CLOAK

ENIGMA V2.1

Λευκή Βίβλος (Αναθεωρημένη)

Φεβρουάριος 2018

ENIGMA

ΕΝΑ ΙΔΙΩΤΙΚΟ, ΑΣΦΑΛΕΣ ΚΑΙ ΜΗ ΑΝΙΧΝΕΥΣΙΜΟ ΣΥΣΤΗΜΑ ΣΥΝΑΛΛΑΓΩΝ ΓΙΑ ΤΟ CLOAKCOIN

1. ΣΥΝΟΨΗ

Το CloakCoin είναι ένα κρυπτονόμισμα που έχει σχεδιαστεί για να διευκολύνει τις ιδιωτικές, ασφαλείς και μη ανιχνεύσιμες αποκεντρωμένες μεταφορές με το Enigma.

Το Cloak είναι ένα διπλό PoW/PoS (Proof of Work, Proof of Stake) νόμισμα, που είναι τώρα στο στάδιο του Proof-of-Stake (τόκων).

Το Enigma είναι το ιδιωτικό, ασφαλές και μη ανιχνεύσιμο σύστημα συναλλαγών του Cloakcoin, που αποτελεί τη βάση της μελλοντικής ανάπτυξης και παρέχει το υποκείμενο σύστημα συναλλαγών για τις αποκεντρωμένες εφαρμογές που εκτελούνται στο δίκτυο του CloakCoin.

Η ιδιωτικότητα σήμερα είναι ίσως πιο σημαντική από ποτέ. Ο βροντερός ρυθμός της τεχνολογικής προόδου έχει διευρύνει γρήγορα τους ορίζοντές μας και συνέδεσε τον κόσμο όπως ποτέ άλλοτε. Χάρη στην εισαγωγή του Bitcoin το 2009, τα κρυπτονομίσματα αρχίζουν σταθερά να γίνονται κυρίαρχα και τώρα μπορούμε να μεταφέρουμε τα ψηφιακά νομίσματα με ασφάλεια σε ολόκληρο τον πλανήτη σε μια στιγμή, χρησιμοποιώντας τη δύναμη του blockchain.

Καθώς η υιοθέτηση των κρυπτονομισμάτων γίνεται πιο διαδεδομένη, η αυξημένη ρύθμιση είναι αναπόφευκτη. Παραμένει να δούμε ποια μορφή θα λάβει αυτός ο κανονισμός, αλλά πολλοί ανησυχούν ότι μπορεί να είναι υπερβολικά δρακόντειο και να σχεδιαστεί για να καταπνίξει κάποιες από τις πιο φιλελεύθερες πτυχές των κρυπτονομισμάτων.

ENIGMA

Το Enigma είναι στην καρδιά του μια αποκεντρωμένη, off-blockchain υπηρεσία ανάμειξης η οποία επιτρέπει στους χρήστες του δικτύου CloakCoin να μεταδίδουν τα Cloak ιδιωτικά και με ασφάλεια ο ένας στον άλλο. Έχει σχεδιαστεί για να διασφαλίζει ότι η διαδικασία ανάμειξης είναι τόσο ασφαλής όσο και μη ανιχνεύσιμη από τρίτους. Αυτό εξασφαλίζει ότι τα νομίσματα Cloak του χρήστη διατηρούνται ασφαλή κατά τη διάρκεια της μεταφοράς και ότι ο αποστολέας και ο δέκτης δεν μπορούν να συσχετιστούν. Τα νομίσματα Cloak δεν μεταφέρονται ποτέ σε ένα ενδιάμεσο μέρος κατά τη διάρκεια του Cloaking, έτσι τα νομίσματα παραμένουν ασφαλή. Εργαζόμαστε επίσης σκληρά για να διασφαλίσουμε ότι το σύστημα Enigma επιβραβεύει τους χρήστες που βοηθούν στις μεταφορές Cloaking και θα συνεχίσει να βελτιώνετε η διαδικασία για να ενθαρρύνει περαιτέρω τους ενεργούς συμμετέχοντες. Μπορεί να συμμετάσχει οποιοσδήποτε με νομίσματα Cloak στην λειτουργία Cloaking, η οποία τους επιτρέπει να αφήνουν το πορτοφόλι τους σε λειτουργία Staking / Cloaking για να τους επιτρέψει να βοηθήσουν παθητικά στο Cloaking και να κερδίσουν σημαντικές ανταμοιβές.

2. ΕΠΙΣΚΟΠΗΣΗ ENIGMA V1.0

Το Enigma είναι η πρώτη δημόσια προσέγγιση του ιδιωτικού, ασφαλούς και μη ανιχνεύσιμου συστήματος πληρωμών. Οι συναλλαγές με το ENIGMA είναι «κρυμμένες» από άλλους χρήστες, οι οποίοι λαμβάνουν ανταμοιβή για τη συνδρομή τους. Οι άλλοι χρήστες παρέχουν εισροές και εκροές στη συναλλαγή Enigma, καθιστώντας αδύνατον να προσδιοριστεί η πραγματική πηγή και ο προορισμός της μεταφοράς των Cloak. Όλα τα μηνύματα του Enigma στο δίκτυο είναι κατακερματισμένα και κρυπτογραφημένα για τον παραλήπτη χρησιμοποιώντας το CloakShield για να διασφαλιστεί η ασφάλεια και η ακεραιότητα των δεδομένων. Ανατρέξτε στην Ενότητα 3 - 'CloakShield' για περισσότερες λεπτομέρειες.

2.1. Η διαδικασία ENIGMA (Για ενεργοποιημένους κόμβους ENIGMA)

ΑΝΑΚΟΙΝΩΣΕΙΣ ENIGMA

Οι κόμβοι του Enigma επικοινωνούν μέσω του δικτύου Cloak και ένας κόμβος παρακολουθεί άλλους ενεργούς κόμβους Enigma. Η Ανακοίνωση Enigma αναμεταδίδει προειδοποίηση σε άλλους κόμβους Enigma του δημόσιου κλειδιού συνεδρίας και του τρέχοντος υπολοίπου του Enigma cloaking.

ΑΙΤΗΜΑ ΑΠΟΚΡΥΨΗΣ ENIGMA

Όταν ένας χρήστης επιθυμεί να στείλει μια κρυφή συναλλαγή Enigma, εκλέγει μία σειρά κόμβων Enigma (με αρκετά υψηλό ισοζύγιο Enigma) και ζητά τη βοήθειά τους στην απόκρυψη. Ένας κόμβος Enigma μπορεί να επιλέξει να βοηθήσει στην απόκρυψη στέλνοντας μια απάντηση αποδοχής στον αιτούντα για να το υποδείξει. Εάν ένας κόμβος του Enigma αρνείται να συμμετάσχει στην απόκρυψη ή δεν ανταποκρίνεται έγκαιρα, ένας εναλλακτικός κόμβος Enigma εκλέγεται και επικοινωνεί.

Η προστασία DDoS (κατανεμημένη άρνηση εξυπηρέτησης) θα βάλει σε μαύρη λίστα τους ενοχλητικούς κόμβους για το υπόλοιπο της περιόδου σύνδεσης. Ένας κόμβος θεωρείται ότι έχει κακή συμπεριφορά αν αρνείται επανειλημμένα να υπογράψει μια συναλλαγή Enigma ή αρνείται να μεταδώσει μηνύματα Enigma. Οι κόμβοι απόκρυψης του Enigma χρησιμοποιούν ένα κλειδί ανταλλαγής Elliptic Curve Diffie Hellman (ECDH) για να αντλήσουν ένα κοινό μυστικό με τον κόμβο εκκίνησης Enigma, ο οποίος χρησιμοποιείται για τη δημιουργία μυστικού κλειδιού για συμμετρική κρυπτογράφηση δεδομένων RSA-256 μεταξύ ενός κόμβου απόκρυψης και του κόμβου του αποστολέα.

