bitcoin vault

Bitcoin Vault: Vàng Điện tử Chống trộm Ngang hàng

Eyal Avramovich github.com/bitcoinvault

Tóm tắt. Tầm nhìn ban đầu của Satoshi Nakamoto cho Bitcoin là tạo ra một phiên bản tiền điện tử ngang hàng. Phần lớn các lần phân tách (fork) giao thức thành công đều cố gắng cải thiện thêm tầm nhìn này và cung cấp một hệ thống thanh toán có thể mở rộng và hiệu quả hơn. Chúng tôi thấy triển vọng lớn nhất của Bitcoin không phải là một phương tiện trao đổi, mà là một tài sản lưu trữ – một dạng ưu việt hơn của vàng, không phải tiền mặt. Chúng tôi đề xuất một loạt các chỉnh sửa cho giao thức ban đầu, nhằm hiện thực hóa triển vọng này thông qua việc tạo ra tài sản lưu trữ điện tử hoàn chỉnh cuối cùng. Bằng cách tăng thời gian xác nhận giao dịch hiệu quả của Bitcoin từ 10 phút lên 24 giờ, chúng tôi có thể khắc phục lỗ hổng lớn nhất của Bitcoin như một dạng vàng dễ bị đánh cắp. Một hệ thống ít hướng đến mục tiêu trả tiền cà phê, mà chú trọng hướng đến mục tiêu là tài sản tiết kiệm cho cuộc sống của một người với sự an tâm tuyệt đối, trong đó mọi giao dịch được cảnh báo trên chuỗi cho 144 khối (block) và có thể bị hủy trong trường hợp khẩn cấp bằng khóa khôi phục chưa từng được sử dụng trước đó và do đó không thể bị tấn công. Chương trình khởi động của hệ thống này không thông qua quá trình hard fork (phân tách cứng), mà thông qua cơ chế đào nhanh hơn, cho phép hệ thống bắt kịp Bitcoin trong một khoảng thời gian ngắn. Chúng tôi hoàn toàn tin tưởng người tạo ra sách trắng (whitepaper) Bitcoin Royale [1], người đã tạo nên tầm nhìn về vàng điện tử không bị trộm cắp. Nhóm chúng tôi muốn tiếp tục với ý tưởng đó và bắt đầu triển khai tất cả các tính năng quan trọng được đề cập dưới đây và làm cho nó trở nên tiên tiến hơn với giải pháp khóa mật thứ 3, được tiết lộ như một tính năng bổ sung trong đoạn 6.2.

1. Giới thiệu

Bitcoin [2] là một hệ thống thanh toán phi tập trung sáng tạo, được ra mắt vào năm 2009, cho phép các bên giao dịch trực tiếp mà không cần thông qua một tổ chức tài chính nào. Hệ thống dựa trên bằng chứng công việc (proof-of-work) để duy trì một sổ cái phân tán không cần người điều hành, hệ thống này sẽ an toàn khi các máy trạm trong hệ thống kiểm soát nhiều sức mạnh CPU hơn bất kỳ số máy trạm của một nhóm tấn công nào. Bitcoin ban đầu được Satoshi Nakamoto, người tạo ra nó, mô tả như một hệ thống tiền mặt điện tử.

Trong nhiều năm qua, đã có nhiều bản sửa đổi giao thức gốc thành công dưới dạng phân tách cơ sở mã nguồn của Bitcoin. Những bản sửa đổi này bao gồm Litecoin [3], được ra mắt vào năm 2011 nhằm giảm thời gian xác nhận giao dịch và thay đổi thuật toán bằng chứng công việc (proof-of-work) để ưu tiên cho phần cứng cấp người tiêu dùng như GPU; Bitcoin Cash [4] được ra mắt vào năm 2017 nhằm mở rộng thông lượng giao dịch của giao thức ban đầu bằng cách tăng kích thước khối; và Bitcoin Gold [5] cũng được ra mắt vào năm 2017, khiến các thiết bị đào chuyên dụng trở nên lỗi thời bằng cách thay đổi thuật toán băm.

