Bitcoin: Hệ thống tiền mặt điện tử ngang hàng

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

Tóm tắt. Một phiên bản tiền điện tử hoàn toàn ngang hàng sẽ cho phép thanh toán trực tuyến được gửi trực tiếp từ bên này sang bên kia mà không cần thông qua tổ chức tài chính. Chữ ký số cung cấp một phần của giải pháp, nhưng những lợi ích chính sẽ bị mất đi nếu vẫn cần một bên thứ ba đáng tin cậy để ngăn chặn chi tiêu trùng lặp.
Chúng tôi đề xuất giải pháp cho vấn đề chi tiêu gấp đôi bằng cách sử dụng mạng ngang hàng. Mạng lưới đánh dấu thời gian giao dịch bằng cách băm chúng thành một chuỗi bằng chứng công việc dựa trên băm đang diễn ra, tạo thành một bản ghi không thể thay đổi nếu không thực hiện lại bằng chứng công việc. Chuỗi dài nhất không chỉ đóng vai trò là bằng chứng về chuỗi sự kiện được chứng kiến, mà còn là bằng chứng cho thấy nó đến từ nhóm sức mạnh CPU lớn nhất. Miễn là phần lớn sức mạnh CPU được kiểm soát bởi các nút không hợp tác để tấn công mạng, chúng sẽ tạo ra chuỗi dài nhất và vượt qua những kẻ tấn công. Bản thân mạng lưới chỉ yêu cầu cấu trúc tối thiểu. Các thông điệp được truyền đi trên cơ sở nỗ lực tối đa, và các nút có thể rời khỏi và tham gia lại mạng lưới tùy ý, chấp nhận chuỗi bằng chứng công việc dài nhất làm bằng chứng về những gì đã xảy ra trong khi chúng vắng mặt.

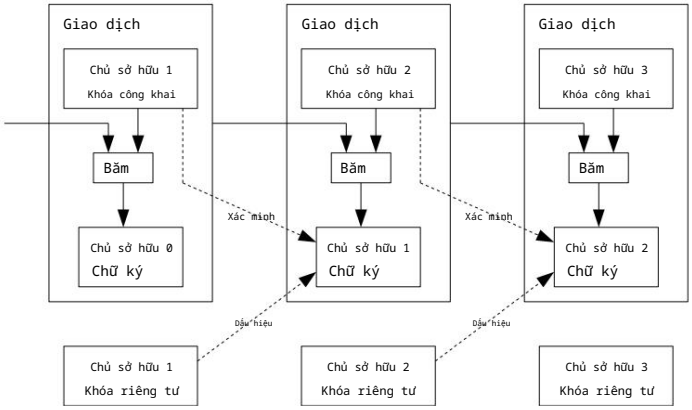
1. Giới thiệu

Thương mại trên Internet gần như hoàn toàn phụ thuộc vào các tổ chức tài chính đóng vai trò là bên thứ ba đáng tin cậy để xử lý thanh toán điện tử. Mặc dù hệ thống hoạt động khá tốt cho hầu hết các giao dịch, nhưng nó vẫn còn những điểm yếu cố hữu của mô hình dựa trên niềm tin.
Các giao dịch hoàn toàn không thể đảo ngược thực sự không khả thi, vì các tổ chức tài chính không thể tránh khỏi việc hòa giải tranh chấp. Chi phí hòa giải làm tăng chi phí giao dịch, hạn chế quy mô giao dịch tối thiểu thực tế và cắt giảm khả năng thực hiện các giao dịch nhỏ lẻ, và còn có chi phí lớn hơn khi mất khả năng thực hiện các khoản thanh toán không thể đảo ngược cho các dịch vụ không thể đảo ngược. Với khả năng đảo ngược, nhu cầu về lòng tin ngày càng lan rộng. Các thương nhân phải cảnh giác với khách hàng của mình, gây phiền hà cho họ để có thêm thông tin hơn mức họ cần.
Một tỷ lệ gian lận nhất định được coi là không thể tránh khỏi. Những chi phí này và sự không chắc chắn trong thanh toán có thể được tránh bằng cách sử dụng tiền mặt trực tiếp, nhưng không có cơ chế nào để thực hiện thanh toán qua kênh truyền thông mà không có bên thứ ba đáng tin cậy.

