uPlexa

Pousser à l'utilisation de la puissance de calcul
de l'ensemble des équipements IoT (Internet of Things)
pour créer un moyen de paiement anonyme sur la blockchain.

Clause de non-responsabilité :

Vous consultez une version traduite du Livre Blanc du 26 novembre 2018. Des modifications des modèles commerciaux, techniques et juridiques pourraient être apportées à l'avenir. Consultez le site web d’uPlexa pour obtenir la dernière version de ce Livre Blanc.

Table des Matières

Introduction & Vision

uPlexa est un système de paiement électronique p2p basé sur l'exploitation de la puissance de l'IoT et sur l'anonymat. Construit sur sa propre Blockchain (chaîne de blocs), utilisant une version modifiée de l'algorithme CryptoNight, uPlexa a été développé afin d'interconnecter la puissance collective des appareils IoT (Internet of Things - internet des objets) dans leur ensemble, en permettant des paiements anonymes, en particulier pour les fournisseurs de services internet et télécom, tout en supportant le commerce électronique anonyme. Il y a plus de 9 milliards d'appareils IoT dans le monde en 2018, avec une prévision de plus de 20 milliards d'ici 2020.

Tout comme Bitcoin, uPlexa est un système de paiement électronique peer-to-peer (p2p). Toutefois, uPlexa prend également en charge les paiements anonymes et un minage IoT rentable. Non seulement l'uPlexa est ASIC-résistant, mais il vise également à être la monnaie la plus rentable à miner pour les utilisateurs d'appareils IoT, en utilisant un pourcentage spécifique de ressources inutilisées. La Blockchain d'uPlexa sera directement accessible et exploitable via le Web, sans besoin de télécharger aucune ressource externe. Malgré tout, des applications téléchargeables seront également disponibles.

En décembre 2017, nous avons été témoins de l'adoption de la plus importante de toutes les cryptomonnaies, Bitcoin. A ce moment, Bitcoin n'était pas prêt à être adopté par une telle base d'utilisateurs, ce qui a entraîné une forte congestion du réseau, et par conséquent des temps de transaction lents et des frais importants. uPlexa ambitionne de résoudre ces problèmes en utilisant son modèle de congestion quasi nulle (Near-Zera Congestion Model NZCM). Le NZCM consiste en un puissant hashrate utilisant la puissance des équipements IoT, tout en limitant les micro-paiements, par l'augmentation des frais liés aux micro-paiements à mesure que les transactions sur le réseau augmentent. Tout paiement qui n'est pas considéré comme un micro-paiement sera toujours soumis à des frais relativement bas. La NZCM utilisera également l'API uPlexa afin d'utiliser les transactions hors chaîne pour les utilisateurs expérimentés d'uPlexa. Il ne s'agit là que de quelques couches simplifiées de la NZCM. Pour en savoir davantage, veuillez vous reporter à la page 6 pour en savoir plus sur NZCM.

L'anonymat et la protection de la vie privée sont parmi les plus grands débats dans le domaine de la cryptomonnaie. uPlexa utilise l'algorithme CryptoNight afin d'assurer des transactions privées intraçables. Avec uPlexa, notre objectif est d'assurer l'anonymat des paiements des fournisseurs d'accès Internet et de services de télécommunications ainsi que du commerce électronique. Pour ce faire, nous négocierons des partenariats avec des fournisseurs de Services Informatiques et de télécommunications, nous lancerons notre propre plateforme de commerce électronique, nous soutiendrons les transactions anonymes, les propriétaires de magasins anonymes, et nous désapprouverons le stockage et la vente de renseignements personnels à des fins commerciales et autres.

Fonctionnement – Le Modèle IoT (Fonctionnalité de Base)

uPlexa utilise une version modifiée de l'algorithme CryptoNight afin de fournir une sécurité incontestable et des paiements anonymes. Après avoir audité l'algorithme CryptoNight original pour nos besoins, nous nous sommes vite rendus compte que le minage via des périphériques IoT en dehors de l'algorithme CryptoNight par défaut, n'est ni directement viable ni rentable. Les modifications apportées à l'algorithme visent donc à rendre l'exploitation de l'IoT plus rentable. Contrairement aux autres systèmes de paiement, la colonne vertébrale de notre réseau sera alimentée par les milliards de dispositifs IoT qui existent dans le monde.

