CLOAK

ENIGMA V2.1

Whitepaper (Aggiornato)

Febbraio 2018

ENIGMA

UN SISTEMA DI TRANSAZIONE PRIVATO,
SICURO E NON TRACCIABILE PER CLOAKCOIN

1. ABSTRACT

CloakCoin è una criptovaluta progettata per facilitare trasferimenti decentralizzati privati, sicuri e non tracciabili con Enigma.

Cloak è una moneta PoW/PoS (Proof of Work, Proof of Stake), che ora si trova nella fase Proof-of-Stake.

Enigma è il sistema di pagamento privato, sicuro e non tracciabile di CloakCoin, che costituisce la base per lo sviluppo futuro e fornisce il sottostante sistema di transazione per le applicazioni decentralizzate in esecuzione sulla rete CloakCoin.

La privacy oggi è forse più importante che mai. Il ritmo tonante del progresso tecnologico ha rapidamente allargato i nostri orizzonti e collegato il mondo come mai prima d'ora. Grazie all'introduzione di Bitcoin nel 2009, le criptovalute si stanno progressivamente spostando nel mainstream e sfruttando il potere della blockchain possiamo ora trasferire, in un istante, valuta digitale in modo sicuro in tutto il mondo.

Man mano che l'adozione delle criptovalute diventa più diffusa, l'aumento della regolamentazione è inevitabile. Resta da vedere quale forma prenderanno questi regolamenti, ma molti sono preoccupati che potrebbero essere eccessivamente draconiani e progettati per soffocare alcuni degli aspetti più libertari delle criptovalute.

ENIGMA

Enigma è di base un servizio di mescolamento, mixing, decentralizzato e off-blockchain che consente agli utenti della rete CloakCoin di trasmettere Cloak in privato e in sicurezza l'uno con l'altro. È stato progettato per garantire che il processo di mixing sia sicuro e non rintracciabile da osservatori di terze parti. Ciò garantisce che le monete Cloak di un utente siano mantenute sicure durante il trasferimento e che il mittente e il destinatario non possano essere associati in qualche modo. Le monete Cloak non vengono mai trasferite ad una parte intermediaria durante il Cloaking, quindi rimangono al sicuro. Abbiamo lavorato duramente anche per garantire che il sistema Enigma premiasse gli utenti che assistono nei trasferimenti di Cloaking e continueremo a migliorare il processo e a stimolare ulteriormente i partecipanti attivi. Chiunque disponga di monete Cloak può partecipare alle operazioni di Cloaking, lasciando il proprio portafoglio in esecuzione in modalità Staking/Cloaking si ha l'opportunità di assistere passivamente al Cloaking e guadagnare ricompense significative.

2. PANORAMICA ENIGMA V1.0

Enigma è la prima versione pubblica del sistema di pagamento privato, sicuro e non tracciabile di Cloak. Le transazioni Enigma sono "mascherate" (cloaked) da altri utenti, che ricevono una ricompensa per la loro assistenza. Gli altri utenti forniscono input e output alla transazione Enigma rendendo impossibile determinare la vera origine e destinazione del trasferimento cloak. Tutti i messaggi Enigma sulla rete sono sottoposti ad hash e crittografati per il destinatario utilizzando CloakShield per garantire la sicurezza e l'integrità dei dati. Si prega di consultare la Sezione 3 - "CloakShield" per maggiori dettagli.

2.1. IL PROCERSSO DI ENIGMA (PER I NODI ABILITATI DA ENIGMA)

ENIGMA ANNOUNCEMENTS

I nodi Enigma comunicano sulla rete Cloak e un nodo tiene traccia di altri nodi Enigma attivi. Enigma Announcement Broadcasts (Annunci di comunicazione di Enigma) avvisa gli altri nodi Enigma della nostra chiave di sessione pubblica e del saldo di cloaking corrente di Enigma.

RICHIESTE CLOAKING ENIGMA

Quando un utente desidera inviare una transazione Cloaked Enigma, vengono scelti una serie di nodi Enigma (con un saldo Enigma sufficientemente alto) e richiede la loro assistenza per il cloaking. Un nodo Enigma può scegliere di assistere nel cloaking e inviare una risposta di accettazione al richiedente per indicarlo. Se un nodo Enigma rifiuta di partecipare al cloaking o non risponde in modo tempestivo, viene scelto un nodo Enigma alternativo e contattato.

La protezione DDoS (distributed denial of service) metterà in black list tutti i nodi malfunzionanti per il resto della sessione. Un nodo è considerato malfatto se rifiuta ripetutamente di firmare una transazione Enigma o si rifiuta di inoltrare i messaggi Enigma. I cloaking nodes (nodi di mascheramento) Enigma utilizzano uno scambio di chiavi Elliptic Curve Diffie Hellman (ECDH) per ottenere una comunicazione criptata (shared secret) con il nodo di avvio di Enigma, che viene utilizzato per generare una chiave segreta condivisa per la crittografia simmetrica RSA-256 tra un nodo di cloaking e il nodo mittente.