Điều cần thiết là một hệ thống thanh toán điện tử dựa trên bằng chứng mật mã thay vì niềm tin, cho phép bất kỳ hai bên nào sẵn sàng giao dịch trực tiếp với nhau mà không cần bên thứ ba đáng tin cậy. Các giao dịch không thể đảo ngược về mặt tính toán sẽ bảo vệ người bán khỏi gian lận, và các cơ chế ký quỹ thông thường có thể dễ dàng được triển khai để bảo vệ người mua. Trong bài báo này, chúng tôi đề xuất một giải pháp cho vấn đề chi tiêu gấp đôi bằng cách sử dụng máy chủ dấu thời gian phân tán ngang hàng để tạo bằng chứng tính toán về thứ tự thời gian của các giao dịch. Hệ thống sẽ an toàn miễn là các nút trung thực cùng nhau kiểm soát nhiều sức mạnh CPU hơn bất kỳ nhóm nút tấn công nào hợp tác.

2. Giao dịch

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

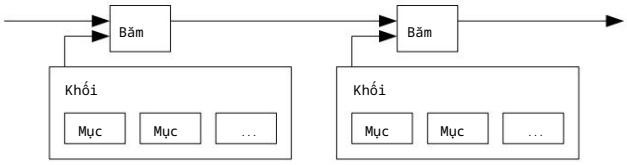


Vấn đề tất nhiên là người nhận tiền không thể xác minh được một trong hai chủ sở hữu không chi tiêu gấp đôi đồng tiền. Một giải pháp phổ biến là thành lập một cơ quan trung ương đáng tin cậy, hay còn gọi là xưởng đúc tiền, để kiểm tra mọi giao dịch xem có chi tiêu gấp đôi hay không. Sau mỗi giao dịch, đồng tiền phải được trả lại xưởng đúc tiền để phát hành đồng tiền mới, và chỉ những đồng tiền được phát hành trực tiếp từ xưởng đúc tiền mới được tin cậy là không bị chi tiêu gấp đôi. Vấn đề với giải pháp này là số phận của toàn bộ hệ thống tiền tệ phụ thuộc vào công ty điều hành xưởng đúc tiền, khi mọi giao dịch đều phải thông qua họ, giống như một ngân hàng vậy.

Chúng ta cần một cách để người nhận tiền biết rằng chủ sở hữu trước đó không ký bất kỳ giao dịch nào trước đó. Đối với mục đích của chúng tôi, giao dịch sớm nhất là giao dịch được tính, vì vậy chúng tôi không quan tâm đến các nỗ lực chi tiêu gấp đôi sau này. Cách duy nhất để xác nhận sự vắng mặt của giao dịch là nhận biết tất cả các giao dịch. Trong mô hình dựa trên xưởng đúc tiền, xưởng đúc tiền nhận biết tất cả các giao dịch và quyết định giao dịch nào đến trước. Để thực hiện điều này mà không cần một bên đáng tin cậy, các giao dịch phải được công bố công khai [1] và chúng tôi cần một hệ thống để những người tham gia đồng ý về một lịch sử duy nhất về thứ tự nhận được chúng. Người nhận tiền cần có bằng chứng cho thấy tại thời điểm của mỗi giao dịch, phần lớn các nút đã đồng ý rằng đó là giao dịch đầu tiên được nhận.