Notre objectif principal est de générer une quantité rentable d'uPlexa, pour aider à payer l'électricité nécessaire à l'exploitation de n'importe quel appareil IoT, en exploitant une partie des ressources inutilisées sur chaque appareil. Cela peut sembler anodin pour les pays développés. Toutefois, dans les pays en développement - où la plupart des appareils IoT sont construits, ceux-ci sont également plus abordables à l'achat. Par exemple, en Asie du Sud-Est et dans d'autres régions, on trouve des téléviseurs connectés, des réfrigérateurs intelligents, des voitures intelligentes et de nombreux appareils mobiles. S'ils étaient en mesure d'obtenir suffisamment de profits pour - au minimum - payer une partie des frais de fonctionnement inhérents, ils seraient dans une bien meilleure situation, car les coûts mensuels d'électricité peuvent représenter jusqu'à 20 % de leur revenu.

Nous prévoyons de prendre en charge la plupart, sinon tous les périphériques IoT, en développant un logiciel spécifique à chaque périphérique pour exploiter uPlexa avec un pourcentage du temps inactif du CPU. La quantité peut être ajustée au choix par l'utilisateur, et nous aurons des plafonds afin d'éviter la surutilisation d'un appareil IoT. Les appareils que nous allons supporter sont :

- Ordinateurs de bureau et portables
- Téléphones mobiles et tablettes
- Téléviseurs intelligents
- Appareils de cuisine intelligents (réfrigérateurs, fours, cafetières, cuisinières, etc.)
- Voitures intelligentes
- Raspberry Pi's
- Serveurs (Datacenters et fermes de serveurs)
- ...Et d'autres, au fur et à mesure que l'IoT continuera de se développer

Principe de Fonctionnement – Frais & Modèle de Congestion Quasi-Nulle (Near-Zero Congestion Model - NZCM)

Afin de réduire l'encombrement du réseau et de maintenir des frais extrêmement bas, nous avons décidé de créer un modèle connu sous le nom de Near-Zero Congestion Model (NZCM), qui comporte plusieurs couches :

Exploitation de la puissance de l'adoption massive de l'IoT
Utilisation de l'API uPlexa NZCM pour les transactions hors chaîne
Désapprobation des microtransactions extrêmement petites
Mise à l'échelle des frais à des taux plus élevés pour les microtransactions

Avec l'énorme quantité d'appareils IoT existants et l'adoption continue de l'IoT, il ne fait aucun doute pour nous que nous obtiendrons une contribution considérable de support réseau pour alimenter notre Blockchain. Cela dit, un autre point positif est que pour les cas d'utilisation majeurs d'uPlexa, l'utilisation de l'API NZCM permettra de ne pas avoir à utiliser la Blockchain réelle pour une grande partie des transactions.

L'API NZCM permettra aux webmasters, développeurs d'applications et organisations de créditer leurs utilisateurs en uPlexa pendant que leurs utilisateurs choisiront de miner pour un un service, une application ou une entreprise spécifiques. Lorsqu'un utilisateur choisit de miner pour une organisation spécifique en utilisant l'API NZCM, l'organisation agit alors en tant que "pool" de minage. Les mineurs exploitent les mines vers un seul porte-monnaie, comme par exemple une boutique en ligne de commerce électronique. Toutes les pièces frappées sont envoyées à l'organisation plutôt qu'au(x) mineur(s) individuel(s). L'uPlexa est alors crédité à l'utilisateur individuel sur sa plate-forme via notre API, plutôt que sur la Blockchain elle-même. Ainsi, lorsqu'un utilisateur dépense son uPlexa miné sur la plate-forme de l'organisation, une transaction n'a pas besoin d'être poussée à travers la Blockchain. La transaction est plutôt traitée par l'intermédiaire de la base de données de l'organisation.

