The Pirate Code

Le livre blanc

Résumé

Une cryptomonnaie entièrement privée ainsi qu'une blockchain provenant de l'écosystème de Komodo. Pirate résout le problème de fongibilité de Zcash par l'élimination de la fonctionnalité de transaction des adresses transparentes dans sa blockchain, qui rend l'usage privé "infaillible". Ce procédé permet à l'utilisateur de disposer d'une base de pièce entièrement shielded dans Pirate chain. En utilisant constamment la technologie "zk-SNARK", les pièces de monnaie Pirate ne laissent aucune trace des métadonnées d'utilisateur dans sa blockchain. Toutes les transactions sortantes autre que les récompenses de blocs de minage et les transactions notariales sont envoyées dans des adresses Sapling blindées, ce qui maximise l'efficacité et l'efficience de la chaîne. Pirate utilise l'algorithme de consensus Equihash PoW provenant de Zcash, avec une couche de sécurité supplémentaire de la preuve de travail retardée de Komodo (dPoW), qui lui fournit une qualité supérieure à celle du BTC sur le niveau de sécurité de la blockchain Pirate.

L'avenir des paiements privés décentralisés est là.

L'avenir des paiements privés décentralisés est là.

SOMMAIRE

Le code PIRATE

La mission de PIRATE

La mission de Pirate est de préserver la vie privée financière des gens dans un système dominé par la transparence des transactions.

Proposition de valeur

Toutes les transactions de la chaîne Pirate sont privées par défaut.

Cela atténue les problèmes de fongibilité que de nombreuses cryptomonnaies possèdent avec l'option de protection de la vie privée dans leur protocole. Ce protocole privé permet aux utilisateurs avec plus d'assurance qu'aucune autorité seront en mesure de "souillés" vos fonds en raison des transactions précédentes, actuellement et dans le futur.

Le coin Pirate est totalement décentralisé

Il n'y a pas de troisième partie qui se charge de vos fonds, à aucun moment. Les transactions privées sont confirmées de manière fiable sur la blockhain ce qui signifie que vous n'avez pas besoin d'une tierce partie pour vérifier que vos transactions sont valides, le code Pirate s'en charge pour vous.

Pirate permet un transfert de valeur sure et rapide.

La chaîne Pirate est sécurisée par un mécanisme plus difficile à crack que le Bitcoin, il s'appelle le "delayed Proof-Of-Work" (dPoW). Les frais d'utilisation sont très peu élevés aussi bien pour le client que le fournisseur. De plus, il n'y a aucune possibilité de frauduleux "chargebacks", aucun fonds erroné pour les périodes de vérification, les transactions sont confirmées et sécurisées en quelques minutes.

Ces caractéristiques peuvent sauver les commerçants et les vendeurs à travers le monde en supprimant les frais de transactions.

Pirate utilise le protocole de confidentialité le plus strict.

Le protocole de protection de la vie privée zk-SNARKS, très avancé et respecté, permet de ne pas exiger que les données de vos transactions soient visibles par le public. Ceci est considéré par beaucoup de développeurs comme l'une des plus importantes et efficaces méthodes pour cacher vos données financières sur la Blockchain.

Pourquoi mettre l'accent sur la vie privée ?

Les crypto offrent de nombreux avantages aux utilisateurs et aux entreprises, mais cela ne devrait pas se faire au détriment de la confidentialité financière.

Aujourd'hui, les monnaies FIAT sont déjà en train de faire un exode massif vers les systèmes digitaux (Japparova en Rupeika-Apoga 2017). La crypto a montré qu'il pouvait offrir de nombreux avantages pour les entreprises, tels que des économies de coûts en termes d'honoraires et notamment la vitesse de transaction. A notre avis, les utilisateurs méritent leur confidentialité dans leurs transactions.

Pourquoi montrer au propriétaire du magasin la taille de votre patrimoine ou vos habitudes de consommation ?

La confidentialité financière peut donc être nécessaire pour toutes les parties qui veulent accepter la cryptomonnaie, comme les vendeurs, les distributeurs, les commerçants, les acheteurs, les fournisseurs, les prestataires de services et les clients. Les entreprises peuvent assurer à leurs clients et à elles-mêmes que les deux parties de la transaction bénéficieront de la meilleure combinaison de confidentialité, de rapidité et de réduction des coûts grâce à l'utilisation de Pirate.

L'équipe

En tant que véritable cryptomonnaie décentralisé, Pirate accueille les développeurs et les contributeurs ayant toutes sortes de compétences.

Déjà plus de 30 contributeurs ont aidé à la croissance et au développement de Pirate Chain depuis ses débuts. Les développeurs travaillent en équipe de manière cohérente pour apporter les connaissances et l'expérience de toutes les parties dans la crypto-sphère. Dans notre groupe diversifié, il y a toujours une personne qui sait comment accomplir une tâche nécessaire, ou une personne qui a un lien avec quelqu'un qui le peut.

Pirate à réaliser de nombreuses premières innovations dans l'industrie de la cryptomonnaie en matière de protection de la vie privée (voir roadmap) et Pirate continuera à travailler avec des tiers sur des techniques innovantes afin de faciliter la protection de la vie privée pour tous.