3. Máy chủ dấu thời gian

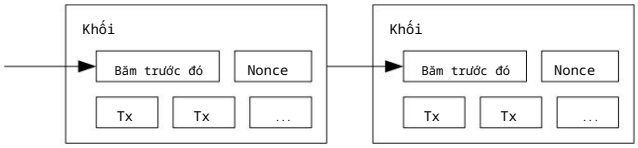
Giải pháp chúng tôi đề xuất bắt đầu với một máy chủ dấu thời gian. Máy chủ dấu thời gian hoạt động bằng cách lấy một hàm băm của một khối các mục cần đóng dấu thời gian và công bố hàm băm rộng rãi, chẳng hạn như trên báo hoặc bài đăng trên Usenet [2-5]. Dấu thời gian chứng minh rằng dữ liệu phải tồn tại tại thời điểm đó, rõ ràng là vậy, để có thể được đưa vào hàm băm. Mỗi dấu thời gian bao gồm dấu thời gian trước đó trong hàm băm của nó, tạo thành một chuỗi, với mỗi dấu thời gian bổ sung củng cố các dấu thời gian trước đó.



4. Bằng chứng công việc

Để triển khai máy chủ dấu thời gian phân tán trên cơ sở ngang hàng, chúng ta sẽ cần sử dụng hệ thống bằng chứng công việc tương tự như Hashcash của Adam Back [6], thay vì các bài đăng trên báo hoặc Usenet.
Bằng chứng công việc bao gồm việc quét tìm một giá trị mà khi được băm, chẳng hạn như với SHA-256, giá trị băm bắt đầu bằng một số bit 0. Lượng công việc trung bình cần thiết tăng theo cấp số nhân với số bit 0 cần thiết và có thể được xác minh bằng cách thực hiện một băm duy nhất.

Đối với mạng lưới dấu thời gian của chúng tôi, chúng tôi triển khai bằng chứng công việc bằng cách tăng một nonce trong khối cho đến khi tìm thấy một giá trị cung cấp cho hàm băm của khối các bit 0 cần thiết. Một khi CPU đã được sử dụng để thỏa mãn bằng chứng công việc, khối không thể được thay đổi mà không thực hiện lại công việc. Vì các khối sau được nối tiếp sau nó, công việc thay đổi khối sẽ bao gồm việc thực hiện lại tất cả các khối sau nó.



Bằng chứng công việc cũng giải quyết vấn đề xác định tính đại diện trong quá trình ra quyết định của đa số. Nếu đa số dựa trên một địa chỉ IP, một phiếu bầu, thì bất kỳ ai có thể phân bổ nhiều IP đều có thể lật đổ nó. Bằng chứng công việc về cơ bản là một CPU, một phiếu bầu. Quyết định của đa số được thể hiện bằng chuỗi dài nhất, chuỗi có nỗ lực bằng chứng công việc lớn nhất được đầu tư vào. Nếu phần lớn sức mạnh CPU được kiểm soát bởi các nút trung thực, thì chuỗi trung thực sẽ phát triển nhanh nhất và vượt qua bất kỳ chuỗi cạnh tranh nào. Để sửa đổi một khối trước đó, kẻ tấn công sẽ phải làm lại bằng chứng công việc của khối đó và tất cả các khối sau đó, sau đó bắt kịp và vượt qua công việc của các nút trung thực. Chúng tôi sẽ chỉ ra sau rằng khả năng kẻ tấn công chậm hơn bắt kịp sẽ giảm theo cấp số nhân khi các khối tiếp theo được thêm vào.

Để bù đắp cho tốc độ phần cứng ngày càng tăng và sự quan tâm thay đổi trong việc vận hành các nút theo thời gian, độ khó của bằng chứng công việc được xác định bằng một đường trung bình động nhắm đến số khối trung bình mỗi giờ. Nếu chúng được tạo ra quá nhanh, độ khó sẽ tăng lên.

5. Mạng lưới

Các bước để chạy mạng như sau:

1) Các giao dịch mới được phát tới tất cả các nút.
2) Mỗi nút thu thập các giao dịch mới vào một khối.
3) Mỗi nút hoạt động để tìm bằng chứng công việc khó khăn cho khối của mình.
4) Khi một nút tìm thấy bằng chứng công việc, nó sẽ phát khối đó tới tất cả các nút.
5) Các nút chỉ chấp nhận khối nếu tất cả các giao dịch trong khối đó đều hợp lệ và chưa được chi tiêu.
6) Các nút thể hiện sự chấp nhận khối của chúng bằng cách làm việc để tạo khối tiếp theo trong chuỗi, sử dụng hàm băm của khối được chấp nhận làm hàm băm trước đó.

