CLOAK

ENIGMA V2.1

Whitepaper / Livre blanc

(Nouvelle version)

ENIGMA

UN SYSTÈME DE TRANSACTION PRIVÉE, SÉCURISÉE ET NON TRAÇABLE POUR CLOAKCOIN

1. RÉSUMÉ

CloakCoin est une crypto-monnaie conçue pour faciliter des transferts décentralisés intraçables, privés et sécurisés grâce à Enigma.

Cloak est un coin qui a une double fonction PoW / PoS (Proof of Work et Proof of Stake: Preuve de travail et Preuve de participation) mais qui est désormais davantage porté sur le Proof of Stake.

Enigma est un système de paiement intraçable, privé et sécurisé de CloakCoin qui pose la base d'un développement futur et fournit le système de transaction fondamental nécessaire aux applications décentralisées fonctionnant sur le réseau CloakCoin.

La protection de la vie privée est sans aucun doute plus importante que jamais. Le rythme retentissant du progrès technologique a rapidement élargi nos horizons et connecté le monde comme jamais auparavant. Grâce à l'introduction du Bitcoin en 2009, la crypto-monnaie se diffuse constamment dans ce courant et nous pouvons maintenant transférer la monnaie numérique en toute sécurité et instantanément à travers le monde, en utilisant le pouvoir de la blockchain.

Comme l'adoption des crypto-monnaies devient plus répandue, une réglementation renforcée est inévitable. Il reste à établir sous quelle forme sera cette réglementation mais nombre d'entre elles sont concernées et cela pourrait s'avérer draconien et avoir pour but d'étouffer certains des aspects les plus libertaires de la crypto-monnaie.

ENIGMA

Enigma est au cœur d'un service de mixage décentralisé, hors blockchain, qui permet aux utilisateurs du réseau CloakCoin d'envoyer des Cloak de façon privée et sécurisée les uns aux autres. Enigma a été conçu pour apporter la garantie que le processus de mixage soit à la fois sécurisé et intraçable pour les observateurs extérieurs. L'utilisateur de Cloak est assuré que ses coins sont gardés en sécurité pendant le transfert et que l'expéditeur comme le receveur ne peuvent être reliés ou associés. Les coins de Cloak ne sont jamais transférés à une tierce personne pendant le Cloaking (création de Cloak); ainsi, les coins restent en sécurité.

Nous avons également travaillé dur pour s'assurer que le système Enigma récompense les utilisateurs qui participent aux transferts de Cloak et qui permettront d'améliorer le processus et conforteront d'autres participants actifs à le faire. Toute personne détentrice de coins Cloak peut participer aux opérations de Cloaking, ce qui lui permet de laisser son wallet (portefeuille numérique) en cours d'exécution en mode Staking/ Cloaking et pouvoir aider passivement à la création de Cloak et ainsi gagner d'importantes récompenses.

2. PRESENTATION D'ENIGMA V1.0

Enigma est la première version publique du système de paiement privé, sécurisé et intraçable que propose Cloak. Les transactions Enigma sont "cloakées" (masquées) par d'autres utilisateurs qui perçoivent une récompense pour leur aide. Ces autres utilisateurs fournissent entrées et sorties (input/output) lors de la transaction Enigma. Il est alors impossible de déterminer la véritable source et la destination du transfert de Cloak. Tous les messages Enigma présents sur le réseau sont hashés et chiffrés pour le destinataire grâce au CloakShield qui assure la sécurité et l'intégrité des données. Reportez-vous à la section 3 "CloakShield" pour plus de détails.

2.1. LE PROCÉDÉ ENIGMA (POUR ACTIVER LES NOEUDS ENIGMA)

LES NOTIFICATIONS ENIGMA

Les nœuds Enigma communiquent dans le réseau Cloak et un nœud garde la trace des autres nœuds actifs d'Enigma. Les diffusions de notifications Enigma préviennent les autres noeuds Enigma de notre clé publique et du solde actuel de la transaction de cloak Enigma.

LES REQUÊTES ENIGMA CLOAKING

Lorsqu'un utilisateur souhaite envoyer une transaction Cloak Enigma, il choisit une série de nœuds Enigma (avec une balance Enigma assez élevée) et demande leur aide pour le cloaking (créer du cloak). Un nœud Enigma peut choisir d'aider à faire du Cloak et envoyer une réponse d'acceptation au demandeur pour l'indiquer. Si un nœud Enigma refuse de participer au cloaking ou ne répond pas dans un délai raisonnable, un nœud Enigma alternatif est choisi et contacté.

La protection DDoS (distributed denial of service / déni de service distribué) exclura toute mauvaise conduite des nœuds pour le reste de la session. Un noeud est considéré défaillant s'il refuse à plusieurs reprises de signer une transaction Enigma ou de relayer les messages Enigma. Les nœuds Cloaking Enigma utilisent un exchange principal Elliptic Curve Diffie Hellman (ECDH) pour calculer un secret partagé avec le nœud initiateur Enigma, qui est utilisé pour créer une clé secrète partagée pour le chiffrement de données symétriques RSA-256 entre un nœud créant du Cloak et le noeud émetteur.

