Bitcoin: Một hệ thống tiền điện tử ngang hàng

Shatoshi Nakamoto

Tổng quan. Một hệ thống tiền điện tử ngang hàng thuần tuý sẽ cho phép các giao dịch trên mạng được gửi từ một bên đến bên còn lại mà không cần thông qua một tổ chức tài chính trung gian nào. Các hình thức chữ ký điện tử giải quyết được một phần của vấn đề, nhưng các lợi ích này sẽ mất đi nếu như vẫn cần có một bên trung gian thứ ba đứng ra để ngăn chặn hiện tượng trùng chi. Chúng ta đề xuất một giải pháp cho hiện tượng trùng chi bằng cách sử dụng một mạng lưới ngang hàng. Mạng lưới này đánh dấu mốc thời gian các giao dịch bằng cách băm chúng thành một chuỗi các bằng chứng lao động dựa trên hàm băm và nối tiếp nhau, tạo nên một hồ sơ không thể chỉnh sửa nếu như không thực hiện lại chuỗi bằng chứng lao động này. Chuỗi dài nhất không chỉ nhằm mục đích làm bằng chứng cho chuỗi sự kiện đã được quan sát, mà còn là bằng chứng rằng nó được tạo ra từ khối lượng năng lượng CPU lớn nhất. Chừng nào các đầu nút kiểm soát phần lớn năng lượng CPU không thông đồng để tấn công mạng lưới, chúng sẽ tạo ra chuỗi dài nhất và bỏ xa các kẻ tấn công. Bản thân mạng lưới yêu cầu một cấu trúc khá giản đơn. Các thông tin trong mạng lưới được lan truyền với tinh thần nhiều nhất có thể, và các điểm nút trong mạng lưới có thể rời bỏ và quay lại bất cứ lúc nào, chỉ cần chấp nhận chuỗi bằng chứng lao động dài nhất là minh chứng cho các sự kiện xảy ra trong lúc vắng mặt.

1 Giới thiệu

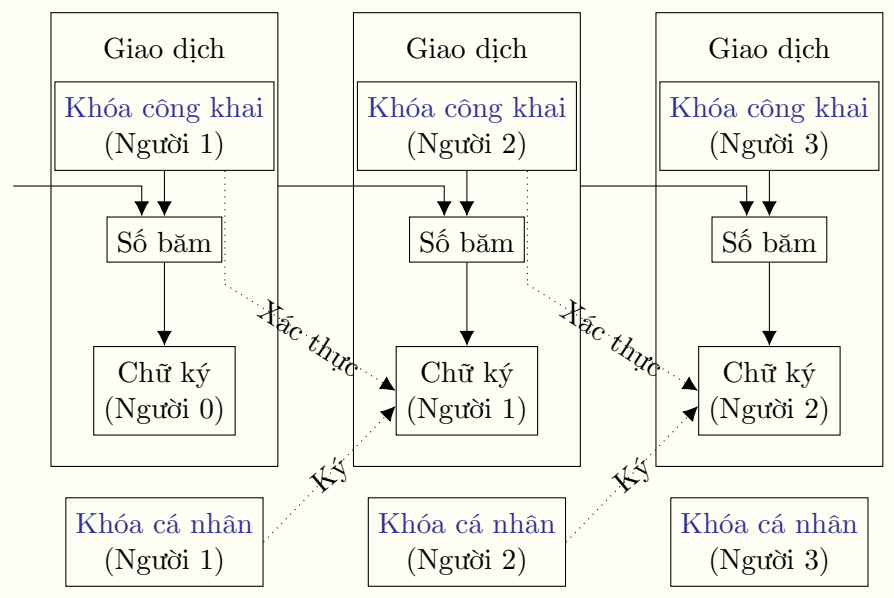
Các hoạt động thương mại trên Internet ngày nay gần như phụ thuộc một cách tuyệt đối vào các tổ chức tài chính hoạt động với danh nghĩa một bên thứ ba được tin tưởng đứng ra tiến hành các giao dịch điện tử. Trong khi hệ thống này hoạt động đủ tốt đối với hầu hết các giao dịch, nó phải gánh chịu những điểm yếu cố hữu của một mô hình dựa trên sự tin tưởng. Các giao dịch không hoàn trả là không thực sự khả thi, vì các tổ chức tài chính này không thể tránh được việc phải đứng ra giải quyết các tranh chấp. Chi phí của việc đứng ra trung gian làm tăng chi phí giao dịch, giới hạn về quy mô tối thiểu đối với một giao dịch và làm mất đi tính khả thi cho các giao dịch nhỏ thường ngày, đồng thời cũng tiềm ẩn những tổn thất lớn hơn trong việc mất đi những giao dịch

không thể hoàn trả đối với những dịch vụ không thể hoàn trả. Khả năng hoàn trả đối với giao dịch đi kèm với vấn đề phụ thuộc vào sự tin tưởng. Các nhà buôn phải cảnh giác trước khách hàng của họ, hạch sách họ với nhiều thông tin hơn cần thiết. Một phần rủi ro gian lận nhất định được coi là không thể tránh được. Những chi phí và sự không chắc chắn này có thể được phòng ngừa bởi các cá nhân tham gia những giao dịch sử dụng tiền vật lý, nhưng không có cơ chế nào tương tự dành cho các kênh giao dịch mà mà không có bên thứ ba đứng ra đảm bảo.

