CashWeb: Giao thức tích hợp tiền mã hóa cho Hệ thống nhắn tin liên kết chống thư rác và Xuất bản-Đăng ký

Shammah Chancellor
shammah.chancellor@proton.me
https://t.me/TheLotusNetwork

Ngày 21 tháng 2 năm 2026
Version 1.1

Tóm tắt nội dung

Chúng tôi trình bày CashWeb, một bộ giao thức toàn diện tích hợp các cơ chế kinh tế dựa trên tiền mã hóa với hạ tầng nhắn tin liên kết nhằm cho phép giao tiếp chống thư rác mà không cần kiểm duyệt tập trung. Giao thức sử dụng một cơ chế chống thư rác "đốt-để-nói" (burn-to-speak) mới lạ, trong đó người gửi đính kèm các khoản thanh toán tiền mã hóa nhỏ có thể xác minh bằng mật mã học mà không yêu cầu bên trung gian tin cậy. Chúng tôi cung cấp đặc tả hình thức cho ba thành phần cốt lõi: (1) giao thức Bằng chứng Thanh toán (POP) liên kết giá trị trên chuỗi với hành động ngoài chuỗi, (2) nhắn tin liên kết với quản lý danh tính bằng mật mã học, và (3) hệ thống xuất bản-đăng ký cho phát sóng theo chủ đề. Phân tích kinh tế cho thấy cơ chế đốt tạo ra sự răn đe tối ưu chống thư rác trong khi vẫn duy trì khả năng tiếp cận cho giao tiếp hợp lệ. Kiến trúc hệ thống tận dụng các tiêu chuẩn web đã được thiết lập (HTTP/2, WebSockets) và các nguyên tố mật mã học để cho phép tích hợp liền mạch với hạ tầng hiện có. Phân tích lý thuyết cho thấy giao thức đạt được khả năng chống thư rác với chi phí tăng theo dưới tuyến tính theo quy mô mạng, trong khi triển khai thực nghiệm chứng minh tính khả thi thực tế cho các ứng dụng nhắn tin thời gian thực.

1 Giới thiệu

1.1 Vấn đề tập trung hóa

Sự phát triển của các giao thức truyền thông internet bộc lộ một mâu thuẫn cơ bản giữa phi tập trung và khả năng sử dụng. Các hệ thống ban đầu như Usenet **??**, SMTP **??** và XMPP **??** được thiết kế như các mạng liên kết cho phép giao tiếp ngang hàng mà không có cơ quan trung ương. Tuy nhiên, cấu trúc chi phí bất đối xứng vốn có trong các giao thức này—nơi chi phí xử lý tin nhắn do người nhận chịu trong khi chi phí gửi gần như không đáng kể—đã tạo ra các động cơ kinh tế cho hành vi lạm dụng, cuối cùng đẩy người dùng về phía các nền tảng tập trung.

Đến năm 2020, mức độ tập trung của hạ tầng truyền thông đã đạt mức chưa từng có: Google, Apple và Microsoft cộng lại kiểm soát 85% thị phần ứng dụng email **?**, trong khi Facebook báo cáo hơn 2 tỷ người dùng và Gmail phục vụ 1,5 tỷ tài khoản hoạt động **?**. Sự tập trung này, dù

mang lại tiện lợi cho người dùng, đã đưa vào các rủi ro hệ thống bao gồm kiểm duyệt, giám sát và các điểm thất bại đơn lẻ làm tổn hại đến tầm nhìn ban đầu về giao tiếp internet phân tán.

1.2 Cơ chế kinh tế chống thư rác

Thách thức căn bản trong các hệ thống nhắn tin phi tập trung là ngăn chặn thư rác mà không có bộ lọc tập trung. Các phương pháp truyền thống dựa vào chi phí tính toán (Hashcash **?**) hoặc các hệ thống danh tiếng yêu cầu xác minh danh tính liên tục. Mặc dù các cơ chế này cung cấp một số bảo vệ, chúng có những hạn chế đáng kể: bằng chứng công việc tính toán mở rộng kém với khả năng tăng tốc phần cứng hiện đại, và các hệ thống danh tiếng tạo ra rào cản gia nhập cho người dùng mới trong khi vẫn dễ bị tấn công Sybil.

Sự xuất hiện của các mạng tiền mã hóa, đặc biệt là Bitcoin **?**, cho phép một phương pháp mới: cơ chế bằng chứng thanh toán kinh tế nơi tính xác thực của tin nhắn được xác minh thông qua bằng chứng mật mã học về việc phá hủy giá trị thay vì công việc tính toán. Phương pháp này, ban đầu được Finney **?** đề xuất là "Bằng chứng Công việc Có thể Tái sử dụng" (Reusable Proof of Work), hiện có thể được triển khai mà không cần bên trung gian tin cậy bằng cách sử dụng các mạng tiền mã hóa phi tập trung.

1.3 Đóng góp

Bài báo này trình bày CashWeb, một bộ giao thức toàn diện giải quyết vấn đề tập trung hóa thông qua ba đóng góp chính:

1. **Giao thức Bằng chứng Thanh toán Hình thức**: Chúng tôi đặc tả một giao thức mật mã học hoàn chỉnh để liên kết các giao dịch tiền mã hóa trên chuỗi với các hành động nhắn tin ngoài chuỗi, cho phép các cơ chế chống thư rác có thể xác minh mà không cần bên tin cậy.

2. **Thiết kế Hạ tầng Liên kết**: Chúng tôi trình bày một kiến trúc có khả năng mở rộng kết hợp máy chủ khóa để quản lý danh tính và máy chủ chuyển tiếp để định tuyến tin nhắn, được thiết kế để hỗ trợ khối lượng giao dịch cần thiết cho việc áp dụng rộng rãi trong khi vẫn duy trì tính phi tập trung.

3. **Phân tích Bảo mật Kinh tế**: Chúng tôi cung cấp phân tích lý thuyết chứng minh rằng các cơ chế tỷ lệ đốt phù hợp đạt được sự đánh đổi tối ưu giữa ngăn chặn thư rác và khả năng tiếp cận của người dùng hợp lệ, với các giới hạn hình thức về chi phí tấn công và xác suất thành công.

Giao thức được thiết kế để triển khai trên mạng tiền mã hóa Lotus **?**, một chuỗi Bằng chứng Công việc (Proof-of-Work) với hỗ trợ gốc cho các đầu ra `OP_RETURN` mang giá trị và chính sách tiền tệ thích ứng được đặc tả trong **?**. Lotus hiện đang hoạt động; CashWeb cung cấp giao thức lớp ứng dụng hoàn thành ngăn xếp kinh tế. Giao thức tận dụng các tiêu chuẩn web đã được thiết lập và duy trì tương thích với hạ tầng internet hiện có. Kinh nghiệm triển khai với mạng xã hội Stamp cung cấp sự xác nhận ban đầu cho phương pháp cốt lõi.

Bài báo này là bài thứ ba trong một chuỗi bài. **?** thiết lập nền tảng lý thuyết: trong bất kỳ hệ thống đồng thuận không cần phép nào, chi tiêu bảo mật cân bằng được neo vào giá trị rủi

ro kỳ vọng, và Bằng chứng Công việc (PoW) duy nhất làm cho chi tiêu này có thể đọc được về mặt giao thức thông qua tín hiệu công việc được tiết lộ đối kháng. **?** phát triển các hàm ý chính sách tiền tệ, đặc tả một cơ chế hai vòng không cần oracle sử dụng tín hiệu công việc PoW cho phát thải đuôi thích ứng và đốt-để-nói như một bể hấp thụ cung nội sinh. Bài báo hiện tại đặc tả đầy đủ cơ chế đốt-để-nói như một giao thức nhắn tin liên kết. Do đó, đốt-để-nói phục vụ vai trò kép trên toàn ngăn xếp: ngăn chặn thư rác ở lớp ứng dụng và quản lý cung tiền tệ nội sinh ở lớp giao thức.

