CLOAK

ENIGMA V2.1

Whitepaper (Revised)

February 2018

ENIGMA

HỆ THỐNG GIAO DỊCH RIÊNG TƯ, BẢO MẬT VÀ KHÔNG THỂ TRUY XUẤT DÀNH CHO CLOAKCOIN

1. TÓM TẮT

CloakCoin là tiền số mã hóa được thiết kế để tạo điều kiện cho các giao dịch phi tập trung, riêng tư, bảo mật và không thể truy xuất với Enigma.

Cloak là một coin PoW/PoS (Proof of Work, Proof of Stake) kép, hiện đang trong giai đoạn Proof of Stake (sinh lãi).

Enigma là hệ thống thanh toán riêng tư, an toàn và không thể truy xuất của CloakCoin, tạo cơ sở cho sự phát triển tương lai và cung cấp hệ thống giao dịch nền tảng cho các ứng dụng phi tập trung chạy trên mạng lưới CloakCoin.

Vấn đề bảo mật hiện nay có lẽ quan trọng hơn bao giờ hết. Tốc độ tiến bộ như vũ bão của công nghệ đã nhanh chóng mở rộng tầm nhìn của chúng ta và kết nối thế giới hơn bao giờ hết. Nhờ sự ra đời của Bitcoin vào năm 2009, tiền số mã hóa đang dần trở thành xu hướng và bây giờ chúng ta có thể chuyển tiền kỹ thuật số an toàn trên toàn thế giới ngay lập tức, với sức mạnh của blockchain.

Khi tiền số mã hóa được chấp nhận rộng rãi hơn, ngày càng có nhiều điều luật hơn là không thể tránh khỏi. Tác động của những điều luật này là có thể thấy trước, nhưng nhiều người lo ngại nó có thể là quá hà khắc và nhằm kiềm chế một số khía cạnh tự do của tiền điện tử.

ENIGMA

Enigma là một dịch vụ kết hợp phi tập trung, off-blockchain (ngoài chuỗi) cho phép người dùng trên mạng lưới CloakCoin chuyển Cloak riêng tư và bảo mật cho nhau. Nó được thiết kế để đảm bảo quá trình kết hợp được an toàn và không thể truy xuất bởi các nhà quan sát bên thứ ba. Điều này đảm bảo các Cloak coin của người dùng được lưu giữ an toàn trong quá trình giao dịch và người gửi và người nhận không thể bị ràng buộc hoặc liên kết với nhau. Cloak coin không bao giờ được chuyển đến một bên trung gian trong suốt thời gian Cloaking, vì vậy coin vẫn an toàn. Chúng tôi cũng đã làm việc chăm chỉ để đảm bảo hệ thống Enigma thưởng cho người dùng hỗ trợ các giao dịch Cloaking và sẽ tiếp tục cải thiện quy trình và khuyến khích thêm những người tham gia tích cực. Bất kỳ ai có coin Cloak đều có thể tham gia vào hoạt động Cloaking, cho phép họ để ví của mình chạy ở chế độ Staking/Cloaking cho phép nó hỗ trợ thụ động trong Cloaking và kiếm được phần thưởng đáng kể.

2. TỔNG QUAN ENIGMA V1.0

Enigma là giải pháp công khai đầu tiên của hệ thống thanh toán riêng tư, an toàn và không thể truy xuất của Cloak. Các giao dịch Enigma bị "che giấu" khỏi những người dùng khác, những người nhận được phần thưởng vì sự trợ giúp của họ. Những người dùng khác cung cấp đầu vào và đầu ra cho giao dịch Enigma làm cho giao dịch không thể xác định nguồn và đích đúng của giao dịch phải che giấu. Tất cả các thông điệp Enigma trên mạng lưới được băm và mã hóa cho người nhận nhờ CloakShield để đảm bảo tính bảo mật và toàn vẹn dữ liệu. Vui lòng xem Phần 3 - 'CloakShield' để biết thêm chi tiết.

2.1. QUY TRÌNH ENIGMA (ĐỐI VỚI CÁC NODE ENIGMA CHO PHÉP)

THÔNG BÁO ENIGMA

Các node Enigma giao tiếp qua mạng lưới Cloak và một node sẽ truy xuất các node Enigma đang hoạt động khác. Phát thông báo Enigma (Enigma Announcement Broadcasts) cảnh báo các node Enigma khác về chìa khóa phiên công khai và số dư Enigma phải che giấu hiện tại.

YÊU CẦU CHE GIẤU ENIGMA

Khi một người dùng muốn gửi một Giao dịch Bí mật (Cloaked Enigma), họ chọn một loạt các node Enigma (với số dư Enigma đủ cao) và yêu cầu họ hỗ trợ che giấu. Node Enigma có thể hỗ trợ che giấu và gửi phản hồi chấp nhận cho người yêu cầu để cho biết điều này. Nếu một node Enigma từ chối tham gia che giấu hoặc không trả lời kịp thời, một node Enigma thay thế sẽ được chọn và liên lạc.

Bảo vệ DDoS (distributed denial of service) sẽ đưa vào danh sách đen bất kỳ node nào có hành vi không đúng đối với phần còn lại của phiên. Một node được cho là có hành vi không đúng nếu nó liên tục từ chối ký giao dịch Enigma hoặc từ chối chuyển tiếp thông điệp Enigma. Các node che giấu Enigma sử dụng giao thức trao đổi khóa Elliptic Curve Diffie Hellman (ECDH) để lấy bí mật được chia sẻ bằng node khởi tạo Enigma, được sử dụng để tạo ra khóa bí mật được chia sẻ để mã hóa dữ liệu RSA-256 đối xứng giữa node che giấu và node người gửi.