Thứ chúng ta cần là một hệ thống thanh toán điện tử dựa trên nền tảng bằng chứng mã hóa thay vì dựa trên niềm tin, cho phép hai bên giao dịch trực tiếp với nhau mà không cần đến một bên thứ ba đứng ra đảm bảo. Các giao dịch không thể đảo ngược về mặt thuật toán sẽ bảo vệ người bán khỏi các hành vi gian lận, và các cơ chế bảo chứng thông dụng có thể được thực hiện một cách dễ dàng để bảo vệ người mua. Trong bài viết này, chúng ta đề xuất một giải pháp cho vấn đề trùng chi sử dụng một máy chủ lưu trữ mốc thời gian ngang hàng nhằm tạo ra các bằng chứng tính toán cho thứ tự của các giao dịch. Hệ thống này là đảm bảo an toàn chừng nào tập thể các điểm đầu nút trung thực trong mạng lưới kiểm soát số lực CPU nhiều hơn bất kỳ nhóm các đầu nút công kích nào khác.

2 Các giao dịch

Chúng ta định nghĩa một đồng điện tử là một chuỗi các chữ ký điện tử. Mỗi người chủ sở hữu chuyển đồng tiền cho người sở hữu tiếp theo bằng cách ký một số băm của giao dịch trước đó và khóa công khai của của người chủ tiếp theo rồi thêm chữ ký này vào đuôi của đồng tiền. Người trả có thể xác thực chữ ký này để xác thực chuỗi sở hữu của đồng tiền này.

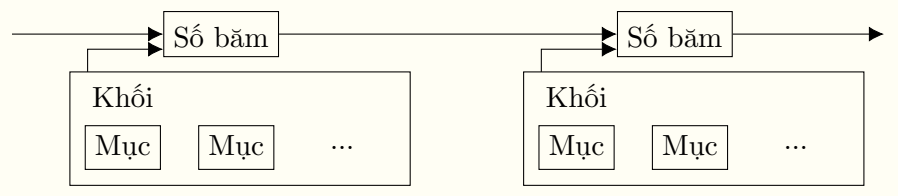


Vấn đề ở đây là người gửi tiền không thể xác thực rằng một trong số những người sở hữu đồng tiền đã không trùng chi đồng tiền này. Một giải pháp thường thấy là đưa vào một bên trung gian được tin cậy, hay nhà phát hành, với mục đích kiểm tra từng giao dịch xem có hiện tượng trùng chi hay không. Sau mỗi giao dịch, đồng tiền phải được đưa về cho nhà phát hành để tung ra một đồng tiền mới, và chỉ những đồng tiền do chính nhà phát hành tung ra mới được tin là đã không bị trùng chi. Vấn đề với giải pháp này là số phận của toàn bộ hệ thống phụ thuộc vào nhà phát hành, với tất cả giao dịch phải thông qua họ, giống như một ngân hàng.

Chúng ta cần tìm cách sao cho người trả tiền biết được những chủ sở hữu trước đó của đồng tiền đã không ký bất kỳ một giao dịch nào. Với mục đích của chúng ta, chỉ có giao dịch đầu tiên là giao dịch được công nhận, và chúng ta không phải quan tâm đến các ý định trùng chi sau đó. Cách duy nhất để xác định sự tồn tại của một giao dịch là phải nhận thức được tất cả các giao dịch. Trong mô hình dựa trên nhà phát hành, họ phải nhận thức được tất cả các giao dịch và quyết định xem giao dịch nào xảy ra trước. Để làm được điều này mà không cần đến một bên trung gian tin cậy, các giao dịch phải được thông báo một cách công khai (Dai 1998), và chúng ta cần một hệ thống sao cho những người tham gia nhất trí về một lịch sử duy nhất về thứ tự sở hữu của đồng tiền. Người trả tiền cần bằng chứng rằng vào thời điểm của mỗi giao dịch, phần lớn các điểm đầu nút đồng ý rằng đó là giao dịch đầu tiên của đồng tiền này.