Các nút luôn coi chuỗi dài nhất là chuỗi chính xác và sẽ tiếp tục mở rộng nó. Nếu hai nút phát sóng các phiên bản khác nhau của khối tiếp theo cùng lúc, một số nút có thể nhận được phiên bản này hoặc phiên bản kia trước. Trong trường hợp đó, chúng sẽ xử lý phiên bản đầu tiên nhận được, nhưng vẫn giữ lại nhánh còn lại phòng trường hợp nó trở nên 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 xử lý nhánh kia sẽ chuyển sang nhánh dài hơn.

Phát sóng giao dịch mới không nhất thiết phải đến được tất cả các nút. Miễn là chúng đến được nhiều nút, chúng sẽ sớm được đưa vào một khối. Phát sóng khối cũng chấp nhận các tin nhắn bị mất. Nếu một nút không nhận được một khối, nó sẽ yêu cầu khối đó khi nhận được khối tiếp theo và nhận ra rằng nó đã bỏ lỡ một khối.

6. Khuyến khích

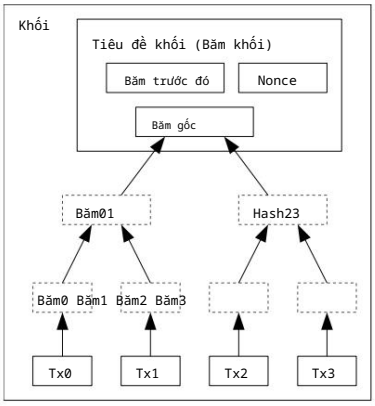
Theo quy ước, giao dịch đầu tiên trong một khối là một giao dịch đặc biệt khởi tạo một đồng tiền mới thuộc sở hữu của người tạo khối. Điều này tạo thêm động lực cho các nút hỗ trợ mạng lưới và cung cấp một cách thức ban đầu để phân phối tiền vào lưu thông, vì không có cơ quan trung ương nào phát hành chúng.
Việc bổ sung đều đặn một lượng tiền xu mới không đổi tương tự như việc thợ đào vàng phải tiêu tốn tài nguyên để đưa vàng vào lưu thông. Trong trường hợp này, thứ bị tiêu tốn là thời gian CPU và điện năng.

Ưu đãi cũng có thể được tài trợ bằng phí giao dịch. Nếu giá trị đầu ra của một giao dịch nhỏ hơn giá trị đầu vào, phần chênh lệch sẽ là phí giao dịch được cộng vào giá trị ưu đãi của khối chứa giao dịch đó. Khi một số lượng coin nhất định được đưa vào lưu thông, ưu đãi có thể chuyển hoàn toàn sang phí giao dịch và hoàn toàn không bị ảnh hưởng bởi lạm phát.

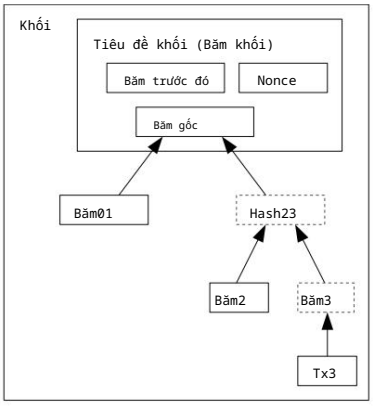
Động lực này có thể giúp khuyến khích các nút trung thực. Nếu một kẻ tấn công tham lam có thể tập hợp được nhiều sức mạnh CPU hơn tất cả các nút trung thực, hắn ta sẽ phải lựa chọn giữa việc sử dụng nó để lừa đảo người khác bằng cách lấy lại khoản thanh toán của mình, hoặc sử dụng nó để tạo ra các đồng coin mới. Hắn ta nên thấy việc tuân thủ luật lệ, những luật lệ mang lại lợi ích cho hắn ta với nhiều đồng coin mới hơn tất cả những người khác cộng lại, sẽ có lợi hơn là làm suy yếu hệ thống và tính hợp lệ của tài sản của chính mình.

