Augur: một Oracle Phân cấp và Nền tảng Dự báo Thị trường

Jack Peterson, Joseph Krug, Micah Zoltu, and Austin K. Williams và Stephanie Alexander
Nền tảng Dự báo

(Ngày 11 tháng 5 năm 2018)

Augur là không cần sự tin cậy, một oracle phân cấp và là một nền tảng dự đoán thị trường. Kết quả của các thị trường dự đoán của Augur được chọn bởi những người dùng giữ token Reputation gốc của Augur, là những người đặt token của họ vào kết quả quan sát thực tế và ngược lại, nhận phí thanh toán từ các thị trường. Cấu trúc khuyến khích của Augur được thiết kế để đảm bảo rằng báo cáo kết quả trung thực, chính xác luôn là lựa chọn có lợi nhất cho người giữ token Reputation. Người giữ token có thể đăng liên kết Reputation lớn dần để tranh luận các kết quả thị trường được đề xuất. Nếu kích thước của các liên kết này đạt đến một ngưỡng nhất định, Reputation chia tách thành nhiều phiên bản, mỗi phiên bản cho mỗi kết quả có thể có của thị trường tranh luận; người giữ token phải trao đổi token Reputation của họ cho một trong các phiên bản này. Các phiên bản Reputation không tương ứng với kết quả thực tế sẽ trở nên vô giá trị, vì sẽ không có ai tham gia vào các thị trường dự đoán trừ khi họ tin tưởng rằng thị trường sẽ giải quyết chính xác. Do đó, người giữ token sẽ chọn phiên bản duy nhất của Reputation mà họ biết là sẽ tiếp tục có giá trị: phiên bản tương ứng với thực tế.

Augur là một Phần mềm quản trị cơ sở dữ liệu oracle phân cấp và là một nền tảng dự đoán thị trường. Trong một thị trường dự báo, các cá nhân có thể suy đoán về kết quả của các sự kiện trong tương lai; những người dự đoán kết quả một cách chính xác giành được tiền, và những người dự đoán không chính xác mất tiền [1–3]. Giá của một thị trường dự đoán có thể được dùng như một chỉ báo chính xác và được hiệu chỉnh tốt về khả năng xảy ra sự kiện [4–7].

Sử dụng Augur, mọi người sẽ có khả năng giao dịch trong các thị trường dự đoán với chi phí rất thấp. Chi phí tham gia giả định đáng kể duy nhất là hoa hồng cho người tạo thị trường và cho người dùng báo cáo về kết quả của thị trường khi sự kiện đã diễn ra. Kết quả là một thị trường dự đoán đáp ứng các yêu cầu về sự tin tưởng, và sự cạnh tranh, bên cạnh đó chi phí sẽ thấp ngang bằng các các lực lượng thị trường và cạnh tranh có thể thúc đẩy thị trường.

Trong lịch sử, thị trường dự đoán đã được tập trung hóa. Cách đơn giản nhất để tổng hợp các giao dịch trong thị trường dự đoán là cho một thực thể đáng tin cậy để duy trì một sổ cái; tương tự, cách đơn giản nhất để xác định kết quả của một sự kiện và phân phối các khoản thanh toán cho các nhà giao dịch là cần có một thẩm phán khách quan, đáng tin cậy để xác định kết quả của thị trường. Tuy nhiên, thị trường dự đoán tập trung có nhiều rủi ro và hạn chế: chúng không cho phép tham gia toàn cầu, chúng hạn chế loại thị trường hoặc giao dịch có thể được tạo ra và yêu cầu những nhà giao dịch tin tưởng nhà điều hành thị trường không ăn cắp tiền và giải quyết thị trường một cách chính xác.

Augur nhắm đến việc giải quyết thị trường một cách hoàn toàn phân cấp. Các mạng phân cấp, không trung thực, chẳng hạn như Bitcoin [8] và Ethereum [9], loại bỏ rủi ro khi nhu cầu cá nhân trở thành tham nhũng hoặc trộm cắp. Vai trò duy nhất của các nhà phát triển Augur là xuất bản các hợp đồng thông minh cho mạng Ethereum. Các hợp đồng của Augur hoàn toàn tự động: các nhà phát triển không có khả năng chi tiền trong hợp đồng ký quỹ, không kiểm soát cách thị trường giải quyết, không chấp thuận hoặc từ chối trao đổi hoặc các giao dịch khác trên mạng, không thể hoàn tác giao dịch, không thể sửa đổi hoặc hủy bỏ lệnh, vv. Augur *oracle* cho phép thông tin được di chuyển từ thế giới thực sang một blockchain mà không dựa vào một trung gian đáng tin cậy. Augur sẽ là oracle phân cấp đầu tiên trên thế giới.

I. CÁCH THỨC HOẠT ĐỘNG CỦA AUGUR

Thị trường Augur chia thành bốn giai đoạn: *hình thành*, *trao đổi*, *báo cáo* và *thiết lập*. Bất kỳ ai cũng có thể tạo thị trường dựa trên mọi sự kiện trong thế giới thực. Giao dịch bắt đầu ngay lập tức sau khi tạo thị trường và tất cả người dùng đều được tự do giao dịch trên bất kỳ thị trường nào. Sau khi một sự kiện xảy ra trên một thị trường, kết quả của sự kiện được xác định bởi oracle của Augur. Khi kết quả được xác định, các nhà giao dịch có thể đóng vị trí của họ và thu thập các khoản thanh toán của họ.

Augur có một token gốc, Reputation (REP). REP cần thiết cho những người sáng tạo thị trường và bởi các phóng viên khi họ báo cáo về kết quả của các thị trường được tạo ra trên nền tảng Augur. Phóng viên báo cáo về một thị trường bằng cách *staking* REP của họ trên một trong những kết quả có thể của thị trường. Bằng cách này, các reporter tuyên bố kết quả mà trên đó cổ phần được đặt phù hợp với kết quả thực tế của sự kiện tiềm ẩn của thị trường. Sự đồng thuận của các reporter của thị trường được coi là "sự thật" với mục đích xác định kết quả của thị trường. Nếu báo cáo kết quả của một reporter không phù hợp với sự đồng thuận của các reporter khác, Augur phân phối lại REP dựa trên kết quả không đồng thuận của reporter này cho các reporter có báo cáo với

sự đồng thuận cao hơn.

Bằng cách sở hữu REP và tham gia vào báo cáo chính xác về kết quả của sự kiện, chủ sở hữu token có quyền được hưởng một phần phí trên nền tảng. Mỗi token REP được stake cho phép chủ sở hữu của nó chiếm một phần bằng phí thị trường của Augur. Phóng viên càng sở hữu nhiều REP và càng báo cáo chính xác, thì càng kiếm được nhiều chi phí cho công việc của họ trong việc giữ an toàn cho nền tảng hơn.

Mặc dù REP đóng một vai trò trung tâm trong các hoạt động của Augur, nhưng nó không được sử dụng để giao dịch trong các thị trường của Augur. Các nhà giao dịch sẽ không bao giờ cần sở hữu hoặc sử dụng REP, vì họ không bắt buộc phải tham gia vào quá trình báo cáo.

A. Sự Hình Thành Thị Trường

Augur cho phép bất kỳ ai tạo thị trường về bất kỳ sự kiện nào sắp tới . *người tạo thị trường* đặt *thời gian kết thúc sự kiện* và chọn *phóng viên được chỉ định* để báo cáo kết quả của sự kiện. Các phóng viên được chỉ định không đơn phương quyết định kết quả của thị trường; cộng đồng luôn có cơ hội tranh luận và sửa chữa báo cáo của các phóng viên được chỉ định.

Tiếp theo, người tạo thị trường chọn *nguồn dẫn chứng* mà các reporter nên sử dụng để xác định kết quả. Nguồn dẫn chứng có thể đơn giản là "kiến thức chung", hoặc nó có thể là một nguồn cụ thể, chẳng hạn như "Bộ Năng lượng Hoa Kỳ", bbc.com hoặc địa chỉ của một điểm cuối API cụ thể. [1] Họ cũng đặt *phí cho người tạo*, là khoản phí mà người giao dịch trả cho người tạo thị trường theo hợp đồng thị trường (xem Phần I D để biết chi tiết về phí). Cuối cùng, người tạo thị trường đăng hai liên kết: *liên kết hợp lệ*, và *liên kết không hiển thị báo cáo chỉ định* (còn được gọi ngắn gọn là *liên kết không hiển thị*).

Liên kết hợp lệ được thanh toán bằng ETH và được trả lại cho người tạo thị trường nếu thị trường giải quyết bất kỳ kết quả nào khác ngoài kết quả *không hợp lệ*.[2] Liên kết hợp lệ khuyến khích người sáng tạo thị trường tạo thị trường dựa trên các sự kiện được xác định rõ ràng với kết quả khách quan, rõ ràng. Kích thước của liên kết hợp lệ được đặt động, dựa trên tỷ lệ kết quả không hợp lệ trong các thị trường gần đây. [3]

Liên kết không hiển thị bao gồm hai phần: *liên kết không hiển thị 'gas'* (thanh toán bằng ETH) và *liên kết không hiển thị 'REP'* (thanh toán bằng REP). Các liên kết này được trả lại cho người tạo thị trường nếu phóng viên được chỉ định của thị trường thực sự báo cáo trong ba ngày đầu tiên sau *thời gian kết thúc sự kiện* của thị trường. Nếu phóng viên được chỉ định không gửi báo cáo của họ trong 3 ngày, thì người tạo thị trường sẽ hủy bỏ liên kết không hiển thị và liên kết đó được gửi cho *phóng viên công khai đầu tiên* người báo cáo trên thị trường (xem phần I C 6). Điều này khuyến khích người tạo thị trường chọn một phóng viên được chỉ định đáng tin cậy, và sẽ giúp thị trường giải quyết một cách nhanh chóng.

Liên kết không hiển thị 'gas' hướng tới việc đảm bảo phí gas (phí nội bộ để thực hiện giao dịch) cho reporter công khai đầu tiên. Điều này ngăn chặn tình huống mà phí gas của reporter công khai đầu tiên quá cao để báo cáo có lãi. Liên kết không hiển thị 'gas' được đặt ở mức gấp hai lần phí gas trung bình để báo cáo trong cửa sổ phí trước đó.

Trong trường hợp reporter được chỉ định không báo cáo, liên kết không hiển thị 'REP' sẽ được gửi cho reporter công khai đầu tiên dưới hình thức tiền thưởng cho kết quả được báo cáo của họ, để người reporter công khai đầu tiên nhận được liên kết không hiển thị 'REP' nếu và chỉ nếu họ báo cáo chính xác. Cũng như liên kết hợp lệ, liên kết không hiển thị 'REP' được điều chỉnh động dựa trên tỷ lệ các reporter được chỉ định không báo cáo đúng thời hạn trong cửa sổ phí trước đó. [4]

Người tạo thị trường tạo ra thị trường và đăng tất cả các liên kết được yêu cầu thông qua một giao dịch Ethereum duy nhất. Sau khi giao dịch được xác nhận, thị trường sẽ hoạt động và giao dịch bắt đầu.

B. Giao Dịch

Những người tham gia thị trường dự báo kết quả của các sự kiện bằng cách giao dịch *cổ phiếu* của những kết quả thị trường đó. Một *bộ cổ phiếu hoàn chỉnh* là tập hợp các cổ phần bao gồm một cổ phần của mỗi kết quả hợp lệ có thể có của sự kiện [10]. Một bộ hoàn chỉnh được tạo bởi công cụ đối sánh hợp đồng của Augur khi cần để hoàn thành giao dịch.

Ví dụ, hãy xem xét một thị trường có hai kết quả có thể, A và B. Alice sẵn sàng trả 0,7 ETH cho một cổ phần của A và Bob sẵn sàng trả 0,3 ETH cho một một cổ phần của B. [5] Đầu tiên, Augur khớp các đơn đặt hàng này với

[1] Ví dụ, nếu một thị trường trên " Nhiệt độ cao (ở độ Fahrenheit -độ F) vào ngày 10 tháng 4 năm 2018 tại Sân bay Quốc tế San Francisco, theo báo cáo của Weather Underground "theo nguồn dẫn chứng của https: // www .wunderground.com / history / airport / KSFO / 2018/4/10 / DailyHistory.html, các phóng viên sẽ chỉ cần truy cập URL đó và nhập nhiệt độ cao được hiển thị ở đó dưới dạng báo cáo của họ.

[2] Một *thị trường không hợp lệ* là một thị trường được xác định là không hợp lệ bởi các phóng viên bởi vì không có kết quả nào được liệt kê bởi người tạo thị trường là chính xác, hoặc bởi vì từ ngữ thị trường là mơ hồ hoặc chủ quan; Xem Phần III F để thảo luận.

[3] Xem Phụ lục E 1 để biết chi tiết.

[4] Xem Phụ lục E 2 để biết chi tiết.

[5] Ban đầu, các giao dịch trong thị trường của Augur sẽ sử dụng coin gốc của Ethereum, Ether (ETH). Các bản phát hành tiếp theo của Augur sẽ bao gồm việc hỗ trợ cho các thị trường bằng các token tùy ý được phát hành trên mạng lưới Ethereum, bao gồm các cổ phiếu của các thị trường khác cũng như token có thể đổi thành tiền bảo chứng ('stablecoins '), nếu/khi có sẵn.

Hình 1. Phác thảo đơn giản về chu kỳ của thị trường dự đoán.

nhau và thu tổng cộng 1 ETH từ Alice và Bob.[6]Sau đó, Augur tạo ra một bộ cổ phần hoàn chỉnh, cấp cho Alice cổ phầnA và Bob cổ phần B. Đây là cổ phần của các kết quả tồn tại, khi các cổ phần được tạo ra, chúng có thể được giao dịch một cách tự do.

Các hợp đồng giao dịch của Augur duy trì một cuốn sổ đặt hàng cho mọi thị trường được tạo ra trên nền tảng này. Bất kỳ ai cũng có thể tạo đơn đặt hàng mới hoặc điền vào đơn đặt hàng có sẵn bất kỳ lúc nào. Các đơn đặt hàng được điền bởi một công cụ đối sánh tự động tồn tại trong các hợp đồng thông minh của Augur. Yêu cầu mua hoặc bán cổ phiếu được thực hiện ngay lập tức nếu có một đơn hàng khớp lệnh đã có trên sổ lệnh. Nó có thể được lấp đầy bằng cách mua cổ phiếu từ hoặc bán cổ phần cho những người tham gia khác, trong đó, có thể liên quan đến việc phát hành bộ hoàn chỉnh mới hoặc đóng các bộ hoàn chỉnh hiện có. Ông cụ đối sánh của Augur luôn yêu cầu số lượng cổ phiếu tối thiểu và / hoặc tiền mặt cần thiết để bù đắp giá trị rủi ro. Nếu không có lệnh khớp, hoặc yêu cầu chỉ có thể được điền một phần, thì phần còn lại được đặt trên sổ lệnh làm đơn hàng mới. Đơn đặt hàng không bao giờ được thực hiện ở mức giá thấp hơn giá giới hạn do nhà giao dịch quy định, nhưng có thể được thực hiện ở mức giá tốt hơn. Đơn đặt hàng chưa thực hiện hoạc chỉ được thự hiện một phần có thể bị xóa khỏi sổ đặt hàng của người tạo đơn đặt hàng bất kỳ lúc nào. Lệ phí được trả bởi người giao dịch chỉ khi bộ cổ phần hoàn chỉnh được bán; phí giải quyết được thảo luận chi tiết hơn trong phần I D.