CHẤP NHẬN CHE GIẤU ENIGMA

Khi node Enigma chấp nhận yêu cầu 'che giấu', nó cung cấp danh sách các đầu vào và đầu ra giao dịch được sử dụng cho giao dịch Enigma. Số tiền đầu vào được cung cấp bởi node che giấu phải lớn hơn hoặc bằng số tiền gửi Enigma (cộng với bất kỳ khoản phí nào). Các đầu ra được lựa chọn cẩn thận sao cho chúng khớp với đầu ra thực của giao dịch Enigma càng gần đúng càng tốt. Nếu địa chỉ đầu ra của Enigma chưa được sử dụng trước đó, một địa chỉ thay đổi mới sẽ được tạo ra bởi ‘Người che giấu’ (‘Cloaker’). Nếu địa chỉ đầu ra của Enigma trước đó đã nhận được tiền, địa chỉ hiện tại có hoạt động tương tự sẽ được ‘Người che giấu’ chọn để trả lại số tiền đầu vào của họ và nhận phần thưởng ‘che giấu’ Enigma.

GIAO DỊCH ENIGMA ‘ĐƯỢC CHE GIẤU’

Người gửi Enigma xây dựng một giao dịch 'che giấu' bằng cách sử dụng các đầu vào và đầu ra được cung cấp bởi các node Enigma Cloaker. Người gửi Enigma sau đó thêm đầu vào và đầu ra của mình vào giao dịch, trước khi xáo trộn tất cả các đầu vào và đầu ra giao dịch để tạo điều kiện thuận lợi cho việc ‘che giấu’. Giao dịch 'được che giấu' sau đó được mã hóa và gửi (bằng CloakShield) cho mỗi Người che giấu tham gia. Các node Cloaker kiểm tra giao dịch để đảm bảo các đầu vào và đầu ra mà chúng cung cấp có trong giao dịch 'được che giấu' và một hoặc nhiều đầu ra của chúng có được thưởng với đầy đủ phí không.

Nếu kiểm tra giao dịch được thông qua, giao dịch được ký (SIGHASH_ ALL + SIGHASH_ANYONECANPAY), được mã hóa và chuyển lại cho Người gửi Enigma. Một khi tất cả Người che giấu Enigma đã ký giao dịch, Người gửi Enigma xác nhận giao dịch đã ký là hợp lệ và ký tên. Giao dịch 'được che giấu' sau đó đã sẵn sàng để gửi tới mạng lưới.

2.2.1. TRUY XUẤT CÁC NODE ENIGMA CLOAKING

Enigma cho phép các node trên mạng lưới Cload phát thông báo đến các node khác. Các thông báo Enigma này chứa ID khóa công khai của node và số dư hiện có cho các hoạt động che giấu Enigma. Các node giữ một danh sách các node Enigma hoạt động khác trên mạng để chúng có thể giao tiếp với nhau để che giấu. Các ID node được tạo trên cơ sở từng phiên; khởi động lại client sẽ làm mới ID hiện tại.

1. Mỗi ví tạo ra một cặp khóa công khai/bí mật (secp256k1) cho phiên khi khởi động.

2. Ví thông báo định kỳ khóa công khai và số dư Cloaking của phiên cho các node khác trên mạng Cloak.

3. Các node truy xuất các node Enigma Cloaking đang hoạt động khác và có thể trao đổi với chúng trực tiếp hoặc gián tiếp (qua CloakShield Onion Routing).

2.2.2. KHỞI TẠO GIAO DỊCH ENIGMA

ALICE muốn gửi 10 CLOAK cho BOB bằng 5 node phối hợp.

1. Alice phát yêu cầu Enigma đến mạng lưới, chứa khóa công khai phiên Enigma của cô và số lượng Cloak cô muốn gửi. Yêu cầu của cô được gửi an toàn thông qua một chuỗi 5 node Enigma để che giấu người khởi tạo.

2. Catherine đã bật ‘Chế độ Che giấu’ và tạo ra một kênh mã hóa CloakShield an toàn để liên lạc an toàn với Alice. Catherine sau đó xây dựng một gói phản hồi Enigma và gửi nó an toàn cho Alice. Phản hồi này chứa danh sách các yếu tố đầu vào và đầu ra của Catherine mà Alice sẽ sử dụng để 'che giấu' giao dịch của mình.

3. Alice giải mã và xử lý phản hồi Enigma của Catherine và tạo ra một giao dịch Enigma bằng cách sử dụng các đầu vào và đầu ra của mình kết hợp với các đầu vào và đầu ra của Catherine. Giao dịch này được mã hóa và gửi cho Catherine để ký.

4. Catherine giải mã giao dịch Enigma và thực hiện một số kiểm tra tính toàn vẹn trên giao dịch để đảm bảo đầu vào và đầu ra mà mình cung cấp có được sử dụng đúng và mình có được thưởng đầy đủ không. Nếu giao dịch Enigma vượt qua các bài kiểm tra, Catherine ký nó, mã hóa nó và chuyển nó cho Alice.

5. Alice tiến hành kiểm tra thêm về giao dịch đã ký trước khi mình ký tên. Giao dịch sau đó được gửi đến mạng lưới (được gửi an toàn qua các node Enigma) để đưa vào block.

6. Khi giao dịch kết thúc, Bob sẽ nhận được tiền từ Alice và Catherine sẽ nhận phần thưởng ‘Cloaking’ vì đã hỗ trợ giao dịch Enigma.

7. Do đầu vào và đầu ra của Catherine phản chiếu của Alice, nên không thể xác định chính xác người nhận và người gửi thật sự của giao dịch Enigma.