ΑΠΟΔΟΧΗ ΑΠΟΚΡΥΨΗΣ ENIGMA

Όταν ένας κόμβος Enigma δέχεται ένα αίτημα "απόκρυψης", παρέχει μια λίστα εισροών και εκροών συναλλαγής που θα χρησιμοποιηθούν για τη συναλλαγή Enigma. Τα ποσά εισόδου που παρέχονται από έναν κόμβο απόκρυψης πρέπει να είναι μεγαλύτερα ή ίσα με το ποσό αποστολής του Enigma (συν τυχόν χρεώσεις). Οι εκροές είναι προσεκτικά επιλεγμένες ότι ταιριάζουν όσο το δυνατόν περισσότερο με την πραγματική απόδοση της συναλλαγής Enigma. Εάν η διεύθυνση εκροών Enigma δεν έχει χρησιμοποιηθεί προηγουμένως, δημιουργείται μια νέα διεύθυνση αλλαγής από τον "Cloaker". Εάν η διεύθυνση εκροών Enigma έχει λάβει προηγουμένως χρήματα, μια ήδη υπάρχουσα διεύθυνση με παρόμοια δραστηριότητα επιλέγεται από τον Cloaker για να επιστρέψει τα κεφάλαια εισροών και να λάβει την ανταμοιβή 'απόκρυψης' Enigma.

Η 'ΚΡΥΦΗ' ΣΥΝΑΛΛΑΓΗ ENIGMA

Ο αποστολέας Enigma δημιουργεί μια ‘κρυφή’ συναλλαγή χρησιμοποιώντας τις εισροές και εκροές που παρέχονται από τους κόμβους Enigma Cloaker. Στη συνέχεια ο αποστολέας Enigma προσθέτει τις δικές του εισροές και εκροές στη συναλλαγή πριν από την ανακατάταξη όλων των συναλλαγών εισροών και εκροών για τη διευκόλυνση της «απόκρυψης». Η ‘κρυφή’ συναλλαγή κρυπτογραφείται και αποστέλλεται (χρησιμοποιώντας το CloakShield) σε κάθε ένα συμμετέχοντα Cloaker. Οι κόμβοι των Cloaker ελέγχουν τη συναλλαγή για να εξασφαλίσουν ότι οι εισροές και οι εκροές που παρείχαν είναι παρόντες στη συναλλαγή «cloaked» και ότι ένα ή περισσότερα από τα αποτελέσματά τους έχουν επίσης επιβραβευτεί με επαρκείς χρεώσεις.

Εάν περάσουν οι έλεγχοι συναλλαγών, η συναλλαγή υπογράφεται (SIGHASH_ ALL + SIGHASH_ANYONECANPAY), κρυπτογραφείται και μεταφέρεται ξανά στον αποστολέα Enigma. Αφού όλοι οι Enigma Cloakers έχουν υπογράψει τη συναλλαγή, ο αποστολέας Enigma επιβεβαιώνει ότι η υπογεγραμμένη συναλλαγή είναι έγκυρη και την υπογράφει. Τότε η 'Κρυφή' συναλλαγή είναι έτοιμη για υποβολή στο δίκτυο.

2.2.1. ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΤΩΝ ΚΟΜΒΩΝ ΑΠΟΚΡΥΨΗΣ ENIGMA

Το Enigma ενεργοποιεί τους κόμβους στο δίκτυο Cloak και αναμεταδίδει ανακοινώσεις στους άλλους κόμβους. Αυτές οι ανακοινώσεις Enigma περιέχουν το κοινό αναγνωριστικό ec-key του κόμβου και το τρέχον διαθέσιμο υπόλοιπο για τις εργασίες απόκρυψης του Enigma. Οι κόμβοι διατηρούν μια λίστα με άλλους ενεργούς κόμβους του Enigma στο δίκτυο, ώστε να μπορούν να επικοινωνούν για σκοπούς απόκρυψης. Οι ταυτότητες των κόμβων παράγονται με βάση την περίοδο σύνδεσης. η επανεκκίνηση του προγράμματος θα ανανεώσει την τρέχουσα ταυτότητα.

1. Κάθε πορτοφόλι δημιουργεί ένα ζευγάρι κλειδιών δημόσιο / μυστικό (secp256k1) για την περίοδο λειτουργίας κατά την εκκίνηση.

2. Το πορτοφόλι ανακοινώνει το δημόσιο κλειδί του και το υπόλοιπο του Cloaking για την περίοδο λειτουργίας σε άλλους κόμβους του δικτύου Cloak.

3. Οι κόμβοι παρακολουθούν άλλους ενεργούς κόμβους απόκρυψης Enigma και μπορούν να επικοινωνήσουν μαζί τους άμεσα ή έμμεσα (μέσω του CloakShield Onion Routing).

2.2.2. ΕΝΑΡΞΗ ΜΙΑΣ ΣΥΝΑΛΛΑΓΗΣ ENIGMA

Η ALICE επιθυμεί να στείλει 10 CLOAK στον BOB χρησιμοποιώντας 5 κόμβους ανάμειξης.

1. Η Alice μεταδίδει ένα αίτημα Enigma στο δίκτυο, που περιέχει το δημόσιο κλειδί της συνεδρίας Enigma και το ποσό του Cloak που επιθυμεί να στείλει. Το αίτημά της δρομολογείται με ασφάλεια μέσω μιας σειράς από πέντε κόμβους Enigma για να καλύψει τον εντολέα.

2. Η Catherine έχει ενεργοποιημένη τη λειτουργία "Απόκρυψης" και δημιουργεί ένα ασφαλές κανάλι κρυπτογράφησης CloakShield για ασφαλή επικοινωνία με την Alice. Έπειτα η Catherine κατασκευάζει ένα πακέτο απάντησης Enigma και το στέλνει με ασφάλεια στην Alice. Η απάντηση περιέχει μια λίστα με εισροών και εκροών της Catherine που η Alice θα χρησιμοποιήσει για να «κρύψει» τη συναλλαγή της.

3. Η Alice αποκρυπτογραφεί και επεξεργάζεται την ανταπόκριση του Enigma της Catherine και δημιουργεί μια συναλλαγή Enigma χρησιμοποιώντας τις δικές της εισροές και εκροές που αναμιγνύονται με τις εισροές και εκροές της Catherine. Αυτό είναι κρυπτογραφημένο και αποστέλλεται στην Catherine για υπογραφή.

4. Η Catherine αποκρυπτογραφεί τη συναλλαγή Enigma και εκτελεί έναν αριθμό ελέγχων ακεραιότητας της συναλλαγής για να διασφαλίσει ότι οι εισροές και οι εκροές που παρέχει έχουν χρησιμοποιηθεί σωστά και ότι έχει ανταμειφθεί επαρκώς. Εάν η συναλλαγή Enigma περάσει τις δοκιμές, η Catherine την υπογράφει, την κρυπτογραφεί και την μεταδίδει στην Alice.

