Bitcoin: Hệ thống tiền tệ điện tử ngang hàng

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Tóm tắt nội dung

Hệ thống tiền tệ điện tử ngang hàng là hệ thống cho phép các khoản thanh toán được gửi trực tiếp từ một thành viên tới một thành viên khác mà không cần thông qua các tổ chức tài chính. Các chữ ký số cung cấp một phần giải pháp hệ thống, nhưng những lợi ích chính sẽ bị mất nếu một bên thứ ba tin cậy vẫn được yêu cầu ngăn chặn gian lận double-spending. Chúng tôi đề xuất một giải pháp cho vấn đề double-spending sử dụng mạng lưới ngang hàng. Bằng cách băm thành chuỗi liên tục các "bằng chứng công việc" (proof-of-work) dựa vào bảng băm, các giao dịch sử dụng mạng lưới nhãn thời gian sẽ tạo thành một bản ghi mà không thể thay đổi nếu không làm lại "bằng chứng công việc". Chuỗi dài nhất sẽ không chỉ được dùng làm bằng chứng của chuỗi các sự kiện đã chứng kiến, mà còn chứng minh rằng nó đến chủ yếu từ sức mạnh của CPU. Miễn là phần lớn sức mạnh CPU còn được kiểm soát bởi các nút thật, chúng sẽ sinh ra chuỗi dài nhất và vượt qua những chuỗi tấn công. Bản thân mạng lưới giao dịch yêu cầu phải có cấu trúc tối thiểu. Các tin nhắn sẽ được truyền đi với hiệu quả tốt nhất, và các nút có thể rời khỏi rồi tham gia trở lại mạng lưới theo ý muốn, nhận chuỗi "bằng chứng công việc" làm bằng chứng cho những gì đã diễn ra khi các nút đó rời mạng lưới.

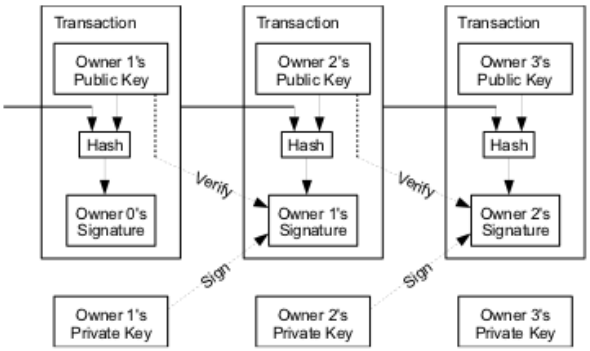
1 Giới thiệu

Thương mại trên mạng Internet đã gần như hoàn toàn coi các tổ chức tài chính là bên thứ ba được tin cậy để xử lý các thanh toán điện tử. Trong khi làm việc khá tốt đối với hầu hết các giao dịch, hệ thống này vẫn tồn tại những điểm yếu cố hữu của mô hình tín nhiệm (the trust based model). Các giao dịch mà hoàn toàn không thể đảo ngược không thực sự là có thể xảy ra được, vì các tổ chức tài chính không thể tránh được các tranh chấp trung gian. Chi phí trung gian làm tăng cao các chi phí giao dịch, hạn chế mức giao dịch tối thiểu và làm giảm khả năng giao dịch với các mức giao dịch nhỏ thông thường, và phải mất chi phí cao hơn để thực hiện các thanh toán không thể đảo ngược cho các dịch vụ không thể đảo ngược. Với khả năng đảo ngược, nhu cầu tín nhiệm đã lan rộng. Các thương gia phải thận trọng với khách hàng của họ, sách nhiễu họ bởi nhiều thông tin hơn bình thường họ cần. Một tỉ lệ gian lận nhất định đã được công nhận là không thể tránh khỏi. Các chi phí và thanh toán không chắc chắn này có thể tránh được bằng cách sử dụng tiền tệ vật lý, nhưng không có cơ chế nào tồn tại để thực hiện các thanh toán qua một kênh thông tin liên lạc mà thiếu một bên được tin cậy.

