ĐỀ XUẤT NGÂN QUỸ CHO ETHEREUM CLASSIC

BÁO CÁO NGHIÊN CỨU
Ngày 07 tháng 03 năm 2017

Nhóm Veritas
Dmytro Kaidalov, Lyudmila Kovalchuk,
Andrii Nastenko, Mariia Rodinko,
Oleksiy Shevtsov, Roman Oliynykov
IOHK.io

Tóm lược

Chúng tôi đề xuất Hệ thống Ngân quỹ Ethereum Classic (ECTS) với mục đích chính là thiết lập một cơ chế tài trợ phi tập trung để phát triển và duy trì nền tảng Ethereum Classic. Bất kỳ ai cũng có thể gửi một đề xuất dự án và các bên liên quan sẽ quyết định về sự cần thiết của nó thông qua một thủ tục bỏ phiếu minh bạch. Hệ thống hoàn toàn có thể xác minh được, không có ảnh hưởng đáng kể đến hiệu suất của ETC. Báo cáo cũng tính đến ECIP 1017 thay đổi chính sách tiền tệ và lịch trình phát thải của Ethereum Classic. Chúng tôi kỳ vọng rằng việc triển khai ECTS sẽ tăng tính ổn định và triển vọng của hệ thống, mang lại lợi ích bổ sung cho cả các bên liên quan và thợ đào từ một hệ thống ổn định hơn và dễ dự đoán hơn.

Nội dung

1. Giới thiệu

Hiện tượng Crypto nổi lên vào năm 2008 với Bitcoin [1]. Sau đó, hàng trăm loại Crypto khác nhau đã được phát minh và hiện tại vốn hóa thị trường của 10 loại Crypto phổ biến nhất đã vượt quá 17 tỷ đô la Mỹ [2]. Các tổ chức tài chính và chính phủ truyền thống thể hiện sự quan tâm đến việc áp dụng các công nghệ Blockchain do ngành này phát triển [3,4,5].

Sự vắng mặt của quyền kiểm soát tập trung đối với quy trình hoạt động là một tính năng chính được mong đợi từ các hệ thống Blockchain. Nó có thể được đảm bảo với sự phi tập trung và quản trị đa số trung thực. Khi không có cơ quan trung ương kiểm soát việc phát hành và giao dịch Crypto, nó được coi là một sự đảm bảo nghiêm túc cho sự ổn định hoạt động và thúc đẩy sự quan tâm của người dùng đối với Crypto.

Trong ngắn hạn, một hoạt động Crypto đòi hỏi phải có một phần lớn các Node trung thực phi tập trung hỗ trợ bảo trì sổ cái phân tán.

Ở góc độ trung và dài hạn, một yếu tố bổ sung là rất quan trọng. Bất kỳ loại Crypto nào cũng tồn tại như một hệ thống kỹ thuật phức tạp, đòi hỏi thiết kế và triển khai liên tục nhiều giao thức và thuật toán phức tạp, do đó, đòi hỏi mức ngân sách thích hợp. Thiếu kinh phí sẽ dẫn đến hoạt động Crypto bị đóng băng và thiếu quy trình giải quyết vấn đề. Việc tài trợ không thường xuyên với các khoản đóng góp tự nguyện được quản lý yếu kém có thể dẫn đến các lỗ hổng bảo mật và sự bất ổn của hệ thống sẽ ảnh hưởng đến tỷ giá hối đoái và dẫn đến việc tạm dừng đáng kể việc mở rộng thị trường của nó. Do đó, nguồn vốn ổn định cho việc hỗ trợ và phát triển hệ thống là chìa khóa cho triển vọng thị trường trung và dài hạn của Crypto.

Chúng ta có thể xem xét các lựa chọn khác nhau để cung cấp nguồn vốn cần thiết. Nó có thể là tiền huy động từ các quỹ mạo hiểm quan tâm đến tiềm năng của công nghệ Blockchain hoặc nó có thể là tiền quyên góp của cộng đồng được huy động thông qua quá trình huy động vốn cộng đồng. Cách tiếp cận thứ ba là tự cung cấp Crypto để đảm bảo tài trợ bền vững [6,7,8].

Báo cáo này giới thiệu một đề xuất cho Hệ thống Ngân quỹ ETC (ECTS) nhằm cung cấp một hệ thống tài trợ bền vững cho sự phát triển Crypto dưới sự kiểm soát của cộng đồng.

1.1. Mục tiêu và tính chất mong muốn của hệ thống ngân quỹ

Hệ thống ngân quỹ ETC là một quy trình được cộng đồng kiểm soát và phi tập trung để cấp vốn cho sự phát triển Ethereum Classic. Hệ thống ngân quỹ được trình bày không phải là một hệ thống quản trị toàn diện với hệ thống con áp dụng

Hardfork, nhưng nó chỉ là một công cụ để cấp vốn phát triển Crypto.
ECTS được thiết kế để có các đặc tính sau.

1. Được hỗ trợ và tăng cường sự ổn định cũng như triển vọng trong tương lai của nền tảng Ethereum Classic. Những thợ đào Crypto cũng như người dùng thông thường sẽ không có ảnh hưởng tiêu cực nhưng được hưởng lợi từ một hệ thống ổn định hơn và dễ dự đoán hơn.
2. Tính toán được chấp nhận và tải không gian Blockchain cho hệ thống, không có ảnh hưởng đến hiệu suất.
3. Khả năng cho bất kỳ ai gửi đề xuất tài trợ (với hệ thống được bảo vệ khỏi DoS) và lựa chọn những cái tốt nhất.
4. Các thành viên cộng đồng có động lực để lựa chọn các đề xuất tài trợ. Các cử tri quan tâm đến sự ổn định và phát triển hơn nữa của Crypto, vì vậy hãy tham gia vào quá trình này.
5. Một động lực kinh tế tức thì để trở thành cử tri và tham gia vào quá trình ra quyết định. ETCS nên hỗ trợ một nhóm cử tri tự cân bằng để đảm bảo mức độ tham gia tốt (nếu số lượng người tham gia giảm xuống thì phần thưởng cho mỗi người tham gia sẽ tăng lên, sẽ thu hút các thành viên mới).
6. Các quyết định được đưa ra là minh bạch và có thể truy xuất nguồn gốc. Mọi người truy cập vào ETC Blockchain đều có thể hoàn toàn và độc lập xác minh tính đúng đắn các hoạt động của ngân quỹ.
7. Thường xuyên ra quyết định cấp vốn với nhiều thời gian để phân tích và hạn chế thiệt hại nặng nề do các đề xuất không phù hợp.
8. Thủ tục bỏ phiếu nên giảm thiểu sự phức tạp của các chiến lược bỏ phiếu. Không có cử tri nào nên thắng hoặc thua cuộc bỏ phiếu sớm hơn những người khác.
9. Một thủ tục ủy quyền cho phép cử tri theo dõi những người tham gia đủ tiêu chuẩn đáng tin cậy để đưa ra các quyết định cần phân tích chuyên sâu về thời gian và kỹ năng.
10. Các thuộc tính bảo mật thích hợp để bảo vệ hệ thống khỏi những người tham gia độc hại. Một kẻ tấn công phải liên quan đến các nguồn lực đáng kể để thu được lợi nhuận tiềm năng nhỏ. Khả năng để những người trung thực can thiệp và ngăn chặn các cuộc tấn công tiếp theo.

Chúng tôi đã thiết kế các chức năng liên quan cho ECTS được đề xuất, việc phân tích chính thức là hoãn lại cho các giai đoạn nghiên cứu tiếp theo.

1.2. Tổng quan về đề xuất hệ thống ngân quỹ

Ở đây chúng tôi cung cấp một cái nhìn tổng quan về hệ thống ngân quỹ được đề xuất. Mô tả chi tiết được đưa ra trong các phần sau.

Đường ống tài trợ phát triển được thiết kế như là quá trình chuyển tiền vào các tài khoản được liên kết với các đề xuất được cộng đồng chấp thuận. Các đề xuất được tài trợ sẽ giải quyết các nhiệm vụ nâng cao và bảo trì Crypto.

Việc chuyển tiền sẽ được thực hiện trong một số Block không đổi được gọi là Epoch ngân quỹ với thời gian khoảng một tháng. Vào cuối mỗi Epoch, một Block thanh toán với các giao dịch Coinbase bổ sung cho ví đề xuất được phát hành.

Ngân sách tài trợ của Epoch sẽ có giới hạn trên không đổi. Nó có thể được trình bày như sau: mỗi Block được phát hành trong Epoch cung cấp số lượng tiền xác định trước (thu được trong chính sách tiền tệ) cho ngân quỹ. Các đề xuất dự án được tài trợ vào cuối Epoch lên đến 80% số tiền ngân quỹ này.

Bất kỳ ai cũng có thể gửi đề xuất trước khi bắt đầu Epoch khi đề xuất được tài trợ. Việc đệ trình đề xuất đốt 5 đồng Coin và được đưa vào Blockchain (do đó, danh sách các đề xuất sẽ được tài trợ trong Epoch luôn được ấn định trước). Một đề xuất có thể yêu cầu tài trợ cho một Epoch duy nhất hoặc cho nhiều Epoch.

Các đề xuất được phê duyệt để cấp vốn trong Epoch hiện tại thông qua biểu quyết ngưỡng mờ (FTV - Fuzzy Threshold Voting) . Mỗi cử tri có thể đưa ra một lá phiếu cho biết “có”, “không” hoặc “bỏ phiếu trắng” cho một đề xuất cụ thể (các lá phiếu cho các đề xuất khác nhau từ một cử tri thường được nhóm lại với nhau để tiết kiệm không gian Blockchain).

Điểm đề xuất là số phiếu “có” trừ đi số phiếu “không”. Các đề xuất có ít nhất 10% (trong tổng số phiếu bầu) chênh lệch dương là những ứng viên có thể chấp nhận được và tất cả những đề xuất còn lại đều bị loại bỏ. Các ứng viên được chấp nhận được xếp hạng theo điểm số của họ và đề xuất phổ biến nhất được tài trợ theo số tiền được yêu cầu, sau đó là ứng viên được chấp nhận tiếp theo, v.v. cho đến khi đạt đến giới hạn (một số phần của Epoch ngân quỹ có thể vẫn chưa tiêu hết; Coin cho nó hoàn toàn không được phát hành).

Các lá phiếu được giữ bí mật trong giai đoạn đầu tiên của Epoch (với thời gian khoảng 26 ngày), thay vào đó, mọi cử tri phải cung cấp cam kết tương ứng cho một lá phiếu biểu quyết (Voting Ballot). Giai đoạn cuối cùng (khoảng 4 ngày) đang được mở, nơi mỗi cử tri được khuyến khích mở lá phiếu của mình (điều đó phải hoàn toàn tương ứng với cam kết đã ban hành trước đó). Các lá phiếu mở cũng được đưa vào Blockchain.

Cử tri là các bên liên quan đến Crypto đã thực hiện một khoản tiền đặt cọc bị khóa đặc biệt, từ 500 Coin (một giao dịch khóa đặc biệt được phát hành). Chủ sở hữu có thể rút tiền đặt cọc bằng cách phát hành một giao dịch khác và số tiền đặt cọc đó sẽ khả dụng sau 3 Epoch tài trợ đầy đủ. Do đó, danh sách cử tri trong mỗi Epoch cũng luôn được cố định, tương tự như danh sách các đề xuất. Quyền biểu quyết tỷ lệ thuận với quy mô tiền đặt cọc tương ứng với tổng của tất cả các khoản tiền đặt cọc bỏ phiếu.

Có động lực để thực hiện các khoản tiền đặt cọc bỏ phiếu và tham gia vào quá trình bỏ phiếu. Mỗi cử tri sẽ nhận được phần thưởng từ số tiền 20% còn lại của ngân quỹ, theo chia sẻ của họ đối với tổng số tiền đặt cọc bỏ phiếu (tương tự như quyền biểu quyết). Phần thưởng ngân quỹ của cử tri được trả trong phần của họ tỷ lệ thuận với số lượng đề xuất được bỏ phiếu (đối với tổng số đề xuất trong Epoch hiện tại). Nếu một cử tri bỏ qua một số đề xuất, các đồng Coin tương ứng sẽ không được phát hành (không có sự phân phối lại cho các cử tri khác).

Một cử tri có thể ủy quyền cho một lá phiếu đề xuất cụ thể hoặc một tập hợp cho một cử tri khác. Trong trường hợp này, lá phiếu mở của họ (và cam kết tương ứng) có giá trị đặc biệt “theo ID cử tri” thay vì “có” / “không” / “bỏ phiếu trắng”. Khi xếp hạng đề xuất, quyền biểu quyết được ủy quyền cho một đề xuất (hoặc tập hợp của nó) sẽ được thêm vào phiếu bầu của đại biểu. Ủy quyền đầy đủ cho một số đại biểu cụ thể cũng được cung cấp.

Lưu ý rằng tất cả các thông số hệ thống được giới thiệu (chẳng hạn như số lượng Coin cho ngân quỹ hoặc số lượng phần thưởng của cử tri) cũng như các giải pháp kiến trúc không được đặt thành đá và là chủ đề để các thành viên cộng đồng phân tích và thảo luận thêm.

2. Hệ thống ngân quỹ của Ethereum Classic

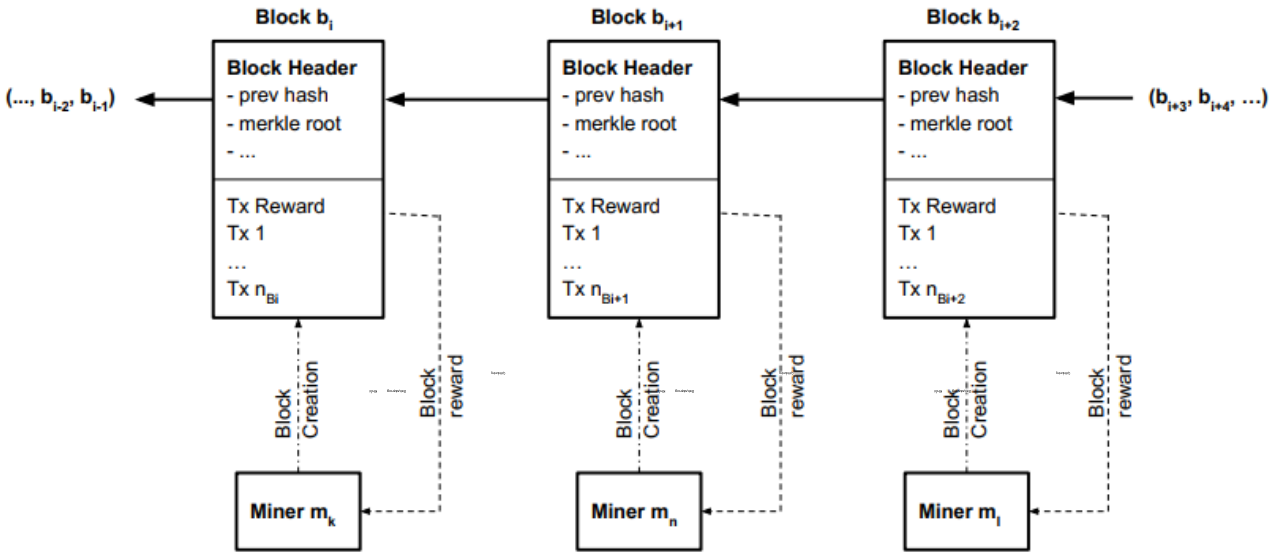
Trong phần này, chúng tôi đưa ra mô tả tóm tắt về hệ thống ngân quỹ có thể được triển khai để thiết lập cơ chế tự tài trợ cho hệ thống Crypto dựa trên Blockchain. Chúng tôi tập trung vào Ethereum Classic Blockchain, nhưng mô hình này có thể được sử dụng cho các Crypto khác, có thể với một số sửa đổi.

Đầu tiên, chúng tôi thảo luận ngắn gọn về Ethereum Classic Blockchain, chương trình phần thưởng của nó và sau đó tìm hiểu mô tả chi tiết về hệ thống ngân quỹ được đề xuất.

2.1. Ethereum Classic Blockchain

Tổng quan, Ethereum Classic là một sổ cái công khai phi tập trung dựa trên bằng chứng công việc với ngôn ngữ lập trình Turing-Complete được tích hợp sẵn cho phép viết các hợp đồng thông minh và các ứng dụng phi tập trung [9,10].

Nền tảng của Ethereum Classic Blockchain về cơ bản giống như Bitcoin, là loại Crypto nổi tiếng và thành công nhất tại thời điểm hiện tại [1]. Tính nhất quán của một sổ cái công khai của các Block trong một kế hoạch dựa trên bằng chứng công việc được bảo đảm thông qua quá trình khai thác phi tập trung. Các thợ đào liên tục cố gắng giải quyết một vấn đề tính toán khó là tìm ra giá trị Hash thấp hơn một số mục tiêu. Trong trường hợp thành công, họ có cơ hội tạo một Block và nhận phần thưởng từ Block này (Hình 2.1).



Hình 2.1: Sơ đồ chung của một hệ thống Blockchain

Chúng tôi không đi quá sâu vào chi tiết kỹ thuật của nền tảng Ethereum, mặc dù có nhiều thay đổi đáng chú ý so với Bitcoin, bao gồm tài khoản thay vì UTXO, cấu trúc bên trong được cải thiện, ngôn ngữ tập lệnh Turing-Complete, v.v. Bạn đọc quan tâm có thể tìm thấy tất cả thông tin cần thiết trong các nguồn gốc [8,9]. Thay vào đó, chúng tôi chỉ nêu bật một số điều có liên quan theo một cách nào đó đến hệ thống ngân quỹ được đề xuất.

Trước hết, cần đề cập rằng thời gian Block trung bình là khoảng 14 giây. Nó có nghĩa là khoảng B_{month} = 1.851.428 Block được tạo sau mỗi 30 ngày.

Sự khác biệt quan trọng thứ hai là phần thưởng Block. Mỗi Block bao gồm một khoản thanh toán phần thưởng đặc biệt cho thợ đào đã tạo ra Block này. Hiện tại trong Ethereum Classic, phần thưởng này tương đương với 5 đồng Coin mới được tạo (Uncle Block không được xem xét ở đây). Nó xấp xỉ $R_{month} = B_{month} \cdot 5$ = 9.257.140 Coin mỗi tháng. Toàn bộ phần thưởng được trả cho các thợ đào và đây là nguồn tiền mới duy nhất trong hệ thống.

Tóm lại, chúng ta có thể nói rằng mặc dù Ethereum cung cấp các tính năng nâng cao như ngôn ngữ lập trình Turing-Complete, cây Merkle cải tiến, giao thức GHOST được sửa đổi, các nguyên tắc cơ bản tương tự như các nguyên tắc được sử dụng trong Bitcoin và các Altcoin bằng chứng công việc khác.

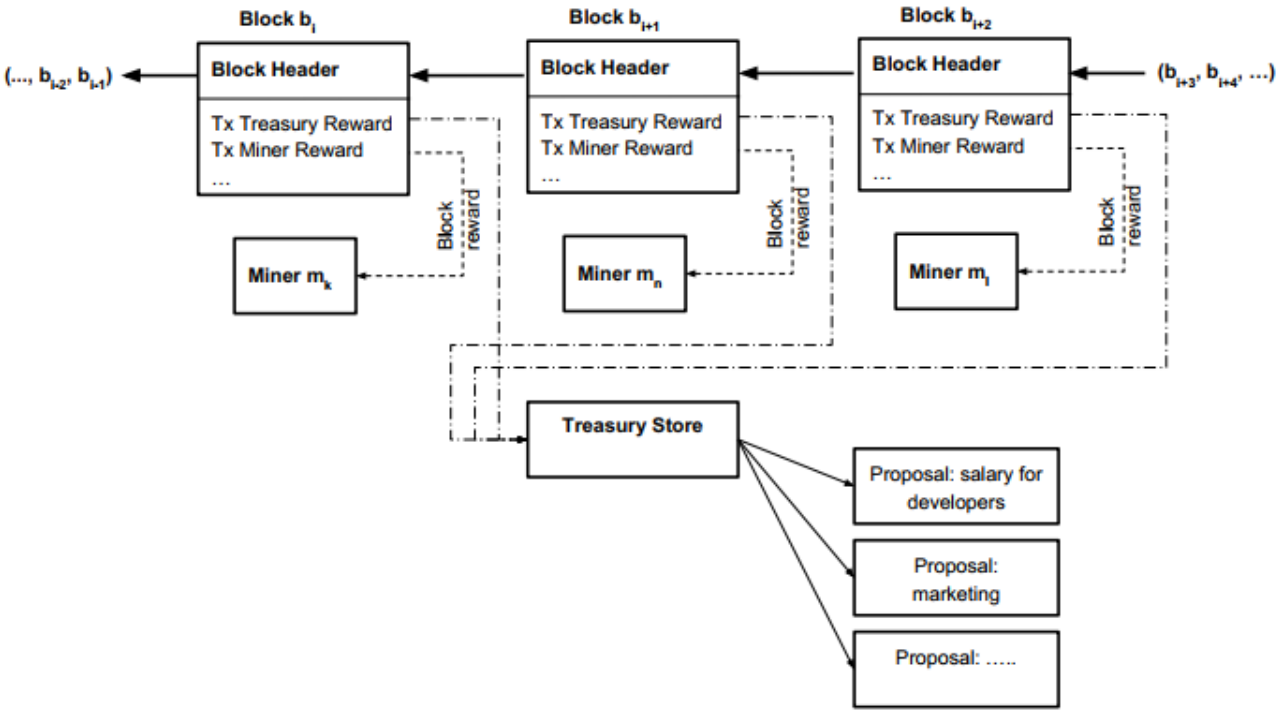
2.2. Mô hình ngân quỹ cơ bản

Ý tưởng cơ bản là giới thiệu một cơ chế cấp vốn cho các đề xuất khác nhau từ một kho ngân quỹ. Nguồn vốn cho các đề xuất có thể được phân bổ thông qua cơ chế khen thưởng. Hiện tại, hệ thống ngân quỹ nổi tiếng và thành công nhất đã được triển khai trong Crypto Dash [6,11,12]. Nó được gọi là Hệ thống quản trị Dash và được cho là sử dụng một sơ đồ đơn giản trong đó 10% phần thưởng Block Coinbase được thu thập để tài trợ cho các đề xuất khác nhau.

Mô hình ngân quỹ được đề xuất cho nền tảng Ethereum Classic dựa vào phần thưởng Block như một nguồn tài trợ. Ý tưởng chung được trình bày trên Hình 2.2. Có một thực thể - "Kho Ngân quỹ" (Treasury Store) - đóng vai trò là nơi tích lũy tiền để sử dụng trong tương lai. Kho như vậy không nhất thiết phải được triển khai dưới dạng tài khoản đặc biệt hoặc hợp đồng thông minh; tiền trong ngân quỹ có thể dễ dàng được tính toán cho một chiều cao Block cụ thể và được tạo ra khi nó thực sự cần thiết. Trong trường hợp này không cần giao dịch trả thưởng đặc biệt để đưa tiền vào kho ngân quỹ. Các đề xuất có thể được tài trợ trực tiếp từ các giao dịch Coinbase. Các quyết định liên quan đến tài trợ của các đề xuất cụ thể có thể được các bên liên quan đưa ra chung thông qua thủ tục bỏ phiếu.

Bản thân đề xuất là một yêu cầu tài trợ. Nó tồn tại dưới dạng lá phiếu đề xuất được gửi lên Blockchain để mọi cử tri hợp lệ có thể xem xét và bỏ phiếu. Bất kỳ ai cũng có thể gửi một lá phiếu đề xuất. Ví dụ: đại diện nhóm phát triển cốt lõi có thể yêu cầu thanh toán cho các dịch vụ cơ sở hạ tầng CNTT, lương của nhà phát triển, v.v.

Trong phần này, chúng tôi trình bày kiến trúc cấp cao của hệ thống ngân quỹ được đề xuất cho Ethereum Classic.



Hình 2.2: Kho ngân quỹ

2.2.1. Epoch tài trợ

Thủ tục cấp vốn bao gồm nhiều giai đoạn. Một điểm quan trọng là quá trình này là lặp đi lặp lại. Chúng tôi sẽ gọi mỗi lần lặp lại là một *Epoch tài trợ*.

Epoch tài trợ là một khoảng thời gian (được tính bằng Block) trong đó một nhóm cử tri được xác định trước quyết định về việc phân bổ vốn trong số các đề xuất được xác định trước. Các khoản tiền được tích lũy trong Epoch.

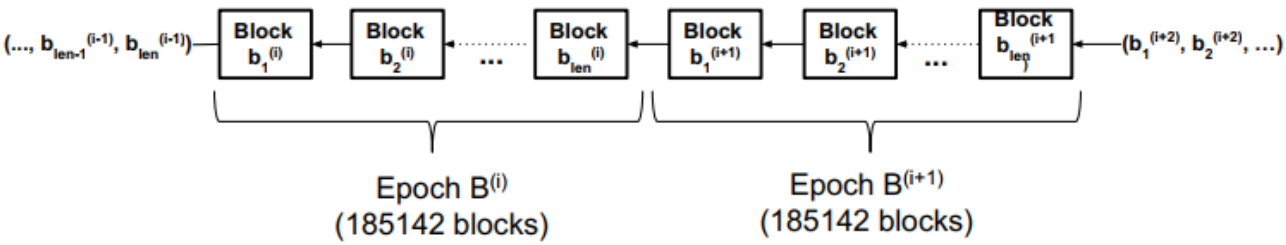
Chính thức hơn, hãy đặt $B = (B^{(1)}, B^{(2)},...)$ là một Blockchain của Crypto có hệ thống ngân quỹ, trong đó $B^{(i)} = (b_1^{(i)}, b_2^{(i)},\ldots, b_{len}^{(i)})$ đại diện cho một Epoch tài trợ thứ *i* bao gồm các *len* Block. Giới hạn tài trợ cho Epoch thứ *i* được xác định là

$$Tr(B^{(i)}) = \sum_{j=1}^{len} tr(b_j^{(i)}), \qquad (2.1)$$

trong đó $tr(b_j^{(i)})$ là một phần của phần thưởng Block được giao cho kho ngân quỹ.