L'ACCEPTATION DU CLOAK ENIGMA

Lorsqu'un nœud Enigma accepte une demande de "Cloaking" (création de Cloak), il donne une liste d'entrées et de sorties (Input/Output) qui est utilisée pour la transaction Enigma. Les quantités d'entrées fournies par un noeud cloak doivent être supérieures ou égales au montant Enigma envoyé (plus les frais). Les sorties sont soigneusement sélectionnées pour qu'elles correspondent à la véritable sortie de la transaction Enigma de façon à ce que ça soit le plus proche possible. Si l'adresse de sortie Enigma n'a pas été utilisée précédemment, une nouvelle adresse sera générée par le "Cloaker"(créateur de Cloak). Si l'adresse de sortie Enigma a déjà reçu des capitaux, une adresse déjà existante ayant une activité similaire est choisi par le "Cloaker" pour retourner les capitaux d'entrée et recevoir la récompense pour avoir créé le cloak Enigma.

LA TRANSACTION CLOAKÉE (MASQUÉE) ENIGMA

L'Expéditeur Enigma créé une transaction cloakée (masquée) en utilisant les entrées et les sorties fournies par les nœuds Enigma. L'Expéditeur Enigma ajoute alors ses propres entrées et sorties à la transaction, avant de remanier toutes les entrées et sorties de la transaction pour faciliter le "cloaking" (création de cloak). La transaction "cloakée" est ensuite chiffrée et envoyée (à l'aide de CloakShield) à chaque Cloaker participant. Les nœuds créateurs de Cloak vérifient la transaction pour s'assurer que les entrées et

les sorties qu'ils fournissent sont présents dans la transaction "cloakée" et qu'une ou plusieurs de leurs sorties ont également été récompensées par des commissions adéquates.

Si les contrôles de transaction sont passés, la transaction est signée (SIGHASH_ ALL+SIGHASH_ANYONECANPAY), chiffrée et transmise à l' Expéditeur Enigma (Enigma Sender). Une fois que tous les créateurs de Cloaks Enigma ont signé la transaction, l'Expéditeur Enigma confirme que la transaction signée est valide et la signe. La transaction "cloakée" est alors prête à être transmise au réseau.

2.2.1. LA TRAÇABILITÉ DES NOEUDS ENIGMA

Les nœuds Enigma activés sur le réseau Cloak transmettent des notifications aux autres noeuds. Ces notifications Enigma contiennent l'identifiant public ec-key (clé ec > courbe elliptique) du nœud et le solde actuel disponible pour les opérations de création de cloaks Enigma. Les nœuds conservent une liste d'autres nœuds actifs Enigma sur le réseau afin qu'ils puissent communiquer sur les objectifs de création de cloaks. Les identifiants des nœuds sont générés lors de séances au cas par cas; redémarrer le compte rafraichira l'identifiant actuel.

1. Chaque wallet (portefeuille numérique) crée une paire de clés: clé publique / privée (secp256k1) pour le démarrage de la session.

2. Le wallet communique régulièrement sa clé publique et son solde de cloaks aux autres nœuds du réseau Cloak sur la session en cours.

3. Les nœuds gardent une trace des autres noeuds actifs Enigma créant des cloaks et peuvent communiquer avec eux directement ou indirectement (via le routeur en oignon CloakShield).

2.2.2. DÉMARRER UNE TRANSACTION ENIGMA

ALICE souhaite envoyer 10 CLOAK à BOB en utilisant 5 nœuds mixants.

1. Alice transmet une requête Enigma sur le réseau, contenant sa clé de session publique Enigma et la quantité de Cloak qu'elle souhaite envoyer. Sa requête traverse en toute sécurité une série de 5 nœuds Enigma pour masquer l'expéditeur.

2. Catherine a un "Mode Cloaking" actif et crée un canal CloakShield sécurisé et chiffré pour avoir une communication fiable avec Alice. Catherine construit alors un paquet de réponses Enigma et l'envoie en toute sécurité à Alice. La réponse contient une liste des entrées et des sorties de Catherine qu'Alice utilisera pour "cloaker" (masquer) sa transaction.

3. Alice déchiffre, traite la réponse Enigma de Catherine et crée une transaction Enigma en utilisant ses propres entrées et sorties mélangées avec celles de Catherine. Sa transaction est alors chiffrée et envoyée à Catherine pour la signature.

4. Catherine déchiffre la transaction Enigma et effectue un grand nombre de contrôles d'intégrité sur la transaction pour s'assurer que les entrées et les sorties fournies ont été correctement utilisées et que la récompense en retour est suffisante. Si la transaction Enigma réussit les tests, Catherine la signe, la chiffre et la transmet à Alice.