Vậy thứ ta cần là một hệ thống thanh toán điện tử dựa vào bằng chứng mật mã thay vì tín nhiệm, cho phép hai bên sẵn sàng có thể giao dịch trực tiếp với nhau mà không cần đến một bên thứ ba được tin cậy nào cả. Các giao dịch được tính toán để không đảo ngược được sẽ bảo vệ người bán khỏi gian lận, và các cơ chế ký quỹ có thể được thực hiện dễ dàng nhằm bảo vệ người mua. Trong bài báo này, chúng tôi đề xuất một giải pháp cho vấn đề double-spending sử dụng máy chủ nhãn thời gian phân phối ngang hàng để sinh bằng chứng tính toán cho các giao dịch theo thứ tự thời gian. Hệ thống này rất an toàn, miễn là các nút thật tập trung kiểm soát được phần sức mạnh CPU lớn hơn các nhóm nút hợp tác tấn công.

2 Các giao dịch

Chúng tôi định nghĩa một đồng tiền điện tử là một chuỗi các chữ ký số. Mỗi chủ sở hữu chuyển đồng tiền cho người tiếp theo bằng cách ký số một bảng băm gồm giao dịch trước và khóa công khai của người sở hữu tiếp theo và thêm chúng vào cuối đồng tiền. Người được nhận tiền có thể xác nhận các chữ ký để xác nhận chuỗi sở hữu.



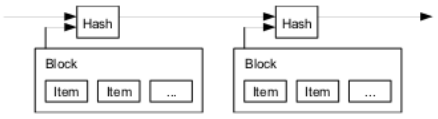
Vấn đề ở đây tất nhiên là người nhận tiền không thể xác nhận rằng một trong những người sở hữu đã không thực hiện gian lận double-spend đối với đồng tiền. Sau mỗi giao dịch, đồng tiền sẽ phải trở lại nguồn cung cấp để xuất ra một đồng tiền mới, và chỉ có những đồng tiền được xuất trực tiếp từ nguồn cung cấp đó mới được tin là không gian lận. Vấn đề với giải pháp này là số phận của toàn bộ hệ thống tiền tệ phụ thuộc vào công ty cung cấp, tức là mỗi giao dịch phải đi qua đó, như một ngân hàng.

Chúng ta cần một cách để người nhận tiền có thể biết rằng những người sở hữu trước đã không ký giao dịch nào trước đó. Đối với mục đích của chúng tôi, giao dịch đầu tiên sẽ là giao dịch thực hiện đếm, nên chúng tôi không quan tâm đến việc cố gắng thực hiện các gian lận double-spend sau đó. Cách duy nhất để xác nhận sự vắng mặt của một giao dịch là phải nhận biết được tất cả các giao dịch. Trong mô hình dựa vào nguồn cung cấp, nguồn cấp phải quan tâm đến tất cả các giao dịch và quyết định giao dịch nào đến trước. Để làm được điều đó mà không cần bên thứ ba tin cậy, các giao dịch phải được công bố công khai [1], và chúng ta cần một hệ thống để những người tham gia có sự đồng thuận về một lịch sử giao dịch duy nhất theo thứ tự mà họ đã được nhận. Người nhận tiền phải có bằng chứng rằng ở thời điểm thực hiện mỗi giao dịch, phần lớn các nút đồng ý rằng đó là lần nhận đầu tiên.

3 Máy chủ nhãn thời gian

Giải pháp mà chúng tôi đề xuất bắt đầu với một máy chủ nhãn thời gian. Máy chủ nhãn thời gian làm việc bằng cách lấy một bảng băm của một khối các mục để gán nhãn thời gian rồi công bố rộng rãi bảng băm đó, qua một bài báo hay Usenet [2-5] chẳng hạn. Nhãn thời gian chứng tỏ rằng dữ liệu

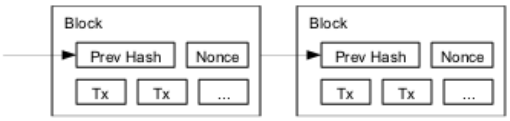
phải rõ ràng tồn tại ở thời điểm lưu trong nhãn thời gian đó, để có thể được đưa vào bảng băm. Mỗi nhãn thời gian gồm nhãn thời gian liền trước trong bảng băm của nó, tạo thành một chuỗi, với mỗi nhãn thời gian thêm vào sau lại gia cố nhãn thời gian trước đó.