L'utilisation-type d'uPlexa est principalement pour les paiements anonymes à destination des fournisseurs d'accès Internet et de télécommunications, ainsi que pour le commerce électronique. De ce fait, les micro-transactions ne sont pas une priorité majeure. Nous souhaitons à l'avenir nous concentrer sur un réseau CryptoNight lightning pour supporter les microtransactions uPlexa et autres transactions CryptoNight. Cependant, comme uPlexa ne prend pas directement en charge les micro-transactions, il y aura une limite minimale sur la quantité d'uPlexa qui peut être envoyée (pas moins de 1 uPlexa). Ce montant peut être modifié à tout moment par forkag, selon la valeur d'uPlexa. Pour les micro-transactions de moins de 5 uPlexa, il y aura une mise à l'échelle des frais. Ainsi,

si vous envoyez moins de 5 uPlexa lorsque le réseau est inondé de micro-paiements, les frais de ces micro-transactions augmenteront deux fois plus que n'importe quelle transaction standard. L'idée sous-jacente est de neutraliser les attaques réseau et de réduire l'utilisation des micro-paiements via uPlexa. uPlexa n'est pas, pour le moment, une cryptomonnaie qui se concentre sur les microtransactions (<0.15 dollars US)

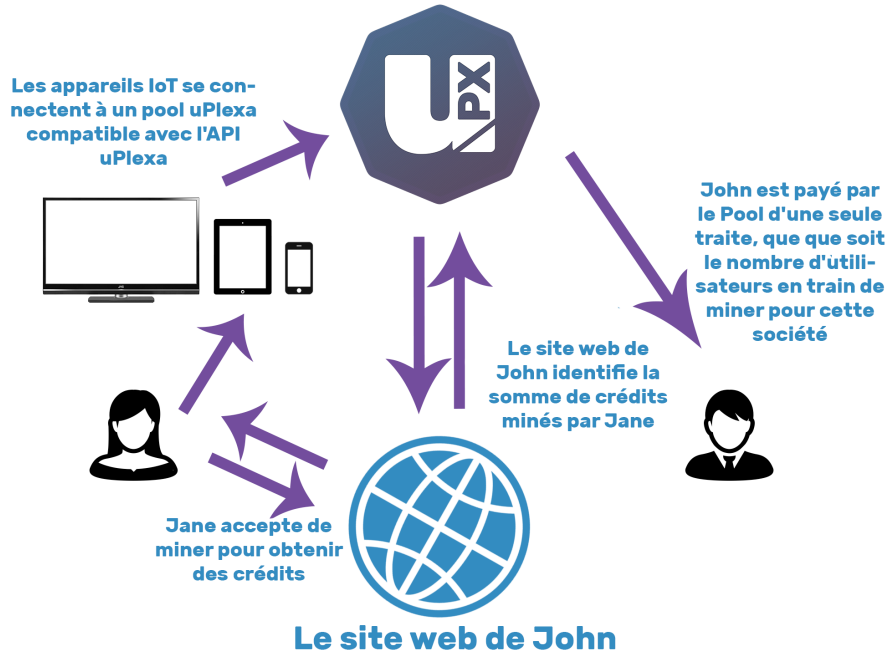
L’API uPlexa NZCM

L'API uPlexa peut être utilisée pour aider à réduire la congestion du réseau en utilisant moins de transactions sur la chaîne, réduisant ainsi les frais pour les entreprises et les projets.

Principe de Fonctionnement

Admettons que John - le propriétaire de johnswebsite.com, souhaite fournir un système de crédit à ses utilisateurs afin qu'ils puissent acheter des biens, des services ou faire des dons. Il peut demander à ses utilisateurs de connecter leurs appareils IoT à son site Web en ligne afin de miner des pièces uPlexa. En retour, les utilisateurs seront récompensés par des crédits sur le site en utilisant l'API uPlexa. Une fois que l’tilisateur aura miné suffisamment de JohnCredits, il sera en mesure d'effectuer un achat ou d'utiliser une partie de ces crédits pour une ristourne sur le site Web de John.

Pendant ce processus, le résultat de ce minage est envoyé vers un seul portefeuille, le portefeuille de John. Cependant, chaque utilisateur individuel et le nombre de hachages qu'il a résolus sont suivis via l'API uPlexa. Ainsi, lorsque l'utilisateur Jane souhaite faire un achat, le montant est déduit de son solde via l'API, plutôt que de faire une transaction séparée depuis son portefeuille vers celui de John.



