Bitcoin: Một hệ thống tiền mặt điện tử ngang hàng

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

Tóm tắt. Một phiên bản tiền mặt 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 một tổ chức tài chính.

Chữ ký số cung cấp một phần giải pháp, nhưng những lợi ích chính sẽ mất đi nếu vẫn cần một bên thứ ba đáng tin cậy để ngăn chặn việc chi tiêu gấp đôi. Chúng tôi đề xuất một giải pháp cho vấn đề chi tiêu gấp đôi bằng cách sử dụng mạng ngang hàng. Mạng đánh dấu thời gian các giao dịch bằng cách băm chúng vào một chuỗi bằng chứng công việc dựa trên băm liên tục, tạo thành một bản ghi không thể thay đổi mà không cần làm lại bằng chứng công việc. Chuỗi dài nhất không chỉ đóng vai trò là bằng chứng về trình tự các sự kiện đã 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 yêu cầu cấu trúc tối thiểu. Các tin nhắn được phát trên cơ sở nỗ lực tốt nhất và các nút có thể rời khỏi và tham gia lại mạng theo ý muốn, chấp nhận chuỗi bằng chứng công việc dài nhất làm bằng chứng về những gì đã xảy ra khi chúng vắng mặt.

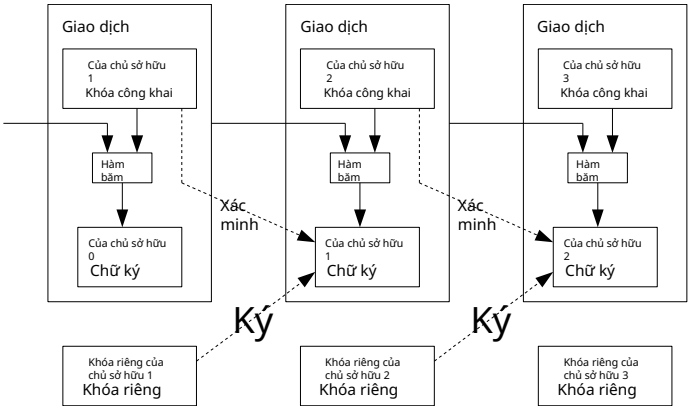
1. Giới thiệu

Thương mại trên Internet gần như hoàn toàn dựa vào các tổ chức tài chính đóng vai trò là bên thứ ba đáng tin cậy để xử lý các khoản thanh toán điện tử. Mặc dù hệ thống hoạt động đủ tốt cho hầu hết các giao dịch, nhưng nó vẫn phải chịu những điểm yếu vốn có của mô hình dựa trên lòng tin. Các giao dịch hoàn toàn không thể đảo ngược thực sự là không thể, vì các tổ chức tài chính không thể tránh khỏi việc hòa giải các tranh chấp. Chi phí hòa giải làm tăng chi phí giao dịch, hạn chế quy mô giao dịch thực tế tối thiểu và cắt bỏ khả năng thực hiện các giao dịch thông thường nhỏ, và có một chi phí lớn hơn trong việc 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 lan rộng. Người bán phải cảnh giác với khách hàng của họ, làm phiền họ để có thêm thông tin so với những gì họ cần. Một tỷ lệ gian lận nhất định được chấp nhận là không thể tránh khỏi. Những chi phí và sự không chắc chắn về thanh toán này có thể tránh được khi gặp trực tiếp bằng cách sử dụng tiền tệ vật chất, nhưng không có cơ chế nào để thực hiện thanh toán qua kênh liên lạc 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 lòng 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 mà việc đảo ngược bằng tính toán là không thực tế 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 ra bằng chứng tính toán về thứ tự thời gian của các giao dịch. Hệ thống an toàn miễn là các nút trung thực cùng nhau kiểm soát nhiều sức mạnh CPU hơn bất kỳ nhóm nút tấn công hợp tác nào.

