ phiếu được xác định trước), thì phần thưởng mới có thể được rút.

Khuyến khích DRep

DReps có thể được trả thù lao cho công việc của họ. Nghiên cứu về các mô hình khuyến khích vẫn đang được tiến hành và chúng tôi không muốn trì hoãn việc triển khai CIP này trong khi vấn đề này được giải quyết.

Do đó, đề xuất tạm thời của chúng tôi là ký quỹ Lovelace từ kho bạc Cardano hiện tại cho đến khi quyết định cực kỳ quan trọng này có thể được cộng đồng nhất trí, thông qua cơ chế quản trị trên chuỗi đang được xây dựng.

Ngoài ra, DReps có thể tự trả tiền cho chính họ thông qua các trường hợp hành động quản trị "Rút tiền từ Kho bạc". Hành động như vậy sẽ có thể kiểm toán trên chuỗi và phải phản ánh thỏa thuận ngoài chuỗi giữa DReps và những người ủy thác.

Các hành động quản trị

Chúng tôi định nghĩa bảy loại hành động quản trị khác nhau. Một hành động quản trị là một sự kiện trên chuỗi được kích hoạt bởi một giao dịch và có một thời hạn mà sau đó nó không thể được ban hành nữa.

- Một hành động được cho là được phê chuẩn khi nó thu thập đủ phiếu bầu ủng hộ (thông qua các quy tắc và tham số được nêu chi tiết bên dưới).
- Một hành động không được phê chuẩn trước hạn chót thì sẽ bị cho là đã hết hạn.
- Một hành động đã được phê chuẩn được cho là đã được ban hành khi nó đã được kích hoạt trên mạng lưới.

Hành động	Mô tả
1. Đề xuất Bất tín nhiệm	Một đề xuất tạo ra một trạng thái Bất tín nhiệm đối với Ủy ban Hiến pháp hiện tại
2. Cập nhật ủy ban và/hoặc ngưỡng và/hoặc điều khoản	Thay đổi các thành viên của Ủy ban Hiến pháp, và/hoặc ngưỡng chữ ký của nó, và/hoặc các điều khoản
3. Hiến pháp mới hoặc Tập lệnh Rào chắn	Một sửa đổi Hiến pháp hoặc Tập lệnh Rào chắn, được ghi lại dưới dạng mã băm trên chuỗi
4. Khởi tạo Hard-Fork	Kích hoạt một nâng cấp không tương thích ngược của mạng lưới; yêu cầu có nâng cấp phần mềm trước đó
5. Thay đổi tham số giao thức	Bất kỳ thay đổi nào đối với một hoặc nhiều tham số giao thức có thể cập nhật, ngoại trừ các thay đổi đối với các phiên bản giao thức chính ("hard fork")
6. Rút tiền từ kho bạc	Rút tiền từ kho bạc
7. Thông tin	Một hành động không có tác dụng trên chuỗi, ngoài một bản ghi trên chuỗi

Bất kỳ người nắm giữ ADA nào cũng có thể nộp một hành động quản trị lên chuỗi. Họ phải đặt cọc một khoản tiền với giá trị bằng với tham số *govActionDeposit* tính bằng Lovelace, sẽ được trả lại khi hành động được hoàn tất (cho dù nó được **phê chuẩn** hay **đã hết hạn**). Số tiền đặt cọc sẽ được thêm vào **quỹ đặt cọc**, tương tự như các khoản đặt cọc khóa cổ phần. Nó cũng sẽ được tính vào cổ phần của địa chỉ phần thưởng mà nó sẽ được trả lại, để không làm giảm sức mạnh bỏ phiếu của người nộp đề xuất, để bỏ phiếu cho các hành động của chính họ (và cạnh tranh).

Nếu có một Tập lệnh Rào chắn, giao dịch phải bao gồm tập lệnh đó trong tập hợp các bằng chứng trực tiếp hoặc thông qua các đầu vào tham chiếu, và bất kỳ yêu cầu nào khác mà Tập lệnh Rào chắn đưa ra phải được đáp ứng.

Lưu ý rằng một đề xuất Bất tín nhiệm là một biện pháp cực đoan cho phép người nắm giữ ADA thu hồi quyền lực đã được trao cho Ủy ban Hiến pháp hiện tại.

Lưu ý thêm: Một hành động quản trị riêng lẻ có thể chứa nhiều cập nhật tham số giao thức. Nhiều tham số được liên kết với nhau và có thể yêu cầu di chuyển đồng bộ.

Phê chuẩn

Các hành động quản trị được phê chuẩn thông qua các hành động bỏ phiếu trên chuỗi. Các loại hành động quản trị khác nhau có các yêu cầu phê chuẩn khác nhau nhưng luôn liên quan đến hai trong số ba cơ quan quản trị, ngoại trừ hành động **Khởi tạo hard-fork** và các **tham số giao thức** liên quan đến bảo mật, yêu cầu phê chuẩn của tất cả các cơ quan quản trị. Tùy thuộc vào loại hành động quản trị, một hành động sẽ được phê chuẩn khi một sự kết hợp của các điều kiện sau xảy ra:

- Ủy ban Hiến pháp phê duyệt hành động (số lượng thành viên bỏ phiếu Thuận phải đáp ứng được ngưỡng của Ủy ban Hiến pháp)
- DRep phê duyệt hành động (cổ phần được kiểm soát bởi các DRep bỏ phiếu Thuận phải đáp ứng một ngưỡng nhất định của tổng cổ phần bỏ phiếu đang hoạt động)
- SPO phê duyệt hành động (cổ phần được kiểm soát bởi các SPO bỏ phiếu Thuận phải đáp ứng một ngưỡng nhất định trên tổng cổ phần đang được hoạt động uỷ thác cổ phần trong một epoch)

Cảnh báo: Như đã giải thích ở trên, sự phân phối cổ phần sẽ áp dụng khác nhau đối với DRep và SPO.

Một đề xuất thành công về các hành động **Bất tín nhiệm, Cập nhật Ủy ban Hiến pháp, Thay đổi Hiến pháp** hoặc **Hard-fork**, sẽ làm trì hoãn việc phê chuẩn tất cả các hành động quản trị khác cho đến epoch đầu tiên sau khi chúng được ban hành. Điều này cung cấp cho Ủy ban Hiến pháp mới được cập nhật sẽ có đủ thời gian để bỏ phiếu cho các đề xuất hiện tại, đánh giá lại các đề xuất hiện có đối với một hiến pháp mới và đảm bảo rằng các thay đổi ngữ nghĩa tùy ý về nguyên tắc do việc ban hành một hard-fork gây ra sẽ không có hậu quả không mong muốn khi kết hợp với các hành động khác.

Yêu cầu

Bảng sau đây là chi tiết các yêu cầu phê chuẩn cho từng kịch bản hành động quản trị. Các cột đại diện:

- **Loại hành động quản trị**
 - Loại hành động quản trị. Lưu ý rằng các cập nhật tham số giao thức được nhóm thành bốn loại.
- Ủy ban Hiến pháp (viết tắt là **CC**)
 - Giá trị ✓ cho biết Ủy ban Hiến pháp phải phê duyệt hành động này.
 - Giá trị - có nghĩa là phiếu bầu của Ủy ban Hiến pháp không được áp dụng.
- **DRep**
 - Ngưỡng phiếu DRep phải đạt được dưới dạng phần trăm của cổ phần bỏ phiếu hoạt động.
- **SPO**
 - Ngưỡng phiếu SPO phải đạt được dưới dạng phần trăm của cổ phần do tất cả các Pool uỷ thác nắm giữ.
 - Giá trị - có nghĩa là phiếu bầu của SPO không áp dụng.