5. Alice effectue d'autres contrôles sur la transaction signée avant de la signer elle-même. La transaction est ensuite introduite dans le réseau (acheminée de manière sécurisée via les nœuds Enigma) pour être inclue dans un bloc.

6. Lorsque la transaction est finalisée, Bob recevra les fonds d'Alice et Catherine recevra une récompense "Cloaking" pour avoir contribué à la transaction Enigma.

7. En raison des entrées et des sorties de Catherine reflétant celles d'Alice, il est impossible de déterminer le véritable expéditeur et destinataire de la transaction Enigma.

EXEMPLE DE TRANSACTION ENIGMA

ALICE wants to send coins anonymously to BOB.

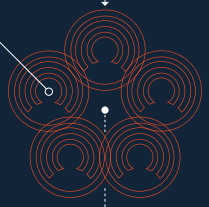
ALICE (−10.0992) CLOAK

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

ENIGMA mixer nodes begin communicating.

CATHERINE

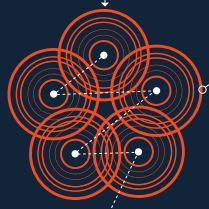
Every coin holder can announce themselves as a Mixer Node, also known as a "Cloaker".



Every participant remains anonymous and communicates through an encrypted channel.

ALICE's wallet is now connected to mixer nodes.

Each mixer node helps ALICE by shuffling around the transaction.



This network of nodes creates decentralized anonymization similar to TOR Onion Routing.

Mixer nodes get rewarded for Cloaking ALICE's transaction.

(+0.0992) CLOAK

A linear fee from .2% (>1000 coins) to 1% (0 coins) is shared amoungst all participating Cloakers.

The system works seamlessly to ensure complete anonymity and total privacy.

BOB then receives ALICE's encrypted payment

BOB (+10) CLOAK

BOB successfully receives 10 CLOAK anonymously.

3. CLOAKSHIELD

CloakShield fournit des communications sécurisées entre les nœuds dans le réseau Cloak en utilisant un chiffrement symétrique RSA renforcé par un échange de clé Courbe Elliptique Diffie Hellman (ECDH). Cela permet aux nœuds d'échanger des données en toute sécurité, offrant une protection contre les snoopers (fouineurs) et imposteurs (attaque Sybil). CloakShield est conçu pour sécuriser à la fois Enigma et les applications décentralisées CloakCoin et garantira que vos données restent aussi privées que possible.

CloakShield permet l'envoi chiffré de données à un ou plusieurs destinataires. Lors de l'envoi à un destinataire unique, la charge est chiffrée RSA en utilisant le secret partagé ECDH. Lors de l'envoi à plusieurs destinataires, la charge est chiffrée en utilisant une clé unique et la clé est ensuite chiffrée pour chaque destinataire en utilisant la méthode ECDH / RSA.

GÉNÉRER UNE CLÉ DE CHIFFREMENT PARTAGÉE

Afin qu'Alice et Bob puissent communiquer en toute sécurité, ils doivent s'entendre sur une clé de chiffrement partagée. CloakShield utilise ECDH pour la réaliser:

- Alice a la clé privée Enigma dA et la clé publique Enigma QA=dAG (où Gest le générateur de la courbe elliptique). Bob a la clé privée Enigma dB et clé publique Enigma QB=dBG.

- Alice a la clé publique Enigma de Bob dB des notifications d'Enigma qu'il envoie au réseau pour transmettre sa disponibilité pour l'assistance de création de cloak. Elle utilise sa clé privée dA et la clé publique de Bob QB pour calculer le secret partagé dAQB=dAdBG (ECDH_compute_key dans l'OpenSSL).

- Alice crée ensuite un hash secret SHA256 et transmet le hash sur la méthode OpenSSLEVP_BytesToKey afin d'obtenir une clé de chiffrement et IV, qui sera utilisé pour chiffrer les données pour Bob (en utilisant le chiffrement symétrique RSA).

- Alice est maintenant capable de créer des messages sécurisés CloakShield pour Bob.