Introduction

Cryptomonnaie

Depuis la publication du célèbre livre blanc écrit par Satoshi Nakamoto en 2008, Bitcoin est devenu un actif numérique de plusieurs milliards de dollars. Un certain nombre d'autres cryptomonnaies ont vu le jour depuis lors, tentant de combler le vide d'une pléthore de cas d'utilisation, avec leurs propres communautés respectives. L'utilisation des cryptomonnaies comme moyen de paiement est l'un des cas d'utilisation les plus populaires et aussi le but principal pour lequel Satoshi a écrit le livre blanc. L'objectif de Bitcoin est de permettre à chacun de transférer de la valeur n'importe où dans le monde, à tout moment et instantanément, en utilisant une connexion internet de manière "peer-to-peer". Bitcoin utilise un

grand livre distribué pour faciliter et enregistrer les transactions dont la véracité est déterminée par l'algorithme de consensus preuve du travail. (PoW).

Confidentialité

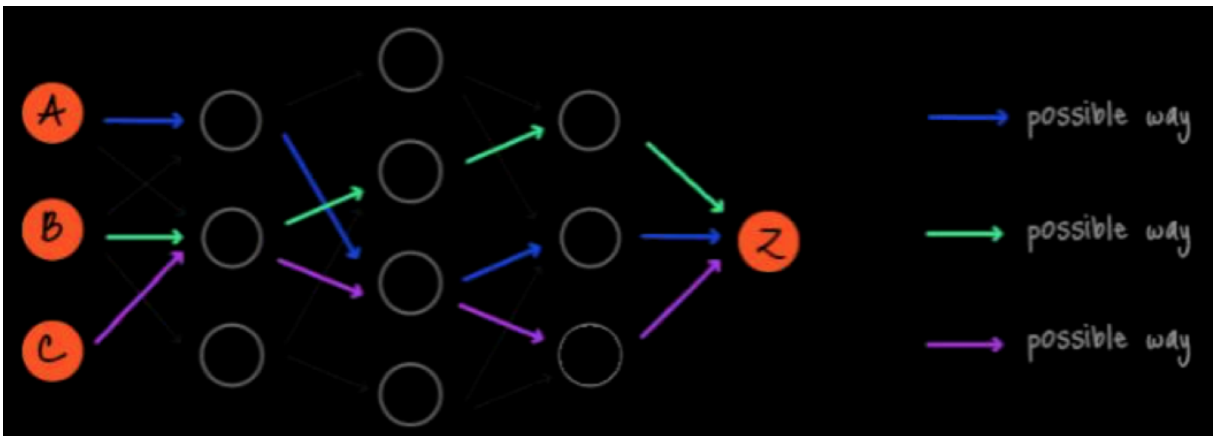
L'une des grandes préoccupations concernant l'utilisation de cette technologie est la capacité des observateurs à analyser votre comportement de dépense et votre situation financière (Moser 2013). Cela compromet grandement la confidentialité financière de l'utilisateur. Un certain nombre de protocoles de cryptomonnaie ont été développés afin d'améliorer les aspects de confidentialité du Bitcoin. Les protocoles les plus notables qui ont été développés jusqu'à présent sont CryptoNote (Van Saberhagen 2013) et ZeroCash (Sasson et al.2014). Le premier protocole utilise les "Ring confidential signatures", tandis que le second utilise le "zero-knowledge proofs" pour obscurcir les transactions et les soldes de comptes, plus de détail à ce sujet par la suite. Les deux protocoles ont leurs avantages et leurs inconvénients. Ce livre blanc traite de la façon dont Pirate (ARRR) tente d'améliorer l'aspect de la confidentialité des paiement décentralisés actuels.

Principaux inconvénients des protocoles de paiement décentralisé actuels.

Monero Ring CT signatures scheme

Monero est un fork de Bytecoin basée sur le protocole CryptoNote qui utilise un schéma de Ring Signature dans ses transactions combiné avec des stealth addresses, des adresses uniques aléatoires pour chaque transaction au nom du destinataire. Les Ring Signatures rendent de plus en plus difficile la traçabilité de l'expéditeur en fonction de la taille de la Ring. Toutefois, cela laisse aux parties la possibilité d'analyser les données disponibles à l'aide d'outils d'analyse sophistiqués, maintenant ainsi qu'à l'avenir.

En raison de l'utilisation des Ring Signatures, l'analyse de la blockchain Monero est difficile, comme le montre la figure 1.



Source : https://cryptonote.org/inside#untraceable-payments

Il est de plus en plus difficile de trouver le bon expéditeur avec des Ring de plus grande taille. La taille de la Ring est le nombre total de signataires possibles, y compris le vôtre, ce qui détermine à son tour la complexité et la difficulté de trouver "la réelle sortie". Un numéro de taille de Ring plus élevé assure donc un niveau d'intimité plus élevé qu'un numéro plus bas. Cependant, il n'est pas conseillé de réutiliser un numéro de taille de Ring reconnaissable pour ne pas se démarquer des autres transactions [3].