Présentation du commerce électronique

L'industrie du commerce électronique représente plus de 2,3 trillions de dollars de revenus mondiaux, avec des estimations à plus de 4,88 trillions de dollars d'ici 2021. Source : https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

L'équipe uPlexa présentera sa propre plateforme de commerce électronique, fondée sur la prise en charge massive de multiples cryptomonnaies, fiat (monnaies fiduciaires), et l'utilisation d'uPlexa comme une passerelle privée, sécurisée et anonyme pour les webmasters et leurs clients. Il n'y aura pas de KYC (Know Your Customer - Connais Ton Client, procédé d'identification et de certification d'un utilisateur) pour nos webmasters, et ils seront payés anonymement via uPlexa. D'autres éléments tels que les développements, les plugins et les designs seront également disponibles sur le marché du commerce électronique pour que les webmasters puissent les acquérir avec des uPlexa pour leur propre magasin.

Le système de commerce électronique uPlexa ne facturera pas de frais aux utilisateurs jusqu'à ce que l'exploitation de la boutique soit rentable. Autrement dit, la boutique est GRATUITE jusqu'à ce que vous commenciez à gagner un minimum de 3 fois les frais mensuels de votre boutique, qui sera d'environ 29 dollars US/mois pour les boutiques de base. Les paiements seront effectués quotidiennement si vous dépassez un montant de >29 dollars US. Autrement, les paiements se feront toutes les deux semaines.

Notre équipe a déjà travaillé dans l'industrie du commerce électronique, de BigCommerce à Wordpress (WooCommerce), en passant par Shopify. Nous allons nous concentrer fortement sur la personnalisation et sur une expérience de commerce électronique anonyme, afin de nous démarquer des autres systèmes de commerce électronique existants, en écoutant les suggestions et les plaintes des clients que ces entreprises ont toujours ignorées. En ce qui nous concerne, nous avons eu de nombreuses idées d'amélioration des conversions pour ces systèmes, améliorations qui n'étaient pas applicables sans modifications majeures. Certaines de ces améliorations sont aujourd'hui en cours de production pour des magasins en direct.

Ceci étant dit, les priorités d'uPlexa en matière de commerce électronique seront à la fois les cryptomonnaies et l'augmentation des conversions pour nos clients.

Anonymat du Service de Paiement

uPlexa établira enfin le lien entre les systèmes de paiements anonymes et les fournisseurs de services. Pour ce faire, de multiples partenariats seront établis avec des entreprises en développement, permettant ainsi aux utilisateurs de payer leurs services sans KYC et d'utiliser uPlexa comme méthode de paiement optionnelle.

Pourquoi les paiements de services devraient-ils être anonymes ?

- - Offrir, grâce à l'anonymat, une protection contre les programmes d'espionnage qui veulent subtiliser vos renseignements personnels.
- - Aider à vous protéger contre la vente de vos données à des fins de marketing ou autres.
- - Payer pour des services, en voyage à l'étranger, sans avoir à subir des frais "touristiques" car uPlexa est une monnaie mondiale, et personne ne sait qui vous êtes ni d'où vous venez.
- - Éviter que d'autres entreprises ne sachent à qui vous envoyez de l'argent, ou quelle entreprise vous pourriez être en train d'acquérir.
- - Garder le secret sur vos fournisseurs d'affaires
- - Échapper à la répression gouvernementale et aux interdictions de service
- - Éviter le chantage des FAI ou des employés qui espionnent vos données.
- - Rémunérer les services des membres de votre famille avec votre propre compte
- - Empêcher les pirates informatiques d'associer un numéro de téléphone à votre nom, ou de pirater votre accès mobile avec vos données personnelles pour accéder à vos comptes en ligne.
-

Les fonctions anonymes d'uPlexa vont bien au-delà de la codification, dans le domaine des grandes entreprises et des politiques concernant KYC et l'anonymat. Le défi le plus difficile sera de trouver des entreprises et des partenaires prêts à proposer une option sûre et anonyme par rapport à leurs systèmes et services. Ainsi, nous mettrons fortement l'accent sur les partenariats stratégiques, tout en récompensant ceux qui aident uPlexa à réaliser son véritable potentiel.