ACCETTAZIONE ENIGMA CLOAKING

Quando un nodo Enigma accetta una richiesta di "cloaking", fornisce un elenco di input e output della transazione da utilizzare per la transazione Enigma. Gli importi di input forniti da un nodo di mascheramento (cloaking node) devono essere maggiori o uguali all'importo di invio Enigma (più le eventuali commissioni). Gli output sono accuratamente selezionati in modo che corrispondano il più fedelmente possibile alla transazione di Enigma. Se l'indirizzo di output di Enigma non è stato precedentemente utilizzato, un nuovo indirizzo di modifica viene generato dal "Cloaker". Se l'indirizzo di output di Enigma ha già ricevuto fondi, un indirizzo esistente con attività simili viene scelto dal "Cloaker" per restituire i fondi di input e ricevere la ricompensa per "cloaking" di Enigma.

LA TRANSAZIONE "CLOAKED" ENIGMA

Enigma Sender costruisce una transazione "mascherata" (Cloaked) utilizzando gli input e gli output forniti dai nodi Enigma Cloaker. Prima di mescolare tutti gli input e gli output delle transazioni per facilitare il "cloaking", Enigma Sender aggiunge quindi i propri input e output alla transazione. La transazione "occultata" viene quindi crittografata e inviata (utilizzando CloakShield) a ciascun Cloaker partecipante. I nodi dei Cloaker controllano la transazione per garantire che gli input e gli output forniti siano presenti nella transazione "occultata" e che uno o più dei loro output siano stati premiati con importi di commissione sufficienti.

Se i controlli delle transazioni vengono passati, la transazione viene firmata (SIGHASH_ ALL + SIGHASH_ANYONECANPAY), crittografata e inoltrata al mittente Enigma. Una volta che tutti gli Enigma Cloaker hanno firmato la transazione, Enigma Sender è pronto a confermare che la transazione firmata è valida e la firma. La transazione "occultata" è quindi pronta per essere inviata alla rete.

2.2.1. TRACKING ENIGMA CLOAKING NODES

I nodi Enigma abilitati sulla rete Cloak comunica gli annunci ad altri nodi. Questi annunci Enigma contengono l'ID ec-key pubblico del nodo e il saldo attualmente disponibile per le operazioni Enigma di cloaking. I nodi mantengono un elenco di altri nodi Enigma attivi sulla rete in modo che possano comunicare per scopi di cloaking. Gli ID dei nodi vengono generati su base di sessione per sessione; il riavvio del client aggiornerà l'ID corrente.

1. Ogni portafoglio all'avvio crea una coppia di chiavi pubblica/segreta (secp256k1) per la sessione.

2. Il portafoglio annuncia periodicamente la sua chiave pubblica e il saldo di Cloaking per la sessione ad altri nodi sulla rete Cloak.

3. I nodi tengono traccia di altri nodi Cloaking Enigma attivi e possono comunicare con loro direttamente o indirettamente (tramite CloakShield Onion Routing).

2.2.2. INIZIO DI UNA TRANSAZIONE ENIGMA

ALICE vuole inviare 10 CLOAK a BOB utilizzando 5 mixer node (nodi mescolatori).

1. Alice trasmette alla rete una richiesta Enigma contenente la sua chiave di sessione pubblica Enigma e la quantità di Cloak che desidera inviare. La sua richiesta viene instradata in modo sicuro attraverso una serie di 5 nodi Enigma per mascherare il creatore.

2. Catherine ha abilitato la modalità Cloaking e crea un canale sicuro crittografato CloakShield per comunicazioni sicure con Alice. Catherine quindi costruisce un pacchetto di risposta Enigma e lo invia in modo sicuro ad Alice. La risposta contiene un elenco di input e output di Catherine che Alice utilizzerà per "nascondere" (Cloak) la sua transazione.

3. Alice decodifica ed elabora la risposta di Enigma di Catherine e crea una transazione Enigma usando i propri input e output combinati con gli input e gli output di Catherine. Tutto questo è criptato e inviato a Catherine per la firma.

4. Catherine decripta la transazione Enigma ed esegue una serie di controlli di integrità sulla transazione per assicurare che gli input e gli output forniti da Alice siano stati correttamente utilizzati e che sia stata ricompensata sufficientemente. Se la transazione Enigma supera i test, Catherine la firma, la crittografa e la trasmette ad Alice.

5. Alice esegue ulteriori controlli sulla transazione firmata prima di firmarla lei stessa. La transazione viene quindi inviata alla rete (instradata in modo sicuro attraverso i nodi Enigma) per l'inclusione in un blocco.