4 Bằng chứng công việc

Để thực thi hệ thống máy chủ nhãn thời gian phân phối trên cơ sở ngang hàng, chúng ta cần sử dụng một hệ thống bằng chứng công việc tương tự như Hashcash của Adam Back [6], chứ không chỉ là các bài báo hay Usenet. Bằng chứng công việc bao hàm việc quét một giá trị mà khi được băm, ví dụ như với SHA-256, bảng băm bắt đầu với một số bit 0. Mức công việc trung bình cần thiết là cấp số nhân của số bit 0 cần thiết và có thể xác nhận bằng cách thi hành một bảng băm đơn.

Đối với mạng lưới nhãn thời gian, chúng tôi thi hành bằng chứng công việc bằng cách tăng thêm một số ngẫu nhiên (nonce) trong khối cho đến khi tìm thấy một giá trị cho bảng băm của khối số bit 0 đã yêu cầu. Một khi hiệu năng của CPU được sử dụng để thỏa mãn bằng chứng công việc, khối đó sẽ không thể bị thay đổi mà không thực hiện lại công việc. Khi các khối về sau được nối chuỗi vào nó, muốn thay đổi khối phải làm lại tất cả các khối sau nó nữa.



Bằng chứng công việc cũng giải quyết vấn đề xác định phản kháng trong việc đưa ra quyết định về phần đa số. Nếu phần đa số dựa vào một-địa-chỉ-IP-một-phiếu, thì có thể bị phá hỏng nếu ai đó có khả năng cấp phát nhiều địa chỉ IP. Bằng chứng công việc bản chất là dựa vào một-CPU-một-phiếu. Quyết định đa số được biểu diễn bởi chuỗi dài nhất, tức là chuỗi có hiệu

quả làm bằng chứng công việc cao nhất. Nếu phần đa số của hiệu năng CPU được kiểm soát bởi các nút thực, chuỗi thật sẽ lớn nhanh nhất và vượt qua bất cứ chuỗi cạnh tranh nào khác. Để thay đổi được một khối đã qua, kẻ tấn công phải làm lại bằng chứng công việc của khối đó và tất cả các khối sau nó rồi bắt kịp và vượt qua công việc của các nút thực. Sau này chúng tôi sẽ chỉ ra rằng xác suất của một kẻ tấn công bắt kịp chậm hơn giảm theo cấp số nhân khi các khối tiếp theo được thêm vào.

Để bù cho việc tốc độ phần cứng ngày càng tăng và những lợi ích khác nhau trong việc chạy các nút theo thời gian, độ khó của bằng chứng công việc được xác định bởi số khối giao dịch trung bình mỗi giờ. Các khối đó được sinh ra càng nhanh, độ khó càng tăng.

5 Mạng lưới

Dưới đây là các bước vận hành của mạng lưới:

1. Các giao dịch mới được truyền đến tất cả các nút.
2. Mỗi nút tập hợp các giao dịch mới vào một khối.
3. Mỗi nút tìm một bằng chứng công việc khó cho khối của nó.
4. Khi một nút tìm được bằng chứng công việc, nó sẽ truyền đến tất cả các nút khác.
5. Các nút chỉ chấp nhận khối nếu tất cả các giao dịch trong khối đó là hợp lệ và chưa được sử dụng.
6. Các nút diễn đạt sự chấp nhận với khối giao dịch bằng cách tạo khối giao dịch tiếp theo trong chuỗi, sử dụng bảng băm của khối đã chấp nhận làm bảng trước.

Các nút luôn xem chuỗi dài nhất là chuỗi đúng và sẽ mở rộng chuỗi đó. Nếu hai nút truyền hai bản khác nhau của khối tiếp theo cùng một lúc, một số nút sẽ nhận được một trong hai bản trước. Trong trường hợp đó, chúng sẽ sử dụng bản đầu tiên mà chúng nhận được, nhưng sẽ dùng nhánh còn lại trong trường hợp chuỗi đó dài hơn. Sự ràng buộc sẽ bị phá vỡ khi bằng chứng công việc tiếp theo được tìm thấy và một nhánh trở nên dài hơn; các nút đang sử dụng nhánh còn lại sẽ chuyển sang dùng nhánh dài hơn.

Các giao dịch mới được truyền đi không nhất thiết phải đến được tất cả các nút. Miễn là các giao dịch đó vẫn đến được nhiều nút, chúng sẽ được thêm vào khối. Các khối truyền đi cũng có thể không đến được một vài nút. Nếu một nút không nhận được một khối giao dịch, khi nó nhận được khối tiếp theo và nhận ra mình đang thiếu một khối, nó sẽ yêu cầu lại khối đó.