Viabilité et rentabilité de l'IoT

uPlexa délivrera des services de minage pour un large éventail d'appareils IoT, depuis les téléphones intelligents et les tablettes jusqu'aux téléviseurs intelligents et même aux voitures connectées. Pour ce faire, nous utiliserons notre logiciel de minage. Le logiciel de minage uPlexa utilise un ensemble spécifique de dispositifs de sécurité afin d'éviter que ces dispositifs ne surchauffent et ne deviennent moins réactifs, en n'utilisant qu'une partie des ressources inutilisées de ces dispositifs. Dans nos tests, le logiciel minier uPlexa nécessite moins de CPU que les applications couramment utilisées telles que l'appareil photo de votre téléphone, Facebook ou Netflix.

Les Maths

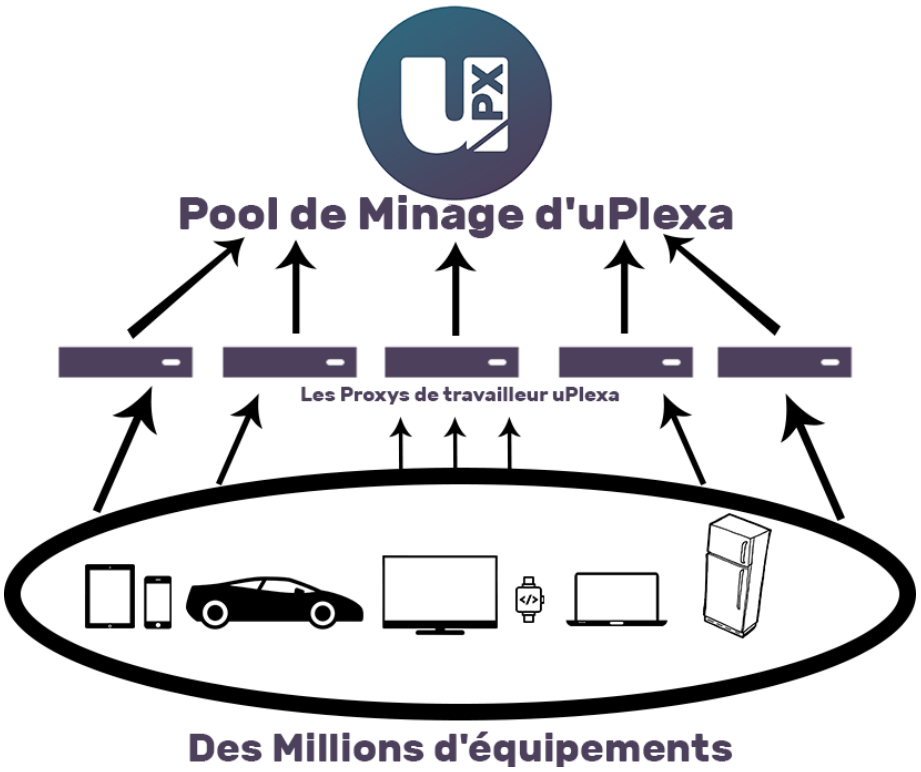
Smartphone standard :

28H/s "plein pot" ou 10H/s avec 35% d'utilisation CPU

Ordinateur Portable Standard :

environ 45H/s "plein pot" ou 16H/s avec 35% d'utilisation CPU

L'utilisation de 35% du CPU fournit un hashrate moyen de 13H/s. Si Alice possède 15 périphériques, elle dispose de 13 * 15 = 195H/s.



La technologie qui rend cela possible et léger est un pool CryptoNight ”forké” associé à un protocole de proxy avancé, pour réduire les connexions au pool. Grâce à notre logiciel, nous sommes capables de supporter jusqu'à deux millions de connexions simultanées sur cinq instances Amazon m5.2xlarge en tant que proxy, et deux instances Amazon m4.16xlarge (une pour le pool, une pour la validation de shares et l'équilibrage de charge).

Rentabilité pour les mineurs

L’application du principe de rentabilité est liée à notre version du protocole CryptoNight, modifié afin de fournir la forme la plus rentable mais aussi anonyme d'exploitation minière de l'IoT. Le protocole CryptoNight est d’origine assez résistant aux ASIC. Cependant, les futurs hardforks obligatoires que l'ensemble du réseau suivra pourraient être nécessaires pour éviter l'exploitation minière ASIC sur notre plate-forme. Ces hardforks ne seront ni intrusifs ni risqués.