VÍ DỤ GIAO DỊCH ENIGMA

ALICE muốn gửi coin ẩn danh cho BOB.

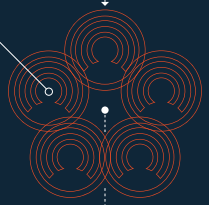
ALICE (−10.0992) CLOAK

(−10) CLOAK + (−0.0992) Enigma fee
= (−10.0992) CLOAK total

Các node trộn ENIGMA bắt đầu trao đổi với nhau.

CATHERINE

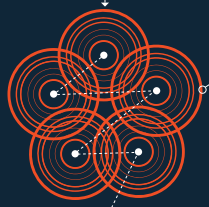
Tất cả người nắm giữ coin đều có thể tuyên bố mình là Node Trộn (Mixer Node), hay còn gọi là 'Người che giấu' (Cloaker)



Tất cả người tham gia đều ẩn danh và giao tiếp với nhau qua kênh được mã hóa.

Ví của ALICE hiện kết nối với các node trộn.

Mỗi node trộn đều giúp ALICE bằng cách xáo trộn giao dịch.



Mạng lưới các node này tạo ra một tổ chức ẩn danh phi tập trung tương tự TOR Onion Routing.

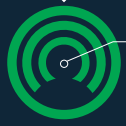
Các node trộn được nhận thưởng vì che giấu giao dịch của ALICE.

(+0.0992) CLOAK

Phí từ 0,2% (>1000 coin) đến 1% (0 coin) được chia sẻ giữa tất cả những người che giấu tham gia.

Hệ thống làm việc liền mạch để đảm bảo tính ẩn danh và riêng tư được toàn vẹn.

BOB sau đó nhận được thanh toán được mã hóa của ALICE.



BOB (+10) CLOAK

BOB nhận thành công 10 CLOAK một cách ẩn danh..

3. CLOAKSHIELD

CloakShield cung cấp phương thức giao tiếp bảo mật giữa các node trên mạng lưới Cloak bằng cách sử dụng mã hóa RSA đối xứng được hỗ trợ bởi một khóa giao dịch Elliptic Curve Diffie Hellman (ECDH). Điều này cho phép các node trao đổi dữ liệu an toàn, bảo vệ khỏi những kẻ đánh cắp (bên trung gian) và kẻ mạo danh (tấn công sybil). CloakShield được thiết kế để bảo mật cả Enigma và các ứng dụng CloakCoin phi tập trung, đồng thời đảm bảo dữ liệu của bạn được giữ riêng tư nhất có thể.

CloakShield cho phép gửi dữ liệu được mã hóa tới một hoặc nhiều người nhận. Khi gửi đến một người nhận duy nhất, giao dịch được mã hóa RSA bằng khóa bí mật chung ECDH. Khi gửi đến nhiều người nhận, giao dịch được mã hóa bằng khóa một lần và sau đó khóa được mã hóa cho từng người nhận bằng phương pháp ECDH/RSA.

TẠO KHÓA MÃ HÓA CHUNG

Để Alice và Bob giao tiếp an toàn, họ phải thống nhất một khóa mã hóa chung. CloakShield sử dụng ECDH để thực hiện việc này:

- Alice có khóa riêng tư Enigma dA và khóa công khai Enigma QA=dAG (trong đó G là một generator tạo đường cong ellip). Bob có khóa riêng tư Enigma dB và khóa công khai Enigma QB=dBG.

- Alice có khóa công khai dB Enigma của Bob từ thông báo Enigma mà anh ta gửi cho mạng lưới để thông báo anh ấy có thể hỗ trợ cloaking. Cô ấy sử dụng khóa riêng tư dA của mình và khóa công khai QB của Bob để tính toán khóa bí mật chung dAQB=dAdBG (ECDH_compute_key trong OpenSSL).

- Alice sau đó tạo hàm băm SHA256 của bí mật và thông qua hàm băm đến phương pháp OpenSSLEVP_BytesToKey để lấy khóa mã hóa và IV, sẽ được dùng để mã hóa dữ liệu cho Bob (bằng mã hóa RSA đối xứng).

- Alice giờ có thể tạo thông điệp được CloakShield bảo mật cho Bob.

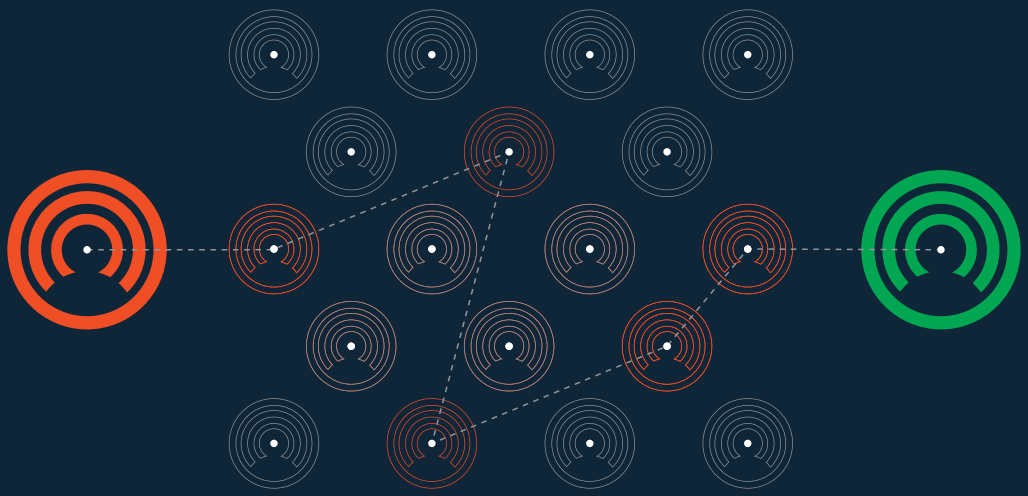
Khi Bob nhận thông điệp được CloakShield từ Alice, anh ta đọc khóa công khai của Alice từ phần tiêu đề (header) thông điệp và tạo ra khóa bí mật chung tương tự như Alice, theo từng bước trên (với khóa bí mật của anh ấy, thay vì của Alice).