Trong khi hầu hết các giao dịch cổ phiếu dự kiến sẽ xảy ra trước khi thị trường được thiết lập, cổ phiếu có thể được giao dịch bất kỳ lúc nào sau khi thị trường được tạo ra. Tất cả tài sản của Augur - bao gồm cổ phần trong thị trường kết quả, token tham gia, cổ phiếu trong liên kết tranh luận và thậm chí quyền sở hữu của thị trường - có thể chuyển nhượng mọi lúc.

C. Báo Cáo

Khi sự kiện cơ bản của thị trường xảy ra, kết quả phải được xác định để thị trường hoàn tất và bắt đầu giải quyết. Kết quả được xác định bởi oracle của Augur, bao gồm các reporter có động cơ lợi nhuận, người chỉ đơn giản là báo cáo kết quả thực tế của sự kiện. Bất kỳ ai sở hữu REP đều có thể tham gia vào việc báo cáo và tranh luận về kết quả. Các reporter có báo cáo nhất quán với sự đồng thuận được khen thưởng về tài chính, trong khi những người có báo cáo không nhất quán với sự đồng thuận bị phạt tiền về tài chính (xem Phần I D 3).

1. Cửa Sổ Phí

Hệ thống báo cáo của Augur chạy trên một chu kỳ *cửa sổ phí* dài 7 ngày liên tiếp . Tất cả các khoản phí do Augur thu thập trong một cửa sổ phí cụ thể sẽ được thêm vào *pool phí báo cáo)* cho cửa sổ phí đó. Vào cuối của cửa sổ phí, 'pool' phí báo cáo được thanh toán cho các chủ sở hữu REP đã tham gia vào quá trình báo cáo. Các reporter nhận được phần thưởng tương ứng với số tiền họ đã đặt cược trong cửa sổ phí đó. Việc tham gia bao gồm: đặt cọc trong một báo cáo ban đầu, tranh luận một kết quả dự kiến, hoặc mua *token tham gia.*

2. Token Tham Gia

Trong bất kỳ cửa sổ phí nào, người sở hữu REP có thể mua bất kỳ số lượng token tham gia nào cho một attorep[7]. Ở cuối cửa sổ phí, họ có thể đổi token tham gia của họ cho mỗi attorep, cộng thêm tỷ lệ phần trăm cổ phần của *pool phí báo cáo* của cửa sổ phí. Nếu không có hành động (*ví dụ*, gửi báo cáo hoặc tranh luận một báo cáo được gửi bởi người dùng khác) cần thiết của phóng viên, phóng viên có thể mua token tham gia để cho biết họ đã hiển thị trên cửa sổ phí. Cũng giống như việc đặt REP, token tham gia có thể được chủ sở hữu đổi thành một *khoản* phí theo tỷ lệ trong cửa sổ phí này.

Như đã thảo luận trong phần II, điều quan trọng là người giữ REP sẵn sàng tham gia vào giải pháp thị trường trong trường hợp cập nhật phần mềm(fork). Token tham gia khuyến khích cho người giữ REP theo dõi nền tảng ít nhất một lần mỗi tuần và do đó, sẵn sàng tham gia nếu nhu cầu phát sinh. Ngay cả những người sở hữu REP không muốn tham gia vào quá trình báo cáo đều được khuyến khích đăng ký với Augur một lần một cửa sổ phí 7 ngày để mua token tham gia và thu phí. Việc đăng ký thường xuyên, tích cực này sẽ đảm bảo rằng họ quen thuộc với cách sử dụng Augur, và biết được lúc cập nhật

[6]Đặc điểm thứ nhất của ETH được sử dụng ở đây để dễ dàng thảo luận. Chi phí thực tế của một nhóm cổ phiếu hoàn chỉnh nhỏ hơn nhiều, xem docs.augur.net/#number-of-ticks để biết thêm chi tiết.

[7]Một *attorep* là 10^{-18} REP.

phần mềm, và do đó sẽ sẵn sàng hơn để tham gia vào khi sự kiện xảy ra.

3. Sự Phát Triển Của Thị Trường

Thị trường Augur có thể ở 7 trạng thái khác nhau sau khi tạo. Các trạng thái tiềm năng, hoặc các 'pha' của một thị trường Augur như sau:

- Trước báo cáo
- Báo cáo được chỉ định
- Báo cáo mở
- Đợi cửa sổ phí tiếp theo để bắt đầu
- Vòng tranh luận
- Fork
- Hoàn thành

Mối quan hệ giữa các trạng thái này có thể được nhìn thấy trong Hình. 2.

4. Trước Báo Cáo

Giai đoạn *trước báo cáo* hoặc *giao dịch* (Hình. 1) là khoảng thời gian bắt đầu sau khi giao dịch bắt đầu trên thị trường, nhưng trước khi sự kiện của thị trường đã qua . Nói chung, đây là thời điểm giao dịch tích cực nhất đối với bất kỳ thị trường Augur cụ thể nào. Khi ngày kết thúc sự kiện đã trôi qua, thị trường bước vào giai đoạn*báo cáo được chỉ định*(Hình. 2a).

5. Reporter Được Chỉ Định

Khi tạo thị trường, người tạo trên thị trường được yêu cầu chọn một reporter được chỉ định và đăng liên kết không hiển thị. Trong giai đoạn báo cáo được chỉ định (Hình. 2a) reporter được chỉ định của thị trường có tối đa ba ngày để báo cáo về kết quả của sự kiện. Nếu reporter được chỉ định không báo cáo trong vòng ba ngày được giao, người tạo thị trường sẽ hủy bỏ liên kết không hiển thị và thị trường tự động bước vào giai đoạn*báo cáo mở* (Hình. 2b).

Nếu reporter được chỉ định gửi báo cáo đúng thời hạn, thì liên kết không hiển thị sẽ được trả lại cho người tạo thị trường. Reporter được chỉ định bắt buộc phải đăng phần giới thiệu của reporter được chỉ định để xem phần chi tiết của người báo cáo được chỉ định[8] về kết quả được báo cáo của họ, báo cáo này sẽ bị hủy nếu thị trường hoàn thành bất kỳ kết quả khác với báo cáo mà họ báo cáo.[9] Ngay sau khi reporter được chỉ định gửi báo cáo của mình, thị trường bước vào giai đoạn *đợi cửa sổ phí tiếp theo để bắt đầu* (Hình. 2c), và kết quả được báo cáo sẽ trở thành *kết quả dự kiến*của thị trường.

6. Báo Cáo Mở

Nếu reporter được chỉ định không báo cáo trong vòng ba ngày được giao, người tạo thị trường sẽ hủy bỏ liên kết không hiển thị, và thị trường ngay lập tức bước vào giai đoạn *báo cáo mở*(Hình. 2b). Ngay sau khi thị trường bước vào giai đoạn báo cáo mở, bất kỳ ai cũng có thể báo cáo kết quả của thị trường. Khi reporter được chỉ định không báo cáo, reporter đầu tiên báo cáo về kết quả của một thị trường được gọi là *reporter công khai đầu tiên.*

Reporter công khai đầu tiên của thị trường nhận được liên kết không hiển thị dưới hình thức đặt cọc vào kết quả đã chọn của họ, vì vậy họ có thể yêu cầu liên kết REP không hiển thị nếu kết quả được báo cáo của họ khớp với kết quả cuối cùng của thị trường. Họ cũng nhận được liên kết không hiển thị 'gas' sau khi thị trường đã hoàn thành nếu như kết quả báo cáo của họ khớp với kết quả cuối cùng của thị trường.

Reporter công khai đầu tiên *không* cần phải đặt cọc bất kỳ REP nào của họ khi báo cáo kết quả của thị trường. Bằng cách này, bất kỳ thị trường nào mà reporter được chỉ định không báo cáo thì có thể lấy kết quả được báo cáo bởi *một ai đó* ngay sau khi bước vào giai đoạn báo cáo mở.

Khi một *báo cáo ban đầu* được nhận bởi reporter ban đầu (cho dù đó là reporter được chỉ định hoặc reporter công khai đầu tiên), kết quả được báo cáo sẽ trở thành kết quả dự kiến của thị trường, và thị trường bước vào gia đoạn chờ cửa sổ phí tiếp theo để bắt đầu giao đoạn (Hình. 2c).

7. Chờ Cửa Sổ Phí Tiếp Theo Để Bắt Đầu

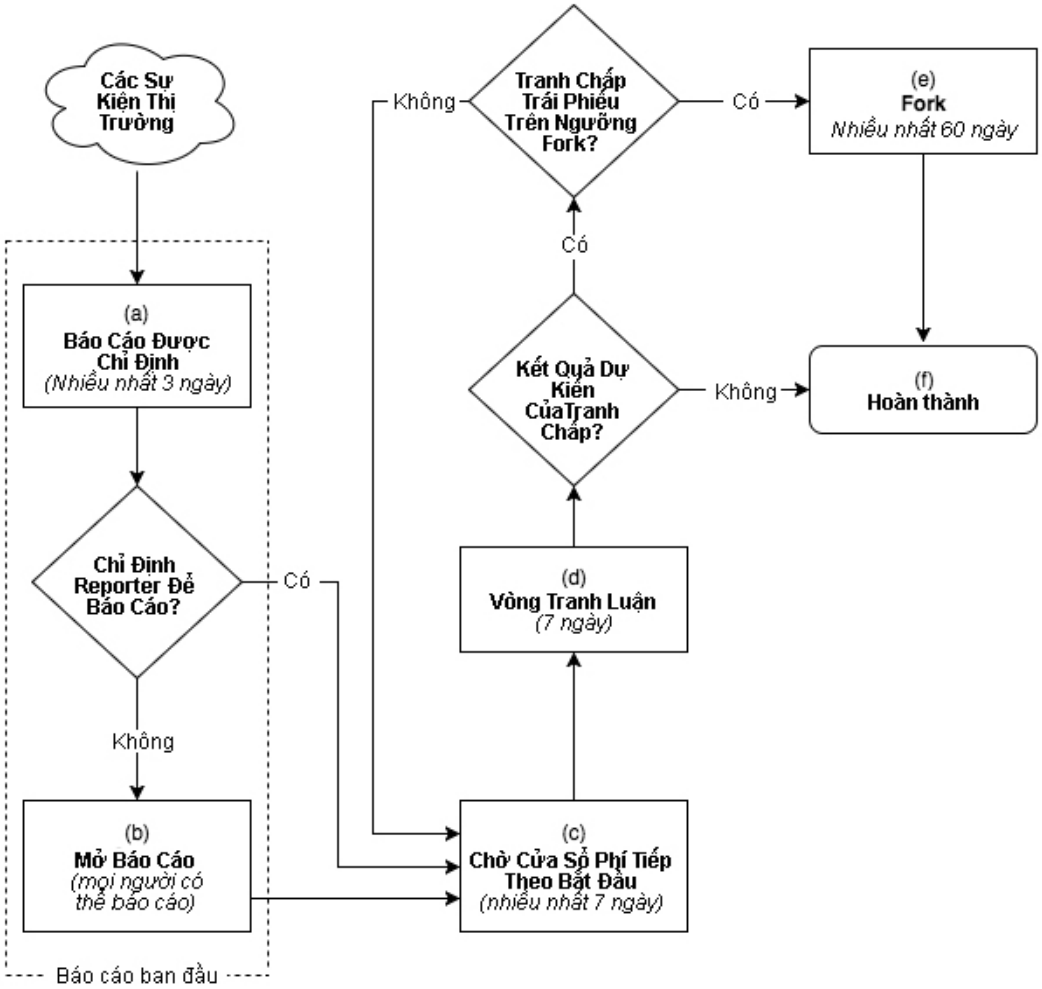
Một khi thị trường nhận được báo cáo ban đầu của nó, nó bước vào giao đoạn chờ cửa sổ phí tiếp theo để bắt đầu giai đoạn (Hình. 2c). Trong giai đoạn này, báo cáo cho thị trường đang bị giữ cho đến khi kết thúc của cửa sổ phí hiện hành. Khi cửa sổ phí tiếp theo bắt đầu, thị trường bước vào giai đoạn *vòng tranh luận.*

8. Vòng Tranh Luận

Vòng tranh luận (Hình. 2d) là khoảng thời gian 7 ngày trong đó bất kỳ người nắm REP nào cũng có cơ hội tranh

[8] Xem phụ lục E 3 để biết chi tiết về giới hạn của reporter được chỉ định

[9] Tiền lãi bị tịch thu được thêm vào 'pool' phí báo cáo của cửa sổ phí được chỉ định của thị trường và được sử dụng để thưởng cho các reporter trung thực; Xem phần I D 3 để biết chi tiết.



Hình 2. Sơ đồ báo cáo.

luận *kết quả dự kiến* của thị trường.[10] (Khi bắt đầu một vòng tranh luận, kết quả dự kiến của một thị trường sẽ trở thành kết quả cuối cùng của thị trường nếu nó không được chủ sở hữu REP tranh luận thành công). Vòng tranh luận bao gồm *staking* REP (trong ngữ cảnh này được gọi là *tranh chấp cổ phần*) trên một kết quả *ngoài* kết quả dự kiến hiện tại của thị trường. Tranh luận *thành công* nếu tổng số cổ phần tranh chấp đối với một số kết quả thỏa mãn yêu cầu *giới hạn liên kết tranh luận* cho vòng hiện tại. Giới hạn liên kết tranh luận được tính như sau.

Giả sử A_n biểu thị tổng số cổ phần trên tất cả các kết quả của thị trường này khi bắt đầu tranh luận vòng n. Gỉa sử ω là bất kỳ kết quả thị trường nào *ngoài* kết quả dự kiến của thị trường vào đầu vòng tranh luận này. Giả sử $S(\omega, n)$ biểu thị tổng số tiền đặt cược vào kết quả ω khi bắt đầu tranh luận vòng n. Sau đó, kích thước của *liên kết tranh luận* cần thiết để tranh luận thành công kết quả dự kiến hiện tại có lợi cho kết quả mới ω trong vòng n được ký hiệu $B(\omega, n)$ và được cho bởi:

$$B(\omega, n) = 2A_n - 3S(\omega, n) \tag{1}$$

Kích thước liên kết được chọn theo cách này để đảm bảo ROI cố định là 50% cho các reporter tranh luận thành công kết quả sai (xem phần II D).