1.4 Tổ chức bài báo

Phần **??** xem xét các công trình liên quan trong cơ chế chống thư rác và nhắn tin liên kết. Phần **??** thiết lập mô hình hệ thống và các giả định về mối đe dọa. Phần **??** cung cấp các đặc tả hình thức của các giao thức cốt lõi. Phần **??** phân tích các thuộc tính kinh tế và đảm bảo chống thư rác. Phần **??** xem xét các thuộc tính bảo mật và khả năng chống tấn công. Phần **??** thảo luận các cân nhắc triển khai thực tế. Phần **??** trình bày kết quả đánh giá lý thuyết và thực nghiệm.

2 Nền tảng và Công trình liên quan

2.1 Cơ chế kinh tế chống thư rác

Việc sử dụng các khuyến khích kinh tế để ngăn chặn thư rác có lịch sử phong phú trong nghiên cứu hệ thống phân tán. Dwork và Naor **?** lần đầu tiên đề xuất yêu cầu bằng chứng công việc tính toán cho việc gửi email, được triển khai trong Hashcash **?** thông qua các bài toán tiền ảnh băm SHA-256. Mặc dù về lý thuyết là hợp lý, các phương pháp tính toán có một số hạn chế thực tế: (1) chi phí tính toán thay đổi đáng kể trên các phần cứng khác nhau, tạo ra sự bất công, (2) các ASIC hiện đại và khả năng tăng tốc GPU có thể giải các bài toán nhanh hơn phần cứng người dùng thông thường hàng bậc đại lượng, và (3) mức độ khó tối ưu đòi hỏi điều chỉnh liên tục khi khả năng tính toán phát triển.

Laurie và Clayton **?** đề xuất các hệ thống bằng chứng công việc sử dụng các hàm tiêu tốn bộ nhớ để giảm lợi thế phần cứng, nhưng các phương pháp này vẫn đòi hỏi tiêu hao năng lượng đáng kể và tạo ra rào cản cho các thiết bị bị hạn chế tài nguyên. Các phương pháp thay thế dựa trên danh tiếng **?** yêu cầu các hệ thống danh tính liên tục mâu thuẫn với mục tiêu bảo mật và tạo ra rào cản gia nhập cao cho người dùng mới hợp lệ.

2.2 Kiểm soát truy cập dựa trên tiền mã hóa

Sự xuất hiện của các mạng tiền mã hóa có thể lập trình cho phép các cơ chế kinh tế tinh vi hơn. Miller và cộng sự **?** đề xuất sử dụng Bitcoin cho các khoản thanh toán vi mô ẩn danh, nhưng phương pháp của họ yêu cầu các giao thức tương tác không thể mở rộng cho các ứng dụng nhắn tin. Các nghiên cứu gần đây về kênh thanh toán **?** và kênh trạng thái **?** cung cấp các cơ chế thanh toán vi mô độ trễ thấp, nhưng yêu cầu các kênh được tài trợ trước tạo ra rào cản khả năng sử dụng.

Phương pháp của chúng tôi khác biệt bằng cách sử dụng phá hủy giá trị không thể khôi phục ("đốt") thay vì chuyển giá trị, loại bỏ nhu cầu hạ tầng thanh toán của người nhận trong khi vẫn duy trì các động cơ kinh tế mạnh mẽ chống lại lạm dụng.

2.3 Hệ thống nhắn tin liên kết

Các kiến trúc nhắn tin liên kết cân bằng lợi ích của phi tập trung với yêu cầu khả năng mở rộng thực tế. XMPP **?** chứng minh tính khả thi của nhắn tin thời gian thực liên kết, nhưng thiếu các cơ chế ngăn chặn thư rác kinh tế. Matrix **?** cung cấp nhắn tin liên kết hiện đại với mã hóa đầu cuối đến đầu cuối, nhưng dựa vào các nhà cung cấp danh tính tập trung và thiếu các cơ chế chống thư rác ngoài giới hạn tốc độ.

Các hệ thống nhắn tin dựa trên blockchain gần đây bao gồm Status **?** và Session **?**, cung cấp quản lý danh tính phi tập trung nhưng không giải quyết các vấn đề khuyến khích kinh tế thúc đẩy tập trung hóa. Phương pháp của chúng tôi tích hợp các cơ chế kinh tế trực tiếp vào thiết kế giao thức để giải quyết những sự không phù hợp khuyến khích căn bản này.

3 Mô hình hệ thống và Kiến trúc

3.1 Các thành viên mạng

Mạng CashWeb bao gồm bốn loại thành viên:

Định nghĩa 1 (Các thành viên mạng)**.** *Đặt $\mathcal{U} = \{u_1, u_2, \ldots, u_n\}$ là tập hợp người dùng, $\mathcal{R} = \{r_1, r_2, \ldots, r_m\}$ là tập hợp máy chủ chuyển tiếp, $\mathcal{K} = \{k_1, k_2, \ldots, k_\ell\}$ là tập hợp máy chủ khóa, và $\mathcal{T} = \{t_1, t_2, \ldots, t_p\}$ là tập hợp các chủ đề xuất bản-đăng ký.*

Người dùng ($u_i \in \mathcal{U}$): Các thành viên cuối gửi và nhận tin nhắn. Mỗi người dùng kiểm soát một ví tiền mã hóa và có thể tạo ra các bằng chứng thanh toán mật mã học. Người dùng tương tác với mạng thông qua phần mềm client quản lý tài liệu khóa và các giao dịch thanh toán.

Máy chủ chuyển tiếp ($r_i \in \mathcal{R}$): Các máy chủ liên kết lưu trữ và chuyển tiếp các tin nhắn được mã hóa thay mặt cho người dùng. Máy chủ chuyển tiếp xác minh bằng chứng thanh toán trước khi chấp nhận tin nhắn, cung cấp lớp phòng thủ thư rác đầu tiên. Họ không có quyền truy cập vào nội dung tin nhắn do mã hóa đầu cuối đến đầu cuối.

Máy chủ khóa ($k_i \in \mathcal{K}$): Các máy chủ phân tán duy trì sổ đăng ký toàn cầu về khóa công khai của người dùng và siêu dữ liệu liên quan. Máy chủ khóa cho phép người dùng khám phá các máy chủ chuyển tiếp và thiết lập các kênh liên lạc an toàn mà không cần liên lạc trước.

Chủ đề ($t_i \in \mathcal{T}$): Các kênh được đặt tên trong hệ thống xuất bản-đăng ký cho phép truyền thông phát sóng. Các chủ đề là phi tập trung—bất kỳ người dùng nào cũng có thể tạo chủ đề và bất kỳ máy chủ chuyển tiếp nào cũng có thể truyền bá tin nhắn chủ đề dựa trên danh sách người đăng ký.

3.2 Mô hình mối đe dọa

Chúng tôi xem xét môi trường đối nghịch Byzantine nơi các thành viên có thể tùy ý lệch khỏi các đặc tả giao thức. Mô hình mối đe dọa của chúng tôi bao gồm:

Kẻ tấn công thư rác: Các đối thủ cố gắng gửi khối lượng lớn tin nhắn không mong muốn để phá vỡ giao tiếp hoặc lãng phí tài nguyên mạng. Chúng tôi giả định kẻ tấn công có tài nguyên tính toán và tài chính đáng kể nhưng có hạn.