Loại hành động quản trị	CC	DRep	SPO
1. Đề xuất Bất tín nhiệm	-	P1	Q1
2a. Cập nhật ủy ban/ngưỡng (trạng thái bình thường)	-	P2a	Q2a
2b. Cập nhật ủy ban/ngưỡng (trạng thái Bất tín nhiệm)	-	P2b	Q2b
3. Hiến pháp mới hoặc Tập lệnh Rào chắn	✓	P3	-

4. Khởi tạo Hard-fork	✓	P4	Q4
5a. Thay đổi tham số giao thức, nhóm mạng	✓	P5a	-
5b. Thay đổi tham số giao thức, nhóm kinh tế	✓	P5b	-
5c. Thay đổi tham số giao thức, nhóm kỹ thuật	✓	P5c	-
5d. Thay đổi tham số giao thức, nhóm quản trị	✓	P5d	-
6. Rút tiền từ kho bạc	✓	P6	-
7. Thông tin	✓	100	100

Mỗi ngưỡng này là một tham số quản trị. Có một ngưỡng bổ sung, ngưỡng Q5, liên quan đến các tham số giao thức liên quan đến bảo mật, được giải thích bên dưới. Các ngưỡng ban đầu nên được toàn bộ cộng đồng Cardano lựa chọn. Tất cả các ngưỡng cho hành động Thông tin được đặt thành 100% vì đặt nó thấp hơn sẽ dẫn đến không thể thăm dò trên ngưỡng.

Một số tham số liên quan đến các thuộc tính bảo mật của hệ thống. Bất kỳ đề xuất nào cố gắng thay đổi một tham số như vậy đều yêu cầu bỏ phiếu bổ sung của SPO, với ngưỡng Q5.

Các tham số giao thức liên quan đến bảo mật là:

- *maxBlockBodySize*
- *maxTxSize*
- *maxBlockHeaderSize*
- *maxValueSize*
- *maxBlockExecutionUnits*
- *txFeePerByte* *txFeeFixed*
- *utxoCostPerByte*
- *govActionDeposit*
- *minFeeRefScriptCostPerByte*

Lưu ý: Có thể hợp lý cho một số hoặc tất cả các ngưỡng được điều chỉnh theo Lovelace được đăng ký tích cực để bỏ phiếu. Ví dụ: một ngưỡng có thể thay đổi giữa 51% đối với mức đăng ký cao và 75% đối với mức đăng ký thấp. Hơn nữa, ngưỡng kho bạc cũng có thể được điều chỉnh, tùy thuộc vào tổng số Lovelace được rút ra hoặc các ngưỡng khác nhau có thể được đặt cho các mức rút khác nhau.

Lưu ý: Để đạt được tính hợp pháp, ngưỡng chấp nhận tối thiểu không nên thấp hơn 50% cổ phần được ủy quyền.

Giới hạn

Ngoài các hành động **Rút tiền từ kho bạc** và **Thông tin**, chúng tôi bao gồm một cơ chế để đảm bảo rằng các hành động quản trị cùng loại không vô tình xung đột với nhau theo cách không mong muốn.

Mỗi hành động quản trị phải bao gồm ID hành động quản trị cho hành động được ban hành gần nhất của loại hành động đó. Điều này có nghĩa là hai hành động cùng loại có thể được ban hành cùng một lúc, nhưng chúng phải được thiết kế một cách có chủ đích để thực thi được.

Thực thi

Các hành động đã được phê chuẩn trong epoch hiện tại được ưu tiên thực thi như sau:

- Đề xuất bất tín nhiệm
- Cập nhật ủy ban/ngưỡng
- Hiến pháp mới hoặc Tập lệnh Rào chắn
- Khởi tạo Hard Fork
- Thay đổi tham số giao thức
- Rút tiền từ kho bạc
- Thông tin

Lưu ý: Hành động Thông tin không thể được phê chuẩn hoặc thực thi vì chúng không có ảnh hưởng nào đến giao thức.

Thứ tự thực thi

Các hành động quản trị được thực thi theo thứ tự chấp nhận vào chuỗi. Điều này giải quyết các xung đột, ví dụ: có hai thay đổi tham số cạnh tranh.

Vòng đời

Các hành động quản trị chỉ được kiểm tra để phê chuẩn tại ranh giới epoch. Sau khi được phê chuẩn, các hành động được đưa vào giai đoạn thực thi.

Do đó, tất cả các hành động quản trị được gửi sẽ:

- được phê chuẩn, sau đó được thực thi
- hoặc hết hạn sau một số epoch

Trong tất cả các trường hợp, tiền đặt cọc được trả lại ngay lập tức.

Tất cả các hành động quản trị được thực thi tại ranh giới epoch sau khi được phê chuẩn.

Nội dung

Mỗi hành động quản trị sẽ bao gồm:

- một số tiền đặt cọc (được ghi lại kể từ khi số tiền đặt cọc là một tham số giao thức có thể cập nhật)
- một địa chỉ nhận thưởng để nhận tiền đặt cọc khi nó được trả lại
- một móc neo cho bất kỳ siêu dữ liệu nào cần thiết để giải thích cho hành động

- một giá trị mã băm để ngăn chặn xung đột với các hành động cạnh tranh cùng loại (như mô tả trước đó)

Ngoài ra, mỗi hành động sẽ bao gồm một số yếu tố cụ thể cho loại của nó

Loại hành động quản trị	Dữ liệu bổ sung
1. Đề xuất Bất tín nhiệm	Không có
2. Cập nhật ủy ban/ngưỡng	Bộ băm khóa xác minh (các thành viên bị xóa khỏi uỷ ban), một bản đồ của băm khóa xác minh đến số epoch (thành viên mới và giới hạn nhiệm kỳ của họ) và một giá trị phần trăm (ngưỡng mới)
3. Hiến pháp mới hoặc Tập lệnh Rào chắn	Một neo cho Hiến pháp và một băm kịch bản tùy chọn của Tập lệnh Rào chắn
4. Khởi tạo hard-fork	Phiên bản giao thức chính mới (lớn hơn)
5. Thay đổi tham số giao thức	Các tham số đã thay đổi
6. Rút tiền từ kho bạc	Một ánh xạ từ thông tin chứng chỉ cổ phần đến một số dương tính bằng Lovelace
7. Thông tin	Không có dữ liệu bổ sung

Lưu ý: Phiên bản giao thức chính mới phải lớn hơn chính xác một so với phiên bản giao thức hiện tại. Do đó, bất kỳ hai epoch liên tiếp nào cũng sẽ có cùng phiên bản giao thức chính hoặc phiên bản sau sẽ có phiên bản giao thức chính lớn hơn một.

Lưu ý nữa: Không thể có sự trùng lặp các thành viên ủy ban - mỗi cập thông tin xác thực trong một Ủy ban phải là duy nhất.

Mỗi hành động quản trị được chấp nhận trên chuỗi sẽ được gán một ID duy nhất (còn được gọi là ID hành động quản trị), bao gồm mã băm giao dịch tạo ra nó và chỉ mục trong thân giao dịch trỏ đến nó.

Nhóm Tham số Giao thức

Chúng tôi đã nhóm các tham số giao thức thay đổi theo loại, cho phép đặt các ngưỡng khác nhau cho mỗi nhóm.

Tuy nhiên, chúng tôi không hạn chế mỗi hành động quản trị tham số giao thức phải được chứa trong một nhóm. Trong trường hợp một hành động quản trị mang theo các cập nhật cho nhiều tham số từ các nhóm khác nhau, ngưỡng tối đa của tất cả các nhóm liên quan sẽ áp dụng cho bất kỳ hành động quản trị nào như vậy.

Các nhóm tham số *mạng*, *kinh tế* và *kỹ thuật* thu thập các tham số giao thức hiện có được giới thiệu trong kỷ Shelley, Alonzo và Babbage. Ngoài ra, chúng tôi giới thiệu một nhóm quản trị mới dành riêng cho các tham số quản trị mới sẽ được giới thiệu bởi CIP-1694.