Le problème fondamental des méthodes de mélange de pièces est que les données de transaction ne sont pas cachées par le cryptage. RingCT est un système de dissociation où l'information est encore visible dans la blockchain. Gardez à l'esprit qu'une vulnérabilité pourrait être découverte à un moment donné dans le futur, ce qui permet la traçabilité puisque la blockchain de Monero fournit un enregistrement de chaque transaction qui a eu lieu.

L'implantation des adresses protégées de Zcash et les types de dépenses

Zcash, une implémentation du système de paiement anonyme décentralisé ZeroCash, ajouté à un cela un système de paiement

sécurisé par le zero-knowledge (zk-SNARK) au système de paiement transparent existant utilisé par Bitcoin (Hopwood et al. 2016). L'utilisation de paiements shielded ou non-shielded est laissée au libre choix de l'utilisateur. Le pourcentage de transactions shielded est supposé augmenter car la récente mise en oeuvre de "Sapling" par Zcash ne rend le traitement des transactions shielded qu'une fraction plus intensive en calcul que celui des transactions non-shielded (Bowe 2017). Malheureusement, le pourcentage relativement élevé de transaction et de soldes non-shielded nuit à la fongibilité des pièces car il est possible de lier des transactions lors d'activités de paiement "privées" et donc éventuellement de les relier au mélange des pièces. C'est notamment le cas lors d'une "transaction aller-retour", c'est à dire, l'envoi du nombre exact de pièce d'une adresse transparente (t-addr) à une adresse shielded (z-addr) et de retour à une autre adresse transparente (Quesnelle 2017). Nous nous référons dans ce papier à ce phénomène comme le "problème de fongibilité".

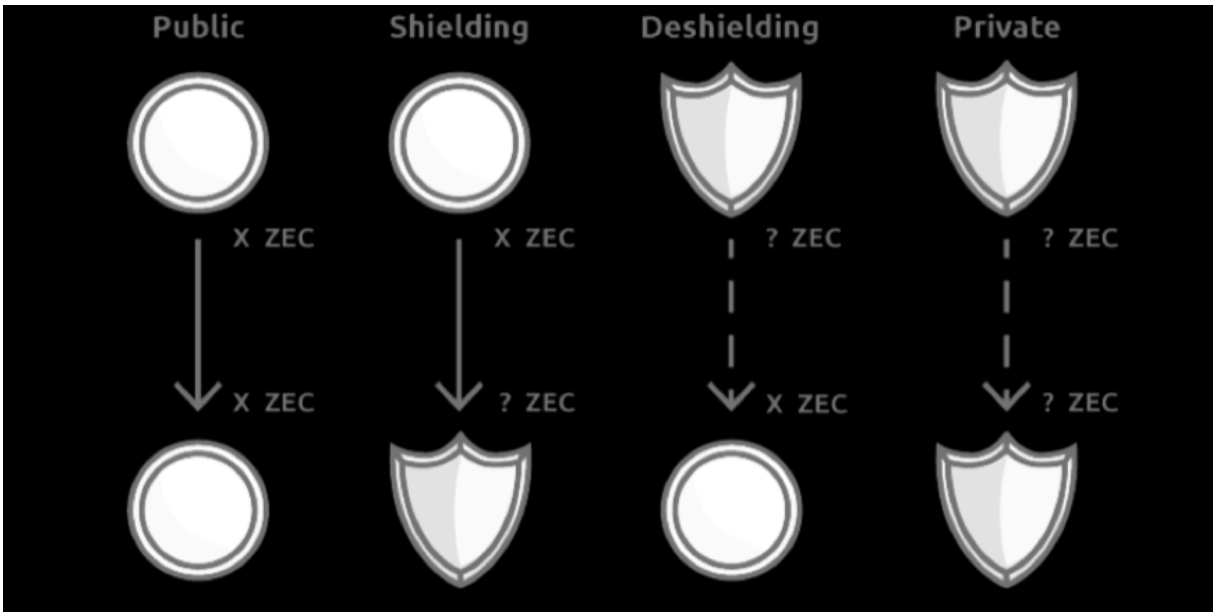


Figure 2 à 4 options pour dépenser du Zcash.
Source : https://z.cash/blog/sapling-transaction-anatomy/

Comme le montre la Figure 2, les utilisateurs de Zcash ont la possibilité d'effectuer 4 types différents de transactions dans le protocole Zcash actuel. Le fait de pouvoir envoyer une adresse

publique à une adresse protégée et vice versa met grandement en danger la fongibilité des pièces de monnaie. Il est possible d'identifier des modèles de mélange de pièces parmi les différents types de transactions lorsque les utilisateurs renvoient des pièces à des adresses transparentes, comme c'est le cas dans les cas suivantes : les " transactions aller-retour ", car il a été démontré que ce comportement présente une forte capacité de liaison (Quesnelle 2017).
Les mises à niveau de performance de Sapling ont malheureusement un coût en termes de confidentialité car les transactions Sapling révèlent plus de métadonnées que les " anciennes " opérations "JoinSplit". Les transactions en pointillés indiquent le nombre d'entrées et de sorties utilisées. Cette fonctionnalité augmente les options permettant de différencier les types de transaction, d'analyser les données de transaction et éventuellement d'identifier le comportement lié au mixage.
Pour réduire ou éliminer ce risque, il est important soit de réduire l'utilisation d'adresses transparentes, soit de simplement les désactiver dès le début dans une nouvelle chaîne de blocage telle que Pirate.