Theo tầm nhìn ban đầu, trọng tâm trong các đợt phân tách này cũng như các đợt khác là nhằm biến Bitcoin thành một hệ thống tiền mặt tốt hơn. Các hạn chế của giao thức ban đầu như phí giao dịch cao, thời gian xác nhận 10 phút và thông lượng chỉ xấp xỉ 4 giao dịch mỗi giây đã cản trở khả năng cạnh tranh của Bitcoin với các hệ thống thanh toán trực tuyến tập trung hiện nay.

2. Tiền Điện tử hoặc Vàng Điện tử

Mặc dù Bitcoin không cho thấy sự thành công trong việc thuyết phục người tiêu dùng chấp nhận nó như một loại tiền điện tử, nhưng nó đã có những thành công đáng kể hơn theo hướng trở thành một dạng vàng điện tử. Có một đề tài tranh luận lâu nay trong ngành là liệu Bitcoin có nổi lên như một phương tiện trao đổi, hay trên thực tế sẽ là một tài sản lưu trữ. Vàng không phải là một phương tiện thanh toán hiệu quả cho hàng hóa và dịch vụ hàng ngày. Người tiêu dùng chủ yếu đầu tư vào vàng để chống lạm phát và bảo toàn sức mua trong tương lai. Không giống như các loại tiền tệ quốc gia, chính sách tiền tệ cố định và nguồn cung hạn chế của Bitcoin khiến nó trở nên đặc biệt hấp dẫn trong vấn đề này.

Lịch sử cho thấy các hệ thống hiếm khi được thiết kế để đáp ứng nhiều mục tiêu tương khắc cùng một lúc. Việc tối ưu hóa Bitcoin để trở thành một phương tiện trao đổi tốt hơn sẽ làm giảm tiềm năng trở thành tài sản lưu trữ của nó. Tương tự, nếu tiếp tục loại bỏ các đặc tính cần thiết của một loại tiền điện tử, chúng ta có thể cải thiện đáng kể tiện ích của Bitcoin như một loại vàng điện tử. Trong bài viết này, chúng tôi đề xuất một loạt các sửa đổi cho giao thức Bitcoin ban đầu, tập trung vào một mục tiêu duy nhất – tạo ra một tài sản lưu trữ hoàn chỉnh sau cùng.

Nếu không còn ưu tiên phấn đấu để trở thành một hệ thống thanh toán trực tuyến, thì chúng tôi không cần phải chú trọng đến phí giao dịch hoặc thông lượng giao dịch. Sau tất cả, vàng rất tốn kém để vận chuyển và thường được mua để đầu tư dài hạn. Một tính chất đặc biệt liên quan đến nỗ lực của chúng tôi là thời gian xác nhận giao dịch. Sự đánh đổi về khía cạnh này, chẳng hạn như tăng đáng kể thời gian xác nhận trung bình 10 phút của Bitcoin, có thể mang lại những lợi thế chính. Dù sao thì chúng tôi cũng không kỳ vọng vận chuyển một lô hàng là vàng qua nhiều địa điểm trong thời gian dưới 10 phút, nên sự đánh đổi này có vẻ cũng tự nhiên.

3. Vấn đề Trộm cắp

Yêu cầu chính của một tài sản lưu trữ là không bị thất thoát. Trộm cắp là một trong những rủi ro chính gây mất mát khi giao dịch bằng bất kỳ thứ gì có giá trị. Vàng có nhiều ưu điểm trong vấn đề này. Hành vi trộm cắp vàng ngoài đời thực có mức độ rủi ro cao hơn đáng kể so với bất kỳ cuộc tấn công trên mạng nào vào tài sản điện tử. Ngoài ra, kẻ trộm sẽ gặp khó khăn trong việc giấu một lượng lớn vàng bị đánh cắp khỏi sự truy lùng của chính quyền, đặc biệt là để đưa qua biên giới. Rửa và thanh lý số lượng lớn vàng bị đánh cắp mà không để lộ danh tính là một việc không hề đơn giản.