7. Lấy lại dung lượng đĩa

Khi giao dịch mới nhất trong một đồng tiền được chôn dưới đủ số khối, các giao dịch đã chi tiêu trước đó có thể được loại bỏ để tiết kiệm dung lượng đĩa. Để thuận tiện cho việc này mà không làm hỏng hàm băm của khối, các giao dịch được băm trong Cây Merkle [7][2][5], với chỉ phần gốc được bao gồm trong hàm băm của khối.
Sau đó, các khối gỗ cũ có thể được nén chặt bằng cách cắt bỏ các cành cây. Các khối gỗ bên trong không cần phải được lưu trữ.



Giao dịch được băm trong cây Merkle

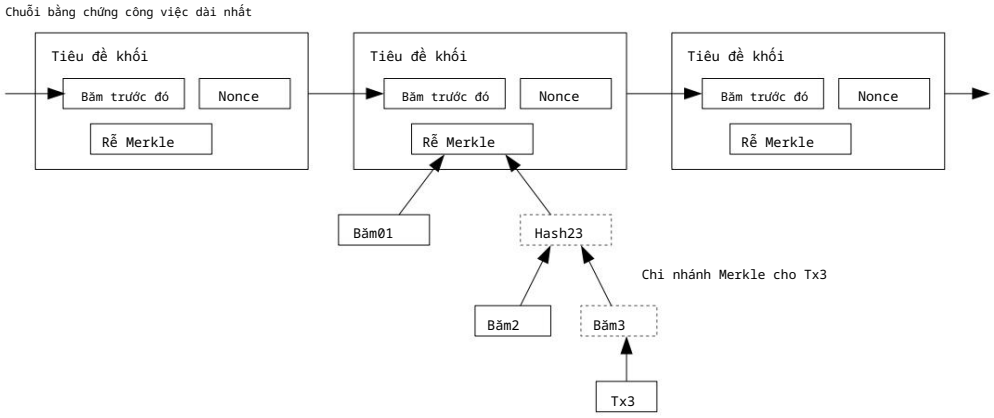


Sau khi cắt tỉa Tx0-2 khỏi khối

Tiêu đề khối không có giao dịch sẽ có dung lượng khoảng 80 byte. Giả sử các khối được tạo ra cứ sau 10 phút, thì 80 byte * 6 * 24 * 365 = 4,2 MB mỗi năm. Với các hệ thống máy tính thường được bán với 2 GB RAM tính đến năm 2008, và Định luật Moore dự đoán mức tăng trưởng hiện tại là 1,2 GB mỗi năm, việc lưu trữ sẽ không phải là vấn đề ngay cả khi tiêu đề khối phải được lưu trong bộ nhớ.

8. Xác minh thanh toán đơn giản

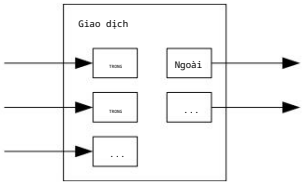
Có thể xác minh thanh toán mà không cần chạy toàn bộ một nút mạng. Người dùng chỉ cần giữ một bản sao tiêu đề khối của chuỗi bằng chứng công việc dài nhất, có thể lấy được bằng cách truy vấn các nút mạng cho đến khi chắc chắn mình có chuỗi dài nhất, và lấy nhánh Merkle liên kết giao dịch với khối chứa dấu thời gian của giao dịch. Người dùng không thể tự mình kiểm tra giao dịch, nhưng bằng cách liên kết giao dịch với một vị trí trong chuỗi, họ có thể thấy rằng một nút mạng đã chấp nhận giao dịch đó, và các khối được thêm vào sau đó xác nhận thêm rằng mạng đã chấp nhận giao dịch đó.