2. Giao dịch

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

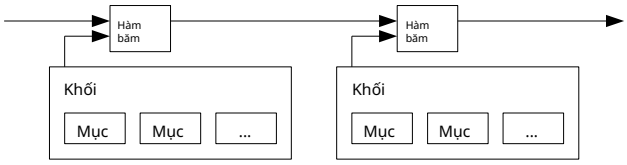


Vấn đề tất nhiên là người được trả tiền không thể xác minh rằng một trong những chủ sở hữu đã không chi tiêu gấp đôi đồng tiền. Một giải pháp phổ biến là giới thiệu một cơ quan trung ương đáng tin cậy, hoặc cơ quan đúc tiền, để kiểm tra mọi giao dịch xem có chi tiêu gấp đôi hay không. Sau mỗi giao dịch, đồng tiền phải được trả lại cho cơ quan đúc tiền để phát hành một đồng tiền mới và chỉ những đồng tiền được phát hành trực tiếp từ cơ quan 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 cơ quan đúc tiền, với mọi giao dịch đều phải thông qua họ, giống như một ngân hàng.

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

3. Máy chủ dấu thời gian

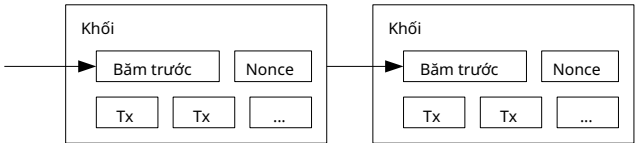
Giải pháp chúng tôi đề xuất bắt đầu với một máy chủ dấu thời gian. Một máy chủ dấu thời gian hoạt động bằng cách lấy một hàm băm của một khối các mục cần được đánh dấu thời gian và công bố rộng rãi hàm băm đó, chẳng hạn như trên một tờ báo hoặc bài đăng trên Usenet [2-5]. Dấu thời gian chứng minh rằng dữ liệu phải tồn tại vào thời điểm đó, rõ ràng là để 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 những dấu thời gian trước đó.



4. Bằng chứng công việc

Để triển khai một máy chủ dấu thời gian phân tán trên cơ sở ngang hàng, chúng ta sẽ cần sử dụng một 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 liên quan đến việc quét một giá trị mà khi được băm, chẳng hạn như với SHA-256, hàm băm bắt đầu bằng một số bit không. Công việc trung bình cần thiết là hàm mũ theo số lượng bit không cần thiết và có thể được xác minh bằng cách thực thi một hàm băm duy nhất.

Đối với mạng 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 không cần thiết. Khi nỗ lực của CPU đã được chi để làm cho nó đáp ứng bằng chứng công việc, khối không thể được thay đổi mà không cần làm lại công việc. Vì các khối sau được xâu chuỗi sau nó, công việc thay đổi khối sẽ bao gồm việc làm lại tất cả các khối sau nó.



Bằng chứng công việc cũng giải quyết vấn đề xác định đại diện trong quyết định đa số làm. Nếu đa số dựa trên một địa chỉ IP-một phiếu bầu, nó có thể bị lật đổ bởi bất kỳ ai có thể phân bổ nhiều IP. Bằng chứng công việc về cơ bản là một CPU-một phiếu bầu. Quyết định đa số được thể hiện bằng chuỗi dài nhất, có nỗ lực bằng chứng công việc lớn nhất được đầu tư vào nó. Nếu phần lớn sức mạnh CPU được kiểm soát bởi các nút trung thực, chuỗi trung thực sẽ phát triển nhanh nhất và vượt qua mọi chuỗi cạnh tranh. Để sửa đổi một khối trong quá khứ, một kẻ tấn công sẽ phải làm lại bằng chứng công việc của khối và tất cả các khối sau nó và sau đó bắt kịp và vượt qua công việc của các nút trung thực. Chúng tôi sẽ chỉ ra sau rằng xác suất một 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 việc tăng tốc độ phần cứng và sự quan tâm khác nhau trong việc chạy các nút theo thời gian, độ khó của bằng chứng công việc được xác định bởi một đường trung bình động nhắm mục tiêu một số khối trung bình mỗi giờ. Nếu chúng được tạo quá nhanh, độ khó sẽ tăng lên.