5. Η Alice πραγματοποιεί περαιτέρω ελέγχους στην υπογεγραμμένη συναλλαγή πριν υπογράψει και η ίδια. Στη συνέχεια, η συναλλαγή υποβάλλεται στο δίκτυο (δρομολογείται με ασφάλεια μέσω κόμβων Enigma) για να συμπεριληφθεί σε ένα μπλοκ.

6. Όταν ολοκληρωθεί η συναλλαγή, ο Bob θα λάβει τα χρήματα από την Alice και η Catherine θα λάβει μια ανταμοιβή "Απόκρυψης" για την βοήθεια που παρείχε στην συναλλαγή Enigma.

7. Λόγω των εισροών και των εκροών της Catherine που αντικατοπτρίζουν την Alice, δεν είναι δυνατόν να εξακριβωθεί ο πραγματικός αποστολέας και αποδέκτης της συναλλαγής Enigma.

ΠΑΡΑΔΕΙΓΜΑ ΣΥΝΑΛΛΑΓΗΣ ENIGMA

Η Alice θέλει να στείλει νομίσματα ανώνυμα στον BOB.

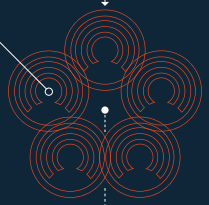
ALICE (−10.0992) CLOAK

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

Οι κόμβοι ανάμιξης ENIGMA αρχίζουν να επικοινωνούν.

CATHERINE

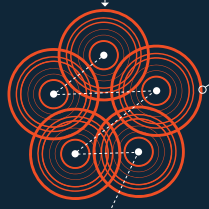
Κάθε κάτοχος νομισμάτων μπορεί να αναγγελθεί ως Κόμβος Μίξης, γνωστός και ως "Cloaker".



Κάθε συμμετέχων παραμένει ανώνυμος και επικοινωνεί μέσω κρυπτογραφημένου καναλιού.

Το πορτοφόλι της ALICE είναι τώρα συνδεδεμένο με κόμβους ανάμιξης.

Κάθε κόμβος ανάμιξης βοηθά την ALICE με το να ανακατευθύνεται γύρω από τη συναλλαγή.



Αυτό το δίκτυο κόμβων δημιουργεί αποκεντρωμένη ανωνυμία όμοια με το TOR Onion Routing.

Οι κόμβοι ανάμιξης ανταμείβονται για την κρυφή συναλλαγή της ALICE.

(+0.0992) CLOAK

Ένα επιτόκιο από 0,2% (> 1000 κέρματα) έως 1% (0 κέρματα) μοιράζεται μεταξύ όλων των συμμετεχόντων.

Το σύστημα λειτουργεί άψογα για να εξασφαλίσει ολοκληρωμένη ανωνυμία και πλήρη ιδιωτικότητα.

Στη συνέχεια, ο BOB λαμβάνει την κρυπτογραφημένη πληρωμή της ALICE.

BOB (+10) CLOAK

Ο BOB λαμβάνει με επιτυχία ανώνυμα 10 CLOAK.

3. CLOAKSHIELD

Το CloakShield παρέχει ασφαλή επικοινωνία μεταξύ κόμβων στο δίκτυο Cloak χρησιμοποιώντας συμμετρική κρυπτογράφηση RSA υποστηριζόμενη από μια Elliptic Curve Diffie Hellman key exchange (ECDH). Αυτό επιτρέπει στους κόμβους να ανταλλάσσουν δεδομένα με ασφάλεια, προσφέροντας προστασία από αδιάκριτους και απατεώνες (επίθεση sybil). Το CloakShield έχει σχεδιαστεί για να διασφαλίζει τόσο τις εφαρμογές Enigma όσο και τις αποκεντρωμένες εφαρμογές του CloakCoin και να διασφαλίζει ότι τα δεδομένα σας παραμένουν όσο το δυνατόν πιο ιδιωτικά.

Το CloakShield επιτρέπει την κρυπτογραφημένη αποστολή δεδομένων σε έναν ή περισσότερους παραλήπτες. Όταν αποστέλλεται σε ένα μόνο παραλήπτη, το φορτίο είναι κρυπτογραφημένο με RSA χρησιμοποιώντας το κοινό μυστικό του ECDH. Όταν στέλνετε σε πολλούς παραλήπτες, το ωφέλιμο φορτίο κρυπτογραφείται χρησιμοποιώντας ένα κλειδί μιας χρήσης και το κλειδί κρυπτογραφείται για κάθε έναν από τους παραλήπτες χρησιμοποιώντας τη μέθοδο ECDH / RSA.

ΔΗΜΙΟΥΡΓΩΝΤΑΣ ΕΝΑ ΚΡΥΠΤΟΓΡΑΦΗΜΕΝΟ ΚΛΕΙΔΙ ΚΟΙΝΗΣ ΧΡΗΣΗΣ.

Προκειμένου η Alice και ο Bob να επικοινωνούν με ασφάλεια, πρέπει να συμφωνήσουν σε ένα κοινό κλειδί κρυπτογράφησης. Το CloakShield χρησιμοποιεί το ECDH για να το επιτύχει:

- Η Alice έχει ιδιωτικό κλειδί Enigma dA και δημόσιο κλειδί Enigma QA = dAG (όπου G είναι ο δημιουργός για την ελλειπτική καμπύλη). Ο Bob έχει ιδιωτικό κλειδί Enigma dB και δημόσιο κλειδί Enigma QB = dBG.

- Η Alice έχει το δημόσιο Enigma κλειδί dB του Bob από τις ανακοινώσεις Enigma που στέλνει στο δίκτυο για να ανακοινώσει τη διαθεσιμότητά του για την βοήθεια της απόκρυψης. Αυτή χρησιμοποιεί το ιδιωτικό κλειδί της dA και το δημόσιο κλειδί QB του Bob για να υπολογίσει το κοινό μυστικό dAQB = dAdBG (ECDH_compute_key στο OpenSSL).

- Η Alice στη συνέχεια δημιουργεί ένα SHA256 hash του μυστικού και περνάει το hash με τη μέθοδο OpenSSLEVP_BytesToKey για να παράγει ένα κλειδί κρυπτογράφησης και IV, που θα χρησιμοποιηθεί για την κρυπτογράφηση δεδομένων για τον Bob (χρησιμοποιώντας συμμετρική κρυπτογράφηση RSA).

- Η Alice είναι πλέον σε θέση να δημιουργήσει ασφαλή μηνύματα CloakShield για τον Bob.