Các liên kết tranh luận không cần phải được thanh toán toàn bộ bởi một người dùng duy nhất. Nền tảng Augur cho phép các thành viên tham gia vào các liên kết tranh luận crowdsource. Bất kỳ người dùng nào nhìn thấy kết quả dự kiến không chính xác đều có thể tranh luận kết quả đó bằng cách đặt REP vào một kết quả khác với kết quả dự kiến. Nếu bất kỳ kết quả nào (ngoài kết quả dự kiến) tích lũy đủ số lượng tranh luận để lấp đầy liên kết tranh luận, kết quả dự kiến hiện tại sẽ được tranh luận thành công.

Trong trường hợp tranh luận thành công, thị trường

[10] hực tế vòng tranh luận trùng với cửa sổ phí rõ ràng là một vấn đề thuận tiện; về nguyên tắc, vòng tranh luận và thời gian của cửa sổ phí có thể khác nhau.

sẽ trải qua một vòng tranh luận khác, hoặc nó sẽ vào trạng thái *ngã ba* (Hình. 2e). Nếu kích thước của liên kết tranh luận đầy đủ lớn hơn 2,5% của tất cả REP, thì thị trường sẽ vào trạng thái fork. Nếu kích thước của liên kết tranh luận đầy đủ ít hơn 2,5% của tất cả REP, thì kết quả mới được chọn sẽ trở thành kết quả dự kiến mới của thị trường và thị trường trải qua một vòng tranh luận khác.

Tất cả các cổ phần tranh luận được giữ trong ký quỹ trong suốt vòng tranh luận. Nếu liên kết tranh luận không thành công, thì cổ phần tranh luận được trả lại cho chủ sở hữu của nó vào cuối vòng tranh luận. Nếu không có tranh luận thành công trong vòng 7 ngày tranh luận, thị trường sẽ vào trạng thái *hoàn thành* (Hình. 2f), và kết quả dự kiến của nó được chấp nhận là *kết quả cuối cùng* . Kết quả cuối cùng của thị trường là kết quả dự kiến đi qua một vòng tranh luận mà không bị tranh luận thành công, hoặc được xác định thông qua một fork. Các hợp đồng của Augur coi các kết quả cuối cùng là *sự thật* và trả tiền một cách phù hợp.

Tất cả cổ phần tranh luận không thành công được trả lại cho chủ sở hữu ban đầu vào cuối mỗi vòng tranh luận. Tất cả cổ phần tranh luận thành công được áp dụng cho kết quả mà nó đã giành được, và vẫn tồn tại cho đến khi thị trường được hoàn thành (hoặc cho đến khi một fork xảy ra ở một số thị trường khác của Augur). Tất cả các cổ phần tranh luận (dù thành công hay không thành công) sẽ nhận được một phần của *'pool' phí báo cáo* [11] Từ cửa sổ phí hiện hành.

9. Fork

Trạng thái fork (Hình. 2e) là trạng thái đặc biệt kéo dài đến 60 ngày. Forking là phương pháp phân tích thị trường cuối cùng; nó là một quá trình đột phá và rất ít xuất hiện. Một fork được gây ra khi có một thị trường với một kết quả với một liên kết tranh luận thành công đầy đủ của ít nhất 2,5% của tất cả REP. Thị trường này được gọi là *forking market (thị trường nâng cấp)*

Khi một fork được bắt đầu, một quá trình 60 ngày[12] *giai đoạn forking* bắt đầu. Tranh luận cho tất cả các thị trường không hoàn thành khác được giữ cho đến khi kết thúc giai đoạn này. Thời gian phân tách dài hơn nhiều so với cửa sổ phí thông thường vì nền tảng cần cung cấp thời gian cho các chủ sở hữu REP và các nhà cung cấp dịch vụ (ví dụ như ví và sàn) để chuẩn bị. Kết quả cuối cùng của một fork không thể bị tranh luận.

Mọi thị trường Augur và tất cả các token REP tồn tại trong một số *không gian*. Token REP có thể được sử dụng để báo cáo kết quả (và do đó kiếm được phí) *chỉ* cho các thị trường tồn tại trong cùng một không gian như token REP. Khi Augur ra mắt lần đầu tiên, tất cả các thị trường và tất cả REP sẽ tồn tại cùng nhau trong *không gian nguyên thủy*.

Khi một thị trường fork, không gian mới được tạo ra. Việc tạo ra một *không gian con* mới cho mỗi kết quả có thể có của thị trường fork (bao gồm không hợp lệ, như được thảo luận trong phần **??**). Ví dụ, một thị trường "nhị phân" có 3 kết quả có thể có: A, B, và không hợp lệ. Do đó, thị trường nhị phân sẽ tạo ra ba không gian con mới: không gian A, không gian B và không gian không hợp lệ. Ban đầu, các vũ trụ mới được tạo ra này trống: chúng không chứa thị trường hoặc mã REP.

Khi một fork được khởi tạo, *không gian cái* trở thành vĩnh viễn *khóa*. Trong một vũ trụ bị khóa, không có thị trường mới nào có thể được tạo ra. Người dùng có thể tiếp tục giao dịch cổ phiếu tại các thị trường trong vũ trụ bị khóa và thị trường trong vũ trụ bị khóa có thể vẫn nhận được báo cáo ban đầu của họ. Tuy nhiên, không có phần thưởng báo cáo nào được thanh toán ở đó và các thị trường trong vũ trụ bị khóa không thể được hoàn thành. Để các thị trường hoặc token REP trong vũ trụ bị khóa hữu ích, trước tiên chúng phải được di chuyển đến một vũ trụ con.

Những người có token REP trong vũ trụ cái có thể di chuyển token của họ đến một vũ trụ con mà họ chọn. Sự lựa chọn này nên được xem xét cẩn thận, bởi vì việc di chuyển là một chiều; nó không thể đảo ngược. Token không thể được giữ các vũ trụ con tương đương. *di chuyển là một cam kết vĩnh viễn của token REP đến một kết quả thị trường cụ thể.* Token REP di chuyển đến các vũ trụ khác nhau nên được coi là các token riêng biệt, và các nhà cung cấp dịch vụ như ví và sàn nên liệt kê chúng như vậy.

Khi một fork được bắt đầu, tất cả REP đặt cược trên tất cả các thị trường không phải fork là *không đặt cược* để nó được tự do di chuyển đến một vũ trụ con trong quá trình fork. [13]

Cho dù vũ trụ con nào được nhiều REP di chuyển đến nhất vào cuối giai đoạn fork trở thành *vũ trụ giành chiến thắng*, và kết quả tương ứng của nó trở thành kết quả cuối cùng của thị trường fork. Thị trường chưa hoàn thành trong vũ trụ cái có thể được di chuyển chỉ đến vũ trụ chiến thắng và, nếu đã nhận được một báo cáo ban đầu, thì được đặt ngược trở lại giai đoạn chờ cửa sổ phí tiếp theo để bắt đầu giai đoạn mới.

Không có giới hạn thời gian để di chuyển token từ vũ trụ cái sang vũ trụ con. Token có thể được di chuyển sau giai đoạn fork, nhưng chúng sẽ không được tính vào việc

[11] Bất kỳ khoản phí thanh toán và liên kết hợp lệ nào được thu thập trong một cửa sổ phí sẽ được thêm vào 'pool' phí báo cáo của cửa sổ phí đó. Ở cuối cửa sổ phí, 'pool' phí báo cáo được thanh toán cho người dùng theo tỷ lệ số tiền họ đã đặt trong cửa sổ phí đó.

[12] Giai đoạn forking có thể ít hơn 60 ngày: một giai đoạn forking kết thúc khi hoặc là 60 ngày đã trôi qua, hoặc hơn 50% của tất cả các REP ban đầu được di chuyển đến các không gian nhỏ hơn.

[13] Ngoại lệ duy nhất là REP được đặt cược bởi reporter ban đầu khi họ thực hiện báo cáo ban đầu. REP đó vẫn được đặt cược vào kết quả báo cáo ban đầu và được tự động di chuyển đến vũ trụ con giành được fork.

xác định vũ trụ chiến thắng. Để khuyến khích sự tham gia nhiều hơn trong giai đoạn fork, tất cả những người sở hữu di chuyển REP của họ trong vòng 60 ngày kể từ ngày bắt đầu một fork sẽ nhận được thêm 5% REP bổ sung trong vũ trụ con mà họ di chuyển [14]. Phần thưởng này được trả bằng cách kết hợp các token REP mới. [15]

Reporter đã đặt cược REP vào một trong những kết quả của thị trường fork không thể thay đổi vị trí của họ trong một fork. REP đã được đặt cược vào một kết quả trong vũ trụ cái chỉ có thể di chuyển đến vũ trụ con tương ứng với kết quả đó. Ví dụ: nếu một reporter đã giúp hoàn thành một liên kết tranh luận thành công có lợi cho kết quả A trong một vòng tranh luận, thì REP họ đã đặt cược vào kết quả A chỉ có thể được di chuyển sang vũ trụ A trong một fork.

Các vũ trụ tương đương hoàn toàn không liên kết với nhau. Các token REP tồn tại trong một vũ trụ không thể được sử dụng để báo cáo về các sự kiện hoặc kiếm được phần thưởng từ các thị trường trong vũ trụ khác. Vì người dùng có lẽ sẽ không muốn tạo ra hoặc giao dịch trên thị trường trong vũ trụ có oracle không đáng tin cậy, REP tồn tại trong vũ trụ không tương ứng với thực tế khách quan không có khả năng kiếm được bất kỳ khoản phí nào, và do đó không nên giữ bất kỳ thị trường quan trọng nào. Do đó, các token REP di chuyển đến một vũ trụ không tương ứng với thực tế khách quan nên không giữ giá trị thị trường, bất kể vũ trụ sai khách quan có kết thúc là vũ trụ chiến thắng sau một fork hay không. Điều này có hậu quả an ninh quan trọng, mà chúng ta thảo luận trong phần II.

10. Hoàn Thành

Một thị trường đi vào trạng thái hoàn thành (Hình. 2f) nếu nó đi qua vòng tranh luận 7 ngày mà kết quả dự kiến của nó không bị phản đối, hoặc sau khi hoàn thành một fork. Kết quả của một fork không thể được tranh luận và luôn luôn được coi là cuối cùng vào cuối giai đoạn fork. Khi một thị trường được hoàn thành, người giao dịch có thể thiết lập trực tiếp vị trí của mình với thị trường. Khi một thị trường bước vào trạng thái hoàn thành, chúng ta xem kết quả được chọn của nó là *kết quả cuối cùng.*

D. Thiết Lập Thị Trường

Một nhà giao dịch có thể đóng vị trí của mình bằng một trong hai cách: bằng cách bán cổ phần mà họ nắm giữ cho một nhà giao dịch khác để đổi lấy tiền hoặc bằng cách thanh toán cổ phần của họ với thị trường. Ở trên đã đề cập rằng mọi cổ phần đều tồn tại như một phần của một bộ hoàn chỉnh khi tổng cộng 1 ETH đã được ký quỹ với Augur.[6] Để lấy 1 ETH đó khỏi ký quỹ, các nhà giao dịch phải cung cấp cho Augur một bộ hoàn chỉnh hoặc , nếu thị trường đã hoàn thành, một phần của kết quả chiến thắng. Khi sự trao đổi này xảy ra, chúng ta nói các nhà giao dịch đang *giải quyết bằng hợp đồng thị trường.*

Ví dụ, hãy xem xét một thị trường không hoàn thành với các kết quả có thể có A và B. Giả sử Alice cổ phần của kết quả A mà cô ấy muốn bán với giá 0,7 ETH và Bob có cổ phần của kết quả B mà anh ta muốn bán với giá 0,3 ETH. Đầu tiên, Augur khớp các lệnh này và thu thập các cổ phần A và B từ những người tham gia. Sau đó, Augur cho 0,7 ETH (trừ phí) cho Alice và 0,3 ETH (trừ phí) cho Bob.

Ví dụ thứ hai, xem xét một thị trường hoàn thiện có kết quả chiến thắng là A. Alice có cổ phần của A và muốn nạp tiền vào. Cô ấy gửi cổ phần của mình là A sang Augur và đổi lại nhận được 1 ETH (trừ phí).

1. Phí Thanh Toán

Thời gian duy nhất Augur thu lệ phí là khi người tham gia thị trường đang giải quyết với hợp đồng thị trường. Augur tính hai khoản phí trong quá trình thanh toán: phí người tạo và phí báo cáo. Cả hai khoản phí này đều tương ứng với số tiền được thanh toán. Vì vậy, trong ví dụ giải quyết trước khi hoàn thành ở trên, nơi Alice nhận được 0,7 ETH và Bob nhận 0,3 ETH, Alice sẽ trả 70% phí trong khi Bob sẽ trả 30%.

Phí người tạo được thiết lập bởi người tạo thị trường trong quá trình tạo thị trường và được trả cho người tạo thị trường khi thiết lập. Phí báo cáo được đặt động (xem PhầnII C) và được trả cho các reporter tham gia vào quá trình báo cáo.

2. Thiết Lập Thị Trường Không Hợp Lệ

Trong trường hợp một thị trường giải quyết dưới dạng không hợp lệ, các nhà giao dịch thanh toán với hợp đồng thị trường nhận được số ETH bằng nhau cho các cổ phần của từng kết quả. Nếu thị trường có kết quả có thể có N (không bao gồm kết quả không hợp lệ), và chi phí của một bộ cổ phần hoàn chỉnh là C ETH, thì người giao dịch sẽ nhận được C/N ETH cho mỗi cổ phần được thanh toán với hợp đồng thị trường. [16]

---

[14] Điều này xảy ra ngay cả khi thời gian chờ đã kết thúc sớm do hơn 50% REP được di chuyển đến một số vũ trụ con.

[15] Hiệu ứng của việc bổ sung này vào nguồn cung tiền của REP là rất nhỏ. Ví dụ, nếu 20% của tất cả REP hiện có được di chuyển trong thời gian của một fork, tiền thưởng này sẽ dẫn đến sự gia tăng 1% trong nguồn cung tiền của REP. Hơn nữa, fork rất ít khi xảy ra.

[16] Giao dịch không thể đơn giản được giải quyết nếu thị trường giải quyết dưới dạng không hợp lệ do hạn chế về kỹ thuật. Cổ phần của kết quả là các token, có thể được giao dịch trực tiếp giữa người dùng; ETH và cổ phần do đó không thuộc quyền kiểm soát của

3. Phân Phối Lại Danh Tiếng

Nếu một thị trường hoàn thành mà không bắt đầu một fork, tất cả REP đặt cược vào bất kỳ kết quả nào khác ngoài kết quả cuối cùng của thị trường sẽ bị mất và phân phối cho người dùng đặt cược vào kết quả cuối cùng của thị trường tương ứng với số lượng REP họ đặt cược. Kích thước liên kết tranh luận được chọn sao cho bất kỳ ai tranh luận thành công một kết quả có lợi cho kết quả cuối cùng của thị trường đều được thưởng 50% ROI trên cổ phần tranh luận của họ.[17] Đây là một động lực mạnh mẽ cho các reporter tranh luận các kết quả dự kiến sai lệch.