Ngoài ra còn có một danh sách các dự án $P^{(i)} = (p_1^{(i)}, p_2^{(i)},\ldots, p_{p(i)}^{(i)})$ tại Epoch tài trợ thứ *i* sẽ được bình chọn bởi nhóm cử tri $V^{(i)} = (v_1^{(i)}, v_2^{(i)},\ldots, v^{(i)}_{v(i)})$ để quyết định phân bổ quỹ $Tr(B^{(i)})$ (cử tri cũng nhận được một số phần của các quỹ này như một phần thưởng, nó được thảo luận trong phần 2.4.2).

Nói chung, toàn bộ Blockchain được chia thành các Epoch có thời hạn không đổi (Hình 2.3). Thời hạn Epoch tương đương với 1 tháng (30 ngày). Nền tảng Ethereum Classic có thời gian Block trung bình gần 14 giây, điều đó có nghĩa là thời lượng Epoch sẽ là *len* = 185.142 Block.



Hình 2.3: Các Epoch tài trợ

2.2.2. Các giai đoạn của Epoch

Trong phần này, chúng tôi xác định các giai đoạn khác nhau của Epoch tài trợ và thảo luận về mục đích của từng giai đoạn đó. Nói chung, các giai đoạn tiếp theo có thể được đánh dấu như sau: đệ trình (Submission) , bỏ phiếu (Voting) và hoàn thiện (Finalization).

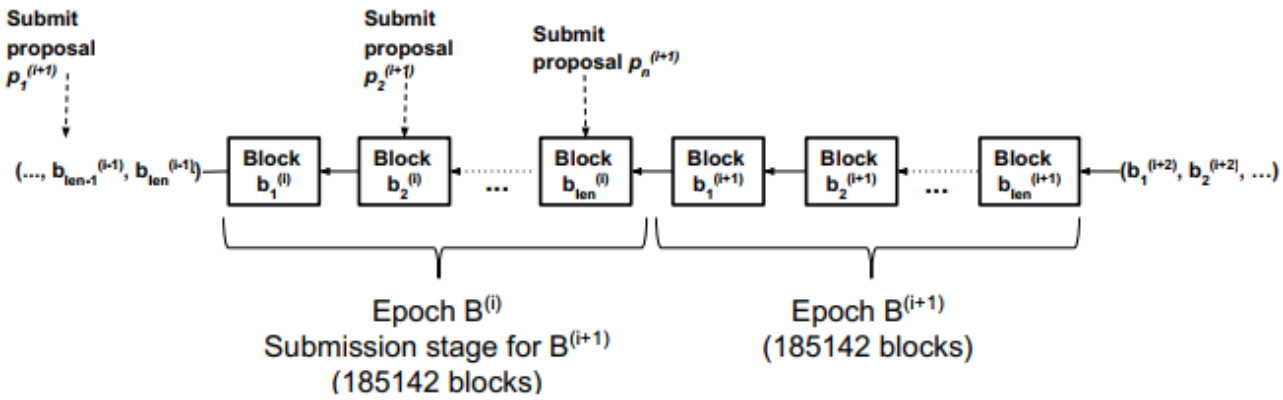
Sự cần thiết của các giai đoạn bỏ phiếu và hoàn thiện riêng biệt bắt nguồn từ thực tế là chúng tôi sử dụng một cam kết / kế hoạch tiết lộ đơn giản [13] để giữ bí mật các lá phiếu bỏ phiếu trong quá trình bỏ phiếu.Việc tiết lộ phiếu bầu chỉ xảy ra ở giai đoạn hoàn thiện khi tất cả các cử tri đã gửi cam kết của họ.

Giai đoạn đệ trình: Mục đích của giai đoạn đệ trình là thu thập các đề xuất cần được xem xét bởi cử tri. Nó kéo dài trước khi Epoch tài trợ bắt đầu vì một tập hợp đề xuất $P^{(i)} = (p_1^{(i)}, p_2^{(i)},\ldots, p_{p(i)}^{(i)})$ nên được cố định tại thời điểm bắt đầu bỏ phiếu.

Các đề xuất nên được đệ trình vào một trong những Epoch trước Epoch mà nó sẽ được bỏ phiếu và thanh toán (Hình 2.4). Mục đích của việc hạn chế như vậy khá đơn giản: cần có ít nhất một chu kỳ bỏ phiếu đầy đủ để cử tri có đủ thời gian xem xét tất cả các đề xuất. Không có hạn chế nào về việc gửi sớm, nhưng việc bỏ phiếu cho một đề xuất cụ thể sẽ chỉ diễn ra trong Epoch mà đề xuất đó yêu cầu tài trợ.

Vì vậy, nếu một đề xuất được cho là sẽ được bỏ phiếu và thanh toán trong Epoch $B^{(t)}$ thì nó nên được đệ trình trong Epoch $B^{(i)}$ với $i < t$.

Đặc tả chi tiết của một lá phiếu đề xuất được đưa ra trong các phần tiếp theo. Bây giờ chỉ cần đề cập rằng tất cả các đề xuất hợp lệ đều được đưa vào Blockchain, do đó, việc tìm hiểu khi nào một đề xuất cụ thể được gửi đi là điều không cần thiết.



Hình 2.4: Trình tự đề xuất

Giai đoạn bỏ phiếu: Trong giai đoạn bỏ phiếu, các cử tri bày tỏ ý kiến của họ về các đề xuất đã đệ trình. Việc lựa chọn cử tri sẽ được thảo luận sau; ở đầu mỗi Epoch luôn có một tập hợp các cử tri được xác định duy nhất $V^{(i)} = (v_1^{(i)}, v_2^{(i)},\ldots, v^{(i)}_{v(i)})$.

Ở giai đoạn này, các cử tri đệ trình các cam kết cho lá phiếu biểu quyết của họ. Bản thân các lá phiếu biểu quyết vẫn được giữ bí mật tại thời điểm này. Chúng chỉ nên được mở ở giai đoạn hoàn thiện khi tất cả các cử tri đã gửi cam kết của họ. Theo cách đơn giản như vậy, sự bí mật được cung cấp cho thủ tục bỏ phiếu vốn là một đặc tính rất đáng mong đợi của các chương trình bỏ phiếu (xem Phụ lục A và [14]).

Chính thức hơn, trong Epoch tài trợ $B^{(i)}$, một cử tri $v_1^{(i)}$ tính toán và công bố cam kết $c^{(i)}_{v1}$ đại diện duy nhất cho lá phiếu biểu quyết $vb^{(i)}_{v1}$ của họ:

$$c_{v_1}^{(i)} = H(vb_{v_1}^{(i)} \mid\mid r), \tag{2.2}$$

Trong đó $H(x)$ là một hàm Hash mạnh về mặt mật mã và r là một số giá trị ngẫu nhiên do cư tri tạo ra.

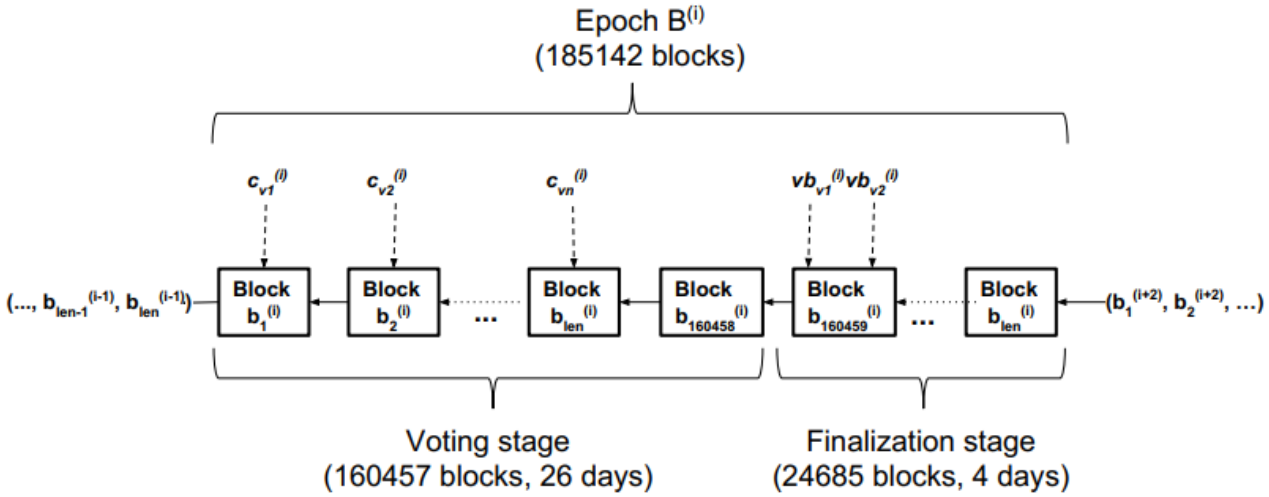
Giai đoạn bỏ phiếu kéo dài k Block đầu tiên của Epoch trong đó k = 160.457. Giá trị

của *k* được chọn sao cho nó xấp xỉ bằng 26 ngày (Hình 2.5).

Các cam kết cho Epoch hiện tại chỉ được tính đến nếu chúng được đưa vào Blockchain (trong các Block $b_1^{(i)}$, $b_2^{(i)}$, … , $b_{160457}^{(i)}$).

Một cử tri cụ thể chỉ có thể đưa ra một cam kết cho mỗi Epoch. Một cam kết được coi là chỉ có giá trị nếu nó được ký bởi một cử tri hợp lệ.

Vì vậy, ở cuối giai đoạn bỏ phiếu sẽ có một tập hợp các cam kết $C^{(i)} = c^{(i)}_{v1}, c^{(i)}_{v2}, \dots, c^{(i)}_{vn}$). Lưu ý rằng không nhất thiết tất cả các cử tri phải nộp các cam kết của họ. Trong trường hợp này, phiếu bầu của họ sẽ tự động được tính là "bỏ phiếu trắng".



Hình 2.5: Các giai đoạn của Epoch

Thủ tục bỏ phiếu cụ thể và cấu trúc của một lá phiếu biểu quyết sẽ được thảo luận trong các phần tiếp theo.

Giai đoạn hoàn thiện: Giai đoạn hoàn thiện kéo dài 24.685 Block (khoảng 4 ngày) vào cuối Epoch tài trợ (Hình 5). Trong giai đoạn này, những cử tri đã gửi cam kết trong giai đoạn bỏ phiếu phải gửi lá phiếu biểu quyết của họ $vb^{(i)}_{vj}$ cùng với sự ngẫu nhiên *r* (mở về sơ đồ cam kết / tiết lộ), vì vậy mọi người có thể kiểm tra xem lá phiếu biểu quyết có tương ứng với một số cam kết đã đệ trình trước đó $c^{(i)}_{vj}$.

Một lá phiếu biểu quyết chứa tất cả thông tin liên quan đến các tùy chọn của người dùng trong số các đề xuất. Lá phiếu biểu quyết chỉ hợp lệ nếu nó được xây dựng đúng cách:

- Người dùng đã ký vào lá phiếu biểu quyết là một cử tri hợp lệ;
- Cam kết cho lá phiếu biểu quyết này đã được cùng một cử tri đệ trình trước đó;
- Lá phiếu biểu quyết chỉ chứa phiếu bầu cho các đề xuất từ tập hợp $P^{(i)} = (p_1^{(i)}, p_2^{(i)}, \dots, p_{p(i)}^{(i)})$;
- Nó được bao gồm trong một trong các Block $b^{(i)}_{160459}, \dots, b^{(i)}_{len-1}$.

Không nhất thiết là tất cả các cử tri gửi cam kết cũng sẽ gửi phiếu bầu ở giai đoạn hoàn thiện, nhưng chúng tôi giả định rằng họ sẽ làm (một cơ chế khuyến khích cho

việc này sẽ được thảo luận thêm).

Cuối cùng khi kết thúc giai đoạn hoàn thiện (sau Block $b^{(i)}_{len-1}$) sẽ có tập hợp các phiếu biểu quyết xác định $VB^{(i)} = (vb^{(i)}_{v1}, \dots, vb^{(i)}_{vm})$ đại diện cho các lựa chọn của cử tri. Tất cả các lá phiếu biểu quyết đều được đưa trực tiếp vào Blockchain để mọi người có thể xem và xác minh kết quả.

Block cuối cùng trong Epoch $b^{(i)}_{len}$ là Block thanh toán. Nó không chứa các cam kết hoặc phiếu biểu quyết mà thay vào đó nó chứa các giao dịch với các khoản thanh toán cho các đề xuất chiến thắng.

2.3. Nộp đề xuất

Bước đầu tiên để nhận được tiền từ hệ thống ngân quỹ là gửi đề xuất dự án. Bất kỳ ai cũng có thể gửi đề xuất đến mạng lưới. Trong phần này, chúng tôi mô tả quá trình đệ trình cùng với định dạng của một lá phiếu biểu quyết.

2.3.1. Hình thành lá phiếu đề xuất

Một đề xuất $p_j^{(i)}$ được gửi lên mạng lưới phải tuân theo một định dạng đặc biệt. Chỉ những đề xuất hợp lệ mới được đưa vào Blockchain. Có 6 trường dữ liệu bắt buộc, chúng được thể hiện trong Bảng 2.1.

Bảng 2.1: Dữ liệu đề xuất

Tên trường dữ liệu	Mô tả
1. Tên đề xuất	Các ký hiệu có thể là [a-z, A-Z, 0-9]. Nó nên được đặt duy nhất trong số bất kỳ tên đề xuất hiện có.
2. URL đến mô tả đề xuất	Một chuỗi ký tự đại diện cho một URL đến mô tả.
3. Hash của mô tả đề xuất	Giá trị Hash của mô tả. Ví dụ: nếu URL liên kết đến tệp PDF có mô tả, giá trị Hash này là giá trị Hash của tệp PDF.
4. Block bắt đầu (Start Block)	Số Block khi khoản thanh toán đầu tiên được mong đợi. Lưu ý rằng một khoản thanh toán chỉ có thể xảy ra trong Block cuối cùng của Epoch $b^{(i)}_{len}$. Vì vậy số Start Block phải chia hết cho *len*.
5. Block kết thúc (End Block)	Số Block khi khoản thanh toán cuối cùng dự kiến sẽ được thực hiện. Nó phải lớn hơn hoặc bằng Start Block và cũng như chia hết cho *len*.
6. Địa chỉ thanh toán	Phải là một địa chỉ tài khoản hợp lệ.

7. Số tiền thanh toán	Phải là giá trị không âm, không vượt quá ngân sách tối đa của Epoch tài trợ ($0 < $ *Số tiền thanh toán* $\leq Pr(B^{(i)})$.
8. ID giao dịch tài sản thế chấp	ID của một giao dịch tài sản thế chấp. Một giao dịch tài sản thế chấp là khoản thanh toán tối thiểu cho việc nộp đề xuất.

Lưu ý rằng có hai giá trị *startBlock*($p_j^{(i)}$) và *endBlock*($p_j^{(i)}$) đại diện cho khoảng thời gian tài trợ cho đề xuất $p_j^{(i)}$. Nếu $p_j^{(i)}$ là thanh toán một lần, thì cả hai giá trị đều bằng nhau: *startBlock*($p_j^{(i)}$) = *endBlock*($p_j^{(i)}$). Nếu không, có đề xuất thanh toán nhiều lần:

$$k \cdot len = endBlock(p_j^{(i)}) - startBlock(p_j^{(i)}), \qquad (2.3)$$

trong đó *k* đại diện cho một số khoản thanh toán và *len* là quy mô của Epoch tài trợ.

2.3.2. Quy tắc đệ trình và chi phí

Trước khi gửi đề xuất, một giao dịch ký quỹ đặc biệt phải được tạo (một giao dịch như vậy chỉ có thể được giới thiệu bởi một đề xuất). Giao dịch này đốt 5 đồng Coin, đây là khoản thanh toán tối thiểu cho việc gửi đề xuất. Mục đích của việc thanh toán như vậy là ngăn chặn các cuộc tấn công DoS, vì vậy việc Spam mạng lưới với các đề xuất độc hại sẽ khó hơn và tốn kém hơn.

Sau khi đệ trình, đề xuất được chuyển tiếp qua mạng P2P tới tất cả các Node giống như một giao dịch điển hình. Để đề xuất có hiệu lực, nó phải được đưa vào Blockchain ít nhất là *len* Block trước *startBlock*($p_j^{(i)}$) (xem đoạn "Giai đoạn đệ trình").

2.3.3. Các điều khoản khác: thu hồi và giảm tiền

Hệ thống ngân quỹ được đề xuất cho phép thu hồi một đề xuất đã nộp trước đó. Nó có thể khá hữu ích trong các tình huống khác nhau, ví dụ như trong trường hợp một đề xuất đã được phê duyệt khác triển khai chức năng nâng cao hơn (các nhà phát triển hủy bỏ nhiều Epoch tài trợ đã được phê duyệt trước đó để ủng hộ đề xuất mới hơn đã được phê duyệt của họ).

Trong trường hợp này, chủ sở hữu của đề xuất có thể gửi một giao dịch thu hồi mà không mất phí. Để có hiệu lực, giao dịch đó nên được đưa vào Blockchain trước Block thanh toán. Trong trường hợp này, các lá phiếu biểu quyết cho dự án này sẽ không được tính và bản thân đề xuất cũng không được xem xét trong quá trình lựa chọn người chiến thắng. Không thể thu hồi số tiền đã được phân bổ.

Cũng có thể giảm số lượng Coin được yêu cầu. Cách tiếp cận tương tự cũng có thể áp dụng trong trường hợp này: giao dịch như vậy nên được đưa vào Blockchain trước Block thanh toán.

2.4. Cử tri

Một trong những phần quan trọng nhất của hệ thống ngân quỹ đã phát triển là xác định một tập hợp các cử tri $V^{(i)}$, những người được trao quyền tham gia vào thủ tục bỏ phiếu trong Epoch $B^{(i)}$. Tầm quan trọng của phần này của hệ thống xuất phát từ thực tế là những cử tri được lựa chọn phải được khuyến khích thích đáng để hành động không chỉ vì lợi ích của họ mà còn vì lợi ích của toàn bộ hệ thống.

Một giải pháp dễ dàng cho vấn đề này là trao quyền biểu quyết cho tất cả các bên liên quan trong hệ thống (theo số lượng cổ phần mà họ sở hữu). Trong trường hợp này, danh sách các bên liên quan được cố định tại một thời điểm nào đó (ví dụ: sau Block $b^{(i-1)}_{len}$ cuối cùng trong Epoch trước) và những người có số dư dương có thể tham gia bỏ phiếu trong Epoch $B^{(i)}$. Nhưng một sơ đồ như vậy có những nhược điểm đáng kể:

- Nó không giới thiệu các khuyến khích cá nhân trực tiếp để tham gia. Tại sao một người nào đó sẽ dành thời gian để xem xét các đề xuất và bỏ phiếu cho các đề xuất, nếu họ không có bất kỳ lợi ích nào để làm điều đó so với những người không tham gia;
- Cổ phần của người tham gia không bị khóa nên họ có thể tiêu ngay sau Block $b^{(i-1)}_{len}$. Nó có nghĩa là các bên không liên quan sẽ quyết định các đề xuất, đây là tài sản không mong muốn của hệ thống vì nó có thể dẫn đến các quyết định không tối ưu hoặc thậm chí độc hại;
- Sự tham gia không được kiểm soát sẽ làm phức tạp các ước tính về gánh nặng mạng lưới và tính toán. Trong trường hợp xấu nhất, nó sẽ dẫn đến một tình huống khi các bên liên quan hoàn toàn bất khả tri và không muốn tham gia.

Tất cả lập luận được đề cập ở trên cho thấy sự cần thiết của một thủ tục lựa chọn cử tri mạnh mẽ hơn với các động lực mạnh mẽ để tham gia và cư xử trung thực.

Giải pháp được đề xuất dựa trên các khoản tiền đặt cọc bị khóa mà các cử tri muốn tham gia thủ tục bỏ phiếu phải nộp. Một động lực để làm như vậy là một phần thưởng đặc biệt được trả vào cuối mỗi Epoch tài trợ.

Ý tưởng sử dụng tiền đặt cọc cũng được sử dụng trong các loại Crypto khác, ví dụ như ở Tezos [15,16] và Dfinity [8].

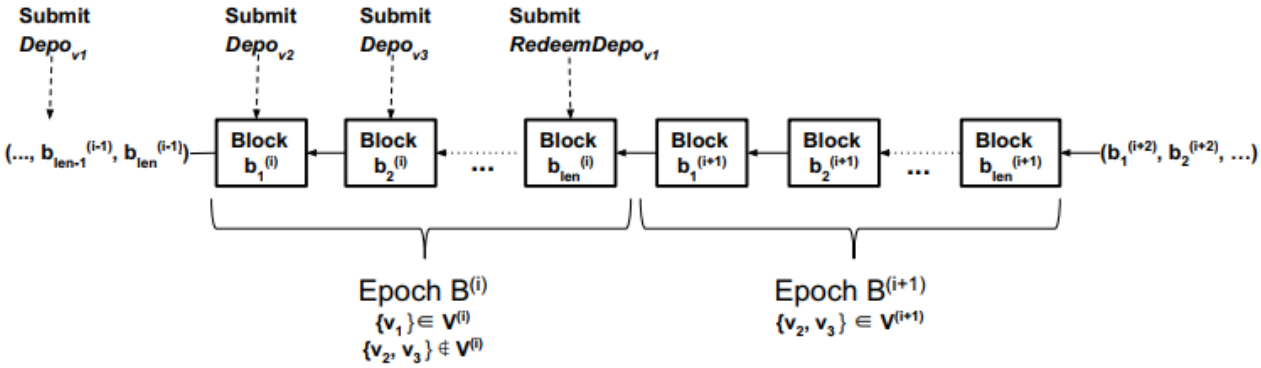
2.4.1. Nộp tiền đặt cọc và mua lại

Việc triển khai kỹ thuật các khoản tiền đặt cọc bị khóa khá đơn giản: người dùng v_j đăng giao dịch đặc biệt $Depo_{vj}$ lên Blockchain nơi họ xác định số lượng tiền gửi $amount(Depo_{vj})$. Lưu ý rằng để giao dịch $Depo_{vj}$ hợp lệ, người dùng phải có đủ số lượng Coin trong ví:

$$balance(v_j) \geq amount(Depo_{vj}), \qquad (2.4)$$

trong đó hàm *balance*(v_j) trả về một lượng cổ phần thuộc sở hữu của cư tri v_j.

Người dùng sẽ nhận được quyền biểu quyết trong Epoch $B^{(i+1)}$ sau Epoch $B^{(i)}$ nơi khoản tiền đặt cọc được thực hiện (Hình 2.6).



Hình 2.6: Nộp tiền đặt cọc và mua lại

Số lượng tiền đặt cọc không được nhỏ hơn ngưỡng tối thiểu *amount*($Depo_{vj}$) ≥ *minDepo*. Hiện tại, chúng tôi giả định rằng *minDepo* = 500. Ngưỡng như vậy là cần thiết vì một số lý do sẽ được chứng minh sau.

Vì giao dịch $Depo_{vj}$ đã được gửi nên người dùng không thể chi tiêu số cổ phần tương ứng. Để mở khóa các khoản tiền đã đặt cọc, người dùng cần gửi một giao dịch khác $RedeemDepo_{vj}$. Sau đó, sau thời gian đóng băng t_{freeze}, họ sẽ có thể truy cập vào tiền của mình. Hiện tại, chúng tôi cho rằng

$$t_{\text{freeze}} = 3 * len(Blocks),$$

trong đó *len* là kích thước của Epoch tài trợ. Có nghĩa là người dùng nên đợi 3 Epoch đầy đủ. Thời gian đóng băng t_{freeze} chỉ bắt đầu từ Epoch $B^{(i+1)}$ ngay sau Epoch $B^{(i)}$, khi việc mua lại được thực hiện. Người dùng không có quyền tham gia bỏ phiếu trong thời gian đóng băng t_{freeze}, nhưng giữ quyền này cho đến cuối Epoch hiện tại.

Đề án được đề xuất có một lợi thế đáng kể: nó luôn giữ cho một Epoch tài trợ cụ thể $B^{(i)}$ nhất quán, các nhóm cử tri $V^{(i)}$ và đề xuất $P^{(i)}$ được xác định và không thể thay đổi trong Epoch này. Điều này làm giảm một số Vectơ tấn công có thể xảy ra và cung cấp các cách tiếp cận tốt hơn để phân tích chính thức trong tương lai. Quy mô tiền đặt cọc cũng hạn chế việc tạo ra quá nhiều tài khoản bỏ phiếu cũng như bảo vệ hệ thống khỏi các cuộc tấn công tràn ngập.

2.4.2. Khuyến khích

Một cơ chế phần thưởng đặc biệt được đưa ra để khuyến khích các bên liên quan đặt cọc cổ phần của họ và tham gia bỏ phiếu. Như chúng ta đã thảo luận trong phần 2.2.1, số lượng Coin dành cho ngân quỹ bằng $Tr(B^{(i)})$ trên mỗi Epoch. Một phần của các quỹ này hướng đến phần thưởng cho các cử tri.

Gọi $Vr(B^{(i)})$ là phần thưởng cho những cử tri cho Epoch $B^{(i)}$ hiện tại. Theo gợi ý

rằng phần thưởng cho các cử tri được trích ngân quỹ tài trợ, chúng ta có

$$Vr(B^{(i)}) = k_{Vr} \cdot Tr(B^{(i)}), \quad (2.5)$$

trong đó k_{Vr} là một phần của ngân quỹ tài trợ trả cho cử tri, $0 \leq k_{Vr} < 1$.