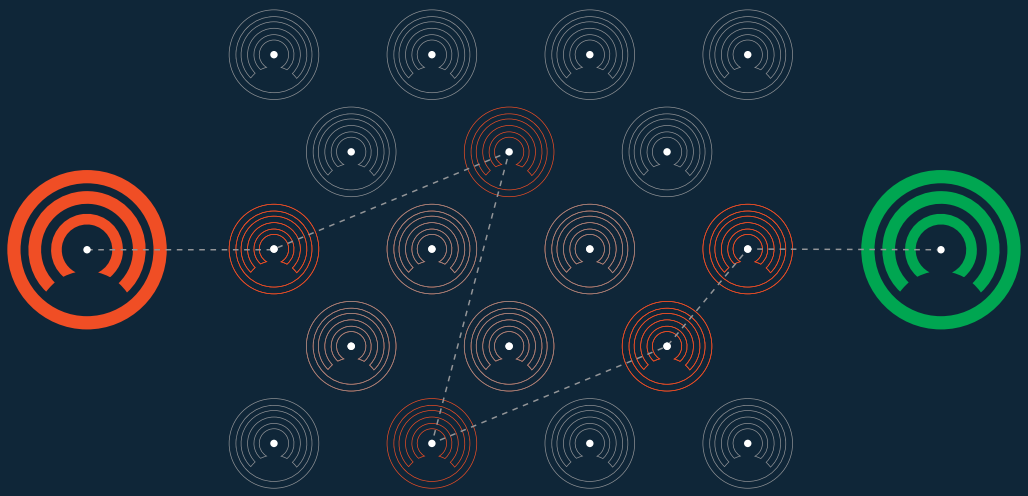
Όταν ο Bob παίρνει ένα μήνυμα Cloak Shielded από την Alice, διαβάζει το δημόσιο κλειδί της Alice από την κεφαλίδα του μηνύματος και παράγει το ίδιο κοινόχρηστο μυστικό κλειδί με την Alice, σύμφωνα με τα παραπάνω βήματα (με το μυστικό του κλειδί, αντί της Alice).

Το πορτοφόλι Cloak διατηρεί μια λίστα ενεργών κλειδιών CloakShield και θα ελέγξει τη λίστα για ένα υπάρχον κλειδί CloakShield προτού δημιουργήσει ένα.

ΔΕΔΟΜΕΝΑ CLOAKSHIELD

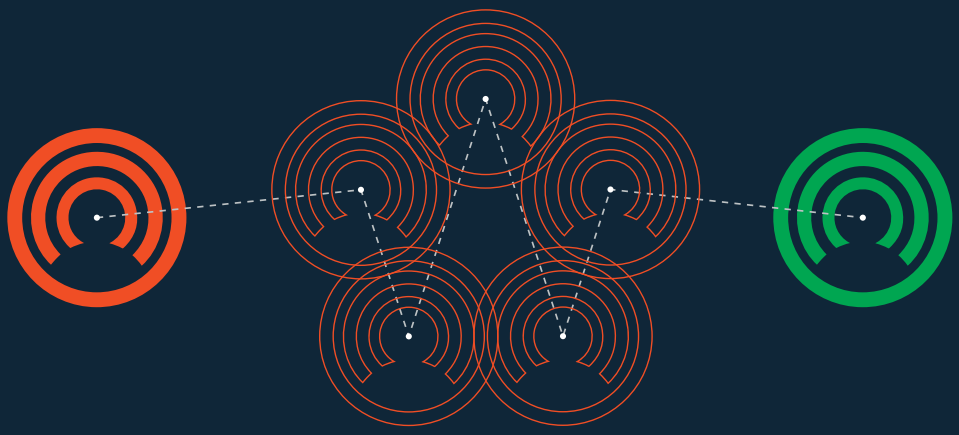
Το CloakShield επιτρέπει σε οποιαδήποτε αντικείμενα δεδομένων Cloak να μεταδίδονται με ασφάλεια σε έναν ή περισσότερους παραλήπτες. Ένα πακέτο δεδομένων CloakShield περιέχει το δημόσιο κλειδί Enigma του αποστολέα και τα δημόσια κλειδιά hashes των παραληπτών.

Οι κεφαλίδες του CloakShield περιέχουν ένα hash επαλήθευσης, το οποίο δημιουργείται χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα και τα ακατέργαστα μη κρυπτογραφημένα δεδομένα. Αυτός το hash επαληθεύεται κατά τη διάρκεια της αποκρυπτογράφησης των δεδομένων CloakShield για να διασφαλιστεί ότι οι πληροφορίες του παραλήπτη στην κεφαλίδα αντιστοιχούν στο κλειδί κρυπτογράφησης και ότι τα δεδομένα δεν έχουν αλλοιωθεί.



CLOAKSHIELD ONION ROUTING

Το Onion routing είναι μια τεχνική (που χρησιμοποιείται από το TOR) για την ανώνυμη επικοινωνία μέσω ενός δικτύου υπολογιστών. Σε ένα δίκτυο Onion, τα μηνύματα εγκλωβίζονται σε στρώματα κρυπτογράφησης, ανάλογα με τα στρώματα ενός Onion. Τα κρυπτογραφημένα δεδομένα μεταδίδονται μέσω μιας σειράς κόμβων δικτύου που ονομάζονται Onion routers, καθένας από τους οποίους "ξεφλουδίζει" ένα μόνο στρώμα, αποκαλύπτοντας τον επόμενο προορισμό των δεδομένων. Όταν το τελικό στρώμα αποκρυπτογραφείται, το μήνυμα φτάνει στον προορισμό του. Ο αποστολέας παραμένει ανώνυμος επειδή κάθε διαμεσολαβητής γνωρίζει μόνο τη θέση των αμέσως προηγούμενων και των επόμενων κόμβων.



ONION ROUTING ANALOGY

Η προσθήκη της λειτουργίας " onion routing" στο δίκτυο Enigma (χρησιμοποιώντας το CloakShield) επιτρέπει στους κόμβους να επικοινωνούν έμμεσα για να παρακάμψουν την ανάλυση κυκλοφορίας. Αυτό παρεμποδίζει τις προσπάθειες προσδιορισμού ποιοι κόμβοι επικοινωνούν μεταξύ τους ή ποιοι κόμβοι υποβάλλουν συναλλαγές στο δίκτυο CloakCoin. Όταν ένας κόμβος Enigma επιθυμεί να επικοινωνήσει με έναν άλλο κόμβο Enigma, επιλέγει έναν αριθμό άλλων κόμβων Enigma για να λειτουργήσει ως αναμεταδότης για την επικοινωνία. Κάθε κρυπτογραφημένη στρώση μπορεί να αποκρυπτογραφηθεί μόνο από το σχεδιαζόμενο αναμεταδότη [για τον οποίο το συγκεκριμένο στρώμα κρυπτογραφήθηκε]. Μετά την αποκρυπτογράφηση ενός στρώματος, ο αναμεταδότης μεταδίδει τα δεδομένα στον επόμενο κόμβο αναμετάδοσης. Αυτή η δρομολόγηση συνεχίζεται έως ότου τα δεδομένα φθάσουν στον αποδέκτη τους και όλα τα στρώματα έχουν αποκρυπτογραφηθεί με τη σειρά τους από τους επιλεγμένους κόμβους αναμετάδοσης. Λόγω της αυτοτελούς φύσης του δικτύου Enigma, οι κόμβοι εξόδου δεν απαιτούνται και το CloakShield εξασφαλίζει ότι δεν υπάρχει κίνδυνος ανάγνωσης ή αλλαγής των κρυπτογραφημένων δεδομένων από τον κόμβο αναμετάδοσης.