Do đó, việc xác minh vẫn đáng tin cậy miễn là các nút trung thực kiểm soát mạng, nhưng sẽ dễ bị tấn công hơn nếu mạng bị kẻ tấn công áp đảo. Mặc dù các nút mạng có thể tự xác minh giao dịch, nhưng phương pháp đơn giản hóa này có thể bị đánh lừa bởi các giao dịch giả mạo của kẻ tấn công miễn là kẻ tấn công vẫn có thể tiếp tục áp đảo mạng. Một chiến lược để bảo vệ chống lại điều này là chấp nhận cảnh báo từ các nút mạng khi chúng phát hiện một khối không hợp lệ, nhắc nhở phần mềm của người dùng tải xuống toàn bộ khối và các giao dịch được cảnh báo để xác nhận sự không nhất quán. Các doanh nghiệp nhận thanh toán thường xuyên có thể vẫn muốn chạy các nút riêng của họ để bảo mật độc lập hơn và xác minh nhanh hơn.

9. Kết hợp và chia tách giá trị

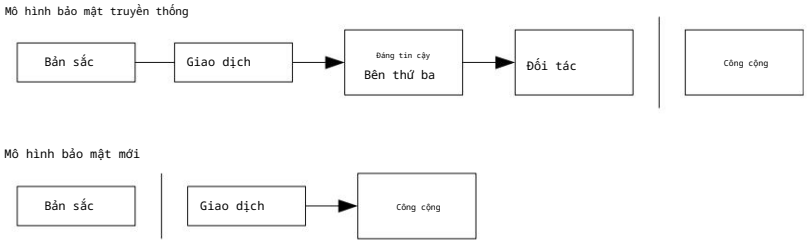
Mặc dù có thể xử lý từng đồng xu riêng lẻ, nhưng việc tạo một giao dịch riêng cho mỗi xu trong một lần chuyển khoản sẽ rất bất tiện. Để cho phép phân chia và kết hợp giá trị, các giao dịch bao gồm nhiều đầu vào và đầu ra. Thông thường, sẽ có một đầu vào duy nhất từ một giao dịch lớn hơn trước đó hoặc nhiều đầu vào kết hợp các khoản tiền nhỏ hơn, và tối đa hai đầu ra: một cho khoản thanh toán và một trả lại tiền thừa, nếu có, cho người gửi.



Cần lưu ý rằng việc phân tán dữ liệu (fan-out), tức là một giao dịch phụ thuộc vào nhiều giao dịch khác, và các giao dịch này lại phụ thuộc vào nhiều giao dịch khác nữa, không phải là vấn đề ở đây. Không bao giờ cần phải trích xuất một bản sao hoàn chỉnh, độc lập của lịch sử giao dịch.

10. Quyền riêng tư

Mô hình ngân hàng truyền thống đạt được mức độ riêng tư nhất định bằng cách hạn chế quyền truy cập thông tin cho các bên liên quan và bên thứ ba đáng tin cậy. Việc phải công bố công khai tất cả các giao dịch ngăn cản phương pháp này, nhưng quyền riêng tư vẫn có thể được duy trì bằng cách chặn luồng thông tin ở một nơi khác: bằng cách giữ khóa công khai ẩn danh. Công chúng có thể thấy ai đó đang gửi một khoản tiền cho người khác, nhưng không có thông tin nào liên kết giao dịch với bất kỳ ai. Điều này tương tự như mức độ thông tin được công bố bởi các sàn giao dịch chứng khoán, nơi thời gian và quy mô của từng giao dịch, hay còn gọi là "băng ghi âm", được công khai, nhưng không cho biết các bên tham gia là ai.



Như một tường lửa bổ sung, một cặp khóa mới nên được sử dụng cho mỗi giao dịch để ngăn chúng bị liên kết với một chủ sở hữu chung. Việc liên kết vẫn là không thể tránh khỏi với các giao dịch đa đầu vào, điều này chắc chắn sẽ tiết lộ rằng dữ liệu đầu vào của chúng thuộc sở hữu của cùng một chủ sở hữu. Rủi ro là nếu chủ sở hữu của một khóa bị tiết lộ, việc liên kết có thể tiết lộ các giao dịch khác thuộc cùng một chủ sở hữu.