6. Quando la transazione è finalizzata, Bob riceverà i fondi da Alice e Catherine riceverà una ricompensa 'Cloaking' per l'assistenza nella transazione Enigma.

7. A causa degli input ed output di Catherine che rispecchiano quelli di Alice, non è possibile accertare il vero mittente e destinatario della transazione Enigma.

ESEMPIO DI TRANSAZIONE ENIGMA

ALICE vuole inviare monete in modo anonimo a BOB.

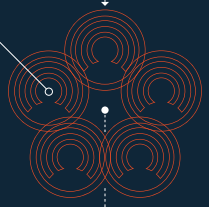
ALICE (−10.0992) CLOAK

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

Gli ENIGMA mixer node iniziano a comunicare.

CATHERINE

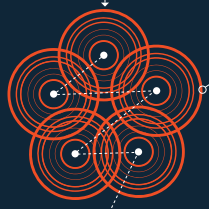
Ogni possessore di monete può segnalarsi come un Mixer Node, noto anche come "Cloaker".



Ogni partecipante rimane anonimo e comunica attraverso un canale crittografato.

Il portafoglio di ALICE è ora collegato ai mixer node.

Ogni mixer node aiuta ALICE mischiando la transazione.



Questa rete di nodi crea un'anonimizzazione decentralizzata simile all'Onion Routing TOR.

I Mixer node vengono ricompensati per effettuare il Cloaking della transazione di ALICE

(+0.0992) CLOAK

Una commissione lineare dallo 0,2% (>1000 monete) all'1% (0 monete) è condivisa tra tutti i Cloaker partecipanti.

Il sistema funziona perfettamente per garantire l'anonimato completo e la privacy totale.

BOB riceve quindi il pagamento crittografato di ALICE

BOB (+10) CLOAK

BOB riceve con successo 10 CLOAK in modo anonimo.

3. CLOAKSHIELD

CloakShield fornisce comunicazioni sicure tra i nodi sulla rete Cloak utilizzando la crittografia simmetrica RSA supportata da uno scambio di chiavi Elliptic Curve Diffie Hellman (ECDH). Ciò consente ai nodi di scambiare dati in modo sicuro, fornendo protezione dai ficcanaso (man in the middle, intermediario) e impostori (sybil attack). CloakShield è progettato per proteggere sia Enigma che le applicazioni CloakCoin decentralizzate e garantisce che i tuoi dati rimangano il più privati possibile.

CloakShield consente l'invio crittografato di dati a uno o più destinatari. Quando si invia a un singolo destinatario, il carico viene crittografato tramite RSA utilizzando il metodo di criptazione (shared secret) ECDH. Quando si invia a più destinatari, il carico viene crittografato utilizzando una chiave ad utilizzo unico e la chiave viene quindi crittografata per ciascun destinatario utilizzando il metodo ECDH/RSA.

GENERARE UNA CHIAVE DI CRITTOGRAFIA CONDIVISA

Affinché Alice e Bob possano comunicare in modo sicuro, devono concordare una chiave di crittografia condivisa. Per compiere questo CloakShield usa ECDH :

- Alice ha la chiave privata Enigma dA e la chiave pubblica Enigma QA=dAG (dove G è il generatore per la curva ellittica/elliptic-curve). Bob ha la chiave privata Enigma dB e la chiave pubblica Enigma QB=dBG.

- Alice ha la chiave pubblica Enigma dB di Bob dagli Enigma announcements che invia alla rete per annunciare la sua disponibilità per l'assistenza per il cloaking. Lei utilizza la sua chiave privata dA e la chiave pubblica QB di Bob per calcolare il metodo di criptazione "shared secret" dAQB=dAdBG (ECDH_compute_key in OpenSSL).

- Alice allora crea un hash SHA256 del "secret" e passa l'hash al metodo OpenSSLEVP_BytesToKey per ricavare una chiave di crittografia e IV (initialization vector), che verrà utilizzata per crittografare i dati per Bob (utilizzando la crittografia RSA simmetrica).

- Alice è ora in grado di creare messaggi protetti da CloakShield per Bob.