Kẻ tấn công Sybil: Các đối thủ tạo ra nhiều danh tính giả để khuếch đại năng lực gửi tin nhắn hoặc thao túng các hệ thống danh tiếng.

Kẻ tấn công hạ tầng mạng: Các đối thủ kiểm soát máy chủ chuyển tiếp hoặc máy chủ khóa và có thể cố gắng kiểm duyệt, phân tích lưu lượng, hoặc tấn công từ chối dịch vụ.

Kẻ tấn công kinh tế: Các đối thủ cố gắng thao túng các cơ chế kinh tế, bao gồm các cuộc tấn công tái chế phí nơi kẻ tấn công thu hồi quỹ đã đốt thông qua kiểm soát khai thác hoặc trình xác thực.

Chúng tôi giả định mạng tiền mã hóa cơ bản (ví dụ: Bitcoin, Lotus) cung cấp các đảm bảo bảo mật tiêu chuẩn bao gồm tính bất biến của giao dịch và khả năng chống tấn công chi tiêu kép. Chúng tôi không xem xét các cuộc tấn công vào chính mạng tiền mã hóa.

3.3 Các nguyên tắc thiết kế

Thiết kế giao thức tuân thủ một số nguyên tắc chính:

Bảo mật kinh tế: Bảo vệ chống thư rác nên xuất phát từ các động cơ kinh tế thay vì rào cản tính toán hoặc kiểm duyệt tập trung, đảm bảo rằng các cuộc tấn công trở nên cực kỳ tốn kém trong khi việc sử dụng hợp lệ vẫn có thể chi trả được.

Bảo mật theo thiết kế: Nội dung tin nhắn và mô hình truyền thông nên được giữ riêng tư đối với các bên thứ ba, bao gồm cả các nhà cung cấp hạ tầng mạng.

Khả năng mở rộng liên kết: Hệ thống nên hỗ trợ việc áp dụng ở quy mô toàn cầu thông qua kiến trúc liên kết trong khi vẫn duy trì các thuộc tính phi tập trung.

Tương thích ngược: Giao thức nên tích hợp với hạ tầng internet hiện có và các khung phát triển để giảm thiểu rào cản áp dụng.

4 Đặc tả giao thức cốt lõi

4.1 Giao thức Bằng chứng Thanh toán (POP)

Giao thức Bằng chứng Thanh toán cho phép xác minh mật mã học rằng một lượng tiền mã hóa cụ thể đã bị đốt (phá hủy vĩnh viễn) liên quan đến một hành động ngoài chuỗi cụ thể. Không giống như các hệ thống thanh toán truyền thống chuyển giá trị giữa các bên, giao thức POP tạo ra bằng chứng có thể xác minh về việc phá hủy giá trị không thể khôi phục hoặc chi tiêu kép.

Định nghĩa 2 (Giao thức Bằng chứng Thanh toán)**.** *Giao thức POP là một bộ ba* (Setup, Commit, Verify) *trong đó:*

- $\text{Setup}(1^\lambda) \to pp$*: Tạo các tham số công khai cho tham số bảo mật* λ*.*
- $\text{Commit}(sk, m, v) \to (\pi, \tau)$*: Với khóa bí mật* sk*, tin nhắn* m *và giá trị* v*, xuất ra bằng chứng* π *và giao dịch* τ*.*

- VERIFY$(\pi, \tau, m, v) \to \{0, 1\}$*: Xác minh rằng giao dịch* τ *đốt giá trị* v *và được liên kết bằng mật mã học với tin nhắn* m*.*

4.1.1 Xây dựng đầu ra không thể tiêu

Trước khi đặc tả thuật toán, chúng tôi định nghĩa nguyên tố cốt lõi:

Định nghĩa 3 (Địa chỉ không thể tiêu / Đầu ra OP_RETURN)**.** *Cho một giá trị cam kết 32 byte* h_m*,* UNSPENDABLEADDRESS(h_m) *biểu thị tập lệnh đầu ra* `OP_RETURN` $\langle h_m \rangle$*. Một đầu ra giao dịch có giá trị* v *được gửi đến tập lệnh này bị phá hủy có thể xác minh: (i) các đầu ra* `OP_RETURN` *không hợp lệ về mặt đồng thuận như các đầu vào chi tiêu, do đó không bên nào có thể xây dựng một giao dịch chi tiêu hợp lệ; (ii) các nút tuân thủ đánh dấu các đầu ra như vậy là miễn UTXO, loại bỏ vĩnh viễn giá trị khỏi lưu thông. Một tải trọng băm SHA-256 32 byte phù hợp trong giới hạn dữ liệu* `OP_RETURN` *80 byte, để lại chỗ cho trường định danh giao thức và phiên bản 4 byte.*

Mạng Lotus, mục tiêu triển khai dự định của CashWeb, hỗ trợ các đầu ra `OP_RETURN` có giá trị khác không theo quy tắc đồng thuận, làm cho cách trên là cách xây dựng chính. Đối với các chuỗi cấm các đầu ra `OP_RETURN` có giá trị khác không (chính sách Bitcoin tiêu chuẩn), một cách xây dựng thay thế gửi v đến địa chỉ P2PKH(HASH160(`0x0000...00`$\|h_m$)): một địa chỉ P2PKH hợp lệ về mặt cú pháp mà không có khóa riêng tư nào tồn tại (vì tìm tiền ảnh của HASH160 là không khả thi về mặt tính toán). Điều này cung cấp tính không thể tiêu xác suất thay vì tính không thể tiêu được thực thi bằng đồng thuận của cách xây dựng chính.

4.1.2 Xây dựng

Cách xây dựng giao thức POP của chúng tôi tận dụng các đầu ra OP_RETURN trong các giao dịch kiểu Bitcoin để nhúng dữ liệu cam kết trong khi đảm bảo phá hủy quỹ:

Algorithm 1 Xây dựng Bằng chứng Thanh toán

Require: Tin nhắn m, lượng đốt v, khóa bí mật người dùng sk
Ensure: Bằng chứng π và giao dịch τ
1: $pk \leftarrow$ DERIVEPUBLIC(sk)
2: $h_m \leftarrow$ HASH$(m \| pk \|$ TIMESTAMP$())$
3: $addr_{burn} \leftarrow$ UNSPENDABLEADDRESS(h_m)
4: $\tau \leftarrow$ CREATETRANSACTION$(sk, v, addr_{burn}, h_m)$
5: $\sigma \leftarrow$ SIGN$(sk, \tau \| m)$
6: $\pi \leftarrow (\tau, \sigma, m, v, pk)$
7: **return** π, τ

Cách xây dựng đảm bảo một số thuộc tính quan trọng:

Không thể khôi phục: Quỹ gửi đến $addr_{burn}$ không thể tiêu được chứng minh bởi vì địa chỉ được dẫn xuất từ một hàm băm không có tiền ảnh đã biết.

Tính duy nhất: Mỗi cặp tin nhắn-thanh toán tạo ra một cam kết duy nhất không thể tái sử dụng cho các tin nhắn khác.

Khả năng xác minh: Bất kỳ bên nào cũng có thể xác minh bằng chứng bằng cách kiểm tra giao dịch trên blockchain và xác nhận các chữ ký mật mã học.

4.2 Quản lý danh tính và Đăng ký khóa

Người dùng trong CashWeb duy trì các danh tính bí danh dựa trên mật mã học khóa công khai. Mỗi danh tính bao gồm một cặp khóa (sk, pk) trong đó khóa công khai phục vụ như là định danh toàn cầu của người dùng.