Avec notre algorithme, l’objectif est d'équilibrer le minage GPU et CPU autant que possible, en termes de coût par dollar pour le matériel de minage des utilisateurs. L'idée derrière l'exploitation minière de l'IoT est d'avoir de nombreux dispositifs d'IoT connectés à travers le monde, ce qui aidera à minimiser la centralisation de l'exploitation minière, tout en maintenant un flux régulier de profit pour nos mineurs, afin d'aider continuellement à traiter les transactions sur la Blockchain uPlexa.

Avec uPlexa, les gens peuvent utiliser une Blockchain sur laquelle il est rentable de miner uPlexa, en se connectant directement à l'un des pools publics uPlexa. Ils peuvent également choisir de se connecter au pool d’une entreprise, d’un site Web ou d’un jeu afin d'obtenir des crédits sur ladite plate-forme.

Explication technique - Présentation de CryptoNight

l’Algorithme CryptoNote

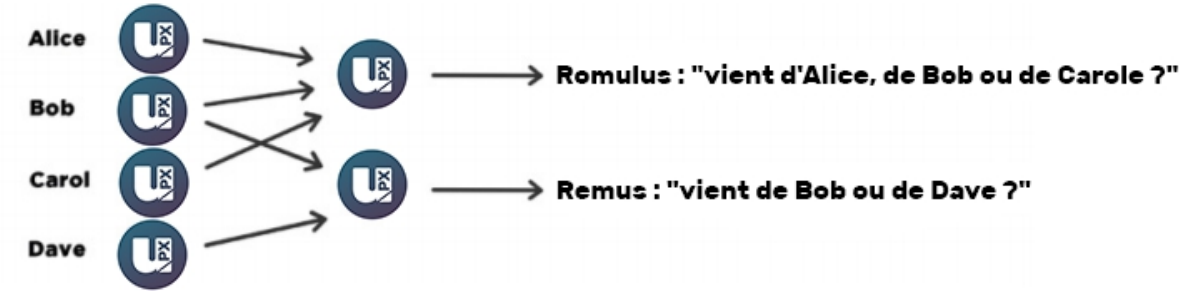
L'algorithme CryptoNote est publié sous licence open source et a été adopté et intégré dans uPlexa car il constitue une base de noyau de cryptomonnaie solide et bien testée. Il s'agit de la même technologie de base de la blockchain qui est utilisée à la fois par Monero (une des 10 premières cryptomonnaies) et Bytecoin (une des 15 premières cryptomonnaies).

Des paiements Intraçables

Le processus de vérification habituel d’une signature numérique ordinaire (p. ex. (EC)DSA, Schnorr, etc.) implique la clé publique du signataire.
C'est une condition nécessaire, car la signature prouve effectivement que l'auteur possède la clé secrète correspondante. Mais ce n'est pas toujours une condition suffisante.

La signature en anneau (“Ring Signature”) est un procédé plus sophistiqué qui, en fait, peut nécessiter la mise en oeuvre de plusieurs clés publiques différentes pour la vérification. Dans le cas d’une signature en anneau, nous avons un groupe d'individus, chacun avec sa propre clé secrète et publique. La mention certifiée par les signatures en anneau est que le signataire d'un message donné est un membre du groupe. La principale distinction avec les systèmes de signature numérique ordinaires est que le signataire a besoin d'une seule clé secrète, mais qu'un vérificateur ne peut établir l'identité exacte du signataire. Par conséquent, si vous rencontrez une signature en anneau avec les clés publiques d'Alice, Bob et Carol, vous pouvez seulement affirmer que l'un de ces individus était le signataire mais vous ne serez pas en mesure de l’identifier précisément.

Ce concept peut être utilisé pour rendre intraçables les transactions numériques envoyées sur le réseau en utilisant les clés publiques des autres membres dans la signature en anneau qui s'appliquera à la transaction. Cette méthode atteste que le créateur de la transaction est apte à dépenser le montant spécifié dans la transaction, mais que son identité ne pourra être distinguée de celle des utilisateurs dont il a utilisé les clés publiques dans ses signatures en anneau.