Từ đó, số tiền ngân quỹ tài trợ được giao cho chính các đề xuất sẽ là

$$Pr(B^{(i)}) = (1 - k_{Vr}) \cdot Tr(B^{(i)}) = Tr(B^{(i)}) - Vr(B^{(i)}). \quad (2.6)$$

Chúng tôi lấy $k_{Vr} = 0.2$, cơ sở lý luận của sự lựa chọn này sẽ được đưa ra trong các phần tiếp theo.

Câu hỏi quan trọng thứ hai là phần thưởng của cử tri $Vr(B^{(i)})$ sẽ được phân bổ như thế nào trong tập hợp những cử tri $V^{(i)} = (v_1^{(i)}, v_2^{(i)}, \ldots, v^{(i)}_{v(i)})$. Hãy nhớ rằng tập $V^{(i)}$ và phần thưởng $Vr(B^{(i)})$ là các hằng số trong Epoch tài trợ $B^{(i)}$. Để giới thiệu chức năng phân phối, trước tiên chúng ta cần xác định khái niệm về *quyền biểu quyết*.

Định nghĩa 2.1. Một cử tri $v_j^{(i)}$ có *quyền biểu quyết* $vp_{vj}(i)$ phản ánh khả năng của họ để ảnh hưởng đến kết quả cuối cùng. Quyền biểu quyết $vp_{vj}(i)$ được xác định như sau:

$$vp_{v_j^{(i)}} = \frac{Depo_{v_j^{(i)}}}{\sum_{v_k^{(i)} \in V^{(i)}} Depo_{v_k^{(i)}}}, \quad (2.7)$$

vì vậy quyền biểu quyết gần bằng với phần cổ phần đã đặt cọc của cử tri $v_j^{(i)}$ so với tổng số tiền đặt cọc của tất cả cử tri trong Epoch $B^{(i)}$ (bao gồm $v_j^{(i)}$).

Giờ đây, thật dễ dàng để xác định giới hạn trên của phần thưởng bỏ phiếu cho một cử tri. Nó tỷ lệ thuận với quyền biểu quyết của họ:

$$vr_{v_j^{(i)}} \leq Vr(B^{(i)}) \cdot vp_{v_j^{(i)}}. \quad (2.8)$$

Chức năng phần thưởng chính xác sẽ phụ thuộc vào một tham số nữa được gọi là *Tỷ lệ tham gia.*

Định nghĩa 2.2. Cho một tập hợp tất cả các đề xuất $P^{(i)} = (p_1^{(i)}, p_2^{(i)}, \ldots, p_{p(i)}^{(i)})$ trong Epoch $B^{(i)}$, chúng ta xác định *Tỷ lệ tham gia* của một cử tri $v_j^{(i)}$ như sau:

$$prate_{v_j^{(i)}} = \frac{\#\left\{p_k^{(i)},\ so\ that\ p_k^{(i)} \in vb_{v_j}^{(i)}\right\}}{\#P^{(i)}}. \quad (2.9)$$

Nói một cách đơn giản, nó là một phần của các đề xuất được xem xét và bỏ phiếu bởi cử tri $v_j^{(i)}$.

Hàm phần thưởng được định nghĩa như sau:

$$vr_{v_j^{(i)}} = prate_{v_j^{(i)}} \cdot Vr(B^{(i)}) \cdot vp_{v_j^{(i)}}. \quad (2.10)$$

Vì vậy, có thể dễ dàng nhận thấy rằng phần thưởng phụ thuộc vào sự tham gia của cử tri. Chương trình như vậy tạo ra động lực trực tiếp để tham gia vào một thủ tục bỏ phiếu. Cùng với khái niệm về thời kỳ đóng băng, nó tạo thêm động lực để cư xử trung thực. Hỗ trợ các đề xuất độc hại sẽ phản ánh ngay lập tức về giá của đồng Coin và theo đó làm giảm giá trị thực tế của số tiền đặt cọc.

2.5. Nguồn ngân quỹ

Như đã đề cập trong phần 2.2.1 "Epoch tài trợ", các nguồn duy nhất cho ngân quỹ là phần thưởng Block và phí giao dịch. Chức năng ngân quỹ được giới thiệu như sau:

$$Tr(B^{(i)}) = \sum_{j=1}^{len} tr(b_j^{(i)}),$$

$$tr(b_j^{(i)}) = br(b_j^{(i)}) + fees(b_j^{(i)}),$$

trong đó $br(b_j^{(i)})$ là phần thưởng Block của Block $b_j^{(i)}$ cụ thể và $fees(b_j^{(i)})$ là phần phí giao dịch dành cho ngân quỹ.

2.5.1. Tài trợ trong chính sách tiền tệ ECIP-1017

Một chính sách tiền tệ mới và lịch phát hành Coin đã được đề xuất để thảo luận mở trong cộng đồng Ethereum Classic vào cuối năm 2016 [37]. Tuy nhiên, quyết định cuối cùng về việc áp dụng chính sách vẫn chưa được đưa ra và chúng tôi sẽ thảo luận về cách hệ thống ngân quỹ được trình bày phù hợp với chính sách tiền tệ mới.

Đề xuất ECIP-1017 "Chính sách tiền tệ và sửa đổi cuối cùng đối với lịch trình phát hành của Ethereum Classic" giới thiệu một số thay đổi quan trọng đối với chính sách tiền tệ hiện tại. Những thay đổi chính như sau:

1. Phần thưởng Block không còn liên tục theo thời gian nữa. Giả định rằng nó sẽ giảm 20% với mỗi Epoch mới (hãy nhớ rằng Epoch trong Ethereum Classic tương đương với 5.000.000 Block tương đương khoảng 2,3 năm).
2. Phần thưởng cho các Uncle Block giảm đáng kể. Theo chính sách mới, thợ đào Uncle Block sẽ chỉ nhận được 0,125 Coin thay vì 4,325 Coin như hiện nay.

Tính chất quan trọng nhất mà các quy tắc mới mang lại cho hệ thống là cung tiền có giới hạn cố định. Cộng đồng Ethereum Classic thường thừa nhận rằng một mô hình giới hạn sẽ mang lại sự ổn định lâu dài cho toàn bộ hệ thống và thu hút nhiều nhà đầu tư hơn.

Tuyên bố chung về chính sách tiền tệ của Ethereum Classic [38] tuyên bố tổng nguồn cung là khoảng 210 triệu ETC, không vượt quá 230 triệu ETC. Do đó, với phương án chính, chúng tôi cho rằng việc cấp vốn bằng ngân quỹ là hoàn toàn phù hợp với chính sách tiền tệ mới.

Ngân quỹ được tăng lên từ phần thưởng Block và phí giao dịch. Phần thưởng Block sẽ giảm 20% trong mỗi Epoch mới. Để bù đắp cho khoản giảm này và đảm bảo nguồn vốn ngân quỹ ổn định, một phần phí giao dịch cũng được gửi đến ngân quỹ.

Chúng tôi đề xuất gửi tới ngân quỹ tối đa 20%[1] phần thưởng Block, để lại cho những thợ đào từ 80% trở lên (khoảng 4/5 phần thưởng Block vẫn còn dành cho thợ đào và tối đa 1/5 sẽ được chuyển đến ngân quỹ).

Thời gian triển khai trong 18 tháng cũng được xem xét, khi nguồn tài trợ ngân quỹ tuần tự sẽ tăng từ 1/18 giá trị lên toàn bộ số tiền. Trong tháng đầu tiên, kho bạc nhận được 1/18 x 1/5 = 1/90 phần thưởng Block, hoặc ước chừng 1,1% phần thưởng Epoch và những thợ đào nhận được 99%. Trong tháng thứ hai, ngân quỹ được tài trợ cho 2/18 x 1/5 = 1/45 phần thưởng Block hoặc 2,2% được chuyển đến ngân quỹ, và 97,8% sẽ được nhận bởi các thợ đào, v.v. (3,3% + 96,7%, 4,4% + 95,6%, v.v.). Đối với tháng thứ 18, vào cuối giai đoạn triển khai và sau đó, ngân quỹ được tài trợ ở mức 20% (1/5) phần thưởng Block, và thợ đào nhận được 80% phần thưởng Block.

Xem xét tại thời điểm viết bài, phí giao dịch không đáng kể so với phần thưởng Block, ban đầu phần thưởng Block sẽ đóng vai trò chính trong việc cấp vốn, trong khi phí giao dịch sẽ quan trọng trong tương lai. Đối với Epoch đầu tiên, sau khi triển khai ngân quỹ đầy đủ, có thể chuyển trực tiếp đến ngân quỹ ETC lên đến 185.142 Coin (185.142 Block x 5 Coin x 20%) trên một Epoch. Giá trị Fiat của quỹ này dự kiến sẽ tăng theo thời gian như nó đã xảy ra với Dash sau khi triển khai DGS.

Chúng tôi giả định rằng tùy chọn này sẽ phù hợp hơn vì nó hoàn toàn tương thích với ECIP-1017.

Một lựa chọn thay thế của nguồn tài trợ ngân quỹ mà chúng tôi thấy là ít thích hợp hơn, nhưng rất đáng để thảo luận là tăng phần thưởng Block dành riêng cho ngân quỹ, vì vậy sẽ không cần phải phân bổ lại phần thưởng của thợ đào. Tùy chọn như vậy sẽ yêu cầu thay đổi chính sách tiền tệ ECIP-1017 vì sẽ cần phát hành thêm Coin cho ngân quỹ. Trong trường hợp tăng phần thưởng Block lên 1 Coin, do đó, nó sẽ tăng số lượng Coin cuối cùng được phát hành trong năm 2288 từ 210.725.892,25 (như được đề xuất trong ECIP-1017) lên 235.725.892,27 (tương đương 11,5%). Hơn nữa, thay đổi này có thể được giới thiệu vào đầu Epoch thứ hai khi phần thưởng của thợ đào sẽ giảm 20% (từ 5 xuống 4 Coin). Đồng thời, một đồng Coin bổ sung có thể được giới thiệu cho ngân quỹ. Vì vậy, tổng phần thưởng Block sẽ không thay đổi (bằng 5 Coin) cho Epoch thứ hai. Lưu

[1]Việc lựa chọn giá trị chính xác của phần thưởng Block được giao cho ngân quỹ là một vấn đề cần thảo luận thêm.

ý rằng trong trường hợp này, người ta cũng cho rằng phần thưởng ngân quỹ sẽ giảm 20% mỗi Epoch theo quy tắc ECIP-1017, do đó, mô hình cung ứng tiền tệ giới hạn không bị phá vỡ. Để bù đắp cho mức giảm này, chúng tôi giả định rằng một phần phí giao dịch sẽ được chuyển cho ngân quỹ.

Xem xét hai tùy chọn này, có vẻ như lựa chọn thay thế yêu cầu thay đổi thêm về chính sách tiền tệ sẽ có lợi hơn cho các thợ đào, vì nó cung cấp nhiều Coin trực tiếp hơn cho các thợ đào. Nhưng lợi nhuận của thợ đào phụ thuộc vào giá của đồng Coin, quyền ưu tiên của thợ đào có thể được thay đổi thành ngân quỹ phù hợp chính xác với ECIP-1017. Việc tăng tỷ giá trao đổi là một trong những hệ quả dự kiến chính của việc áp dụng ngân quỹ, sẽ mang lại lợi nhuận cho thợ đào nhiều hơn so với lựa chọn thay thế kèm theo rủi ro cho các nhà đầu tư Crypto, v.v. Tỷ giá trao đổi tăng 20% (bắt buộc trong khoảng thời gian 18 tháng) hoàn toàn bù đắp cho các thợ đào cho việc sửa đổi đó. Sự gia tăng hơn nữa sẽ cải thiện lợi nhuận của thợ đào (cũng như lợi nhuận cho các nhà đầu tư , v.v.) với chính sách tiền tệ ổn định và có thể dự đoán được.

Do đó, việc áp dụng ngân quỹ, cùng với việc tuân thủ nghiêm ngặt ECIP-1017 mang lại những lợi ích sau cho thợ đào.

1. Các nhà đầu tư Crypto sẽ được đảm bảo không có rủi ro nào từ việc phát hành thêm Coin (giữ cho các khoản đầu tư của họ không bị lạm phát, ít nhất là về số lượng Coin) sẽ dẫn đến việc tăng đầu tư vào ETC với ảnh hưởng tích cực đến tỷ giá trao đổi của ETC.
2. Từ ít phụ thuộc hơn đến độc lập hoàn toàn của ETC khỏi sự hỗ trợ từ bên ngoài (điều đó sẽ cung cấp thêm tính ổn định và khả năng dự đoán).
3. Được cấp chuyên môn nghiệp vụ lâu dài của cộng đồng ETC cho sự phát triển các dự án ETC.
4. Tiếp thị và các hoạt động khác để thúc đẩy ETC và mở rộng hơn nữa với sự gia tăng thị phần ETC.

2.5.2. Chính sách tiền tệ kế thừa

Trong trường hợp không chắc chắn nếu ECIP-1017 bị từ chối, ngân quỹ cũng có thể được sử dụng trong chính sách tiền tệ ETC hiện tại.

Hiện tại, phần thưởng Block trong Ethereum tương đương với 5 Coin và tất cả số tiền này được lấy bởi thợ đào. Chúng tôi đề xuất phân bổ lại phần thưởng Block để 1 Coin (chiếm 20% tổng phần thưởng Block) sẽ được phân bổ vào ngân quỹ.

Số lượng ngân quỹ trên mỗi Epoch tài trợ là:

$$Tr(B^{(i)}) = \sum_{j=1}^{len} tr(b_j^{(i)}) = len = 185.142 \text{ (Coin)}.$$

Tuy nhiên, cần phải chỉ ra rằng để ETC phát triển hơn nữa, chúng tôi thích lựa chọn áp dụng ECIP-1017 với sự tuân thủ nghiêm ngặt của ngân quỹ với các nguyên tắc của nó.

2.6. Phương thức bầu cử

Trong phần này, chúng tôi sẽ đưa ra mô tả về quy tắc bầu cử cốt lõi của bất kỳ quy trình bỏ phiếu nào.

Nhìn chung, phương pháp bỏ phiếu khá đơn giản: đưa ra một nhóm cử tri và một nhóm đề xuất, mỗi cử tri đưa ra một lá phiếu biểu quyết trong đó họ đánh dấu mỗi đề xuất bằng một trong các giá trị có thể: Chấp nhận, Bỏ phiếu trắng hoặc Từ chối. Sau khi thu thập tất cả các lá phiếu biểu quyết, có thể tính điểm cuối cùng cho mỗi đề xuất, gần bằng sự chênh lệch giữa số đồng Coin chấp nhận đề xuất và đồng Coin từ chối. Nếu điểm của một đề xuất ít nhất là 10% trên tổng số Coin đã gửi thì nó được coi là được chấp nhận. Sau đó, tất cả các đề xuất được chấp nhận được sắp xếp theo thứ tự giảm dần theo điểm số của chúng và được tài trợ cho từng người một cho đến khi hết Epoch ngân quỹ tài trợ (hoặc các đề xuất). Nếu một đề xuất không phù hợp với ngân sách còn lại, thì nó sẽ bị bỏ qua và quá trình tiếp tục với các đề xuất sau (hãy nhớ rằng điều kiện cần thiết để đề xuất được chấp nhận là ít nhất 10% cử tri ủng hộ theo quyền biểu quyết của họ).

Bây giờ chúng tôi đưa ra một mô tả chính thức cho một cuộc bầu cử E và quy tắc bầu cử R; xác định một tập hợp những người chiến thắng $W(B^{(i)})$.

Một *cuộc bầu cử* $E = \{P^{(i)}, V^{(i)}, VB^{(i)}\}$ được cho bởi tập đề xuất dự án $P^{(i)} = \{p_1{}^{(i)}, p_2{}^{(i)},\ldots, p_{p(i)}{}^{(i)}\}$, tập cử tri $V^{(i)} = \{v_1{}^{(i)}, v_2{}^{(i)},\ldots, v_{v(i)}{}^{(i)}\}$ và tập hợp phiếu bầu $VB^{(i)} = \{vb_{v1}{}^{(i)}, \ldots, vb_{vm}{}^{(i)}\}$, trong đó mỗi $vb_{vj}{}^{(i)}$ đại diện cho sở thích của cử tri $v_j{}^{(i)} \in V^{(i)}$. Phiếu biểu quyết của cử tri thứ j gồm 3 tập hợp $vb_{vj}{}^{(i)} = \{vb_{vj}{}^{Y}, vb_{vj}{}^{A}, vb_{vj}{}^{N}\}$:

- $vb_{vj}{}^{Y} \subseteq P^{(i)}$ (tập hợp các đề xuất $vb_{vj}{}^{Y} = \{p^{(i)}{}_{\mu j(1)}, p^{(i)}{}_{\mu j(2)}, \ldots, p^{(i)}{}_{\mu j(nj)}\}$ được bỏ phiếu tích cực bởi cử tri $v_j{}^{(i)} \in V^{(i)}$);
- $vb_{vj}{}^{A} \subseteq P^{(i)}$ (tập hợp các đề xuất $vb_{vj}{}^{A} = \{p^{(i)}{}_{gj(1)}, p^{(i)}{}_{gj(2)}, \ldots, p^{(i)}{}_{gj(mj)}\}$ được bỏ phiếu trung lập bởi cử tri $v_j{}^{(i)} \in V^{(i)}$);
- $vb_{vj}{}^{N} \subseteq P^{(i)}$ (tập hợp các đề xuất $vb_{vj}{}^{N} = \{p^{(i)}{}_{\eta j(1)}, p^{(i)}{}_{\eta j(2)}, \ldots, p^{(i)}{}_{\eta j(kj)}\}$ được bỏ phiếu tiêu cực bởi cử tri $v_j{}^{(i)} \in V^{(i)}$).

Một cử tri $v_j{}^{(i)}$ không thể đưa ra các phiếu bầu khác nhau cho cùng một đề xuất: $(vb_{vj}{}^{Y} \cap vb_{vj}{}^{N} = \emptyset) \wedge (vb_{vj}{}^{Y} \cap vb_{vj}{}^{A} = \emptyset) \wedge (vb_{vj}{}^{N} \cap vb_{vj}{}^{A} = \emptyset)$. Kết quả là $vb_{vj}{}^{(i)} \subseteq P^{(i)}$ (một tập hợp các đề xuất đã được bỏ phiếu bởi cử tri $v_i \in V$ luôn là một tập con của P).

Lưu ý rằng có thể một số đề xuất $v_j{}^{(i)} \notin vb_{vj}{}^{(i)}$. Có nghĩa là cử tri $v_j{}^{(i)}$ đã không bỏ phiếu cho đề xuất này. Trong trường hợp này, người ta cho rằng cử tri đã bỏ phiếu

trắng. Hãy nhớ rằng nếu một đề xuất không được đưa vào phiếu bầu một cách rõ ràng, phần thưởng của người dùng tương ứng sẽ bị giảm theo các quy tắc được trình bày trong phần 2.4.2. “Khuyến khích".

Quy tắc bầu cử R là một ánh xạ cho trước một cuộc bầu cử $E = \{P^{(i)}, V^{(i)}, VB^{(i)}\}$ xuất ra một tập hợp những người chiến thắng $W(B^{(i)}) = \{p^{(i)}_{\varpi(1)}, p^{(i)}_{\varpi(2)}, \dots, p^{(i)}_{\varpi(k)}\}$ được chọn để thanh toán trong Epoch tài trợ $B^{(i)}$. Tập hợp những người chiến thắng cuối cùng là tập hợp con của tất cả các đề xuất $W(B^{(i)}) \subseteq P^{(i)}$.

Để xác định quy tắc bầu cử *R*, chúng tôi sẽ nhắc lại hai hàm tiện ích là $amount(p_j^{(i)})$ và $Pr(B^{(i)})$:

- $amount(p_j^{(i)})$ đưa ra một đề xuất $p_j^{(i)}$ trả lại một số tiền theo yêu cầu của đề xuất này;
- $Pr(B^{(i)})$ cho một Epoch tài trợ $B^{(i)}$ trả lại giới hạn phần thưởng cho Epoch này (đó là số tiền tối đa có thể được trả cho tất cả các đề xuất).

Quy tắc bầu cử $R(E)$ trả về một tập hợp những người chiến thắng theo các quy tắc sau.

1. Gọi $score(p_k^{(i)})$ là hàm cho một đề xuất nhất định $p_k^{(i)} \in P^{(i)}$ trả về điểm cho đề xuất này $score(p_k^{(i)}) = \sum_{j=1}^{p(i)} (pre\ f(p_k^{(i)}, vb_{vj}^{(i)} * depo_{vj})$, trong đó $depo_{vj}$ là số lượng Coin đặt cọc[2] bởi cử tri v_j và hàm *pre f* trả về sở thích của họ liên quan đến đề xuất $p_k^{(i)}$:

$$pref(p_k^{(i)}, vb_{v_j}^{(i)}) = 1 \quad if\ p_k^{(i)} \in vb_{v_j}^{Y},$$

$$pref(p_k^{(i)}, vb_{v_j}^{(i)}) = -1 \quad if\ p_k^{(i)} \in vb_{v_j}^{N},$$

$$pref(p_k^{(i)}, vb_{v_j}^{(i)}) = 0 \quad if\ p_k^{(i)} \in vb_{v_j}^{A} \vee p_k^{(i)} \notin vb_{v_j}^{(i)}.$$

2. Cho $P^{(i)}_{accept} = \{p^{(i)}_{\chi(1)}, p^{(i)}_{\chi(2)}, \dots, p^{(i)}_{\chi(\iota(z))}\} \subseteq P^{(i)}$ là danh sách các đề xuất được sắp xếp sao cho $score(p^{(i)}_{\chi(1)}) \geq score(p^{(i)}_{\chi(2)}) \geq \dots \geq score(p^{(i)}_{\chi(\iota(z))})$, và với mỗi $p_k^{(i)} \in P^{(i)}_{accept}$, nó thể hiện $score(p_k^{(i)}) \geq 0{,}1 \cdot \sum_{vj \in V(i)} depo_{vj}$ (đề xuất có $score(p_k^{(i)}) < 0{,}1 \cdot |V^{(i)}|$ được coi là không được chấp nhận và không được đưa vào tập hợp $P^{(i)}_{accept}$).
3. Tập hợp những người chiến thắng $W(B^{(i)}) = \{p^{(i)}_{\varpi(1)}, p^{(i)}_{\varpi(2)}, \dots, p^{(i)}_{\varpi(k)}\}$ bao gồm các đề xuất từ $P^{(i)}_{accept}$ trong đó $score(p^{(i)}_{\varpi(1)}) \geq score(p^{(i)}_{\varpi(2)}) \geq \dots \geq score(p^{(i)}_{\varpi(k)})$, sao cho $\sum_{j=1}^{k} amount\ (p^{(i)}_{\varpi(j)}) \leq Pr(B^{(i)})$.

[2]Nói chung, nhân với tổng số phản ánh quyền biểu quyết của một cử tri cụ thể. Trong trường hợp này, hàm score hiển thị số lượng cổ phần ủng hộ đề xuất (thay vì số lượng cử tri).

Hãy nhớ rằng giới hạn phần thưởng $Pr(B^{(i)})$ của Epoch tài trợ $B^{(i)}$ được xác định như sau:

$$Pr(B^{(i)}) = (1 - k_{Vr}) \cdot Tr(B^{(i)}) = (1 - k_{Vr}) \cdot \sum_{j=1}^{len} tr(b_j^{(i)});$$

trong đó $tr(b_j^{(i)})$ là một phần của phần thưởng Block dành cho ngân quỹ và k_{Vr} là một phần của ngân quỹ tài trợ trả cho cử tri ($k_{Vr} = 0{,}2$).

2.6.1. Phiếu hoà (Tie Vote)

Về mặt lý thuyết, có thể có hai hoặc nhiều đề xuất có điểm số bằng nhau, $score(p_n^{(i)}) = score(p_m^{(i)}) = \ldots = score(p_k^{(i)})$ nhưng không thể được đưa vào $W(B^{(i)})$ đồng thời vì nó sẽ vượt quá giới hạn tài trợ $Pr(B^{(i)})$. Trong trường hợp này, chúng tôi cần các quy tắc bổ sung để xếp hạng các đề xuất như vậy để có thể xác định đề xuất nào sẽ chiến thắng.

Trong mô hình của chúng tôi, chúng tôi giả định các quy tắc đơn giản sau để phá vỡ mối quan hệ áp dụng từng quy tắc một cho đến khi giải quyết xong phiếu hòa:

1. Các đề xuất được xếp hạng theo số tiền thu thập được từ các Epoch tài trợ trước đó. Chúng tôi biểu thị hàm trả về số tiền là $score_{\text{prev}}(p_j^{(i)})$. Một đề xuất cụ thể sẽ có $score_{prev}(p_j^{(i)}) > 0$ chỉ trong trường hợp đó là đề xuất nhiều Epoch (yêu cầu tài trợ liên tục trong hơn một Epoch) và nó đã nhận được tiền trong các Epoch trước đó. Quy tắc như vậy sẽ mang lại lợi thế cho các dự án nổi tiếng và đã được chấp nhận trước đó:

$$score_{prev}(p_n^{(i)}) \geq score_{prev}(p_m^{(i)}) \geq \ldots \geq score_{prev}(p_k^{(i)}).$$

2. Nếu vẫn còn một số phiếu bầu giữa một số đề xuất, thì đề xuất đó sẽ được giải quyết theo quy tắc “ai đến trước được phục vụ trước” (FCFS). Các đề xuất đã được gửi trước đó (bao gồm cho Block trước đó; có chỉ số thấp hơn trong trường hợp cùng Block) có một lợi thế.

Tuy nhiên, khi chúng tôi xem xét các quy tắc giải quyết bằng phiếu hoà, dự kiến rằng những sự kiện như vậy có thể hiếm khi xảy ra.