11. Tính toán

Chúng tôi xem xét kịch bản kẻ tấn công cố gắng tạo ra một chuỗi thay thế nhanh hơn chuỗi trung thực. Ngay cả khi điều này thành công, nó cũng không khiến hệ thống bị ảnh hưởng bởi những thay đổi tùy ý, chẳng hạn như tạo ra giá trị từ hư không hoặc lấy đi số tiền không thuộc về kẻ tấn công. Các nút sẽ không chấp nhận một giao dịch không hợp lệ làm phương thức thanh toán, và các nút trung thực sẽ không bao giờ chấp nhận một khối chứa chúng. Kẻ tấn công chỉ có thể cố gắng thay đổi một trong các giao dịch của chính mình để lấy lại số tiền đã chi tiêu gần đây.

Cuộc đua giữa chuỗi trung thực và chuỗi tấn công có thể được mô tả như một bước đi ngẫu nhiên nhị thức. Sự kiện thành công là chuỗi trung thực được mở rộng thêm một khối, tăng khoảng cách dẫn trước lên +1, và sự kiện thất bại là chuỗi tấn công được mở rộng thêm một khối, giảm khoảng cách đi -1.

Xác suất kẻ tấn công bắt kịp từ một khoản thâm hụt nhất định tương tự như bài toán Gambler's Ruin. Giả sử một người chơi có tín dụng không giới hạn bắt đầu ở mức thâm hụt và có khả năng chơi vô số lần để cố gắng đạt điểm hòa vốn. Chúng ta có thể tính xác suất anh ta đạt điểm hòa vốn, hay xác suất kẻ tấn công bắt kịp chuỗi trung thực, như sau [8]:

p = xác suất một nút trung thực tìm thấy khối tiếp theo
q = xác suất kẻ tấn công tìm thấy khối tiếp theo qz
= xác suất kẻ tấn công sẽ bắt kịp từ z khối phía sau

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

Với giả định p > q, xác suất giảm theo cấp số nhân khi số khối mà kẻ tấn công phải bắt kịp tăng lên. Với tỷ lệ cược bất lợi, nếu kẻ tấn công không may mắn tấn công ngay từ đầu, cơ hội của hắn sẽ trở nên cực kỳ nhỏ bé khi hắn càng tụt lại phía sau.

Bây giờ, chúng ta xem xét người nhận của một giao dịch mới cần chờ bao lâu trước khi đủ chắc chắn rằng người gửi không thể thay đổi giao dịch. Chúng ta giả định người gửi là một kẻ tấn công muốn khiến người nhận tin rằng hắn đã trả tiền cho hắn trong một thời gian, rồi sau đó chuyển sang trả lại cho chính hắn sau một khoảng thời gian. Người nhận sẽ được cảnh báo khi điều đó xảy ra, nhưng người gửi hy vọng rằng mọi chuyện sẽ quá muộn.

Người nhận tạo một cặp khóa mới và cung cấp khóa công khai cho người gửi ngay trước khi ký. Điều này ngăn người gửi chuẩn bị một chuỗi khối trước bằng cách liên tục xử lý nó cho đến khi đủ may mắn để đạt được bước tiến xa hơn, rồi thực hiện giao dịch ngay tại thời điểm đó. Sau khi giao dịch được gửi đi, người gửi không trung thực sẽ bắt đầu bí mật làm việc trên một chuỗi song song chứa phiên bản thay thế của giao dịch.

Người nhận sẽ đợi cho đến khi giao dịch được thêm vào một khối và z khối đã được liên kết sau đó. Người nhận không biết chính xác tiến độ mà kẻ tấn công đã đạt được, nhưng giả sử các khối trung thực mất thời gian trung bình dự kiến cho mỗi khối, thì tiến độ tiềm năng của kẻ tấn công sẽ là một phân phối Poisson với giá trị kỳ vọng:

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

Để có được xác suất kẻ tấn công vẫn có thể bắt kịp lúc này, chúng ta nhân mật độ Poisson cho mỗi lượng tiến bộ mà hắn có thể đạt được với xác suất hắn có thể bắt kịp từ thời điểm đó:

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

Sắp xếp lại để tránh tính tổng phần đuôi vô hạn của phân phối...