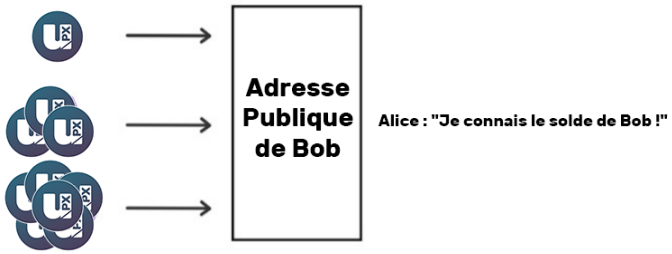


Transactions intraçables

Il est à souligner que les transactions tierces ne vous empêchent pas de dépenser votre propre argent. Votre clé publique peut apparaître dans des dizaines de signatures en anneau d'autres personnes, mais seulement comme un facteur de confusion (même si vous avez déjà utilisé la clé secrète correspondante pour signer votre propre transaction). De plus, si deux utilisateurs créent des signatures en anneau avec le même jeu de clés publiques, les signatures seront différentes (à moins qu'ils n'utilisent la même clé privée).

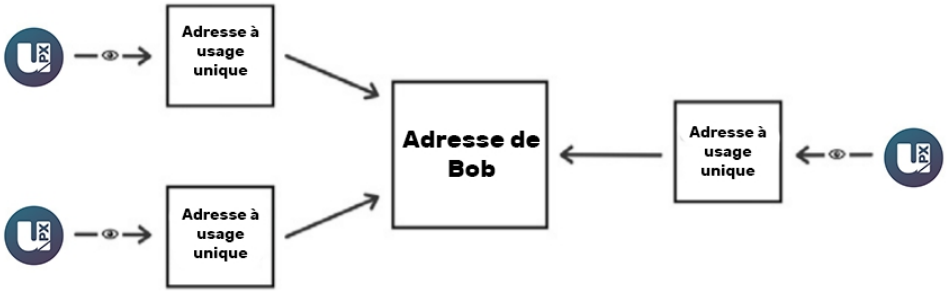
Transactions non corrélatives

En général, lorsque vous affichez votre adresse publique, n'importe qui peut vérifier toutes vos transactions entrantes, même si elles sont cachées derrière une signature en anneau. Pour éviter les liens, vous pouvez créer des centaines de clés et les envoyer à vos débiteurs en privé, mais cela vous prive de la commodité d'avoir une seule adresse publique.



Le CryptoNote façon uPlexa résout ce dilemme par la création automatique de plusieurs clés uniques et à usage unique, dérivées de la clé publique unique, pour chaque paiement p2p. La solution réside dans une modification intelligente du protocole d'échange de Diffie-Hellman. À l'origine, il permet à deux parties de produire une clé secrète commune dérivée de leurs clés publiques. Dans notre version, l'expéditeur utilise l'adresse publique du destinataire et ses propres données aléatoires pour calculer une clé unique pour le paiement.

L'expéditeur ne peut générer que la partie publique de la clé, alors que seul le destinataire peut calculer la partie privée ; le destinataire est donc le seul à pouvoir débloquer les fonds une fois la transaction engagée. Il a juste besoin d'effectuer un contrôle à formule unique sur chaque transaction pour vérifier si elle lui appartient. Ce processus implique sa clé privée, donc aucun tiers ne peut effectuer cette vérification et identifier le lien entre la clé unique générée par l'expéditeur, et l'adresse publique unique du destinataire.



Un élément important de notre protocole est l'utilisation de données aléatoires par l'expéditeur. Il en résulte toujours une clé unique différente, même si l'émetteur et le récepteur restent identiques pour toutes les transactions (c'est pourquoi la clé est appelée "clé à usage unique"). De plus, même s'il s'agit de la même personne, toutes les clés à usage unique seront également absolument uniques.

Double Preuve de Dépense

Des signatures entièrement anonymes permettraient de dépenser les mêmes fonds plusieurs fois, ce qui, bien entendu, est incompatible avec le fondement de tout système de paiement. Le problème peut être résolu comme suit.