2.7. Ủy quyền

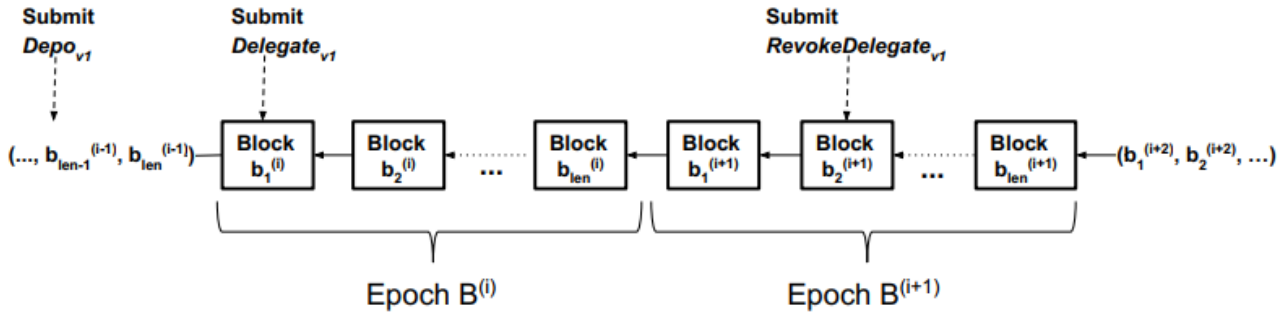
Để nhận được phần thưởng, cử tri cần phải trực tuyến để theo dõi danh sách các đề xuất, xem xét chúng và bỏ phiếu. Để giảm thiểu rủi ro về tỷ lệ tham gia thấp hoặc phân tích đề xuất kém, và để cung cấp cho cử tri sự linh hoạt hơn, chúng tôi đưa ra một kế hoạch ủy quyền, theo đó cử tri có thể tự động theo dõi một số cử tri khác.

Có hai loại ủy quyền: ủy quyền đầy đủ và ủy quyền một lần cho một đề xuất cụ thể. Trong khi uỷ quyền đầy đủ cần một giao dịch cụ thể, thì uỷ quyền một lần được thực hiện trực tiếp thông qua một lá phiếu biểu quyết.

2.7.1. Ủy quyền đầy đủ

Việc thực hiện ủy quyền đầy đủ là khá đơn giản. Chúng tôi chỉ cần hai loại giao dịch bổ sung: một loại cho việc ủy quyền và một loại khác để thu hồi.

Hình 2.7 đại diện cho ý tưởng cơ bản. Để ủy quyền quyền bỏ phiếu của mình, người dùng cần gửi giao dịch đặc biệt $Delegate_{vj}$. Giao dịch này sẽ trỏ đến cử tri (đại biểu) cụ thể sẽ được theo sau (ví dụ: nó có thể chứa khóa công khai của họ).



Hình 2.7: Ủy quyền

Giao dịch $Delegate_{vj}$ có thể được phát hành bất kỳ lúc nào bởi một cử tri hợp lệ (người đã đặt cọc). Lưu ý rằng việc ủy quyền và thu hồi sẽ chỉ có hiệu lực trong Epoch hiện tại nếu chúng được gửi trước giai đoạn hoàn thiện.

Ngay cả khi đã ủy quyền, cử tri vẫn có quyền tự bỏ phiếu. Ví dụ: họ có thể bỏ phiếu cho một số đề xuất mà họ quan tâm và ủy quyền các quyết định về các đề xuất khác cho người khác. Lá phiếu biểu quyết của người dùng được ưu tiên hơn lá phiếu biểu quyết của một đại biểu. Vì vậy, các phiếu bầu của đại biểu sẽ chỉ được tính đến nếu người dùng ban đầu không đưa chúng vào lá phiếu biểu quyết của họ (hoặc họ không phát hành lá phiếu biểu quyết nào cả).

Để thu hồi quyền ủy quyền, người bỏ phiếu cần gửi giao dịch $RevokeDelegate_{vj}$.

Để thay đổi đại biểu, cử tri cần hủy bỏ đại biểu trước đó. Chỉ một ủy quyền và một thu hồi được phép trong một Epoch.

Lưu ý rằng nếu một đại biểu chưa biểu quyết cho một số đề xuất, thì một cử tri ủy quyền cho quyền biểu quyết của mình sẽ không nhận được phần thưởng cho những đề xuất này. Nếu một đại biểu tự ủy quyền cho phiếu bầu của mình, thì phần thưởng uỷ quyền phải được trả cho những người thực sự đã bỏ phiếu.

2.7.2. Ủy quyền một lần

Một uỷ quyền cho một đề xuất cụ thể cho phép cử tri đưa vào lá phiếu biểu quyết của mình một giá trị đặc biệt “theo ID cử tri” thay vì “có” / “không” / “bỏ phiếu trắng”. Trong trường hợp này, bỏ phiếu đối với đề xuất này sẽ giống như phiếu biểu quyết của đại biểu tương ứng.

Các quy tắc tương tự như đối với ủy quyền đầy đủ được áp dụng ở đây. Nếu đại biểu

không bỏ phiếu cho đề xuất đó thì được coi là không bỏ phiếu của cử tri ban đầu (vì vậy họ sẽ không nhận được phần thưởng).

Uỷ quyền một lần được ưu tiên hơn so với uỷ quyền đầy đủ, vì vậy nếu cử tri bao gồm tuyên bố "làm theo lời cử tri $Delegate^t_{vj}$" cho một số đề xuất, thì phiếu bầu của $Delegate^t_{vj}$ sẽ được thực hiện trước. Nếu $Delegate^t_{vj}$ chưa bỏ phiếu, thì phiếu bầu của toàn bộ đại biểu sẽ được tính đến.

2.7.3. Phân phối phần thưởng

Trong trường hợp ủy quyền, một số phần thưởng bỏ phiếu được chuyển đến các đại biểu. Một mặt, nó khuyến khích đại biểu bỏ phiếu có chủ ý hơn (để nhiều cử tri muốn theo dõi họ hơn), mặt khác, nó ngăn cản việc ủy quyền thiếu suy nghĩ.

Có một tham số $0 \leq k_{Del} \leq 1$ xác định phần thưởng bỏ phiếu thuộc về đại biểu nào (k_{Del} = 0,05). Hãy nhớ lại phần 2.4.2 “Khuyến khích” rằng chức năng khen thưởng cho một cử tri được xác định là

$$vr_{v_j^{(i)}} = prate_{v_j^{(i)}} \cdot Vr(B^{(i)}) \cdot vp_{v_j^{(i)}},$$

trong đó

- $Prate_{vj}(i)$ là tỷ lệ tham gia (số đề xuất được bỏ phiếu so với tổng đề xuất);
- $Vr(B^{(i)})$ là tổng phần thưởng bỏ phiếu cho Epoch $B^{(i)}$;
- $vp_{vj}(i)$ là quyền biểu quyết của cử tri $v_j^{(i)}$.

Khi một cử tri có thể có nhiều uỷ quyền trong một Epoch cụ thể (một uỷ quyền đầy đủ và một số uỷ quyền một lần), chúng tôi sẽ xác định một tập hợp các uỷ quyền cho cử tri v_j cụ thể là $Delegate_{vj} = \{Delegate^1_{vj}, \ldots, Delegate^n_{vj}\}$.

Nếu một cử tri đã ủy quyền (đầy đủ hoặc một lần), chức năng phần thưởng của họ sẽ được xác định như sau:

$$vr_{v_j^{(i)}} = (prate_{v_j^{(i)}} + \sum_{t=1}^{n} pdrate^t_{v_j^{(i)}} \cdot (1 - k_{Del})) \cdot Vr(B^{(i)}) \cdot vp_{v_j^{(i)}},$$

trong đó

$$pdrate^t_{v_j^{(i)}} = \frac{\#\left\{p_k^{(i)},\ so\ that\ p_k^{(i)} \notin vb_{v_j}^{(i)} \wedge p_k^{(i)} \in vb^{(i)}_{Delegate^t_{v_j}}\right\}}{\#P^{(i)}}.$$

Nói theo nghĩa đen $pdrate^t_{vj}(i)$ là một phần của các đề xuất, nơi được bỏ phiếu bởi $Delegate^t_{vj}$. Bây giờ, thật dễ dàng để xác định phần thưởng của $Delegate^t_{vj}$:

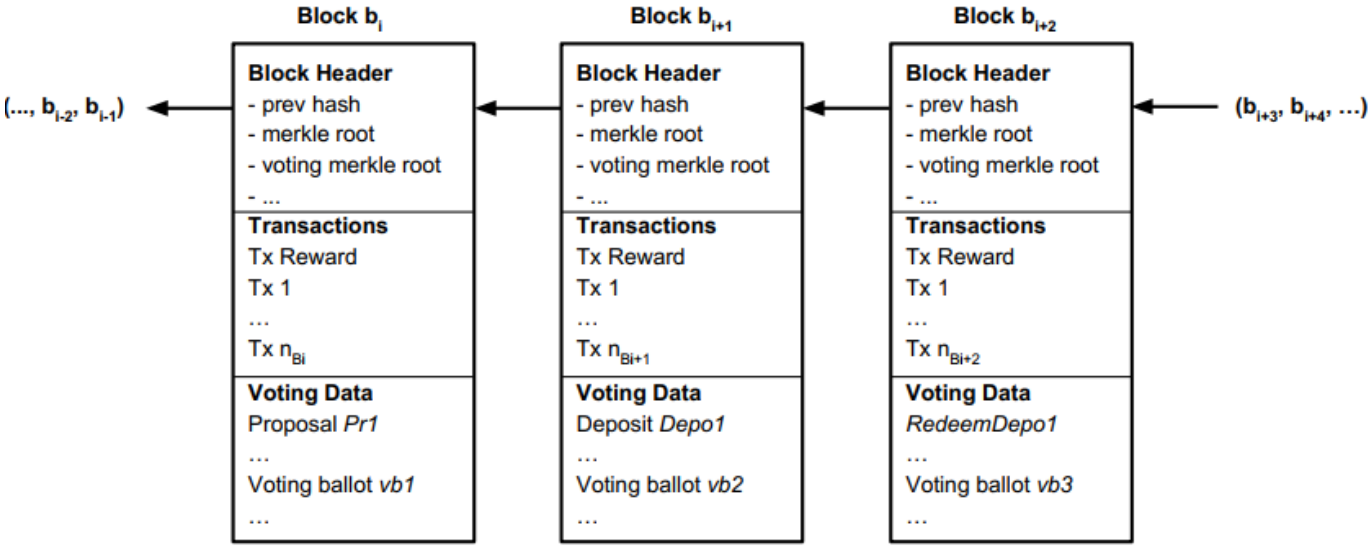
$$dr^t_{v_j^{(i)}} = pdrate^t_{v_j^{(i)}} \cdot k_{Del} \cdot Vr(B^{(i)}) \cdot vp_{v_j^{(i)}}.$$

3. Phương pháp triển khai kỹ thuật

Trong phần này, chúng tôi trình bày ngắn gọn mô tả cấp cao về các tùy chọn triển khai.

3.1. Thực hiện đồng thuận cốt lõi

Giải pháp khả thi đầu tiên là tích hợp ngân quỹ trực tiếp vào thuật toán đồng thuận cốt lõi. Tất cả dữ liệu liên quan đến bỏ phiếu cần được đưa vào Block cùng với các hành động chuyển đổi thông thường (ví dụ: chúng có thể được kết hợp thành cây Merkle). Quy tắc xác thực Block nhận được tiêu chí bổ sung.



Hình 3.1: Block mở rộng với dữ liệu liên quan đến bỏ phiếu

Việc thực hiện này có nhiều ưu điểm và dường như là lựa chọn tốt nhất cho ngân quỹ. Nó cung cấp một hệ thống hiệu quả, linh hoạt và mạnh mẽ có quy mô cao, có thể dễ dàng hỗ trợ hàng chục nghìn cử tri, nhiều đề xuất và có tiềm năng lớn để phát triển hơn (đối với giao thức bỏ phiếu mật mã tiên tiến, v.v.). Nhược điểm của cách tiếp cận này là nó yêu cầu cải tiến thêm định dạng Block và các quy tắc xác nhận.

Do đó, việc triển khai đồng thuận cốt lõi có vẻ là tối ưu cho phiên bản hoàn thiện của ngân quỹ.

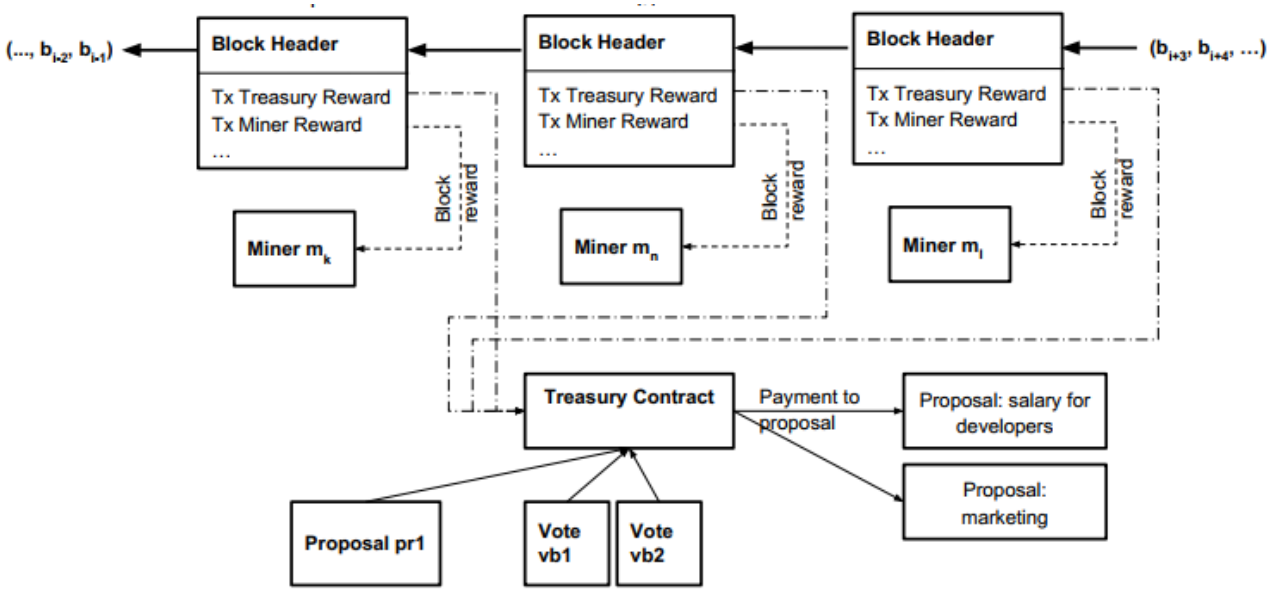
3.2. Thực hiện hợp đồng thông minh

Nền tảng Ethereum có một hệ thống hợp đồng thông minh nội bộ mạnh mẽ với ngôn ngữ tập lệnh Turing-Complete, có thể triển khai hệ thống ngân quỹ như một hợp đồng thông minh đặc biệt. Trong trường hợp này, cử tri sẽ chỉ giao tiếp bằng các hợp đồng thông minh, nơi tất cả dữ liệu liên quan đến quá trình bỏ phiếu sẽ được lưu trữ.

Cách tiếp cận như vậy cũng đòi hỏi một Hard-fork. Ưu điểm của cách tiếp cận này là giao thức đồng thuận cốt lõi cần ít sửa đổi hơn so với tùy chọn trước đó (cần thực hiện phân phối phần thưởng Block mới, với sự tham gia của hợp đồng ngân quỹ). Nhưng cách tiếp cận như vậy có những nhược điểm, ví dụ như hạn chế về khả năng

EVM, hạn chế về hiệu quả thực hiện, vấn đề tiềm ẩn với sự ủng hộ của một số lượng cử tri cần thiết và hạn chế về phạm vi phát triển (ví dụ: không thể thực hiện các giao thức bỏ phiếu tiên tiến trong tương lai). Bên cạnh đó, các hợp đồng thông minh cũng sẽ yêu cầu phí (dẫn đến việc sử dụng tài nguyên tính toán không hiệu quả: một phần của phần thưởng Block đi qua hợp đồng thông minh để được trả lại cho các thợ đào).

Hợp đồng thông minh có thể được sử dụng ở giai đoạn triển khai ban đầu, tuy nhiên, theo quan điểm của chúng tôi, việc triển khai đồng thuận cốt lõi dường như là cách tiếp cận tối ưu cho phiên bản hoàn thiện của ngân quỹ.



Hình 3.2: Hợp đồng thông minh ngân quỹ

4. Cơ sở lý luận về thiết kế

Trong phần này, chúng tôi đưa ra lý do thiết kế cho các giải pháp kiến trúc đã được trình bày ở trên.

4.1. Epoch tài trợ và quy mô của nó

Một khía cạnh quan trọng trong khi phát triển hệ thống ngân quỹ với nguồn vốn thường xuyên là thời hạn của mỗi kỳ tài trợ. Thời lượng Epoch không được quá lâu, do đó, sự chậm trễ trước khi nộp và thanh toán đề xuất phù hợp với các ứng dụng trong thế giới thực; mặt khác, thời gian của một Epoch không được quá ngắn để cho các cử tri sẽ có đủ thời gian để xem xét và bỏ phiếu cho tất cả đề xuất, v.v.

Khoảng thời gian 1 tháng là một giá trị đã được khẳng định trong thực tế. Rất nhiều hoạt động khác nhau trong thế giới tài chính được giới hạn bởi phạm vi 1 tháng. Trong trường hợp của ngân quỹ, nó cũng thích hợp vì những lý do sau:

1. Nó cho phép kiểm soát việc thực hiện dự án hàng tháng. Ví dụ, nếu có dự án dài hạn, nó sẽ được đánh giá lại mỗi Epoch tài trợ, và nếu cộng đồng cử tri không hài lòng với kết quả, họ có thể ngừng tài trợ. Việc cắt giảm đó có thể được thực hiện trên giai đoạn đầu khi tổn thất tài chính còn nhỏ.

2. Một tháng là khoảng thời gian khá dài nên các cử tri có đủ thời gian để cân nhắc kỹ lưỡng các quyết định.
3. Phần thưởng cho việc bỏ phiếu cũng được trả vào cuối Epoch tài trợ, vì vậy cử tri không cần chờ đợi quá lâu để nhận phần thưởng.

4.2. Bỏ phiếu dựa trên Blockchain

Kênh giao tiếp duy nhất trong hệ thống ngân quỹ được đề xuất là chính một Blockchain. Nó có nghĩa là tất cả các thông điệp (ví dụ như tiền đặt cọc, đề xuất, phiếu biểu quyết, ủy quyền, v.v.) được lưu trữ trực tiếp dưới một hình thức giao dịch đặc biệt. Vì vậy, toàn bộ thủ tục bỏ phiếu là không tương tác và không yêu cầu giao tiếp trực tiếp giữa các cử tri.

Việc xây dựng toàn bộ quy trình trên Blockchain mang lại lợi ích to lớn so với việc trao đổi thông điệp đơn giản qua mạng lưới P2P và lưu giữ một cơ sở dữ liệu bỏ phiếu riêng biệt. Nó cung cấp mức độ cao hơn nhiều về tính minh bạch và khả năng xác minh chung của hệ thống, cũng như cho phép xác minh đầy đủ mà không cần các bên đáng tin cậy. Mọi người đều có thể dễ dàng kiểm tra xem kết quả bỏ phiếu có tương ứng với sự ưa thích thực sự của cử tri hay không vì tất cả các lá phiếu biểu quyết có thể được tính toán lại. Tính hợp lệ của danh sách cử tri cũng có thể dễ dàng xác minh bằng cách kiểm tra các giao dịch đặt cọc liên quan.

Bỏ phiếu dựa trên Blockchain đáp ứng các thuộc tính bỏ phiếu mong muốn sau đây [14, 17]:

1. **Đảm bảo đủ điều kiện.** Với chuỗi Block nhất quán, rất dễ dàng để kiểm tra xem chỉ những cử tri hợp lệ mới thực hiện phiếu bầu của họ và chỉ một lần. Nó có thể được thực hiện bằng cách kiểm tra xem hành động chuyển tiền đặt cọc đã được thực hiện trước khi lá phiếu biểu quyết được phát hành và đây chỉ là một lá phiếu biểu quyết cho một cử tri cụ thể.
2. **Tính công bằng.** Không có kết quả ban đầu nào có thể ảnh hưởng đến các cử tri còn lại. Điều này cũng đúng với sơ đồ bỏ phiếu đã trình bày vì trong giai đoạn bỏ phiếu, các cam kết duy nhất được gửi lên Blockchain, vì vậy không ai có thể xem kết quả của những cử tri khác trong giai đoạn bỏ phiếu.
3. **Khả năng kiểm chứng cá nhân.** Một cử tri có thể xác minh rằng lá phiếu của mình đã thực sự được đếm. Nó rất dễ dàng để thấy rằng tài sản này cũng dành cho việc bỏ phiếu dựa trên Blockchain.
4. **Khả năng kiểm chứng phổ quát.** Kết quả được công bố thực sự là tổng của tất cả các phiếu bầu.

4.3. Số tiền ngân quỹ

Các nguồn duy nhất có thể có của ngân quỹ tài trợ là phần thưởng Block và phí giao dịch. Cụ thể, mỗi Block cung cấp một phần tiền thưởng hoặc phí giao dịch (hoặc cả hai) cho ngân quỹ (có thể xem chi tiết hơn trong phần 2.5. "Nguồn ngân quỹ").

Bây giờ trong Ethereum Classic, mỗi Block mới tạo ra 5 Coin mới được trả hoàn toàn cho thợ đào. Với hệ thống ngân quỹ, chúng tôi giả định rằng mỗi Block sẽ đóng góp một Coin vào ngân quỹ (đối với cả hai tùy chọn áp dụng ECIP-1017). Một lượng Coin cần thiết cho hệ thống ngân quỹ đã được chọn theo giá thực tế của Ethereum Classic trên thị trường. Tại thời điểm viết bài, ETC có giá khoảng 1,3 USD[3]. Có nghĩa là tổng quỹ hàng tháng của ngân quỹ ước tính là 241.000 USD, trong đó 193.000 USD được cho là được trả cho chính các đề xuất và 48.000 USD cho các cử tri là phần thưởng của họ. Những giá trị này cũng cung cấp biên độ an toàn đủ lớn cho những rủi ro có thể xảy ra khi tỷ giá trao đổi của ETC giảm.

4.4. Quy trình bỏ phiếu

4.4.1. Các đề xuất cố định và cử tri

Một tính chất quan trọng của kế hoạch bỏ phiếu đã phát triển là các bộ đề xuất và cử tri được ấn định trước khi cuộc bỏ phiếu bắt đầu. Giải pháp kiến trúc như vậy làm giảm các hành động độc hại có thể xảy ra trong quá trình bỏ phiếu (ví dụ: không thể đưa ra một đề xuất độc hại vào cuối giai đoạn bỏ phiếu và nhanh chóng chấp nhận nó, vì vậy các cử tri khác không có đủ thời gian để phân tích và bác bỏ nó). Điều này cũng làm giảm đáng kể các chiến lược bỏ phiếu đối nghịch và đơn giản hóa các phân tích lý thuyết sâu hơn.

4.4.2. Bỏ phiếu kín

Các lá phiếu kín là điểm mấu chốt để cung cấp tài sản công bằng. Nó được chấp nhận rộng rãi rằng tính chất này rất quan trọng đối với một sơ đồ bình chọn tốt [14, 17, Phụ lục A.3]. Nó đảm bảo rằng không ai có thể có bất kỳ kiến thức nào về kiểm đếm từng phần trước khi giai đoạn đếm bắt đầu. Kiến thức về việc kiểm phiếu một phần có thể ảnh hưởng đến ý định của những cử tri chưa bỏ phiếu và mang lại lợi thế cho họ để sửa đổi chiến lược bỏ phiếu của họ theo một kiến thức mới.

Bằng cách cung cấp tài sản công bằng với các cuộc bỏ phiếu kín, chúng tôi đảm bảo rằng tất cả các cử tri đều bình đẳng về quyền và khả năng.

[3]Theo cặp USDT / ETC trên https://poloniex.com/exchange#usdt, v.v.

4.5. Cơ cấu khuyến khích

Trong phần 2.4.2. "Khuyến khích", chúng tôi đã trình bày vai trò được trả tiền của cử tri trong hệ thống ngân quỹ. Chức năng khen thưởng cho cử tri cũng đã được trình bày. Ý tưởng chính của kế hoạch khuyến khích là tham gia vào thủ tục bỏ phiếu với một số lượng hợp lý các bên liên quan trung thực và hợp lý. Mặt khác, số lượng người bình chọn ít nhất phải có thể dự đoán được và nó không được quá lớn, do đó, tải tính toán và lưu trữ phù hợp với hệ thống Blockchain.

4.5.1. Số lượng cử tri dự kiến

Hãy nhớ rằng tổng phần thưởng cho cử tri được xác định như sau:

$$Vr\,(B^{(i)}) = k_{Vr} \cdot Tr\,(B^{(i)}),$$

trong đó k_{Vr} là một phần của ngân quỹ tài trợ trả cho cử tri. Phần thưởng được phân phối cho cử tri tùy theo quyền biểu quyết và tỷ lệ tham gia. Trước đây chúng tôi đã nói giá trị phù hợp cho tham số k_{Vr} là 0,2 nghĩa là 20% ngân quỹ tài trợ mỗi tháng được trả cho cử tri và phần còn lại (80%) được trả cho các đề xuất.

Sẽ là hợp lý khi giả định rằng các bên liên quan chỉ gửi cổ phần của họ nếu lãi suất ít nhất là một giá trị $k_{MinReward}$. Vì vậy, tham số $k_{MinReward}$ xác định thu nhập hàng năm được đo lường theo tỷ lệ với số tiền đặt cọc.