Thật không may, chi phí để làm những việc này đối với Bitcoin rẻ hơn rất nhiều. Số tiền được bảo vệ bởi giao thức với các bộ khóa mật mã. Nếu lấy được quyền truy cập điện tử vào các khóa này, kẻ tấn công sẽ chiếm giữ toàn bộ số tiền từ xa, ngay lập tức và không thể thu hồi. Rửa số tiền đánh cắp cũng dễ dàng hơn nhiều vì các giao dịch được thực hiện với tên giả, có thể ngăn chặn việc truy xuất nguồn gốc bằng cách sử dụng các bộ trộn [6] và có thể tạo hàng loạt các danh tính giả mạo. Do đó, hoạt động

trộm cắp tiền điện tử đang gia tăng với hơn 1 tỷ đô la bị đánh cắp trong năm 2018 [7]. Danh sách các sự cố lớn được thống kê trong cộng đồng [8] cho thấy ngay cả các tổ chức chuyên nghiệp áp dụng thành thạo các phương pháp bảo mật mới nhất cũng có thể bị tấn công.

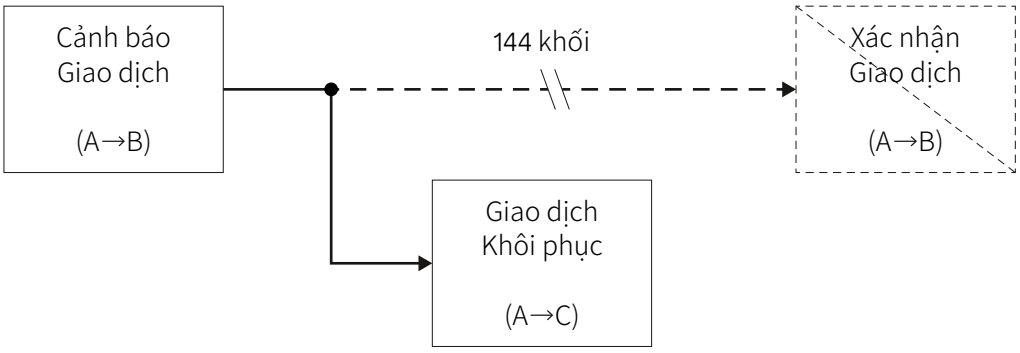
Việc quản lý an toàn các khóa mật của người dùng cuối đang là một trong những thách thức lớn của Bitcoin. Vì các khóa phải được sử dụng thường xuyên để tương tác với số tiền và các giao dịch đã ký phải được truyền qua Internet, nên cuối cùng thì mọi khóa đều dễ bị tấn công. Các hoạt động với ý định bảo mật như chia tiền giữa các ví "nóng" và "lạnh" là khá rắc rối và rất khó giải quyết vấn đề tận gốc. Các sự cố cho thấy ví nóng luôn là nơi giữ số tiền đáng kể [9, 10] và việc sử dụng ví lạnh chỉ làm giảm số lần tương tác với các khóa nhưng không thể tránh khỏi hoàn toàn [11].

4. Giải pháp Chống trộm cắp

Là một phương tiện để loại bỏ nguy cơ bị trộm cắp, chúng tôi đề xuất một giải pháp dựa trên tập lệnh khóa mới, tinh vi và sửa đổi giao thức. Một giao dịch được thực hiện bằng cách sử dụng tập lệnh khóa mới sẽ bị trì hoãn 24 giờ theo mặc định. Khi một thợ đào thêm một giao dịch vào một khối mới, giao dịch sẽ không được cam kết ngay lập tức. Thay vào đó, giao dịch này sẽ được thêm vào chuỗi dưới dạng cảnh báo trong thời lượng 144 khối (giả sử thời gian khối là 10 phút). Nếu không bị xáo trộn trong 144 khối, giao dịch sẽ thay đổi từ trạng thái cảnh báo sang "xác nhận".