5. Mạng

Các bước để chạy mạng như sau:

1) Các giao dịch mới được phát đến 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 nó.
4) Khi một nút tìm thấy bằng chứng công việc, nó sẽ phát khối cho tất cả các nút.
5) Các nút chấp nhận khối chỉ khi tất cả các giao dịch trong đó hợp lệ và chưa được chi tiêu.
6) Các nút thể hiện sự chấp nhận của chúng đối với khối 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 làm việc trên mở rộng nó. Nếu hai nút phát các phiên bản khác nhau của khối tiếp theo đồng thời, một số nút có thể nhận được phiên bản này hoặc phiên bản kia trước. Trong trường hợp đó, chúng hoạt động trên phiên bản đầu tiên chúng nhận được, nhưng lưu nhánh kia trong 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 hoạt động trên nhánh kia sau đó sẽ chuyển sang nhánh dài hơn.

Các chương trình 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 có khả năng chịu đựng các tin nhắn bị bỏ. Nếu một nút không nhận được một khối, nó sẽ yêu cầu nó khi nó nhận được khối tiếp theo và nhận ra nó đã bỏ lỡ một khối.

6. Khuyến khích

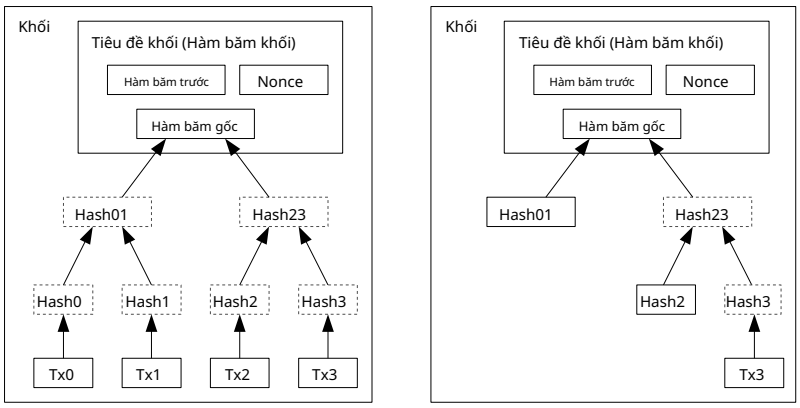
Theo quy ước, giao dịch đầu tiên trong một khối là một giao dịch đặc biệt bắt đầu một đồng tiền mới thuộc sở hữu của người tạo ra khối đó. Điều này tạo thêm động lực cho các nút hỗ trợ mạng và cung cấp một cách để phân phối tiền ban đầu vào lưu thông, vì không có cơ quan trung ương nào phát hành chúng. Việc bổ sung liên tục một lượng tiền mới không đổi tương tự như việc những người khai thác vàng chi tiêu tài nguyên để thêm vàng vào lưu thông. Trong trường hợp của chúng tôi, đó là thời gian CPU và điện năng được chi tiêu.

Động lực cũng có thể được tài trợ bằng phí giao dịch. Nếu giá trị đầu ra của một giao dịch là ít hơn giá trị đầu vào của nó, sự khác biệt là phí giao dịch được thêm vào giá trị khuyến khích của khối chứa giao dịch. Khi một số lượng tiền xu được xác định trước đã được đưa vào lưu thông, động lực có thể chuyển hoàn toàn sang phí giao dịch và hoàn toàn không có lạm phát.

Động lực có thể giúp khuyến khích các nút luôn trung thực. Nếu một kẻ tấn công tham lam có thể tập hợp nhiều sức mạnh CPU hơn tất cả các nút trung thực, anh ta sẽ phải lựa chọn giữa việc sử dụng nó để lừa đảo mọi người bằng cách đánh cắp lại các khoản thanh toán của mình hoặc sử dụng nó để tạo ra những đồng tiền mới. Anh ta nên thấy việc tuân thủ các quy tắc có lợi hơn, những quy tắc có lợi cho anh ta với nhiều đồng tiền mới hơn tất cả những người khác cộng lại, hơn là phá hoại hệ thống và tính hợp lệ của sự giàu có của chính mình.