Đây là một nhiệm vụ rất quan trọng, đòi hỏi phân tích kinh tế phức tạp bên ngoài để ước tính giá trị chính xác của $k_{MinReward}$ phù hợp cho các bên liên quan, bởi vì nó phụ thuộc vào nhiều yếu tố kinh tế khác nhau mà khó có thể dự đoán được trong thế giới thực. Có lẽ yếu tố ảnh hưởng nhất là rủi ro biến động giá.

Từ các ví dụ trong thế giới thực[4], chúng ta có thể giả định rằng lãi suất tối thiểu cho các nhà đầu tư Crypto là khoảng 10% lợi nhuận hàng năm. Do đó, chúng tôi cũng đã lấy $k_{MinReward} = 0{,}1$ làm điểm bắt đầu trong tính toán.

Khi tổng phần thưởng của cử tri mỗi tháng được cố định bằng $Vr(B^{(i)})$, chúng tôi có thể ước tính tổng phần thưởng mỗi năm. Giả sử một năm tài trợ bao gồm 12 Epoch tài trợ (trên thực tế, nó sẽ ít hơn 365 ngày một chút vì một Epoch tài trợ tương đương với khoảng 30 ngày). Chúng ta có phần thưởng hàng năm Ar được xác định như sau:

$$Ar\,(B^{(i)}) = Vr\,(B^{(i)}) \cdot 12 = k_{Vr} \cdot Tr\,(B^{(i)}) \cdot 12.$$

[4]Theo một nghĩa nào đó, một cấu trúc khuyến khích tương tự được sử dụng trong Crypto Dash, nơi được gọi là các Masternode gửi tiền cổ phần của họ, cung cấp một số dịch vụ (bao gồm bỏ phiếu cho các đề xuất) và nhận phần thưởng cho việc này [4,5]. Theo như Dash đã được triển khai và khá phổ biến (top 10 theo Khối lượng theo http://poloniex.com), rất hữu ích khi thấy phần thưởng thực sự đạt được. Tại thời điểm viết bài, các tính toán của chúng tôi cho thấy lợi nhuận hàng năm của các khoản đầu tư cho các Masternode Dash xấp xỉ 10%. Các tính toán này gần giống với các tính toán được cung cấp trên http://dashmasternode.org.

Hãy nhớ rằng $Tr(B^{(i)}) = \sum_{j=1}^{len} tr(b_j^{(i)}) = 185.142$, vì vậy cuối cùng

$$Ar\ (B^{(i)}) = k_{Vr} \cdot 185142 \cdot 12 = k_{Vr} \cdot 2221704\ Coin.$$

Do các bên liên quan muốn lợi nhuận từ các khoản đầu tư ít nhất là 10% mỗi năm, chúng ta dễ dàng tính số lượng cổ phần *EAS* dự kiến sẽ tham gia để duy trì tỷ lệ này:

$$EAS = \frac{k_{Vr} \cdot Tr(B^{(i)}) \cdot 12}{k_{MinReward}} = k_{Vr} \cdot 22217040.$$

Như đã biết, nguồn cung của ETC bằng $60.102.216 \cdot (1{,}198 + 0{,}26n)$, trong đó n là số năm sau Block Genesis [8]. Tại thời điểm viết bài, tổng cung ETC ≈ 88.390.704. Từ đó, chúng ta có thể đánh giá tỷ lệ % của tổng số cổ phần dự kiến sẽ được đặt cọc:

$$EAS_{\%} = \frac{EAS}{88390704} \cdot 100\% = \frac{k_{Vr} \cdot Tr(B^{(i)}) \cdot 12}{k_{MinReward} \cdot 88390704} \cdot 100\%.$$

Vì vậy, có hai tham số chính có ảnh hưởng đáng kể đến $EAS_{\%}$: số lượng phần thưởng Block dành cho ngân quỹ và phần ngân quỹ tài trợ được trao cho cử tri. Điều chỉnh hai tham số này, chúng ta có thể tìm thấy sự cân bằng giữa nguồn cung ngân quỹ và số lượng cổ phần tham gia dự kiến.

Như chúng tôi đã nêu, giá trị ban đầu của các tham số được đề cập được lấy như sau:

1. $k_{Vr} = 0{,}2$, để 20% ngân quỹ tài trợ chuyển đến tay cử tri;
2. $tr(b_j^{(i)}) = 1$, do đó 1 đồng Coin mới trên mỗi Block được phát hành cho nhu cầu của ngân quỹ.

Theo đó, chúng ta có $EAS_{\%} = 8\%$, có nghĩa là với các tham số như vậy, dự kiến rằng 8% tổng số cổ phần sẽ tham gia vào một thủ tục bỏ phiếu[5]. Thoạt nhìn, có vẻ như tỷ lệ tham gia không đủ cao để đảm bảo thủ tục bỏ phiếu, nhưng hãy nhớ rằng 8% cổ phần này sẽ quyết định việc phân bổ xấp xỉ 0,2% tổng số cổ phần (phát hành cho ngân quỹ) mỗi tháng.

Số lượng cử tri tuyệt đối cũng sẽ phụ thuộc vào *minDepo* quy định số tiền tối thiểu của tiền đặt cọc được gửi. Điều chỉnh tham số này, có thể điều chỉnh hiệu quả tổng số người tham gia trong một thủ tục bỏ phiếu. Lấy *minDepo* = 500, chúng ta có thể ước tính số lượng cử tri dự kiến tối đa (*MENV*):

$$MENV = \frac{EAS}{minDepo} = \frac{4443408}{500} = 8886\ (Cử\ tri).$$

Lưu ý rằng rất ít khả năng tất cả các khoản tiền gửi ở mức tối thiểu là 500 Coin. Vì vậy, số lượng cử tri thực tế nên thấp hơn.

[5]Chúng ta cần phải đề cập rằng tỷ lệ tham gia dự kiến sẽ giảm từ năm này sang năm khác, cũng như số lượng Coin được phát hành tương đối do việc tạo ra các đồng Coin mới cho phần thưởng Block.

4.5.2. Tấn công 55%

Để có quyền kiểm soát được đảm bảo đối với quá trình bỏ phiếu, kẻ tấn công cần có 55% quyền biểu quyết, dự kiến sẽ chiếm khoảng 4,4% tổng số cổ phần trong hệ thống. Trong trường hợp này, họ sẽ có thể đẩy bất kỳ đề xuất ác ý nào lên. Giả sử rằng lợi nhuận từ hành động này bằng 0,2% tổng số lượng cổ phần mỗi tháng, theo đó, cuộc tấn công chỉ hợp lý nếu tác động tiêu cực đến giá Token nhỏ hơn $\frac{0,2}{4,4} \cdot 100\% = 4,5\%$.

Bất kỳ hành động độc hại thành công nào dự kiến sẽ tác động đáng kể đến giá Token và cũng như khoản tiền đặt cọc của kẻ tấn công (mức giảm giá dự kiến hơn 4,5%), điều đó làm cho các cuộc tấn công như vậy trở nên vô lý.

4.5.3. Nhóm cử tri tự cân bằng

Một lượng cố định của tổng phần thưởng mang lại thuộc tính quan trọng cho hệ thống đã phát triển. Nó trở nên tự cân bằng về số lượng cổ phần tham gia (do đó sẽ được phản ánh trên số cử tri thực tế). Nghĩa là sau đợt khởi động ban đầu, một lượng cổ phần tham gia sẽ đạt đến một giá trị nhất quán nào đó (chúng tôi mong đợi lên đến 8% tổng số cổ phần) và sau đó giá trị này chủ yếu được giữ lại.

Nếu một lượng đáng kể cổ phần đặt cọc bị thu hồi, thì nó sẽ tự động tăng phần thưởng cho những cử tri khác. Đổi lại, phần thưởng tăng thêm sẽ thu hút các bên liên quan mới gửi tiền cho đến khi phần thưởng cuối cùng đạt được giá trị nhất quán. Lập luận tương tự cũng có tác dụng ngược lại, và nó sẽ ngăn không cho đặt cọc quá nhiều.

Khi hệ thống phát triển, hệ thống trở nên ổn định và đáng tin cậy hơn, do đó sẽ tăng giá trị $EAS_{\%}$ vì có ít rủi ro hơn cho các bên liên quan, vì vậy họ có thể chấp nhận lãi suất thấp hơn.

4.5.4. Thời kỳ đóng băng

Lý do đằng sau việc đưa ra thời kỳ đóng băng t_{freeze} là cung cấp một cơ chế để hạn chế cử tri khỏi các hành động ác ý và khuyến khích họ đưa ra các lựa chọn tối ưu. Nếu một cử tri có hành động ác ý, nó sẽ ngay lập tức ảnh hưởng đến giá của đồng Coin tương ứng làm giảm giá trị thực tế của số tiền đặt cọc.

Vì vậy, cử tri được khuyến khích hành động theo cách mà nó ít nhất sẽ duy trì sự ổn định của toàn bộ hệ thống và giá Token. Trong thực tế, giả sử rằng các cử tri sẵn sàng tăng lợi nhuận của họ, chúng tôi mong đợi các quyết định hợp lý.

Cùng với phần thưởng trực tiếp cho sự tham gia tích cực, thời kỳ đóng băng tạo ra một hệ thống được thiết lập tốt để đưa ra các quyết định tối ưu liên quan đến các khoản đầu tư vào các đề xuất khác nhau.

4.6. Quy tắc bầu cử

Quy tắc bầu cử (hệ thống bỏ phiếu) là một trong những thành phần chính của hệ thống ngân quỹ Crypto cần được lựa chọn rất cẩn thận. Có rất nhiều hệ thống bỏ phiếu khác nhau: bỏ phiếu đa số, bỏ phiếu ưu tiên, bỏ phiếu chính, v.v. [18, 19, 20, 21, v.v.] Chúng có các cách tiếp cận và tính chất khác nhau, nhưng tất cả chúng đều cố gắng đáp ứng cùng một mục tiêu - để đáp ứng càng nhiều cử tri có kết quả bầu cử càng tốt. Đó là một nhiệm vụ khó khăn vì cử tri có thể hành động một cách chiến lược (từ bỏ sự ưa thích trực tiếp của họ) để tăng khả năng hài lòng của chính họ. Việc phân tích các hành vi đó thuộc phạm vi của các phương pháp lý thuyết trò chơi.

So sánh hệ thống bỏ phiếu thường dựa trên tập hợp các tiêu chí cụ thể: quy tắc đa số, điều kiện Pareto, tính độc lập của các lựa chọn thay thế không liên quan (IIA-Independence of Irrelevant Alternatives), định lý bất khả thi của Arrow, phương pháp của Condorcet, tiêu chí người chiến thắng Condorcet (người thua cuộc), tiêu chí tính đơn điệu, tiêu chí tham gia, v.v. . [22] Tuy nhiên, không có hệ thống bỏ phiếu nào đáp ứng tất cả tiêu chí. Hơn nữa, trong khi lựa chọn quy tắc bầu cử cho một hệ thống quản trị, cần tính đến một số đặc tính khác như tính đơn giản của phiếu bầu và tính toán, chi phí máy bỏ phiếu thấp, v.v. cần được tính đến.

4.6.1. Các loại hệ thống bỏ phiếu

Có các loại hệ thống bỏ phiếu chính sau đây [21]:

- Bỏ phiếu đa số (Plurality Voting) [18];
- Bỏ phiếu theo đa số (Majority Voting);
- Bỏ phiếu ưu tiên (xếp hạng) (Borda, STV, IRV, v.v.)[19,20];
- Bỏ phiếu chính (đánh giá) (Phê duyệt, Phạm vi, Tích lũy) [21].

Các hệ thống này về cơ bản được định hướng cho các cuộc bầu cử một người chiến thắng, nhưng hầu hết chúng cũng có thể được sử dụng trong các cuộc bầu cử nhiều người chiến thắng.

Hệ thống bỏ phiếu đa số là một hệ thống bỏ phiếu mà trong đó mỗi cử tri chỉ được phép bỏ phiếu cho một ứng cử viên và ứng cử viên nào nhận được nhiều (đa số) phiếu hơn các ứng cử viên khác sẽ được bầu [18]. Quy tắc đa số còn được gọi là quy tắc đa số đơn giản (không phải đa số tuyệt đối). Nếu chỉ có hai lựa chọn thay thế thì đó là một thủ tục rất tốt. Tuy nhiên, đối với nhiều hơn hai lựa chọn thay thế, bỏ phiếu đa số có một số vấn đề [18, 21]:

- Thông tin về sự ưa thích của cử tri bị bỏ qua (chỉ ứng viên được yêu thích nhất mới có thể được chọn);

- Có sự phân tán phiếu bầu giữa các ứng cử viên giống nhau về mặt tư tưởng;
- Nó khuyến khích cử tri không bỏ phiếu cho người yêu thích thực sự của họ, nếu ứng cử viên đó được coi là có ít cơ hội chiến thắng;
- Khuyến khích cử tri bỏ phiếu cho một trong hai ứng cử viên mà họ dự đoán là có nhiều khả năng chiến thắng nhất, ngay cả khi sự ưa thích thực sự của họ là không, vì lá phiếu cho bất kỳ ứng cử viên nào khác có thể sẽ không ảnh hưởng đến kết quả cuối cùng.

Bỏ phiếu đa số (Plurality Voting) được phân biệt với hệ thống bỏ phiếu theo đa số (Majority Voting), trong đó, để giành chiến thắng, một ứng cử viên phải nhận được đa số phiếu tuyệt đối (nhiều hơn tất cả các ứng cử viên khác cộng lại) [18]. Bỏ phiếu theo đa số (Majority Voting) có các vấn đề gần giống như bỏ phiếu đa số (Plurality Voting).

Bỏ phiếu ưu tiên hoặc xếp hạng mô tả một số hệ thống bỏ phiếu nhất định trong đó cử tri xếp hạng kết quả theo thứ bậc trên thang thứ tự. Khi lựa chọn trong số nhiều hơn hai lựa chọn, hệ thống bỏ phiếu ngay lập tức cung cấp một số lợi thế so với bỏ phiếu đa số. Một trong những ưu điểm chính là kết quả bầu cử sẽ phản ánh chính xác hơn mức độ ủng hộ cho tất cả các ứng viên.

Có nhiều hệ thống bỏ phiếu ưu tiên: bỏ phiếu tức thời (IRV) [19], hệ thống Borda [23], biểu quyết có thể chuyển nhượng một lần (STV) [24], phương pháp Schulze [25], hệ thống bỏ phiếu ưu tiên cho một người chiến thắng tối ưu (hệ thống GT) dựa trên tính toán các chiến lược hỗn hợp tối ưu [26] v.v.

Ví dụ, hệ thống IRV có đa số người chiến thắng [19], nhưng không đáp ứng một số tiêu chí (IIA, người chiến thắng Condorcet và tiêu chí về tính đơn điệu) và có xác suất ràng buộc trong bầu cử cao hơn so với bỏ phiếu đa số [22].

Hệ thống bỏ phiếu Borda [23] đơn giản, minh bạch và ổn định trước những thay đổi nhỏ trong thứ hạng, nhưng nó cũng không đáp ứng một số tiêu chí (quy tắc đa số, người chiến thắng Condorcet và tiêu chí nhân bản độc lập) [22].

Phân tích được thực hiện trong [27] đã cho thấy một số khiếm khuyết của bỏ phiếu ưu tiên được hình thành như bốn nghịch lý sau đây.

1. *Nghịch lý No-Show*. Việc bổ sung các lá phiếu giống hệt nhau với ứng cử viên *x* xếp hạng cuối cùng có thể thay đổi người chiến thắng từ một ứng cử viên khác thành *x*.
2. *Nghịch lý Thwarted-Majoaries*. Một ứng cử viên có thể đánh bại mọi ứng cử viên khác khi so sánh trực tiếp với đa số phiếu có thể thua cuộc bầu cử.

3. *Nghịch lý nhiều quận*. Một ứng cử viên có thể giành chiến thắng ở từng quận riêng biệt, nhưng sẽ thua trong cuộc tổng bầu cử ở các quận kết hợp.
4. *Nghịch lý nhiều hơn là ít hơn*. Nếu người chiến thắng được xếp hạng cao hơn bởi một số cử tri, tất cả những thứ khác không thay đổi thì một ứng cử viên khác có thể đã thắng.

Mặc dù xác suất của những nghịch lý này dường như là rất nhỏ, nhưng cho đến khi nhận được ước tính của họ, mối lo ngại về việc bỏ phiếu ưu tiên vẫn còn.

Hơn nữa, định lý bất khả thi của Arrow [28,29] và định lý Gibbard–Satterthwaite [30] chứng minh rằng bất kỳ hệ thống bỏ phiếu hữu ích nào cho một người chiến thắng dựa trên xếp hạng ưu tiên đều có xu hướng bị thao túng. Định lý Gibbard–Satterthwaite đã chỉ ra rằng bất kỳ phương pháp bỏ phiếu có thứ hạng nào không phải là độc tài đều dễ bị bỏ phiếu chiến thuật (Tactical Voting).

Hệ thống bỏ phiếu chính [20] là hệ thống bỏ phiếu cho phép một cử tri đánh giá hoặc xếp hạng độc lập cho mỗi ứng cử viên trong số ít nhất hai cấp độ phê duyệt. Hệ thống chính đơn giản nhất có thể là bỏ phiếu phê duyệt, chỉ cho phép hai hạng "được phê duyệt" hoặc "không được phê duyệt".

Theo [20], dưới bất kỳ hệ thống chính nào, nếu một ứng cử viên được cho điểm tối đa vì lý do chiến lược thì cử tri vẫn có thể cho điểm đó cho tất cả các ứng cử viên mà họ xếp hạng cao hơn. Nó chân thành hơn và nếu có bất kỳ tác dụng nào, nó sẽ góp phần vào chiến thắng của một ứng cử viên được cử tri ưa thích hơn là lựa chọn chiến lược của họ. Các hệ thống chính được coi là ưu việt không kém so với các hệ thống đa số theo cả bỏ phiếu chiến lược và chân thành.

Bỏ phiếu phê duyệt (AV) là một phương thức bỏ phiếu cho phép cử tri phê duyệ bất kỳ số lượng ứng cử viên nào [31]. Người chiến thắng là (các) ứng cử viên được chọn bởi số lượng cử tri lớn nhất. Bỏ phiếu phê duyệt thường được thảo luận nhiều nhất trong bối cảnh cuộc bầu cử chỉ có một người chiến thắng, nhưng các biến thể sử dụng hình thức bỏ phiếu phê duyệt cũng có thể được áp dụng cho các cuộc bầu cử nhiều người chiến thắng (nói chung).

AV có một số ưu điểm [32]:

- Sự đơn giản;
- Quy trình bỏ phiếu thực tế nhanh chóng và dễ dàng;
- Kết quả dễ hiểu: một danh sách đơn giản về các ứng cử viên cùng với số phiếu họ nhận được;
- Có xu hướng chọn những ứng cử viên có thể đánh bại tất cả các đối thủ trực tiếp;

- Có xu hướng chọn những người chiến thắng ôn hòa hơn;
- Các ứng cử viên thay thế có được một biện pháp hỗ trợ chính xác hơn;
- Nó miễn nhiễm với Push-Over[6] và Burying[7].

Theo AV, cử tri có thể quyết định về ứng cử viên sẽ bỏ phiếu theo 2 cách sau [33]:

- Họ chia tất cả các ứng cử viên thành hai nhóm: những người họ phê duyệt và không phê duyệt. Không có sự khác biệt giữa các ứng viên trong mỗi nhóm (không ai vượt trội hơn ai trong nhóm). Bỏ phiếu như vậy được gọi là lưỡng phân (Dichotomous).
- Họ có một số danh sách ưu tiên *P* và bình chọn theo danh sách này.

Không có phân tích đầy đủ về việc bỏ phiếu chiến lược theo AV. Hầu hết các phân tích AV tồn tại dựa trên một giả định rằng sự ưa thích của cử tri chỉ đơn giản là lưỡng phân. Tuy nhiên, bỏ phiếu lưỡng phân và bỏ phiếu theo một danh sách ưu tiên riêng có những tính chất khá khác nhau. Tính phức tạp của phân tích AV được xác định bởi tập hợp các kết quả khá lớn (lớn hơn kết quả bỏ phiếu ưu tiên) [34].

Có một số biến thể AV. Được biết đến nhiều nhất là bỏ phiếu chấp thuận sự hài lòng và bỏ phiếu Có-Không.

Bỏ phiếu chấp thuận sự hài lòng (SAV) [35] là một hệ thống bỏ phiếu áp dụng cho các cuộc bầu cử nhiều người chiến thắng. Nó sử dụng một lá phiếu chấp thuận, theo đó cử tri có thể phê duyệt bao nhiêu ứng cử viên tùy thích (không có thứ hạng). Điểm hài lòng của cử tri là một phần nhỏ trong số các ứng cử viên được chấp thuận của họ được bầu. Nếu *k* ứng cử viên được bầu, SAV chọn tập hợp *k* ứng cử viên đạt tối đa tổng điểm hài lòng của tất cả các cử tri.

Trong **bỏ phiếu Có-Không**, mỗi cử tri có thể bỏ phiếu "có", bỏ phiếu trắng hoặc bỏ phiếu "không", kết quả là "có" hoặc "không" và tất cả các cử tri đóng vai trò hoán đổi cho nhau. Có nhiều quy tắc xác định kết quả bầu cử: quy tắc đa số tuyệt đối, quy tắc đa số tuyệt đối đủ điều kiện, quy tắc đa số đơn giản (hoặc "tương đối"), bỏ phiếu sử dụng tỷ lệ và hạn ngạch chênh lệch.

4.6.2. Sơ đồ bỏ phiếu cho hệ thống ngân quỹ

Phân tích cho thấy không có hệ thống bỏ phiếu nào đáp ứng tất cả các tiêu chí: trong khi một số trong số chúng không đáp ứng tiêu chí IIA và Condorcet, những hệ thống khác không đáp ứng được thuộc tính Pareto hoặc tính đơn điệu, v.v.

[6]Push-Over (còn được gọi là bỏ phiếu linh tinh) là một kiểu bỏ phiếu chiến thuật, trong đó một cử tri xếp một lựa chọn thay thế yếu kém cao hơn, nhưng không phải với hy vọng sẽ được bầu.

[7]Burying là một kiểu bỏ phiếu chiến thuật, trong đó một cử tri xếp hạng một cách chân thành một phương án thay thế thấp hơn với hy vọng đánh bại nó.

Cũng không có hệ thống bỏ phiếu nào hoàn toàn miễn nhiễm với bỏ phiếu chiến lược. Hệ thống bỏ phiếu chính được coi là ít bị tổn thương hơn đối với bỏ phiếu chiến lược so với các hệ thống đa số và ưu tiên [20].

Bỏ phiếu ưu tiên xuất hiện trái ngược với bỏ phiếu đa số và cho phép cử tri thể hiện sự ưa thích của mình một cách chính xác hơn. Tuy nhiên, việc phân tích các hệ thống bỏ phiếu ưu tiên đã cho thấy chúng có một số nghịch lý và rất dễ bị ảnh hưởng bởi bỏ phiếu chiến lược và chế độ độc tài.

AV có một số lợi thế so với ưu tiên: tính đơn giản, xu hướng bầu chọn người chiến thắng vừa phải hơn, biện pháp hỗ trợ chính xác hơn cho các ứng cử viên thay thế, v.v. Không có lý do lớn để sử dụng bỏ phiếu phạm vi vì nó phức tạp, nhưng thực tế là các thuộc tính tương tự như AV. Hơn nữa, hệ thống ngân quỹ (quản trị) Crypto được biết đến nhiều nhất sử dụng biến thể của AV như bỏ phiếu Có-Không-Bỏ phiếu trắng: Dash [6], The DAO [7], Fermat [36], v.v. Do đó, một số tuỳ chọn bỏ phiếu chấp thuận là giải pháp phù hợp nhất cho hệ thống ngân quỹ ETC.

Chúng tôi cũng đề xuất sử dụng bỏ phiếu Có-Không-Bỏ phiếu trắng, vì vậy trong mô hình của chúng tôi, mỗi cử tri có thể bỏ phiếu "có", "không" hoặc "bỏ phiếu trắng". Bên cạnh đó, chúng tôi thực hiện quyền bỏ phiếu theo tỷ trọng số tiền đặt cọc (quyền biểu quyết tỷ lệ thuận với số tiền mà cử tri đặt cọc). Giống như trong Dash, kết quả bầu cử được xác định bằng cách sử dụng hạn ngạch chênh lệch: phương án thay thế đánh bại nguyên trạng nếu số phiếu "có" vượt quá số phiếu "không" ít nhất một số tuyệt đối được chỉ định hoặc hạn ngạch chênh lệch d.

Cuối cùng, sự khác biệt quan trọng giữa hệ thống bỏ phiếu của chúng tôi và bỏ phiếu Có-Không cổ điển là trong mô hình của chúng tôi (và trong các hệ thống bỏ phiếu ngân quỹ Crypto khác), số người chiến thắng linh động và giới hạn bởi phần thưởng của ngân quỹ tài trợ. Thực tế, con số này phụ thuộc vào số Coin được phân bổ cho ngân quỹ và số tiền theo yêu cầu của đề xuất chiến thắng. Rõ ràng, các điều kiện như vậy cần được tính đến trong phân tích chính thức của hệ thống bỏ phiếu. Chúng tôi đề xuất một mô hình bỏ phiếu chính thức mới xem xét tất cả các sửa đổi đã đề cập là **Bỏ phiếu theo ngưỡng mờ** (FTV-Fuzzy Threshold Voting). Phụ lục A bao gồm mô tả và phân tích của mô hình được đề xuất.

4.7. Gánh nặng tính toán và lưu trữ

Nó trở nên rất quan trọng đối với hệ thống đã phát triển để ước tính chi phí tính toán được giới thiệu. Trong phần này, chúng tôi chỉ ra rằng hệ thống được đề xuất không có tác động đáng kể đến hiệu suất chung của ETC.