Nhóm mạng bao gồm:

- Kích thước tối đa của thân khối (*maxBlockBodySize*)
- Kích thước tối đa của giao dịch (*maxTxSize*)
- Kích thước tối đa của tiêu đề khối (*maxBlockHeaderSize*)
- Kích thước tối đa của giá trị tài sản được chuỗi hoá (*maxValueSize*)
- Số lượng tối đa các đơn vị thực thi tập lệnh trong một giao dịch đơn lẻ (*maxTxExecutionUnits*)
- Số lượng tối đa các đơn vị thực thi tập lệnh trong một khối đơn lẻ (*maxBlockExecutionUnits*)
- Giá trị tối đa khoản thế chấp đầu vào (*maxCollateralInputs*)

Nhóm kinh tế bao gồm:

- Hệ số phí tối thiểu (*txFeePerByte*)
- Hằng số phí tối thiểu (*txFeeFixed*)
- Tiền đặt cọc đối với khóa ủy quyền tính bằng Lovelace (*stakeAddressDeposit*)
- Tiền đặt cọc đối với đăng ký pool tính bằng Lovelace (*stakePoolDeposit*)
- Mở rộng tiền tệ (*monetaryExpansion*)
- Phần cắt cho kho bạc (*treasuryCut*)
- Phí cố định tối thiểu cắt cho pool (*minPoolCost*)
- Tiền đặt cọc tối thiểu cho mỗi byte UTxO được chuỗi hoá tính theo Lovelace (*utxoCostPerByte*)
- Giá của các đơn vị thực thi Plutus (*executionUnitPrices*)

Nhóm kỹ thuật bao gồm:

- Ảnh hưởng tiền cam kết của pool (*poolPledgeInfluence*)
- Số epoch tối đa để pool thông báo giải thể (*poolRetireMaxEpoch*)
- Số lượng pool mong muốn (*stakePoolTargetNum*)
- Mô hình chi phí thực thi Plutus (*costModels*)
- Tỷ lệ thế chấp cần thiết cho các tập lệnh (*collateralPercentage*)

Nhóm quản trị bao gồm:

Tất cả các tham số giao thức mới được giới thiệu trong CIP này:

- Ngưỡng bỏ phiếu quản trị (*P1, P2a, P2b, P3, P4, P5a, P5b, P5c, P5d, P6, Q1, Q2a, Q2b, Q4, Q5*)
- Thời gian tối đa của hành động quản trị tính theo số epoch (*govActionLifetime*)
- Số tiền đặt cọc đối với hành động quản trị (*govActionDeposit*)
- Số tiền đặt cọc đối với DRep (*dRepDeposit*)
- Nhiệm kỳ hoạt động của DRep tính theo số epoch (*dRepActivity*)

- Quy mô tối thiểu Ủy ban Hiến pháp (`committeeMinSize`)
- Nhiệm kỳ tối đa cho các thành viên Ủy ban Hiến pháp tính theo số epoch (`committeeMaxTermLength`)

Bỏ phiếu

Mỗi giao dịch bỏ phiếu bao gồm:

- ID hành động quản trị
- Vai trò - thành viên Ủy ban Hiến pháp, DRep hoặc SPO
- Chứng chỉ quản trị cho vai trò
- Một neo tùy chọn (như được định nghĩa ở trên) cho thông tin liên quan đến phiếu bầu
- Phiếu bầu 'Thuận'/'Chống'/'Trắng'

Đối với SPO và DRep, số phiếu được bỏ (cho dù là 'Thuận', 'Chống' hay 'Trắng') tỷ lệ thuận với số Lovelace được ủy quyền cho họ tại thời điểm kiểm tra phê chuẩn hành động. Đối với các thành viên Ủy ban Hiến pháp, mỗi thành viên ủy ban hiện tại có một phiếu bầu.

Cảnh báo: Phiếu bầu 'Trắng' không được bao gồm trong "cổ phần bỏ phiếu hoạt động".

Lưu ý rằng một phiếu trắng rõ ràng khác với việc không tham gia bỏ phiếu. Cổ phần chưa đăng ký không bỏ phiếu sẽ hoạt động như một phiếu 'Trắng', trong khi cổ phần đã đăng ký không bỏ phiếu sẽ hoạt động như một phiếu 'Chống'. Để tránh nhầm lẫn, chúng tôi sẽ chỉ sử dụng từ phiếu 'Trắng' từ thời điểm này trở đi để chỉ một phiếu trắng trên chuỗi.

Chứng chỉ quản trị sẽ kích hoạt các xác minh phù hợp trong sổ cái theo quy tắc sổ cái UTxO hiện có (tức là kiểm tra chữ ký cho các khóa xác minh và thực thi bộ xác thực với một địa chỉ người bỏ phiếu cụ thể và mục đích tập lệnh Plutus mới cho các tập lệnh). Có thể bỏ phiếu nhiều lần cho mỗi hành động quản trị bởi một chứng chỉ duy nhất.

Các phiếu bầu được nộp đúng cách sẽ ghi đè lên bất kỳ phiếu bầu cũ nào cho cùng một chứng chỉ và vai trò. Điều đó có nghĩa là người bỏ phiếu có thể thay đổi quan điểm của họ về bất kỳ hành động nào nếu họ chọn. Ngay khi một hành động quản trị được phê chuẩn, quá trình bỏ phiếu kết thúc và các giao dịch chứa thêm phiếu bầu là không hợp lệ.

Trạng thái quản trị

Khi một hành động quản trị được nộp thành công lên chuỗi, tiến trình của nó sẽ được theo dõi bởi trạng thái sổ cái. Cụ thể, những thông tin sau sẽ được theo dõi:

- ID của hành động quản trị
- Epoch mà hành động hết hạn
- Số tiền đặt cọc
- Địa chỉ nhận thưởng sẽ nhận được tiền đặt cọc khi nó được trả lại
- Tổng số phiếu 'Thuận'/'Chống'/'Trắng' của Ủy ban Hiến pháp cho hành động này

- Tổng số phiếu 'Thuận'/'Chống'/'Trắng' của DRep cho hành động này
- Tổng số phiếu 'Thuận'/'Chống'/'Trắng' của SPO cho hành động này

Thay đổi ảnh chụp cổ phần

Vì ảnh chụp cổ phần thay đổi tại mỗi ranh giới epoch, nên phải tính toán lại tổng số khi kiểm tra phê chuẩn mỗi hành động quản trị chưa được phê chuẩn. Điều này có nghĩa là một hành động có thể được thực thi ngay cả khi phiếu bầu của DRep hoặc SPO không thay đổi (vì sự ủy quyền phiếu bầu có thể đã thay đổi).

Định nghĩa liên quan đến cổ phần bỏ phiếu

Chúng tôi định nghĩa một số thuật ngữ mới liên quan đến cổ phần bỏ phiếu:

- Lovelace chứa trong đầu ra giao dịch được coi là *hoạt động để bỏ phiếu* (tức là nó tạo thành "cổ phần bỏ phiếu hoạt động"):
 - Nó chứa một chứng chỉ cổ phần đã đăng ký.
 - Chứng chỉ cổ phần đã đăng ký đã ủy quyền quyền bỏ phiếu của mình cho một DRep.
- Liên quan đến một tỷ lệ phần trăm P nào đó, ngưỡng phiếu bầu của DRep (SPO) đã được đáp ứng nếu tổng cổ phần tương đối đã được ủy quyền cho các DRep (SPO) bỏ phiếu 'Thuận' cho một hành động quản trị ít nhất là P .