Notre solution

Pirate a pour objectif d'améliorer considérablement la confidentialité et la sécurité de Monero et de résoudre le "problème de fongibilité" de Zcash. Pour ce faire, la chaîne Pirate n'accepte que les transactions blindées "Sapling" (z-tx), à l'exception des récompenses minières et des notaires, comme expliqué dans la section dPoW. De plus, la chaîne Pirate est sécurisée par le mécanisme de preuve du travail retardé, ce qui rend ses caractéristiques de confidentialité et de sécurité actuellement inégalées dans l'industrie de la blockchain en comparaison aux pièces de confidentialité existantes.

PIRATEchain : Confidentialité, fongibilité et sécurité

29 août 2018 — L'appel de l'anonymat total

Pirate a commencé le 29 août en Discorde comme une idée d'une pièce 100% zk-SNARKS. Le travail de développement de jl777c sur les asset chain de Komodo, a permis de renforcer l'utilisation des transactions protégées en ajustant les paramètres de l'asset chain dans une nouvelle asset chain (Grewal 2018). Une asset chain est un fork de Komodo qui devient une véritable Blockchain indépendante. Pirate a d'abord commencé comme une expérience pour observer si les z-transactions forcées fonctionneraient, mais la communauté a rapidement réalisé son potentiel après que jl777c ait implémenté avec succès la preuve du travail retardée, rendant Pirate totalement opérationnel.

Komodo — Fork de Zcash — zk-SNARKs

Pirate est une asset chain de l'écosystème de la plate-forme Komodo. Le projet Komodo se concentre sur l'autonomisation des entrepreneurs de la blockchain et de l'utilisateur moyen de cryptomonnaie avec la liberté et la facilité d'utilisation grâce à la technologie de la blockchain (Lee 2018). Komodo a commencé comme un fork de la très populaire pièce de monnaie de confidentialité, Zcash. Le projet Zcash lui-même est un fork du Bitcoin. Ainsi, toutes les fonctionnalités conçues par Satoshi Nakamoto dans le protocole Bitcoin sont également disponibles dans Komodo qui conserve les mêmes caractéristiques de confidentialité inhérentes à Zcash. Parmi ces caractéristiques figurent les paramètres Zcash et la technologie zk-SNARK qui est l'une des formes les plus puissantes de protection de confidentialité dans les blockchain existantes, car la confidentialité fournie est permanente.

Cette affirmation est même soulignée par le représentant principal de Monero, Riccardo “fluffypony” Spagni :

“Les zkSNARKs de ZCash offrent des caractéristiques d’intraçabilité beaucoup plus fortes que celles de Monero (mais un ensemble de données privées beaucoup plus petit et des risques systémiques beaucoup plus élevés).

Komodo asset chain

Une asset chain (officiellement une chaîne parallèle) est une blockchain créée indépendamment qui hérite de toutes les fonctionnalités de Komodo comme la compatibilité BarterDEX, le Zero Knowledge Privacy et le delayed Proof-of-Work, mais qui possède également de nombreuses spécifications personnalisées telles que le costum coin supply et un port RPC personnalisé. D’autres fonctionnalités personnalisées sont actuellement en cours d’ajout (PTY X 2018).
D’autres exemples d‘asset chain Komodo tel que, Bitcoin Hush (BTCH), ChainZilla (ZILLA), DEX, Equalizer (EQL), KMDice, Monaize (MNZ), PUNGO, REVS, SuperNET, Utrum et ZEX.

z-transactions forcées

La meilleure solution au “problème de fongibilité” est de désactiver la possibilité d’envoyer des fonds aux adresses transparentes, à notre avis. Cela élimine l’existence de transactions transparentes et des soldes transparents, qui sont souvent la cause première de la diminution de la fongibilité. Cité par le développeur principal de Zcash lui-même en réponse à l’article intitulé “On the linkability of Zcash transactions” de Jeffrey Quesnelle :

“Ma réponse est que nous allons plutôt interdire les transactions non protégées. Encore plus simple.”

Delayed Proof-of-Work : Maximum de sécurité et de flexibilité

Qu'est-ce que le Delayed Proof-of-Work ?

La preuve différée du travail (dPoW) provient de Komodo et fournit une forme unique et innovante de sécurité qui est aussi forte que le réseau auquel elle s'attache, mais qui n'exige pas le coût de fonctionnement de ce réseau. La preuve de travail différée est une solution qui utilise plusieurs méthodes existantes dans un système de consensus hybride unique qui est aussi économe en énergie que le Proof-of-Stake (PoS), tout en étant sécurisée par le Proof-of-Work (PoW) du Bitcoin. Les utilisateurs qui construisent des blockchain (asset chain) dans l'écosystème Komodo peuvent choisir d'avoir un block-hash, servant de "snapshot" de leur propre blockchain insérée dans la blockchain principale Komodo. De cette manière, les enregistrements de l'asset chain sont indirectement inclus dans le bloc-hash de Komodo qui est poussé sur la blockchain du réseau le plus fort (actuellement Bitcoin).