Ví Cloak giữ danh sách các khóa CloakShield hoạt động và sẽ kiểm tra danh sách khóa CloakShield hiện có trước khi tạo cái mới.

DỮ LIỆU CLOAKSHIELD

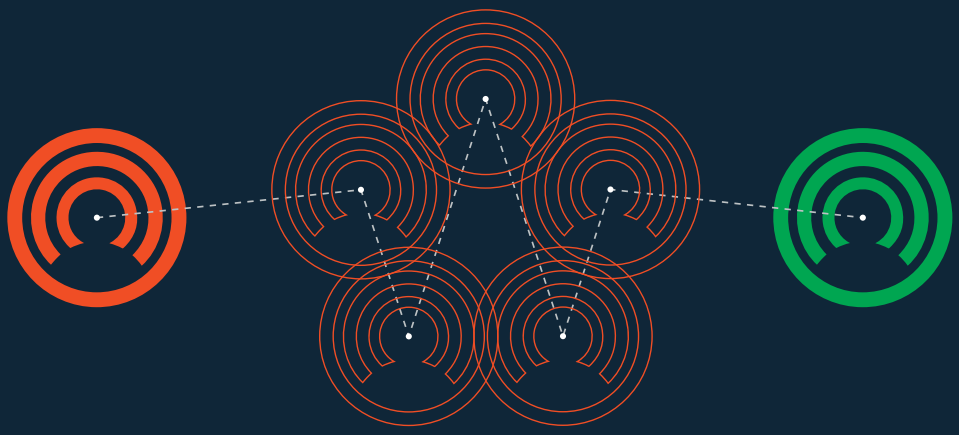
CloakShield cho phép bất kỳ đối tượng dữ liệu Cloak nào được xếp theo thứ tự và truyền an toàn đến một hoặc nhiều người nhận. Tiêu đề gói dữ liệu CloakShield chứa khóa công khai Enigma của người gửi và các khóa công khai băm của người nhận.

Tiêu đề của CloakShield chứa hàm băm xác minh, được tạo ra bằng cách sử dụng khóa công khai của người gửi và dữ liệu thô chưa được mã hóa. Hàm băm này được xác minh trong quá trình giải mã dữ liệu CloakShield để đảm bảo rằng thông tin người nhận trong tiêu đề khớp với khóa mã hóa và dữ liệu đó chưa bị thay đổi.



KỸ THUẬT CLOAKSHIELD ONION ROUTING

Onion routing là một kỹ thuật (được TOR sử dụng) để giao tiếp ẩn danh qua mạng máy tính. Trong một mạng lưới onion, các thông điệp được đóng gói trong các lớp mã hóa, tương tự như các lớp của củ hành (onion). Dữ liệu đã mã hóa được truyền qua một chuỗi các node mạng được gọi là onion router (bộ định tuyến củ hành), mỗi node sẽ “bóc” đi một lớp vỏ, khám phá điểm đến tiếp theo của dữ liệu. Khi lớp cuối cùng được giải mã, thông điệp sẽ đến đích của nó. Người gửi vẫn ẩn danh vì mỗi bên trung gian chỉ biết vị trí của node ngay trước và sau nó.



ONION ROUTING ANALOGY

Việc bổ sung chức năng ‘oninon routing' vào mạng Enigma (sử dụng CloakShield) cho phép các node giao tiếp gián tiếp để phá vỡ phân tích lưu lượng truy cập. Điều này ngăn cản nỗ lực xác định các node nào đang giao tiếp với nhau hoặc các node nào đang gửi các giao dịch đến mạng lưới CloakCoin. Khi một node Enigma muốn giao tiếp với một node Enigma khác, nó chọn một số node Enigma khác để hoạt động như các rơle để giao tiếp. Mỗi lớp đã mã hóa chỉ có thể được giải mã bằng rơle đã định [cho lớp cụ thể đã được mã hóa quy định]. Sau khi giải mã một lớp, rơle chuyển dữ liệu đến node rơle tiếp theo. Việc định tuyến này tiếp tục cho đến khi dữ liệu đến được người nhận đã định của nó và tất cả các lớp đã được giải mã lần lượt bởi các node rơle được chọn. Do bản chất khép kín của mạng Enigma, các node thoát là không cần thiết và CloakShield đảm bảo không có nguy cơ node rơle đọc hoặc thay đổi dữ liệu đã mã hóa.

4. ĐỊA CHỈ STEALTH

Cloak sử dụng hệ thống Enigma để tạo điều kiện thuận lợi cho các giao dịch riêng tư/bảo mật.

CLOAKSHIELD – GIAO TIẾP NODE NÀY VỚI NODE KHÁC

Khi khởi động, mỗi ví Cloak tạo ra một cặp khóa [NID_secp256k1] (Khóa Mã Hóa Cloaking/ CEK) cho phép chúng lấy được các khóa bí mật đặc biệt bằng ECDH với khóa riêng tư của chúng và khóa công khai của người nhận. Giao tiếp này tạo cơ sở cho tất cả các giao tiếp giữa các node liên quan đến Enigma. Xem 'src / enigma / cloakshield.h / .cpp' để biết thêm thông tin về điều này. Giao tiếp đã mã hóa dựa trên ECDH này cũng được sử dụng cho dữ liệu onion routing, được xử lý bởi CloakShield.