Lý do

- Vai trò của Ủy ban Hiến pháp
- Có chủ ý bỏ qua xác minh danh tính
- Giảm quyền lực của các thực thể có lượng ADA lớn
- Dựa trên phân phối cổ phần của Pool ủy thác
- Tách biệt việc khởi tạo hard fork khỏi các thay đổi tham số giao thức tiêu chuẩn
- Mục đích của DRep
- Bảng yêu cầu phê chuẩn
- Đề xuất bất tín nhiệm
- Cập nhật ủy ban/ngưỡng (tình trạng bất tín nhiệm)
- Sự linh hoạt của hành động quản trị thông tin
- Khởi tạo hard fork
- Cấu trúc siêu dữ liệu mới
- Kiểm soát số lượng hành động quản trị đang hoạt động
- Không có AVST

Vai trò của Ủy ban Hiến pháp

Thoạt nhìn, Ủy ban Hiến pháp có vẻ là một ủy ban đặc biệt được trao quyền bổ sung đối với DRep. Tuy nhiên, vì DRep có thể thay thế Ủy ban Hiến pháp bất cứ lúc nào và phiếu bầu của DRep cũng được yêu cầu để phê chuẩn mọi hành động quản trị, nên Ủy ban Hiến pháp không có nhiều quyền hơn (và thực tế có thể ít hơn) so với DRep. Với điều này, ủy ban

đóng vai trò gì và tại sao nó không thừa? Câu trả lời là ủy ban giải quyết vấn đề khởi động của khuôn khổ quản trị mới. Thật vậy, ngay khi chúng ta kích hoạt và cho phép khuôn khổ này trở nên hoạt động trên chuỗi, thì nếu không có Ủy ban Hiến pháp, sẽ nhanh chóng cần có đủ DRep để hệ thống không chỉ dựa vào phiếu bầu của SPO. Chúng tôi chưa thể dự đoán cộng đồng sẽ tích cực đăng ký làm DRep như thế nào, cũng như các chủ sở hữu ADA khác sẽ phản ứng như thế nào đối với việc ủy quyền phiếu bầu.

Do đó, Ủy ban Hiến pháp đi vào hoạt động để đảm bảo hệ thống có thể chuyển đổi từ trạng thái hiện tại sang quản trị phi tập trung đầy đủ trong thời gian tới. Hơn nữa, về lâu dài, ủy ban có thể đóng vai trò cố vấn và tư vấn trong các quyết định quản trị bằng cách là một nhóm đại diện được bầu chọn và được chú ý đến phán quyết và hướng dẫn của họ trong các quyết định quản trị. Trên hết, ủy ban được yêu cầu luôn tuân thủ Hiến pháp và phê chuẩn các đề xuất theo các điều khoản của Hiến pháp.

Có chủ ý bỏ qua xác minh danh tính

Lưu ý rằng CIP này không đề cập đến bất kỳ loại xác thực hoặc xác minh danh tính nào cho các thành viên của Ủy ban Hiến pháp hoặc DRep. Điều này là cố ý. Chúng tôi hy vọng rằng cộng đồng sẽ cân nhắc mạnh mẽ chỉ bỏ phiếu và ủy quyền cho những DRep cung cấp một cái gì đó giống như DID để xác định danh tính của họ. Tuy nhiên, việc thực thi xác minh danh tính là rất khó khăn nếu không có một oracle tập trung nào đó, điều mà chúng tôi cho là một bước đi sai hướng.

Giảm quyền lực của các thực thể có lượng ADA lớn

Các cơ chế khác nhau, chẳng hạn như bỏ phiếu bậc hai, đã được đề xuất để bảo vệ chống lại các thực thể có nhiều ảnh hưởng. Tuy nhiên, trong một hệ thống dựa trên "1 Lovelace, 1 phiếu", việc chia cổ phần thành các số lượng nhỏ và hoàn tác sự bảo vệ là vô cùng dễ dàng. Nếu không có hệ thống xác minh danh tính trên chuỗi, chúng tôi không thể áp dụng bất kỳ biện pháp nào như vậy.

Dựa trên phân phối cổ phần của pool uỷ thác

Giao thức Cardano dựa trên cơ chế đồng thuận Proof-of-Stake, vì vậy việc sử dụng phương pháp quản trị dựa trên cổ phần là hợp lý. Tuy nhiên, có nhiều cách có thể được sử dụng để xác định cách ghi lại phân phối cổ phần giữa các thành viên tham gia. Như một lời nhắc nhở, các địa chỉ mạng hiện có thể chứa hai bộ thông tin xác thực: một để xác định ai có thể mở khóa tiền tại một địa chỉ (còn được gọi là thông tin xác thực thanh toán) và một có thể được ủy quyền cho một pool uỷ thác (còn được gọi là thông tin xác thực ủy quyền).

Thay vì định nghĩa một bộ thông tin xác thực thứ ba, chúng tôi đề xuất tái sử dụng các thông tin xác thực ủy quyền hiện có, sử dụng một chứng chỉ trên chuỗi mới để xác định phân phối cổ phần quản trị. Điều này ngụ ý rằng tập hợp các DRep có thể (và có khả năng sẽ) khác với tập hợp các SPO, tạo ra sự cân bằng. Mặt khác, điều đó có nghĩa là phân phối cổ phần quản trị chịu ảnh hưởng từ cùng những thiếu sót như đối với sản xuất khối: ví dụ, các nhà cung cấp phần mềm ví phải hỗ trợ các sơ đồ ủy quyền nhiều và phải tạo điều kiện cho việc

phân chia cổ phần thành các tài khoản phụ nếu một chủ sở hữu ADA muốn ủy quyền cho nhiều DRep, hoặc một chủ sở hữu ADA phải tự tay chia cổ phần của mình nếu ví của họ không hỗ trợ điều này.

Tuy nhiên, lựa chọn này cũng hạn chế nỗ lực triển khai trong tương lai cho các nhà cung cấp ví và giảm thiểu nỗ lực cần thiết cho người dùng cuối tham gia giao thức quản trị. Điều sau là một mối quan tâm đủ lớn để biện minh cho quyết định. Bằng cách dựa trên cấu trúc hiện có, hệ thống vẫn quen thuộc với người dùng và tương đối dễ thiết lập. Điều này tối đa hóa cả cơ hội thành công và tỷ lệ tham gia vào khuôn khổ quản trị.

Tách biệt việc khởi tạo hard fork khỏi các thay đổi tham số giao thức tiêu chuẩn

Trái ngược với các cập nhật tham số giao thức khác, các hard fork (hoặc chính xác hơn là thay đổi số phiên bản chính của giao thức) yêu cầu nhiều sự chú ý hơn. Thật vậy, trong khi các thay đổi tham số giao thức khác có thể được thực hiện mà không cần thay đổi phần mềm đáng kể, thì một hard fork giả định rằng phần lớn mạng lưới đã được nâng cấp nốt mạng Cardano để hỗ trợ tập hợp các tính năng mới được giới thiệu bởi bản nâng cấp. Điều này có nghĩa là thời gian của sự kiện hard fork phải được thông báo trước cho tất cả người dùng Cardano và yêu cầu sự phối hợp giữa các nhà vận hành Pool ủy thác, nhà cung cấp ví, nhà phát triển DApp và nhóm phát hành nốt mạng.

Do đó, đề xuất này, không giống như cơ chế ở kỷ Shelley, thúc đẩy việc khởi tạo hard fork như một hành động quản trị độc lập, khác biệt với các cập nhật tham số giao thức.

Mục đích của DReps

Không có gì trong đề xuất cải tiến này giới hạn các SPO trở thành DReps. Vậy tại sao chúng ta cần DReps? Câu trả lời là các SPO được chọn hoàn toàn để sản xuất khối, và không phải tất cả các SPO đều muốn trở thành DReps. Cử tri có thể chọn ủy quyền phiếu bầu của mình cho DReps mà không cần phải xem xét liệu họ có phải là nhà sản xuất khối tốt hay không, và các SPO có thể chọn đại diện cho các chủ sở hữu ADA hoặc không.

Bảng yêu cầu phê duyệt

Các yêu cầu trong bảng yêu cầu phê duyệt được giải thích ở đây. Hầu hết các hành động quản trị đều có cùng loại yêu cầu: Ủy ban Hiến pháp và các DReps phải đạt đủ số phiếu 'Thuận'. Điều này bao gồm các hành động sau:

- Cập nhật ủy ban/ngưỡng (trạng thái bình thường)
- Hiến pháp mới
- Thay đổi tham số giao thức
- Rút tiền từ quỹ
- Đề xuất bất tín nhiệm

Một đề xuất bất tín nhiệm thể hiện sự thiếu tin tưởng của cộng đồng Cardano đối với Ủy ban Hiến pháp hiện tại, do đó Ủy ban Hiến pháp không nên tham gia vào loại hành động quản trị này. Trong tình huống này, SPOs và DReps sẽ đại diện cho ý chí của cộng đồng.