4.2.1 Đăng ký danh tính

Các danh tính mới được đăng ký với mạng máy chủ khóa thông qua giao thức sau:

Algorithm 2 Đăng ký danh tính

Require: Cặp khóa người dùng (sk, pk), địa chỉ máy chủ chuyển tiếp $addr_{relay}$, phí đăng ký v_{reg}
Ensure: Bản ghi danh tính trong mạng máy chủ khóa

$metadata \leftarrow \{\text{“}relay\text{”} : addr_{relay}, \text{“}timestamp\text{”} : \textsc{Now}()\}$
$(\pi_{reg}, \tau_{reg}) \leftarrow \text{POP.}\textsc{Commit}(sk, metadata, v_{reg})$
$record \leftarrow (pk, metadata, \pi_{reg})$
for each keyserver $k_i \in \mathcal{K}$ **do**
    $\textsc{Send}(record, k_i)$
end for

4.2.2 Xoay khóa và Khôi phục

Giao thức hỗ trợ xoay khóa để cho phép khôi phục từ việc khóa bị xâm phạm hoặc mất. Người dùng có thể đăng ký trước các khóa khôi phục hoặc sử dụng dẫn xuất khóa xác định phân cấp để xoay liền mạch:

Algorithm 3 Xoay khóa

Require: Cặp khóa hiện tại (sk_{old}, pk_{old}), cặp khóa mới (sk_{new}, pk_{new}), phí xoay v_{rot}
Ensure: Bản ghi danh tính được cập nhật

$rotation\_msg \leftarrow (pk_{old}, pk_{new}, \textsc{Now}())$
$\sigma_{old} \leftarrow \textsc{Sign}(sk_{old}, rotation\_msg)$
$\sigma_{new} \leftarrow \textsc{Sign}(sk_{new}, rotation\_msg)$
$(\pi_{rot}, \tau_{rot}) \leftarrow \text{POP.}\textsc{Commit}(sk_{new}, rotation\_msg, v_{rot})$
$update \leftarrow (pk_{old}, pk_{new}, \sigma_{old}, \sigma_{new}, \pi_{rot})$
for each keyserver $k_i \in \mathcal{K}$ **do**
    $\textsc{Send}(update, k_i)$
end for

4.3 Nhắn tin liên kết với Đốt-để-Gửi

Giao thức nhắn tin cốt lõi tích hợp giao tiếp tin nhắn mật mã học với bảo vệ chống thư rác kinh tế. Các tin nhắn được mã hóa đầu cuối đến đầu cuối và bao gồm bằng chứng thanh toán để chứng minh cam kết của người gửi.

4.3.1 Xác minh và lưu trữ tin nhắn

Máy chủ chuyển tiếp xác minh các tin nhắn đến trước khi lưu trữ:

Algorithm 4 Giao thức gửi tin nhắn

Require: Khóa công khai người nhận pk_{recv}, nội dung tin nhắn *content*, lượng đốt v_{msg}
Ensure: Tin nhắn được giao đến máy chủ chuyển tiếp của người nhận

$(pk_{sender}, sk_{sender}) \leftarrow$ GetUserKeys()
$relay_{recv} \leftarrow$ KeyserverLookup(pk_{recv})
$k_{shared} \leftarrow \text{ECDH}(sk_{sender}, pk_{recv})$
$msg_{encrypted} \leftarrow$ Encrypt$(k_{shared}, content)$
$message \leftarrow (pk_{sender}, pk_{recv}, msg_{encrypted},$ Timestamp$())$
$(\pi_{msg}, \tau_{msg}) \leftarrow$ POP.Commit$(sk_{sender}, message, v_{msg})$
$delivery\_req \leftarrow (message, \pi_{msg})$
HTTPPost$(delivery_req, relay_{recv})$

Algorithm 5 Xác minh tin nhắn bởi máy chủ chuyển tiếp

Require: Yêu cầu giao tin nhắn $delivery\_req = (message, \pi_{msg})$
Ensure: Tin nhắn được chấp nhận hoặc từ chối

$(message, \pi_{msg}) \leftarrow delivery\_req$
$(pk_{sender}, pk_{recv}, msg_{encrypted}, timestamp) \leftarrow message$
if POP.Verify$(\pi_{msg}, message) \neq 1$ **then**
    return "Bị từ chối: Bằng chứng thanh toán không hợp lệ"
end if
if BurnAmount$(\pi_{msg}) < v_{min}$ **then**
    return "Bị từ chối: Lượng đốt không đủ"
end if
StoreMessage$(message, \pi_{msg})$
return "Được chấp nhận"

4.4 Xuất bản-Đăng ký với Đốt-để-Phát sóng

Hệ thống xuất bản-đăng ký mở rộng giao thức nhắn tin để hỗ trợ phát sóng theo chủ đề. Người dùng có thể đăng ký các chủ đề và nhận tất cả các tin nhắn được đăng lên các chủ đề đó, với mức độ ưu tiên của tin nhắn được xác định bởi lượng đốt.

Định nghĩa 4 (Đăng ký chủ đề)**.** *Một đăng ký chủ đề là một bộ ba (u_i, t_j, r_k) chỉ ra rằng người dùng u_i đăng ký chủ đề t_j thông qua máy chủ chuyển tiếp r_k.*

Algorithm 6 Phát sóng tin nhắn chủ đề

Require: Định danh chủ đề $topic\_id$, nội dung tin nhắn $content$, lượng đốt $v_{broadcast}$
Ensure: Tin nhắn được phân phối đến tất cả người đăng ký chủ đề
$(pk_{sender}, sk_{sender}) \leftarrow$ GetUserKeys()
$topic\_msg \leftarrow (pk_{sender}, topic\_id, content,$ Timestamp())
$(\pi_{broadcast}, \tau_{broadcast}) \leftarrow$ POP.Commit$(sk_{sender}, topic_msg, v_{broadcast})$
$broadcast\_req \leftarrow (topic\_msg, \pi_{broadcast})$
for each relay server $r_i \in \mathcal{R}$ **do**
  SendToRelayIfSubscribers$(broadcast_req, topic_id, r_i)$
end for

Cơ chế phát sóng bao gồm sắp xếp ưu tiên tin nhắn và giới hạn tốc độ dựa trên lượng đốt:

Algorithm 7 Ưu tiên hóa tin nhắn chủ đề

Require: Tập hợp tin nhắn chủ đề $M = \{m_1, m_2, \ldots, m_k\}$ với lượng đốt $\{v_1, v_2, \ldots, v_k\}$
Ensure: Lịch giao tin nhắn được ưu tiên
$priority\_queue \leftarrow$ EmptyQueue()
for each message $m_i \in M$ **do**
  $priority_i \leftarrow f(v_i)$ trong đó f là hàm tăng đơn điệu
  Insert$(priority_queue, m_i, priority_i)$
end for
while NotEmpty$(priority_queue)$ **and** BandwidthAvailable() **do**
  $m_{next} \leftarrow$ PopMax$(priority_queue)$
  DeliverMessage(m_{next})
end while

5 Phân tích kinh tế và Thuộc tính chống thư rác

5.1 Kinh tế học tỷ lệ đốt và Phân tích cân bằng

Hiệu quả của cơ chế đốt-để-nói phụ thuộc vào việc thiết lập các tỷ lệ đốt làm cho các cuộc tấn công thư rác không khả thi về mặt kinh tế trong khi vẫn bảo tồn khả năng tiếp cận cho người dùng hợp lệ. Chúng tôi mô hình hóa điều này như một vấn đề cân bằng lý thuyết trò chơi, theo khung ngăn chặn tối ưu của Becker (**?**), được mở rộng sang môi trường phi tập trung nơi việc thực thi được thực hiện thông qua bằng chứng mật mã học về phá hủy giá trị.