Lợi ích của cảnh báo trên chuỗi là chủ sở hữu coin sẽ nhận được thông báo trước không qua kiểm duyệt mỗi khi coin của họ được di chuyển. Chủ sở hữu sẽ có 24 giờ để hành động dựa trên cảnh báo và có thể hủy lệnh chuyển tiền nếu có hành vi trái phép diễn ra. Trì hoãn rút tiền là một phương pháp tiêu chuẩn của ngành chống trộm đã được chứng minh trong ví lưu ký và hệ thống ngân hàng truyền thống. Ví dụ, Coinbase Vault [12] có thời gian chờ là 48 giờ. Giải pháp đề xuất của chúng tôi cung cấp sự bảo vệ tương tự mà không cần đến bên thứ ba.

Hủy khẩn cấp giao dịch ở trạng thái cảnh báo yêu cầu một giao dịch khôi phục đặc biệt, được thực hiện ngay lập tức mà không bị trì hoãn 24 giờ. Giao dịch khôi phục sẽ yêu cầu khóa khôi phục đặc biệt, khóa này phải được tích hợp vào tập lệnh khóa trong quá trình tạo ví. Không thể thay đổi một khóa khôi phục đã được đăng ký cho một ví cụ thể.



Khóa khôi phục mật được sử dụng cho việc hủy khẩn cấp, phải là một khóa mới chưa từng được sử dụng trước đây. Khóa này có thể được tạo ngoại tuyến và chưa từng được kết nối với Internet hoặc được nhập vào bất kỳ thiết bị nào. Quá trình đăng ký chỉ yêu cầu phần công khai của khóa này, đảm bảo rằng khóa mật vẫn chưa được sử dụng. Không giống như các khóa ví lạnh đôi khi cần được sử dụng và do đó dễ bị đánh cắp, khóa khôi phục chỉ được sử dụng lần đầu tiên trong trường hợp hủy khẩn cấp và do đó hoàn toàn có thể chống trộm. Khi khóa khôi phục đã được sử dụng, nó sẽ được coi là đã bị xâm phạm và tất cả tiền phải được chuyển ngay vào ví mới được bảo vệ bởi khóa khôi phục mới, chưa qua sử dụng.