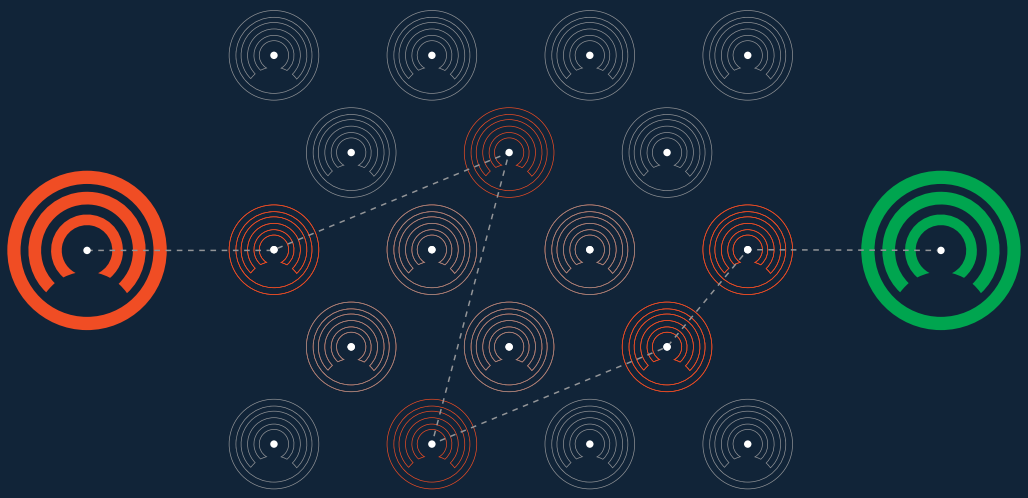
Quand Bob reçoit un message Shielded (blindé) de Cloak d'Alice, il lit la clé publique d'Alice depuis l'en-tête du message et crée la même clé partagée secrète qu'Alice, selon les étapes ci-dessus (avec sa clé secrète, à la place de celle d'Alice).

Le wallet Cloak établit une liste des clés actives CloakShield et vérifie la liste pour une clé existante CloakShield avant de créer une clé.

LES DONNÉES CLOAKSHIELD

CloakShield permet à tous les objets de données Cloak d'être intégrés et transmis en toute sécurité à un ou plusieurs destinataires. L'en-tête d'un paquet de données CloakShield renferme la clé publique Enigma de l'expéditeur et les hashs de clés publiques des destinataires.

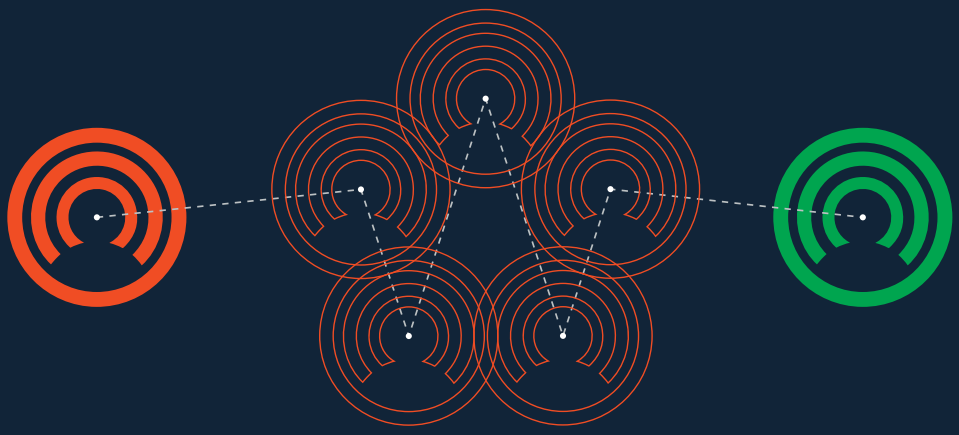
L'en-tête CloakShield contient un hash de vérification, créé en utilisant la clé publique de l'expéditeur et les données brutes non chiffrées. Ce hash est vérifié lors du chiffrement des données CloakShield pour s'assurer que les informations du destinataire dans l'en-tête correspond à la clé de chiffrement et que les données n'ont pas été modifiées.



LE ROUTAGE EN OIGNON CLOAKSHIELD

Le routage en oignon est une technique (utilisée par TOR) pour avoir une communication anonyme sur un réseau informatique. Dans un réseau en oignons, les messages sont encapsulés dans les couches de chiffrement, analogues aux couches d'un oignon. Les données chiffrées sont transmises à travers une série de nœuds de réseau appelés routeurs oignon, chaque "écorce" forme une seule couche, divulguant la prochaine destination des données.

Lorsque la couche finale est déchiffrée, le message arrive à sa destination. L'expéditeur reste anonyme car chaque intermédiaire ne connaît que l'emplacement des nœuds se situant juste avant et après.



L'ANALOGIE DU ROUTAGE EN OIGNON

L'ajout de la fonctionnalité «routage en oignon» au réseau Enigma (en utilisant CloakShield) permet aux nœuds de communiquer indirectement pour contourner les analyses de trafic. Cela compromet les tentatives d'identification permettant de savoir quels nœuds communiquent entre eux ou quels nœuds soumettent des transactions au réseau CloakCoin. Quand un nœud Enigma souhaite communiquer avec un autre nœud Enigma, il sélectionne un certain nombre d'autres nœuds Enigma qui se relaient pour établir la communication. Chaque couche chiffrée ne peut être déchiffrée par le relais prévu (pour lequel la couche spécifique a été chiffrée).

Après avoir déchiffré une couche, le relais transmet les données au prochain nœud relais. Ce routage continue ainsi jusqu'à ce que les données parviennent au destinataire prévu et que toutes les couches aient été déchiffrées à tour de rôle par les nœuds relais sélectionnés. Parce que le réseau Enigma est de nature autonome, les nœuds de sortie ne sont pas requis et CloakShield s'assure qu'il n'y a aucun risque qu'un noeud relais puisse lire ou modifier les données chiffrées.