Cập nhật ủy ban/ngưỡng (trạng thái bất tín nhiệm)

Tương tự như đề xuất Bất tín nhiệm, việc bầu ra Ủy ban Hiến pháp phụ thuộc vào cả SPOs và DReps để đại diện cho ý chí của cộng đồng.

Tính linh hoạt của hành động quản trị Thông tin

Mặc dù không ràng buộc trên chuỗi, hành động quản trị Thông tin có thể hữu ích trong một số tình huống. Điều này bao gồm:

- Phê duyệt một CIP
- Quyết định về tệp khởi tạo (Genesis) cho một kỷ nguyên sổ cái mới
- Ghi lại phản hồi ban đầu cho các hành động quản trị tương lai

Khởi tạo Hard-Fork

Bất kể cơ chế quản trị nào, sự tham gia của SPO là cần thiết cho bất kỳ hard fork nào vì họ phải nâng cấp phần mềm node của mình. Vì lý do này, chúng tôi làm cho sự hợp tác của họ trở nên rõ ràng trong hành động quản trị khởi tạo hard fork bằng cách luôn yêu cầu phiếu bầu của họ. Ủy ban Hiến pháp cũng bỏ phiếu, thể hiện tính hợp hiến của một hard fork. Các DReps cũng bỏ phiếu, để đại diện cho ý chí của mọi cổ đông.

Cấu trúc siêu dữ liệu mới

Các hành động quản trị, các phiếu bầu và chứng nhận, và Hiến pháp sử dụng các trường siêu dữ liệu mới, dưới dạng URL và mã băm đảm bảo tính toàn vẹn (tương tự cấu trúc siêu dữ liệu cho việc đăng ký pool uỷ thác). Siêu dữ liệu được sử dụng để cung cấp ngữ cảnh. Các hành động quản trị cần giải thích lý do tại sao hành động đó là cần thiết, những chuyên gia nào đã được tham vấn, v.v. Vì kích thước giao dịch không nên giới hạn dữ liệu giải thích này, chúng tôi sử dụng URL thay thế.

Điều này, tuy nhiên, cũng giới thiệu các vấn đề mới. Nếu một URL không hoạt động, điều gì sẽ xảy ra với việc bỏ phiếu cho hành động đó? Chúng ta có nên mong đợi mọi người bỏ phiếu 'Chống'? Đây có phải là một điểm yếu trong hệ thống quản trị không? Trong trường hợp này, hình ảnh trước của mã băm có thể được truyền đạt theo các cách khác nhau, nhưng chúng ta nên chuẩn bị cho tình huống này. Liệu có nên có một bản tóm tắt về sự giải thích ở trên chuỗi không?

Thay thế: Sử dụng siêu dữ liệu giao dịch

Thay vì sử dụng các trường chuyên biệt trong định dạng giao dịch, chúng ta có thể sử dụng trường siêu dữ liệu giao dịch hiện có.

Siêu dữ liệu liên quan đến quản trị có thể được xác định rõ ràng bằng cách đăng ký một nhãn siêu dữ liệu CIP-10. Trong đó, cấu trúc của siêu dữ liệu có thể được xác định bởi CIP

này (định dạng chính xác sẽ được xác định sau), sử dụng một chỉ số để ánh xạ ID hành động bỏ phiếu hoặc hành động quản trị đến URL và hàm băm siêu dữ liệu tương ứng.

Điều này tránh việc phải thêm các trường bổ sung vào thân giao dịch, với rủi ro là sẽ làm cho việc gửi bỏ qua trở nên dễ dàng hơn. Tuy nhiên, vì siêu dữ liệu yêu cầu có thể dễ trống (hoặc có thể trở đến một URL không hoạt động), nên việc gửi không cung cấp siêu dữ liệu đã dễ dàng, và do đó không rõ liệu điều này có làm cho tình huống tồi tệ hơn hay không.

Lưu ý rằng siêu dữ liệu giao dịch không bao giờ được lưu trữ trong trạng thái sổ cái, vì vậy việc kết hợp siêu dữ liệu với các hành động và phiếu bầu trong tùy chọn thay thế này sẽ phụ thuộc vào các máy khách, và sẽ không có sẵn dưới dạng truy vấn trạng thái sổ cái.

Kiểm soát số lượng hành động quản trị đang hoạt động

Vì các hành động quản trị có sẵn cho bất kỳ ai để nộp, chúng ta cần một cơ chế nào đó để ngăn những cá nhân chịu trách nhiệm bỏ phiếu bị choáng ngợp bởi một loạt các đề xuất. Một khoản tiền đặt cọc lớn là một cơ chế như vậy, nhưng điều này có thể trở thành rào cản đối với một số người khi nộp một hành động. Tuy nhiên, huy động nguồn lực từ cộng đồng với một tập lệnh Plutus luôn là một lựa chọn để thu thập khoản tiền đặt cọc.

Mặt khác, chúng ta có thể chấp nhận khả năng có nhiều hành động đang hoạt động tại bất kỳ thời điểm nào và thay vào đó dựa vào xã hội hóa ngoài chuỗi để hướng sự chú ý của cử tri đến những hành động xứng đáng. Trong kịch bản này, Ủy ban Hiến pháp có thể chọn chỉ xem xét các đề xuất đã thu hút đủ số phiếu từ DReps.

Không có AVST

Một bản dự thảo trước đây của CIP này bao gồm khái niệm về AVST, tức là "ngưỡng cổ phần bỏ phiếu hoạt động". Mục đích của AVST là đảm bảo tính hợp pháp của mỗi phiếu bầu, loại bỏ khả năng mà chẳng hạn như 9 trong số 10 Lovelace có thể quyết định số phận của hàng triệu thực thể trên Cardano. Thực sự có hai mối quan tâm ở đây mà đáng được tách biệt:

Mối quan tâm đầu tiên là vấn đề khởi động hệ thống, tức là đạt được thời điểm ban đầu khi đủ số cổ phần được đăng ký để bỏ phiếu. Mối quan tâm thứ hai là hệ thống có thể mất đi sự tham gia theo thời gian. Một vấn đề với AVST là nó tạo động lực cho các SPO mong muốn một đăng ký bỏ phiếu thấp (vì khi đó phiếu bầu của họ sẽ có trọng lượng hơn). Đây hoàn toàn không phải là một sự chỉ trích đối với các SPO hiện tại, mà là một vấn đề với các động lực xấu.

Do đó, chúng tôi đã chọn giải quyết hai mối quan tâm này theo cách khác nhau. Chúng tôi giải quyết vấn đề khởi động như đã mô tả trong phần về khởi động. Chúng tôi giải quyết vấn đề tham gia lâu dài bằng cách không cho phép rút phần thưởng (sau giai đoạn khởi động) trừ khi cổ phần được ủy quyền cho một DRep (bao gồm hai trường hợp đặc biệt, cụ thể là **'Abstain'** - Không tham gia, và **'No Confident'** - Bất tín nhiệm).