Ainsi, la technologie dPoW permet même aux blockchain les plus faibles de bénéficier du taux de hachage de Bitcoin, ce qui rend l'utilisation de l'énergie de Bitcoin plus écologique car elle sécurise l'écosystème entier de la technologie dPoW en plus de lui-même (Jl777c 2016). Outre Pirate, dPoW a été implémenté avec succès dans un grand nombre d'asset chain telles que Game Credits, Einsteinium (EMC2), Pungo et HUSH entre autres (Komodostats 2018)

Quels sont les mécanismes à l'origine du delayed proof-of-work (dPoW) ?

Le service de sécurité de Komodo est assuré par des noeuds notariaux qui sont nécessaires pour enregistrer les hachures en bloc sur la blockchain Bitcoin, appelée notarization (Figure 3). L'authentification notariale implique la création d'une transaction bitcoin signée par un

groupe contenant le plus récent bloc-hash de Komodo, signé par une combinaison inconnue de 33 des 64 noeuds notariaux (Jl777c 2016). Les Block-hashes de la chaîne Pirate sont insérés dans la blockchain Komodo de manière opportune et en utilisant la même méthode. De cette manière, même une seule copie survivante de la blockchain principale de Komodo permettra à tout l'écosystème des asset chain d'écraser toute tentative de modification par un attaquant. Les noeuds notariaux paient les frais de transaction Bitcoin pour l'authentification de la Blockchain Komodo. Les frais de transaction bitcoin pour les noeuds notariaux sont compensés par des récompenses de bloc et des frais de transaction de la chaîne de blocs Komodo allant vers les noeuds notaires. On s'attend donc à ce que les intérêts financiers des parties prenantes votent pour des noeuds notariaux avec lesquels les parties prenantes sont à l'aise. Ils sont 64 nœuds notariaux, largement répartis en élection et devraient représenter de manière optimale un écosystème décentralisé, ce qui rend tout type d'attaque de 51% hautement improbable.

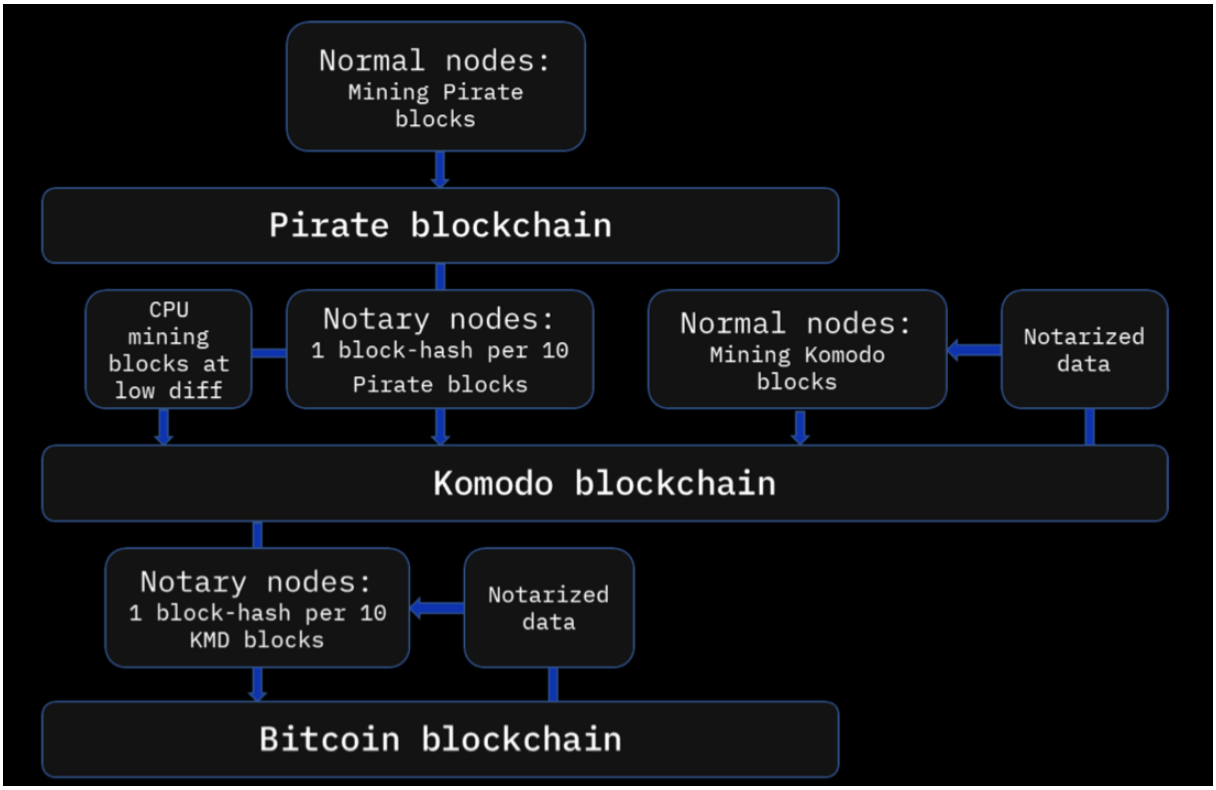


Figure 3 Représentation schématique de la preuve de travail retardée.