Khi onion routing được kích hoạt, client sẽ cố gắng xây dựng một onion route hợp lệ cho dữ liệu bằng cách sử dụng danh sách các máy ngang hàng Enigma mà nó biết. Node có thể không có kết nối trực tiếp đến các máy ngang hàng Enigma, nhưng điều đó không cần thiết vì các gói dữ liệu CloakData (dữ liệu được đóng gói để định tuyến bằng CloakShield) được chuyển tiếp ngang hàng. Một onion route thường sẽ bao gồm 3 tuyến riêng biệt đến node đích, với 3 node hop trên mỗi tuyến. Nhiều tuyến được sử dụng để xử lý với các tình huống node định tuyến rớt xuống ngoại tuyến.

Các node định kỳ gửi Thông báo Enigma (src/enigma/ enigmaann.h) cho các máy ngang hàng để quảng cáo dịch vụ của họ cho việc onion routing. Các node khác trên mạng lưu trữ các thông báo (cho đến khi chúng hết hạn hoặc được thay thế bằng bản cập nhật) và sử dụng chúng để xây dựng các onion route.

VÍ DỤ GIAO DỊCH ĐỊA CHỈ CHE GIẤU

Khi một node gửi giao dịch Enigma đến địa chỉ che giấu (stealth address), những việc sau sẽ xảy ra:

1. Người gửi tạo đầu vào để che số tiền được gửi, phần thưởng Enigma và phí mạng lưới (1% ở 0 coin đến 0,2% ở 1.000 coin trở lên).

2. Người gửi tạo đối tượng CloakingRequest (chứa số che giấu (stealth nonce) chỉ riêng cho yêu cầu này).

3. Người gửi tạo 2-4 địa chỉ thanh toán che giấu một lần bằng địa chỉ che giấu của người nhận và chia số tiền được gửi ngẫu nhiên cho các địa chỉ.

4. Người gửi quyết định có bao nhiêu người tham gia sẽ được sử dụng. Có thể chọn từ 5-25 người tham gia (mỗi người tham gia sẽ nhận 80-120% phí Enigma được chia đều).

5. Người gửi định tuyến onion route CloakRequest đến mạng lưới. Yêu cầu chứa 'số tiền gửi' để Người che giấu biết bao nhiêu để giữ lại.

6. Người che giấu nhận CloakRequest và quyết định tham gia.

7. Người che giấu cung cấp đầu vào X đến người gửi và địa chỉ che giấu, và hàm băm che giấu (cho giao dịch của họ).

8. Người che giấu gửi PhảnHồiChấpNhậnCloaking đến Người Gửi. Nó chứa địa chỉ che giấu, số che giấu và đầu vào TX.

9. Người gửi chờ đến khi đủ Người che giấu chấp nhận.

10. Người gửi tạo giao dịch Enigma bằng đầu vào của mình và đầu vào Người che giấu. Đầu vào được xáo trộn.

11. Người gửi tạo đầu ra TX cho tất cả Người che giấu. Đầu ra được chia ngẫu nhiên và trả lại cho họ. Điều này cũng có thể phân bổ phần thưởng che giấu cho những Người che giấu.

12. Người gửi tạo ra phần tiền thu về của riêng họ cho Enigma TX. Đây là những địa chỉ thanh toán che giấu một lần.

13. Người gửi tính phí TX của mạng và trừ đi phần thu về.

14. Người gửi gửi Enigma TX cho Người che giấu để ký.

15. Người che giấu kiểm tra TX để đảm bảo đầu vào có hiện diện và chính xác và địa chỉ thanh toán một lần liên kết với một trong các địa chỉ che giấu để thanh toán phần vượt số tiền đầu vào.

16. Người che giấu ký tên hoặc từ chối TX và gửi chữ ký đến Người gửi.

17. Người gửi đối chiếu chữ ký và chuyển TX đã ký đến mạng.

18. Các node quét giao dịch mới đến cho thanh toán che giấu cũng như thanh toán Enigma và phát hiện bất kỳ thanh toán hoặc thay đổi. Các cặp khóa và địa chỉ được tạo ra cho bất kỳ thanh toán khớp nào và các địa chỉ/khóa được tạo ra được lưu vào ví địa phương (local wallet)

5. TƯƠNG LAI CỦA ENIGMA – HƯỚNG PHÁT TRIỂN TIẾP THEO

Enigma tạo ra cốt lõi của CloakCoin và sẽ tiếp tục được phát triển và cải thiện khi chúng tôi tiến lên cùng CloakCoin. Dưới đây là một số tính năng được lên kế hoạch cho các bản sửa đổi trong tương lai:

THUẬT TOÁN PROOF-OF-STAKE ĐƯỢC CẢI THIỆN

Proof of Stake (PoS) là một phương pháp bảo mật mạng lưới tiền số mã hóa dựa trên người dùng thể hiện quyền sở hữu coin để ký block.

Về lâu dài, xác suất ký block là tỷ lệ thuận với số lượng coin sở hữu, một người sở hữu 1% tổng cung coin sẽ có thể ký 1% của tất cả các block proof of stake. So với cách tiếp cận proof of work, proof of stake đòi hỏi ít sức mạnh tính toán hơn đáng kể, và do đó sử dụng ít năng lượng hơn.