Trước hết, chúng ta nên đề cập rằng tất cả các giao dịch ECTS đều có mức độ phức tạp tính toán hợp lý (hoặc mức tiêu thụ phí Gas nếu nó được triển khai dưới

dạng hợp đồng thông minh). Chúng có thể được so sánh với các giao dịch chuyển tiền đơn giản trong Ethereum.

Có một số loại giao dịch:

1. Deposit / RevokeDeposit - loại giao dịch này dự kiến sẽ không quá thường xuyên. Sau khi một bên liên quan đặt cọc, họ có thể tham gia vào thủ tục bỏ phiếu cho đến khi bị thu hồi, vì vậy họ không cần phải thực hiện việc này trong mỗi Epoch tài trợ.
2. Delegate / RevokeDelegate - loại giao dịch này được cho là sẽ hiếm. Sau khi một cử tri quyết định về việc ủy quyền, họ không cần phải gửi lại giao dịch ủy quyền trong mỗi Epoch tài trợ.
3. Phiếu đề xuất - một giao dịch đặc biệt để đệ trình đề xuất dự án. Một số đề xuất mới được mong đợi trong mỗi Epoch tài trợ. Tuy nhiên, từ kinh nghiệm của các Crypto khác, chúng tôi không chắc số lượng đề xuất mới sẽ nhiều hơn vài chục.
4. Cam kết / Phiếu biểu quyết - đây là những giao dịch thường xuyên nhất vì mỗi cử tri sẽ gửi một cam kết và phiếu biểu quyết tương ứng trong mỗi Epoch tài trợ.
5. Thanh toán - giao dịch một lần vào cuối mỗi Epoch để thanh toán tiền cho người được chấp nhận các đề xuất.

Có thể thấy rằng gánh nặng tính toán phụ thuộc rất nhiều vào số cử tri. Ở phần trước, chúng ta đã biết tập hợp các cử tri là tự cân bằng, vì vậy mức độ tham gia bình thường của cử tri được mong đợi trong quá trình hoạt động bình thường. Do có một hạn chế kinh tế đối với tổng số tiền đặt cọc, số lượng cử tri dự kiến tối đa được ước tính là *MENV* = 8886 (xem phần 4.5.1. “Số lượng cử tri dự kiến”). Giả sử chúng ta có 8886 cử tri và 100 đề xuất (khó có thể có số lượng lớn đề xuất như vậy trong thế giới thực, nhưng cần phải ước tính tổng chi phí tính toán cao nhất). Do mỗi cử tri chỉ có thể gửi một giao dịch đặt cọc và ủy quyền cho mỗi Epoch, chúng ta có thể ước tính số lượng giao dịch tối đa cho một Epoch tài trợ (*MNT*):

$$MNT = 100 + 8886 \cdot 4 = 35644 \ (Giao\ dịch).$$

Do Ethereum Classic có thể xử lý trung bình lên đến 15 TPS, tương đương khoảng $38{,}8 \cdot 10^6$ giao dịch trên mỗi Epoch tài trợ, chúng ta có thể tính toán chi phí giao dịch (*TO*) được giới thiệu bởi hệ thống ngân quỹ:

$$TO_{\%} = \frac{35644}{38.8 \cdot 10^6} \cdot 100\% = 0.09\%.$$

Vì vậy, có thể thấy rằng ngay cả với tải tính toán được đánh giá quá cao, tác động của hệ thống ngân quỹ đối với hiệu suất Ethereum là không đáng kể.

4.8. Các hướng phát triển thêm

Trong quá trình phát triển ECTS, chúng tôi đã tính đến kinh nghiệm của Hệ thống quản trị Dash (DGS), hệ thống được triển khai thực tế tiên tiến nhất thuộc loại như vậy, cung cấp hiệu quả nguồn vốn cho nhóm Dash kể từ tháng 9 năm 2015.

Đối với các bước nghiên cứu tiếp theo, chúng tôi dự định sẽ xem xét kinh nghiệm đã thu được về các chi tiết bỏ phiếu cụ thể để tạo thêm động lực để đạt được sự đồng thuận về các đề xuất ngân quỹ. Bên cạnh đó, chúng tôi làm việc trên giao thức bỏ phiếu mật mã tiên tiến để cải thiện thêm các thuộc tính lý thuyết của sơ đồ bỏ phiếu (có thể hữu ích trong tương lai, khi hệ thống đạt đến mức độ trưởng thành cao).

5. Tổng quan về các cuộc tấn công

Phần này cung cấp một cái nhìn tổng quan ngắn gọn về các cuộc tấn công tiềm ẩn vào hệ thống ngân quỹ được đề xuất. Như đã đề cập ở trên, phiên bản hiện tại của báo cáo không cung cấp phân tích chính thức chặt chẽ, chứng minh lý thuyết trò chơi, v.v., để lại điều đó cho các giai đoạn nghiên cứu tiếp theo.

Các cuộc tấn công vào hệ thống ngân quỹ có thể có các mục tiêu sau:

1. Để có toàn quyền hoặc một phần quyền kiểm soát đối với tiền trong ngân quỹ để sở hữu chúng (ăn cắp tiền trong ngân quỹ).
2. Để chặn hoạt động ngân quỹ để ngăn chặn việc tài trợ cho sự phát triển Crypto (tấn công DoS).

Rõ ràng, nếu kẻ tấn công có toàn quyền kiểm soát và đánh cắp tiền trong ngân quỹ, họ sẽ chặn hoạt động của ngân quỹ, vì vậy việc thực hiện kiểu tấn công đầu tiên dẫn đến việc tự động thực hiện kiểu tấn công thứ hai.

Nhưng các phương pháp tiếp cận có thể tồn tại trong đó kẻ tấn công không thể ăn cắp ngân quỹ tài trợ, nhưng vì một số mục đích cố gắng chặn tài trợ Crypto.

5.1. Kiểm soát tiền trong ngân quỹ

5.1.1. Tấn công trực tiếp vào thủ tục bỏ phiếu

Tất cả thông tin ngân quỹ đều được đưa vào Blockchain, do đó, việc làm giả quy trình lựa chọn người chiến thắng (xem 4.2) phải phá vỡ giao thức đồng thuận Crypto cơ bản.

5.1.2. Ảnh hưởng đến quá trình bỏ phiếu

Các đề xuất và danh sách cử tri là cố định và không thể thay đổi trong Epoch ngân quỹ (xem phần 4.4.1). So với các hệ thống bỏ phiếu khác, hệ thống được

chọn (hệ thống bỏ phiếu ngưỡng mờ) có:

- Đặc tính rất tốt để bày tỏ ý kiến trung thực của đa số (tối đa hóa mức độ hài lòng chung);
- Kẻ tấn công ít thao túng các chiến lược hơn (không có trường hợp nghịch lý nào xảy ra, chẳng hạn như trong bỏ phiếu ưu tiên);
- Dễ hiểu mà không cần tìm hiểu sâu về tài liệu bỏ phiếu chuyên ngành (để biết thêm chi tiết xem phần 4.6).

Các lá phiếu được cam kết bí mật và được mở khi mọi cử tri đã thực hiện cam kết của họ. Điều đó hạn chế đáng kể chiến lược của những kẻ tấn công. Do đó, kế hoạch bỏ phiếu là minh bạch và dễ kiểm chứng. Một số tính chất của sơ đồ được chính thức phân tích và chứng minh trong Phụ lục A.

5.1.3. Kiểm soát "tài khoản ngân quỹ"

Ngân quỹ được đề xuất không có tài khoản cụ thể cho việc tích lũy và phân phối lại quỹ để thực hiện đồng thuận cốt lõi. Tiền được gửi trực tiếp đến tài khoản của chủ sở hữu đề xuất. Để tổ chức một cuộc tấn công kiểu này thành công, cần phải kiểm soát nhiều tài khoản, điều này phá vỡ Crypto cơ bản.

5.1.4. Hối lộ bộ phận có ảnh hưởng của cử tri

Kẻ tấn công và những người tham gia hối lộ phải có đủ số lượng cổ phần và các cuộc tấn công thành công dẫn đến giảm tỷ giá trao đổi của Crypto. Do bị khóa tiền đặt cọc trong 3 tháng (xem phần 2.4), cuộc tấn công dự kiến sẽ có ảnh hưởng tiêu cực đến cổ phần đối địch (đối với một số loại tiền Fiat có giá trị không đổi).

Ngân sách ngân quỹ hàng tháng thấp hơn đáng kể so với số tiền cần thiết để kiểm soát nó, vì vậy tổn thất dự kiến cao hơn lợi nhuận của kẻ tấn công. Có một động cơ kinh tế cho một bên liên quan hợp lý trung thực tham gia vào ngân quỹ bỏ phiếu giúp có đủ số lượng cử tri trung thực đủ lớn (xem phần 4.5.3).

5.1.5. Tấn công 55%

Để có quyền kiểm soát được đảm bảo đối với quá trình bỏ phiếu, kẻ tấn công cần có trên 55% quyền biểu quyết, hiện được dự đoán là khoảng 4,4% tổng số cổ phần trong hệ thống. Một cuộc tấn công thành công làm giảm tỷ giá trao đổi, do đó, tổn thất dự kiến của các khoản tiền đặt cọc độc hại bị khóa cao hơn lợi nhuận của kẻ tấn công (xem phần 4.5.2 và 5.1.4).

5.2. Ngăn chặn hoạt động của ngân quỹ

5.2.1. Đưa ra số lượng lớn các đề xuất

Mỗi đề xuất có một chi phí cố định (5 Coin trong đề xuất này). Do đó, để tấn công

hệ thống, kẻ tấn công phải đốt số lượng cổ phần tương ứng với số lượng đề xuất của họ. Hơn nữa, phần mềm ứng dụng khách bỏ phiếu có thể dễ dàng sắp xếp các yêu cầu theo nguồn tài trợ được yêu cầu, do đó, các đề xuất gian lận sẽ không ảnh hưởng đến các đề xuất trung thực (hoặc một cuộc tấn công DoS sẽ yêu cầu một ngân sách tương đương với một cuộc tấn công tốn kém hơn để giành quyền kiểm soát tất cả số tiền trong ngân quỹ).

5.2.2. Tạo quá nhiều tài khoản bỏ phiếu

Để trở thành cử tri, cần đặt cọc một lượng cổ phần (500 Coin trong đề xuất này). Xem xét mức dự trữ đáng kể về hiệu suất sơ đồ bỏ phiếu, số tiền đặt cọc cần thiết cho cuộc tấn công này cao hơn so với việc giành quyền kiểm soát tất cả số tiền trong ngân quỹ.

5.2.3. Tạo ra nhiều cam kết và mở từ mỗi tài khoản bỏ phiếu

Chỉ có một cam kết cho mỗi cử tri được đưa vào Blockchain (tất cả phần còn lại đều bị các thợ đào loại bỏ). Chỉ một lần mở tương ứng với cam kết mới được đưa vào Blockchain.

Do đó, kiến trúc ngân quỹ chỉ chấp nhận một cam kết và mở cho mỗi tài khoản bỏ phiếu.

Cùng với điều này, có một số lượng giao dịch ủy quyền hạn chế (một giao dịch trên mỗi Epoch) cũng ngăn kẻ tấn công thực hiện tấn công thành công.

6. Kết luận

Hệ thống Ngân quỹ Ethereum Classic (ECTS) được đề xuất nhằm tạo ra quy trình phi tập trung được kiểm soát bởi cộng đồng để tài trợ cho sự phát triển và cải tiến Crypto hơn nữa.

ECTS có khả năng tính toán được chấp nhận và tải không gian Blockchain cho hệ thống, không có ảnh hưởng đáng kể đến hiệu suất ETC.

Nguồn vốn phát triển được cung cấp thông qua việc chuyển tiền thường xuyên đến các tài khoản được liên kết với các đề xuất được cộng đồng phê duyệt nhằm giải quyết các nhiệm vụ cải tiến và bảo trì Crypto.

Hệ thống mở và có thể xác minh, vì vậy bất kỳ ai cũng có thể cung cấp đề xuất và theo dõi bất kỳ quyết định nào được đưa ra trong hệ thống, cho đến toàn bộ lịch sử hoạt động của ECTS.

Lựa chọn người chiến thắng để tài trợ trong số tất cả các đề xuất được thực hiện bởi các thành viên cộng đồng ETC, người đã khóa cổ phần của mình và khuyến khích tham gia vào hoạt động ngân quỹ trung thực.

Sơ đồ bỏ phiếu được chọn cho ECTS (bỏ phiếu ngưỡng mờ - FTV) có ưu điểm

hơn các sơ đồ bỏ phiếu khác. Nó cũng được giới thiệu mô hình toán học chính thức của FTV và một số tính chất của nó đã được chứng minh.

Các cử tri trong ECTS có khả năng ủy quyền cho những người tham gia đủ tiêu chuẩn đáng tin cậy (những người cũng có động lực riêng).

Phân tích ban đầu không tìm thấy cuộc tấn công nào vào ECTS cho phép kẻ tấn công tăng cổ phần của họ (một kẻ tấn công làm mất tiền của họ ngay cả trong trường hợp rất khó xảy ra là có toàn quyền kiểm soát ngân quỹ hệ thống). Những người tham gia cộng đồng trung thực luôn có khả năng can thiệp để ngăn chặn các cuộc tấn công trong tương lai.

Các phân tích chính thức chi tiết và các bằng chứng được lên kế hoạch cho các giai đoạn tiếp theo của nghiên cứu.

Chúng tôi kỳ vọng rằng việc triển khai ECTS sẽ tăng tính ổn định của ETC và triển vọng trong tương lai, mang lại lợi ích bổ sung cho cả các bên liên quan và thợ đào từ một hệ thống ổn định hơn và có thể dự đoán được.

Hãy nhớ rằng tất cả các tham số hệ thống đã giới thiệu (chẳng hạn như số lượng Coin cho ngân quỹ tài trợ hoặc số tiền thưởng của cử tri) cũng như các giải pháp kiến trúc không được đặt trong đá và chủ đề để phân tích và thảo luận thêm với các thành viên cộng đồng.

7. Tài liệu tham khảo

[1] Satoshi Nakamoto. Bitcoin: Hệ thống tiền mặt điện tử ngang hàng.

[2] Vốn hóa thị trường Crypto: http://coinmarketcap.com/

[3] Tập đoàn Blockchain R3CEV: trạng thái hiện tại.
https://www.linkedin.com/pulse/r3cev-Blockchain-consortium-present-state-carlo-rw-de-meijer.

[4] Chính phủ Nga đang thử nghiệm Blockchain để lưu trữ tài liệu.
http://www.coindesk.com/the-nga-Government-is-testing-Blockchain-for-document-storage /.

[5] Công cụ theo dõi Block: Chính phủ tin tưởng vào Blockchain.
http://fintechranking.com/2017/02/04/blockchain-tracker-Government-trust-inblockchain/.

[6] E. Duffield, D. Diaz. Dash: Một loại Crypto trung tâm riêng tư .
https://www.dash.org/wp- content /uploads/2015/04 /Dash-WhitepaperV1.pdf

[7] Báo cáo chính thức: TỔ CHỨC TỰ ĐỘNG PHÂN TÍCH ĐỂ TỰ ĐỘNG HÓA QUẢN TRỊ.

[8] D. Williams. DFINITY "Hệ thống thần kinh Blockchain". https://medium.com/dfinity-network-blog/the-dfinity-Blockchain-neuro-system-a5dd1783288e # .pwji0ajtf.

[9] White Paper Ethereum https://github.com/ethereum/wiki/wiki/White-Paper.

[10] Gavin Wood. Ethereum: Sổ cái giao dịch chung phi tập trung an toàn.

[11] Hệ thống quản trị Dash: Phân tích và đề xuất cải tiến. https://iohk.io/research/papers/dash-management-system-analysis-and-suggest-for-improvement/.

[12] Hệ thống quản trị Dash: Phản hồi của nhóm chính Dash đối với báo cáo "Hệ thống quản trị Dash: Phân tích và đề xuất cải tiến" https://www.dash.org/wp-content/ uploads/2016/12/ Dash-Govern-System-Dash-Core-Team-Response.pdf.

[13] Gilles Brassard, David Chaum, và Claude Crepeau, Bằng chứng tiết lộ kiến thức tối thiểu, Tạp chí Khoa học Máy tính và Hệ thống, tập. 37, trang 156–189, 1988.

[14] Stephanie Delaune, Steve Kremer và Mark Ryan. Xác minh các thuộc tính loại quyền riêng tư của các giao thức bỏ phiếu điện tử. Tạp chí An ninh Máy tính, 17 (4): 435–487, 2009.

[15] LM Goodman. Tezos - một sổ cái Crypto tự sửa đổi. White Paper.

[16] LM Goodman. Tezos: Báo cáo định vị Crypto tự sửa đổi.

[17] Svetlana Z. Lowry, Poorvi L. Vora. Các thuộc tính mong muốn của hệ thống bỏ phiếu. http://ws680.nist.gov/publication/get_pdf.cfm? pub id = 903961.

[18] Hệ thống đa số / theo đa số. Chế độ truy cập: https://www.mtholyoke.edu/acad/polit/damy/BeginnningReading/plurality.htm.

[19] Steven Hill. "Bỏ phiếu tiêu hủy tức thì ". Chế độ truy cập: https://static.newamerica.org/attachments/4119-instant-runoff-voting/NAF_10big_Ideas_9.677a9863789b4a23bc356ed7940b5cb8.pdf.

[20] Claude Hillinger. "Trường hợp bỏ phiếu theo chủ nghĩa bất tài (Utilitarian)".

[21] Thủ tục bỏ phiếu và tính chất của chúng.

[22] Eric Erdmann. "Điểm mạnh và mặt hạn chế của các phương pháp bỏ phiếu cho các cuộc bầu cử chính trị".

[23] Peter Emerson. "Số lượng Borda ban đầu và bỏ phiếu một phần".

[24] Phiếu bầu có thể chuyển nhượng một lần http://www.electoral-reform.org.uk/single-transferable-vote.

[25] Schulze, Markus. "Một phương pháp bầu cử người chiến thắng đơn nhất mới, độc lập với bản sao, đối xứng đảo ngược và Condorcet nhất quán". Lựa chọn xã hội

và Phúc lợi 36,2 (2011): 267-303.

[26] Ronald L. Rivest và Emily Shen. “Hệ thống bỏ phiếu ưu tiên cho một người chiến thắng tối ưu Dựa trên Lý thuyết trò chơi ”.

[27] Peter C. Fishburn và Steven J. Brams. “Nghịch lý của Bỏ phiếu Ưu tiên”.

[28] Arrow, Kenneth J. “Khó khăn trong khái niệm phúc lợi xã hội”.

[29] Arrow, Kenneth J. “Sổ tay về Lựa chọn Xã hội và Phúc lợi”.

[30] Andrew C. Eggers. “Một Chứng minh Đơn giản của Định lý Gibbard-Satterthwaite”.

[31] Brams, Steven, Fishburn, Peter. "Biểu quyết Phê duyệt".

[32] Https://electology.org/approval-voting.

[33] Niemi, R. (1984). Vấn đề về Hành vi Chiến lược trong Bỏ phiếu Phê duyệt. Tạp chí Khoa học Chính trị Mỹ, 78 (4), 952-958.doi:10.2307/1955800.

[34] Steven J. Brams, M. Remzi Sanver. “Các chiến lược quan trọng đang được bỏ phiếu phê duyệt: Ai được cai trị và bị cai trị”.

[35] Steven J. Brams, D. Marc Kilgour. “Bỏ phiếu phê duyệt sự hài lòng”.

[36] Fermat, Internet của con người và nền kinh tế giữa con người với con người. https://hackernoon.com/fermat-the-internet-of-people-and-the-person-to-person-economy ce933865a0b0#.e07m1vd9b.

[37] ECIP-1017. Chính sách tiền tệ và sửa đổi cuối cùng đối với lịch trình phát thải Ethereum Classic.
https://github.com/ethereumproject/ECIPs/blob/master/ECIPs/ECIP-1017.md

[38] Tuyên bố chung về Chính sách tiền tệ của Ethereum Classic.
https://iohk.io/blog/ethereum-classic/a-Joint-statement-on-ethereum-classicics-money-policy/.

A. Phụ lục. Mô hình bỏ phiếu - Bỏ phiếu theo ngưỡng mờ

A.1. Giới thiệu

Trong tài liệu này, chúng tôi giới thiệu một mô hình toán học cho hệ thống bỏ phiếu được sử dụng chủ yếu trong Crypto [1]. Chúng tôi gọi nó là Bỏ phiếu theo ngưỡng mờ (FTV - Fuzzy Threshold Voting). Từ “mờ” nhấn mạnh rằng tập hợp những người chiến thắng trong một số trường hợp có thể chứa những ứng viên có điểm thấp hơn và không thể chứa những ứng viên có điểm cao hơn. Tính chất này là kết quả của thực tế là kết quả bỏ phiếu không chỉ phụ thuộc vào điểm số của các ứng cử viên (tức là thứ hạng của họ trong lá phiếu của cử tri) mà còn phụ thuộc vào các yếu tố khác - ngân sách của các dự án tương ứng (thực tế là các dự án là ứng cử viên). Sự khác biệt

chính giữa mô hình bỏ phiếu của chúng tôi so với AV (cũng như các mô hình bỏ phiếu khác) [2 - 11]. Một mặt, đây cũng là vấn đề chính của mô hình FTV, bởi vì tất cả các phân tích lý thuyết hiện có cho các mô hình bỏ phiếu đều thất bại trong trường hợp này. Mặt khác, kiến thức về ngân sách của các dự án cung cấp cho cử tri một số thông tin bổ sung giúp họ đưa ra quyết định cân nhắc hơn trong khi bỏ phiếu hoặc để hình thành các lựa chọn chính xác hơn.

Mô hình bỏ phiếu FTV được đề xuất được coi là một sự tổng quát của mô hình bỏ phiếu Có-Không với các tính năng mở rộng.

Sự phụ thuộc hai yếu tố của thủ tục bỏ phiếu và ngưỡng mờ của nó làm cho việc phân tích lý thuyết của mô hình này trở nên phức tạp hơn nhiều. Nhưng mặc dù vậy, chúng tôi vẫn thu được một số kết quả có thể được coi là loại suy của các kết quả chính đối với mô hình AV cổ điển [12, 13].

Trong phần này, ngoài việc xây dựng một mô hình toán học thích hợp cho hệ thống bỏ phiếu mới, chúng tôi cũng phân tích các tính chất chính của nó, chẳng hạn như tính tối ưu (theo một nghĩa nào đó) của thủ tục bỏ phiếu, sự tồn tại của các chiến lược có thể chấp nhận, lợi thế của việc bỏ phiếu chân thành và sự cần thiết bỏ phiếu kín. Chúng tôi cũng chỉ ra rằng một trong những lợi thế không thể nghi ngờ của mô hình này là quy tắc Condorcet. Nó có nghĩa là người chiến thắng Condorcet, hoặc người lãnh đạo rõ ràng về cuộc bỏ phiếu, luôn thuộc về nhóm người chiến thắng (ngoại trừ, có thể trong một số trường hợp không thể xảy ra của cuộc bỏ phiếu hòa cụ thể).

A.2. Định nghĩa mô hình FTV

Trong phần tiếp theo, chúng tôi sẽ chủ yếu sử dụng các thuật ngữ và định nghĩa từ [12]. Chúng tôi ký hiệu I là tập hữu hạn *các cử tri* và X là tập hữu hạn *các dự án* (*phương án*, *ứng cử viên*) và với $n \in N$: $L^{(n)} = \{-n, -(n - 1), \dots, -1, 0, 1; \dots, n - 1, n\}$. Tập hợp $L^{(n)}$ chứa tất cả các thứ hạng mà cử tri có thể đưa ra cho các dự án. Chúng tôi giả sử $\#I \geq 2$ và $\#X \geq 2$. Mọi cử tri $i \in I$ đều có sự ưa thích X được biểu thị bằng một hàm tiện ích $u_i : X \to R$. Trong một số trường hợp cụ thể, chúng tôi sẽ giả định rằng $u_i : X \to L^{(n)}$, tức là tập hợp các sự ưa thích có thể có trùng với tập hợp các xếp hạng của dự án. Ví dụ, Mệnh đề (A.2) cho thấy tính tối ưu của thủ tục bỏ phiếu ở một khía cạnh nào đó được chứng minh chỉ với những hạn chế như vậy. Nhưng những hạn chế này khá phù hợp và gần với thực tế hơn nhiều so với mô hình SAV [14] hoặc trong mô hình PAV (Proportional AV) [15], bởi vì mô hình của chúng tôi nghiêm túc tính đến mức độ ưa thích của tất cả các cử tri.

Cho hai dự án $x, y \in X$, cử tri i tìm thấy x ít nhất *tốt bằng* y nếu $u_i(x) \leq u_i(y)$. Một dự án x là cao trong u_i nếu với mọi $y \in X$ thì $u_i(x) \geq u_i(y)$. Chúng ta nói rằng x thấp trong u_i nếu với mọi $y \in X$ thì $u_i(x) \leq u_i(y)$. Chúng ta gọi là u_i là *trống* bất cứ khi nào i

không quan tâm đến tất cả các lựa chọn thay thế, tức là $u_i(x) \geq u_i(y)$ với mọi $x, y \in X$. Nếu u_i là trống thì mọi dự án đều có giá trị u_i thấp và cao. Nếu u_i không trống thì các dự án có u_i cao hơn và những dự án thấp hơn trong các tập hợp rời rạc trong biểu mẫu giao diện người dùng. Chúng tôi giả định rằng mỗi dự án mà cử tri thích có một số "xếp hạng" dương trong sự ưa thích của họ và mỗi dự án mà cử tri không thích có một số "xếp hạng" âm.

Một *lá phiếu* B_i của cử tri i là một phân vùng bất kỳ của tập X trên $2n + 1$ tập con $H_i^{(l)}$, $l \in L^{(n)}$, thỏa mãn các điều kiện sau:

1. $H_i^{(l)} \cap H_i^{(k)} = \emptyset$ với bất kỳ $l, k \in L^{(n)}$, $l \neq k$;
2. $U_{l \in S} H_i^{(l)} = X$.