Định nghĩa 5 (Chi phí tấn công thư rác)**.** *Đối với kẻ tấn công cố gắng gửi N tin nhắn thư rác với lượng đốt B mỗi tin nhắn, tổng chi phí tấn công là:*

$$C_{attack}(N, B) = N \cdot B + C_{operational}(N)$$

trong đó $C_{operational}(N)$ đại diện cho chi phí tính toán và hạ tầng.

Định nghĩa 6 (Lợi ích người dùng hợp lệ)**.** *Lợi ích của người dùng hợp lệ khi gửi một tin nhắn với lượng đốt B là:*

$$U_{legit}(B) = V_{communication} - B - C_{friction}(B)$$

trong đó $V_{communication}$ là giá trị thu được từ giao tiếp tin nhắn thành công và $C_{friction}(B)$ đại diện cho chi phí khả năng sử dụng.

Tỷ lệ đốt tối ưu B^* tối đa hóa việc áp dụng của người dùng hợp lệ trong khi giảm thiểu khả năng tồn tại của thư rác. Để thu được dạng có thể xử lý được, chúng tôi đặc tả các dạng hàm:

Định nghĩa 7 (Hàm phúc lợi xã hội)**.** *Định nghĩa:*

$$W(B) = U_0 - \alpha B - \frac{D\sigma}{B},$$

trong đó $U_0 > 0$ là giá trị trên mỗi tin nhắn đối với người dùng hợp lệ đại diện, $\alpha > 0$ là chi phí biên của họ về việc đốt, $D > 0$ là thiệt hại xã hội trên mỗi tin nhắn thư rác, và $\sigma > 0$ là khối lượng thư rác ở chi phí đốt đơn vị. Số hạng αB nắm bắt sự giảm thặng dư người dùng hợp lệ từ việc đốt cao hơn; số hạng $D\sigma/B$ nắm bắt tổng thiệt hại thư rác, giảm theo $1/B$ theo kinh tế học kẻ gửi thư rác hợp lý (kẻ gửi thư rác cân bằng doanh thu thư rác biên với chi phí đốt biên).

Theo đặc tả này, tỷ lệ đốt tối ưu là:

$$B^* = \sqrt{\frac{D\sigma}{\alpha}},$$

cân bằng ngăn chặn với khả năng tiếp cận ở dạng đóng. Thiệt hại xã hội thư rác D cao hơn hoặc xu hướng thư rác σ cao hơn đòi hỏi B^* cao hơn; chi phí biên người dùng hợp lệ α thấp hơn cũng làm tăng B^*.

Định lý 8 (Tỷ lệ đốt tối ưu)**.** *Tỷ lệ đốt tối ưu B^* thỏa mãn:*

$$\frac{\partial}{\partial B}\left[\sum_{i=1}^{n} U_{legit}^{i}(B) - \alpha \cdot E[N_{spam}(B)]\right] = 0$$

trong đó α đại diện cho chi phí xã hội của thư rác và $E[N_{spam}(B)]$ là số lượng kỳ vọng của tin nhắn thư rác ở tỷ lệ đốt B.

Chứng minh. Tồn tại. Khi $B \to 0$, thư rác không bị ràng buộc và $W(B) \to -\infty$. Khi $B \to \infty$, người dùng hợp lệ bị loại bỏ về giá và $W(B) \to -\infty$. Vì W liên tục, một cực đại nội tại tồn tại theo định lý giá trị cực đoan trên bất kỳ khoảng compact con nào chứa cực đại.

Điều kiện bậc nhất. Tại điểm tối ưu nội tại B^*, điều kiện được nêu thỏa mãn bằng cách vi phân.

Tính duy nhất đạt được theo giả định bổ sung rằng $W(B)$ là nghiêm ngặt lõm, điều này thỏa mãn khi lợi ích hợp lệ là lõm theo B và khối lượng thư rác là lồi theo $1/B$—các giả định tiêu chuẩn trong tài liệu ngăn chặn tối ưu (**?**). □

5.2 Lượng hóa khả năng chống Sybil

Cơ chế đốt cung cấp khả năng chống Sybil vốn có vì mỗi danh tính yêu cầu cam kết kinh tế thay vì chỉ công việc tính toán:

Mệnh đề 9 (Giới hạn tấn công Sybil)**.** *Đối với kẻ tấn công có ngân sách $\mathcal{B}$, số lượng danh tính Sybil tối đa bị giới hạn bởi:*

$$N_{sybil} \leq \frac{\mathcal{B}}{v_{reg} + k \cdot v_{msg}}$$

trong đó v_{reg} là phí đăng ký danh tính và k là số lượng tin nhắn kỳ vọng trên mỗi danh tính.

Giới hạn này chứng minh rằng các cuộc tấn công Sybil tăng tuyến tính với ngân sách kẻ tấn công thay vì tài nguyên tính toán, cung cấp các đảm bảo kháng cự có thể dự đoán.

5.3 Ngăn chặn tấn công tái chế phí

Một cân nhắc bảo mật quan trọng là ngăn chặn kẻ tấn công thu hồi quỹ đã đốt thông qua kiểm soát khai thác hoặc hạ tầng xác nhận. Chúng tôi giải quyết vấn đề này thông qua đốt phí một phần:

Định nghĩa 10 (Cơ chế đốt phí một phần)**.** *Đối với mỗi giao dịch có phí F, một phần $\beta \in (0, 1]$ bị đốt trong khi phần còn lại $(1 - \beta)F$ được trả cho các thợ mỏ:*

$$B_{total} = B_{explicit} + \beta \cdot F$$

trong đó $B_{explicit}$ là lượng đốt rõ ràng và F là phí giao dịch.

Tham số β được chia sẻ với khung chính sách tiền tệ thích ứng trong **?**, nơi cùng tỷ lệ đốt phí đồng thời hoạt động như một cơ chế giảm phát cung nội sinh. Các vai trò chống thư rác và tiền tệ do đó được hợp nhất về mặt cấu trúc: một hằng số giao thức đơn β cung cấp cả sàn chi phí tấn công lớp ứng dụng và quản lý cung lớp tiền tệ.

Định lý 11 (Kháng cự tái chế phí)**.** *Theo cơ chế đốt phí một phần, kẻ tấn công kiểm soát phần μ của hàm băm mạng có thể thu hồi nhiều nhất $(1 - \beta)\mu$ chi phí tấn công của họ, đảm bảo chi phí tấn công ròng vẫn dương đối với $\mu < \beta$.*

Phân tích cân bằng. Định lý **??** đưa ra điều kiện đủ ($\mu < \beta$) để chi phí tấn công ròng vẫn dương. Liệu μ cân bằng trong trò chơi khai thác có thỏa mãn điều kiện này hay không phụ thuộc vào lợi nhuận tương đối của khai thác so với gửi thư rác. Một thợ mỏ-kẻ gửi thư rác so sánh lợi nhuận khai thác trung thực (tỷ lệ thuận với μ) với lợi nhuận thư rác (tỷ lệ thuận với khối lượng tin nhắn, bị giới hạn bởi hạ tầng kẻ tấn công). Vì khai thác trung thực tăng theo μ và thư rác thì không, các thợ mỏ lớn có ít động lực gửi thư rác hơn so với các thợ mỏ nhỏ. Điều này gợi ý rằng điều kiện $\mu < \beta$ tự thực thi trong các chế độ điển hình đối với β hợp lý, mặc dù một bằng chứng hình thức đòi hỏi một đặc tả rõ ràng về các hàm chi phí khai thác và gửi thư rác—được hoãn lại cho công việc trong tương lai.