6 Ưu đãi

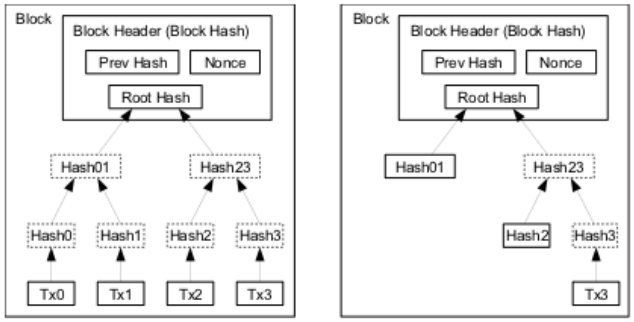
Theo quy ước, giao dịch đầu tiên trong một khối là một giao dịch đặc biệt bắt đầu một đồng tiền mới của người tạo khối giao dịch. Điều này thêm ưu đãi cho các nút để hỗ trợ mạng lưới, và cung cấp một cách để bắt đầu phân phối các đồng tiền vào dòng lưu thông, khi không có trung tâm chịu trách nhiệm phát hành. Việc thêm một số lượng đồng tiền mới nhất định cũng tương tự như những người khai thác vàng tiêu dùng nguồn tài nguyên để thêm vàng vào dòng lưu thông. Trong trường hợp của chúng tôi, đó chính là tiêu dùng thời gian chạy CPU và điện. Quỹ ưu đãi có thể được tạo bằng cách thu phí giao dịch. Nếu giá trị đầu ra của một giao dịch nhỏ hơn giá trị đầu vào, sẽ có một sự khác biệt là có một khoản phí giao dịch được thêm vào giá trị ưu đãi của khối chứa giao dịch. Khi có một số lượng tiền xác định trước tham gia vào dòng lưu thông, toàn bộ ưu đãi có thể chuyển tiếp thành phí giao dịch và hoàn toàn không bị lạm phát.

Sự ưu đãi có thể giúp các nút không bị làm giả. Nếu một kẻ tấn công tham lam nào đó có thể tập hợp lượng sức mạnh CPU lớn hơn tất cả các nút thực, hắn sẽ phải chọn giữa việc sử dụng sức mạnh đó để lừa đảo mọi người bằng cách ăn trộm lại chính các thanh toán của mình, hoặc sử dụng để sinh ra những đồng tiền mới. Hắn phải thấy rằng chơi đúng luật sẽ có lợi hơn, những quy tắc có lợi cho anh ta với nhiều tiền mới hơn tất cả những người khác hợp lại, hơn là phá hoại chính hệ thống và giá trị pháp lý của tài sản riêng của mình.

7 Cải thiện không gian đĩa

Khi giao dịch mới nhất trong một đồng tiền đã được thêm vào sau một số lượng khối giao dịch vừa đủ, các giao dịch đã được sử dụng trước nó có thể sẽ được loại bỏ để tiết kiệm không gian đĩa. Để có thể thuận tiện hơn mà không phải phá vỡ bảng băm của khối giao dịch, các giao dịch được băm

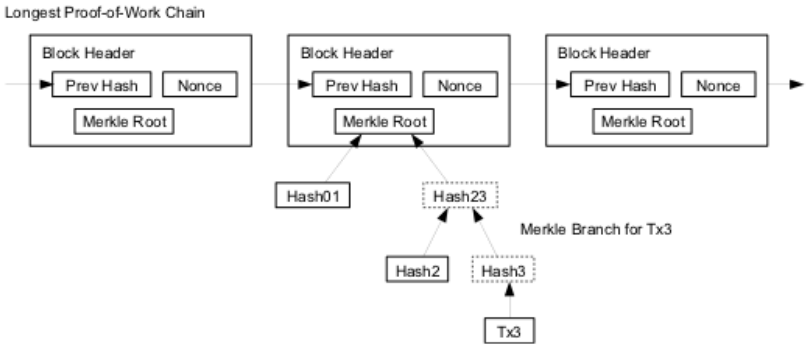
thành một cây Merkle (Merkle Tree) [7][2][5], trong đó chỉ có gốc nằm trong bảng băm của khối giao dịch. Các khối cũ sau đó có thể được nén lại bằng cách cắt các nhánh của cây đó. Không cần phải lưu các bảng băm ở phía trong lại.