7. Thu hồi không gian đĩa

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



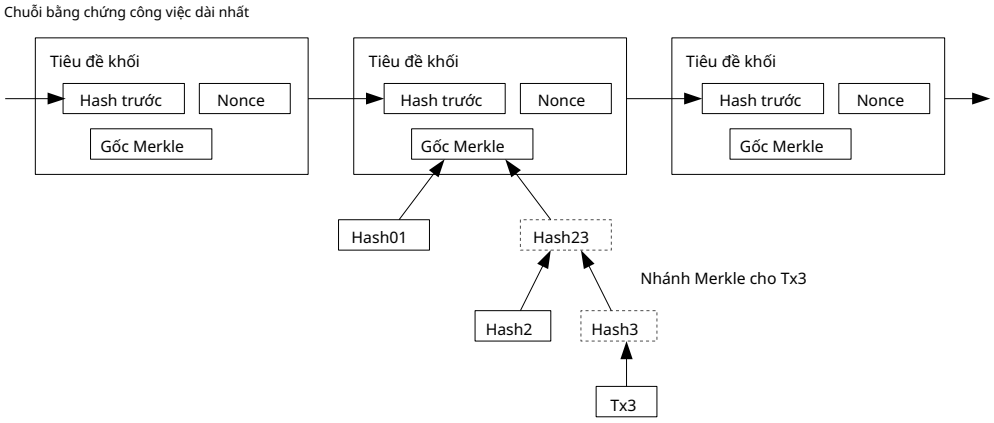
Các giao dịch được băm trong Cây Merkle

Sau khi cắt tỉa Tx0-2 khỏi khối

Một tiêu đề khối không có giao dịch sẽ có khoảng 80 byte. Nếu chúng ta cho rằng các khối được tạo ra cứ sau 10 phút, 80 byte * 6 * 24 * 365 = 4,2MB mỗi năm. Với các hệ thống máy tính thường bán với 2GB RAM kể từ năm 2008 và Luật Moore dự đoán mức tăng trưởng hiện tại là 1,2GB mỗi năm, dung lượng lưu trữ sẽ không phải là vấn đề ngay cả khi các tiêu đề khối phải được giữ trong bộ nhớ.

8. Xác minh thanh toán đơn giản

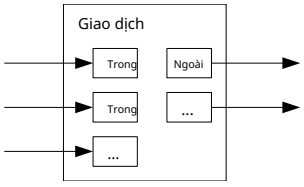
Có thể xác minh thanh toán mà không cần chạy một nút mạng đầy đủ. Người dùng chỉ cần giữ một bản sao của các tiêu đề khối của chuỗi bằng chứng công việc dài nhất, mà anh ta có thể nhận được bằng cách truy vấn các nút mạng cho đến khi anh ta tin rằng mình có chuỗi dài nhất và lấy nhánh Merkle liên kết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



Như vậy, việc xác minh là đáng tin cậy miễn là các nút trung thực kiểm soát mạng, nhưng dễ bị tấn công hơn nếu mạng bị áp đảo bởi một kẻ tấn công. Trong khi các nút mạng có thể tự xác minh các giao dịch, phương pháp đơn giản có thể bị đánh lừa bởi các giao dịch bịa đặt của kẻ tấn công miễn là kẻ tấn công có thế 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 họ phát hiện một khối không hợp lệ, nhắc phần mềm của người dùng tải xuống khối đầy đủ 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 của riêng họ để có bảo mật độc lập hơn và xác minh nhanh hơn.