Donc, pour attaquer Pirate, l'attaquant aurait besoin de détruire :

- Toutes les copies existantes de Pirate chain;
- Toutes les copies de la chaîne principale de Komodo;
- Le réseau de sécurité PoW (Bitcoin) dans lequel les données notariées de la chaîne de blocs Komodo sont insérées.

De plus, les noeuds notariaux ont la liberté de passer du processus d'authentification à un autre réseau PoW si un changement dans les taux de hachage entre les grandes blockchains se produit à l'avenir. La Preuve du Travail Retardée offre à Pirate une sécurité supérieure au niveau Bitcoin, tout en évitant les coûts financiers excessifs et les coûts non écologiques. Grâce à la flexibilité de dPoW, il offre une nature plus flexible et adaptative que Bitcoin lui-même.

Exemple d'attaque sur la blockchain

Il existe un certain nombre d'exemples qui soulignent la nécessité d'un mécanisme comme la preuve différée du travail (dPoW) :

En avril 2018, un bug dans le mécanisme de reciblage des algorithmes de Vergecurrency (XVG) a été exploité au moyen d'une attaque à 51%. En utilisant des horodatages usurpés, le besoin d'un algorithme différent pour chaque bloc a été contourné. Les hackers ont pu soumettre des blocs à la chaîne à une vitesse d'extraction de 1 bloc par seconde, minant ainsi 99% des blocs des pools légitimes et leur faisant perdre de l'argent (Ocminer 2018a). Au cours du mois de mai 2018, la même attaque s'est produite mais avec une approche différente : les hackers ont envoyé un bloc avec l'algorithme Scrypt contenant un horodatage usurpé suivi d'un bloc avec l'algorithme Lyra2re contenant un horodatage usurpé, en répétant ce processus et réduisant ainsi la difficulté, les hackers ont pu extraire plusieurs blocs par minute (Ocminer 2018b).

Le 16 mai 2018, Bitcoin Gold a été attaqué par un acteur inconnu qui a réussi à voler plus de 388,000 BTG à partir des échanges de devises cryptographiques, la totalité des pièces valaient 17.5 millions de dollars pendant l'attaque (Roberts 2018).

NiceHash offre actuellement une puissance de hachage plus que suffisante pour la location afin d'attaquer un certain nombre de cryptocurrencies de petites et moyennes capitalisations. Le terme "Nicehashable" a été inventé pour la possibilité de louer du hash pour attaquer une pièce de monnaie, des sites ont déjà fait leur apparition pour montrer les opportunités de piratage (EXAKING 2018).

L'intégration et l'activation de Sapling

Sapling intégration

L'intégration de Sapling dans Pirate chain a été un succès grâce à la coopération entre les membres de l'écosystème Komodo, et un remerciement particulier à Mike Toutonghi du projet Veruscoin.

Pirate est synonyme de transactions rapides, bon marché et 100% privées. Sapling est la meilleure version de la technologie zk-SNARKS qui offre cela. Pour cette raison, l'utilisation de Sapling est forcée à partir du 15 février 2019 pour s'assurer que la chaîne fonctionne efficacement et en privé. Les utilisateurs qui possèdent Pirate doivent migrer leurs pièces de monnaie de leur adresse Sprout vers une adresse Sapling avant cette date.

L'heure de l'activation de Sapling était basée sur l'horodatage du bloc vers le 15 décembre, à 1 heure du matin (UTC). La date limite pour la migration de Sprout à Sapling a été fixée au 15 février 2019 afin de créer un sentiment d'urgence et d'impliquer tous les propriétaires de Pirate. Plus la migration est effectuée tôt, meilleure est la situation pour les échanges centralisés et autres applications tierces.

Une application décentralisée (dApp) appelée “zMigrate” qui convertit automatiquement les fonds de l’utilisateur dans les adresses Sprout en une adresse Sapling a été développée par jl777c pour simplifier le processus de migration vers Sapling. Tous les nœuds étaient nécessaires pour achever ce processus avant le 15 février 2019 et les pools ont également fait le saut vers les adresses Sapling après le hard-fork.