4. ΑΟΡΑΤΕΣ ΔΙΕΥΘΥΝΣΕΙΣ

Το Cloak χρησιμοποιεί το σύστημα Enigma για να παράσχει ιδιωτικές / ασφαλείς συναλλαγές

CLOAKSHIELD - ΕΠΙΚΟΙΝΩΝΙΑ ΚΟΜΒΟ ΜΕ ΚΟΜΒΟ

Κατά την εκκίνηση, κάθε πορτοφόλι Cloak δημιουργεί ένα κλειδί (NID_secp256k1] keypair (Cloaking Encryption Key / CEK) για να τους επιτρέψει να αντλούν ad hoc μυστικά χρησιμοποιώντας το ECDH με το ιδιωτικό κλειδί τους και το δημόσιο κλειδί του παραλήπτη. Αυτή η επικοινωνία αποτελεί τη βάση σε όλες τις επικοινωνίες κόμβο με κόμβο που σχετίζονται με το Enigma. Δείτε "src / enigma / cloakshield.h / .cpp" για περισσότερες πληροφορίες σχετικά με αυτό. Αυτή η κρυπτογραφημένη επικοινωνία με βάση το ECDH χρησιμοποιείται επίσης για τα δεδομένα onion - routing, τα οποία διαχειρίζεται το CloakShield.

Όταν το onion routing είναι ενεργοποιημένο, ο πελάτης θα προσπαθήσει να κατασκευάσει μία έγκυρη διαδρομή για τα δεδομένα χρησιμοποιώντας τον κατάλογο των χρηστών Enigma που γνωρίζει. Ο κόμβος μπορεί να μην έχει άμεση σύνδεση με τα Enigma peers, αλλά αυτό δεν είναι απαραίτητο, καθώς τα Cloak-Data (πακέτα δεδομένων για δρομολόγηση με CloakShield) μεταδίδονται με τη διαδικασία peer-to-peer. Ένα onion route συνήθως αποτελείται από 3 ξεχωριστές διαδρομές στον κόμβο προορισμού, με 3 κόμβους hops ανά διαδρομή. Πολλαπλές διαδρομές χρησιμοποιούνται για να αντιμετωπίσουν καταστάσεις όπου ένας κόμβος δρομολόγησης πέφτει εκτός σύνδεσης.

Οι κόμβοι στέλνουν περιοδικά μια ανακοίνωση Enigma (src / enigma / enig-maann.h) στα peers για να διαφημίσουν τις υπηρεσίες τους για onion routing.
λλοι κόμβοι του δικτύου αποθηκεύουν τις ανακοινώσεις (μέχρι να λήξουν ή να αντικατασταθούν με μια ενημερωμένη έκδοση) και να τις χρησιμοποιήσουν για να κατασκευάσουν onion routing.

ΠΑΡΑΔΕΙΓΜΑ ΣΥΝΑΛΛΑΓΗΣ ΑΟΡΑΤΗΣ ΔΙΕΥΘΥΝΣΗΣ.

Όταν ένας κόμβος στέλνει μια συναλλαγή Enigma σε μια αόρατη διεύθυνση, συμβαίνουν τα εξής:

1. Ο αποστολέας δημιουργεί εισροές για την κάλυψη του ποσού που αποστέλλεται, τις ανταμοιβές Enigma και τα τέλη δικτύου (1% σε 0 νομίσματα έναντι 0,2% σε 1000 και άνω νομίσματα).
2. Ο αποστολέας δημιουργεί ένα αντικείμενο CloakingRequest (που περιέχει μοναδικό αόρατο nonce για αυτό το αίτημα).
3. Ο αποστολέας παράγει μεταξύ 2 και 4 μοναδικών αόρατων διευθύνσεων πληρωμής χρησιμοποιώντας την αόρατη διεύθυνση των παραληπτών και διαχωρίζει τυχαία το ποσό μεταξύ των διευθύνσεων.
4. Ο αποστολέας αποφασίζει πόσοι συμμετέχοντες πρόκειται να χρησιμοποιηθούν. Από 5 μέχρι 25 συμμετέχοντες μπορούν να επιλεγούν (κάθε συμμετέχων παίρνει το 80 με 120% ενός εξίσου διαιρούμενου τέλους Enigma).
5. Αποστολές onion routes στο δίκτυο του CloakRequest. Η αίτηση περιέχει το "ποσό αποστολής", έτσι ώστε οι Cloakers να γνωρίζουν το ποσό που πρέπει να κρατήσουν.
6. Ο Cloaker παίρνει το CloakRequest και αποφασίζει να συμμετάσχει.
7. Ο Cloaker παρέχει X εισροές στον αποστολέα και μία αόρατη διεύθυνση και αόρατο Hash (για την αλλαγή τους).
8. Ο Cloaker στέλνει CloakingAcceptResponse στον αποστολέα. Αυτό περιέχει την αόρατη διεύθυνση, αόρατο nonce και εισόδους TX.
9. Ο αποστολέας περιμένει εως ότου αρκετοί Cloakers να το αποδεχτούν.
10. Ο αποστολέας δημιουργεί μία συναλλαγή Enigma χρησιμοποιώντας δικές του εισόδους και εισόδους του Cloaker. Οι είσοδοι αναμιγνύονται.
11. Ο αποστολέας δημιουργεί εξόδους TX για όλους τους Cloakers. Οι έξοδοι χωρίζουν τυχαία την αλλαγή τους και την επιστρέφουν σε αυτές. Αυτό επίσης αποδίδει την ανταμοιβή απόκρυψης στους Cloakers.

12. Ο αποστολέας δημιουργεί τις δικές του αλλαγές επιστροφής για το Enigma TX. Αυτές είναι μοναδικές διευθύνσεις πληρωμών.

13. Ο αποστολέας υπολογίζει το τέλος δικτύου TX και αφαιρεί αυτό από την δική του επιστροφή αλλαγής.

14. αποστολέας στέλνει το Enigma TX στους Cloakers για υπογραφή.

15. Οι Cloakers ελέγχουν το TX για να εξασφαλίσουν ότι οι εισροές τους είναι παρούσες και σωστές και ότι υπάρχουν διευθύνσεις πληρωμής μιας χρήσης που συνδέονται με μία από τις αόρατες διευθύνσεις τους με πληρωμή που υπερβαίνει το ποσό εισροών.

16. Οι Cloakers υπογράφουν ή απορρίπτουν το TX και στέλνουν τις υπογραφές στον αποστολέα.

17. Ο αποστολέας συγκεντρώνει τις υπογραφές και μεταδίδει το οριστικοποιημένο, υπογεγραμμένο TX στο δίκτυο.

18. Οι κόμβοι σαρώνουν τις εισερχόμενες συναλλαγές για αόρατες πληρωμές και πληρωμές Enigma και εντοπίζουν τυχόν πληρωμές ή αλλαγές. Τα κλειδιά και οι διευθύνσεις που δημιουργούνται είναι για τυχόν πληρωμές που αντιστοιχούν και αυτά τα κλειδιά / διευθύνσεις που δημιουργούνται αποθηκεύονται στο τοπικό πορτοφόλι.

5. ΤΟ ΜΕΛΛΟΝ ΤΟΥ ENIGMA – ΠΕΡΑΙΤΕΡΩ ΕΞΕΛΙΞΗ.

Το ENIGMA αποτελεί τον πυρήνα του CloakCoin και θα συνεχίσει να αναπτύσσεται και να βελτιώνεται καθώς προχωράμε με το CloakCoin. Εδώ είναι μερικά από τα χαρακτηριστικά που σχεδιάζονται για μελλοντικές αναθεωρήσεις:

ΒΕΛΤΙΩΜΕΝΟΣ ΑΛΓΟΡΙΘΜΟΣ PROOF-OF-STAKE

Proof of Stake (PoS) είναι μια μέθοδος διασφάλισης ενός δικτύου κρυπτονομισμάτων που βασίζεται σε χρήστες που κατέχουν νομίσματα για να υπογράφουν Blocks.