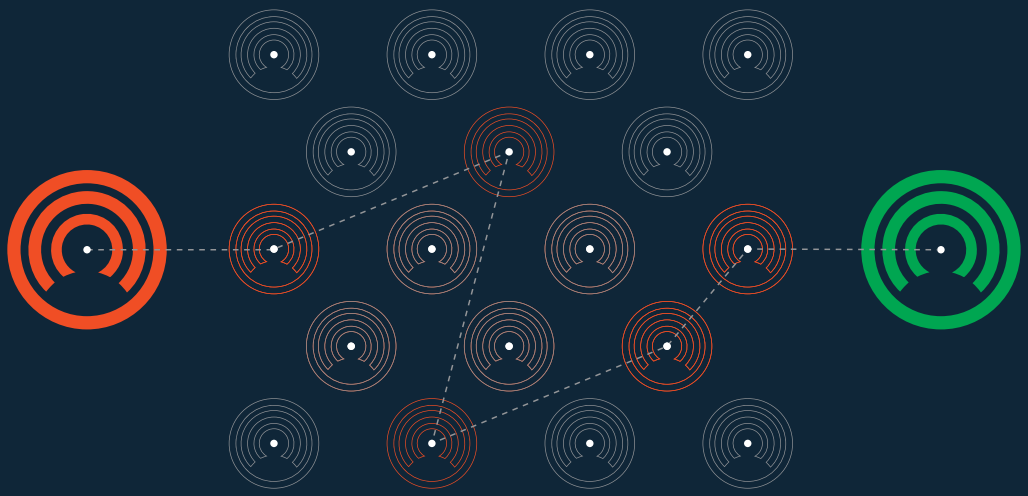
Quando Bob riceve un messaggio Cloak Shielded da Alice, legge la chiave pubblica di Alice dall'header del messaggio e genera la stessa chiave di "shared secret" di Alice, come per i passaggi precedenti (con la sua chiave segreta, anziché quella di Alice).

Il portafoglio Cloak mantiene un elenco di chiavi CloakShield attive e controllerà l'elenco per una chiave CloakShield esistente prima di generarne una.

CLOAKSHIELD DATA

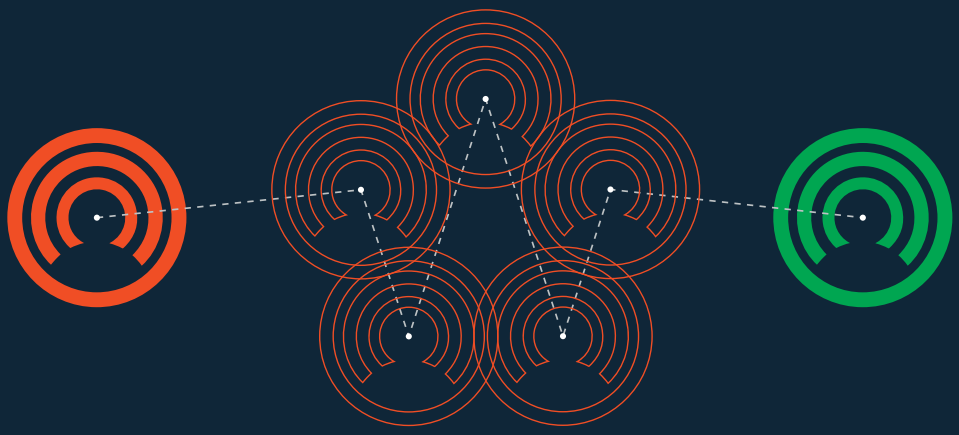
CloakShield consente a qualsiasi data object Cloak di essere serializzato e trasmesso in modo sicuro a uno o più destinatari. Un data packet-header di CloakShield contiene la chiave pubblica Enigma del mittente e gli hash delle chiavi pubbliche dei destinatari.

Gli Header di CloakShield contengono un hash di verifica, che viene generato utilizzando la chiave pubblica del mittente e raw unencrypted data. Questo hash viene verificato durante la decrittografia dei dati di CloakShield per garantire che le informazioni sul destinatario nell'header corrispondano alla chiave di crittografia e che i dati non siano stati modificati.



ONION ROUTING DI CLOAKSHIELD

L'Onion routing (routing della cipolla) è una tecnica (utilizzata da TOR) per la comunicazione anonima su una rete di computer. In una rete onion, i messaggi sono incapsulati in layer di crittografia, analoghi agli strati di una cipolla. I dati crittografati vengono trasmessi attraverso una serie di nodi di rete chiamati onion router, ognuno dei quali "sbuccia" un singolo livello, scoprendo la destinazione successiva dei dati. Quando il livello finale viene decifrato, il messaggio arriva a destinazione. Il mittente rimane anonimo perché ogni intermediario conosce solo la posizione dei nodi immediatamente precedenti e seguenti.



ONION ROUTING ANALOGY

L'aggiunta della funzionalità "onion routing" alla rete Enigma (utilizzando CloakShield) consente ai nodi di comunicare indirettamente per eludere l'analisi del traffico. Questo ostacola i tentativi di determinare quali nodi comunicano tra loro o quali nodi inviano le transazioni alla rete CloakCoin. Quando un nodo Enigma desidera comunicare con un altro nodo Enigma, seleziona un numero di altri nodi Enigma che fungono da ritrasmettitori per la comunicazione. Ogni layer crittografato può essere decodificato solo dal relè previsto [per il quale il layer specifico è stato crittografato]. Dopo la decodifica di un layer, il ritrasmettitore passa i dati al successivo nodo di inoltro. Questo instradamento continua fino a quando i dati raggiungono il destinatario previsto e tutti i layer sono stati decodificati a turno dai nodi di inoltro selezionati. A causa della natura autonoma della rete Enigma, i nodi di uscita non sono necessari e CloakShield garantisce che non vi sia il rischio che un nodo di trasmissione legga o altera i dati crittografati.