3 Hệ thống máy chủ mốc thời gian

Giải pháp mà chúng ta đề xuất bắt đầu với một hệ thống máy chủ mốc thời gian. Một máy chủ mốc thời gian hoạt động bằng cách đánh mốc thời gian số băm của một khối gồm các hạng mục và công bố rộng rãi số băm này, giống như là trên báo hoặc trong mạng lưới Usenet (Massias, Avila, and Quisquater 1999; Haber and Stornetta 1990; Bayer, Haber, and Stornetta 1993; Haber and Stornetta 1997). Mốc thời gian này chứng minh rằng dữ liệu này hiển nhiên phải tồn tại vào thời điểm đó thì mới có thể được đưa vào hàm băm. Mỗi mốc thời gian bao gồm mốc thời gian trước đó trong số băm, tạo thành một chuỗi nối tiếp, với mỗi một mốc thời gian mới lại kiên cố cho những mốc thời gian trước nó.

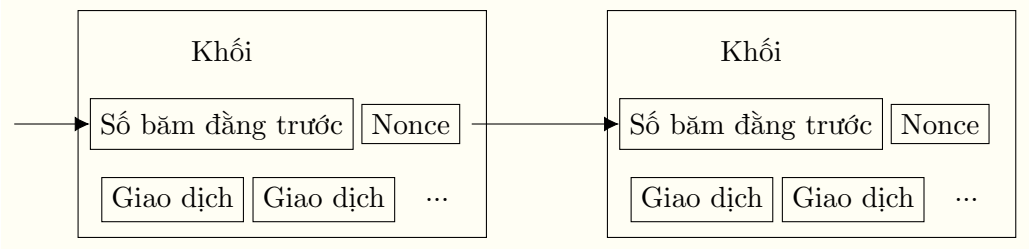


4 Bằng chứng lao động

Để thiết kế một máy chủ mốc thời gian phân quyền với nền tảng ngang hàng, chúng ta cần phải sử dụng một hệ thống bằng chứng lao động tương tự như Hashcash của Adam

Back (2002), không như là trên báo hoặc mạng lưới Usenet. Bằng chứng lao động liên quan đến việc tìm kiếm một giá trị mà khi đưa vào hàm băm, ví dụ như hàm SHA-256, số băm tạo ra sẽ bắt đầu bằng một số lượng bit 0 nào đó. Lực tính toán trung bình sẽ tăng theo cấp mũ của số lượng bit 0 mà ta yêu cầu và có thể được kiểm tra bằng cách thực hiện một phép băm duy nhất.

Đối với mạng lưới mốc thời gian đang xây dựng, ta thiết kế bằng chứng lao động bằng cách tăng tiến một số nonce trong khối cho đến khi tìm được một giá trị mà kết quả băm của nó bắt đầu với số bit 0 yêu cầu. Một khi lực tính toán CPU đã được sử dụng để thoả mãn bằng chứng lao động này, khối giao dịch không thể được hoàn tác mà không thực hiện lại công việc từ đầu. Khi các khối sau đã được móc nối vào khối này, để thay đổi nội dung của khối sẽ dẫn đến việc làm lại toàn bộ các khối đằng sau nó.



Bằng chứng lao động còn giải quyết vấn đề về việc thể hiện quyết định dựa trên đa số. Nếu khái niệm số đông được thực hiện dưới hình thức "mỗi địa chỉ IP một phiếu", nó có thể bị lật đổ bởi bất cứ ai có sở hữu rất nhiều IP. Bằng chứng lao động về căn bản là hình thức "mỗi CPU một phiếu". Nếu quyết định đa số được thể hiện bằng chuỗi dài nhất, tức là có nhiều lực tính toán đã được đầu tư vào đó nhất. Nếu phần lớn năng lượng CPU được kiểm soát bởi các điểm đầu nút trung thực, thì chuỗi khối trung thực sẽ phát triển nhanh nhất và vượt xa bất kỳ các chuỗi cạnh tranh nào khác. Để chỉnh sửa một khối trong quá khứ, kẻ tấn công sẽ phải thực hiện lại bằng chứng lao động của khối đó và tấn cả các khối đằng sau đó cho đến khi bắt kịp và vượt qua tiến độ của các điểm nút trung thực. Chúng ta sẽ thấy ở mục sau rằng xác suất một kẻ tấn công chậm hơn có thể bắt kịp sẽ suy giảm theo cấp số mũ của các khối nối tiếp đã được thêm vào.

5 Mạng lưới

Các bước để vận hành mạng lưới này như sau:

1. Các giao dịch mới được công bố cho tất cả các điểm đầu nút.
2. Mỗi điểm đầu nút thu thập các giao dịch vào trong các khối.
3. Mỗi điểm đầu nút thực hiện tính toán để tìm một bằng chứng lao động cho khối của nó.
4. Khi điểm đầu nút tìm ra bằng chứng lao động, nó sẽ loan báo cho tất cả các điểm đầu nút khác.

5. Các điểm đầu nút khác chấp nhận khối này chỉ khi tất cả giao dịch trong đó là hợp lệ và chưa từng được dùng trong giao dịch khác.