Lưu ý rằng một hoặc nhiều tập con $H_i^{(l)}$, $l \in L^{(n)}$ có thể trống.

Ngay sau định nghĩa này, số lượng phiếu bầu có thể có (hoặc số chiến lược bỏ phiếu) cho mỗi cử tri bằng $(\#X)^{2n+1}$.

Khi cử tri i, với $i \in I$, nộp lá phiếu $B_i = (H_i^{(-n)}, \ldots, H_i^{(0)}, \ldots, H_i^{(n)})$, chúng ta nói *i phê duyệt* các dự án trong $H_i^{(l)}$, trong đó $l > 0$, *với điểm (dương) l*, *bỏ phiếu trắng* đối với các dự án ở $H_i^{(0)}$ và *từ chối* các dự án ở $H_i^{(l)}$, trong đó $l < 0$, *với điểm (âm) l*.

Đối với mỗi cử tri i, với $i \in I$, người nộp lá phiếu $B_i = (H_i^{(-n)}, \ldots, H_i^{(0)}, \ldots, H_i^{(n)})$, chúng tôi xác định *hàm score* $s_i : X \to L$, trong đó $s_i(x) = l$ nếu $x \in H_i^{(l)}$.

Mô hình FTV khá giống với mô hình Bỏ phiếu phê duyệt (AV), nhưng cũng có một số khác biệt cơ bản. Sự khác biệt đầu tiên là trong định nghĩa của một lá phiếu. Trong mô hình AV, lá phiếu B_i chỉ bao gồm các ứng cử viên được chấp thuận, tức là các ứng cử viên từ $H_i^{(l)}$ với l dương. Và tất cả các ứng cử viên này đều có cùng "xếp hạng" trong lá phiếu bất chấp sự ưa thích của cử tri. Chúng ta cũng có thể nói rằng trong mô hình AV $n = 1$ và $H_i^{(0)} = \emptyset$ với mỗi $i \in I$. Những khác biệt khác mà chúng ta sẽ thấy bên dưới trong định nghĩa của hàm score và trong định nghĩa của thủ tục bỏ phiếu.

Đối với mô hình AV, các hạn chế tự nhiên sau đây thường được thực hiện [12, 13] để hạn chế tập hợp các chiến lược bỏ phiếu mà một cử tri được cho là có thể sử dụng:

1. Người ta cho rằng cử tri sử dụng các chiến lược không được đánh giá cao thường được gọi là "*chiến lược có thể chấp nhận*" và có thể được đặc trưng như sau: nếu sở thích của cử tri là nghiêm ngặt, họ sẽ phê duyệt ứng cử viên ưa thích của mình, họ không phê duyệt ứng cử viên kém nhất và không có ràng buộc nào được áp đặt cho các ứng viên trung gian khác.
2. Hạn chế khác là *yêu cầu về sự chân thành*, quy định rằng khi cử tri phê

duyệt một ứng cử viên, họ cũng phê duyệt tất cả các ứng cử viên mà họ hoàn toàn thích ứng cử viên này.

Nhưng mô hình của chúng tôi khá khác so với AV. Chúng tôi sẽ không hạn chế các chiến lược theo cách tương tự, nhưng chúng tôi sẽ sử dụng một số định nghĩa về việc bỏ phiếu chân thành cho FTV. Hãy để cử tri i có một số sựa ưa thích nhất định về tập hợp X của tất cả các dự án.

Định nghĩa A.2.1. Cho $u_i : X \to L^{(n)}$. Chúng tôi nói rằng cử tri i *bỏ phiếu một cách chân thành* (theo nghĩa hẹp) nếu với bất kỳ $x \in X$ thì quyền bình đẳng diễn ra:

$$u_i(x) = \sum_{l \in L} l \cdot \delta(x, H_i^{(l)}),$$

trong đó

$$\delta(a, A) = \begin{cases} 1, & \text{if } a \in A \\ 0, & \text{otherwise.} \end{cases}$$

Định nghĩa A.2.2. Chúng ta nói rằng cử tri i *bỏ phiếu chân thành* (theo nghĩa rộng) *cho hai dự án* $x, y \in X$, nếu bất đẳng thức

$$u_i(x) > u_i(y)$$

liên quan đến bất đẳng thức $s_i(x) \geq s_i(y)$ (hoặc liên quan đến $x \in H_i^{(l)}$, $y \in H_i^{(j)}$) với $l \geq j$).

Chúng ta nói rằng cử tri i *bỏ phiếu chân thành* (theo nghĩa rộng) nếu họ bỏ phiếu chân thành cho bất kỳ $x, y \in X$.

Định nghĩa A.2.3. Chúng ta sẽ gọi tập $B = (B_i)$ với $i \in I$ của tất cả các lá phiếu là *một hồ sơ lá phiếu* và với mọi $i \in I$ xác định $B_{-i} := B \backslash B_i = (B_j)$ với $j \in I \backslash \{i\}$. Chúng ta sẽ viết $B = (B_i, B_{-i})$ bất cứ khi nào chúng ta muốn làm nổi bật sự phụ thuộc của B đối với lá phiếu thứ i. Chúng ta gọi B_{-i} là một *hồ sơ lá phiếu mà không có* i.

Định nghĩa A.2.4. Với một hồ sơ B, *điểm của dự án* $x \in X$ là

$$s(x, B) = \sum_{l \in L} l \cdot \#\{i \in I : x \in H_i^{(l)}\}.$$

Lưu ý rằng trong mô hình AV, điểm của ứng viên $x \in X$ được xác định là

$$s(x, B) = \#\{i \in I : x \in B_i\}.$$

- số phiếu bầu mà ứng cử viên x thuộc về.

Định nghĩa A.2.5. Với một hồ sơ B, chúng ta nói rằng dự án $x \in X$ là *ứng viên có thể chấp nhận được*, nếu

$$s(x, B) \geq 0{,}1 \cdot |I|.$$

Trong mô hình này, chỉ những ứng viên được chấp nhận mới có thể là người chiến thắng.

Định nghĩa A.2.6. Chúng ta đặt một giá trị dương M nào đó và sẽ gọi giá trị này là *ngân sách chung* (*Common Budget*) được cấp để thực hiện các dự án từ tập X.

Đối với mỗi dự án $x \in X$, chúng ta đặt một giá trị dương $m(x)$ là *ngân sách của dự án* x. Theo đó, chúng ta sẽ giả sử rằng $\forall x \in X : m(x) \leq M$.

Định nghĩa A.2.7. Chúng ta nói rằng một số tập hợp con $S \in X$ *làm cạn kiệt ngân sách chung* M nếu các điều kiện sau đây được giữ nguyên:

1. $\sum_{x \in S} m(x) \leq M$;
2. Nếu $S \neq X$ thì $\forall y \in X \setminus S : \sum_{x \in S} m(x) + m(y) > M$.

Cho một hồ sơ bỏ phiếu B, trong số tất cả các dự án (được chấp nhận) $X = \{x_i\}$ với $i \in I$, chúng ta phải chọn tập hợp *những người chiến thắng* (*những dự án chiến thắng*) $W(B) \in X$. Một mặt, những người chiến thắng phải là những dự án có điểm cao nhất; mặt khác, tập hợp những người chiến thắng phải sử dụng hết ngân sách chung M. Hạn chế thứ hai xác định thêm một sự khác biệt giữa các mô hình AV và FTV.

Định nghĩa A.2.8. Cho $\#X = k$ và cho một hồ sơ bỏ phiếu B, các trình tự

$$x_1, \ldots, x_k, x_i \in X, \tag{A1}$$

được tổ chức theo cách mà

$$s(x_1, B) \geq \ldots \geq s(x_k, B). \tag{A.2}$$

Tiếp theo, chúng tôi sẽ giả định rằng với một hồ sơ lá phiếu B, các điều kiện (A.1), (A.2) được giữ nguyên.

Định nghĩa A.2.9. (Thủ tục bỏ phiếu). Để xác định tập hợp $W(B) \in X$ của những người chiến thắng (dự án chiến thắng), chúng tôi sẽ sử dụng quy trình bỏ phiếu (lặp lại) sau:

1. $x_1 \in W(B)$; (A.3)
2. Cho $i = \underline{2, k} : x_i \in W(B) \Leftrightarrow \sum_{j=1}^{i-1} m(x_j)\delta(x_j, W(B)) + m(x_i) \leq M$.

Chúng tôi cần nhấn mạnh rằng thủ tục bỏ phiếu FTV (A.3) là điểm khác biệt chính của mô hình FTV so với mô hình AV, bởi vì trong trường hợp FTV, nhóm người chiến thắng không chỉ phụ thuộc vào "điểm số" của các ứng cử viên, mà còn phụ thuộc vào ngân sách của họ, và sự phụ thuộc sau này là rất cần thiết trong việc hình thành nhóm người chiến thắng. Sự phụ thuộc này kéo theo rất nhiều khó khăn trong phân tích lý thuyết của mô hình FTV. Sự khác biệt chính là có thể có hai dự án $x, y \in X$ sao cho dưới một hồ sơ B nào đó $s(x, B) > s(y, B)$ và $y \in W(B)$ nhưng $x \notin W(B)$. Tính năng này không thể chứng minh một số tuyên bố thường áp dụng cho các mô hình bỏ phiếu "cổ điển". Vì lý do này, đôi khi chúng tôi sẽ đơn giản hóa thủ tục bỏ phiếu để chứng minh các tuyên bố chính.

Định nghĩa A.2.10. (Thủ tục bỏ phiếu được đơn giản hóa). Để giữ (A.2), (A.1) theo một thủ tục bỏ phiếu đơn giản với một hồ sơ lá phiếu B,

$$W(B) = \{x_1, x_2, \ldots, x_t\},$$

trong đó

$$t = max\{l \geq 1 : \sum_{i=1}^{l} m(x_i) \leq M\}. \qquad (A.4)$$

Theo sự đơn giản hóa này, tập hợp các người chiến thắng $W(B)$ sao cho nếu $x_i \in W(B)$ với $i \geq 2$ thì $x_i \in W(B)$ với mọi $j = \underline{1, i - 1}$. Nhưng chúng ta nên lưu ý rằng ngay cả trong trường hợp này, ngưỡng vẫn còn mờ và số lượng người chiến thắng cũng vậy. Cũng lưu ý rằng thủ tục bỏ phiếu A.3 và A.4 giống hệt nhau khi và chỉ khi hồ sơ lá phiếu B sao cho đối với một số t $(1 \leq t \leq n)$: $\{x_1, ..., x_t\}$ làm cạn kiệt ngân sách chung M.

Bây giờ chứng minh một số tính chất quan trọng của thủ tục bỏ phiếu A.3 và A.4.

Đề xuất A.1. ***(i)*** *Theo thủ tục bỏ phiếu A.3 và A.4, người chiến thắng Condorcet (nếu tồn tại) luôn thuộc về nhóm người chiến thắng.*

(ii) *Quy trình bỏ phiếu A.3 và A.4 thỏa mãn quy tắc đơn điệu:*

- ***a.*** *Nếu $x \in W(B)$ và đối với một số hồ sơ $B^{\sim}$: $s(x, B^{\sim}) > s(x, B)$ và $s(y, B^{\sim}) = s(y, B)$ với mọi $y \in X \setminus \{x\}$ thì $x \in W(B^{\sim})$;*
- ***b.*** *Nếu $x \notin W(B)$ và đối với một số hồ sơ $B^{\sim}$: $s(x, B^{\sim}) < s(x, B)$ và $s(y, B^{\sim}) = s(y, B)$ với mọi $y \in X \setminus \{x\}$ thì $x \notin W(B^{\sim})$.*

Chứng minh. 1) Gọi $x \in X$ sao cho

$$\forall i \in I \quad \forall y \in X \setminus \{x\}: s_i(x) \geq s_i(y).$$

Sau đó đối với bất kỳ hồ sơ B và bất kỳ $y \in X \setminus \{x\}$

$$s(x, B) = \sum_{i \in I} s_i(x) \geq \sum_{i \in I} s_i(y) = s(y, B),$$

do đó $s(x, B) = max_{y \in X} s(y, B)$.

Theo Định nghĩa A.2.6, $m(x) \leq M$. Vậy theo thủ tục bỏ phiếu A.3 hoặc A.4 $x \in W(B)$ cho bất kỳ hồ sơ B. Câu lệnh đầu tiên được chứng minh.

2) Giả sử một số hồ sơ B $x \in W(B)$ và hồ sơ bỏ phiếu $B^{\sim}$ sao cho

$$s(x, B^{\sim}) > s(x, B) \text{ và với mọi } y \in X \setminus \{x\}: s(y, B) = s(y, B^{\sim}).$$

Cho các dự án $x_1, \ldots, x_n$ được viết theo định nghĩa A.2.8. Và đặt dưới hồ sơ lá phiếu B $x = x_i$ với $i = 1, n$. Khi $x \in W(B)$ thì $\sum_{j=1}^{i} m(x_j) \leq M$. Nếu $s(x, B^{\sim}) > s(x, B)$, sau đó dưới hồ sơ lá phiếu $B^{\sim}$ $x = x_{i-l}$ cho một số l sao cho $0 \leq l \leq i - 1$. Khi đó $\sum_{j=1}^{i-l} m(x_j) \leq \sum_{j=1}^{i} m(x_j) \leq M$, do đó $x \in W(B^{\sim})$.

Phần **a** của tuyên bố thứ hai được chứng minh.

Để chứng minh phần **b**, chúng ta có thể sử dụng các cân nhắc tương tự.

Mệnh đề đã được chứng minh.

Lưu ý A.1. Trong trường hợp $\forall x, y \in X$: $s(x, B) \neq s(y, B)$ các điều kiện (A.3) xác định duy nhất tập W. Nhưng trong trường hợp ngược lại (như trong mô hình của chúng tôi), một cuộc bỏ phiếu ràng buộc có thể xảy ra. Trong những gì sau đây, chúng tôi giả định rằng trong trường hợp bỏ phiếu ràng buộc, một số thủ tục công bằng được sử dụng.

Chúng tôi cho rằng cử tri bỏ phiếu kín bằng cách gửi lá phiếu trong khi mô hình FTV được sử dụng làm chức năng kết quả. Vì vậy, chúng tôi coi một trò chơi dạng bình thường trong đó chiến lược được đặt cho bất kỳ cử tri i nào là tập hợp của tất cả các lá phiếu có thể có (phân vùng của X). Do đó, hồ sơ lá phiếu B cũng là hồ sơ chiến lược và kết quả là tập hợp các dự án chiến thắng $W(B) \subset X$.

Vì $W(B)$ thường chứa nhiều hơn một dự án, nên phân tích chiến lược của chúng tôi yêu cầu kiến thức về sở thích của cử tri đối với các tập hợp không trống của X. Chúng tôi giả định rằng các ràng buộc về kết quả bị phá vỡ theo Lưu ý A.1 và các phiếu bầu đánh giá kết quả bởi các tiện ích Von-Neumann Morgenstern dự kiến. Vì vậy, tiện ích mà cử tri i gắn vào một tập hợp S các dự án chiến thắng là

$$u_i(S) = \frac{1}{\#S} \sum_{x \in S} u_i(x). \qquad \text{(A.5)}$$

Lý tưởng nhất, chúng tôi muốn chọn tập hợp $W(B)$ của các dự án chiến thắng theo cách sao cho tập hợp này sẽ tối đa hóa kết quả trung bình

$$U(S) = \frac{1}{\#I} \sum_{x \in I} u_i(S). \qquad \text{(A.6)}$$

Nhưng, nói chung nó không phải như vậy đối với thủ tục bỏ phiếu của chúng tôi.

Tuy nhiên, chúng ta có thể đưa ra một số điều kiện đủ để W đạt chức năng cực đại (A.6).

Mệnh đề A.2. *Giả sử, cho một hồ sơ lá phiếu B và theo các điều kiện (A.1), (A.2), (A.4), $W = W(B) = \{x_1, \dots, x_t\}$. Sau đó, theo giả định bỏ phiếu chân thành của FTV (theo nghĩa hẹp):*

$$\max_{S \subset X:\ |S| \geq t} U(S) = U(W),$$

tức là giá trị trung bình (trên tất cả cả tri) của chức năng đạt yêu cầu, hoặc kết quả trung bình, nhận giá trị này là giá trị lớn nhất trên tập hợp những người chiến thắng được xác định bởi thủ tục bỏ phiếu (A.3).

Chứng minh. Viết lại hàm (A.6) bằng cách sử dụng (A.5) theo cách sau:

$$U(S) = \frac{1}{\#I}\sum_{i\in I} u_i(S) = \frac{1}{\#I}\sum_{i\in I}(\frac{1}{\#S}\sum_{x\in S} u_i(x)) = \frac{1}{\#I}\frac{1}{\#S}\sum_{x\in S}(\sum_{i\in I} u_i(x)). \quad (A.7)$$

Dễ dàng nhận thấy điều đó theo giả định chân thành của FTV và theo định nghĩa về điểm số của dự án

$$\sum_{i\in I} u_i(x) = s(x, B).$$

Vì vậy, chúng ta có thể viết lại biểu thức (A.7) dưới dạng

$$U(S) = \frac{1}{\#I}\frac{1}{\#S}\sum_{x\in S}(\sum_{i\in I} u_i(x)) = \frac{1}{\#I}\frac{1}{\#S}\sum_{x\in S} s(x; B).$$

Bây giờ đủ để chứng minh rằng với bất kỳ $S \subset X$, $\#S = f \geq t$, $S = \{s_1, \dots, s_f\}$:

$$U(S) \leq U(W).$$

Theo định nghĩa của hàm $U(S)$, điều này tương đương

$$\frac{\sum_{i=1}^{f} s(s_i, B)}{f} \leq \frac{\sum_{i=1}^{t} s(x_i, B)}{t}. \quad (A.8)$$

Xác định $T = S \cap W$, $W^{\sim} = W \setminus S$, $S^{\sim} = S \setminus W$, $f = t + v$ và

$$\Sigma_1 = \sum_{x\in T} s(x, B), \Sigma_2 = \sum_{x\in \tilde{W}} s(x, B), \Sigma_3 = \sum_{x\in \tilde{S}} s(x, B).$$

Để $|W^{\sim}| = z$ thì $|S^{\sim}| = v + z$. Bây giờ chúng ta có thể viết lại (A.8) như sau:

$$\frac{\Sigma_1 + \Sigma_3}{t + v} \leq \frac{\Sigma_1 + \Sigma_2}{t},$$

hoặc

$$t\Sigma_1 + t\Sigma_3 \leq t\Sigma_1 + v\Sigma_1 + t\Sigma_2 + v\Sigma_2,$$

hoặc

$$t\Sigma_3 \leq v\Sigma_1 + t\Sigma_2 + v\Sigma_2. \quad (A.9)$$

Theo các điều kiện của mệnh đề này, $W = \{x_1, \dots, x_t\}$, do đó $S^{\sim} \subset \{x_{t+1}, \dots, x_k\}$, trong đó $k = \#X$ và với mọi $x \in W$ và mọi $y \in S^{\sim}$: $s(x, B) < s(y, B)$. Cũng lưu ý rằng Σ_1 bao gồm $t - z$ mục, Σ_2 bao gồm z mục và Σ_3 bao gồm $v + z$ mục.

Sau đó, chúng ta có thể ước lượng phần bên trái của (A.9) là

$$t\Sigma_3 \leq t(v + z) \cdot max_{x\in\tilde{S}} s(x, B) \leq t(v + z) \cdot min_{x\in W} s(x, B).$$

Tương tự, chúng ta có thể ước tính phần bên phải của (A.9) là

$$v\Sigma_1 + t\Sigma_2 + v\Sigma_2 \geq (tz + v(t - z) + vz) \cdot min_{x\in W} s(x; B) = t(z + v) \cdot min_{x\in W} s(x; B),$$

và (A.9) đúng, thì bất đẳng thức tương đương (A.8) cũng đúng.

Hệ quả A.1. *Giả sử, cho một hồ sơ lá phiếu B và với các điều kiện (A.1), (A.2), W = W(B) = {x_1, ... , x_t}.*

Tương tự với bất kỳ S ⊂ X, điều kiện sau đây được giữ nguyên: nếu S sử dụng hết ngân sách chung M, thì |S| ≥ t.

Theo giả định bỏ phiếu chân thành của FTV (theo nghĩa hẹp):

$$max_{S \subset X,\ S\ exhausts\ M}\ U(S) = U(W).$$

Hệ quả này có nghĩa là trong các điều kiện của nó, tập hợp những người chiến thắng được chọn theo mô hình bỏ phiếu (A.3) là sự lựa chọn tốt nhất để "làm hài lòng" trung bình tất cả các cử tri.

Lưu ý A.2. Mệnh đề A.2 cũng đúng khi sự ưa thích của cử tri tỷ lệ với các phần tử của *L*, tức là khi ∃ $C > 0$, ∀$i \in I$, ∀$x \in X$: $u_i(x) \in C \cdot L = \{-Cn, \dots, -C, 0, C, \dots, Cn\}$.

A.3. Một số thuộc tính của mô hình FTV

Bây giờ chúng tôi sẽ thảo luận về một số thuộc tính của mô hình AV, mà chúng tôi muốn nó đúng (ít nhất là với một số sửa đổi) với mô hình FTV. Đầu tiên, chúng tôi đưa ra một số thuộc tính cơ bản của mô hình AV và sẽ cho thấy bằng cách sử dụng Counterexample, các thuộc tính này không chạy cho mô hình FTV.

Sau đó, chúng tôi sẽ nêu một số thuộc tính khác, theo một nghĩa nào đó có thể được coi là tương tự của các thuộc tính mô hình AV và sẽ chứng minh các thuộc tính này phù hợp với mô hình FTV.

Đầu tiên, chúng ta cần thêm một số định nghĩa từ [12].

Định nghĩa A.3.1. Đối với bất kỳ cử tri *i* có sự ưa thích u_i, chúng tôi nói rằng *lá phiếu B_i (yếu) chiếm ưu thế hơn lá phiếu B_i˜* khi và chỉ khi

$$u_i(W(B_i, B_{-i})) \geq u_i(W(\tilde{B}_i, B_{-i}))$$

cho tất cả B_{-i} và

$$u_i(W(B_i, B_{-i})) > u_i(W(\tilde{B}_i, B_{-i}))$$

đối với một số B_{-i}.

Một lá phiếu *không bị chi phối (Undominated)* khi và chỉ khi nó không bị chi phối bởi lá phiếu nào.

Tiếp theo [13], chúng tôi cũng gọi những lá phiếu không bị chi phối là *có thể chấp nhận được (Admissible)* và có thể sử dụng một trong hai từ.

Mệnh đề sau đây mô tả các lá phiếu được chấp nhận cho mô hình AV.

Mệnh đề A.3. *(i) Nếu u_i là trống thì tất cả các lá phiếu đều có thể được chấp nhận cho cử tri i.*

(ii) Để số lượng cử tri ít nhất là ba người. Nếu u_i không rỗng thì lá phiếu B_i được chấp nhận cho cử tri i khi và chỉ khi B_i chứa mọi ứng cử viên có điểm u_i cao và không có ứng cử viên nào có điểm u_i thấp.

Chứng minh. Phần (i) là nhỏ và theo sau trực tiếp từ định nghĩa.

Phần (ii) rất được quan tâm. Nói một cách đại khái, nó tuyên bố rằng tốt hơn cho một cử tri bỏ phiếu "một cách chân thành" hoặc "theo sự ưa thích của họ", ít nhất là cho người thích hợp nhất và cho các dự án ít được ưa thích nhất.

Bây giờ chúng ta cho thấy rằng phần (ii) nói chung là không phù hợp với mô hình FTV.

Ví dụ A.1. Counterexample

Cho tập các cử tri $I = \{1, ..., 10\}$, tập các dự án $X = \{x_1, ..., x_7, y\}$, $L = \{-2, -1, 0, 1, 2\}$, và $\forall i \in I$: $u_i(x) \in L$.

Xác định ngân sách chung là $M = 7$ và ngân sách của các dự án là

$$m(x_i) = 1, \text{ i} = \underline{1, 7}; m(y) = 3.$$

Bảng A.1: Lựa chọn của cử tri đầu tiên

Dự án, x_i	x_1	x_2	x_3	x_4	x_5	x_6	x_7	y
$u_1(x_i)$	0	0	0	0	1	1	1	2

Dưới đây chúng ta xem xét hai lựa chọn bỏ phiếu cho cử tri đầu tiên. Trong lựa chọn đầu tiên, họ bỏ phiếu "chân thành" cho dự án y được ưa thích nhất với phiếu $\tilde{B}_1$, tức là dự án y có xếp hạng $\tilde{B}_1$ (mặc dù điều đó không quan trọng nhưng không làm mất đi tính tổng quát, chúng ta có thể cho rằng họ cũng chân thành bỏ phiếu cho các dự án khác). Ở lựa chọn thứ hai, họ bỏ phiếu theo cách ngược lại với lá phiếu B_1, trong đó ngoại trừ dự án y, tất cả các dự án đều có cùng xếp hạng như trong lá phiếu $\tilde{B}_1$, và dự án y có xếp hạng nhỏ nhất. Chúng ta sẽ chỉ ra rằng đối với một số B_{-1}:

$$u_1(W(B_1, B_{-1})) > u_1(W(\tilde{B}_1, B_{-1})).$$

Phương án 1: Cử tri bỏ phiếu cho y **theo sở thích của họ**.

Cho lá phiếu $\tilde{B}_1$, $y \in H_1^{(2)}$.

Để các phiếu bầu khác tạo thành hồ sơ B_{-1} sao cho trong hồ sơ $\tilde{B} = (\tilde{B}_1, B_1)$ điểm của các dự án được phân bổ theo Bảng A.2.