4. INDIRIZZI STEALTH

Cloak utilizza il sistema Enigma per facilitare le transazioni private/sicure.

CLOAKSHIELD - COMUNICAZIONE DA NODO A NODO

All'avvio, ciascun portafoglio Cloak genera una coppia di chiavi [NID_secp256k1] (Cloaking Encryption Key / CEK) per consentire loro di ricavare "secret" ad-hoc utilizzando ECDH con la loro chiave privata e la chiave pubblica del destinatario. Questa comunicazione costituisce la base su tutte le comunicazioni da nodo a nodo relative a Enigma. Vedi 'src/enigma /cloakshield.h/.cpp' per maggiori informazioni su questo. Questa comunicazione crittografata basata su ECDH viene utilizzata anche per gli onion-routed data, i dati trasmessi in modalità onion, che è gestita da CloakShield.

Quando l'onion routing è abilitato, il client tenterà di costruire un itinerario onion valido per i dati utilizzando l'elenco di peer Enigma di cui è a conoscenza. Il nodo potrebbe non avere una connessione diretta con i peer Enigma, ma ciò non è necessario in quanto i pacchetti CloakData (dati impacchettati per il routing con CloakShield) vengono trasmessi peer-to-peer. Un itinerario onion (onion route) consisterà generalmente in 3 percorsi distinti al nodo di destinazione, con 3 cambi di nodo per itinerario. Percorsi multipli sono utilizzati per far fronte a situazioni in cui un nodo di routing non fosse in linea.

I nodi inviano periodicamente un annuncio Enigma (src/enigma/enigmaann.h) ai peer per pubblicizzare i loro servizi per l'onion routing. Altri nodi sulla rete memorizzano gli annunci (finché non scadono o vengono sostituiti con un aggiornamento) e li usano per costruire onion routes.

ESEMPIO DI TRANSAZIONE INDIRIZZO STEALTH

Quando un nodo invia una transazione Enigma ad un indirizzo stealth, accade quanto segue:

1. Il mittente genera degli input per coprire l'importo inviato, la ricompensa Enigma e la commissione del network (1% per 0 monete fino allo 0,2% per 1000 monete e superiori).
2. Il mittente genera un oggetto CloakingRequest (contenente un nonce stealth unico per questa richiesta).
3. Il mittente genera da 2 a 4 indirizzi di pagamento stealth unici utilizzando gli indirizzi stealth dei destinatari e divide l'importo inviato a caso tra gli indirizzi.
4. Il mittente decide quanti partecipanti saranno utilizzati. possono essere scelti da 5 a 25 partecipanti (ogni partecipante riceve l'80-120% di una fee Enigma equamente divisa).
5. I mittente trasmette il CloakRequest via onion al network. La richiesta contiene l '"importo da inviare" in modo che i Cloakers sappiano quanto riservare.
6. Il Cloaker raccoglie la CloakRequest e decide di partecipare.
7. Il Cloaker fornisce X input al mittente e un indirizzo stealth e un hash nascosto, per il loro change (resto).
8. Il Cloaker invia CloakingAcceptResponse (risposta di cloaking accettato) al mittente. Questo contiene l'indirizzo stealth, nonce stealth e input della transazione.
9. Il mittente attende fino a quando un numero sufficiente di Cloaker ha accettato.
10. Il mittente crea la transazione Enigma utilizzando i propri input e gli input dei Cloaker. Gli input sono mescolati.
11. Il mittente crea gli output della transazione per tutti i Cloaker. Gli output sono l'importo della transazione più le commissioni che sono casualmente divise da 2 a 4 volte per partecipante. Questo assegna anche la ricompensa di cloaking ai Cloakers.

12. Il mittente assegna un indirizzo unico stealth per ogni output.

13. Il mittente calcola la commissione di rete dalla dimensione della transazione risultante che viene poi aggiunta alla transazione.

14. Il mittente invia la transazione Enigma ai Cloakers per la firma.
15. I Cloakers controllano la transazione per assicurarsi che i loro input siano presenti e corretti e che ci siano indirizzi di pagamento ad uso unico collegati ad uno degli indirizzi stealth con un pagamento che superi l'importo dell'input.

16. I Cloaker firmano o rifiutano la transazione e inviano le firme al Mittente.
17. Il mittente confronta le firme e trasmette alla rete la transazione finalizzata e firmata.