4. LES ADRESSES CACHÉES

Cloak utilise le système Enigma pour faciliter les transactions privées / sécurisées

CLOAKSHIELD - LES COMMUNICATIONS ENTRE NOEUDS

Au démarrage, chaque wallet Cloak génère une paire de clés [NID_ secp256k1] (Cloaking Encryption Key: CEK) pour lui permettre d'obtenir des secrets ad hoc en utilisant ECDH avec leur clé privée et la clé publique du destinataire. Ce moyen de communication constitue la base de toutes les communications entre les nœuds relatifs à Enigma. Veuillez vous référer à "src / enigma / cloakshield.h / .cpp" pour plus d'informations à ce sujet. Cette communication chiffrée basée sur ECDH est également utilisée pour les données par routage en oignon, qui sont gérées par CloakShield.

Lorsque le routage en oignon est activé, le client tente de construire une route en oignon valide pour les données en utilisant la liste des pairs prévus par Enigma. Le nœud peut ne pas avoir de connexion directe avec les pairs Enigma, mais ce n'est pas nécessaire avec CloakData (transferts de données pour le routage avec CloakShield) puisque les paquets sont relayés en peer-to-peer (pair-à-pair). Une route en oignon sera typiquement constituée de 3 routes distinctes vers le noeud de destination, avec 3 sauts de nœud par route. Plusieurs itinéraires sont utilisés pour faire face à des situations où un nœud de routage se retrouve en mode hors connexion.

Les nœuds envoient régulièrement aux intermédiaires une notification Enigma (src / enigma / enigmaann.h) pour faire savoir leurs services pour le routage en oignon. D'autres nœuds présents sur le réseau stockent les notifications (jusqu'à leur expiration ou leur remplacement par une mise à jour) et les utilisent pour construire les routes en oignon.

EXEMPLE DE TRANSACTION D'UNE ADRESSE CACHÉE

Lorsqu'un noeud envoie une transaction Enigma à une adresse cachée, voici ce qui se produit:

1. L'expéditeur génère des entrées pour couvrir le montant envoyé, la récompense Enigma et le frais de réseau (De 1% pour 0 coins à 0,2% pour 1000 coins et plus).

2. L'expéditeur crée un objet CloakingRequest (contenant une valeur unique et cachée pour cette requête).

3. L'expéditeur crée entre 2 et 4 adresses cachées de paiement unique en utilisant l'adresse cachée des bénéficiaires et divise le montant envoyé au hasard entre les adresses.

4. L'expéditeur décide du nombre de participants qui seront utilisés. De 5 à 25 participants peuvent être choisis (chaque participant obtient 80 à 120% d'une commission Enigma équitablement répartie).

5. L'expéditeur fait passer en onion les requêtes Cloak au réseau. La requête comporte le "montant à envoyer" de manière à ce que les Cloakers puissent savoir combien réserver.

6. Le Cloaker récupère la CloakRequest (la requête Cloak) et décide de participer.

7. Le Cloaker fournit X entrées à l'expéditeur ainsi qu'une adresse et un hash cachés (pour leur retour de monnaie).

8. Le Cloaker envoie la CloakingAcceptResponse à l'expéditeur. Ce qui contient une adresse et une valeur cachées ainsi que des entrées de transaction.

9. L'expéditeur attend jusqu'à ce que suffisamment de Cloakers aient accepté.

10. L'expéditeur crée une transaction Enigma en utilisant ses propres entrées et celles du Cloaker. Les entrées sont ainsi mélangées.

11. L'expéditeur crée des transactions de sorties pour tous les Cloakers. Les sorties divisent au hasard leur retour de monnaie et leur renvoie. Cela prévoit également la rétribution pour avoir crée des cloaks, versée aux Cloakers.

12. L'expéditeur crée ses propres retours de monnaie pour les transactions Enigma. Ce sont des adresses de paiement cachées et uniques.

13. L'expéditeur calcule les frais de transaction du réseau et les soustrait à ses propres retours de monnaie.

14. L'expéditeur envoie la transaction Enigma aux Cloakers pour signature.

15. Les cloakers vérifient la transaction pour s'assurer que leurs entrées sont présentes et correctes et qu'il existe des adresses de paiement ponctuelles liées à l'une de leurs adresses cachées avec un paiement qui dépasse le montant d'entrée.

16. Les Cloakers signent ou rejettent la transaction et envoient les signatures à l'expéditeur.

17. L'expéditeur rassemble les signatures et transmet la transaction signée et finalisée au réseau.

18. Les nœuds analysent les transactions entrantes pour les paiements cachés et les paiements Enigma et repère tout paiement ou retour de monnaie. Les keypairs (paires de clés) et les adresses sont créées pour tout paiement de contrepartie ainsi que pour les clés / adresses créées et sont ensuite enregistrées dans le wallet local.