II. ƯU ĐÃI VÀ BẢO MẬT

Có một mối quan hệ mạnh mẽ giữa thị trường 'mũ'của REP và sự tin cậy của giao thức chia tách của Augur. Nếu thị trường mũ của REP đủ lớn[18], và kẻ tấn công hợp lý về mặt kinh tế, thì kết quả thắng fork phải tương ứng với thực tế khách quan. Trong thực tế, nó có thể cho Augur hoạt động bình thường mà không sử dụng các reporter được chỉ định và vòng tranh luận. *Chỉ* sử dụng quy trình chia tách, oracle sẽ báo cáo trung thực.

Tuy nhiên, fork đang gây rối và mất thời gian. Một fork mất đến 60 ngày để giải quyết một thị trường duy nhất và chỉ có thể giải quyết một thị trường tại một thời điểm. Trong 60 ngày mà thị trường được giải quyết, tất cả các thị trường khác chưa được hoàn thành sẽ phải ngưng lại. [19] Các nhà cung cấp dịch vụ phải cập nhật và người sở hữu REP phải di chuyển REP của họ sang một trong các vũ trụ con mới. Do đó, chỉ nên sử dụng fork khi chúng thật sự cần thiết. Fork giống như là một lựa chọn hạt nhân.

Nhưng mà, một khi nó đã được thiết lập fork có thể được tin cậy để xác định sự thật, các ưu đãi có thể được sử dụng để khuyến khích người tham gia hành xử trung thực mà không cần phải thực sự bắt đầu một fork. *Đó là mối đe dọa đáng tin cậy của một fork, và niềm tin rằng fork sẽ giải quyết chính xác, đó là nền tảng của hệ thống khuyến khích của Augur.*

Tiếp theo, chúng ta thảo luận về các điều kiện mà theo đó hệ thống chia tách có thể được tin cậy để xác định sự thật. Sau đó chúng ta thảo luận về hệ thống khuyến khích và cách nó tạo động lực viếc giải quyết nhanh chóng và chính xác của tất cả các thị trường.

A. Tính Toàn Vẹn Của Giao Thức Phân Nhánh

Ở đây chúng ta thảo luận về độ tin cậy của quá trình chia tách và các điều kiện theo đó nó có thể được tin cậy. Để dễ thảo luận, khi đề cập đến fork, chúng ta sẽ nói đến vũ trụ con tương ứng với thực tại khách quan như vũ trụ True, và bất kỳ vũ trụ con nào khác như vũ trụ False. Chúng ta sẽ đề cập đến vũ trụ cón nhận được nhiều REP nhất trong giai đoạn fork là vũ trụ chiến thắng và tất cả các vũ trụ con khácllà vũ trụ thua.

Đương nhiên, chúng ta luôn muốn vũ trụ True trở thành vũ trụ chiến thắng và vũ trụ False là vũ trụ thua. Chúng ta nói rằng giao thức chia tách đã bị tấn công thành công bất cứ khi nào vũ trụ False là vũ trụ chiến thắng của một fork - do đó dẫn đến thị trường phân chia (và, có khả năng, tất cả các thị trường không hoàn thành) được thanh toán sai.

Cách tiếp cận của chúng tôi nhằm đảm bảo oracle sắp xếp các vấn đề theo cách mà lợi ích tối đa cho một kẻ tấn công thành công là ít hơn chi phí tối thiểu thực hiện các cuộc tấn công. Chúng tôi chính thức hóa điều này như sau.

1. Lợi Ích Tối Đa Cho Một Kẻ Tấn Công

Kẻ tấn công tấn công oracle thành công sẽ làm cho tất cả các thị trường Augur không hoàn thành chuyển sang vũ trụ False. Nếu kẻ tấn công điều khiển phần lớn REP trong vũ trụ False, thì kẻ tấn công có thể buộc tất cả các thị trường không hoàn thành giải theo cách kẻ đó muốn. Trong trường hợp cực đoan nhất, kẻ đó có thể nắm bắt tất cả các quỹ được ký quỹ ở tất cả các thị trường đó. [20]

Định nghĩa 1. Chúng tôi xác định và biểu thị bằng I_a, *lợi tức gốc* của Augur là giá trị của tổng số tiền được ký quỹ trong các thị trường Augur chưa được lọc. [21]

Định nghĩa 2. Chúng tôi xác định một *thị trường ký sinh* là bất kỳ thị trường nào không trả phí báo cáo cho Augur, nhưng lại giải quyết theo độ phân giải của thị trường Augur nguyên bản.

Định nghĩa 3. Chúng tôi xác định và biểu thị bằng I_p, *lợi tức mở ký sinh* là giá trị của tổng số tiền được ký quỹ trong tất cả các thị trường ký sinh, giải quyết theo thị trường Augur nguyên bản chưa được hoàn tất.

Trong trường hợp cực đoan nhất, kẻ tấn công cũng sẽ có thể nắm bắt tất cả tiền trong tất cả các thị trường ký sinh mà giải quyết theo các thị trường Augur nguyên bản chưa được hoàn thiện.

Augur và không thể trả lại cho chủ sở hữu ban đầu nếu thị trường hoàn tất dưới dạng không hợp lệ.

[17] Xem Định lý 3trong Phụ lục A.

[18] Xem phần II A để biết chi tiết.

[19] Các nhà giao dịch có thể tiếp tục giao dịch trên các thị trường đó, nhưng những thị trường đó không thể hoàn thành cho đến sau thời gian chờ đợi).

[20] Điều này sẽ yêu cầu kẻ tấn công nắm giữ *tất cả* cổ phiếu của một số kết quả nhất định, và sau đó buộc thị trường hoàn thành theo kết quả đó.

[21] Điều này bao gồm các thị trường bên ngoài trả phí báo cáo cho Augur.

Chú ý 1. Lợi ích tối đa (gộp lại) cho kẻ tấn công tấn công oracle thành công là $I_a + I_p$.

2. Lợi Tức Mở Ký Sinh Là Không Xác Định

Augur có thể đo lường chính xác và hiệu quả I_a. Tuy nhiên, I_p nói chung không thể được biết đến, vì có thể tồn tại tùy ý nhiều thị trường ký sinh ngoại tuyến, mỗi thị trường có lợi tức mở lớn tùy ý. Vì lợi ích tối đa có thể cho kẻ tấn công bao gồm số lượng I_p không thể biết được, người ta không bao giờ có thể chắc chắn một cách khách quan rằng oracle là an toàn chống khi lại những kẻ tấn công hợp lý về kinh tế.

Tuy nhiên, nếu chúng tôi sẵn sàng khẳng định rằng I_p được giới hạn hợp lý trong thực tế, thì chúng tôi có thể xác định các điều kiện theo đó chúng tôi có thể khẳng định rằng oracle là an toàn.

3. Chi Phí Tối Thiểu Của Một Cuộc Tấn Công Thành Công

Tiếp theo, hãy xem xét chi phí tấn công oracle. Giả sử P biểu thị giá REP. Giả sử ϵ biểu thị một attorep [22]. Giả sử M biểu thị tổng số tiền REP trong sự tồn tại ('cung tiền 'của REP). Giả sử S biểu thị tỷ lệ M sẽ được di chuyển đến vũ trụ True trong giai đoạn chia tách của một fork.

Vì vậy, sản phẩm SM đại diện cho số tiền tuyệt đối của REP được chuyển đến vũ trụ True trong thời gian chia tách của một fork, và sản phẩm PM là giá trị thị trường của REP.

Giả sử P_f biểu thị giá REP được di chuyển đến vũ trụ False mà kẻ tấn công chọn. Lưu ý rằng nếu $P \leq P_f$ thì oracle sẽ không an toàn đối với những kẻ tấn công hợp lý về kinh tế, bởi vì nó phải ít nhất là lợi nhuận để chuyển REP đến vũ trụ False nếu không nó sẽ không được chuyển đến.

4. Tính Toàn Vẹn

Giả định 1. *Các reporter không phải là kẻ tấn công sẽ không bao giờ chuyển REP đến vũ trụ* False *trong fork.* [23]

Theo thiết kế, một cuộc tấn công thành công trên oracle yêu cầu REP nhiều hơn để được di chuyển đến một số vũ trụ False so với vũ trụ True trong giai đoạn chia tách của một fork. Theo giả định, chỉ kẻ tấn công mới di chuyển REP đến vũ trụ False. Số lượng REP được di chuyển đến vũ trụ True trong khoảng thời gian báo cáo được biểu thị bằng SM. Vì vậy, muốn thành công, kẻ tấn công phải di chuyển ít nhất $SM + \epsilon$ REP. Để đơn giản, chúng ta sẽ bỏ qua ϵ không đáng kể, và nói rằng một cuộc tấn công thành công đòi hỏi phải di chuyển ít nhất SM REP, có giá trị SMP trước khi di chuyển, tới một số vũ trụ False.

Nếu kẻ tấn công chuyển SM REP trong khoảng thời gian báo cáo của một fork, kẻ đó sẽ nhận được SM REP trên vũ trụ con chuyển tới. [24] Nếu kẻ tấn công di chuyển đến vũ trụ False thì giá trị của những coin đó sẽ trở thành SMP_f. Do đó chi phí tối thiểu cho kẻ tấn công là $(P - P_f)SM$.

Chú ý 2. Số lượng tối thiểu REP một kẻ tấn công thành công phải di chuyển đến vũ trụ False trong một fork là SM, chi phí cho kẻ tấn công $(P - P_f)SM$.

Lưu ý rằng nếu $S > \frac{1}{2}$ thì một cuộc tấn công là *không thể* vì không có đủ REP bên ngoài vũ trụ True để bất kỳ vũ trụ False nào trở thành vũ trụ chiến thắng.

Với những kẻ tấn công hợp lý về mặt kinh tế, oracle sẽ giải quyết các kết quả tương ứng với thực tế khách quan nếu lợi ích tối đa của kẻ tấn công thấp hơn chi phí tấn công tối thiểu. Theo quan sát 1& 2 chúng ta có thể thấy rằng điều này xảy ra bất cứ khi nào $S > \frac{1}{2}$ or $I_a + I_p < (P - P_f)SM$. Điều này cho chúng ta định nghĩa chính thức về tính toàn vẹn.

Định nghĩa 4. (Thuộc tính Toàn vẹn) Giao thức forking có *tính toàn vẹn* bất cứ khi nào $S > \frac{1}{2}$ hoặc bất cứ khi nào $I_a + I_p < (P - P_f)SM$.

Bất đẳng thức trên có thể được giải quyết cho PM để xem xét mối quan hệ giữa tính toàn vẹn giao thức giả định và giới hạn thị trường của REP.

Định lý 1. *(Định lý Bảo mật Tổng Vốn Hóa Thị Trường) Giao thức forking có tính toàn vẹn nếu và chỉ khi:*

1. $S > \frac{1}{2}$, *hoặc*
2. $P_f < P$ *và giá trị thị trường của REP lớn hơn* $\frac{(I_a + I_p)P}{(P - P_f)S}$.

Chứng minh. Giả sử giao thức forking có tính toàn vẹn. Sau đó, theo định nghĩa, $S > \frac{1}{2}$ hoặc $I_a + I_p < (P - P_f)SM$. Giả sử $I_a + I_p < (P - P_f)SM$. Vì $I_a + I_p \geq 0$ and $SM > 0$, chúng ta biết $P_f < P$. Sau đó, giải $I_a + I_p <$

[22] Một *attorep* là 10^{-18} REP.

[23] Có thể có trường hợp một số reporter không độc hại di chuyển REP đến vũ trụ False một cách vô tình hoặc bất cẩn. Tuy nhiên, hành vi như vậy là, trên thực tế, không thể phân biệt được khi cộng tác với kẻ tấn công.

[24] Trong thực tế, kẻ tấn công sẽ nhận được $1.05S$ REP trong vũ trụ con vì 5% là tiền thưởng để di chuyển trong vòng 60 ngày kể từ ngày bắt đầu fork. Chúng tôi bỏ qua phần thưởng 5% ở đây để dễ dàng thảo luận. Để xem một cuộc thảo luận bao gồm tiền thưởng 5%, xem Phụ lục **??**.

$(P - P_f)SM$ cho PM, chúng ta thấy $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Vì vậy, hướng đầu tiên được chứng minh.

Bây giờ giả sử rằng $S > \frac{1}{2}$, hoặc $P_f < P$ và $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$. Nếu $S > \frac{1}{2}$, thì giao thức forking có tính toàn vẹn theo định nghĩa. Nếu $P_f < P$ và $\frac{(I_a+I_p)P}{(P-P_f)S} < PM$, thì giải quyết bất đẳng thức cho $I_a + I_p$, chúng ta thấy $I_a + I_p < (P - P_f)SM$, và giao thức forking có tính toàn vẹn. □

B. Giả Định Của Chúng Tôi Và Hệ Quả Của Chúng

Chúng tôi tin rằng các nhà giao dịch sẽ không muốn giao dịch trên Augur trong một vũ trụ nơi các reporter đã nói dối. Chúng tôi cũng tin rằng những người sáng tạo trên thị trường sẽ không trả tiền để tạo ra thị trường Augur trong một vũ trụ không có người giao dịch. Trong một vũ trụ không có thị trường hoặc giao dịch, REP không cung cấp bất kỳ cổ tức nào cho những người nắm giữ nó. Do đó, chúng tôi tin rằng REP được gửi đến vũ trụ False sẽ không giữ giá trị thị trường không đáng kể và chúng tôi mô hình hóa điều này bằng cách cho phép $P_f = 0$.

Chúng tôi cho rằng hoàn toàn hợp lý khi mong chờ ít nhất 20% REP hiện tại được di chuyển đến Kết quả thực sự trong giai đoạn báo cáo của fork, và chúng tôi mô hình hóa điều này bằng cách cho phép $S \geq \frac{1}{5}$. Chúng tôi cũng sẵn sàng đáp ứng lợi tức mở ký sinh lớn đến 50% lợi tức mở gốc, và vì vậy chúng tôi để $I_a \geq 2I_p$.

Theo các giả định này, Định lý 1 cho chúng ta biết rằng giao thức forking có tính toàn vẹn bất cứ khi nào giá trị thị trường mũ của REP đạt ít nhất 7,5 lần lợi tức mở gốc.[25]

C. Vốn Hóa Thị Trường Nudges

Cách Augur lấy thông tin về giá REP cũng giống cách mà nó nhận được bất kỳ thông tin nào khác về thế giới thực: thông qua một thị trường Augur. Điều này cho phép Augur khả năng tính toán vốn hóa thị trường hiện tại của REP. Augur cũng có thể đo lường lợi tức mở gốc hiện tại, và do đó có thể xác định giới hạn thị trường nào cần được nhắm mục tiêu để đáp ứng các yêu cầu về tính toàn vẹn của Augur.