Bảng A.2: Điểm của các dự án trong hồ sơ $\tilde{B} = (\tilde{B}_1, B_1)$

Dự án, x_i	x_1	x_2	x_3	x_4	y	x_5	x_6	x_7
$s(x_i, \tilde{B})$	8	7	6	5	4	3	2	1

Trong trường hợp này $W(\tilde{B}) = \{x_1, \ldots, x_4, y\}$ và $u_1(W(\tilde{B})) = \frac{2}{5} = \frac{14}{35}$.

Lựa chọn 2: Cử tri bỏ phiếu cho y **trái ngược với sở thích của họ**.

Cho phiếu B_1, $y \in H_1^{(-2)}$.

Để các cử tri khác bỏ phiếu như trong phương án 1 và phiếu bầu của họ tạo thành cùng một hồ sơ B_{-1}. Sau đó trong hồ sơ $B = (B_1, B_{-1})$ điểm của các dự án được phân bổ theo Bảng A.3.

Bảng A.3: Điểm của các dự án theo hồ sơ $B = (B_1, B_{-1})$

Dự án, x_i	x_1	x_2	x_3	x_4	x_5	x_6	x_7	y
$s(x_i, B)$	8	7	6	5	3	2	1	0

Trong trường hợp này $W(B) = \{x_1; \ldots, x_7\}$ và $u_1(W(B)) = \frac{3}{7} = \frac{15}{35}$, tức là $u_1(W(B)) > u_1(W(\tilde{B}))$.

Sau ví dụ này, chúng ta có thể kết luận rằng: nói một cách đại khái, chân thành không phải là chiến lược tốt nhất trong mô hình này. Nhưng dưới đây chúng ta sẽ thấy rằng vẫn sẽ có một số ý nghĩa để bỏ phiếu một cách chân thành.

Bây giờ chúng tôi chứng minh một số phát biểu cho mô hình FTV đặc biệt giống với các sai sót đề xuất của mô hình AV được chứng minh trong Mệnh đề (A.3).

Mệnh đề A.4. *Theo thủ tục bỏ phiếu* (A.4)*, các tuyên bố tiếp theo có:*

(i) Nếu u_i là trống thì tất cả các lá phiếu đều có thể được chấp nhận cho cử tri i.

(ii) Nếu đối với một số cử tri $i \in I$ và một số dự án $y \in X$, hàm tiện ích u_i thỏa mãn bất đẳng thức

$$u_i(y) \geq \sum_{x \in X \setminus \{y\}} |u_i(x)|,$$

thì lá phiếu B_i chỉ được chấp nhận đối với cử tri i nếu $y \in H_i^{(n)}$.

(iii) Nếu đối với một số cử tri $i \in I$ và một số dự án $y \in X$, hàm tiện ích u_i thỏa mãn bất đẳng thức

$$u_i(y) \leq -\sum_{x \in X \setminus \{y\}} |u_i(x)|,$$

thì lá phiếu B_i chỉ được chấp nhận đối với cử tri i nếu $y \in H_i^{(-n)}$.

Chứng minh. (i) Phần (i) theo sau trực tiếp từ định nghĩa.

(ii) Xét một lá phiếu $B_i = \{H_i^{(-n)}, \ldots, H_i^{(n)}\}$ mà $y \notin H_i^{(n)}$. Có nghĩa là đối với lá phiếu B_i, $y \in H_i^{(v)}$ với $-n \leq v \leq n-1$. Gọi $\tilde{B}_1$ là lá phiếu mà $\tilde{H}_i^{(v)} = H_i^{(v)} \setminus \{y\}$, $\tilde{H}_i^{(n)} = H_i^{(n)} \cup \{y\}$và $\tilde{H}_i^{(j)} = H_i^{(j)}$ cho tất cả $j \in L \setminus \{v, n\}$. Chúng tôi sẽ chứng minh rằng $\tilde{B}_i$ áp đảo B_i.

Với bất kỳ B_{-i}, ngoại trừ y thì tất cả các ứng cử viên đều có cùng điểm tại (B_i, B_{-i}) và

$(\tilde{B}_i; B_{-i})$ trong khi điểm của y được nâng lên $n - v$ đơn vị ở hồ sơ lá phiếu sau này. Do đó, liên quan đến tập hợp dự án chiến thắng $Y = W(B_i, B_{-i})$ và $\tilde{Y} = W(\tilde{B}_i; B_{-i})$, ba trường hợp sau là đầy đủ:

1. $y \notin Y, y \notin \tilde{Y}$;
2. $y \in Y, y \in \tilde{Y}$;
3. $y \notin Y, y \in \tilde{Y}$.

Trong hai trường hợp đầu tiên $Y = \tilde{Y}$ nên $u_i(Y) = u_i(\tilde{Y})$.

Trong trường hợp thứ ba, đặt $Y = \{x_1, ..., x_t\}$, sau đó $\tilde{Y} = \{x_1, ..., y, ..., x_{t-l}\}$ với $0 \le l \le t - 1$. Chúng tôi chỉ ra rằng trong trường hợp này $u_i(\tilde{Y}) > u_i(Y)$. Nó đủ để chứng minh rằng với mọi l thì $0 \le l \le t - 1$,

$$\frac{\sum_{j=1}^{t} u_i(x_j)}{t} \le \frac{\sum_{j=1}^{t-l} u_i(x_j) + u_i(y)}{t-l+1}. \qquad (A.10)$$

Xác định

$$\Sigma_1 = \sum_{j=1}^{t-l} u_i(x_j), \Sigma_2 = \sum_{j=t-l+1}^{t} u_i(x_j), \Sigma = \sum_{j=1}^{t} u_i(x_j) = \Sigma_1 + \Sigma_2.$$

Bất đẳng thức (A.10) tương đương với bất đẳng thức

$$u_i(y) \ge \frac{\Sigma \cdot (t-l+1)}{t} - \Sigma_1 = \frac{\Sigma \cdot (t-l+1) - \Sigma_1 \cdot t}{t} = \frac{\Sigma_2 \cdot (t-l+1) - \Sigma_1 \cdot (l-1)}{t}. \quad (A.11)$$

Chúng tôi ước tính phần bên phải của bất đẳng thức (A.11):

$$\frac{\Sigma_2 \cdot (t-l+1) - \Sigma_1 \cdot (l-1)}{t} \le$$

$$\le \frac{|\Sigma_2| \cdot (t-l+1) + |\Sigma_1| \cdot (l-1)}{t} \le \frac{(t-l+1)\sum_{x \in X \setminus \{y\}} |u_i(x)| + (l-1)\sum_{x \in X \setminus \{y\}} |u_i(x)|}{t} =$$

$$= \sum_{x \in X \setminus \{y\}} |u_i(x)| \le u_i(y),$$

trong đó bất đẳng thức sau tuân theo các điều kiện của định lý. Vậy bất đẳng thức (A.11) đúng và bất đẳng thức (A.10) cũng vậy.

Bây giờ chúng ta phải chứng minh rằng tồn tại một số hồ sơ B_{-i} rằng

$$u_i(W(\tilde{B}_i; B_{-i})) > u_i(W(B_i; B_{-i})).$$

Đặt hồ sơ B_{-i} sao cho chính xác $\lceil 0.1 \cdot \#I \rceil - v - 1$ cử tri bỏ phiếu với $y \in H_1$ và $z \in H_0$ với bất kỳ $z \in X \setminus \{y\}$. Tất cả các cử tri còn lại bỏ phiếu $z \in H_0$ cho bất kỳ $z \in X$. Khi đó với $B = (B_i; B_{-i})$:

$$s(y, B) = \lceil 0.1 \cdot \#I \rceil - v - 1 + v = \lceil 0.1 \cdot \#I \rceil - 1;$$

$$s(z, B) = 0, \text{ với mọi } z \in X \setminus \{y\},$$

nên $W(B) = \emptyset$ và $u_i(W(B)) = 0$.

Đồng thời, đối với hồ sơ $B^{\sim} = (B^{\sim}_i; B_{-i})$:

$$s(y, \tilde{B}) = \lceil 0.1 \cdot \#I \rceil - v - 1 + n \geq \lceil 0.1 \cdot \#I \rceil \text{ vì } n \geq v - 1;$$

$$s(z, B) = 0, \text{ với mọi } z \in X \setminus \{y\},$$

do đó $W(B^{\sim}) = \{y\}$ và $ui(W(B^{\sim})) = u_i(y)$.

Sau đó, dưới hồ sơ B_{-i}, $u_i(W(\tilde{B}_i; B_{-i}) > u_i(W(B_i; B_{-i})$. Phần (ii) được chứng minh.

(iii) Xét một lá phiếu $B_i = \{H_i^{(-n)}; \ldots; H_i^{(n)}\}$ mà $y \notin H_i^{(-n)}$. Có nghĩa là đối với lá phiếu B_i, $y \in H_i^{(v)}$ đối với một số $-(n-1) \leq v \leq n$. Gọi $\tilde{B}_i$ là lá phiếu mà $H^{\sim}_i{}^{(v)} = H_i^{(v)} \setminus \{y\}$, $H^{\sim}_i{}^{(-n)} = H_i^{(-n)} \cup \{y\}$ và $H^{\sim}_i{}^{(j)} = H_i^{(j)}$ với mọi $j \in L \setminus \{v, -n\}$. Chúng tôi sẽ chứng minh rằng $\tilde{B}_i$ áp đảo B_i.

Cho B_{-i} bất kỳ, ngoại trừ y thì tất cả các ứng cử viên đều có cùng điểm tại $(B_i; B_{-i})$ và $(\tilde{B}_i; B_{-i})$ trong khi điểm của y giảm đi $n + v$ đơn vị ở hồ sơ lá phiếu sau. Do đó, liên quan đến tập hợp các dự án chiến thắng $Y = W(B_i; B_{-i})$ và $Y^{\sim} = W(\tilde{B}_i; B_{-i})$, ba trường hợp sau là đầy đủ:

1. $y \notin Y, y \notin \tilde{Y}$;
2. $y \in Y, y \in \widetilde{Y}$;
3. $y \in Y, y \notin \tilde{Y}$.

Trong hai trường hợp đầu tiên $Y = Y^{\sim}$ nên $u_i(Y) = u_i(Y^{\sim})$.

Trong trường hợp thứ ba, đặt $Y^{\sim} = \{x_1, \ldots, x_t\}$, sau đó $Y = \{x_1, \ldots, y, \ldots, x_{t-l}\}$ với $0 < l \leq t - 1$. Chứng tỏ rằng trong trường hợp này $u_i(Y^{\sim}) \geq u_i(Y)$. Nó đủ để chỉ ra rằng với mọi l thì $0 < l \leq t - 1$,

$$\frac{\sum_{j=1}^{t} u_i(x_j)}{t} \geq \frac{\sum_{j=1}^{t-l} u_i(x_j) + u_i(y)}{t - l + 1}. \qquad (A.12)$$

Xác định

$$\Sigma_1 = \sum_{j=1}^{t-l} u_i(x_j), \Sigma_2 = \sum_{j=t-l+1}^{t} u_i(x_j), \Sigma = \sum_{j=1}^{t} u_i(x_j) = \Sigma_1 + \Sigma_2.$$

Bất đẳng thức (A.12) tương đương với bất đẳng thức

$$u_i(y) \geq \frac{\Sigma \cdot (t - l + 1)}{t} - \Sigma_1 = \frac{\Sigma \cdot (t - l + 1) - \Sigma_1 \cdot t}{t} = \frac{\Sigma_2 \cdot (t - l + 1) - \Sigma_1 \cdot (l - 1)}{t}. \quad (A.13)$$

Ước lượng phần bên phải của bất đẳng thức (A.13):

$$\frac{\Sigma_2 \cdot (t-l+1) - \Sigma_1 \cdot (l-1)}{t} \geq$$

$$\geq \frac{-|\Sigma_2| \cdot (t-l+1) - |\Sigma_1| \cdot (l-1)}{t} \geq \frac{-(t-l+1)\sum_{x \in X \setminus \{y\}} |u_i(x)| - (l-1)\sum_{x \in X \setminus \{y\}} |u_i(x)|}{t} =$$

$$= - \sum_{x \in X \setminus \{y\}} |u_i(x)| \geq u_i(y),$$

trong đó bất đẳng thức cuối cùng tuân theo các điều kiện của định lý.

Vậy các bất đẳng thức (A.12), (A.13) là đúng.

Bây giờ chúng ta phải chứng minh rằng tồn tại một số hồ sơ B_{-i} mà

$$u_i\,(W\,(\tilde{B}_i;\, B_{-i})) > u_i\,(W\,(B_i;\, B_{-i})).$$

Đặt hồ sơ B_{-i} sao cho chính xác

$\lceil 0.1 \cdot \#I \rceil$ + n - 1 cử tri bỏ phiếu với $y \in H_1$ và $z \in H_0$ với bất kỳ $z \in X \backslash \{y\}$. Tất cả các cử tri còn lại bỏ phiếu $z \in H_0$ với bất kỳ $z \in X$.

Dễ dàng thấy rằng trong trường hợp này $W(\tilde{B}) = \emptyset$ và $u_i\,(W\,(\tilde{B})) = 0$.

Đồng thời, $W\,(B) = \{y\}$ và $u_i\,(W\,(B)) = u_i\,(y)$, do đó

$$u_i\,(W\,(\tilde{B}_i;\, B_{-i})) > u_i\,(W\,(B_i;\, B_{-i}))$$

và phần (iii) được chứng minh.

Mệnh đề A.5. *Giả sử u_i không phải là rỗng. Giả sử $x, y \in X$ với $u_i\,(x) > u_i\,(y)$ thì cử tri i bỏ phiếu chân thành với lá phiếu B_i sao cho $s_i\,(x) > s_i\,(y)$. Khi đó:*

1) *Nếu $u_i\,(x) > 0$ thì tồn tại một hồ sơ B_{-i} sao cho bất kỳ lá phiếu $\tilde{B}_i$ với $s_i'(x) < s_i'(y)$:*

$$u_i\,(W\,(B_i;\, B_{-i})) > u_i\,(W\,(\tilde{B}_i;\, B_{-i})); \qquad \text{(A.14)}$$

2) *Nếu $u_i\,(x) \leq 0$ thì tồn tại một hồ sơ B_{-i} sao cho bất kỳ lá phiếu $\tilde{B}_i$ với $s_i'(x) < s_i'(y)$:*

$$u_i\,(W\,(B_i;\, B_{-i})) \geq u_i\,(W\,(\tilde{B}_i;\, B_{-i})); \qquad \text{(A.15)}$$

và đối với một số $\widehat{B}_i$ với $s_i'(x) < s_i'(y)$:

$$u_i\,(W\,(B_i;\, B_{-i})) > u_i\,(W\,(\widehat{B}_i;\, B_{-i})); \qquad \text{(A.16)}$$

Chứng minh. Trong lá phiếu B_i: $s_i\,(x) = a$, $s_i\,(y) = b$ ($a > b$).

1. Xét trường hợp $u_i\,(x) > 0$.

Cho hồ sơ B_{-i} sao cho chính xác $\lceil 0.1 \cdot \#I \rceil$ - a cử tri bỏ phiếu với $x, y \in H_1$ và $z \in H_0$ với bất kỳ $z \in X \setminus \{x, y\}$. Tất cả các cử tri còn lại bỏ phiếu $z \in H_0$ cho bất kỳ $z \in X$.

Khi đó đối với $B = (B_i, B_{-i})$:

$$s(x, B) = \lceil 0.1 \cdot \#I \rceil - a + a = \lceil 0.1 \cdot \#I \rceil;$$

$$s(y, B) = \lceil 0.1 \cdot \#I \rceil - a + b < \lceil 0.1 \cdot \#I \rceil,$$

vì vậy

$$W(B) = \{x\}$$

và

$$u_i(W(B)) = u_i(x)$$

Bây giờ $\tilde{B}_i$ là lá phiếu bất kỳ với $s_i'(x) < s_i'(y)$. Cho $s_i'(x) = c$, $s_i'(y) = d$. Xác định $B^{\sim} = (\tilde{B}_i; B_{-i})$.

Khi đó:

$$W(B^{\sim}) = \{\{x; y\}, \text{nếu } c \geq a; \{y\}, \text{nếu } c < a \text{ và } d \geq a; \{\emptyset\}, \text{nếu } d < a\}. \quad (A.17)$$

Trong mọi trường hợp từ (A.17), $u_i(W(B^{\sim})) < u_i(W(B))$, do các điều kiện $u_i(x) > 0$ và $u_i(x) > u_i(y)$ (chúng tôi đặt $u_i(\emptyset) = 0$), và bất đẳng thức (A.14) được chứng minh.

2. Bây giờ hãy xem xét trường hợp khi $u_i(x) \leq 0$.

Cho hồ sơ B_{-i} sao cho chính xác $\lceil 0.1 \cdot \#I \rceil$ - a - 1 cử tri bỏ phiếu với $x, y \in H_1$ và $z \in H_0$ với bất kỳ $z \in X \setminus \{x, y\}$. Tất cả các cử tri còn lại bỏ phiếu $z \in H_0$ cho bất kỳ $z \in X$.

Khi đó đối với $B = (B_i, B_{-i})$:

$$s(x, B) = \lceil 0.1 \cdot \#I \rceil - a - 1 + a < \lceil 0.1 \cdot \#I \rceil;$$

$$s(y, B) = \lceil 0.1 \cdot \#I \rceil - a - 1 + b < \lceil 0.1 \cdot \#I \rceil,$$

vì vậy

$$W(B) = \emptyset$$

và

$$u_i(W(B)) = 0.$$

Bây giờ $\tilde{B}_i$ là lá phiếu bất kỳ với $s_i'(x) < s_i'(y)$. Cho $s_i'(x) = c$, $s_i'(y) = d$. Khi đó đối với hồ sơ $B^{\sim} = (\tilde{B}_i; B_{-i})$ tồn tại các tùy chọn sau:

$$W(B^{\sim}) = \{\{x; y\}, \text{nếu } c > a; \{y\}, \text{nếu } c \leq a \text{ và } d > a; \{\emptyset\}, \text{nếu } d \leq a\}. \quad (A.18)$$

Trong hai trường hợp đầu tiên từ (A.18), $u_i(W(B^{\sim})) < u_i(W(B))$ và trong trường hợp thứ ba $u_i(W(B^{\sim})) = u_i(W(B))$. Các bất đẳng thức (A.15), (A.16) được chứng minh.

A.4. Sự cần thiết của bỏ phiếu kín

Bây giờ chúng ta hãy xem việc giữ kết quả bỏ phiếu kín cho đến khi kết thúc thủ tục bỏ phiếu có ý nghĩa như thế nào. Dưới đây, chúng tôi mô tả tình huống khi cử tri i là người bỏ phiếu cuối cùng, có thể thay đổi hoàn toàn nhóm người chiến thắng, đặc biệt là biết được hồ sơ B_{-i} với tất cả các phiếu bầu khác. Người ta có thể xây dựng nhiều ví dụ phức tạp hơn có cùng một kết quả.

Theo những gì sau đây đối với một số $x \in X$, chúng ta sẽ biểu thị $s\ (x;\ B_{-i})$ điểm của dự án x trong hồ sơ B_{-i} và $W(B_{-i})$ tập hợp những người chiến thắng trong hồ sơ B_{-i}, tức là tập hợp trong số các dự án chiến thắng theo thủ tục bỏ phiếu (A.3) khi điểm của chúng là $s\ (x;\ B_{-i})$.

Mệnh đề A.6. *Tồn tại hồ sơ B_{-i}, lá phiếu B_i và phân phối ngân sách $m = \{m(x_i),\ i \in I\}$ mà*

$$W(B_{-i}) \cap W(B_i, B_{-i}) = \emptyset$$

(tức là cử tri i bỏ phiếu với B_i có thể thay đổi hoàn toàn những người chiến thắng).

Chứng minh. Để chứng minh tuyên bố, hãy đưa ra ví dụ có liên quan. Cho $l = 1$ và dưới hồ sơ B_{-i}, trình tự của các dự án (theo thứ tự điểm giảm dần) là

$$x_1, \ldots, x_n$$

và phân bổ ngân sách là:

$$m(x_1) = 0,5 \cdot M,\ m(x_2) = M,\ m(x_3) + \ldots + m(x_k) = 0,5 \cdot M \text{ với } k \leq n.$$

Sau đó, với giả định rằng tất cả các ứng cử viên $x_1, \ldots, x_k$ đều được chấp nhận và theo hồ sơ B_{-i}, tập hợp những người chiến thắng là

$$W_1 = W(B_{-i}) = \{x_1, x_3, \ldots, x_k\}.$$

Cho lá phiếu B_i sao cho $H_i^{(1)} = \{x_2\}$, $H_i^{(-1)} = \{x_1\}$ và $H_i^{(0)} = X \setminus \{x_1, x_2\}$.

Khi đó $W_2 = W\ (B_i;\ B_{-i}) = \{x_2\}$.

Hai bộ chiến thắng W_1 và W_2 hoàn toàn khác nhau mà $W_1 \cap W_2 = \emptyset$ và tuyên bố được chứng minh.

Vì vậy, thậm chí chỉ một cử tri (biết tất cả các lá phiếu khác) cuối cùng cũng có thể thay đổi nhóm người chiến thắng. Tất nhiên, sẽ dễ dàng hơn để làm điều này khi họ biết các lá phiếu còn lại của cử tri.

A.5. Kết luận

Chúng tôi đã đưa ra mô tả chính thức về hệ thống bỏ phiếu được sử dụng trong ECTS cũng như phân tích ban đầu về các thuộc tính của nó. Chúng tôi gọi hệ thống này là biểu quyết theo ngưỡng mờ (FTV). Các kết quả chính như sau:

1. Chúng tôi đã trình bày mô hình toán học cho hệ thống bỏ phiếu FTV. Điểm khác biệt chính của hệ thống này so với hệ thống bỏ phiếu Có-Không-Bỏ phiếu trắng là thủ tục bỏ phiếu không chỉ phụ thuộc vào điểm số của các ứng cử viên mà còn phụ thuộc vào một số yếu tố khác. Trong trường hợp của chúng tôi, yếu tố này là số tiền theo yêu cầu của mỗi đề xuất.
2. Chúng tôi đã chứng minh hệ thống FTV được trình bày đáp ứng một số thuộc tính quan trọng nhất đối với hệ thống bỏ phiếu - tiêu chí Condorcet và quy tắc đơn điệu (Monotone).
3. Chúng tôi đã chứng minh một số tuyên bố liên quan đến các chiến lược bỏ phiếu khả thi.
4. Chúng tôi đã phân tích tầm quan trọng của bỏ phiếu kín và chứng minh rằng ngay cả một cử tri đơn lẻ cũng có thể thay đổi hoàn toàn nhóm người chiến thắng nếu họ biết lá phiếu của các cử tri khác.

A.6. Tài liệu tham khảo

[1] E. Duffield, D. Diaz. Dash: Một loại Crypto trung tâm về quyền riêng tư . White Paper. https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdfA.

[2] A. Gibbard.. Thao tác với các sơ đồ bỏ phiếu: Một kết quả chung. http://courses.math.tufts.edu/math19/duchin/gibbard.pdf.

[3] Brams, Fisburn. Đi từ lý thuyết đến thực hành: Sự thành công hỗn hợp của việc bỏ phiếu tán thành. http://www.nyu.edu/gsas/dept/politics/faculty/brams/theory to practice.pdf.

[4] J. Laslier. Bỏ phiếu chiến lược trong Bầu cử nhiều người chiến thắng với Bỏ phiếu phê duyệt: Lý thuyết cho các cuộc bầu cử lớn. http://www.barcelona-ipeg.eu/wp-content/uploads/2015/09/reasoncommitteeapproval_v2_2016_04_13.pdf.

[5] Niemi, R.(1984). Vấn đề về Hành vi Chiến lược trong Bỏ phiếu Phê duyệt. Tạp chí Khoa học Chính trị Hoa Kỳ, 78(4),952-958. doi: 10.2307/1955800.

[6] Ottewell, Guy (2004) [1987]. "Số học biểu quyết". Hội thảo Phổ thông. Truy cập ngày 08 tháng 05 năm 2010. http://www.universalworkshop.com/ARVOfull.htm.

[7] Remzi Sanver, Jean-FranÂ¸cois Laslier. Các trò chơi biểu quyết phê duyệt cơ bản. https://halshs.archives-ouvertes.fr/hal-00445835/document.

[8] D. Baumeister et. al. Các khía cạnh tính toán của việc bỏ phiếu phê duyệt. http://ftp.cs.rochester.edu/pub/papers/theory/09.tr944.Computational_

Aspects_of_Approval_Voting.pdf.

[9] E. Erdmann. Điểm mạnh và điểm hạn chế của các phương pháp bỏ phiếu cho các cuộc bầu cử chính trị. http://www.d.umn.edu/math/Technical%20Reports/Technical%20Reports%202007- /TR% 202011/TR_201_4.pdf.

[10] S. Park, R. Rivest. Hướng tới Bỏ phiếu Bảo mật bậc hai. https://eprint.iacr.org/2016/400.pdf.

[11] F. Maniquet, P. Mongin. Biểu quyết tán thành và Định lý bất khả thi của Arrow. http://www.isid.ac.in/˜pu/seminar/30_11_2011_Paper.pdf.

[12] Jean-FranA˜§ois Laslier, M. Remzi Sanver (2010) Trò chơi bỏ phiếu phê duyệt cơ bản. Palaiseau, Pháp.

[13] Brams, SJ và PC. Fishburn (1983) Bỏ phiếu phê duyệt. Boston: Birkh¨auser.

[14] Brams, SJ, & Kilgour, DM (2014). Biểu quyết chấp thuận hài lòng. Trong Quyền lực và Thủ tục Bỏ phiếu (trang 323-346). Nhà xuất bản Quốc tế Springer.

[15] https://arxiv.org/ftp/arxiv/papers/1602/1602.05248.pdf.

Người dịch: Nguyễn Văn Tú

Telegram: https://t.me/Tulibra

Link gốc: https://iohk.io/en/research/library/papers/a-proposal-for-an-ethereum-classic-treasury-system/