Thay đổi sau hội thảo Longmont (Tháng 3 năm 2023)

- Cảm ơn những người tham dự hội thảo.
- Đã thêm nhiệm kỳ của Ủy ban Hiến pháp.
- Hai tùy chọn bỏ phiếu "đã được xác định trước" mới: không tham gia và bất tín nhiệm.
- Hành động quản trị "Thông tin" mới.
- Sử dụng phân phối cổ phần DRep mới nhất để phê chuẩn. Điều này có nghĩa là nếu DRep của bạn bỏ phiếu không như ý muốn, bạn có thể ngay lập tức trở thành DRep và bỏ phiếu theo ý muốn của mình.
- Khóa một số ADA từ kho bạc hiện tại cho các khuyến khích DRep tiềm năng trong tương lai.
- Loại bỏ các hành động kho bạc theo tầng để thay thế bằng một cái gì đó thích ứng (do đó ngưỡng "có" sẽ phụ thuộc vào: bao nhiêu ada, cổ phần bỏ phiếu đã đăng ký cao như thế nào và có thể là bao nhiêu ada được phát hành mỗi epoch)
- Chia các cập nhật tham số giao thức thành bốn nhóm: mạng, kinh tế, kỹ thuật và chính phủ.
- Hầu hết các hành động quản trị có thể được thực thi (sau khi phê chuẩn) ngay lập tức. Tất cả trừ: tham số giao thức và hard fork.
- Loại bỏ giới hạn "một hành động cho mỗi loại mỗi epoch" để thay thế bằng việc theo dõi ID hành động cuối cùng của mỗi loại và bao gồm điều này trong hành động.
- Không có AVST.
- Giai đoạn khởi động: Cho đến khi X% ADA được đăng ký để bỏ phiếu hoặc Y epoch đã trôi qua, chỉ có thể thay đổi tham số và hard fork xảy ra. Thay đổi PP chỉ cần ngưỡng CC, HF cần CC và SPO. Sau giai đoạn khởi động, chúng tôi đưa ra khuyến khích để giữ DRep thấp, nhưng cơ chế này tự động nói lỏng.
- Mục đích kích bản Plutus mới cho DRep.
- Nhiều lần rút kho bạc trong một epoch.
- Một phần về vấn đề đệ quy "làm thế nào để chúng ta phê chuẩn CIP này".
- Thay đổi giao thức truy vấn trạng thái cục bộ.
- Ý tưởng mới, nếu có thời gian: Cân nhắc phiếu bầu cổ phần SPO bằng cách nào đó.
- DRep có thể chỉ định DRep khác nhận được người ủy quyền của họ trong trường hợp họ mất nhiệm.
- Giảm tiền đặt cọc hành động chính phủ nếu một thành viên của CC ký vào nó (có nghĩa là nó đã trải qua một số quy trình).
- Bao gồm băm của cấu hình genesis (tương lai) trong đề xuất HF.

Thay đổi sau hội thảo Edinburgh (Tháng 7 năm 2023)

- Thêm Tập lệnh Rào chắn, có thể kiểm soát những gì được phép rút kho bạc và thay đổi tham số giao thức.
- Loại bỏ việc bỏ các hành động quản trị. Ảnh hưởng duy nhất của điều này là trong trường hợp một hành động bất tín nhiệm được thông qua, các hành động vẫn tồn tại. Tuy nhiên, chỉ có các đề xuất ủy ban mới được thiết kế để xây dựng trên cơ sở hành động bất tín nhiệm đó mới có thể được thực thi. Nếu một ủy ban mới được bầu khi một số hành động đó chưa hết hạn, các hành động đó có thể được phê chuẩn nhưng ủy ban mới phải phê duyệt chúng.
- Tất cả các hành động quản trị được thực thi một epoch sau khi được phê chuẩn.
- Di chuyển các hạn chế sau khởi động vào 'Ý tưởng khác'.
- Thêm một phần về các số tiền đặt cọc khác nhau vào 'Ý tưởng khác'.

- Thêm một phần cho một AVS tối thiểu vào 'Ý tưởng khác'.
- Đổi tên một số tham số giao thức.
- Đổi tên TALLY thành GOV.
- Biến Hiến pháp thành một neo.
- Làm lại các neo nào là bắt buộc và cái nào là tùy chọn.
- Sửa chữa các mâu thuẫn và phần thừa từ các phiên bản cũ.

Thay đổi liên quan đến bảo mật và các sửa lỗi khác (Tháng 1 năm 2024)

- Bảo vệ các thay đổi liên quan đến bảo mật đằng sau phiếu bầu của SPO.
- Hệ thống không chuyển sang trạng thái Bất tín nhiệm với số lượng thành viên CC hoạt động không đủ, CC chỉ không thể hành động.
- Làm rõ rằng các thành viên CC có thể sử dụng bất kỳ loại thông tin xác thực nào.

Tháng 5 năm 2024

- Cập nhật phần về giai đoạn khởi động.
- Đề cập đến tham số Q_5 bị thiếu.
- Các sửa chữa/thay đổi nhất quán nhỏ khác.

Lộ Trình Kích Hoạt

Tiêu chí chấp nhận

Một kỷ nguyên số cái mới được kích hoạt trên mạng chính Cardano, triển khai các thông số kỹ thuật trên.

Kế hoạch triển khai

Các tính năng trong CIP này yêu cầu một đợt hard fork.

Tài liệu này mô tả một sự thay đổi lớn đối với hệ thống quản trị của Cardano. Chúng tôi đề xuất thực hiện các thay đổi thông qua hai đợt hard fork: đợt đầu tiên bao gồm tất cả các tính năng mới nhưng một số sẽ bị vô hiệu hóa trong giai đoạn khởi động, và đợt thứ hai sẽ kích hoạt tất cả các tính năng.

Trong các phần tiếp theo, chúng tôi cung cấp thêm chi tiết về các mục công việc triển khai đã được xác định. Ngoài ra, phần cuối cùng sẽ đưa ra một số câu hỏi mở cần được hoàn thiện. Chúng tôi hy vọng những câu hỏi này có thể được giải quyết thông qua các workshop và thảo luận cộng đồng.

Phê duyệt đề xuất này

Phê duyệt đề xuất này là một vấn đề vòng lặp: chúng ta cần một khung quản trị nào đó để đồng ý về việc khung quản trị cuối cùng sẽ như thế nào. Như đã nhiều lần nêu ra, CIP không có tính quyền lực, cũng không phải là cơ chế quản trị. Thay vào đó, chúng mô tả các giải pháp kỹ thuật đã được cộng đồng chuyên gia đánh giá là hợp lý từ góc độ kỹ thuật.

CIP-1694 có thể đi xa hơn so với phạm vi thông thường của quy trình CIP và có mong muốn mạnh mẽ để phê duyệt CIP này thông qua một quy trình nào đó. Tuy nhiên, quy trình đó vẫn chưa được xác định và vẫn còn là một câu hỏi mở. Quy trình phê duyệt cuối cùng có khả năng sẽ là sự pha trộn của nhiều ý tưởng khác nhau, chẳng hạn như:

- Thu thập ý kiến từ các workshop cộng đồng, tương tự như workshop Colorado tháng 2-3 năm 2023.
- Thực hiện các hành động bỏ phiếu trên một testnet công cộng, với sự tham gia đủ.
- Thăm dò các SPO đã thành lập.
- Sử dụng Project Catalyst để thu thập ý kiến từ cộng đồng bỏ phiếu hiện có (mặc dù nhỏ về cổ phần hoạt động).

Thay đổi trong cấu trúc giao dịch

Các yếu tố mới sẽ được thêm vào cấu trúc giao dịch, và các khả năng cập nhật và MIR hiện có sẽ bị loại bỏ. Cụ thể:

- Các hành động quản trị và phiếu bầu sẽ bao gồm hai trường mới trong cấu trúc giao dịch.
- Ba loại chứng nhận mới sẽ được thêm vào ngoài các loại hiện có:
 - Đăng ký DRep
 - Hủy đăng ký DRep
 - Ủy quyền phiếu bầu
- Tương tự, các chứng nhận MIR và khởi tạo sẽ bị loại bỏ.
- Một mục đích bỏ phiếu mới sẽ được thêm vào các ngữ cảnh kịch bản Plutus. Điều này sẽ cung cấp, đặc biệt, phiếu bầu cho các kịch bản trên chuỗi.

Cảnh báo

Như thường lệ, chúng tôi sẽ cung cấp đặc tả CDDL cho mỗi thay đổi này.