6. Các điểm đầu nút thể hiện sự chấp thuận khối này của mình bằng cách bắt đầu tính toán cho khối tiếp theo, sử dụng số băm của khối đã được chấp thuận như là kết quả băm của khối trước đó.

Các điểm đầu nút luôn luôn coi chuỗi dài nhất là chuỗi chính xác và sẽ luôn tìm cách để kéo dài nó. Nếu hai điểm đầu nút đồng thời công bố các phiên bản khác nhau của của khối tiếp theo, thì các nút trong mạng lưới sẽ tiếp nhận thông tin về một trong hai phiên bản trước phiên bản còn lại. Trong trường hợp đó, các điểm đầu nút sẽ tiếp tục làm việc trên nhánh chứa phiên bản chuỗi đầu tiên mà chúng nhận được, nhưng sẽ lưu nhánh của còn lại phòng khi nhánh đó có thể trở nên dài hơn sau này. Thế ngang bằng giữa hai nhánh sẽ bị phá vỡ một khi có bằng chứng lao động mới được tìm ra và một chuỗi trở nên dài hơn chuỗi còn lại; khi đó các điểm đầu nút đang làm việc bên nhánh ngắn hơn sẽ chuyển về nhánh dài hơn.

6 Động cơ

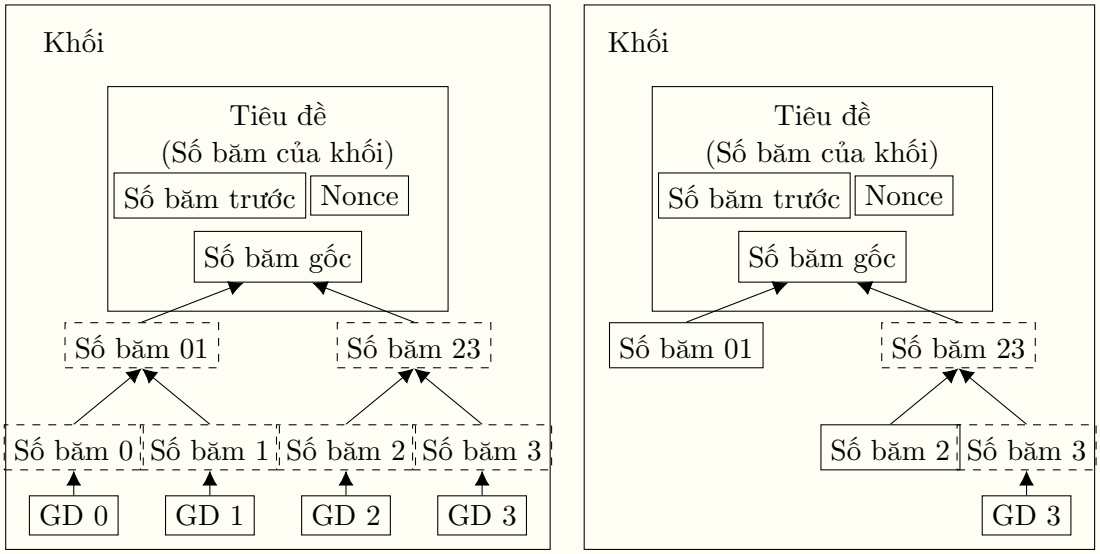
Theo quy ước, giao dịch đầu tiên trong mỗi khối là một giao dịch mà sẽ bắt đầu một đồng tiền mới thuộc quyền sở hữu của người tạo ra khối. Điều này làm tăng động cơ cho các điểm đầu nút tham gia hỗ trợ cho mạng lưới và cung cấp một cơ chế để đẩy những đồng tiền mới vào lưu thông, vì vốn không có một cơ quan thẩm quyền nào đứng ra để phát hành chúng cả. Việc đều đặn thêm một khối lượng tiền cố định vào lưu thông là tương đồng với việc những thợ đào đầu tư nguồn lực để tìm thêm vàng đưa vào lưu thông. Trong trường hợp này, thời gian và điện năng CPU chính là nguồn lực của chúng ta.

Phí giao dịch cũng có thể góp phần tăng cường động lực này. Nếu giá trị đầu ra của một giao dịch nhỏ hơn giá trị đầu vào của giao dịch đó, thì phần chênh lệch giữa hai giá trị này được coi như phí giao dịch và sẽ gia tăng giá trị động cơ cho khối nào chứa giao dịch này. Khi mà một số lượng tiền mới nhất định đã được đưa vào lưu thông, động cơ này có thể dần chuyển hóa thành chỉ bao gồm phí giao dịch và hệ thống sẽ hoàn toàn phi lạm phát.