La migration vers Sapling

dApp zMigrate est un programme autonome qui interagit avec le deamon “Komodod”. Le dApp enverra Pirate dans les adresses Sprout de l’utilisateur à une adresse transparente randomisée à usage unique dans un maximum de 10K Pirate par transaction. Autant de t-addresses uniques sont créées pour déplacer tous les fonds, la dernière transaction contenant probablement moins de 10K (sauf si les fonds sont divisibles par 10K). Par conséquent, les fonds de chaque t-addr sont envoyés à l’adresse blindée Sapling désignée. De cette manière, l’utilisateur contrôle les fonds tout le temps et le mouvement des fonds transparents aura l’air aussi homogène que possible afin de réduire les dommages causés à la fongibilité de la chaîne. Le résultat du processus est que tous les fonds de l’utilisateur sont transférés de l’ancienne adresse Sprout à l’adresse Sapling de son choix.

Les améliorations techniques de Sapling permettent de développer les caractéristiques suivantes :

- Point-of-Sale integration
- Hardware wallets
- Web Shop Plugins (Fast)
- Wallet mobile grâce à la vérification simple des paiements (zSPV)

Caractéristiques techniques

Pirate chain contient les caractéristiques techniques et caractéristiques suivantes après le 15 décembre :

- L'algorithme de minage : Equihash — Proof-of-Work
- Delayed Proof-of-Work
- Block-time : 60 secondes
- Frais de transactions : 0.0001 ARRR
- Signature de transaction en quelques secondes
- Transaction par seconde : 50–80 TPS
- Envoi jusqu'à 100 adresses en une seule transaction
- Tailles Tx de +-2000 octets avec un maximum de 200kB
- Utilisation de la mémoire de seulement 40 Mo (Rasberry Pi)
- Block size de 4 mB maximum
- Affichage de tout ce qui permet de voir toutes les transactions envoyées d'une adresse assignée.
- Possibilité de générer un nombre "infini" de portefeuille Lite.

Calendrier des émissions

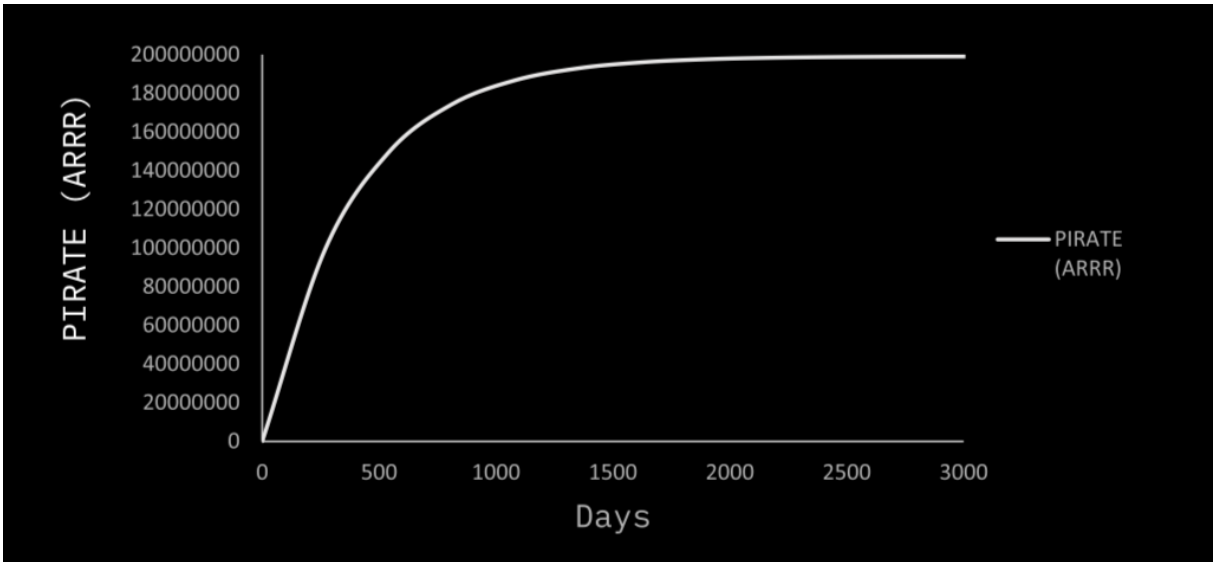


Figure 4 : L'émission des jetons Pirate (ARRR)

Le supply maximum est d'environ 200 millions de PIRATE (ARRR).

TOR support

Il est possible d'exécuter Pirate chain sur le réseau TOR et d'obscurcir votre adresse IP, le numéro qui est lié à votre emplacement géographique. En tant qu'utilisateur, vous avez besoin d'un navigateur TOR et des binaires Komodo pour pouvoir exécuter Pirate chain. Un guide étape par étape est disponible sur pirate.black. La demande de support TOR a été partagée avec les développeurs d'Agama Wallet. Une fois fait, la configuration de Tor pour un coin ou une asset chain est très facile.

Support des échanges décentralisés

La communauté n'était pas certaine que les échanges centralisés puissent accepter Pirate dans un premier temps en raison de l'absence d'adresses transparentes. Peu de temps après la création de Pirate, l'équipe a travaillé avec des développeurs et des codeurs pour faciliter l'utilisation des dépôts et retraits d'adresses Z comme une

première mondiale. Cet échange particulier est DigitalPrice et a été lancée avec succès fin octobre 2018.