5. LE FUTUR D'ENIGMA – PROCHAIN DÉVELOPPEMENT

Enigma est au coeur de CloakCoin et continuera à être développé et amélioré au fur et à mesure de notre progression sur CloakCoin. Voici quelques-unes des caractéristiques conçues pour les modifications à venir:

AMÉLIORER L'ALGORITHME PROOF-OF-STAKE

Le Proof of Stake / PoS (Preuve de participation) est un procédé pour sécuriser un réseau de crypto-monnaie qui repose sur des utilisateurs qui fournissent des coins pour être en mesure de signer des blocs.

À la longue, la probabilité de signer des blocs devient proportionnelle au nombre de coins possédés. Une personne qui possède 1% de la production totale de coins sera en mesure de signer 1% de tous les blocs Proof of Stake. En comparaison avec la méthode du Proof of Work (Preuve de travail), le Proof of Stake nécessite beaucoup moins de puissance de calcul et donc moins d'énergie consommée.

LA MATURATION DU COIN (COIN AGE) ET LE PROOF-OF-STAKE LINÉAIRE

Le concept du Coin Age (Maturation du Coin) est fondamental pour la plupart des exécutions du Proof of Stake, y compris celles de CloakCoin. C'est essentiellement un indicateur qui permet de calculer combien de temps une personne possédant des coins les a gardé sans les dépenser ou les déplacer. Dès lors qu'une transaction est terminée, les coins faisant partie de cette transaction commencent à s'accumuler sur Coin Age (qui commence à zéro). Dans sa forme la plus simple, intitulée "linear coin age" (Maturation linéaire de la monnaie), les coins s'accumuleront à chaque minute / heure / année de maturation. Par exemple, une personne qui détient 365 coins pendant 100 jours accumule 36 500 jours de maturation du coin, ou environ 100 années-pièce (une "année-pièce" tient compte des années bissextiles, et donc ce n'est pas exactement 365 jours mais ~ 365,24 jours).

La conception linéaire du Proof-of-Stake a fait l'objet de critiques en ce qui concerne la maturation du coin. Beaucoup soutiennent que ce Proof-of-Stake linéaire favorise l'accumulation des coins (ce qui peut avoir un effet négatif sur le volume des échanges et des transferts). Un autre reproche fait vis-à-vis du Proof-of-Stake linéaire concerne l'effet qu'il peut avoir sur

la sécurité du réseau. Les applications du Proof-of-Stake linéaire souffrent souvent à cause des utilisateurs qui se connectent périodiquement au réseau Cloak pour staker leurs coins, puis se déconnectent une fois que tout le Coin Age ai été détruit.

L'utilisateur attend alors que la maturation du coin se soit reconstituée avant de répéter le processus connection-staking-déconnection. Cela n'assure pas la meilleure sécurité possible pour le réseau, et un algorithme Proof-of-Stake qui récompense le staking fréquent ou constant qui serait plus bénéfique pour CloakCoin et les coins liés au Proof-of-Stake.

Pour s'assurer que les Cloakers Enigma soient récompensés le plus largement possible, Coin Age devrait être retiré de l'algorithme du CloakCoin Proof-of-Stake. Cela garantirait aux Cloakers de recevoir la récompense du staking dans son ensemble ainsi que toutes les récompenses de la création de cloaks Enigma.

L'ajout supplémentaire d'une composante de vitesse dans le calcul des récompenses de staking continuerait à récompenser les nœuds actifs de cloaking Enigma, encourageant les utilisateurs à participer au cloaking Enigma afin d'améliorer la qualité du réseau de cloaking Enigma et d'augmenter leurs intérêts gagnés en plus des récompenses Cloaking gagnées.

En plus d'offrir de plus grandes récompenses aux utilisateurs participant activement, l'algorithme sera amélioré pour le Proof-of-Stake qui fournit à son tour les améliorations susmentionnées à la sécurité du réseau.

LA FUSION OU LA DIVISION DES TRANSACTIONS ENIGMA

Enigma produit actuellement une seule transaction "Cloakée" par transfert. Nous sommes en train de travailler sur une mise à jour de la structure Enigma qui permettra aux transactions multiples d'Enigma d'être réunies dans une super transaction Enigma. Les transactions "cloakées" multiples seront alors efficacement contenues; ce qui fournira un anonymat encore

plus grand pour les utilisateurs de Cloak. Cette extension permettra aux utilisateurs de sélectionner le nombre de transactions Enigma co-opérationnelles dont ils ont besoin en plus du nombre de Cloakers.