Mỗi vũ trụ bắt đầu với phí báo cáo mặc định là 1%. Nếu giá thị trường hiện tại thấp hơn mục tiêu, thì phí báo cáo sẽ tự động tăng (nhưng sẽ không bao giờ cao hơn 33,3%), gây áp lực lên giá REP và / hoặc giảm áp lực lên lợi tức mở gốc mới. Nếu giá trị vốn hóa thị trường hiện tại cao hơn mục tiêu, thì phí báo cáo sẽ tự động giảm (nhưng sẽ không bao giờ thấp hơn 0,01%) để các nhà giao dịch không phải trả nhiều hơn mức cần thiết để giữ an toàn cho hệ thống.

Phí báo cáo được xác định như sau. Giải sử r là phí báo cáo từ cửa sổ trước đó, giải sử t là giá trị vốn hóa thị trường mục tiêu, giải sử c là giá trị vốn hóa thị trường hiện tại. Sau đó, phí báo cáo cho cửa sổ phí hiện tại được đưa ra bởi $\max\left\{\min\left\{\frac{t}{c}r, \frac{333}{1000}\right\}, \frac{1}{10,000}\right\}$.

D. Tận Dụng Mối Đe Dọa Của Một Fork

Như đã đề cập ở trên, fork là một bước đột phá và và một cách để thị trường dần dần được hoàn thành. Thay vì sử dụng quy trình forking để giải quyết mọi thị trường, Augur tận dụng *mối đe dọa* của một fork để giải quyết thị trường một cách hiệu quả.

Ở trên cũng đã đề cập rằng bất kỳ cổ phần nào tranh luận thành công một kết quả có lợi cho kết quả cuối cùng của thị trường sẽ nhận được 50% ROI trên cổ phần tranh luận của họ.[26] Trong trường hợp của một fork, bất kỳ REP đặt cược vào bất kỳ kết quả sai của thị trường sẽ mất tất cả giá trị kinh tế, trong khi bất kỳ REP nào được đặt trên kết quả đúng của thị trường được thưởng thêm 50% REP trong vũ trụ con tương ứng với kết quả thực sự của thị trường (bất kể kết quả của fork). Do đó, nếu được đẩy lên một fork, các chủ sở hữu REP tranh luận kết quả sai ủng hộ cho kết quả đúng sẽ luôn đi trước, trong khi người nắm REP đặt cược vào kết quả sai sẽ thấy REP mất tất cả giá trị kinh tế.

Chúng tôi tin rằng tình trạng này là đủ để đảm bảo rằng tất cả các kết quả dự kiến sai sẽ được tranh luận thành công.

III. CÁC VẤN ĐỀ TIỀM NĂNG & RỦI RO

A. Thị Trường Ký Sinh

Ở trên cũng đã đề cập một thị trường ký sinh là bất kỳ thị trường nào không trả phí báo cáo cho Augur, nhưng lại giải quyết theo độ phân giải của thị trường Augur nguyên bản. Bởi vì thị trường ký sinh không có bất kỳ reporter nào để trả tiền, họ có thể cung cấp dịch vụ tương tự như Augur với mức phí thấp hơn. Điều này có thể gây ra những hậu quả nghiêm trọng cho tính toàn vẹn của giao thức forking của Augur.

Đặc biệt, nếu các thị trường ký sinh thu hút sự quan tâm về giao dịch ra khỏi Augur, thì các reporter của Augur sẽ nhận được ít phí báo cáo hơn. Điều này sẽ tạo áp lực giảm giá đối với thị trường của REP. Nếu giá trị thị trường của REP giảm quá thấp, tính toàn vẹn của

[25] Xem Phụ lục B đối với một số các giả định thay thế và hậu quả của chúng.

[26] Được đo bằng REP tồn tại trong vũ trụ tương ứng với kết quả cuối cùng của thị trường; xem Định lý 3 trong Phụ lục A.

giao thức forking bị đặt vào tình trạng nguy hiểm (Định lý 1). Kết quả là, các thị trường ký sinh có khả năng đe dọa khả năng tồn tại lâu dài của Augur, nên cần phải phản đối kịch liệt.

Cách bảo vệ tốt nhất của chúng tôi chống lại các thị trường ký sinh là làm cho giao dịch trên nền tảng Augur càng rẻ càng tốt (trong khi vẫn duy trì tính toàn vẹn của oracle), để giảm thiểu phần thưởng cho việc chạy một thị trường ký sinh.

B. Biến Động Của Lợi Tức Mở

Sự gia tăng lớn, đột ngột, và bất ngờ của lợi tức mở – giống như những gì có thể được nhìn thấy trong một sự kiện thể thao phổ biến – dẫn đến sự gia tăng nhanh chóng yêu cầu về thị trường cho tính toàn vẹn giao thức giả định (Định lý 1). Khi yêu cầu về vốn hóa thị trường vượt quá giới hạn thị trường, có nguy cơ những kẻ tấn công hợp lý về kinh tế gây ra một fork để giải quyết không chính xác. Trong khi Augur cố gắng đẩy giá thị trường mũ lên trong các tình huống như vậy (xem phần II C), các cách thức này là không hợp lệ và chỉ được điều chỉnh một lần trong mỗi cửa sổ phí 7 ngày.

Điều đó không mang lại lợi ích gì, tuy nhiên, điều đáng chú ý là các nhà đầu cơ chứng kiến sự gia tăng đột ngột về lợi tức mở có thể mua REP với dự đoán mức trần và phản ứng của thị trường, do đó đẩy giá thị trường của REP lên, đó có lẽ là điểm mà tính toàn vẹn của giao thức fork không còn bị đe dọa nữa. Vì vậy, khoảng thời gian oracle dễ bị tổn thương có thể không đủ dài để kẻ tấn công khai thác thành công lỗ hổng này.

C. Các Nguồn Phân Giải Không Phù Hợp Hoặc Độc Hại

Trong quá trình tạo thị trường, người tạo thị trường đã chọn nguồn giải pháp mà các reporter nên sử dụng để xác định kết quả của sự kiện được đề cập. Nếu người tạo thị trường chọn nguồn giải quyết không phù hợp hoặc độc hại, các reporter trung thực có thể mất tiền.

Ví dụ, giả sử thị trường được đề cập có kết quả A và B, và người tạo thị trường, Serena, đã chọn trang web của riêng mình, attacker.com, làm nguồn giải pháp. Sau khi kết thúc sự kiện của thị trường, Serena - người cũng là reporter được chỉ định cho thị trường - báo cáo kết quả A và cập nhật attacker.com để chỉ ra rằng kết quả B là kết quả chính xác. Các reporter trung thực kiểm tra attacker.com sẽ thấy rằng báo cáo ban đầu là không chính xác và trong suốt vòng tranh luận đầu tiên, nên tranh luận thành công kết quả dự kiến có lợi cho kết quả B. Serena sẽ cập nhật attacker.com để chỉ ra rằng kết quả A là kết quả chính xác, và thị trường sau đó sẽ tham gia vòng tranh luận thứ hai của nó. Một lần nữa, các reporter kiểm tra attacker.com sẽ thấy rằng kết quả dự kiến (kết quả B) là không chính xác và có thể tranh luận thành công. Serena có thể lặp lại hành vi này cho đến khi thị trường giải quyết. Dù thị trường giải quyết thế nào, thì một số reporter trung thực cũng sẽ mất tiền.

Một số biến thể của cuộc tấn công này tồn tại. Chỉ đơn giản là bỏ qua các thị trường với các nguồn phân giải không rõ ràng là không đủ, trong trường hợp thị trường như vậy gây ra một fork, tất cả các chủ sở hữu REP sẽ phải chọn một vũ trụ con để di chuyển REP của họ. Các reporter nên cảnh giác với các thị trường với các nguồn phân giải không rõ ràng. Các thị trường như vậy phải được xác định công khai để các reporter có thể phối hợp để đảm bảo các thị trường đó hoàn thành là không hợp lệ.

D. Truy Vấn Oracle Tự Tham Khảo

Các thị trường giao dịch về hành vi tương lai của oracle của Augur có thể có những tác động không mong muốn đối với hành vi của chính oracle [11]. Ví dụ, hãy xem xét một thị trường giao dịch trên câu hỏi, "Liệu có bất kỳ reporter được chỉ định nào không gửi báo cáo trong khoảng thời gian báo cáo ba ngày trước ngày 31 tháng 12 năm 2018 hay không?" Đặt cược vào kết quả Không của thị trường này có thể đóng vai trò như một sự khuyến khích sai lầm cho các reporter được chỉ định cố ý không báo cáo. Nếu một reporter được chỉ định có thể mua đủ Có cổ phiếu với mức giá đủ thấp để bù đắp cho sự mất mát của liên kết không hiển thị, họ có thể cố tình không báo cáo.

Nếu giá trị thị trường của REP đủ lớn (Định lý 1) thì các truy vấn oracle tự tham chiếu này sẽ không đe dọa tính toàn vẹn của giao thức forking. Tuy nhiên, chúng có thể ảnh hưởng tiêu cực đến hiệu suất của Augur bằng cách gây ra sự chậm trễ trong việc hoàn thành thị trường. Trong khi thị trường vẫn hoàn thành chính xác, loại hành vi này là gây rối và không được chấp nhận.

E. Không Chắc Chắn Tham Gia Fork

Chúng ta không thể biết trước bao nhiêu REP sẽ được chuyển đến vũ trụ True trong giai đoạn phân tách của một fork, vì vậy chúng ta không thể biết trước liệu thị trường mũ có đủ lớn để oracle có tính toàn vẹn hay không (Định lý 1). Chúng tôi tin rằng tính toàn vẹn của giao thức forking có thể không mạnh hơn niềm tin của chúng tôi trong các giả định của chúng tôi về mức độ ràng buộc thấp hơn về sự tham gia trung thực trong một giai đoạn fork. Chúng tôi giả định rằng ít nhất 20% của tất cả REP sẽ di chuyển đến vũ trụ con True trong thời gian phân tách của một fork, nhưng chúng tôi không thể đảm bảo điều này.

Augur fork khác với blockchain fork: sau một blockchain fork, một người dùng sở hữu một con trên chuỗi cái bây giờ sẽ sở hữu một coin trên cả hai nhánh. Bỏ qua các cuộc tấn công lập lại, blockchain fork đặt ra ít rủi ro cho người dùng. Tuy nhiên, sau một Augur fork, một người dùng sở hữu một token REP trong vũ trụ cái

có thể di chuyển coin đó đến một trong những vũ trụ con. Nếu người dùng di chuyển token của họ đến bất kỳ vũ trụ nào khác ngoài vũ trụ tương đương, token của họ có thể mất tất cả giá trị. Do đó, việc di chuyển REP trong giai đoạn cố định của một fork, trước khi nó rõ ràng là vũ trụ con đã đạt được sự đồng thuận, cho thấy người dùng có nguy cơ. Rủi ro đó có thể ngăn cản sự tham gia giai đoạn phân tách của các fork tiếp theo.

Trong nỗ lực bù đắp rủi ro này và khuyến khích tham gia trong giai đoạn phân tách, tất cả các chủ token chuyển REP của họ trong vòng 60 ngày kể từ ngày bắt đầu một fork sẽ nhận được thêm 5% REP trong vũ trụ con mà họ di chuyển (xem Phần **??**). Tuy nhiên, chúng tôi không thể biết trước liệu khoản tiền thưởng 5% này có đủ để bù đắp rủi ro và khuyến khích tham gia trong giai đoạn chia tách hay không.

F. Thị Trường Mơ Hồ Hoặc Chủ Quan

Chỉ những sự kiện có kết quả có thể biết được một cách khách quan mới phù hợp để sử dụng trong thị trường Augur. Nếu các reporter tin rằng thị trường không thích hợp để giải quyết bởi nền tảng - ví dụ, bởi vì nó mơ hồ, chủ quan hoặc kết quả không được biết đến trong ngày kết thúc sự kiện - họ nên báo cáo thị trường là Không hợp lệ . Nếu thị trường giải quyết dưới dạng Không hợp lệ, các nhà giao dịch được thanh toán với giá trị bằng nhau cho tất cả các kết quả có thể có; đối với thị trường vô hướng, thương nhân được trả một nửa của giá tối thiểu và giá tối đa của thị trường.

Đó có thể là thị trường tưởng tượng nơi một số reporter chắc chắn rằng kết quả là A và những người khác chắc chắn rằng kết quả là B. Ví dụ, năm 2006, TradeSports cho phép người dùng suy đoán xem liệu Bắc Triều Tiên sẽ phóng một tên lửa đạn đạo ra ngoài không phận trước cuối tháng 7/2006 hay không. Vào ngày 5 tháng 7 năm 2006, Bắc Triều Tiên phóng thành công một tên lửa đạn đạo hạ cánh bên ngoài không phận, và sự kiện đã được báo cáo rộng rãi bởi giới truyền thông thế giới và được xác nhận bởi nhiều nguồn của chính phủ Hoa Kỳ. Tuy nhiên, Bộ Quốc phòng Mỹ đã không xác nhận sự kiện, theo yêu cầu của hợp đồng TradeSports. TradeSports kết luận rằng các điều kiện của hợp đồng chưa được đáp ứng và được thanh toán tương ứng.[27]

Đây là trường hợp mà tinh thần của thị trường – để dự đoán việc phóng tên lửa – rõ ràng là hài lòng, nhưng ngôn ngữ của thị trường – để dự đoán liệu Bộ Quốc phòng Hoa Kỳ có xác nhận việc phóng tên lửa – hay không. TradeSports, là một trang web tập trung, đã có thể đơn phương tuyên bố kết quả của thị trường. Nếu một tình huống như vậy phát sinh trong thị trường Augur, người nắm giữ REP có thể có những ý kiến khác nhau về cách thị trường nên giải quyết, và đặt REP của họ cho phù hợp. Trong trường hợp xấu nhất, điều này có thể dẫn đến một fork nơi REP trong nhiều hơn một vũ trụ con duy trì một giá trị thị trường khác không.

LỜI CẢM ƠN

Chúng tôi cảm ơn Abraham Othman, Alex Chapman, Serena Randolph, Tom Haile, George Hotz, Scott Bigelow và Peronet Despeignes vì những phản hồi và góp ý hữu ích của họ.

[1] J. Wolfers and E. Zitzewitz. Prediction markets. *Journal of Economic Perspectives*, 18(2):107–126, 2004.

[2] James Surowiecki. *The Wisdom of Crowds*. Anchor, 2005.

[3] R. Hanson, R. Oprea, and D. Porter. Information aggregation and manipulation in an experimental market. *Journal of Economic Behavior & Organization*, 60(4):449–459, 2006.