Động cơ này cũng khuyến khích các điểm đầu nút hoạt động một cách trung thực. Nếu một kẻ tấn công tham lam nào đó có thể tập trung nhiều năng lực CPU hơn tất cả các điểm nút trung thực, anh ta sẽ phải lựa chọn giữa việc sử dụng nó để lừa gạt người khác bằng cách cướp lại số tiền mà anh ta đã sử dụng, hoặc dùng lực tính toán này để tạo ra tiền mới. Anh ta sẽ sớm nhận thấy rằng việc chơi theo quy tắc là có lợi hơn, vì quy tắc đó sẽ thưởng cho anh ta số lượng tiền nhiều hơn tất cả những người còn lại cộng lại, còn hơn là làm suy yếu cả hệ thống và cả tính hợp lệ của số tiền anh ta có.

7 Lấy lại không gian trên đĩa

Một khi giao dịch mới nhất trong đồng tiền được đào sâu dưới đủ số lượng khối, những giao dịch đằng trước nó có thể được bỏ đi để tiết kiệm không gian lưu trữ trên đĩa. Để tạo điều kiện cho việc này mà không ảnh hưởng đến số băm của các khối, các giao dịch sẽ được băm thông qua một cây Merkle (Merkle 1980; Massias, Avila, and Quisquater 1999; Haber and Stornetta 1997), và chỉ có gốc cây được bao gồm trong số băm của khối. Các khối cũ có thể được làm gọn bằng cách cắt bỏ các phần nhánh của cây. Các kết quả băm trung gian không cần phải được giữ lại.



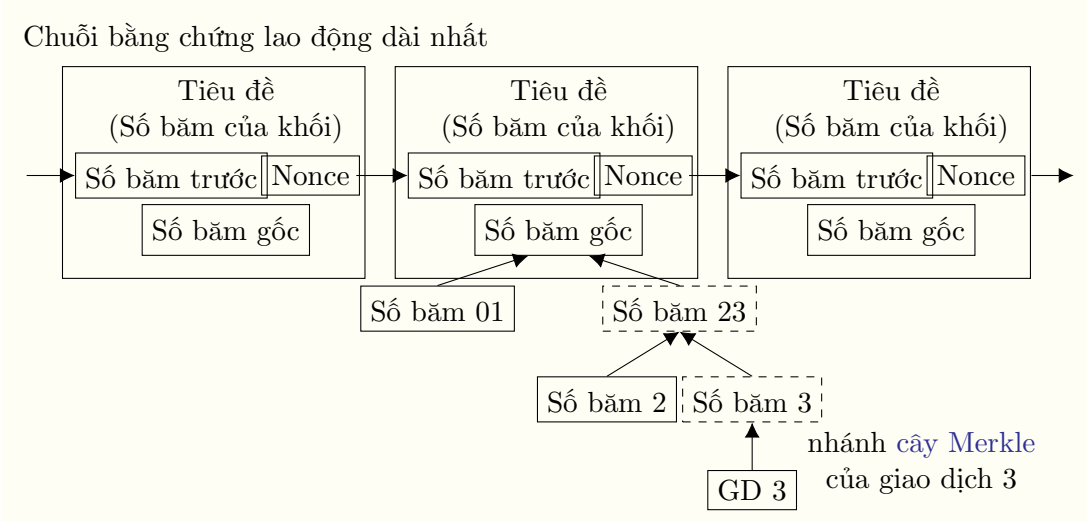
Giao dịch được băm qua một cây Merkle Sau khi lược bớt giao dịch 0-2 trong khối

Phần tiêu đề của một khối không có giao dịch có dung lượng tầm 80 byte. Nếu ta giả định rằng một khối mới được tạo ra mỗi 10 phút, 80 bytes $\times$ 6 $\times$ 24 $\times$ 365 = 4.2MB mỗi năm. Với các hệ thống máy tính thường được bán ra với 20GB RAM vào năm 2008, và mức tăng trưởng dự đoán là 1.2GB mỗi năm theo Định luật Moore, việc lưu trữ sẽ không thành vấn đề thậm chí chúng ta phải lưu trữ phần tiêu đề của tất cả các khối trong bộ nhớ.

8 Giao thức chứng thực giao dịch giản lược

Việc chứng thực các thanh toán mà không cần thiết phải chạy một đầu nút đầy đủ là có khả thi. Một người chỉ cần lưu giữ một bản sao phần tiêu đề của các khối có chuỗi bằng chứng lao động dài nhất, bản sao này có thể có được bằng cách truy vấn các điểm đầu nút trong mạng lưới cho đến khi anh ta thấy thuyết phục rằng anh ta đang có phiên bản chuỗi dài nhất, và nhận nhánh cây Merkle liên kết giao dịch với khối mà giao dịch

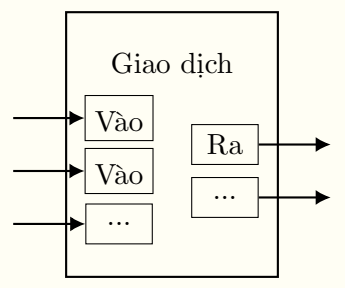
đó được đóng mốc thời gian. Anh ta không thể tự mình kiểm tra được giao dịch này, nhưng bằng cách gắn giao dịch này với một vị trí trong chuỗi khối, anh ta có thể thấy rằng mạng lưới các nút đã chấp nhận giao dịch đó, và các khối được thêm vào chuỗi sau đó càng khẳng định điều này.