Tiêu đề của một khối mà không có giao dịch nào sẽ có kích cỡ khoảng 80 byte. Nếu chúng ta giả sử rằng các khối được sinh ra mỗi 10 phút, 80 bytes * 6 * 24 * 365 = 4.2MB mỗi năm. Với các hệ thống máy tính điển hình với 2GB RAM của năm 2008, và định luật Moore dự đoán sức phát triển hiện tại là 1.2GB mỗi năm, không gian lưu trữ sẽ không phải là vấn đề nếu các tiêu đề của các khối giao dịch phải được giữ trong bộ nhớ.

8 Đơn giản hóa quá trình xác nhận thanh toán

Ta có thể xác nhận các thanh toán mà không cần chạy một nút mạng đầy đủ. Người dùng chỉ cần giữ một bản sao của các tiêu đề khối giao dịch của chuỗi bằng chứng công việc dài nhất, là chuỗi mà anh ta có thể lấy được bằng cách truy vấn các nút mạng cho đến khi anh ta tin chắc rằng anh ta đã có được chuỗi dài nhất, và có được nhánh Merkle liên kết giao dịch với khối giao dịch tương ứng. Anh ta không thể tự kiểm tra giao dịch, nhưng bằng cách liên kết giao dịch đó tới một vị trí trong chuỗi bằng chứng công việc, anh ta có thể thấy rằng một nút mạng đã chấp nhận nó, và các khối được thêm vào sau đó sẽ càng xác nhận rằng mạng lưới đã chấp nhận giao dịch này.

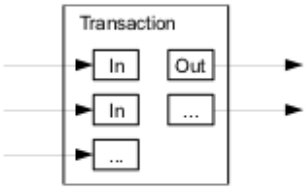


Như vậy, việc xác nhận là đáng tin cậy miễn là các nút thực vẫn kiểm soát mạng lưới, nhưng việc xác nhận sẽ có thể bị tấn công nếu mạng lưới bị những kẻ tấn công chế ngự. Khi các nút mạng có thể tự xác nhận các giao dịch, phương pháp rút gọn lại có thể bị lừa bởi các giao dịch tạo sẵn của những kẻ tấn công khi chúng còn có thể tiếp tục chế ngự mạng lưới. Chiến lược để chống lại việc làm này chính là nhận các cảnh báo từ các nút mạng khi họ phát hiện ra một khối nào đó không hợp lệ, nhắc nhở phần mềm của người dùng tải toàn bộ khối giao dịch và các giao dịch có cảnh báo để xác minh sự mâu thuẫn. Các doanh nghiệp mà thường xuyên nhận thanh toán chắc hẳn vẫn muốn tự chạy các nút riêng của họ để có sự bảo mật riêng biệt và xác nhận nhanh hơn.

9 Hợp và tách giá trị

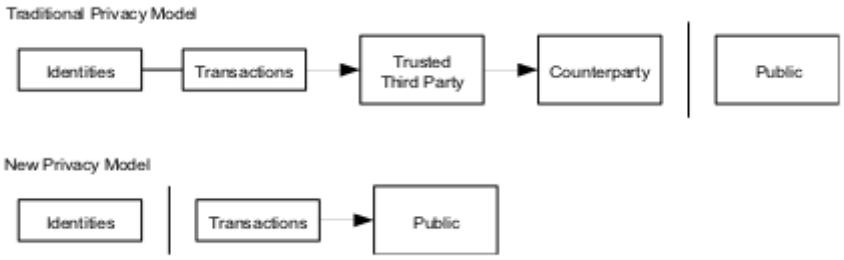
Mặc dù ta có thể sử dụng những đồng tiền riêng lẻ với nhau, nhưng việc tạo các giao dịch riêng biệt cho mỗi đồng tiền trong một lần vận chuyển sẽ dẫn đến khó sử dụng. Để cho phép các giá trị có thể tách ra v hợp lại, các giao dịch sẽ chứa nhiều đầu vào và đầu ra. Thông thường sẽ có cả đầu vào đơn từ một giao dịch lớn hơn trước đó hoặc đầu vào đa hợp nhiều số lượng nhỏ lại, và hầu hết là hai đầu ra: một cho việc thanh toán, và một trả về sự thay đổi cho người gửi, nếu có.