5.4 Khả năng phản ứng giá không cần oracle

Giao thức đạt được sự ổn định giá mà không có oracle bên ngoài bằng cách tính tất cả các tham số theo đơn vị tiền mã hóa trong khi cho phép các thành viên thị trường điều chỉnh lượng đốt dựa trên đánh giá giá trị bên ngoài:

Mệnh đề 12 (Khả năng phản ứng giá)**.** *Khi giá bên ngoài của tiền mã hóa tăng theo hệ số γ, người dùng hợp lý sẽ giảm lượng đốt của họ khoảng $1/\gamma$, duy trì chi phí tính theo tiền pháp định không đổi mà không thay đổi giao thức.*

Cơ chế này cho phép điều chỉnh tự động đối với các thay đổi giá bên ngoài mà không cần đầu vào oracle hoặc quyết định quản trị. Thuộc tính không cần oracle là yêu cầu thiết kế chung với khung tiền tệ thích ứng của **?**; tính đọc được của chi tiêu bảo mật PoW làm cho thiết kế tiền tệ không cần oracle có thể được thiết lập trong **?**.

6 Phân tích bảo mật

6.1 Các thuộc tính bảo mật mật mã học

Giao thức cung cấp các đảm bảo bảo mật mật mã học tiêu chuẩn:

Định lý 13 (Bảo mật tin nhắn)**.** *Theo giả định Diffie-Hellman Quyết định, nội dung tin nhắn không thể phân biệt về mặt tính toán với ngẫu nhiên đối với các đối thủ không có quyền truy cập vào khóa riêng tư của người gửi hoặc người nhận.*

Định lý 14 (Không thể phủ nhận thanh toán)**.** *Theo tính không thể giả mạo của chữ ký số, bằng chứng thanh toán không thể bị giả mạo bởi các đối thủ không có quyền truy cập vào khóa riêng tư của người trả tiền.*

Định lý 15 (Tính xác thực danh tính)**.** *Theo tính kháng va chạm của hàm băm và tính không thể giả mạo của chữ ký, các đối thủ không thể mạo danh người dùng hợp lệ mà không có quyền truy cập vào khóa riêng tư của họ.*

6.2 Bảo mật kinh tế chống các đối thủ hợp lý

Chúng tôi phân tích bảo mật chống lại những kẻ tấn công có động cơ kinh tế:

Định lý 16 (Tính không có lợi nhuận của tấn công thư rác)**.** *Đối với các cuộc tấn công thư rác nơi giá trị thu được trên mỗi tin nhắn thành công là v_{spam} và xác suất thành công là $p_{success}$, các cuộc tấn công thư rác không có lợi nhuận khi:*

$$B > \frac{v_{spam} \cdot p_{success}}{1 - \beta\mu}$$

trong đó β là tỷ lệ đốt và μ là tỷ lệ sức mạnh khai thác của kẻ tấn công.

Điều này cung cấp các giới hạn cụ thể cho việc chọn tham số để đảm bảo bảo mật kinh tế.

6.3 Đảm bảo bảo mật và ẩn danh

Mặc dù CashWeb không cung cấp ẩn danh hoàn toàn (khóa công khai phục vụ như là định danh liên tục), nó cung cấp một số bảo vệ bảo mật:

Bảo mật nội dung tin nhắn: Tất cả các tin nhắn được mã hóa đầu cuối đến đầu cuối, ngăn các máy chủ chuyển tiếp và máy chủ khóa truy cập nội dung.

Bảo mật mô hình truyền thông: Máy chủ chuyển tiếp chỉ thấy các tin nhắn được mã hóa cho người dùng được lưu trữ của họ, giới hạn phân tích lưu lượng toàn cầu.

Tính không thể liên kết bí danh: Người dùng có thể tạo ra nhiều bí danh mà không tiết lộ các kết nối giữa chúng, cung cấp quản lý danh tính được phân vùng.

Giới hạn bảo mật siêu dữ liệu. Bảo mật nội dung không ngụ ý bảo mật siêu dữ liệu. Các giao dịch đốt hiển thị công khai trên blockchain; một máy chủ chuyển tiếp quan sát cả blockchain và lưu lượng tin nhắn đến của chính nó có thể tương quan thời gian giao dịch đốt với thời gian đến tin nhắn, có thể liên kết danh tính người trả tiền với người gửi bí danh. Máy chủ khóa ngoài ra học được ánh xạ từ khóa công khai sang địa chỉ máy chủ chuyển tiếp. Hệ thống cung cấp bảo mật *nội dung* và danh tính người gửi *bí danh*, nhưng không hoàn toàn không thể liên kết chống lại đối thủ máy chủ chuyển tiếp hoặc máy chủ khóa thông đồng. Người dùng yêu cầu đảm bảo ẩn danh mạnh hơn nên định tuyến thông qua một mixnet hoặc lớp ẩn danh tương tự trực giao với giao thức này. Đây là giới hạn đã biết của thiết kế hiện tại; các thuộc tính bảo mật mạnh hơn được để lại cho công việc trong tương lai.

6.4 Khả năng phục hồi trước các cuộc tấn công liên minh

Chúng tôi xem xét các cuộc tấn công bởi các liên minh thành viên mạng độc hại:

Mệnh đề 17 (Tính khả dụng máy chủ chuyển tiếp dưới điều kiện thông đồng một phần)**.** *Theo các điều kiện: (i) người dùng duy trì kết nối với $k \geq 2$ máy chủ chuyển tiếp được chọn độc lập, (ii) mỗi máy chủ chuyển tiếp là độc hại với xác suất $f < 1/2$ độc lập, (iii) các máy chủ độc hại thả tin nhắn im lặng: xác suất thất bại giao là nhiều nhất f^k, giảm xuống dưới mục tiêu δ đối với $k \geq \log(1/\delta)/\log(1/f)$.*

*Các đảm bảo thỏa thuận Byzantine hình thức (an toàn và hoạt động dưới $f < 1/3$ nút Byzantine) áp dụng cho mạng máy chủ khóa theo các giả định BFT tiêu chuẩn (**?**). Lớp chuyển tiếp yêu cầu tính khả dụng, không phải tính nhất quán; giao dư thừa là đủ.*

Lưu ý về độ trễ máy chủ khóa. *Đồng thuận BFT trên các máy chủ khóa phân tán địa lý gây ra độ trễ khứ hồi vốn có—thường là 50–500 ms đối với tập phân tán toàn cầu, với nhiều vòng cần thiết để đạt tính cuối cùng. Do đó, đăng ký và cập nhật khóa lan truyền qua mạng máy chủ khóa theo thứ tự giây. Điều này chấp nhận được cho quản lý danh tính (đăng ký không thường xuyên) nhưng loại trừ các đảm bảo thu hồi khóa thời gian thực. Máy chủ chuyển tiếp nên áp dụng khoảng thời gian ân hạn ngắn trước khi tin tưởng các khóa mới đăng ký, và nên triển khai kiểm tra độ mới của khóa cho các tương tác có giá trị cao hoặc lần liên hệ đầu tiên.*

Định lý 18 (Kháng cự liên minh máy chủ khóa)**.** *Mạng máy chủ khóa duy trì tính khả dụng và nhất quán miễn là $f < 1/3$ máy chủ khóa là trung thực, sử dụng các kỹ thuật dung sai lỗi Byzantine tiêu chuẩn.*

7 Cân nhắc triển khai

7.1 Định dạng tin nhắn giao thức và API

CashWeb tận dụng Protocol Buffers **?** để tuần tự hóa tin nhắn có cấu trúc và các API HTTP RESTful để giao tiếp mạng. Các định dạng tin nhắn chính bao gồm:

Đăng ký danh tính:

```
message IdentityRegistration {
  bytes public_key = 1;
  string relay_address = 2;
  ProofOfPayment proof = 3;
  int64 timestamp = 4;
}
```