9. Kết hợp và chia giá trị

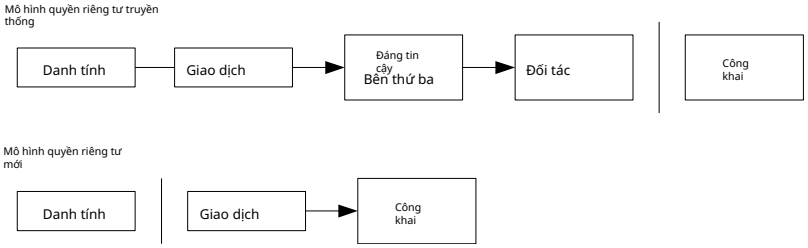
Mặc dù có thể xử lý tiền xu riêng lẻ, nhưng sẽ rất khó khăn khi thực hiện một giao dịch riêng cho mỗi xu trong một lần chuyển. Để cho phép giá trị được chia và kết hợp, các giao dịch chứa nhiều đầu vào và đầu ra. Thông thường sẽ có một đầu vào duy nhất từ một giao dịch trước đó lớn hơn hoặc nhiều đầu vào kết hợp các số tiền nhỏ hơn và tối đa hai đầu ra: một cho thanh toán và một trả lại tiền thừa, nếu có, cho người gửi.



Cần lưu ý rằng fan-out, nơi một giao dịch phụ thuộc vào một số giao dịch và những giao dịch đó phụ thuộc vào nhiều giao dịch khác, không phải là vấn đề ở đây. Không bao giờ cần phải trích xuất một bản sao độc lập hoàn chỉnh về lịch sử của một giao dịch.

10. Quyền riêng tư

Mô hình ngân hàng truyền thống đạt được một mức độ riêng tư bằng cách giới hạn quyền truy cập thông tin cho các bên liên quan và bên thứ ba đáng tin cậy. Sự cần thiết phải công bố công khai tất cả các giao dịch loại trừ phương pháp này, nhưng quyền riêng tư vẫn có thể được duy trì bằng cách phá vỡ luồng thông tin ở một nơi khác: bằng cách giữ cho các khóa công khai ẩn danh. Công chúng có thể thấy rằng ai đó đang gửi một số tiền cho người khác, nhưng không có thông tin liên kết giao dịch với bất kỳ ai. Điều này tương tự như mức độ thông tin được phát hành bởi các sàn giao dịch chứng khoán, nơi thời gian và quy mô của các giao dịch riêng lẻ, "băng", được công khai, nhưng không cho biết các bên là ai.



Như một tường lửa bổ sung, một cặp khóa mới nên được sử dụng cho mỗi giao dịch để giữ cho chúng khỏi bị liên kết với một chủ sở hữu chung. Một số liên kết vẫn không thể tránh khỏi với các giao dịch đa đầu vào, điều này nhất thiết tiết lộ rằng các đầu vào của chúng thuộc sở hữu của cùng một chủ sở hữu. Rủi ro là nếu chủ sở hữu của một khóa được tiết lộ, liên kết có thể tiết lộ các giao dịch khác thuộc về cùng một chủ sở hữu.

11. Tính toán

Chúng tôi xem xét kịch bản một kẻ tấn công cố gắng tạo ra một chuỗi thay thế nhanh hơn chuỗi trung thực. Ngay cả khi điều này được thực hiện, nó không mở hệ thống cho các thay đổi tùy ý, chẳng hạn như tạo ra giá trị từ không khí loãng hoặc lấy tiền chưa bao giờ thuộc về kẻ tấn công. Các nút sẽ không chấp nhận một giao dịch không hợp lệ làm 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 tiền mà anh ta đã chi gần đây.

Cuộc đua giữa chuỗi trung thực và chuỗi tấn công có thể được mô tả là một Binomial Đi bộ ngẫu nhiên. Sự kiện thành công là chuỗi trung thực được mở rộng thêm một khối, tăng mức dẫn đầu của nó thêm +1 và sự kiện thất bại là chuỗi của kẻ tấn công được mở rộng thêm một khối, giảm khoảng cách đi -1.