Lưu ý rằng việc tách các giá trị cũng không phải là vấn đề ở đây ngay cả khi một giao dịch dựa trên nhiều giao dịch khác nhau, và các giao dịch khác nhau đó lại dựa trên nhiều giao dịch khác nhau nữa. Không bao giờ là cần thiết khi trích xuất một bản sao độc lập hoàn chỉnh của lịch sử của một giao dịch.



10 Sự riêng tư

Các mô hình ngân hàng truyền thống đạt được một mức độ về sự riêng tư bằng cách giới hạn truy cập đến thông tin của các thành viên trong đó và thành phần thứ ba được tin tưởng. Sự cần thiết phải công bố tất cả các giao dịch một cách công khai loại trừ phương pháp này, nhưng sự riêng tư vẫn có thể được duy trì bằng cách ngắt dòng thông tin đến một nơi khác: bằng cách giấu tên các khóa công khai. Mạng lưới công khai có thể thấy rằng ai đó đang gửi một lượng tiền cho ai đó khác, nhưng không có thông tin kết nối giao dịch tới bất cứ ai cả. Điều này tương tự như mức độ công bố thông tin giao dịch chứng khoán, trong đó thời gian và kích thước của các giao dịch cá nhân, các "băng", được công bố công khai, nhưng không cho biết các bên ở đây gồm những ai.



Giống như thêm một bức tường lửa, một cặp khóa mới sẽ được sử dụng cho mỗi giao dịch để giữ liên kết từ mỗi giao dịch đó tới người sở hữu chung. Các giao dịch có đầu vào đa cũng không thể tránh được phải sử dụng một vài liên kết, vì các giao dịch đó cũng cần được biểu thị rằng chúng được sở hữu bởi cùng một người. Sự mạo hiểm ở đây là nếu như người sở hữu của một khóa nào đó bị tiết lộ, thì các liên kết sẽ để lộ cả các giao dịch khác của người đó.

11 Tính toán

Chúng tôi đã xem xét kịch bản một của kẻ tấn công khi hắn cố sinh ra một chuỗi thay thế nhanh hơn chuỗi thật. Ngay cả khi làm được điều này, hệ thống cũng vẫn sẽ không bị mở để thay đổi tùy ý, như bí mật tạo ra một giá trị nào đó hoặc lấy tiền mà của người khác. Các nút sẽ không chấp nhận một giao dịch không hợp lệ là thanh toán, và các nút thực sẽ không bao giờ chấp nhận một khối giao dịch chứa các giao dịch đó. Một kẻ tấn công chỉ có thể cố gắng thay đổi một trong các giao dịch mà hắn sở hữu để lấy lại số tiền anh ta mới tiêu.

Cuộc đua giữa chuỗi thật và một chuỗi tấn công có thể mô tả như một bước ngẫu nhiên nhị thức (Binomial Random Walk). Biến cố thành công là biến cố chuỗi thực được mở rộng thêm một khối, củng cố vị trí dẫn trước thêm 1, và biến cố thất bại là biến cố mà chuỗi tấn công được mở rộng thêm một khối, giảm khoảng cách đi 1.

Xác suất một kẻ tấn công có thể bắt kịp từ một mức hụt cho trước cũng tương tự như vấn đề về sự phá sản của một con bạc. Giả sử có một con bạc với mức tín dụng không giới hạn bắt đầu từ một mức thiếu hụt nào đó và chơi vô vàn những ván bạc để cố gắng hòa vốn. Chúng ta có thể tính được xác suất mà ông ta có thể hòa vốn, hoặc cũng là xác suất mà một kẻ tấn công có thể bắt kịp chuỗi bằng chứng công việc thật, như dưới đây [8]:

p = xác suất một nút thật tìm thấy khối tiếp theo

q = xác suất nút tấn công tìm thấy khối tiếp theo

qz = xác suất kẻ tấn công có thể bắt kịp từ khoảng cách z khối giao dịch

$$q_z = \left\{ \begin{array}{ll} 1 & \text{nếu } p \leq q \\ \left(\frac{p}{q}\right)^z & \text{nếu } p > q \end{array} \right\}$$

Với giả định của chúng tôi rằng p > q, xác suất giảm theo cấp số nhân khi số các khối giao dịch kẻ tấn công phải bắt kịp tăng lên. Với sự chênh lệch chống lại hắn như thế, nếu hắn không làm được một đường kiếm may mắn sớm, cơ hội của hắn sẽ tiêu tan dần và hắn sẽ càng tụt về xa hơn ở phía sau.