Vì thế, việc chứng thực là đáng tin cậy chừng nào các điểm nút trung thực còn kiểm soát mạng lưới, nhưng sẽ nguy hiểm hơn nếu mạng lưới này bị áp đảo bởi một kẻ tấn công. Trong khi các điểm nút trong mạng lưới có thể tự xác thực giao dịch cho mình, phương pháp chứng thực giản lược này có thể bị lừa bởi giao dịch giả tạo đến từ một kẻ tấn công, chừng nào kẻ này còn áp đảo trong mạng lưới. Một chiến thuật phòng vệ là nghe lời cảnh báo từ các điểm nút trong mạng lưới khi chúng phát hiện một khối không hợp lệ, nhắc nhở người sử dụng phần mềm tải về phiên bản khối đầy đủ và báo cho các giao dịch khác phải xác thực sự không đồng nhất này. Những doanh nghiệp thường xuyên nhận được các đơn thanh toán hẳn vẫn sẽ muốn chạy đầu nút cho riêng mình để xác thực nhanh hơn và thực hiện bảo mật một cách độc lập hơn.

9 Kết hợp và phân chia giá trị

Mặc dù việc xử lý các đồng tiền một cách đơn lẻ là khả thi, việc tạo ra một giao dịch riêng cho mỗi một xu nhỏ trong giao dịch là khá cồng kềnh. Để giá trị có thể được chia tách và kết hợp, các giao dịch bao gồm nhiều đầu vào và đầu ra. Thông thường, hoặc là sẽ có một đầu vào duy nhất từ một giao dịch lớn hơn trước đó, hoặc là có nhiều đầu vào nhằm cộng gộp các khoản tiền nhỏ, cùng với ít nhất hai đầu ra của giao dịch: một là để dành cho thanh toán, và một để trả lại số tiền thừa cho người gửi, nếu có.

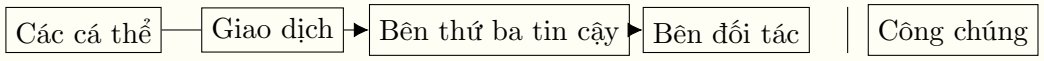


Cần phải chú ý rằng trường hợp phân tách, khi mà một giao dịch phụ thuộc vào một vài giao dịch khác, và các giao dịch đó phụ thuộc vào nhiều giao dịch khác nữa không phải là vấn đề ở đây. Việc trích xuất một bản sao tách biệt lịch sử của một giao dịch là không bao giờ cần thiết.

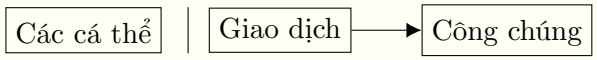
10 Tính bảo mật

Mô hình ngân hàng truyền thống đạt được mức độ bảo mật bằng cách giới hạn quyền tiếp cận thông tin của các bên tham gia và các bên trung gian tin cậy. Sự cần thiết của việc thông báo công khai tất cả các giao dịch là đi ngược lại với mô hình này, nhưng tính riêng tư vẫn có thể được duy trì bằng cách chia dòng chảy của thông tin theo hướng khác: ẩn danh các khóa công khai. Công chúng có thể thấy một ai đó gửi một lượng tiền cho người khác, nhưng không thể liên hệ giao dịch đó với bất cứ ai. Điều này cũng giống như mức độ thông tin mà các sàn giao dịch chứng khoán công bố, khi mà thời gian và quy mô của từng giao dịch - hay những "băng ghi âm" - được công bố công khai, nhưng không để lộ ra các bên giao dịch là những ai.

Mô hình bảo mật truyền thống



Mô hình bảo mật mới



Như một lớp tường lửa bảo mật nữa, mỗi giao dịch nên sử dụng một cặp khóa mới nhằm đảm bảo các khóa không liên hệ với một chủ sở hữu chung. Một số liên kết là không thể tránh được trong những giao dịch nhiều đầu vào, khi mà thông tin chỉ ra rằng các giá trị đầu vào đó là của cùng một chủ sở hữu. Rủi ro ở đây là nếu danh tính chủ sở hữu của một khóa bị tiết lộ, các liên kết cũng sẽ tiết lộ các giao dịch mà thuộc về cùng một chủ sở hữu này.