18. I nodi analizzano le transazioni in entrata per pagamenti stealth e pagamenti Enigma e rilevano eventuali pagamenti o "change". Coppie di chiavi e indirizzi vengono generati per qualsiasi pagamento corrispondente e le chiavi/gli indirizzi generati vengono salvati nel wallet locale.

5. IL FUTURO DI ENIGMA – ULTERIORI SVILUPPI

Enigma costituisce il nucleo di CloakCoin e continuerà ad essere sviluppato e migliorato man mano che avanziamo con CloakCoin. Ecco alcune delle funzionalità pianificate per le future revisioni:

MIGLIOR ALGORITMO PROOF-OF-STAKE

Il Proof of Stake (PoS) è un metodo per proteggere una rete di criptovaluta che si basa sugli utenti che mostrano la proprietà delle monete per firmare i blocchi.

Nel lungo periodo, la probabilità di firmare blocchi è proporzionale alla quantità di monete possedute, un individuo che possiede l'1% della quantità totale di monete sarà in grado di firmare l'1% di tutti i blocchi proof of stake. Rispetto all'approccio "proof of work", il proof of stake richiede una potenza di calcolo significativamente inferiore e quindi un minore consumo di energia.

COIN AGE E PROOF-OF-STAKE LINEARE

Fondamentale per la maggior parte delle implementazioni di Proof of Stake, inclusa quella di CloakCoin, è il concetto di Coin Age (età della moneta). In sostanza, si tratta di una misura che determina la durata del possesso di una moneta senza spenderle o spostarle. Dal momento in cui una transazione viene completata, le monete che facevano parte di quella transazione iniziano ad accumulare Coin Age (che inizia da zero). Nella sua forma più semplice, intitolata "linear coin age", le monete accumulano un minuto/ora/giorno/anno di Coin Age ogni minuto/ora/giorno/anno di età. Ad esempio, una persona che detiene 365 monete per 100 giorni accumula 36.500 "coin days"(monete giornaliere), o circa 100 "coin years" (monete annuali) (Un "coin year" è definito per tenere conto degli anni bisestili, e quindi non è esattamente 365 giorni, ma ~ 365,24 giorni).

I design di proof-of-stake lineari hanno attirato critiche in relazione alla Coin Age. Molti sostengono che la Proof-of-Stake lineare incoraggi l'accumulo di monete (che può avere un effetto dannoso sul commercio e sul volume di trasferimento). Un'altra valida lamentela contro il Proof-of-Stake lineare riguarda l'effetto che può avere sulla sicurezza della rete. Spesso le implementazioni lineari di Proof-of-Stake soffrono del fatto che gli utenti si collegano periodicamente alla rete Cloak per effettuare lo stake delle monete per poi disconnettersi una volta che l'intera Coin Age è stata distrutta. L'utente attende quindi che la Coin Age sia ripristinata prima di ripetere il processo connect-stake-disconnect. Ciò non fornisce la migliore sicurezza per la rete e un algoritmo Proof of Stake che premia lo staking frequente o costante sarebbe più vantaggioso per CloakCoin e le relative valute Proof-of-Stake.

Per garantire che i Cloaker di Enigma vengano ricompensati nel modo più ampio possibile, Coin Age deve essere rimossa dall'algoritmo Proof of Stake di CloakCoin. Ciò assicurerebbe che i Cloaker ricevano sia la ricompensa per lo staking sia qualsiasi ricompensa per l'Enigma Cloaking. L'incorporazione aggiuntiva di una componente di velocità nel calcolo delle ricompense di staking darebbe ulteriori premi ai nodi attivi di Cloaking Enigma, incoraggiando gli utenti a partecipare a Enigma Cloaking per aumentare ulteriormente il loro guadagni oltre ai premi Cloaking guadagnati.

Oltre a fornire maggiori ricompense agli utenti che partecipano attivamente, un algoritmo Proof-of-Stake migliorato fornisce anche i miglioramenti menzionati prima alla sicurezza della rete.

COMBINAZIONE E DIVISIONE DELLE TRANSAZIONI ENIGMA

Enigma crea attualmente una singola transazione "Cloaked" per trasferimento. Al momento stiamo lavorando ad un aggiornamento del framework Enigma che consentirà di combinare più transazioni Enigma in una super-transazione Enigma. Ciò conterrà effettivamente più transazioni "nascoste" e fornirà un anonimato ancora maggiore agli utenti Cloak. Questa estensione consentirà agli utenti di selezionare il numero di transazioni Enigma cooperative che richiedono oltre al numero dei Cloaker.