Bây giờ chúng ta xem người nhận trong một giao dịch mới sẽ phải đợi bao lâu trước khi chắc chắn rằng người gửi sẽ không thể thay đổi giao dịch. Giả sử người gửi là một kẻ tấn công đang muốn người nhận tin rằng hắn sẽ thanh toán cho anh ta ngay trong một thời gian ngắn, sau đó chuyển sang thanh toán lại cho chính mình sau khi một khoảng thời gian đã trôi qua.

Người nhận sẽ được cảnh báo khi điều này xảy ra, nhưng người gửi thì hi vọng rằng thông tin cảnh báo sẽ đến muộn.

Người nhận sinh ra một cặp khóa mới và trao khóa công khai tới người gửi ngay trước khi ký. Điều này giúp ngăn chặn người gửi chuẩn bị chuỗi các khối giao dịch trước thời hạn bằng cách làm việc liên tục cho đến khi may mắn có được đoạn chuỗi đủ dài, sau đó thi hành giao dịch ngay tại thời điểm ấy. Một khi giao dịch đã được gửi đi, kẻ lừa đảo đó sẽ bắt đầu bí mật làm một chuỗi song song chứa bản thay thế của giao dịch của hắn ta.

Người nhận sẽ đợi cho đến khi giao dịch được thêm vào một khối giao dịch và z khối khác đã liên kết với nó. Anh ta sẽ không biết kẻ tấn công đã làm được bao nhiêu, nhưng coi như mỗi khối giao dịch thật cần một khoảng thời gian trung bình, thì tiến độ của kẻ tấn công phải là một hàm phân phối Poisson với giá trị phải là:

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

Để có được xác suất mà kẻ tấn công có thể bắt kịp bây giờ, chúng ta nhân hàm mật độ Poisson của mỗi bước tiến mà có thể hắn đã thực hiện với xác suất hắn có thể bắt kịp từ điểm đó:

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

Biến đổi biểu thức, ta có...

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

Chuyển sang ngôn ngữ 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 với một vài kết quả, chúng ta có thể thấy xác suất giảm theo hàm mũ với 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
```

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 Tổng kết

Chúng tôi đã đề xuất một hệ thống cho các giao dịch điện tử mà không cần dựa vào tín nhiệm. Chúng tôi đã bắt đầu với cơ cấu thông thường về tiền tệ làm bằng các chữ ký số, đó là một cơ cấu cung cấp những kiểm soát rất mạnh về sự sở hữu, nhưng chưa hoàn chỉnh nếu không có một phương pháp ngăn chặn double-spending. Để giải quyết vấn đề này, chúng tôi đã đề xuất một mạng lưới ngang hàng sử dụng bằng chứng công việc để ghi lại lịch sử công khai của các giao dịch mà những kẻ tấn công sẽ không thể tính toán để thay đổi được nếu các nút thật kiểm soát được phần lớn sức mạnh CPU. Mạng lưới đã mạnh mẽ trong sự đơn giản không cấu trúc của nó. Các nút làm việc cùng một lúc với một chút phối hợp. Chúng không cần được xác định, khi các tin nhắn sẽ không định hướng đến một nơi cụ thể nào cả và chỉ cần được truyền đi một hiệu năng cơ sở cao nhất. Các nút có thể rời khỏi và tham gia trở lại mạng lưới bất cứ lúc nào, nhận chuỗi bằng chứng công việc làm bằng chứng cho những gì đã xảy ra khi các nút đó rời khỏi mạng lưới. Các nút sẽ xác nhận thông qua bằng sức mạnh CPU của họ, biểu diễn việc chấp nhận các khối hợp lệ bằng cách mở rộng các khối đó và loại bỏ các khối không hợp lệ bằng cách từ chối làm việc với chúng. Các quy tắc và ưu đãi cần thiết có thể được thi hành với cơ chế đồng thuận này.

Tài liệu liên quan

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on

Information Theory in the Benelux, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.