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

Đang chuyển đổi sang mã C...

```
#include <math.h> double
AttackerSuccessProbability(double q, int z) {

      p kép = 1,0 - q; lambda kép = z * (q /
      p); tổng kép = 1,0; int i, k; đối với (k = 0; k <= z; k+
      +) {



            poisson kép = exp(-lambda); với (i = 1; i <=
            k; i++)
                  poisson *= lambda / i; tổng -=
            poisson * (1 - pow(q / p, z - k));

      } trả về tổng;
}
```

Chạy một số kết quả, chúng ta có thể thấy xác suất giảm theo cấp số nhân 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
```

Giải cho 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 tôi đã đề xuất một hệ thống giao dịch điện tử mà không cần dựa vào lòng tin. Chúng tôi bắt đầu với khuôn khổ thông thường về tiền điện tử được tạo ra từ chữ ký số, cung cấp khả năng kiểm soát quyền sở hữu mạnh mẽ, nhưng sẽ không hoàn thiện nếu không có cách ngăn chặn chi tiêu gấp đôi. Để giải quyết vấn đề này, chúng tôi đã đề xuất một mạng ngang hàng sử dụng bằng chứng công việc để ghi lại lịch sử giao dịch công khai, điều này sẽ nhanh chóng trở nên bất khả thi về mặt tính toán đối với kẻ tấn công nếu các nút trung thực kiểm soát phần lớn sức mạnh CPU. Mạng lưới này mạnh mẽ nhờ sự đơn giản, không có cấu trúc. Các nút hoạt động cùng lúc với ít sự phối hợp. Chúng không cần được xác định, vì các tin nhắn không được định tuyến đến bất kỳ vị trí cụ thể nào và chỉ cần được gửi đi theo cơ chế nỗ lực tối đa. Các nút có thể rời khỏi và tham gia lại mạng lưới tùy ý, chấp nhận chuỗi bằng chứng công việc làm bằng chứng cho những gì đã xảy ra trong khi chúng vắng mặt. Chúng bỏ phiếu bằng sức mạnh CPU của mình, thể hiện sự chấp nhận các khối hợp lệ bằng cách mở rộng chúng và từ chối các khối không hợp lệ bằng cách từ chối xử lý chúng. Bất kỳ quy tắc và khuyến khích cần thiết nào cũng có thể được thực thi với cơ chế đồng thuận này.

Tài liệu tham khảo

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

[2] H. Massias, XS Avila và J.-J. Quisquater, "Thiết kế dịch vụ đóng dấu thời gian an toàn với yêu cầu tin cậy tối thiểu", Trong Hội nghị chuyên đề lần thứ 20 về Lý thuyết thông tin tại Benelux, tháng 5 năm 1999.

[3] S. Haber, WS Stornetta, "Cách đóng dấu thời gian cho một tài liệu kỹ thuật số", Trong Tạp chí Mật mã học, tập 3, số 2, trang 99-111, 1991.

[4] D. Bayer, S. Haber, WS Stornetta, "Cải thiện hiệu quả và độ tin cậy của dấu thời gian kỹ thuật số," Trong Chuỗi II: Phương pháp trong Truyền thông, Bảo mật và Khoa học máy tính, trang 329-334, 1993.

[5] S. Haber, WS Stornetta, "Tên an toàn cho chuỗi bit," Trong Biên bản Hội nghị ACM lần thứ 4 về An ninh máy tính và truyền thông, trang 28-35, tháng 4 năm 1997.

[6] A. Back, "Hashcash - một biện pháp đối phó với từ chối dịch vụ," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] RC Merkle, "Giao thức cho hệ thống mật mã khóa công khai," Trong Proc. 1980 Hội nghị chuyên đề về Bảo mật và Quyền riêng tư, IEEE Computer Society, trang 122-133, tháng 4 năm 1980.

[8] W. Feller, "Giới thiệu về lý thuyết xác suất và các ứng dụng của nó", 1957.