COIN AGE VÀ PROOF OF STAKE TUYẾN TÍNH

Nguyên tắc cơ bản để thực hiện hầu hết các Proof of Stake, bao gồm cả CloakCoin, là khái niệm về Coin Age. Về cơ bản, đây là một thước đo một người sở hữu coin giữ coin bao lâu mà không chi tiêu hoặc di chuyển chúng. Từ thời điểm hoàn thành giao dịch, các coin là một phần của giao dịch bắt đầu tích lũy Coin Age (bắt đầu từ số không). Ở dạng đơn giản nhất của nó, được gọi là "linear coin age" (“tuổi coin tuyến tính”), coin sẽ tích lũy một phút/giờ/ngày/năm của Coin Age thành từng phút/giờ/ngày/năm tuổi. Ví dụ, một người nắm giữ 365 coin trong 100 ngày tích lũy 36.500 ‘coin day’ (ngày coin), hoặc khoảng 100 ‘coin year' (‘năm coin’) (Một 'coin year' được xác định để tính cho cả năm nhuận, và do đó không chính xác 365 ngày, mà là ~ 365,24 ngày).

Thiết kế Proof-of-Stake tuyến tính đã đón nhận nhiều chỉ trích liên quan đến Coin Age. Nhiều người lập luận rằng Proof-of-Stake tuyến tính khuyến khích tích trữ coin (có thể có ảnh hưởng bất lợi đến khối lượng giao dịch và chuyển nhượng). Một số khác than phiền rằng Proof-of-Stake tuyến tính có thể ảnh hưởng đến sự hiệu quả an ninh mạng. Việc triển khai Proof-of-Stake tuyến tính thường bị ảnh hưởng do người dùng kết nối định kỳ với mạng Cloak để đặt cọc tiền của họ và sau đó ngắt kết nối khi tất cả các Coin Age đã bị phá hủy.
Người dùng sau đó đợi cho đến khi Coin Age được bổ sung trước khi lặp lại quá trình kết nối-stake- ngắt kết nối. Điều này không cung cấp sự bảo mật tốt nhất cho mạng, và một thuật toán Proof-of-Stake thưởng thường xuyên hoặc liên tục staking sẽ có lợi nhất cho CloakCoin và tiền Proof-of-Stake có liên quan.

Để đảm bảo những Người che giấu Enigma được khen thưởng càng nhiều càng tốt, Coin Age phải được loại bỏ khỏi thuật toán Proof-of-Stake của CloakCoin. Điều này sẽ đảm bảo rằng Người che giấu nhận được cả phần thưởng toàn phần và bất kỳ phần thưởng Enigma Cloaking nào. Việc bổ sung thành phần tốc độ trong tính toán phần thưởng staking sẽ tiếp tục thưởng cho các node che giấu Enigma đang hoạt động, khuyến khích người dùng tham gia vào Enigma Cloaking để tăng thêm lợi ích thu được của họ ngoài phần thưởng Cloaking kiếm được.

Ngoài việc cung cấp phần thưởng lớn hơn cho người dùng tham gia tích cực, một thuật toán Proof-of-Stake được cải tiến cũng cung cấp những cải tiến nói trên cho hệ thống an ninh.

KẾT HỢP VÀ PHÂN TÁCH GIAO DỊCH ENIGMA

Enigma hiện tạo một giao dịch ‘được che giấu’ cho mỗi lần chuyển.
Chúng tôi hiện đang tiến hành làm bản cập nhật cho framework Enigma sẽ cho phép nhiều giao dịch Enigma được kết hợp thành một siêu giao dịch Enigma. Điều này sẽ giúp nhiều giao dịch 'được che giấu' một cách hiệu quả và cung cấp khả năng ẩn danh lớn hơn cho người dùng Cloak. Việc mở rộng này sẽ cho phép người dùng chọn số lượng các giao dịch Enigma cùng hợp tác mà họ yêu cầu ngoài số lượng Cloakers.

Việc bổ sung này vẫn hoàn toàn phi tập trung, riêng tư và an toàn. Một cải tiến gửi Enigma khác hiện đang được Nhóm Cloak triển khai là khả năng 'che giấu' một lượng lớn Cloak bằng một loạt các giao dịch Enigma nhỏ hơn. Để đạt được điều này, người dùng sẽ chọn số lượng Cloak họ muốn gửi được che giấu đến một địa chỉ. CloakCoin sau đó sẽ làm việc ở nền tảng để tạo ra một số giao dịch Enigma nhỏ hơn với số lượng bằng nhau có thể được che giấu và gửi tới mạng Cloak trong một khoảng thời gian nhất định. Quy trình xử lý theo đợt này sẽ tương thích với các giao dịch Enigma 'kết hợp', cung cấp thêm khả năng bảo vệ che giấu cho việc chuyển tiền.

6. CÂU HỎI THƯỜNG GẶP

NHỮNG NGƯỜI CHE GIẤU HỖ TRỢ GIAO DỊCH ENIGMA NHƯ THẾ NÀO?

Những người che giấu cung cấp một hoặc nhiều đầu vào được sử dụng để ‘che giấu’ đầu vào từ người gửi. Người che giấu cũng cung cấp một loạt các địa chỉ trả lại để trả lại dữ liệu đầu vào của họ và cũng để thưởng cho người che giấu một khoản phí. Địa chỉ trả lại được chọn cẩn thận để ưu tiên địa chỉ hoạt động. Điều này gây khó khăn rất lớn cho bất cứ ai thực hiện phân tích blockchain để xác định đầu ra thực sự của một giao dịch Enigma. Hệ thống Enigma cũng sẽ kiểm tra địa chỉ đích để các đầu ra 'được che giấu' phản chiếu đầu ra thực càng chặt chẽ càng tốt.

GIAO DỊCH ENIGMA MẤT BAO LÂU ĐỂ HOÀN TẤT?