Cet ajout reste bien sûr totalement décentralisé, privé et sécurisé.
Une autre amélioration de la transmission d'Enigma est en train d'être étoffée par l'équipe de Cloak concernant la capacité de cloaker une grande quantité de Cloak comme une série de petites transactions Enigma. Pour y parvenir, un utilisateur choisirait la quantité de Cloak à envoyer déjà "cloakée" à une adresse. CloakCoin travaillerait ensuite en arrière-plan pour créer un certain nombre de plus petites transactions Enigma de cette quantité souhaitée; ces transactions pouvant être cloakées et soumises au réseau Cloak sur une période déterminée. Ce système de dosage sera compatible avec les transactions Enigma "fusionnées"et apportera une plus grande protection pour les transferts lors d'une création de Cloak.

6. FAQ

Q. COMMENT LES CLOAKERS PERMETTENT-ILS LA TRANSACTION ENIGMA?

Les Cloakers fournissent une ou plusieurs entrées qui sont utilisées pour "cloaker" (masquer) l'entrée de l'expéditeur. Les Cloakers utilisent également une série d'adresses de retour qui renvoient leur entrée et récompensent également le Cloaker avec une commission. Les adresses de retour sont soigneusement choisies afin d'établir une priorité aux adresses selon l'activité. En conséquence, il sera beaucoup plus difficile pour quiconque effectue une analyse sur la blockchain d'identifier le vrai résultat d'une transaction Enigma. Le système Enigma vérifiera également l'adresse cible afin que les sorties "cloakées" ("masquées") ressemblent le plus possible à la véritable sortie.

Q. COMBIEN DE TEMPS FAUT-IL AUX TRANSACTIONS ENIGMA POUR ETRE EFFECTUEES?

Les transactions Enigma sont actuellement réparties en une minute. Les nœuds Cloaking, qui aident à “masquer” une transaction Enigma, réservent les fonds nécessaires jusqu'à ce que la transaction Enigma soit effectuée ou que le temps alloué expire. Dans le cas d'une transaction Enigma expirée ou avortée, les fonds sont déverrouillés localement pour une réutilisation.

Q. DE QUELLE FAÇON ENIGMA INFLUENCE LE STAKING?

Tous les coins utilisés lors une transaction Enigma (en tant qu'expéditeur ou cloaker) auront leur coin-age (maturation du coin) remis à zéro. Il convient toutefois de noter que la participation au Cloaking (Création de Cloaks) devrait produire un rendement beaucoup plus élevé que le staking. L'équipe Cloak travaille à la révision de l'algorithme Enigma pour la prochaine sortie hardfork (Enigma 1.1). Veuillez vous référer à la section 5 - “Le futur d'Enigma - Prochain développement - pour plus de détails.

Q. EST-IL NÉCESSAIRE D'AVOIR UN CERTAIN NOMBRE DE CLOAKS DANS MON WALLET (PORTEFEUILLE NUMÉRIQUE) POUR POUVOIR ÊTRE UN CLOAKER ENIGMA?

Vous pouvez offrir vos services pour la création de Cloaks (Cloaking) quel que soit le solde de votre wallet CloakCoin. Lorsque le Cloaking d'Enigma est activé, CloakCoin réserve une partie de votre solde pour participer à la création de Cloaks Enigma, pour laquelle vous gagnez une récompense de cloaking (camouflage). Le montant de la réserve est par défaut d'environ 50%, mais cette valeur peut être ajustée par l'utilisateur. La valeur est choisie de façon aléatoire pour empêcher l'établissement de liens entre les notifications Enigma et le solde de Cloaking annoncé.

Il faut souligner que les wallets avec un solde plus élevé ont une plus grande chance d'être choisi pour être un Cloaker car ils sont plus susceptibles d'avoir le solde de camouflage (Cloaking) disponible pour les transactions plus importantes d'Enigma.

Q. QUELLE PROTECTION Y-A T IL CONTRE UNE ATTAQUE EN TEMPS RÉEL LORSQUE QUELQU'UN CHERCHE DES ENTRÉES ET DES SORTIES IDENTIQUES AU SEIN DE LA BLOCKCHAIN?

Les transactions Enigma regroupent les sorties et sont assurées d'avoir plusieurs quantités équivalentes de sortie pour "cloaker" (masquer) la sortie du destinataire.

Q. L'AUTEUR D'UNE TRANSACTION ENIGMA PEUT-IL ÊTRE IDENTIFIÉ EN EXAMINANT LE SCRIPT DE SIGNATURE POUR DÉTERMINER L'ORDRE DE SIGNATURE?