Μακροπρόθεσμα, η πιθανότητα υπογραφής μπλοκ είναι ανάλογη με την ποσότητα των νομισμάτων που κατέχονται, κάποιος που κατέχει το 1% της συνολικής προσφοράς νομισμάτων θα είναι σε θέση να υπογράψει το 1% όλων των Μπλοκ Proof of Stake. Σε σύγκριση με το Proof of Work, το Proof of Stake απαιτεί σημαντικά λιγότερη υπολογιστική ισχύ και συνεπώς λιγότερη κατανάλωση ενέργειας.

COIN AGE ΚΑΙ ΓΡΑΜΜΙΚΟ PROOF-OF-STAKE

Οι βασικές αρχές για τις περισσότερες εφαρμογές του proof of stake, συμπεριλαμβανομένης αυτής του CloakCoin, είναι η έννοια του Coin Age. Ουσιαστικά, αυτό είναι ένα μέτρο για το πόσο ένας κάτοχος νομισμάτων έχει κρατήσει τα νομίσματα του χωρίς να τα ξοδέψει ή να ταμετακινήση. Από τη στιγμή που ολοκληρώνεται μια συναλλαγή, τα νομίσματα που αποτελούν μέρος της συναλλαγής αρχίζουν να συσσωρεύουν το Coin Age (το οποίο αρχίζει από το μηδέν). Στην απλούστερη μορφή του, με τίτλο “γραμμικό Coin Age”, τα κέρματα θα συγκεντρώνουν ένα λεπτό / ώρα / ημέρα / έτος του Coin Age ανά λεπτό / ώρα / ημέρα / έτος ηλικίας. Για παράδειγμα, ένα άτομο που κατέχει 365 νομίσματα για 100 ημέρες συγκεντρώνει 36.500 «ημέρες νομίσματος» ή περίπου 100 «χρόνια νομισμάτων» (το «έτος κέρματος» ορίζεται για τα χρονικά διαστήματα και επομένως δεν είναι ακριβώς 365 ημέρες, αλλά 365,24 ημέρες).

Το γραμμικό Proof of Stake έχει προσελκύσει επικρίσεις σε σχέση με το Coin Age. Πολλοί υποστηρίζουν ότι το γραμμικό Proof of Stake ενθαρρύνει τη συσσώρευση νομισμάτων (που μπορεί να έχει αρνητικές συνέπειες για το εμπόριο και τον όγκο μεταφοράς). Ένα άλλο έγκυρο παράπονο κατά του γραμμικου Proof of Stake αφορά το αποτέλεσμα που μπορεί να έχει στην ασφάλεια του δικτύου. Οι εφαρμογές γραμμικού Proof of Stake συχνά υποφέρουν επειδή οι χρήστες συνδέονται περιοδικά με το δίκτυο Cloak για να κάνουν Stake τα νομίσματά τους και μόλις καταστραφεί το Coin Age αποσυνδέονται. Στη συνέχεια ο χρήστης περιμένει έως ότου συμπληρώσει το Coin Age πριν επαναλάβει τη διαδικασία σύνδεσης – Stake - αποσύνδεσης. Αυτό δεν παρέχει την καλύτερη ασφάλεια για το δίκτυο και ένας αλγόριθμος Proof-of-Stake που επιβραβεύει το συχνό ή σταθερό staking θα ήταν περισσότερο επωφελής για το CloakCoin και τα συναφή νομίσματα Proof-of-Stake.

Για να διασφαλιστεί ότι οι ανταμοιβές των Enigma Cloakers είναι όσο το δυνατόν πιο επαρκής, το Coin Age θα πρέπει να αφαιρεθεί από τον αλγόριθμο Proof-of Stake του CloakCoin. Αυτό θα εξασφάλιζε ότι οι Cloakers θα λάβουν τόσο την πλήρη ανταμοιβή του staking όσο και κάθε ανταμοιβή Enigma Cloaking. Η πρόσθετη ενσωμάτωση μιας συνιστώσας ταχύτητας στον υπολογισμό των ανταμοιβών staking θα επιβραβεύσει περαιτέρω τους ενεργούς κόμβους Enigma Cloaking, ενθαρρύνοντας τους χρήστες να συμμετέχουν στο Enigma Cloaking για να αυξήσουν περαιτέρω το κερδοφόρο ενδιαφέρον τους, καθώς επίσης και να κερδίσουν ανταμοιβές Cloaking.

Εκτός από την παροχή μεγαλύτερων ανταμοιβών στους ενεργά συμμετέχοντες, ένας βελτιωμένος αλγόριθμος Proof-Stake παρέχει επίσης τις προαναφερθείσες βελτιώσεις στην ασφάλεια του δικτύου.

ΣΥΝΔΥΑΖΟΝΤΑΣ ΚΑΙ ΔΙΑΙΡΩΝΤΑΣ ΤΙΣ ΣΥΝΑΛΛΑΓΕΣ ENIGMA.

Το Enigma προς το παρόν δημιουργεί μία μόνο “κρυφή” συναλλαγή ανά μεταφορά.
Αυτή τη στιγμή δουλεύουμε σε μια ενημέρωση του πλαισίου Enigma που θα επιτρέπει να γίνονται πολλαπλές συναλλαγές Enigma για να συνδυαστούν σε μια υπερ - συναλλαγή Enigma. Αυτό θα περιλαμβάνει αποτελεσματικά, πολλαπλές συναλλαγές "Cloaked" και θα προσφέρει ακόμα μεγαλύτερη ανωνυμία στους χρήστες του Cloak. Αυτή η επέκταση θα επιτρέψει στους χρήστες να επιλέξουν τον αριθμό των συνεταιριστικών συναλλαγών Enigma που χρειάζονται καθώς επίσης και τον αριθμό των Cloakers.

Η προσθήκη αυτή φυσικά παραμένει πλήρως αποκεντρωμένη, ιδιωτική και ασφαλής.
Μία ακόμα βελτίωση αποστολής ENIGMA που συμπληρώνεται αυτή την περίοδο από την ομάδα Cloak είναι η δυνατότητα να 'αποκρύψει' ένα μεγάλο ποσό Cloak ως μια σειρά μικρότερων συναλλαγών Enigma. Για να επιτευχθεί αυτό, ένας χρήστης θα επιλέξει το ποσό των Cloak που θα ήθελε να αποστείλει ‘κρυφά’ σε μια διεύθυνση. Στη συνέχεια, το CloakCoin θα δούλευε στο παρασκήνιο για να δημιουργήσει μια σειρά μικρότερων συναλλαγών Enigma ίσου ποσού, οι οποίες μπορούν να κρυφτούν και να υποβληθούν στο δίκτυο Cloak για μια καθορισμένη χρονική περίοδο. Αυτή η διαδικασία αποστολής δεδομένων θα είναι συμβατή με τις «συνδυασμένες» συναλλαγές Enigma, παρέχοντας περαιτέρω προστασία Cloaking για μεταφορές.