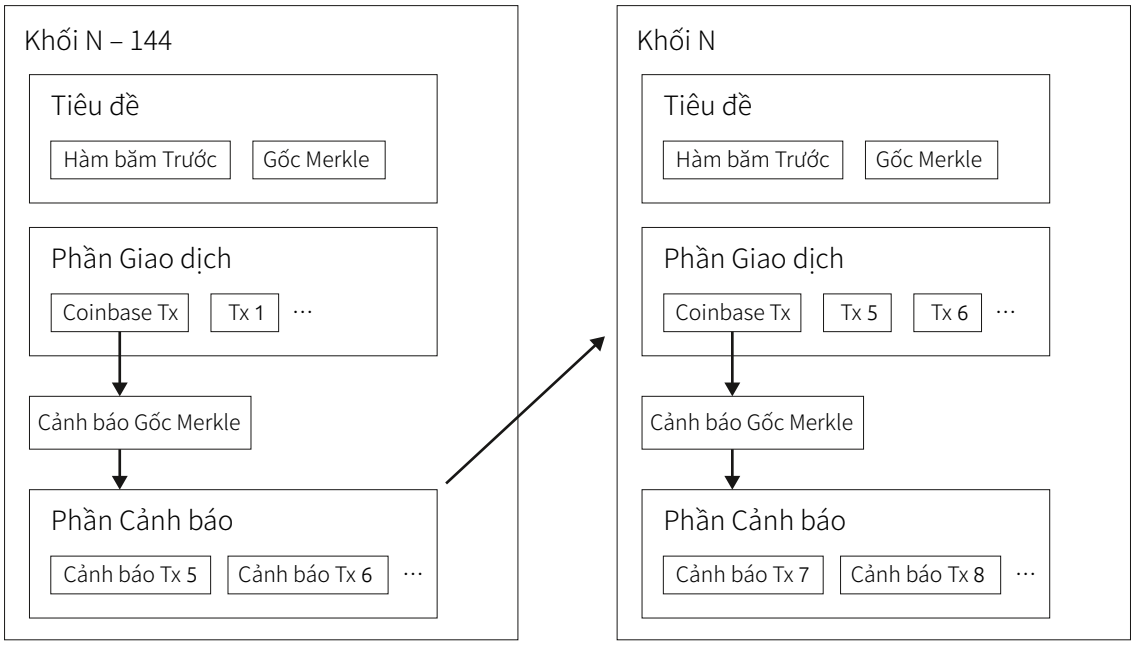
Khái niệm Bitcoin Royale ban đầu về vàng kỹ thuật số đặt ra giả thuyết trì hoãn 24 giờ đối với tất cả các giao dịch trong hệ thống, biến coin thành một tài sản lưu trữ an toàn, chậm di chuyển. Chúng tôi muốn mở rộng khái niệm này để hoàn thiện tốt nhất hai thế giới – vàng kỹ thuật số và tiền kỹ thuật số, mà không có bất kỳ sự xâm phạm nào về vấn đề bảo mật.

Bên cạnh các cảnh báo di chuyển chậm, chúng tôi sẽ thiết đặt các điều kiện để duy trì các giao dịch di chuyển nhanh, “tức thì”. Để cung cấp khả năng bảo mật cao nhất, khi gửi một giao dịch như vậy, người dùng sẽ được yêu cầu thực hiện xác thực 2 yếu tố (2FA) dựa trên blockchain, sử dụng khóa thứ 3 được cung cấp trong quá trình tạo ví.

5. Khối

Giống như giao thức Bitcoin ban đầu, mọi khối đều chứa một danh sách các giao dịch được xác nhận và giữ hàm băm gốc Merkle (Merkle root) của các giao dịch này trong tiêu đề của nó. Vì một số giao dịch phải chờ 24 giờ trên chuỗi, chúng không thể được thêm ngay lập tức vào phần giao dịch của một khối. Thay vào đó, chúng được thêm vào một phần đặc biệt mới không tồn tại trong giao thức Bitcoin gốc – phần cảnh báo. Hàm băm gốc Merkle cho phần cảnh báo được lưu trữ tại đầu vào của giao dịch coinbase duy trì khả năng tương thích tiêu đề khối với Bitcoin ban đầu.

Khi một khối mới được đào, thợ đào sẽ xem lại 144 khối và kiểm tra phần cảnh báo của khối N-144. Tất cả cảnh báo cho các giao dịch vẫn còn hiệu lực sẽ được xác nhận và điền vào phần giao dịch của khối mới.



Các bước để đào khối N như sau:

1) Thêm giao dịch hợp thức mới vào phần cảnh báo của khối N (không được xác nhận).
2) Thêm giao dịch tức thì mới vào phần giao dịch của khối N (đã xác nhận)
3) Thêm giao dịch khôi phục mới vào phần giao dịch của khối N (đã xác nhận).
4) Chuyển qua phần cảnh báo của khối N-144 và thêm các giao dịch hợp lệ vào phần giao dịch của khối N (đã xác nhận).