Các giao dịch Enigma hiện được tính toán mất một phút để hoàn thành. Các node Cloaking giúp 'che giấu' giao dịch Enigma sẽ dự trữ số tiền cần thiết cho đến khi giao dịch Enigma hoàn thành hoặc hết thời gian quy định. Trong trường hợp giao dịch Enigma đã hết hạn hoặc bị hủy, tiền được mở khóa cục bộ để tái sử dụng.

ENIGMA TÁC ĐỘNG STAKING NHƯ THẾ NÀO?

Bất kỳ coins nào được sử dụng trong giao dịch Enigma (với tư cách là Người gửi hoặc Người che giấu) sẽ có thiết lập lại coin-age của họ. Tuy nhiên, cần lưu ý rằng việc tham gia vào việc che giấu sẽ mang lại lợi nhuận cao hơn nhiều so với staking. Đội ngũ Cloak đang làm việc để sửa lại thuật toán Enigma cho bản phát hành hard-fork sắp tới (Enigma 1.1). Vui lòng xem Phần 5 - ‘Tương lai của Enigma – Hướng phát triển tiếp theo’ để biết thêm chi tiết.

TÔI CÓ CẦN MỘT SỐ TIỀN CLOAK NÀO TRONG VÍ CỦA MÌNH ĐỂ TRỞ THÀNH ENIGMA CLOAKER?

Bạn có thể cung cấp các dịch vụ che giấu bất kể số dư trong ví CloakCoin của bạn là bao nhiêu. Khi Enigma Cloaking được kích hoạt, CloakCoin sẽ dành một phần số dư của bạn để tham gia vào Enigma Cloaking, mà bạn sẽ kiếm được phần thưởng Cloaking. Số tiền dự trữ mặc định là ~50%, nhưng giá trị này có thể được người dùng điều chỉnh. Giá trị được chọn sẽ được chọn ngẫu nhiên để ngăn chặn việc liên kết thông báo Enigma bằng số dư Cloaking được quảng cáo.

Cần lưu ý rằng ví với số dư cao hơn có cơ hội cao hơn để được chọn làm Người che giấu vì chúng có nhiều khả năng có số dư Cloaking cần thiết hơn cho các giao dịch Enigma lớn hơn.

VIỆC NÀY BẢO VỆ CHỐNG LẠI TẤN CÔNG THEO THỜI GIAN NƠI MÀ AI ĐÓ TÌM KIẾM ĐẦU VÀO VÀ ĐẦU RA TƯƠNG TỰ TRÊN BLOCKCHAIN NHƯ THẾ NÀO?

Các giao dịch Enigma tập hợp các đầu ra và đảm bảo rằng có nhiều kết quả đầu ra phù hợp để 'che giấu' đầu ra của người nhận.

NGƯỜI KHỞI TẠO GIAO DỊCH ENIGMA CÓ THỂ ĐƯỢC XÁC ĐỊNH BẰNG CÁCH KIỂM TRA CHỮ KÝ ĐỂ XÁC ĐỊNH THỨ TỰ KÝ KHÔNG?

Không. Trong quá trình ký, thứ tự chữ ký của tập lệnh được chọn ngẫu nhiên khi kết hợp các chữ ký. Người gửi và người tham gia che giấu thực hiện việc này.

KẺ NGHE TRỘM CÓ THỂ GIÁM SÁT MẠNG LƯỚI ĐỂ XEM GIAO DỊCH ENIGMA SẮP ĐI RA ĐƯỢC ĐƯA LÊN MẠNG ĐỂ XÁC ĐỊNH NGƯỜI GỬI THỰC KHÔNG?

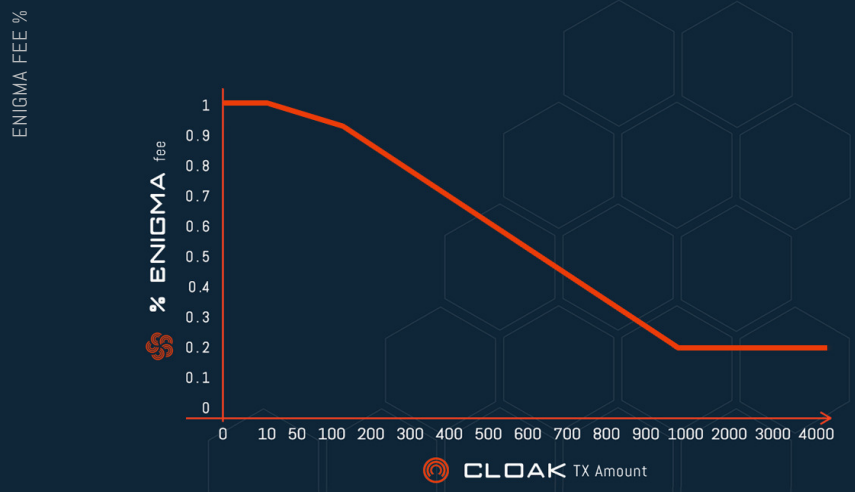
Không. Tất cả các bên gửi giao dịch Enigma vào mạng theo thứ tự ngẫu nhiên. Điều này làm giảm thiểu ngăn chặn các cuộc tấn công nghe trộm như vậy.

CHI PHÍ CHO MỘT GIAO DỊCH ENIGMA LÀ BAO NHIÊU?

1% ở 0 coin đến 0,2% từ 1.000 coin trở lên. Mức này được sử dụng để thưởng cho các node Enigma hỗ trợ che giấu giao dịch Enigma. Phí này sau đó được kết hợp với giao dịch và chia ra giữa những người che giấu. Nó không chỉ là phần thưởng cho người tham gia, mà còn được sử dụng để quyết định số lượng giao dịch khó không thể thực hiện được. Mỗi người tham gia nhận 80-120% của giao dịch Enigma được chia đều nhau.