Tin nhắn được mã hóa:

```
message EncryptedMessage {
  bytes sender_key = 1;
  bytes recipient_key = 2;
  bytes encrypted_content = 3;
  ProofOfPayment burn_proof = 4;
  int64 timestamp = 5;
}
```

Bằng chứng thanh toán:

```
message ProofOfPayment {
  bytes transaction_id = 1;
  bytes signature = 2;
  uint64 burn_amount = 3;
  bytes commitment_data = 4;
}
```

7.2 Kinh tế học máy chủ chuyển tiếp và Khuyến khích

Máy chủ chuyển tiếp phải bền vững về mặt kinh tế trong khi duy trì bảo mật người dùng. Mô hình kinh tế bao gồm:

Nguồn doanh thu:

- Phí đăng ký từ người dùng mới
- Dịch vụ cao cấp tùy chọn (tăng dung lượng lưu trữ, giao ưu tiên)
- Chia sẻ phí giao dịch (đối với các máy chủ chuyển tiếp cũng khai thác)

Cơ cấu chi phí:

- Chi phí lưu trữ cho các tin nhắn được mã hóa

- Chi phí băng thông cho việc giao tin nhắn
- Chi phí tính toán cho xác minh thanh toán

Động lực cạnh tranh: Người dùng có thể di chuyển giữa các máy chủ chuyển tiếp bằng cách sử dụng API tiêu chuẩn, tạo ra áp lực thị trường cho giá cạnh tranh và chất lượng dịch vụ.

7.3 Quản lý đốt phía client và Trải nghiệm người dùng

Các client hướng người dùng phải trừu tượng hóa sự phức tạp của quản lý tiền mã hóa trong khi duy trì bảo mật:

Lựa chọn lượng đốt tự động: Các client có thể triển khai lựa chọn lượng đốt tự động dựa trên:

- Ưu tiên tin nhắn (các tin nhắn khẩn cấp sử dụng tỷ lệ đốt cao hơn)
- Mối quan hệ người nhận (đốt cao hơn cho lần liên hệ đầu tiên)
- Tắc nghẽn mạng (điều chỉnh động dựa trên thời gian giao quan sát được)

Tích hợp ví: Tích hợp liền mạch với các ví tiền mã hóa thông qua các giao diện được tiêu chuẩn hóa, hỗ trợ cả kiến trúc ví giám hộ và không giám hộ.

Bảo vệ bảo mật: Phần mềm client bao gồm các biện pháp bảo vệ tích hợp chống phân tích lưu lượng và các cuộc tấn công thời gian thông qua xử lý hàng loạt tin nhắn và độ trễ ngẫu nhiên.

7.4 Tích hợp với hạ tầng hiện có

Giao thức được thiết kế để triển khai tăng dần bên cạnh các hệ thống truyền thông hiện có:

Cổng Email: Các tin nhắn CashWeb có thể được bắc cầu tới/từ email truyền thống thông qua các dịch vụ cổng xử lý các hoạt động tiền mã hóa.

Tích hợp Web: Các thư viện JavaScript cho phép tích hợp CashWeb trực tiếp trong các ứng dụng web thông qua kết nối WebSocket.

Hỗ trợ di động: Các SDK di động gốc cung cấp các triển khai tiết kiệm pin với quản lý khóa phù hợp cho môi trường di động.

8 Mô hình mối đe dọa và Phân tích tấn công

8.1 Tấn công thư rác và DoS

Tấn công thư rác trực tiếp: Các đối thủ cố gắng gửi khối lượng lớn tin nhắn không mong muốn. Cơ chế đốt làm cho cuộc tấn công này tốn kém: gửi N tin nhắn thư rác với lượng đốt tối thiểu B_{min} tốn ít nhất $N \cdot B_{min}$. Để thư rác có lợi nhuận, kẻ tấn công phải trích xuất giá trị $V > B_{min}$ trên mỗi tin nhắn thành công, điều này khó xảy ra đối với hầu hết các danh mục thư rác.

Tấn công kiệt sức tài nguyên: Các đối thủ cố gắng áp đảo các máy chủ chuyển tiếp với các yêu cầu xử lý tin nhắn. Yêu cầu thanh toán giới hạn khối lượng tấn công, trong khi các máy chủ chuyển tiếp có thể triển khai giới hạn tốc độ bổ sung dựa trên số tiền thanh toán.

Tấn công kiệt sức lưu trữ: Các đối thủ gửi các tin nhắn đã thanh toán hợp lệ để lấp đầy bộ nhớ máy chủ chuyển tiếp. Máy chủ chuyển tiếp có thể triển khai các chính sách quản lý lưu trữ bao gồm xóa tự động các tin nhắn cũ và các tầng lưu trữ cao cấp.

8.2 Tấn công kinh tế

Tấn công tái chế phí: Các đối thủ kiểm soát hạ tầng khai thác cố gắng thu hồi quỹ đã đốt thông qua phí giao dịch. Cơ chế đốt phí một phần (Phần **??**) giới hạn việc thu hồi ở $(1 - \beta)\mu$ trong đó β là tỷ lệ đốt và μ là tỷ lệ sức mạnh băm của kẻ tấn công.

Tấn công Sybil: Các đối thủ tạo ra nhiều danh tính giả để khuếch đại khả năng tấn công. Mỗi danh tính yêu cầu cam kết kinh tế thông qua phí đăng ký, tạo ra sự tăng tuyến tính giữa ngân sách tấn công và khả năng Sybil (Mệnh đề **??**).

Thao túng thị trường: Các đối thủ cố gắng thao túng giá tiền mã hóa để ảnh hưởng đến kinh tế học đốt. Thiết kế không cần oracle làm cho hệ thống phản ứng với nhưng không phụ thuộc vào thao túng giá bên ngoài.

8.3 Tấn công hạ tầng

Kiểm duyệt máy chủ chuyển tiếp: Các máy chủ chuyển tiếp độc hại từ chối giao tin nhắn từ những người gửi cụ thể. Người dùng có thể phát hiện kiểm duyệt thông qua xác nhận giao và di chuyển sang các máy chủ chuyển tiếp thay thế.

Thao túng máy chủ khóa: Các đối thủ cố gắng xuất bản thông tin danh tính giả. Các yêu cầu chữ ký mật mã học ngăn chặn mạo danh, trong khi mạng máy chủ khóa phân tán cung cấp khả năng phục hồi chống lại việc xâm phạm máy chủ đơn lẻ.

Phân vùng mạng: Các đối thủ cố gắng cô lập người dùng hoặc máy chủ khỏi mạng rộng hơn. Kiến trúc liên kết cung cấp nhiều đường truyền thông, trong khi mạng tiền mã hóa cung cấp một cơ chế điều phối toàn cầu.

8.4 Tấn công bảo mật

Phân tích lưu lượng: Các đối thủ theo dõi lưu lượng mạng để suy ra các mô hình truyền thông. Mã hóa đầu cuối đến đầu cuối bảo vệ nội dung tin nhắn, trong khi các client có thể sử dụng định tuyến hành củ hoặc các kỹ thuật tương tự để bảo vệ thêm.

Tấn công thời gian: Các đối thủ tương quan thời gian gửi và nhận tin nhắn để xác định các mối quan hệ truyền thông. Các client có thể triển khai độ trễ ngẫu nhiên và xử lý hàng loạt tin nhắn để giảm tương quan thời gian.

Phân tích thanh toán: Các đối thủ phân tích các giao dịch blockchain để liên kết các khoản thanh toán với tin nhắn. Việc sử dụng các địa chỉ mới cho mỗi giao dịch đốt và trộn giao dịch phù hợp có thể cung cấp bảo mật thêm.