11 Một số tính toán

Ta xét trường hợp một kẻ tấn công tìm cách tạo ra một chuỗi khối mới nhanh hơn chuỗi khối trung thực. Kể cả nếu điều này có thể được thực hiện thành công, cũng không có nghĩa rằng anh ta có thể tùy ý tạo ra bất kỳ thay đổi nào trong hệ thống, như là tạo ra giá trị từ hư vô hay lấy số tiền chưa bao giờ thuộc quyền sở hữu của kẻ tấn công. Các điểm đầu nút đơn giản là sẽ không chấp nhận các thanh toán chứa giao dịch không hợp lệ, và sẽ không bao giờ chấp nhận bất kỳ một khối nào chứa chúng. Một kẻ tấn công chỉ có thể cố thay đổi một giao dịch mà anh ta đã tạo ra và nhận lại số tiền mà anh ta đã chi trong một giao dịch gần đây.

Cuộc đua giữa các điểm đầu nút trung thực và một kẻ tấn công có thể được mô tả như một Bước Ngẫu nhiên phân phối nhị thức. Một sự kiện thành công là chuỗi trung thực được nối dài thêm một khối, tăng khoảng cách dẫn trước của nó thêm +1, và sự kiện thất bại là chuỗi của kẻ tấn công nối dài thêm một khối, giảm khoảng cách đi −1.

Xác suất một kẻ tấn công có thể bắt kịp khi bắt đầu sau là tương tự như bài toán Sạt nghiệp của Con bạc. Giả sử người đánh bạc với nguồn tiền không giới hạn bắt đầu từ thế thua và chơi một số lượng vô hạn ván nhằm cố gắng gỡ hòa. Chúng ta có thể tính xác suất anh ta có thể gỡ hòa, hay xác suất kẻ tấn công có thể bắt kịp với chuỗi khối trung thực như sau (Feller 1968):

- p = xác suất một điểm nút trung thực tìm ra khối tiếp theo
- q = xác suất kẻ tấn công tìm ra khối tiếp theo
- q_z = xác suất kẻ tấn công sẽ bắt kịp từ z khối đằng sau

$$q_z = \begin{cases} 1 & \text{nếu } p \leq q \\ (q/p)^z & \text{nếu } p > q \end{cases}$$

Với giả thiết rằng $p > q$, xác suất sẽ giảm theo cấp số mũ của số khối mà kẻ tấn công phải bắt kịp. Đối mặt với tỉ lệ bất lợi, nếu kẻ tấn công không gặp may mắn ngay từ đầu, cơ hội của anh ta sẽ trở nên càng lúc càng nhỏ khi mà anh ta tiếp tục bị bỏ xa đằng sau.

Chúng ta tiếp tục xét xem người nhận của một giao dịch mới cần phải chờ bao lâu trước khi đủ chắc chắn rằng người gửi không thể thay đổi giao dịch được nữa. Chúng ta giả sử người gửi là một kẻ tấn công, và muốn khiến cho người nhận tin rằng anh ta đã trả tiền được một thời gian, rồi chuyển sang trả tiền cho chính mình một lúc sau đó. Người nhận sẽ được thông báo khi chuyện đó xảy ra, nhưng người gửi mong rằng lúc đó đã quá trễ.

Người gửi nhận được một cặp khóa mới và giao khóa công khai cho người gửi ngay sau khi ký. Điều này ngăn người gửi khỏi việc chuẩn bị sẵn một chuỗi các khối bằng cách xử lý, tính toán liên tục cho đến khi anh ta đủ may mắn để có thể tiến xa phía trước, rồi thực thi giao dịch tại thời điểm đó. Một khi giao dịch đã được gửi đi, người gửi không

trung thực này bắt đầu tạo ra một phiên bản chuỗi song song chứa giao dịch của anh ta.

Người nhận chờ đến khi giao dịch đã được thêm vào khối và z khối đã được nối đằng sau đó. Anh ta không biết được chính xác tiến độ của kẻ tấn công, nhưng giải thiết rằng các khối trung thực được tạo ra với thời gian trung bình kì vọng cho từng khối, mức độ chuẩn bị tiềm năng của kẻ nhóm tấn công là một phân phối Poisson với giá trị kì vọng:

$$\lambda = z\frac{q}{p}$$

Để tính xác suất mà kẻ tấn công có thể đuổi kịp vào thời điểm này, chúng ta nhân hàm mật độ Poisson của khối lượng tiến độ mà anh ta có thể đạt được với xác suất anh có thể bắt kịp tại mỗi thời điểm:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \begin{cases} (q/p)^{(z-k)} & \text{nếu } k \leq z \\ 1 & \text{nếu } k > z \end{cases}$$

Ta sắp xếp lại để tránh cộng phải các giá trị vô hạn ở phần đuôi của phân phối:

$$1 - \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Ta viết dưới dạng ngôn ngữ C:

```c
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
  double p = 1.0 - q;
  double lambda = z * (q / p);
  double sum = 1.0;
  int i, k;
  for (k = 0; k <= z; k++)
    {
      double poisson = exp(-lambda);
      for (i = 1; i <= k; i++)
        poisson *= lambda / i;
      sum -= poisson * (1 - pow(q / p, z - k));
    }
  return sum;
}
```