Thay đổi các quy tắc sổ cái hiện có

- Quy tắc chuyển tiếp PPUP sẽ được viết lại và chuyển từ quy tắc UTxO sang quy tắc LEDGER như một quy tắc GOV mới.
 - Nó sẽ xử lý và ghi lại các hành động quản trị và phiếu bầu.
- Quy tắc chuyển tiếp NEWEPOCH sẽ được sửa đổi.
 - Quy tắc phụ MIR sẽ bị loại bỏ.
 - Một quy tắc RATIFY mới sẽ được giới thiệu để chuẩn bị các hành động quản trị cho việc thực hiện.
 - Nó sẽ phê chuẩn các hành động quản trị và chuẩn bị chúng để thực hiện trong kỷ nguyên hiện tại hoặc tiếp theo, nếu cần.
- Một quy tắc ENACTMENT mới sẽ được gọi ngay sau quy tắc EPOCH. Quy tắc này sẽ thực hiện các hành động quản trị đã được phê chuẩn trước đó.
 - Quy tắc EPOCH sẽ không còn gọi quy tắc phụ NEWPP hoặc tính toán liệu ngưỡng đủ điều kiện có được đáp ứng trên trạng thái PPUP hay không.

Thay đổi giao thức truy vấn trạng thái cục bộ

Khối lượng công việc quản trị trên chuỗi là lớn, nhưng khối lượng công việc ngoài chuỗi cho các công cụ và ứng dụng sẽ còn lớn hơn. Để xây dựng một hệ sinh thái quản trị hiệu quả, sổ cái sẽ phải cung cấp giao diện cho các yếu tố quản trị khác nhau.

Trong khi các phiếu bầu và đăng ký (hủy đăng ký) DRep hiển thị trực tiếp trong các khối và do đó sẽ có thể truy cập qua các giao thức đồng bộ chuỗi cục bộ hiện có; chúng tôi sẽ cần nâng cấp giao thức truy vấn trạng thái cục bộ để cung cấp thêm thông tin chi tiết về các

thông tin khó suy ra từ các khối (tức là những thông tin yêu cầu duy trì trạng thái sổ cái). Các truy vấn trạng thái mới nên bao gồm (ít nhất là):

- Các hành động quản trị hiện đang chuẩn bị cho việc thực hiện
- Các hành động quản trị đang trong quá trình phê chuẩn, với tổng số và tỷ lệ phần trăm của cổ phần 'có', cổ phần 'không' và cổ phần 'bỏ phiếu trắng'
- Ủy ban Hiến pháp hiện tại, và hàm băm bản tóm tắt hiến pháp

Giai đoạn Khởi động

Chúng tôi sẽ cần cẩn thận trong cách khởi động chính phủ non trẻ này. Tất cả các bên liên quan sẽ cần đủ thời gian để tự đăng ký và làm quen với quy trình.

Các điều khoản đặc biệt sẽ được áp dụng trong giai đoạn khởi động ban đầu. Thứ nhất, trong giai đoạn khởi động, phiếu bầu từ Ủy ban Hiến pháp là đủ để thay đổi các tham số giao thức. Thứ hai, trong giai đoạn khởi động, phiếu bầu từ Ủy ban Hiến pháp cùng với phiếu bầu SPO đủ điều kiện là đủ để khởi tạo một đợt hard fork. Thứ ba, các hành động thông tin sẽ có sẵn. Không có hành động nào khác ngoài những hành động được đề cập trong đoạn này có thể thực hiện trong giai đoạn khởi động.

Giai đoạn khởi động kết thúc khi Ủy ban Hiến pháp và các SPO phê chuẩn một đợt hard fork tiếp theo, kích hoạt các hành động quản trị còn lại và sự tham gia của DRep. Điều này có thể sẽ xảy ra sau đợt hard fork Chang một số tháng. Mặc dù tất cả các tính năng sẽ khả dụng về mặt kỹ thuật tại thời điểm này, các yêu cầu bổ sung để sử dụng mỗi tính năng có thể được chỉ định trong hiến pháp.

Hơn nữa, sẽ có một Ủy ban Hiến pháp tạm thời với nhiệm kỳ được xác định, cũng được chỉ định trong tệp cấu hình kỷ nguyên sổ cái tiếp theo. Lịch xoay vòng của ủy ban đầu tiên không tạm thời có thể được bao gồm trong chính hiến pháp. Tuy nhiên, lưu ý rằng vì Ủy ban Hiến pháp không bao giờ bỏ phiếu cho các ủy ban mới, nên thực tế họ không thể thực thi việc xoay vòng.

Các ý tưởng khác / Câu hỏi mở

Bỏ phiếu SPO theo trọng số cam kết

Phiếu bầu của SPO có thể được trọng số thêm bởi cam kết của mỗi SPO. Điều này sẽ cung cấp một cơ chế để cho phép những người có cổ phần thực sự trong trò chơi có phiếu bầu mạnh hơn. Trọng số nên được lựa chọn cẩn thận.

Tự động tái đối với DRep

Một DRep có thể tùy chọn liệt kê một thông tin xác thực DRep khác trong chứng chỉ đăng ký của họ. Khi mãn nhiệm, tất cả các ủy quyền của DRep sẽ tự động được chuyển đến thông tin xác thực DRep được chỉ định. Nếu DRep đó đã mãn nhiệm, việc ủy quyền sẽ được chuyển đến tùy chọn bỏ phiếu 'Abstain'.

Không đăng ký DRep

Vì đăng ký DRep không thực hiện bất kỳ chức năng cần thiết nào, nên các chứng chỉ để (hủy) đăng ký DRep có thể bị xóa bỏ. Điều này làm cho nền dân chủ trở nên linh hoạt hơn vì nó loại bỏ một số quan liêu và cũng loại bỏ nhu cầu về tiền đặt cọc DRep, với chi phí di chuyển mỏ neo là một phần của chứng chỉ đăng ký DRep vào siêu dữ liệu giao dịch.

Giảm tiền đặt cọc cho một số hành động quản trị

Tiền đặt cọc được gắn với các hành động quản trị nhằm ngăn chặn một loạt các hành động quản trị không nghiêm túc, mỗi hành động đều yêu cầu thời gian và sự chú ý của cộng đồng Cardano. Chúng tôi có thể giảm tiền đặt cọc này cho các đề xuất trải qua một số quy trình ngoài chuỗi được thống nhất. Điều này sẽ được đánh dấu trên chuỗi bằng sự chứng thực của ít nhất một thành viên Ủy ban Hiến pháp. Nhược điểm của ý tưởng này là nó mang lại nhiều quyền lực hơn cho Ủy ban Hiến pháp.

Số tiền đặt cọc khác nhau cho các hành động quản trị khác nhau

Nhiều hội thảo cho CIP này đã đề xuất giới thiệu một số tiền đặt cọc khác nhau cho từng loại hành động quản trị. Người ta không rõ liệu đa số có ủng hộ ý tưởng này hay không, nhưng điều này có thể được xem xét nếu rõ ràng là cần thiết.

Cổ phần bỏ phiếu hoạt động tối thiểu

Là một đảm bảo bổ sung để đảm bảo các hành động quản trị không thể được đề xuất ngay trước một hard fork, được bỏ phiếu bởi một DRep với một lượng cổ phần lớn và được thực thi ngay lập tức, có thể có một yêu cầu bổ sung là một số lượng cổ phần tuyệt đối cố định cần phải bỏ phiếu 'Có' cho hành động để được thực thi. Điều này dường như không cần thiết trong thiết kế hiện tại, vì cổ phần của tất cả DRep đã đăng ký hoạt động như một phiếu bầu 'Không' cho đến khi họ thực sự bỏ phiếu. Điều này có nghĩa là để kích bản này xảy ra, kẻ tấn công độc hại cần phải ít nhất kiểm soát phần cổ phần DRep tương ứng với ngưỡng liên quan, tại thời điểm đó điều này cũng có thể được coi là một hành động hợp pháp.

Bao gồm mã băm của cấu hình genesis (tương lai) trong đề xuất hard fork

Một số hard fork yêu cầu cấu hình genesis mới. Điều này đã xảy ra đối với các hard fork Shelley và Alonzo (nhưng không phải Allegra, Mary, Vasil hay Valentine), có thể xảy ra trong tương lai. Tại thời điểm này, đề xuất này không nói gì về cấu hình genesis như vậy: nó được giả định ngầm định là một thỏa thuận ngoài chuỗi. Tuy nhiên, chúng tôi có thể thực thi rằng (mã băm của) một cấu hình genesis cụ thể cũng được chụp lại trong một hành động quản trị hard fork.