6. ΣΥΧΝΕΣ ΕΡΩΤΗΣΕΙΣ

Q. ΠΩΣ ΟΙ CLOAKERS ΒΟΗΘΟΥΝ ΣΕ ΜΙΑ ΣΥΝΑΛΛΑΓΗ ENIGMA

Οι cloakers παρέχουν μία ή περισσότερες εισόδους που χρησιμοποιούνται για την "απόκρυψη" της εισόδου από τον αποστολέα. Οι Cloakers παρέχουν επίσης μια σειρά διευθύνσεων επιστροφής που επιστρέφουν τις εισόδους τους και επίσης επιβραβεύουν το Cloaker με φόρο. Οι διευθύνσεις επιστροφής επιλέγονται προσεκτικά προκειμένου να δοθεί προτεραιότητα στις διευθύνσεις με δραστηριότητα. Αυτό καθιστά πολύ πιο δύσκολο για οποιονδήποτε εκτελεί αναλύσεις blockchain να εντοπίσει την πραγματική έξοδο μιας συναλλαγής Enigma. Το σύστημα Enigma θα ελέγξει επίσης τη στοχοποιημένη διεύθυνση έτσι ώστε οι έξοδοι «cloaked» να αντικατοπτρίζουν την πραγματική έξοδο όσο το δυνατόν πιο κοντά.

Q. ΠΟΣΟΣ ΧΡΟΝΟΣ ΧΡΕΙΑΖΕΤΑΙ ΓΙΑ ΝΑ ΟΛΟΚΛΗΡΩΘΕΙ ΜΙΑ ΣΥΝΑΛΛΑΓΗ ENIGMA;

Οι συναλλαγές Enigma προς το παρόν χρειάζονται ένα λεπτό για να ολοκληρωθούν. Οι κόμβοι Cloaking που βοηθούν στην 'Απόκρυψη' μιας συναλλαγής Enigma θα κρατήσουν τα απαραίτητα κεφάλαια μέχρι να ολοκληρωθεί η συναλλαγή Enigma ή να λήξει ο χρόνος που έχει διατεθεί. την περίπτωση που η συναλλαγή έχει λήξει ή διακοπεί, τα κεφάλαια ξεκλειδώνονται τοπικά για επαναχρησιμοποίηση.

Q. ΠΩΣ ΤΟ ENIGMA ΕΠΗΡΕΑΖΕΙ ΤΟ STAKING;

Οποιαδήποτε νομίσματα που χρησιμοποιούνται σε μια συναλλαγή Enigma (ως αποστολέας ή Cloaker) θα έχουν την επαναφορά του Coin Age τους. Πρέπει να σημειωθεί, ωστόσο, ότι η συμμετοχή στο Cloaking προσφέρει πολύ υψηλότερη απόδοση από το staking. Η ομάδα του Cloak εργάζεται για την αναθεώρηση του αλγορίθμου Enigma για την επερχόμενη έκδοση hardfork (Enigma 1.1). Ανατρέξτε στην ενότητα 5 - «Το μέλλον του ENIGMA - περαιτέρω ανάπτυξη» για περισσότερες λεπτομέρειες.

Q. ΧΡΕΙΑΖΟΜΑΙ ΜΙΑ ΣΥΓΚΕΚΡΙΜΕΝΗ ΠΟΣΟΤΗΤΑ CLOAK ΣΤΟ ΠΟΡΤΟΦΟΛΙ ΜΟΥ ΓΙΑ ΝΑ ΓΙΝΩ ΕΝΑΣ ENIGMA CLOAKER;

Μπορείτε να προσφέρετε τις υπηρεσίες σας για Cloaking ανεξάρτητα από την ποσότητα που περιέχετε στο CloakCoin πορτοφόλι σας. Όταν το Enigma Cloaking είναι ενεργοποιημένο, το CloakCoin θα κρατήσει ένα μέρος του υπολοίπου σας για τη συμμετοχή στο Enigma Cloaking, για το οποίο θα κερδίσετε μια ανταμοιβή Cloaking. Το προεπιλεγμένο ποσό αποθεματικού είναι ~ 50%, αλλά αυτή η τιμή μπορεί να ρυθμιστεί από το χρήστη. Η επιλεγμένη τιμή θα είναι τυχαία ώστε να αποφευχθεί η σύνδεση των ανακοινώσεων του Enigma με το αναφερόμενο ισοζύγιο Cloaking.

Πρέπει να σημειωθεί ότι τα πορτοφόλια με υψηλότερο υπόλοιπο έχουν περισσότερες πιθανότητες να επιλεγούν ως Cloaker, καθώς είναι πιθανότερο να έχουν στη διάθεσή τους το απαιτούμενο ισοζύγιο Cloaking για μεγαλύτερες συναλλαγές Enigma.

Q. ΠΩΣ ΑΥΤΌ ΠΡΟΣΤΑΤΕΥΕΤΕ ΕΝΑΝΤΙΟΝ ΜΙΑΣ ΕΠΙΘΕΣΗΣ ΒΑΣΙΣΜΕΝΗ ΣΤΟ ΧΡΟΝΟ ΟΠΟΥ ΚΑΠΟΙΟΣ ΕΛΕΓΧΕΙ ΤΟ BLOCKCHAIN ΓΙΑ ΟΜΟΙΕΣ ΕΙΣΟΔΟΥΣ ΚΑΙ ΕΞΟΔΟΥΣ

Οι συναλλαγές με αίνιγμα ομαδοποιούν τις εξόδους και διασφαλίζουν ότι έχουν πολλαπλά αντίστοιχα ποσά εξόδου για να «κρύψουν» την έξοδο του παραλήπτη.

Q. ΜΠΟΡΕΙ Ο ΔΗΜΙΟΥΡΓΟΣ ΜΙΑΣ ΣΥΝΑΛΛΑΓΗΣ ENIGMA ΝΑ ΚΑΘΟΡΙΖΕΤΑΙ Ε ΕΤΑΖΟΝΤΑΣ ΤΗΝ ΥΠΟΓΡΑΦΗ ΤΟΥ SCRIPT ΓΙΑ ΝΑ ΚΑΘΟΡΙΣΕΙ ΓΙΑ ΤΗΝ ΕΝΤΟΛΗ ΥΠΟΓΡΑΦΗΣ;

Όχι. Κατά τη διαδικασία υπογραφής, η σειρά υπογραφής του script είναι τυχαία κατά τον συνδυασμό των υπογραφών. Ο αποστολέας και οι συμμετέχοντες Cloakers το κάνουν αυτό.

Q. ΜΠΟΡΕΙ ΚΑΠΟΙΟΣ ΝΑ ΠΑΡΑΚΟΛΟΥΘΗΣΕΙ ΤΟ ΔΙΚΤΥΟ ΓΙΑ ΝΑ ΔΕΙ ΤΙ Ε ΕΡΧΟΜΕΝΕΣ ΣΥΝΑΛΛΑΓΕΣ ENIGMA ΠΟΥ ΥΠΟΒΑΛΛΟΝΤΑΙ ΣΤΟ ΔΙΚΤΥΟ ΚΑΙ ΝΑ ΚΑΘΟΡΙΣΕΙ ΤΟΝ ΠΡΑΓΜΑΤΙΚΟ ΑΠΟΣΤΟΛΕΑ;

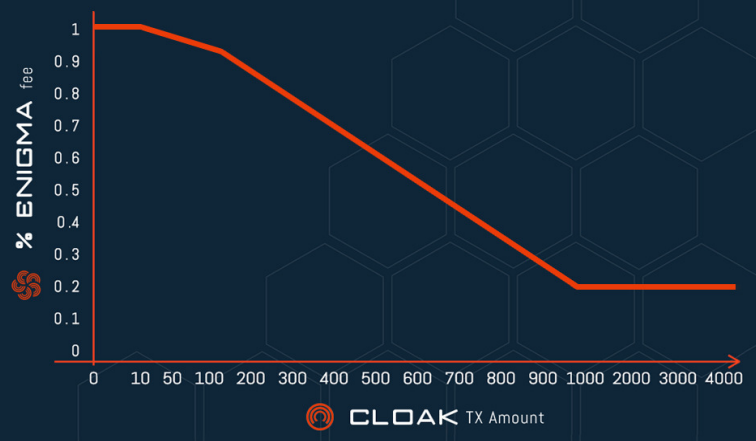
Όχι. Όλες οι ομάδες με τυχαία σειρά υποβάλλουν μια συναλλαγή Enigma στο δίκτυο. Αυτό παρέχει άμβλυνση ενάντια σε τέτοιες επιθέσεις υποκλοπής.