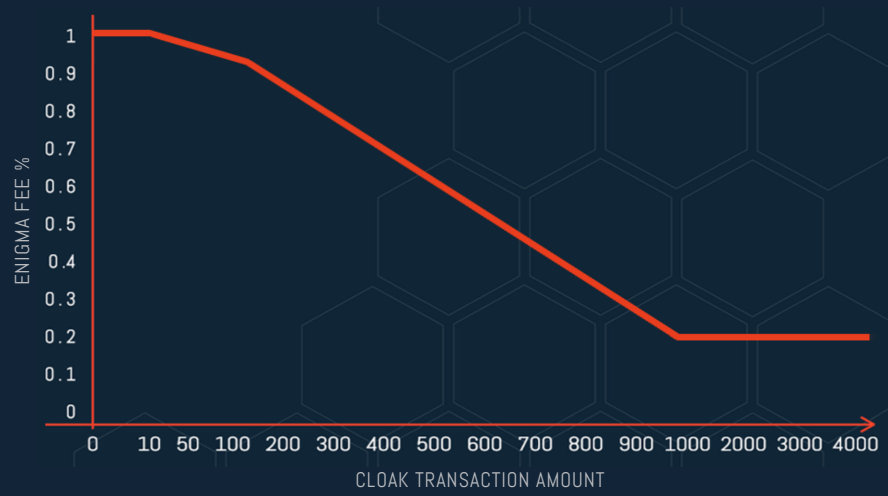
Non. Au cours d'une signature, l'ordre des signatures est aléatoire lors de la combinaison des signatures. Ce sont l'expéditeur et les Cloakers participants qui le font.

Q. QUELS SONT LES FRAIS POUR UNE TRANSACTION ENIGMA?

De 1% pour 0 coin à 0,2% pour 1000 coins et plus. Cette récompense est faite pour les nœuds Enigma qui aident à masquer une transaction Enigma. Les frais sont ensuite mélangés à la transaction et partagés entre les cloakers. Ce n'est pas seulement une récompense pour les participants mais elle est également utilisée pour aider à déterminer le montant de la transaction incroyablement difficile. Chaque participant reçoit 80-120% d'une transaction énigme également divisée.

Q. COMMENT LA COMMISSION ENIGMA EST-ELLE FIXÉE?

Les commissions Enigma sont en pourcentage et facturées par transaction à ces taux:



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. EST-CE QU' ENIGMA NÉCESSITE UN HARD-FORK DU RÉSEAU CLOAK?

Les anciens comptes de CloakCoin géreront les transactions Enigma sans problèmes mais ils ne seront pas en mesure de les créer ou de participer à leur “cloaking” (camouflage). La prochaine révision d'Enigma, cependant, nécessitera un hard-fork en raison des changements de l'algorithme implémenté du Proof-of-Stake et le support de script supplémentaire opcodes pour les caractéristiques du marché (tel que Block Escrow).

Q. QUEL EST LE NOMBRE MAXIMAL DE CLOAKERS QUI PEUVENT PARTICIPER À UNE TRANSACTION ENIGMA?

Le nombre maximum de Cloakers est fixé à 25. Le système Enigma est flexible et ce nombre peut facilement être étendu.

Q. COMMENT ENIGMA PROTÈGE CONTRE LES “MAUVAIS ACTEURS”?

Le système Enigma offre une protection DDoS (attaque par déni de service) étendue aux nœuds “blacklist” (liste noire) pour la durée d'une session. Si un noeud Enigma refuse à plusieurs reprises de signer, ils seront exclus des invitations d'Enigma Cloaking pour le reste de la session en cours.

Nous étudions actuellement des méthodologies supplémentaires pour pénaliser davantage les nœuds Enigma non coopératifs et mettront

probablement en œuvre un système qui exige des Cloakers d'entiercer des frais minimes et remboursables qui pourraient être réclamés à titre de pénalité dans les cas où un nœud tente de bloquer une transaction Enigma en refusant de signer la transaction finalisée.

Il convient de noter que si des nœuds malveillants peuvent tenter de ralentir une transaction Enigma, ils ne sont pas en mesure de voler ou de détourner des fonds.

Q. COMMENT LES TRANSACTIONS FURTIVES D'ENIGMA SONT-ELLES DÉTECTÉES/REÇUES?

Toutes les transactions entrantes sont analysées. Les transactions furtives sont analysées d'abord (en utilisant la pubkey éphémère par défaut contenue dans un fichier aléatoire OP_RETURN Sortie TX). Les transactions Enigma sont ensuite analysées. Les transactions Enigma utilisent également la pubkey éphémère standard mais les paiements se servent d'une étape supplémentaire impliquant une autre clé dérivée. Les sorties Enigma sont générées en utilisant un hash de la pubkey éphémère, un hash d'adresse furtive et privée ainsi que l'indice de sortie.

Lors de la recherche de transactions Enigma, les adresses de paiement à indice zéro sont générées pour chaque adresse furtive appartenant à un utilisateur[HASH (ephemeral_pubkey, hash_stealth_secret, 0)]. Si une correspondance est trouvée pour l'indice zéro d'une adresse furtive, des adresses supplémentaires sont créées pour les autres index [num_tx_outputs] et ceux-ci sont analysés pour détecter les paiements. Veuillez vous référer à FindEnigmaTransactions dans wallet.cpp pour plus d'informations.

Une méthode de lecture semblable est employée par les cloakers avant de signer une transaction Enigma pour s'assurer qu'ils sont correctement indemnisés. Veuillez vous rendre à > GetEnigmaOutputsAmounts dans wallet.cpp pour de plus de détails.

7. RÉFÉRENCES

[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