PHÍ ENIGMA ĐƯỢC XÁC ĐỊNH NHƯ THẾ NÀO?

Phí Enigma % được tính trên mỗi giao dịch theo tỷ lệ như sau:



TX AMOUNT	ENIGMA FEE %	CLOAK FEE
0	1.00	0
10	0.992	0.0992
50	0.96	048
100	0.92	0.92
200	0.84	1.68
300	0.76	2.28
400	0.68	2.72
500	0.60	3.00
600	0.52	3.12
700	044	3.08
800	0.36	2.88
900	0.28	2.52
1000	0.20	2.00
2000	0.20	4.00
3000	0.20	6.00
4000	0.20	8.00

CLOAK TRANSACTION AMOUNT

ENIGMA CÓ YÊU CẦU HARD-FORK MẠNG LƯỚI CLOAK KHÔNG?

Không. Khách hàng cũ của CloakCoin sẽ xử lý các giao dịch Enigma mà không gặp vấn đề gì, nhưng họ sẽ không thể tạo ra chúng hoặc tham gia vào việc 'che giấu' chúng. Tuy nhiên, bản sửa đổi tiếp theo của Enigma sẽ yêu cầu hard-fork do thay đổi thuật toán Proof-of-Stake nền tảng và hỗ trợ cho script opcodes bổ sung cho các tính năng thị trường (chẳng hạn như Block Escrow).

SỐ LƯỢNG NGƯỜI CHE GIẤU TỐI ĐA CÓ THỂ HỖ TRỢ MỘT GIAO DỊCH ENIGMA LÀ BAO NHIÊU?

Số lượng tối đa Người che giấu mặc định là 25. Hệ thống Enigma linh hoạt và con số này có thể dễ dàng tăng lên.

ENIGMA BẢO VỆ CHỐNG LẠI 'NHỮNG NGƯỜI CÓ HÀNH VI XẤU' NHƯ THẾ NÀO?

Hệ thống Enigma có tính năng bảo vệ DDoS mở rộng cho các node 'danh sách đen' trong khoảng thời gian của phiên. Nếu một node Enigma liên tục từ chối ký, chúng sẽ bị loại trừ khỏi lời mời Enigma Cloaking cho phần còn lại của phiên hiện tại. Chúng tôi hiện đang nghiên cứu các phương pháp bổ sung để xử phạt thêm các node Enigma không hợp tác và có khả năng thực hiện một hệ thống yêu cầu Người che giấu ký một khoản phí có thể hoàn trả lại, không đáng kể, có thể được coi là hình phạt trong trường hợp một node cố gắng chặn một giao dịch Enigma bằng cách từ chối ký giao dịch cuối cùng. Cần lưu ý rằng trong khi các node độc hại có thể cố gắng cản trở giao dịch Enigma, chúng không thể ăn cắp hoặc có hành xử không phù hợp với bất kỳ khoản tiền nào.

GIAO DỊCH ENIGMA VÀ STEALTH ĐƯỢC PHÁT HIỆN/NHẬN NHƯ THẾ NÀO?

Tất cả các giao dịch đến đều được quét. Các giao dịch stealth được quét trước tiên (sử dụng pubkey tạm thời mặc định chứa trong đầu ra OP_RETURN TX ngẫu nhiên). Sau đó, các giao dịch Enigma sau đó được quét. Các giao dịch Enigma cũng sử dụng pubkey tạm thời tiêu chuẩn, nhưng các khoản thanh toán sử dụng một bước bổ sung liên quan đến một khóa được lấy từ đó tiếp theo. Các đầu ra Enigma được tạo ra bằng cách sử dụng một hàm băm của pubkey tạm thời, một hàm băm địa chỉ stealth và chỉ mục đầu ra.

Khi quét cho các giao dịch Enigma, các địa chỉ thanh toán zero-index được tạo cho mỗi địa chỉ stealth thuộc sở hữu [HASH (ephemeral_pubkey, hash_stealth_secret, 0)]. Nếu tìm thấy khớp với một zero-index của một địa chỉ stealth, địa chỉ bổ sung được tạo ra cho các chỉ mục còn lại [num_tx_outputs] và chúng được quét để phát hiện thanh toán. Xem FindEnigmaTransactions trong wallet.cpp để biết thêm thông tin.

Một phương pháp quét tương tự được sử dụng bởi Người che giấu trước khi ký một Enigma TX để đảm bảo rằng họ đang nhận được hoàn trả chính xác. Xem GetEnigma OutputsAmounts trong wallet.cpp để biết thêm thông tin.

7. THAM KHẢO

[01] http://bitcoin.org

[02] https://en.bitcoin.it/wiki/Category:Mixing Services

[03] https://wiki.openssl.org/index.php/Elliptic_Curve_Diffie_Hellman

[04] http://blog.ezyang.com/2012/07/secure-multiparty-bitcoin-anonymization

[05] https://bitcointalk.org/index.php?topic=279249.0
(CoinJoin: Bitcoin Privacy for the Real World)

[06] https://bitcointalk.org/index.php?topic=27787.0
(Proof of Stake Instead of Proof of Work)

[07] https://en.bitcoin.it/wiki/Proof_of_Stake

[08] https://en.bitcoin.it/wiki/Deterministic_wallet

[09] https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[10] http://www.onion-router.net

www.cloakcoin.com

https://chat.cloakcoin.com

www.twitter.com/CloakCoin