Q. ΠΟΣΟ ΕΙΝΑΙ ΤΟ ΤΕΛΟΣ ΓΙΑ ΜΙΑ ΣΥΝΑΛΛΑΓΗ ENIGMA

1% στα 0 νομίσματα μέχρι το 2% στα 1000 και σε υψηλότερα νομίσματα. Αυτό χρησιμοποιείται για την επιβράβευση των κόμβων Enigma που βοηθούν στην απόκρυψη μιας συναλλαγής Enigma. Τα τέλη στη συνέχεια αναμειγνύονται με τη συναλλαγή και κατανέμονται μεταξύ των κατόχων. Δεν είναι μόνο ανταμοιβή για τους συμμετέχοντες. αλλά χρησιμοποιειούνται για να καταστήσει τον προσδιορισμό του ποσού της συναλλαγής που είναι ανέφικτα δύσκολο. Κάθε συμμετέχων λαμβάνει το θ-120% μοιρασμένο ισότιμα μιας συναλλαγής enigma.

Q. ΠΩΣ ΚΑΘΟΡΙΖΟΝΤΑΙ ΤΑ ΤΕΛΗ ΤΟΥ ENIGMA;

Το τέλος % Enigma χρεώνεται ανά βάση συναλλαγής με τους εξής συντελεστές:



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

Q. ΑΠΕΙΤΕΙΤΑΙ ΑΠΟ ΤΟ ENIGMA ΕΝΑ HARD - FORK ΤΟΥ ΔΙΚΤΥΟΥ CLOAK;

Όχι. Οι παλαιότεροι πελάτες CloakCoin θα χειριστούν τις συναλλαγές Enigma χωρίς προβλήματα, αλλά δεν θα είναι σε θέση να τις δημιουργήσουν ή να συμμετάσχουν στο “cloaking”. Η επόμενη αναθεώρηση του Enigma, ωστόσο, θα απαιτήσει ένα Hard-Fork λόγω αλλαγών στον υποκείμενο αλγόριθμο Proof-of-Stake και την υποστήριξη για πρόσθετο script opcodes για τα χαρακτηριστικά της αγοράς (όπως Block Escrow).

Q. ΠΟΙΟΣ ΕΙΝΑΙ Ο ΜΕΓΙΣΤΟΣ ΑΡΙΘΜΟΣ ΤΩΝ CLOAKERS ΠΟΥ ΜΠΟΡΕΙ ΝΑ ΒΟΗΘΗΣΕΙ ΣΕ ΜΙΑ ΣΥΝΑΛΛΑΓΗ ENIGMA;

Ο μέγιστος αριθμός Cloakers είναι σταθερός στα 25. Το σύστημα Enigma είναι ευέλικτο και ο αριθμός αυτός μπορεί εύκολα να επεκταθεί.

Q. ΠΩΣ ΠΡΟΣΤΑΤΕΥΕΤΑΙ ΤΟ ENIGMA ΕΝΑΝΤΙΑ ΣΕ "ΚΑΚΟΥΣ ΦΟΡΕΙΣ";

Το σύστημα Enigma διαθέτει εκτεταμένη προστασία DDoS σε «μαύρη λίστα» κόμβων για τη διάρκεια μιας περιόδου σύνδεσης. Εάν ένας κόμβος Enigma αρνείται επανειλημμένα να υπογράψει, θα αποκλειστεί από τις προσκλήσεις Enigma Cloaking για το υπόλοιπο της τρέχουσας περιόδου σύνδεσης. Αυτή τη στιγμή ερευνάμε πρόσθετες μεθοδολογίες για την περαιτέρω ‘τιμωρία’ των μη συνεργάσιμων κόμβων Enigma και πιθανόν να εφαρμόσουμε ένα σύστημα που απαιτεί από τους Cloakers να δεσμεύσουν μια ονομαστική, επιστρεπτέα αμοιβή που θα μπορούσε να αξιωθεί ως ποινή σε περιπτώσεις όπου ένας κόμβος προσπαθεί να αποκλείσει μια συναλλαγή Enigma αρνούμενος να υπογράψει την οριστική συναλλαγή. Πρέπει να σημειωθεί ότι ενώ οι κακοί κόμβοι ενδέχεται να επιχειρήσουν να παρεμποδίσουν μια συναλλαγή Enigma, δεν είναι σε θέση να κλέψουν ή να καταχραστούν οποιαδήποτε κεφάλαια.

Q. ΠΩΣ ΕΝΤΟΠΙΖΟΝΤΑΙ / ΛΑΜΒΑΝΟΝΤΑΙ ΟΙ ΑΟΡΑΤΕΣ ΣΥΝΑΛΛΑΓΕΣ ENIGMA;

Όλες οι εισερχόμενες συναλλαγές σαρώνονται. Οι αόρατες συναλλαγές σαρώνουν πρώτα (χρησιμοποιώντας τον προεπιλεγμένο εφήμερο pubkey που περιέχεται σε μία τυχαία έξοδο OP_RETURN TX). Στη συνέχεια, πραγματοποιούνται σαρώσεις για τις συναλλαγές Enigma. Οι συναλλαγές Enigma χρησιμοποιούν επίσης το τυποποιημένο εφήμερο pubkey, αλλά οι πληρωμές χρησιμοποιούν ένα επιπλέον βήμα που περιλαμβάνει ένα επιπλέον παράγωγο κλειδί. Οι έξοδοι του Enigma δημιουργούνται χρησιμοποιώντας ένα hash του εφήμερου pubkey, μία ιδιωτική αόρατη διεύθυνση Hash και τον δείκτη εξόδου.

Κατά τη σάρωση για συναλλαγές Enigma, οι διευθύνσεις πληρωμής μηδενικού δείκτη δημιουργούνται για κάθε ιδιόκτητη αόρατη διεύθυνση [HASH (ephemeral_pubkey, hash_stealth_secret, 0)]. Εάν εντοπιστεί μια αντιστοίχιση για το μηδενικό δείκτη μιας αόρατης διεύθυνσης, δημιουργούνται πρόσθετες διευθύνσεις για τα υπόλοιπα ευρετήρια [num_tx_outputs] και αυτά σαρώνουν προς ανίχνευση πληρωμών. Δείτε το FindEnigmaTransactions στο wallet.cpp για περισσότερες πληροφορίες.

Μία παρόμοια μέθοδος σάρωσης χρησιμοποιείται από τους Cloakers πριν από την υπογραφή ενός Enigma TX για να εξασφαλιστεί ότι αποζημιώνονται σωστά. Δείτε GetEnigmaOutputsAmounts στο wallet.cpp για περισσότερες πληροφορίες.

7. ΠΑΡΑΠΟΜΠΕΣ

[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