Chạy một số kết quả, chúng ta có thể thấy xác suất giảm theo cấp số mũ theo chiều tăng của z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Giải bài toán đối với P nhỏ hơn 0.1%...

```
P < 0.001
q=0.10  z=5
q=0.15  z=8
q=0.20  z=11
q=0.25  z=15
q=0.30  z=24
q=0.35  z=41
q=0.40  z=89
q=0.45  z=340
```

12 Kết luận

Chúng ta đề xuất một hệ thống giao dịch điện tử mà không phụ thuộc vào sự tin cậy. Ta bắt đầu bằng nền tảng thông thường của các đồng tiền tạo ra bằng chữ ký điện tử,

cho phép kiểm soát quyền sở hữu rất chặt chẽ, nhưng không thể hoàn thiện vì thiếu cách để ngăn chặn hiện tượng trùng chi. Để giải quyết vấn đề này, chúng ta đưa ra một mạng lưới ngang hàng sử dụng bằng chứng lao động để lưu trữ một lịch sử công khai của các giao dịch, đồng thời nhanh chóng khiến cho việc kẻ tấn công thay đổi thông tin đã lưu trữ là không khả thi về mặt thuật toán, chừng nào các điểm nút trung thực còn kiểm soát đa số lực CPU trong hệ thống. Mạng lưới này mạnh mẽ ở tính đơn giản và phi cấu trúc của nó. Các điểm đầu nút hoạt động cùng một lúc mà không cần phối hợp nhiều với nhau. Chúng không cần phải được định danh, vì các thông tin không dẫn tới một địa điểm cụ thể nào và chỉ cần được loan truyền với tinh thần nhiều nhất có thể. Các điểm đầu nút có thể rời bỏ và trở về với mạng lưới tùy ý, chỉ cần chấp nhận chuỗi bằng chứng lao động là minh chứng cho những sự kiện xảy ra trong lúc chúng vắng mặt. Các đầu nút tham gia bỏ phiếu bằng lực CPU, thể hiện sự đồng thuận đối với các khối giao dịch hợp lệ bằng cách kéo dài chúng và từ chối các khối không hợp lệ bằng cách không xử lý các khối đó. Bất kỳ quy tắc và động cơ cần thiết nào cũng có thể được thúc đẩy bằng cơ chế đồng thuận này.

Danh mục thuật ngữ

bài toán Sạt nghiệp của Con bạc Gambler's Ruin problem. 9

Bước Ngẫu nhiên Random Walk. 9

bằng chứng lao động Proof-of-Work. 1, 3–6, 12

cây Merkle Merkle tree. 6, 7

khóa cá nhân private key. 2

khóa công khai public key. 2, 8, 9

nhà phát hành mint. 3

số nonce nonce. 4

tiền vật lý physical currency. 2

trùng chi Double-spending. 1–3, 12

Tài liệu

Back, Adam et al. (2002). *Hashcash-a denial of service counter-measure*. URL: www.hashcash.org/papers/hashcash.pdf.

Massias, H., X. Serret Avila, and J.-J. Quisquater (1999). "Design Of A Secure Timestamping Service With Minimal Trust Requirement". In: *the 20th Symposium on Information Theory in the Benelux*.

Dai, Wei (1998). "b-money, 1998". In: *http://www.weidai.com/bmoney.txt*.

Haber, Stuart and W Scott Stornetta (1997). "Secure names for bit-strings". In: *Proceedings of the 4th ACM Conference on Computer and Communications Security*. ACM, pp. 28–35.

Bayer, Dave, Stuart Haber, and W Scott Stornetta (1993). "Improving the efficiency and reliability of digital time-stamping". In: *Sequences II: Methods in Communication, Security and Computer Science*, pp. 329–334.

Haber, Stuart and W. Scott Stornetta (Aug. 11, 1990). "How to Time-Stamp a Digital Document". In: *Advances in Cryptology-CRYPT0' 90*. Conference on the Theory and Application of Cryptography. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, pp. 437–455. ISBN: 978-3-540-54508-8 978-3-540-38424-3. DOI: 10.1007/3-540-38424-3_32. URL: https://link.springer.com/chapter/10.1007/3-540-38424-3_32 (visited on 01/10/2018).

Merkle, Ralph C (1980). "Protocols for public key cryptosystems". In: *Security and Privacy, 1980 IEEE Symposium on*. IEEE, pp. 122–122.

Feller, William (1968). *An Introduction to Probability Theory and Its Applications, Vol. 1, 3rd Edition*. 3rd edition. S.l.: Wiley. 509 pp. ISBN: 978-0-471-25708-0.