[4] D.M. Pennock, S. Lawrence, C.L. Giles, and F.A. Nielsen. The real power of artificial markets. *Science*, 291:987–988, 2001.

[5] C. Manski. Interpreting the predictions of prediction markets. *NBER Working Paper No. 10359*, 2004.

[6] J. Wolfers and E. Zitzewitz. Interpreting prediction market prices as probabilities. *NBER Working Paper No. 10359*, 2005.

[7] S. Goel, D.M. Reeves, D.J. Watts, and D.M. Pennock. Prediction without markets. In *Proceedings of the 11th ACM Conference on Electronic Commerce*, EC '10, pages 357–366. ACM, 2010.

[8] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf*, 2008.

[9] V. Buterin. A next generation smart contract and decentralized application platform. *https://github.com/ethereum/wiki/wiki/White-Paper*, 2013.

[10] J. Clark, J. Bonneau, E.W. Felten, J.A. Kroll, A. Miller, and A. Narayanan. On decentralizing prediction markets and order books. In *WEIS '14: Proceedings of the 10th Workshop on the Economics of Information Security*, June 2014.

[11] A. Othman and T. Sandholm. Decision rules and decision markets. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: Volume 1 - Volume 1*, AAMAS '10, pages 625–632. International Foundation for Autonomous Agents and Multiagent Systems, 2010.

[12] J. Peterson and J. Krug. Augur: a decentralized, open-source platform for prediction markets. *arXiv:1501.01042v1 [cs.CR]*, 11 2014.

[27] Xem https://en.wikipedia.org/wiki/Intrade#Disputes để biết chi tiết.

Phụ lục A: Thời Gian Hoàn Tthành & Phân Phối Lại

Chúng tôi bắt đầu với một số ký hiệu, định nghĩa và quan sát.

Định nghĩa 5. Với một thị trường nhất định M, giả sử Ω_M là không gian kết quả (hoặc thiết lập các kết quả) là M.

Định nghĩa 6. Với $n \geq 1$ và $\omega \in \Omega_M$, giả sử $S(\omega, n)$ biểu thị tổng số tiền đặt cược vào kết quả ω khi bắt đầu vòng tranh luận n. Điều này bao gồm tất cả các cổ phần từ tất cả các liên kết tranh luận thành công có lợi cho ω trên tất cả các vòng tranh luận trước đó.

Định nghĩa 7. Với $n \geq 1$ và $\omega \in \Omega_M$, giả sử $S(\overline{\omega}, n)$ biểu thị số lượng cổ phần trên tất cả các kết quả trong Ω_M *ngoại trừ* ω khi bắt đầu vòng tranh luận n:

$$S(\overline{\omega}, n) = \sum_{\substack{\gamma \in \Omega_M \\ \gamma \neq \omega}} S(\gamma, n)$$

Định nghĩa 8. Với $n \geq 1$, giả sử A_n biểu thị tổng số cổ phần trên tất cả các kết quả M khi bắt đầu vòng tranh luận n:

$$A_n = \sum_{\omega \in \Omega_M} S(\omega, n)$$

Chú ý 3. Theo sau là $A_n - S(\omega, n) = S(\overline{\omega}, n)$.

Định nghĩa 9. Với $n \geq 1$, giả sử $\hat{\omega}_n$ biểu thị kết quả dự kiến lúc bắt đầu vòng tranh luận n. Ví dụ, $\hat{\omega}_1$ là kết quả được báo cáo bởi báo cáo ban đầu.

Định nghĩa 10. Với $n \geq 1$ và $\omega \neq \hat{\omega}_n$, giả sử $B(\omega, n)$ biểu thị số tiền cổ phần cần thiết để điền thành công một liên kết tranh luận có lợi cho kết quả ω trong vòng tranh luận n.

Như đã đề cập ở trên, số tiền cổ phần cần thiết để điền thành công một liên kết tranh luận có lợi cho kết quả ω trong vòng tranh luận n, trong đó $\omega \neq \hat{\omega}_n$ được cho bởi Phương trình. 1, $B(\omega, n) = 2A_n - 3S(\omega, n)$.

Chú ý 4. Nếu một liên kết tranh luận được điền thành công trong ủng hộ kết quả ω trong vòng tranh luận n, thì $S(\omega, n+1) = B(\omega, n) + S(\omega, n)$. Tức là, cổ phần tranh luận thành công là cổ phần mới duy nhất được áp dụng cho kết quả ω vào cuối vòng tranh luận n.

Chú ý 5. Với tất cả $\omega \neq \hat{\omega}_n, S(\omega, n-1) = S(\omega, n)$. Tức là, nếu một liên kết tranh luận không được điền đầy đủ ủng hộ của kết quả ω, thì không có thêm cổ phần nào được thêm vào kết quả ω vào đầu vòng tranh luận tiếp theo. Điều này là do thực tế rằng tất cả cổ phần tranh luận không thành công được trả lại cho người dùng vào cuối vòng tranh luận.

Chú ý 6. Với tất cả $n \geq 2, A_n = A_{n-1} + B(\hat{\omega}_n, n-1)$. Tức là, tổng số cổ phần trên tất cả các kết quả vào đầu một vòng tranh luận chỉ đơn giản là tổng số cổ phần từ đầu của vòng tranh luận trước cộng với cổ phần tranh luận thành công từ vòng tranh luận trước đó. Tất cả các cổ phần khác được trả lại cho người dùng vào cuối vòng tranh luận trước đó.

Bổ đề 2. $S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$, *for* $n \geq 2$.

Chứng minh. Giả sử một thị trường tham gia tranh luận vòng n, trong đó $n \geq 2$. Trong vòng tranh luận $n-1$, kết quả $\hat{\omega}_{n-1}$phải được tranh luận thành công vì lợi ích của kết quả $\hat{\omega}_n$. Theo Phương trình. 1, kích thước của liên kết tranh luận đó là $B(\hat{\omega}_n, n-1) = 2A_{n-1} - 3S(\hat{\omega}_n, n-1)$. Chú ý 3, điều này có thể được viết lại thành

$$B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = 2S(\overline{\hat{\omega}_n}, n-1) \qquad \text{(A1)}$$

Chúng tôi biết rằng liên kết tranh luận đã được thực hiện thành công trong vòng $n-1$. Chú ý 4, chúng ta thấy rằng $B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = S(\hat{\omega}_n, n)$. Chú ý 5 cho chúng ta biết rằng tổng số tiền đặt cược trên $\overline{\hat{\omega}_n}$ không thay đổi từ vòng $n-1$ đến n, $2S(\overline{\hat{\omega}_n}, n-1) = 2S(\overline{\hat{\omega}_n}, n)$. Vì vậy, Phương trình. A1 giảm xuống $S(\hat{\omega}_n, n) = 2S(\overline{\hat{\omega}_n}, n)$. □

Định lý 3. *Bất kỳ người giữ REP nào tranh luận kết quả thành công có lợi cho kết quả cuối cùng của thị trường sẽ nhận được 50% ROI trên cổ phần tranh luận của họ (được đo bằng REP tồn tại trong vũ trụ tương ứng với kết quả cuối cùng của thị trường), trừ khi thị trường bị gián đoạn bởi một số thị trường khác gây ra một fork.*

Chứng minh. Trong suốt một fork, tất cả những người dùng thành công trong việc điền liên kết tranh luận có lợi cho kết quả cuối cùng của thị trường phân tách (thông qua coin được tao ra trong suốt một fork) 50% lợi nhuận của họ khi họ chuyển cổ phần tranh luận của họ đến vũ trụ tương ứng. Do đó, trong trường hợp thị trường được đề cập đã gây ra một fork, định lý là đúng ngay lập tức. Bây giờ hãy xem xét trường hợp thị trường giải quyết câu hỏi mà không gây ra một fork, và báo cáo không bị gián đoạn bởi một số thị trường khác gây ra một fork.
Biểu thị kết quả cuối cùng của thị trường bởi ω_{Final} và giả sử thị trường giải quyết vào cuối vòng tranh luận n, trong đó $n \geq 2$. Điều đó có nghĩa là kết quả dự kiến cho vòng n là ω_{Final}, và kết quả đó không được tranh luận thành công trong vòng n. Nói cách khác: $\hat{\omega}_n = \omega_{\text{Final}}$. Sau đó, bởi Bổ đề 2 chúng ta biết rằng $S(\omega_{\text{Final}}, n) = 2S(\overline{\omega_{\text{Final}}}, n)$.
Vì thị trường quyết định vào cuối vòng n mà không có thêm cổ phần nào cho bất kỳ kết quả nào, phương trình trên cho thấy số tiền cuối cùng của cổ phần trên kết quả cuối cùng của thị trường, ω_{Final}, và tổng tất cả các cổ phần trên tất cả các kết quả khác của thị trường, $\overline{\omega_{\text{Final}}}$. Lưu ý rằng có sự chính xác gấp đôi số cổ phần trên kết quả cuối cùng của thị trường khi có tất cả các kết quả khác kết hợp.
Augur phân phối lại tất cả các cổ phần trên các kết quả không hoàn thành cho người dùng đã đặt cược ω_{Final}, tương ứng với số lượng REP họ đặt cược. Do đó, những

người dùng đã thực hiện thành công một liên kết tranh luận ủng hộ ω_{Final} nhận được ROI 50% trên REP được đặt cược của họ. □

Tiếp theo, hãy xem xét số vòng tranh luận tối đa cần thiết để giải quyết thị trường. Phương trình. 1 được giảm thiểu khi ω được chọn là kết quả ngoài dự kiến khi bắt đầu vòng tranh luận với số tiền lớn nhất. Bổ đề 2 ngụ ý rằng kết quả không mang tính dự kiến với số lượng cổ phần lớn nhất là kết quả dự kiến của vòng tranh luận trước đó. Do đó, kích thước liên kết tranh luận nhỏ nhất có thể được thực hiện thành công trong vòng tranh luận n, trong đó n $geq2$, là $B(\hat{\omega}_{n-1}, n)$. Nói cách khác, kích thước liên kết tranh luận tăng lên *chậm nhất* khi hai kết quả giống nhau liên tục bị tranh luận có lợi cho nhau. Sau đó, số vòng tranh luận cần thiết cho một thị trường để bắt đầu một fork là *tối đa* khi hai kết quả giống nhau liên tục bị tranh luận có lợi cho nhau. Do đó chúng ta có thể xác định số vòng tranh luận tối đa mà bất kỳ thị trường nào có thể trải qua trước khi bắt đầu một fork bằng cách tìm số vòng tranh luận tối đa có thể xảy ra trong trường hợp cụ thể mà hai kết quả thị trường đó liên tục tranh luận. Chúng ta sẽ kiểm tra trường hợp đó ngay bây giờ.
Giả sử rằng tất cả các liên kết tranh luận thành công được điền ủng hộ cho kết quả dự kiến của vòng tranh luận trước đó. Sau đó, hai kết quả dự kiến được lặp lại có lợi cho nhau là $\hat{\omega}_1$ và $\hat{\omega}_2$.

Chú ý 7. Trong trường hợp hai kết quả dự kiến tương tự liên tục bị tranh luận với nhau, $\hat{\omega}_n = \hat{\omega}_{n-2}$ for all $n \geq 3$.

Định nghĩa 11. Giả sử d biểu thị số tiền đặt cược trên $\hat{\omega}_1$ trong báo cáo ban đầu. Bởi vì kết quả dự kiến cho mỗi vòng được biết đến trong tình huống này, chúng ta có thể đơn giản hóa ký hiệu của chúng ta cho các kích thước liên kết tranh luận. Xác định viết tắt B_n để biểu thị kích thước trái phiếu được yêu cầu cho vòng n, sao cho $B_1 = 2d$ và $B_n = B(\hat{\omega}_{n-1}, n)$ cho tất cả $n \geq 2$. Điều này sẽ làm cho việc đọc và hiểu dễ dàng hơn.

Chú ý 8. Trong trường hợp hai kết quả dự kiến tương tự liên tục bị tranh luận có lợi cho nhau, $S(\hat{\omega}_{n-1}, n) = S(\hat{\omega}_{n-1}, n-2) + B_{n-2}$ for $n \geq 3$. (Nghĩa là, mọi liên kết tranh luận thành công khác được thêm vào cùng một kết quả.)

Bổ đề 4. *Nếu hai kết quả dự kiến tương tự liên tục bị tranh luận có lợi cho nhau, thì đối với tất cả n trong đó* $n \geq 3$*:*

1. $S(\hat{\omega}_{n-1}, n) = \frac{2}{3}B_{n-1}$
2. $A_n = 2B_{n-1}$ *and*
3. $B_n = 3d2^{n-2}$

Chứng minh. (Bằng phương pháp quy nạp cho n)
Giả sử hai kết quả dự kiến giống nhau liên tục tranh luận nhau.
(Trường hợp cơ bản) Theo định nghĩa và Phương trình. 1 chúng ta thực hiện các quan sát sau đây.

- $S(\hat{\omega}_1, 1) = d$, $S(\hat{\omega}_2, 1) = 0$, $A_1 = d$, và $B_1 = 2d$
- $S(\hat{\omega}_1, 2) = d$, $S(\hat{\omega}_2, 2) = 2d$, $A_2 = 3d$, và $B_2 = 3d$
- $S(\hat{\omega}_1, 3) = 4d$, $S(\hat{\omega}_2, 3) = 2d$, $A_3 = 6d$, và $B_3 = 6d$

$S(\hat{\omega}_{3-1}, 3) = S(\hat{\omega}_2, 3) = 2d = \frac{2}{3}(3d) = \frac{2}{3}B_2 = \frac{2}{3}B_{3-1}$, do đó, phần 1 của bổ đề nắm giữ $n = 3$.
$A_3 = 6d = 2(3d) = 2B_2 = 2B_{3-1}$, do đó, phần 2 của bổ đề nắm giữ $n = 3$.
$B_3 = 6d = 3d2^{3-2}$, do đó, phần 3 của bổ đề nắm giữ $n = 3$.

Do đó, bổ đề, toàn bộ, đúng với trường hợp cơ bản của $n = 3$.