Questa aggiunta ovviamente rimane completamente decentralizzata, privata e sicura. Un altro Enigma potenziamento per gli invii attualmente messo a punto dal Cloak Team è la capacità di effettuare il "Cloak" di una grande quantità di Cloak come una serie di piccole transazioni Enigma. Per raggiungere questo obiettivo, un utente sceglie la quantità di Cloak che vorrebbe inviare Cloaked ad un indirizzo. CloakCoin quindi lavorerebbe in background per creare una serie di piccole transazioni Enigma di un importo pari, che possono essere mascherate e inviate alla rete Cloak per un determinato periodo di tempo. Questo processo di batching sarà compatibile con le transazioni "combinate" di Enigma, fornendo ulteriore protezione di Cloaking per i trasferimenti.

6. DOMANDE FREQUENTI

D. COME FANNO I CLOAKER AD ASSISTERE UNA TRANSAZIONE ENIGMA?

I Cloaker forniscono uno o più input che sono usati per "nascondere" l'input dal mittente. I Cloaker forniscono anche una serie di indirizzi di ritorno che restituiscono il loro contributo e premiano il Cloaker con una quota. Gli indirizzi di restituzione sono scelti con attenzione per dare la priorità agli indirizzi con attività. Ciò rende molto più difficile per chiunque esegua l'analisi blockchain individuare il vero output di una transazione Enigma. Il sistema Enigma controllerà anche l'indirizzo di destinazione in modo che gli output "cloaked" rispecchino il vero output il più verosimilmente possibile.

D. QUANTO TEMPO NECESSITA UNA TRANSAZIONE ENGIMA PER ESSERE COMPLETA?

Le transazioni Enigma hanno attualmente fino ad un minuto per completarsi. I nodi di cloaking che aiutano ad effettuare il "Cloak" ad una transazione Enigma riserveranno i fondi necessari fino al completamento della transazione Enigma o alla scadenza del tempo assegnato. Nel caso di una transazione Enigma scaduta o interrotta, i fondi vengono sbloccati localmente per il riutilizzo.

D. IN CHE MODO ENIGMA INFLUISCE SULLO STAKING?

Qualsiasi moneta utilizzata in una transazione Enigma (come Sender/ mittente o Cloaker) avrà il proprio coin-age resettato. Va notato, tuttavia, che la partecipazione al Cloaking dovrebbe fornire un rendimento molto più alto dello staking. Il Cloak Team sta lavorando per rivedere l'algoritmo Enigma per la futura release dell'hard-fork (Enigma 1.1). Si prega di consultare la Sezione 5 - "Il Futuro di Enigma - Ulteriori sviluppi" per maggiori dettagli.

D. HO BISOGNO DI UNA CERTA QUANTITÀ DI CLOAK NEL SALDO DEL MIO PORTAFOGLIO PER ESSERE UN CLOAKER ENIGMA?

Puoi Puoi offrire i tuoi servizi per Cloaking indipendentemente dal saldo nel tuo portafoglio CloakCoin. Quando Enigma Cloaking è abilitato, CloakCoin riserva una parte del tuo saldo per la partecipazione a Enigma Cloaking, per il quale otterrai una ricompensa Cloaking. L'importo di riserva predefinito è ~ 50%, ma questo valore può essere regolato dall'utente. Il valore scelto sarà randomizzato al fine di prevenire il collegamento degli annunci Enigma con il saldo Cloaking pubblicizzato.

Va notato che i portafogli con un saldo più alto hanno una maggiore possibilità di essere scelti come Cloaker in quanto sono più propensi a possedere il saldo Cloaking necessario per le transazioni Enigma più grandi.

Q. COME PROTEGGE QUESTO CONTRO UN "TIME BASED ATTACK" DOVE QUALCUNO ESAMINA LA BLOCKCHAIN IN CERCA DI INPUTS E OUTPUTS IDENTICI?

Le transazioni Enigma raggruppano gli output ed è garantino che abbiano più output corrispondenti per effettuare il "cloak" dell'output del destinatario.

D. PUÒ IL CREATORE DI UNA TRANSAZIONE ENIGMA ESSERE DETERMINATO ESAMINANDO LA FIRMA DELLO SCRIPT PER STABILIRE L'ORDINE DELLE FIRME?

No. Durante la procedura di firma, l'ordine della firma dello script è casuale quando si combinano le firme. Il mittente ed i Cloakers seguono questo principio.

D. PUÒ UNO SPIONE DETERMINARE IL MITTENTE REALE MONITORANDO LA RETE IN CERCA DI TRANSAZIONI ENGIMA USCENTI?

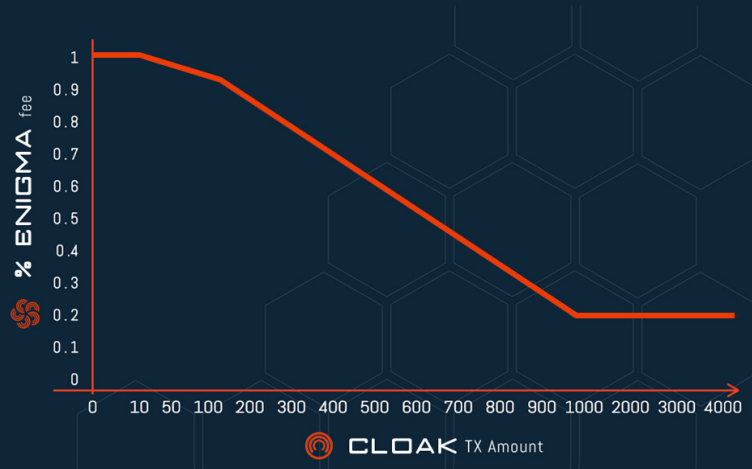
No. Tutte le parti inviano in un ordine casuale una transazione Enigma alla rete. Ciò fornisce una mitigazione contro tali attacchi di intercettazione.