Ngưỡng thích ứng

Như đã thảo luận ở trên, có thể hợp lý khi một số hoặc tất cả các ngưỡng được điều chỉnh theo Lovelace đang hoạt động được đăng ký để bỏ phiếu, để hệ thống cung cấp tính hợp pháp lớn hơn khi chỉ có mức độ cổ phần bỏ phiếu hoạt động thấp. Cơ chế khởi động được đề xuất ở trên có thể bao gồm điều này, tuy nhiên, bằng cách đảm bảo rằng hệ thống quản trị chỉ được kích hoạt khi một mức cổ phần tối thiểu đã được ủy quyền cho DRep.

Đổi tên DRep / trạng thái Bất tín nhiệm?

Người ta đã nói nhiều lần rằng "DRep" như được trình bày ở đây có thể bị nhầm lẫn với DRep của Project Catalyst. Tương tự, một số người đã bày tỏ sự nhầm lẫn giữa trạng thái Bất tín nhiệm, đề xuất Bất tín nhiệm và tùy chọn bỏ phiếu Bất tín nhiệm. Chúng tôi có thể tưởng tượng tìm ra các thuật ngữ tốt hơn cho những khái niệm này.

Hạn chế Rút tiền từ kho bạc

Không có gì ngăn cản việc lấy tiền ra khỏi kho bạc ngoài các phiếu bầu và ngưỡng bỏ phiếu được đề xuất. Vì kho bạc Cardano là một thành phần khá cơ bản của chính sách tiền tệ của nó, chúng ta có thể tưởng tượng việc thực thi (ở cấp độ giao thức) số tiền tối đa có thể được lấy ra khỏi kho bạc trong bất kỳ khoảng thời gian nào.

Biện pháp an toàn cuối cùng, sau khi khởi động

Nhiều người đã tuyên bố rằng họ tin rằng tỷ lệ bỏ phiếu thực tế sẽ không lớn đến mức gây áp lực lên thông lượng của hệ thống. Chúng tôi cũng tin rằng đây có thể là trường hợp, nhưng khi giai đoạn khởi động kết thúc, chúng tôi có thể đưa ra một biện pháp an toàn cuối cùng, tạm thời (điều này cũng sẽ cho phép chúng tôi biện đáp số tiền đặt cọc DRep thấp). Đối với các giá trị của X và Y vẫn cần được xác định, ngay sau khi giai đoạn khởi động kết thúc, khi chúng tôi tính toán phân phối cổ phần DRep cho ranh giới epoch tiếp theo, chúng tôi sẽ chỉ xem xét những DRep nằm trong X DRep hàng đầu được xếp hạng theo số lượng cổ phần, hoặc những DRep có ít nhất Y Lovelace. Mỗi epoch, giá trị của X sẽ tăng và giá trị của Y sẽ giảm, do đó cuối cùng X sẽ hiệu quả vô hạn và Y sẽ bằng không. Lưu ý rằng đây chỉ là một khuyến khích và không có gì thực sự ngăn cản bất kỳ DRep nào bỏ phiếu (mặc dù nó sẽ không được tính nếu không đáp ứng các yêu cầu). Nếu cộng đồng quyết định tại một số điểm rằng thực sự có vấn đề về tắc nghẽn, thì một hard fork có thể được ban hành để giới hạn số lượng DRep theo cách hạn chế hơn. Các số hợp lý cho giá trị ban đầu của X có thể là 5.000-10.000. Các số hợp lý cho giá trị ban đầu của Y có thể là tổng số Lovelace chia cho giá trị ban đầu của X. Cơ chế này nên được đặt để thư giãn với tốc độ mà hạn chế bị loại bỏ hoàn toàn sau khoảng thời gian sáu tháng đến một năm.

Lời cảm ơn

Bản thảo đầu tiên

- Hội thảo Longmont năm 2023 (28/02 → 01/03)
- Hội thảo Thành phố Mexico, Mexico năm 2023 (20/05)
- Hội thảo Buenos Aires, Argentina năm 2023 (20/05)
- Hội thảo Johannesburg, Nam Phi năm 2023 (25/05)
- Hội thảo Bogota, Colombia năm 2023 (27/05)
- Hội thảo Caracas, Venezuela năm 2023 (27/05)
- Hội thảo Manizales, Colombia năm 2023 (27/05)
- Hội thảo Addis Ababa, Ethiopia năm 2023 (27/05 & 28/5)
- Hội thảo Kyoto và Fukuoka, Nhật Bản năm 2023 (27/05 & 10/06)
- Hội thảo Monterey, California năm 2023 (28/05)

- Hội thảo Tlaxcala, Mexico năm 2023 (01/06)
- Hội thảo ảo LATAM năm 2023 (03/06)
- Hội thảo Worcester, Massachusetts năm 2023 (08/06)
- Hội thảo Chicago, Illinois năm 2023 (10/06)
- Hội thảo ảo năm 2023 (12/06)
- Hội thảo Toronto, Canada năm 2023 (15/06)
- Hội thảo Philadelphia, Pennsylvania năm 2023 (17/06)
- Hội thảo Santiago de Chile năm 2023 (17/06)
- Hội thảo ảo năm 2023 (17/06)
- Hội thảo Taipei, Đài Loan năm 2023 (18/06)
- Hội thảo Midgard Vikingcenter Horten, Na Uy năm 2023 (19/06)
- Hội thảo ảo năm 2023 (19/06)
- Hội thảo Thành phố New York, New York năm 2023 (20/06)
- Hội thảo La Cumbre, Argentina năm 2023 (23/06)
- Hội thảo Minneapolis, Minnesota năm 2023 (23/06)
- Hội thảo La Plata, Argentina năm 2023 (23/06)
- Hội thảo Puerto Madryn, Argentina năm 2023 (23/06)
- Hội thảo Accra, Ghana năm 2023 (24/06)
- Hội thảo ảo năm 2023 (24/06)
- Hội thảo Seoul, Hàn Quốc năm 2023 (24/06)
- Hội thảo Abu Dhabi, UAE năm 2023 (25/06)
- Hội thảo Williamsburg, New York năm 2023 (25/06)
- Hội thảo Lagos, Nigeria năm 2023 (28/06)
- Hội thảo Sao Paulo, Brazil năm 2023 (01/07)
- Hội thảo ảo Brazil năm 2023 (04/07)

Bản quyền

CIP này được cấp phép theo CC-BY-4.0

Chú thích

1. Một mô tả chính thức về các quy tắc hiện tại cho các hành động quản trị được đưa ra trong đặc tả sổ cái Shelley.
 - Đối với các thay đổi tham số giao thức (bao gồm cả hard fork), quy tắc chuyển tiếp PPUP (Hình 13) mô tả cách xử lý các cập nhật tham số giao thức và quy tắc chuyển tiếp NEWPP (Hình 43) mô tả cách thực hiện các thay đổi đối với tham số giao thức.
 - Đối với chuyển tiền, quy tắc chuyển tiếp DELEG (Hình 24) mô tả cách xử lý chứng chỉ MIR và quy tắc chuyển tiếp MIR (Hình 55) mô tả cách thực hiện các chuyển động kho bạc và dự trữ.

Lưu ý: Khả năng của quy tắc chuyển tiếp MIR đã được mở rộng trong đặc tả sổ cái Alonzo

2. Có nhiều định nghĩa khác nhau về thuật ngữ "hard fork" trong ngành công nghiệp blockchain. Hard fork thường đề cập đến các cập nhật không tương thích ngược của

một mạng lưới. Trong Cardano, chúng tôi chính thức hóa định nghĩa một cách chặt chẽ hơn bằng cách gọi bất kỳ nâng cấp nào dẫn đến việc xác thực nhiều khối hơn là một "hard fork" và buộc các nốt mạng phải tuân thủ phiên bản giao thức mới, hiệu quả là làm lỗi thời các nốt mạng không thể xử lý được nâng cấp.