(Quy nạp) Giả sử bổ đề là đúng cho tất cả n sao cho $3 \leq n \leq k$. Chúng ta muốn cho thấy rằng bổ đề nắm giữ cho $n = k + 1$. Đó là, chúng ta muốn cho thấy rằng:

(a) $S(\hat{\omega}_k, k+1) = \frac{2}{3}B_k$

(b) $A_{k+1} = 2B_k$ and

(c) $B_{k+1} = 3d2^{k-1}$

Đầu tiên, chúng ta chứng minh phần (a). Theo quan sát 8:

$$S(\hat{\omega}_k, k+1) = S(\hat{\omega}_k, k-1) + B_{k-1}$$

Theo quan sát 7 ở trên chúng ta có thể viết lại là:

$$S(\hat{\omega}_{k-2}, k+1) = S(\hat{\omega}_{k-2}, k-1) + B_{k-1}$$

Theo giả thuyết quy nạp, chúng ta có thể viết lại $S(\hat{\omega}_{k-2}, k-1)$ thành $\frac{2}{3}B_{k-2}$ ở bên phía tay phải để có:

$$S(\hat{\omega}_{k-2}, k+1) = \frac{2}{3}B_{k-2} + B_{k-1}$$

Theo giả thuyết quy nạp, chúng ta có thể viết B_{k-2} as $3d2^{k-4}$ and B_{k-1} as $3d2^{k-3}$:

$$S(\hat{\omega}_{k-2}, k+1) = d2^{k-1}$$

Áp dụng quan sát 7 ở phía bên tay trái, chúng ta nhận được:

$$S(\hat{\omega}_k, k+1) = d2^{k-1}$$

Cuối cùng, lưu ý rằng bằng phương trình trên và giả thuyết quy nạp, $S(\hat{\omega}_k, k+1) = d2^{k-1} = \frac{2}{3}(3d2^{k-2}) = \frac{2}{3}B_k$. Phần (a) được chứng minh.
Tiếp theo, chúng ta chứng minh phần (b). Theo quan sát 6:

$$A_{k+1} = A_k + B_k$$

Theo giả thuyết quy nạp, $A_k = 2B_{k-1}$:

$$A_{k+1} = 2B_{k-1} + B_k$$

Theo giả thuyết quy nạp, $B_{k-1} = 3d2^{k-3}$, vì vậy phía bên tay phải có thể được đơn giản hóa thành

$$A_{k+1} = 3d2^{k-2} + B_k$$

Theo giả thuyết quy nạp, $B_k = 3d2^{k-2}$ để viết lại phía bên tay phải là

$$A_{k+1} = 2B_k,$$

và phần (b) được chứng minh.
Cuối cùng, chúng ta chứng minh phần (c). Theo Phương trình. 1:

$$B_{k+1} = 2A_{k+1} - 3S(\hat{\omega}_k, k+1)$$

Theo quan sát 8, chúng ta có thể viết $S(\hat{\omega}_k, k+1)$ as $S(\hat{\omega}_k, k-1) + B_{k-1}$:

$$B_{k+1} = 2A_{k+1} - 3\left(S(\hat{\omega}_k, k-1) + B_{k-1}\right)$$

Theo quan sát 7, $\hat{\omega}_k = \hat{\omega}_{k-2}$:

$$B_{k+1} = 2A_{k+1} - 3\left(S(\hat{\omega}_{k-2}, k-1) + B_{k-1}\right)$$

Theo quan sát 6, $A_{k+1} = A_k + B_k$:

$$B_{k+1} = 2\left(A_k + B_k\right) - 3\left(S(\hat{\omega}_{k-2}, k-1) + B_{k-1}\right)$$

Theo giả thuyết quy nạp, $A_k = 2B_{k-1}$ and $S(\hat{\omega}_{k-2}, k-1) = \frac{2}{3}B_{k-2}$:

$$B_{k+1} = 2\left(2B_{k-1} + B_k\right) - 3\left(\tfrac{2}{3}B_{k-2} + B_{k-1}\right)$$

Theo giả thuyết quy nạp, $B_k = 3d2^{k-2}$, $B_{k-1} = 3d2^{k-3}$ and $B_{k-2} = 3d2^{k-4}$. Thực hiện các thay thế này và đơn giản hóa sản lượng:

$$B_{k+1} = 3d2^{k-1}$$

Phần (c) được chứng minh, và kết luận bổ đề được chứng minh. □

Định lý 5. *Nếu không bị gián đoạn bởi một số thị trường khác gây ra một fork, một thị trường có thể trải qua tối đa 20 vòng tranh luận trước khi hoàn thành hoặc gây ra một fork.*

Chứng minh. Giả sử rằng một thị trường nhất định không bị gián đoạn bởi một số thị trường khác gây ra một fork. Sau đó, như được trình bày ở trên, chúng ta biết rằng số lượng vòng tranh luận cần thiết cho thị trường để bắt đầu fork được tối đa hóa khi hai kết quả giống nhau liên tục bị tranh luận có lợi cho nhau. Phần 3 của Bổ đề 4 cho chúng ta biết rằng, trong trường hợp này, kích thước liên kết tranh luận cần thiết để tranh luận thành công kết quả dự kiến trong vòng n được cho bởi $3d2^{n-2}$, trong đó d là số tiền đặt cọc trong báo cáo ban đầu.
Chúng ta biết rằng các fork được bắt đầu sau khi thực hiện thành công một liên kết tranh luận với kích thước ít nhất là 2,5% của tất cả REP hiện có và chúng ta cũng biết rằng có khoảng 11 triệu REP tồn tại. Do đó một fork được bắt đầu khi một liên kết tranh luận có kích thước 275,000 REP được lấp đầy. Chúng ta cũng biết rằng $d \geq 0,35$ REP, vì số tiền tối thiểu của cổ phần trên báo cáo ban đầu là 0.35 REP[28].
Giải $3(0.35)2^{n-2} > 275,000$ cho $n \in \mathbb{Z}$ yields $n \geq 20$. Vì vậy, chúng ta có thể đảm bảo rằng một thị trường sẽ giải quyết hoặc gây ra một fork sau khi có tối đa 20 vòng tranh luận. □

Phụ lục B: AlCác Giả Định Thay Thế & Hệ quả

Như đã đề cập ở trên:

- S là tỷ lệ tổng số REP được chuyển đến vũ trụ True trong thời gian chờ đợi
- P là giá REP trong vũ trụ True
- P_f là giá REP đã được chuyển đến vũ trụ False của lựa chọn của kẻ tấn công
- I_a là lợi tức mở gốc của Augur
- I_p là lợi tức mở ký sinh

Augur đưa ra các giả định nhất định về S, P_f, và I_p để đạt được giới hạn thị trường mục tiêu. Cụ thể, Augur giả định rằng ít nhất 20% của tất cả REP sẽ được chuyển đến vũ trụ True trong giai đoạn phân tách của một fork, REP di chuyển đến vũ trụ False sẽ không có, hoặc có giá trị không đáng kể , và lợi tức mở ký sinh tối đa sẽ là một nửa số lợi tức mở gốc. Nói cách khác: $S \geq 0.2$, $P_f = 0$, and $I_a \geq 2I_p$. Theo các giả định này, Định lý 1 cho chúng ta biết rằng giao thức forking có tính toàn vẹn bất cứ khi nào giá trị thị trường của REP lớn hơn 7,5 lần lợi tức mở gốc.
Bạn có thể đưa ra các giả định của riêng bạn về S, P_f và I_p để đi đến kết luận của riêng bạn về mức độ cần thiết của thị trường cho oracle để có tính toàn vẹn trong thực tế. Chúng tôi liệt kê một số kịch bản thay thế ở đây để thuận tiện cho bạn.

Kịch bản 1. Hơn 50% REP hiện có chuyển đến vũ trụ True trong thời gian phân tách. Trong trường hợp này P_f và I_p không quan trọng chút nào. Vì $S > \frac{1}{2}$, giao thức forking có tính toàn vẹn bất kể giá trị thị trường là bao nhiêu. Sẽ không có đủ REP còn lại trên thị trường để kẻ tấn công thành công.

Kịch bản 2. 48% REP hiện tại chuyển đến vũ trụ True trong thời gian phân tách, không có thị trường ký sinh tồn tại và REP được gửi tới vũ trụ False không có giá trị. Trong trường hợp này $S = 0.48$, $I_p = 0$, and $P_f = 0$.Theo các giả định này, giới hạn thị trường của REP phải lớn hơn gấp đôi lợi tức mở gốc của giao thức forking để có tính toàn vẹn.

[28] Xem phần phụ lục E 2 và E 3

Kịch bản 3. 20% 20% REP hiện tại di chuyển đến vũ trụ True trong thời gian phân tách, lợi tức mở ký sinh bằng lợi tức mở gốc và REP chuyển đến vũ trụ False ở mức 5% giá trị của REP đã di chuyển đến vũ trụ texttttTrue. Trong trường hợp này $S = 0.2$, $I_p = I_a$, and $P_f = 0.05P$. Theo các giả định này, vốn hóa thị trường của REP phải lớn hơn khoảng 10,5 lần lợi tức mở gốc đối với giao thức forking có tính toàn vẹn.

Kịch bản 4. Chỉ có 5% of REP hiện tại di chuyển đến vũ trụ True trong thời gian phân tách, lợi tức ký sinh lớn gấp đôi lợi tức mở gốc, và REP được gửi đến vũ trụ False giao dịch ở mức 5% của giá trị của REP được gửi đến vũ trụ True. Trong trường hợp này $S = 0.05$, $I_p = 2I_a$, và $P_f = 0.05P$. Theo các giả định này, vốn hóa thị trường của REP phải lớn hơn khoảng 63 lần lợi tức mở gốc của giao thức forking để có tính toàn vẹn.

Phụ lục C: Ảnh hưởng của Tiền thưởng sớm lên tính toàn vẹn của Giao thức Forking

Để dễ dàng thảo luận, chúng tôi đã bỏ qua phần thưởng việc chuyển tới sớm 5% và một thuật ngữ nhỏ khi thảo luận về tính toàn vẹn của giao thức forking. Ở đây chúng ta xem xét lại Định lý 1 xem xét hai điều đó.

Như đã đề cập ở trên, số lượng REP được gửi đến vũ trụ True trong thời gian báo cáo được biểu thị bằng SM. Vì vậy, để thành công, kẻ tấn công phải di chuyển ít nhất $SM + \epsilon$ REP, có giá trị $(SM + \epsilon)P$ trước khi chuyển tới một số vũ trụ False.

Nếu kẻ tấn công chuyển $SM + \epsilon$ REP vào vũ trụ False trong giai đoạn báo cáo của fork, sẽ nhận được $1,05(SM + \epsilon)$ REP trên vũ trụ con chuyển tới. Theo định nghĩa của P_f, giá trị của các coin được đưa ra bởi $1,05(SM + \epsilon)P_f$. Do đó chi phí tối thiểu cho kẻ tấn công là $(SM + \epsilon)P - 1.05(SM + \epsilon)P_f$, có thể được biểu thị bằng $(SM + \ epsilon)(P - 1.05P_f)$.

Như đã đề cập ở trên, lợi ích tối đa (tổng) cho kẻ tấn công được đưa ra bởi $I_a + I_p$. Do đó, chúng ta nói giao thức forking có tính toàn vẹn bất cứ khi nào $S > \frac{1}{2}$ hoặc:

$$I_a + I_p < (SM + \epsilon)(P - 1.05P_f) \tag{C1}$$

Giải quyết bất đẳng thức trên cho vốn hóa thị trường, PM, chúng ta có thể thấy rằng giao thức forking có tính toàn vẹn khi và chỉ khi:

1. $S > \frac{1}{2}$ hoặc
2. $1.05P_f < P$ và giới hạn thị trường của REP lớn hơn $\frac{P(I_a+I_p-\epsilon(P-1.05P_f))}{S(P-1.05P_f)}$

Như chúng ta có thể thấy, hiệu quả của tiền thưởng của việc chuyển tới sớm theo yêu cầu của thị trường là rất nhỏ.

Phụ lục D: Ảnh hưởng của việc chuyển Tiền thưởng tới sớm đối với Chi phí tối thiểu của một Fork

Để khuyến khích sự tham gia nhiều hơn trong một fork, tất cả những người có token muốn chuyển REP của họ trong vòng 60 ngày kể từ ngày bắt đầu một fork sẽ nhận được thêm 5% REP trong vũ trụ con mà họ chuyển tới. Phần thưởng này được trả thông qua lạm phát tiền tệ.

Tiền thưởng này có thể trở thành một ưu đãi sai lầm nếu chi phí bắt đầu một fork là quá thấp. Đặc biệt, nếu kẻ tấn công có thể nhận được nhiều giá trị hơn từ tiền thưởng 5% REP hơn là nhưng gì bị mất bằng cách bắt đầu một fork, khi đó chúng tôi hy vọng fork này sẽ xảy ra thường xuyên nhất có thể. Cuộc tấn công này, mà chúng tôi gọi là *tấn công lạm phát sữa*, sẽ không dẫn đến oracle báo cáo không chính xác, nhưng điều này sẽ khiến các fork bị gián đoạn và xảy ra thường xuyên.

Để ngăn chặn hành vi này, Augur cần đảm bảo rằng chi phí bắt đầu một fork lớn hơn giá trị tối đa có thể thu được từ tiền thưởng lạm phát 5%. Ở đây, chúng tôi nhận được một ràng buộc thấp hơn về chi phí bắt đầu một fork để ngăn chặn sự khuyến khích nghịch đảo này.

Giả sử P_0 biểu thị giá REP trước fork và P_1 biểu thị giá REP sau fork. Giả sử M_0 biểu thị nguồn cung tiền trước fork và M_1 biểu thị nguồn cung tiền sau fork. Giả sử S biểu thị tỷ lệ M_0 chuyển đến vũ trụ True trong thời gian phân tách của fork. Giả sử b biểu thị số lượng REP cần phải có (tức là, đặt cược vào kết quả False) để bắt đầu một fork. Chúng tôi giả định $b > 1$.

Vì mục đích của phần này, chúng tôi đưa ra giả định thận trọng rằng tất cả REP được chuyển trong giai đoạn phân tách được kiểm soát bởi kẻ tấn công. Chúng tôi tiếp tục giả định (vì nó giảm thiểu chi phí của cuộc tấn công này) rằng tất cả REP được chuyển trong giai đoạn phân tách đều được chuyển đến vũ trụ True.

Với ký hiệu này, SM_0 là số tiền REP được chuyển trong thời gian phân tách, trong khi $(1 - S)M_0$ là số REP *không* được di chuyển trong thời gian phân tách.

$$M_0 = SM_0 + (1 - S)M_0 \tag{D1}$$

Khi tổng số SM_0 REP được chuyển trong thời gian phân tách, tổng số $0,05SM_0$ REP được tạo ra thông qua lạm phát:

$$M_1 = 1.05SM_0 + (1 - S)M_0 \tag{D2}$$

Chỉ tập trung vào tác động của lạm phát, và vì lợi ích của sự đơn giản, chúng tôi giả định rằng vốn hóa thị trường sau khi fork sẽ giống như giới hạn thị trường trước fork [29]:

$$P_0M_0 = P_1M_1 \tag{D3}$$

[29] Chúng tôi nghĩ điều này là thận trọng. Trong thực tế, chúng tôi kỳ vọng thị trường sẽ giảm sau một fork.