Feuille de route

Les dates des éléments suivants de Pirate et des développements de tiers (tels que Tortuga) sont des estimations basées sur une base trimestrielle et classées par ordre d'attente.

- TOR browser support — Q3 2018 (complété)
- 100% Z-address payout mining pools — Q3 2018 (complété)
- First Z-address Discord Tip bot — Q3 2018 (complété)
- Facilitate Z-addresses on a CEX — Q3 2018 (complété)
- Paper Wallet — Q4 2018
- Onboarding referrals — Q4 2018
- Pirate Lottery Bot — Q4 2018
- Sapling — Q1 2019
- Pirate Foundation — Q1 2019
- Tortuga (CEX) — Q1 2019
- Z Simple Payment Verification (zSPV) — Q2 2019
- Hardware wallet integrations — Q3 2019

Le guide Pirate

A bord dans PIRATE

Acheter facilement une petite quantité de PIRATE

https://dexstats.info/onboarding.php

Comment miner

https://dexstats.info/piratecalc.php

Pour commencer

https://medium.com/piratechain/how-to-mine-pirate-step-by-step-with-gpu-s-4c98f3dbcf5e

Choisir sa mining pool

https://miningpoolstats.stream/pirate

Gardez un œil sur le hashrate de Pirate

https://dexstats.info/piratehash.php

Acheter et trade des Pirate (ARRR)

Inscrivez-vous à DigitalPrice et échanger des ARRR pour des BTC, ETH ou KMD.

https://digitalprice.io/order?url=arrr-btc (official PIRATE ref. link)

Médias sociaux

Pirate est actif sur Bitcointalk, Discord, Medium, Reddit, SteemIt, Telegram, Twitter et listé sur Coin statistic.

https://coinpaprika.com/coin/arrr-pirate/ https://discord.gg/mBZhZgzhttps://medium.com/@piratechainhttps://www.reddit.com/user/piratechainhttps://steemit.com/@piratechain https://twitter.com/PirateChainhttps://t.me/piratechain

Code source et wallet

Github: https://github.com/PirateNetwork
Agama
Wallet: https://github.com/KomodoPlatform/Agama/releasesPIRATE
GUI wallet: https://github.com/leto/TreasureChest

References

Bowe, S. 2017. “Cultivating Sapling: Faster zk-SNARKs — Zcash Blog”. Zcash Blog.

EXAKING. 2018. “PoW 51% Attack Cost”. 2018. https://www.exaking.com/51.

Grewal, Satinder. 2018. “Satinder’s notes on the PIRATE chain”. 2018. https://blog.komodoplatform.com/pirates-of-komodo-platform-cdc991b424df.

Hopwood, Daira, Sean Bowe, Taylor Hornby, en Nathan Wilcox. 2016. “Zcash protocol specification”.

Japparova, Irina, en Ramona Rupeika-Apoga. 2017. “Banking Business Models of the Digital Future: The Case of Latvia”. European Research Studies 20 (3A). Professor El Thalassinos: 846.

Jl777c. 2016. “Delayed Proof of Work (dPoW) Whitepaper”. Github. 2016. https://github.com/KomodoPlatform/komodo/wiki/Delayed-Proof-of-Work-(dPoW)-Whitepaper.

Kappos, George, Haaroon Yousaf, Mary Maller, en Sarah Meiklejohn. 2018. “An Empirical Analysis of Anonymity in Zcash”. arXiv preprint arXiv:1805.03180.

Komodostats. 2018. “Asset Chains Notarizations Summary”. 2018. https://komodostats.com/acs.php.

Lee, James. 2018. “Komodo: An Advanced Blockchain Technology, Focused on Freedom.” Komodo. 2018.

Moser, Malte. 2013. “Anonymity of bitcoin transactions”.

Nakamoto, Satoshi. 2008. “Bitcoin: A peer-to-peer electronic cash system”. Working Paper.

Ocminer. 2018a. “Network Attack on XVG / VERGE”. Bitcointalk. 2018. https://bitcointalk.org/index.php?topic=3256693.0.

— — — . 2018b. “Network Attack on XVG / VERGE (Page 57)”. Bitcointalk. 2018. https://bitcointalk.org/index.php?topic=3256693.msg38135174#msg38135174.
PTY X. 2018. “What is a Parallel Chain (Asset Chain)?” Komodo Platform. 2018. https://komodoplatform.atlassian.net/wiki/spaces/KPSD/pages/71729160/What+is+a+Parallel+Chain+Asset+Chain.
Quesnelle, Jeffrey. 2017. “On the linkability of Zcash transactions”. arXiv preprint arXiv:1712.01210.
21
Roberts, Jeff John. 2018. “Bitcoin Spinoff Hacked in Rare ‘51% Attack’”. FORTUNE. 2018. http://fortune.com/2018/05/29/bitcoin- gold-hack/.
Saberhagen, Nicolas Van. 2013. “CryptoNote v 2.0”.
Sasson, Eli Ben, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, en Madars Virza. 2014. “Zerocash: Decentralized anonymous payments from bitcoin”. In 2014 IEEE Symposium on Security and Privacy (SP), 459–74.