D. QUAL È LA TASSA DI COMMISSIONE PER UNA TRANSAZIONE ENIGMA?

1% per 0 monete fino allo 0,2% per 1000 monete e superiori. Viene utilizzata per ricompensare i nodi Enigma che assistono con il cloaking una transazione Enigma. La tassa viene quindi mescolata con la transazione e divisa tra i cloaker. Non è solo una ricompensa per i partecipanti, ma viene utilizzata per aiutare a rendere la determinazione dell'importo della transazione quasi impossibile. Ogni partecipante riceve l'80-120% di una transazione di enigma suddivisa in parti uguali.

D. COME È DETERMINATA LA COMMISSIONE DI ENIGMA?

La percentuale della commissione di Enigma viene addebitata per transazione basata su questi tassi:



IMPORTO TX	COMM.ENIGMA	COMM.CLOAK
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

D. ENIGMA RICHIEDE UN HARD-FORK DELLA RETE CLOAK?

No. I vecchi client CloakCoin gestiranno le transazioni Enigma senza problemi, ma non saranno in grado di crearli o partecipare al "cloaking". La prossima revisione di Enigma, tuttavia, richiederà un hard-fork a causa di modifiche all'algoritmo Proof-of-Stake sottostante e supporto per ulteriori script opcode per le funzionalità di mercato (come Block Escrow).

D. QUAL È IL NUMERO MASSIMO DI CLOAKER CHE POSSONO ASSISTERE IN UNA TRANSAZIONE ENIGMA?

Il numero massimo di Cloaker è fissato a 25. Il sistema Enigma è flessibile e questo numero può essere facilmente esteso.

D. COME PROTEGGE ENIGMA DAI 'MALINTENZIONATI'?

Il sistema Enigma offre una protezione DDoS estesa per inserire i nodi nella "blacklist" per la durata di una sessione. Se un nodo Enigma rifiuta ripetutamente di firmare, saranno esclusi dagli inviti di Cloaking di Enigma per il resto della sessione corrente. Attualmente stiamo ricercando ulteriori metodologie per penalizzare ulteriormente i nodi non cooperativi di Enigma, probabilmente implementeremo un sistema che richieda ai Cloaker una commissione nominale rimborsabile che potrebbe essere richiesta come penalità nei casi in cui un nodo tenta di bloccare una transazione Enigma, rifiutandosi di firmare la transazione finalizzata. Va notato che mentre i nodi malevoli possono tentare di ostacolare una transazione Enigma, non sono in grado di sottrarre o di appropriarsi indebitatamente dei fondi.

D. COME SONO RILEVATE/RICEVUTE LE TRANSAZIONI STEALTH ED ENIGMA?

Tutte le transazioni in entrata sono scansionate. Per prima cosa vengono scansionate le transazioni Stealth (utilizzando la pubkey temporanea/ ephemeral predefinita contenuta in un output casuale TX OP_RETURN). Dopo questo, le transazioni Enigma vengono quindi scansionate. Anche le transazioni di Enigma utilizzano la pubkey standard temporanea , ma i pagamenti utilizzano un passaggio aggiuntivo che coinvolge un'altra chiave derivata. Gli output di Enigma sono generati usando un hash della pubkey temporanea, un hash dell'indirizzo di stealth privato e l'index dell'output.

Quando si esegue la scansione delle transazioni Enigma, vengono generati gli indirizzi di pagamento con indice zero per ciascun indirizzo stealth di proprietà [HASH (ephemeral_pubkey, hash_stealth_secret, 0)]. Se viene trovata una corrispondenza per l'indice zero di un indirizzo stealth, vengono generati ulteriori indirizzi per gli indici rimanenti [num_tx_outputs] e questi vengono scansionati per rilevare i pagamenti. Vedi FindEnigmaTransactions in wallet.cpp per maggiori informazioni.

Un metodo di scansione simile viene utilizzato dai Cloaker prima di firmare una transazione Enigma per garantire che vengano rimborsati correttamente. Vedi GetEnigmaOutputsAmounts in wallet.cpp per maggiori informazioni.

7. RIFERIMENTI

[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