Thay thế D1 và D2 thành D3 và sự đơn giản hóa cho chúng ta:

$$P_1 = \frac{20P_0}{20+S} \tag{D4}$$

Lợi ích (tổng) cho kẻ tấn công khi bắt đầu một fork và lợi dụng tiền thưởng việc chuyển sớm là giá trị của REP sau khi di chuyển trừ đi giá trị REP trước khi di chuyển:

$$1.05SM_0P_1 - SM_0P_0 \tag{D5}$$

Thay thế D4 thành D5 chúng ta nhận được một biểu thức thay thế cho lợi ích (tổng) cho kẻ tấn công:

$$1.05SM_0\frac{20P_0}{20+S} - SM_0P_0 \tag{D6}$$

Như đã đề cập ở trên b là số lượng REP cần phải có để bắt đầu một fork. Do đó, chi phí bắt đầu một fork là bP_0. Do đó, việc thanh toán chi phí bắt đầu một fork để tận dụng lợi thế của tiền thưởng việc chuyển sớm là đáng giá bất cứ khi nào bất đăng thức sau được thỏa mãn:

$$0 < 1.05SM_0\frac{20P_0}{20+S} - SM_0P_0 - bP_0 \tag{D7}$$

Ta thấy rằng $P_0 > 0$, và $S \neq -20$, chúng ta giải b và thấy rằng cuộc tấn công có thể sinh lợi khi:

$$b < \frac{21M_0S}{S+20} - M_0S \tag{D8}$$

Để ngăn chặn sự khích lệ nghịch đảo, Augur phải giải quyết các vấn đề như:

$$b \geq \frac{21M_0S}{S+20} - M_0S \tag{D9}$$

Lưu ý rằng S bị giới hạn trong khoảng $[0,1]$, chúng ta thấy rằng giá trị phía bên phải của bất đẳng thức D9 được tối đa khi $S = 2\sqrt{105} - 20 \approx 0.4939$. Đó là, cuộc tấn công này mang lại lợi nhuận nhất cho kẻ tấn công khi khoảng 49,39% của tất cả REP hiện có được chuyển trong thời gian phân tách. Hãy thận trọng, chúng tôi sử dụng giá trị này cho S.[30]

Thay thế $S = 0.4939$ thành D9 chúng ta nhận được $b \geq 0.012197M_0$. Do đó, nếu chi phí để bắt đầu một fork ít nhất là 1.2197% của REP hiện tại thì tấn công lạm phát sữa không có lợi nhuận.

Như đã đề cập ở trên, một fork được bắt đầu chỉ sau khi một liên kết tranh luận thành công được điền đầy đủ và lớn hơn 2,5% REP hiện tại. Giả sử rằng một liên kết tranh luận như vậy được điền đầy đủ để ủng hộ kết quả ω và một fork được bắt đầu. Kết quả ω là đúng hoặc sai.

Nếu kết quả ω là sai, thì ít nhất 2,5% REP hiện tại được đặt cược vào kết quả sai, và do đó bị tiêu hủy. Vì vậy, lạm phát sữa không có lợi nhuận khi ω là sai. Nếu kết quả ω là đúng, thì Bổ đề 2 cho chúng ta biết rằng ít nhất 1.25% của REP hiện tại (tổng cộng) được đặt cược vào kết quả sai, và do đó bị tiêu hủy. Vì vậy, lạm phát sữa cũng không có lãi khi ω là đúng.

Chính vì lý do này mà việc bắt đầu fork đòi hỏi phải thực hiện thành công một liên kết tranh luận ít nhất là 2.5% REP hiện tại.

Phụ lục E: Điều Chỉnh Kích Thước Liên Kết

Liên kết hợp lệ, liên kết không hiển thị REP, và cổ phần của các reporter được chỉ định được điều chỉnh động dựa trên hành vi của những người tham gia trong cửa sổ phí trước đó. Ở đây chúng tôi mô tả cách chúng tôi điều chỉnh các giá trị đó.

Chúng ta định nghĩa hàm $f : [0,1] \to [\frac{1}{2}, 2]$ bởi:[31]

$$f(x) = \begin{cases} \frac{100}{99}x + \frac{98}{99} & \text{for} \quad x > \frac{1}{100} \\ 50x + \frac{1}{2} & \text{for} \quad x \leq \frac{1}{100} \end{cases} \tag{E1}$$

Hàm f được sử dụng để xác định bội số được sử dụng trong các điều chỉnh này, như được mô tả trong các phần phụ bên dưới. Tóm lại, nếu hành vi không mong muốn xảy ra chính xác 1% thời gian trong cửa sổ phí trước đó, thì kích thước liên kết vẫn giữ nguyên. Nếu nó ít thường xuyên hơn, thì kích thước liên kết sẽ giảm đi một nửa. Nếu nó thường xuyên hơn, thì kích thước liên kết sẽ tăng lên gấp 2 lần.

1. Liên Kết Hợp Lệ

Trong cửa sổ phí đầu tiên sau khi khởi động, liên kết hợp lệ sẽ được đặt ở mức 0,01 ETH. Sau đó, nếu hơn 1% thị trường hoàn thành trong cửa sổ phí trước đó không hợp lệ, liên kết phiếu hợp lệ sẽ được tăng lên. Nếu ít hơn 1% thị trường hoàn thành trong cửa sổ phí trước đó không hợp lệ, thì liên kết hợp lệ sẽ bị giảm (nhưng sẽ không bao giờ thấp hơn 0,01 ETH).

Cụ thể, chúng ta có ν là tỷ lệ của thị trường hoàn thành trong cửa sổ phí trước đó không hợp lệ, và b_v là số tiền của liên kết hợp lệ từ cửa sổ phí trước đó. Sau đó, liên kết hợp lệ cho cửa sổ hiện tại là $\max\left\{\frac{1}{100}, b_v f(\nu)\right\}$.

[30] Trong thực tế, kẻ tấn công không thể ngăn cản những người tham gia khác chuyển REP của chính họ trong thời gian chờ đợi, và do đó không thể đảm bảo rằng S sẽ không vượt quá giá trị lý tưởng của kẻ tấn công về con số 0,4939. Tuy nhiên, vì chúng ta đang chống lại trường hợp xấu nhất, chúng tôi sử dụng $S = 0.4939$.

[31] Công thức này có thể thay đổi khi dữ liệu thực nghiệm thu được từ các thị trường trực tiếp.

2. Liên Kết Không Hiển Thị REP

Trong cửa sổ phí đầu tiên sau khi khởi chạy, liên kết không hiển thị REP sẽ được đặt ở mức 0,35 REP. Cũng giống như liên kết hợp lệ , liên kết không hiển thị REP được điều chỉnh lên hoặc xuống, nhắm mục tiêu tỷ lệ không hiển thị là 1% với mức sàn 0,35 REP.
Cụ thể, chúng tôi cho ρ là tỷ lệ thị trường trong cửa sổ phí trước đó mà các reporter được chỉ định không báo cáo đúng thời hạn và chúng tôi để b_r là số lượng liên kết không hiển thị REP từ cửa sổ phí trước đó. Số lượng liên kết không hiển thị REP cho cửa sổ phí hiện tại là $\max\{0.35, b_r f(\rho)\}$.

3. Cổ phần Reporter được Chỉ định

Trong cửa sổ phí đầu tiên sau khi khởi động, số cổ phần của reporter được chỉ định sẽ được đặt ở mức 0,35 REP. Số lượng cổ phần của reporter được chỉ định được điều chỉnh động theo số lượng báo cáo được chỉ định không chính xác (không khớp với kết quả cuối cùng của thị trường) trong cửa sổ phí trước đó.
Cụ thể, chúng tôi để δ là tỷ lệ các báo cáo được chỉ định không chính xác trong cửa sổ phí trước đó và chúng tôi cho b_d là số cổ phần của reporter được chỉ định trong cửa sổ phí trước đó, sau đó số được cổ phần của reporter chỉ định cho cửa sổ hiện tại là $\max\{0.35, b_d f(\delta)\}$.

Phụ lục F: Thay Đổi Thiết Kế

Chúng tôi có thiết kế hiện tại của Augur sau ba năm nghiên cứu không ngừng nghỉ. Thiết kế nổi lên từ quá trình này khác biệt đáng kể so với tầm nhìn được đưa ra trong sách trắng cũ của chúng tôi [12]. Ở đây, chúng ta thảo luận về ba thay đổi quan trọng cũng như lý do cho những thay đổi đó.

1. Phí Báo Cáo

Trong thiết kế cũ, người tạo thị trường sẽ đặt một khoản phí giao dịch sẽ được chia 50/50 với các reporter. Trong thiết kế hiện tại, phí cho người tạo thị trường và các reporter là độc lập, và phí của reporter được điều chỉnh động bởi chính Augur để giữ cho hệ thống an toàn
Phí trả cho reporter ảnh hưởng đến giá REP, có ảnh hưởng trực tiếp đến tính bảo mật của giao thức forking (Định lý 1). Nếu phí trả cho reporter quá thấp, thì tính toàn vẹn của oracle sẽ bị đe dọa. Nếu phí trả cho reporter quá cao, thì mối đe dọa của thị trường ký sinh tăng lên. Vì vậy, điều quan trọng là các khoản phí trả cho các reporter được điều chỉnh động để duy trì an ninh của Augur, thay vì được quyết định tùy ý bởi những người sáng tạo trên thị trường.
Việc tách lệ phí của reporter khỏi sự lựa chọn của người tạo thị trường cũng đảm bảo rằng các reporter (cùng với đó, tính toàn vẹn giao thức forking) không bị tổn hại bởi sự cạnh tranh giữa những người tạo thị trường để tạo ra thị trường với mức phí thấp nhất. Thị trường chất lượng và báo cáo chất lượng phải được đo lường và thưởng một cách riêng biệt. Cạnh tranh nên được cho phép để thúc đẩy phí của người sáng tạo thị trường về không, mà không phải kéo phí trả cho reporter xuống.

2. Phí Giao Dịch

Trong thiết kế cũ, phí được thu thập từ các nhà giao dịch trên mọi giao dịch. Trong thiết kế mới, lệ phí chỉ được thu từ các nhà giao dịch khi thanh toán trực tiếp với hợp đồng thị trường. Sự thay đổi này đã được thực hiện, một phần, bởi vì Augur không thể theo dõi giao dịch ngoại tuyến. Cổ phần của kết quả thị trường chỉ đơn giản là token, có thể được giao dịch tự do giữa người dùng. Vì thu phí trên mỗi giao dịch là không khả thi, nên thay vào đó, Augur chỉ thu phí khi các nhà giao dịch thanh toán trực tiếp với các hợp đồng thị trường Augur. Một lợi ích bổ sung của phương pháp này là nó làm giảm phí trung bình được trả bởi các nhà giao dịch, điều này sẽ làm cho Augur cạnh tranh hơn.

3. Vũ Trụ

Trong thiết kế cũ, chỉ có một 'phiên bản' của REP, và tổng nguồn cung của nó đã được cố định. Trong thiết kế hiện tại, REP có thể chia thành nhiều phiên bản (vũ trụ) khác nhau, mỗi vũ trụ có thể kết thúc với tổng số REP ít hơn phiên bản gốc.Nếu một fork gây tranh cãi, REP được cung cấp trong mỗi vũ trụ con có thể chỉ là một phần nhỏ của tổng cung trong vũ trụ cái. Trong một fork không gây tranh cãi, tiền thưởng việc chuyển sớm cho người tham gia fork có thể dẫn đến một vũ trụ con có tổng REP nhiều hơn vũ trụ cái của nó.
Các phiên bản REP mới được tạo ra bởi một fork là các token khác nhau, mỗi token có giá và tổng cung cấp riêng, và các nhà cung cấp dịch vụ nên xử lý chúng như vậy. Khi Augur ra mắt lần đầu tiên, sẽ có một vũ trụ duy nhất (vũ trụ gốc) và một phiên bản REP duy nhất, giống như hiện tại. Tuy nhiên, ngay sau khi một fork xảy ra, phiên bản REP duy nhất sẽ chia thành nhiều phiên bản: ví dụ, một thị trường forking với kết quả A và B sẽ sinh ra token mới REP- A , REP- B và REP- không hợp lệ. Ví và sàn giao dịch hỗ trợ REP bây giờ sẽ có bốn phiên bản khác nhau của REP mà họ có thể (trong lý thuyết) hỗ trợ - REP- gốc (phiên bản gốc của REP, mà bây giờ sẽ bị khóa), REP- A, REP- B và REP- không hợp lệ. [32]

[32]Là một vấn đề thực tế, các nhà cung cấp dịch vụ có thể tìm

Tổng số REP trong mỗi vũ trụ con phụ thuộc vào số lượng REP được chuyển đến nó, và khi việc chuyển đó xảy ra. Chuyển REP trong một fork, trước khi nó được rõ ràng mà vũ trụ con đã đạt được sự đồng thuận, khiến người dùng đối mặt với một số lượng nhỏ (nhưng khác không) rủi ro (xem Phần III E),có thể ngăn cản sự tham gia trong quá trình phân tách của fork được tranh luận. Để khuyến khích sự tham gia trong một fork, người dùng phải được bồi thường cho rủi ro.

Những người sử dụng không tham gia trong giai đoạn chia tách của một fork có thể bị phạt bằng cách mất một phần số REP họ đang giữ. Trên thực tế, thiết kế cũ có một cơ chế " sử dụng hoặc mất " để phạt những người không tham gia như thể họ là reporter đã báo cáo sai. Tuy nhiên, việc trừng phạt những người dùng không tham gia tạo ra các vấn đề đáng kể về khả năng sử dụng. Trừng phạt người dùng không tham gia là vấn đề của ví và sàn giao dịch những nơi quản lý REP của khách hàng của họ. Trong trường hợp một fork, sàn giao dịch sẽ cần phải di chuyển REP của khách hàng của họ đến một số vũ trụ con trong thời gian phân tách, hoặc mất một phần của REP của họ. [33]
Thay vì phạt những người không tham gia, những người tham gia fork trong suốt giai đoạn phân tách được thưởng thêm 5% trong vũ trụ con mà họ đang chuyển đến. Nếu 4,76% REP (hoặc nhiều hơn) chuyển đến một vũ trụ bị thua – trong đó 1,25% đến 2,5% đã được cam kết là cổ phần tranh luận – thì tất cả các vũ trụ sẽ có tổng số REP nhỏ hơn vũ trụ mẹ .

---

thấy nó dễ dàng nhất (và ít gây phiền toái cho người dùng của họ) để khuyến khích người dùng tham gia fork, và sau đó chỉ đơn giản là hỗ trợ vũ trụ chiến thắng một khi fork đã giải quyết.

[33]Chúng tôi cũng tìm thấy, như một vấn đề thực tế, mã hợp đồng thông minh cần thiết để thực hiện thưởng forking chỉ sử dụng phân phối lại là vô cùng phức tạp. Sự phức tạp của mã hợp đồng tự nó đã là một nguy cơ về bảo mật, vì vậy chúng tôi đã cố gắng đơn giản hóa việc triển khai bất cứ khi nào có thể.