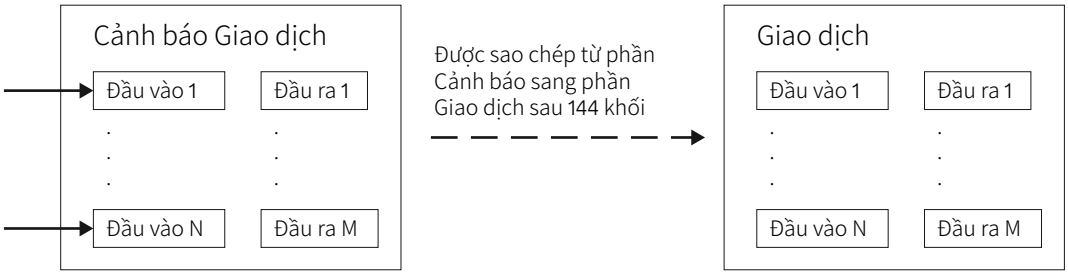
6. Tập lệnh

Chức năng cốt lõi của Bitcoin Vault khả dụng thông qua tập lệnh khóa tinh vi, hoạt động khác nhau dựa trên số chữ ký được trình bày trong tập lệnh mở khóa. Hai biến thể khả dụng:

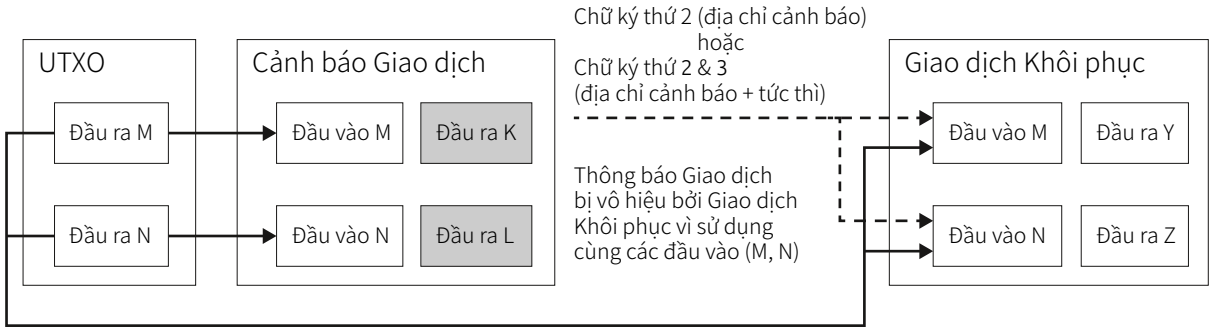
1. Tập lệnh khóa cảnh báo – yêu cầu một hoặc hai chữ ký. Nếu có một chữ ký, một giao dịch cảnh báo được tạo ra. Nếu có hai chữ ký, một giao dịch khôi phục được tạo ra.
2. Tập lệnh khóa cảnh báo + tức thì – yêu cầu một, hai hoặc ba chữ ký. Nếu có một chữ ký, một giao dịch cảnh báo được tạo ra. Nếu có hai chữ ký, một giao dịch tức thì được tạo ra. Nếu có cả ba chữ ký, một giao dịch khôi phục được tạo ra.

7. Giao dịch

Các lượt chuyển coin được thực hiện bằng các giao dịch thông thường giống như trong giao thức Bitcoin. Định dạng của chúng không thay đổi khi chúng được chuyển từ phần cảnh báo sang phần giao dịch.