Xác suất một kẻ tấn công bắt kịp từ một thâm hụt nhất định tương tự như một Gambler's Vấn đề phá sản. Giả sử một người đánh bạc với tín dụng không giới hạn bắt đầu ở mức thâm hụt và chơi có khả năng vô số thử nghiệm để cố gắng đạt đến điểm hòa vốn. Chúng ta có thể tính toán xác suất anh ta từng đạt đến điểm hòa vốn, hoặc một kẻ tấn công từng 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
q_z = xác suất kẻ tấn công sẽ bắt kịp từ z khối phía sau

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

Với giả định của chúng tôi rằng p > q, xác suất giảm theo cấp số nhân khi số lượng khối mà kẻ tấn công phải bắt kịp tăng lên. Với tỷ lệ cược chống lại anh ta, nếu anh ta không thực hiện một cú lao may mắn về phía trước sớm, cơ hội của anh ta sẽ trở nên nhỏ bé khi anh ta tụt lại phía sau.

Bây giờ chúng ta xem xét người nhận một giao dịch mới cần phải đợi bao lâu trước khi đủ chắc chắn rằng người gửi không thể thay đổi giao dịch. Chúng tôi giả định người gửi là một kẻ tấn công muốn làm cho người nhận tin rằng anh ta đã trả tiền cho anh ta trong một thời gian, sau đó chuyển nó để trả lại cho chính mình sau một thời gian. Người nhận sẽ được cảnh báo khi điều đó xảy ra, nhưng người gửi hy vọng rằng 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 các khối trước thời hạn bằng cách làm việc liên tục trên đó cho đến khi anh ta đủ may mắn để đi đủ xa, sau đó thực hiện giao dịch vào thời điểm đó. Khi giao dịch được gửi, người gửi không trung thực bắt đầu bí mật làm việc trên một chuỗi song song chứa một phiên bản thay thế của giao dịch của mình.

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

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

Để có được xác suất kẻ tấn công vẫn có thể bắt kịp bây giờ, chúng ta nhân mật độ Poisson cho mỗi mức độ tiến bộ mà anh ta có thể đã đạt được với xác suất anh ta 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 tổng hợp đuôi vô hạn của phân phối...

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

Chuyển đổi sang mã 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 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 cho các giao dịch điện tử mà không cần dựa vào sự tin cậy. Chúng tôi bắt đầu với khuôn khổ thông thường của tiền xu được tạo từ chữ ký số, cung cấp khả năng kiểm soát mạnh mẽ quyền sở hữu, nhưng không hoàn chỉnh nếu không có cách nào để ngăn chặn việc 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, lịch sử này nhanh chóng trở nên bất khả thi về mặt tính toán để một kẻ tấn công thay đổi nếu các nút trung thực kiểm soát phần lớn sức mạnh CPU. Mạng rất mạnh mẽ trong sự đơn giản không có cấu trúc của nó. Các nút hoạt động đồng thời với ít sự phối hợp. Chúng không cần phải được xác định, vì các tin nhắn không được định tuyến đến bất kỳ vị trí cụ thể nào và chỉ cần được gửi trên cơ sở nỗ lực tốt nhất. Các nút có thể rời khỏi và tham gia lại mạng theo ý muốn, chấp nhận chuỗi bằng chứng công việc như bằng chứng về những gì đã xảy ra khi chúng vắng mặt. Họ bỏ phiếu bằng sức mạnh CPU của mình, bày tỏ sự chấp nhận của họ đối với các khối hợp lệ bằng cách làm việc để mở rộng chúng và từ chối các khối không hợp lệ bằng cách từ chối làm việc trên chúng. Bất kỳ quy tắc và ưu đãi cần thiết nào có thể được thực thi bằng cơ chế đồng thuận này.

Tài liệu tham khảo

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

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

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

[4] D. Bayer, S. Haber, W.S. Stornetta, "Cải thiện hiệu quả và độ tin cậy của việc đóng 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, W.S. Stornetta, "Tên an toàn cho chuỗi bit," Trong Kỷ yếu Hội nghị ACM lần thứ 4 về Bảo mật Máy tính và Truyền thông, trang 28-35, tháng 4 năm 1997.

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

[7] R.C. Merkle, "Giao thức cho hệ mật mã khóa công khai," Trong Proc. Hội nghị chuyên đề năm 1980 về An ninh 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.