9 Đánh giá và Thảo luận

9.1 Kết quả phân tích lý thuyết

Phân tích lý thuyết của chúng tôi chứng minh một số thuộc tính chính:

Khả năng mở rộng kháng thư rác: Chi phí của các cuộc tấn công thư rác tăng tuyến tính với khối lượng tấn công, cung cấp các đảm bảo bảo vệ có thể dự đoán. Đối với tỷ lệ đốt tối thiểu $B_{min} = \$0.01$ mỗi tin nhắn, gửi 1 triệu tin nhắn thư rác tốn ít nhất \$10.000, ngoài chi phí vận hành.

Khả năng tiếp cận người dùng hợp lệ: Đối với các tỷ lệ đốt trong khoảng \$0.01 - \$0.10 mỗi tin nhắn, rào cản kinh tế vẫn tối thiểu cho người dùng hợp lệ (tương đương với chi phí nhắn tin SMS) trong khi cung cấp sự ngăn chặn thư rác đáng kể.

Lợi ích hiệu ứng mạng: Khi việc áp dụng mạng tăng, giá trị của nhắn tin hợp lệ tăng nhanh hơn hiệu quả tấn công thư rác, tạo ra phản hồi tích cực cho sự phát triển hệ thống.

9.2 So sánh với các hệ thống hiện có

Bảng **??** so sánh CashWeb với các phương pháp chống thư rác và nhắn tin hiện có:

Hệ thống	Phi tập trung	Chống thư rác	Bảo mật	Khả năng mở rộng
Email (SMTP)	Một phần	Kém	Kém	Cao
Hashcash	Có	Trung bình	Tốt	Kém
Matrix	Một phần	Kém	Tốt	Trung bình
Signal	Không	Tốt	Xuất sắc	Trung bình
CashWeb	Có	Tốt	Tốt	Cao

Bảng 1: So sánh các hệ thống nhắn tin theo các thuộc tính chính

9.3 Kinh nghiệm triển khai

Mạng xã hội Stamp cung cấp kinh nghiệm triển khai ban đầu với các khái niệm CashWeb. Đặc tả giao thức trong bài báo này là sự hoàn thiện hình thức của một kiến trúc mà các cơ chế cốt lõi của nó—đốt-để-nói, chuyển tiếp liên kết, danh tính máy chủ khóa—đã được tạo mẫu trong Stamp. Các quan sát triển khai bao gồm:

Sự chấp nhận của người dùng: Người dùng thích nghi với nhắn tin dựa trên đốt mà không có ma sát đáng kể khi lượng đốt vẫn dưới khoảng \$0.05 mỗi tin nhắn. Các lượng cao hơn tạo ra sự do dự đáng chú ý cho giao tiếp thông thường.

Giảm thư rác: Các yêu cầu đốt ngăn chặn hiệu quả thư rác tự động; chi phí kinh tế trên mỗi tin nhắn đưa ra một mức sàn vượt quá lợi nhuận kỳ vọng cho các chiến dịch thư rác điển hình. Đo lường hệ thống trên một triển khai sản xuất quy mô lớn được hoãn lại cho công việc thực nghiệm trong tương lai.

Chi phí hạ tầng: Tiêu thụ tài nguyên máy chủ chuyển tiếp mở rộng xấp xỉ tuyến tính với số lượng người dùng trong thử nghiệm ban đầu. Xác minh bằng chứng thanh toán thêm chi phí tính toán khiêm tốn vào định tuyến tin nhắn cơ bản—được chi phối bởi tra cứu trạng thái blockchain thay vì xác minh mật mã học.

Những quan sát này là không chính thức và từ một triển khai quy mô nhỏ. Họ xác nhận phương pháp là khả thi nhưng không thay thế cho đánh giá hiệu suất nghiêm ngặt ở quy mô.

9.4 Giới hạn và Đánh đổi

Phương pháp CashWeb liên quan đến một số đánh đổi vốn có:

Rào cản kinh tế: Mặc dù lượng đốt là tối thiểu cho người dùng hợp lệ, họ có thể tạo ra rào cản cho người dùng ở các vùng bị bất lợi về kinh tế. Công việc trong tương lai có thể khám phá tỷ lệ đốt trượt thang hoặc các cơ chế bằng chứng giá trị thay thế.

Phụ thuộc tiền mã hóa: Hệ thống yêu cầu quyền truy cập vào các mạng tiền mã hóa, điều này có thể giới hạn việc áp dụng ở các vùng có quyền truy cập bị hạn chế hoặc trong số người dùng không thoải mái với tiền mã hóa.

Độ phức tạp khôi phục: Các tình huống mất khóa yêu cầu các quy trình khôi phục phức tạp hơn so với các hệ thống tập trung truyền thống, có thể tạo ra các thách thức về khả năng sử dụng cho người dùng không chuyên kỹ thuật.

9.5 Mở rộng và Ứng dụng trong tương lai

Giao thức CashWeb cung cấp nền tảng cho nhiều mở rộng:

Hệ thống danh tiếng: Điểm danh tiếng người dùng dựa trên phản hồi tin nhắn nhận được có thể cho phép điều chỉnh tỷ lệ đốt động và lọc thư rác cải thiện.

Thị trường nội dung: Cơ chế đốt có thể mở rộng đến các khoản thanh toán vi mô nội dung, cho phép các mô hình kinh tế mới cho việc chia sẻ thông tin và phân phối phương tiện.

Truyền thông IoT: Truyền thông máy-với-máy với thanh toán tự động có thể cho phép các ứng dụng Internet of Things mới nơi các thiết bị trả tiền cho băng thông và tài nguyên xử lý.

Mạng xã hội phi tập trung: Hệ thống xuất bản-đăng ký cung cấp hạ tầng cho các nền tảng mạng xã hội phi tập trung hoàn toàn với sự phù hợp khuyến khích kinh tế.

10 Kết luận

Chúng tôi đã trình bày CashWeb, một bộ giao thức toàn diện giải quyết các vấn đề khuyến khích kinh tế cơ bản thúc đẩy tập trung hóa trong các hệ thống truyền thông internet. Thông qua đặc tả hình thức của các cơ chế chống thư rác đốt-để-nói, thiết kế hạ tầng liên kết và phân tích bảo mật kinh tế, chúng tôi chứng minh rằng tích hợp tiền mã hóa có thể khôi phục tầm nhìn ban đầu về giao tiếp internet phi tập trung trong khi cung cấp khả năng chống thư rác vượt trội so với các phương pháp hiện có.

Sự nhấn mạnh của giao thức vào các cơ chế chống thư rác kinh tế thay vì tính toán hoặc quy định cung cấp một số lợi thế: đảm bảo bảo vệ có thể dự đoán, khả năng mở rộng đến triển khai toàn cầu và khả năng chống lại các cuộc chạy đua vũ trang công nghệ ảnh hưởng đến các phương pháp tính toán. Kinh nghiệm triển khai với mạng xã hội Stamp xác nhận tính khả thi thực tế của phương pháp.

Công việc trong tương lai nên tập trung vào việc giảm rào cản kinh tế cho người dùng bị bất lợi, cải thiện khả năng sử dụng quản lý khóa và khám phá các ứng dụng ngoài nhắn tin cho các vấn đề truyền thông và điều phối khác chịu áp lực tập trung hóa tương tự.

Mục tiêu cuối cùng của CashWeb không chỉ đơn thuần là đổi mới kỹ thuật, mà là khôi phục chủ quyền người dùng đối với giao tiếp kỹ thuật số—cho phép quay trở lại các nguyên tắc sáng lập của internet về phi tập trung và trao quyền cho người dùng trong khi giải quyết các thực tế kinh tế thúc đẩy sự tập trung hóa ban đầu.