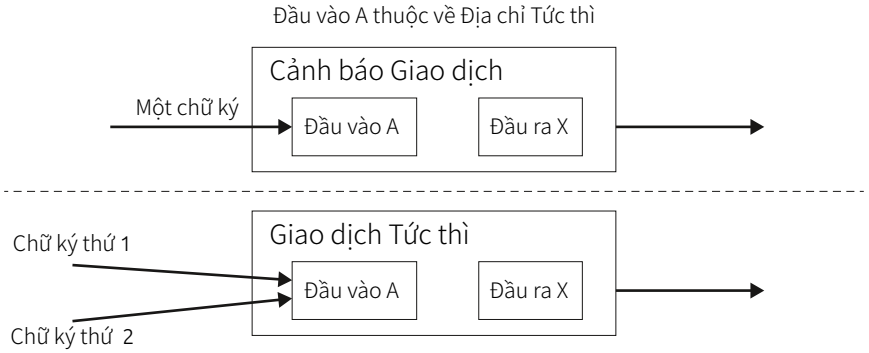
7.1. Giao dịch Khôi phục



Một giao dịch khôi phục sử dụng UTXO (Đầu ra giao dịch chưa chi tiêu) giống như cảnh báo đã khôi phục. Sự khác biệt là nó có nhiều chữ ký hơn cho cùng UTXO: 2 trong trường hợp tập lệnh khóa cảnh báo hoặc 3 trong trường hợp tập lệnh khóa cảnh báo + tức thì. Khi giao dịch khôi phục được xử lý, UTXO đã khôi phục được sử dụng, do đó làm mất hiệu lực mọi cảnh báo hiện có dựa trên UTXO này và ngăn không cho chúng được xác nhận quá 24 giờ trì hoãn.

7.2. Giao dịch Tức thì

Giao dịch tức thì cho phép bỏ qua độ trễ mặc định là 24 giờ để xác nhận giao dịch và tăng tốc độ xác nhận giao dịch lên khoảng 10 phút. Cơ chế của giao dịch này tương tự như ví multisig (nhiều chữ ký). Nó yêu cầu một chữ ký bổ sung từ một khóa mật riêng biệt cần được lưu trữ an toàn tại một vị trí riêng biệt. Đó là lý do tại sao các giao dịch tức thì chỉ được gửi từ các địa chỉ P2SH đặc biệt – địa chỉ tức thì, được tạo từ tập lệnh khóa cảnh báo + tức thì.



8. Khả năng tương thích

Thiết kế của chúng tôi cố gắng làm cho giao thức tương thích tốt nhất có thể với giao thức Bitcoin tiêu chuẩn. Mục tiêu cơ bản là để giảm thiểu số lần thay đổi mã cần thiết đối với các máy trạm, ví, các quỹ vốn chung và máy đào đang có Bitcoin. Tuy nhiên, nếu các thay đổi được thực hiện trên một chuỗi khối (blockchain) đã tồn tại sẵn, chúng sẽ cần một đợt hard fork (phân tách cứng)

Để tránh thay đổi định dạng của tiêu đề khối, vì điều này khiến cho coin không tương thích với các máy đào bitcoin ASIC, hàm băm gốc Merkle cho phần cảnh báo được lưu trữ tại đầu vào của giao dịch coinbase tiêu chuẩn.

Nếu cần phải hard fork (phân tách cứng), thì mục tiêu của chúng tôi là làm cho việc chuyển đổi trở nên dễ dàng nhất có thể cho người dùng coin hiện tại. Tất cả các loại tập lệnh hiện tại không thay đổi trạng thái của chúng, vì vậy tất cả các đồng coin tồn tại trước khi hard fork đều có thể được sử dụng như bình thường. Tuy nhiên, chúng tôi khuyến cáo bạn nên chuyển sang các tập lệnh mới, an toàn hơn.

9. Khuyến khích

Hệ thống vay mượn mô hình khuyến khích từ Bitcoin, mô hình này đã chứng minh sự thành công trong thập kỷ qua. Để kết hợp các cảnh báo, cần có các sửa đổi nhỏ cho mô hình này. Các thợ đào được khuyến khích đưa các cảnh báo giao dịch vào một khối với hứa hẹn về khoản phí được tính từ chênh lệch giữa giá trị đầu ra và đầu vào. Các khoản phí được tính từ các giao dịch khối trong tương lai và được phân phối cho thợ đào ban đầu – người đưa vào các cảnh báo giao dịch.

Thợ đào trong tương lai vẫn sẽ nhận được tiền thưởng cho khối khi đào một khối mới, tất cả các khoản phí từ giao dịch tức thì, đăng ký và khôi phục mới và hứa hẹn về khoản phí trong tương lai từ các cảnh báo giao dịch. Thợ đào trong tương lai bắt buộc tuân theo các quy tắc đồng thuận, phải đưa vào tất cả các cảnh báo từ khối N-144 đến các phần giao dịch, ngoại trừ các phần được thu hồi.

Trong trường hợp hủy bỏ cảnh báo, phí cho thợ đào ban đầu của cảnh báo sẽ không thể phục hồi và tổng chi phí là phí của cảnh báo ban đầu cộng với phí cho giao dịch khôi phục.

10. Công việc Liên quan

Chúng tôi đặc biệt ấn tượng với công việc của Malte Möser và những người khác trên các Giao ước Bitcoin [13]. Việc họ mở rộng ngôn ngữ tập lệnh Bitcoin sẽ kích hoạt những hạn chế về việc sử dụng các đồng coin trong tương lai, điều này có thể được áp dụng để triển khai nhiều biện pháp bảo mật. Yếu tố quan trọng nhất trong công việc này là các giao dịch két an toàn (vault), giống như cơ chế rút tiền trì hoãn theo đề xuất của chúng tôi.

Chúng tôi đã chọn cách triển khai đơn giản hơn, không cần đến một dãy các tập lệnh đệ quy tùy chỉnh cần thực hiện bằng ví. Đề xuất của chúng tôi không chỉ là một phần mở rộng tùy chọn, đó còn là sự thay đổi nền tảng cho giao thức với hiệu ứng bắt buộc rộng rãi đối với các giao dịch. Chuyển gánh nặng của việc thực thi sang các thợ đào và giữ trải nghiệm giao dịch của người dùng cuối giống với mặc định, điều này cho phép chúng tôi tiến hành hiệu quả hơn nhiệm vụ tạo ra vàng điện tử thực sự.

Tài liệu tham khảo

1. Ian Duoteli Fleming, https://bitcoinroyale.org/bitcoinroyale.pdf
2. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://www.bitcoin.org/bitcoin.pdf, 2008.
3. Litecoin Project, “Litecoin, open source P2P digital currency”, https://litecoin.org, 2014.
4. “Bitcoin Cash”, https://www.bitcoincash.org, 2018.
5. bitcoingold.org, “Bitcoin Gold”, https://bitcoingold.org, 2018.
6. J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, “Coinparty: Secure multi-party mixing of bitcoins”, In: *CODASPY ’15*, 2015.
7. CipherTrace, “Cryptocurrency Anti-Money Laundering Report, 2018 Q4”, https://ciphertrace.com/crypto-aml-report-2018q4, 2019.
8. “BLOCKCHAIN GRAVEYARD”, https://magoo.github.io/Blockchain-Graveyard, 2019.
9. C. Zhao, “Binance Security Breach Update (May 7 2019)”, https://binance.zendesk.com/hc/en-us/articles/360028031711, 2019.
10. J. Buck, “Coincheck: Stolen $534M ln NEM Were Stored On Low Security Hot Wallet“, https://cointelegraph.com/news/coincheck-stolen-534-mln-nem-were-stored-on-low-security-hot-wallet, 2018.
11. J. Preissler, “Important Notice: Only trade TIO on trade.io”, https://medium.com/@trade.io/important-notice-only-trade-tio-on-trade-io-823d59fd7104, 2018.
12. KM. Cutler, “Coinbase Launches A More Secure Bitcoin Storage Option Called ‘Vault’”, https://techcrunch.com/2014/07/02/coinbase-vault, 2014.
13. M. Möser, I. Eyal, E. Gün Sirer, “Bitcoin Covenants”, In: *Financial Cryptography and Data Security, FC 2016, Lecture Notes in Computer Science*, Vol. 9604. Springer, Berlin, Heidelberg.