Une signature en anneau est en fait une classe de crypto-algorithmes avec différentes caractéristiques. Le CryptoNote d'uPlexa utilise la version modifiée de la "Traceable ring signature" (signature en anneau traçable). En fait, nous avons transformé la traçabilité en possibilité de corrélation. Cette propriété limite l'anonymat du signataire de la manière suivante : s'il crée plus d'une signature en anneau en utilisant la même clé privée (l'ensemble des clés publiques tierces n'est pas pertinent ici), ces signatures seront liées, ce qui indique une tentative de double dépense.

Pour faciliter la corrélation, le CryptoNote d'uPlexa a introduit un marqueur spécial créé par l'utilisateur lors de la signature, que nous avons appelé une image clé. C'est la valeur d'une fonction cryptographique unidirectionnelle de la clé secrète, donc en termes mathématiques il s'agit d'une image de cette clé. "Unidirectionnel" signifie qu'étant donné qu'on dispose de la seule image de la clé, il est impossible de récupérer la clé privée. D'un autre côté, il est impossible, sur le plan informatique, de trouver une collision (deux clés privées différentes, qui auraient la même image). L'utilisation de n'importe quelle formule, à l'exception de la formule spécifiée, générera une signature invérifiable. En somme, l'image clé est inévitable, sans ambiguïté et pourtant un marqueur anonyme de la clé privée.

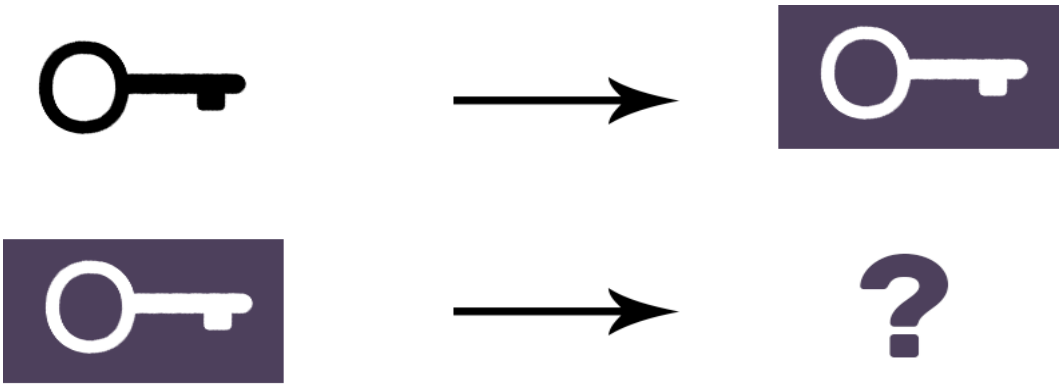
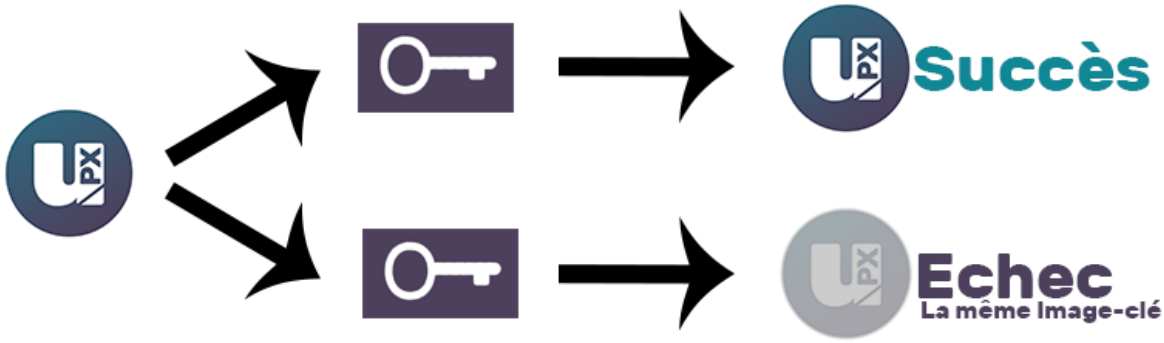


Image-clé via la fonction unidirectionnelle

Tous les utilisateurs conservent la liste des images-clés utilisées (par rapport à l'historique de toutes les transactions valides, elle nécessite une quantité insignifiante de stockage) et rejettent immédiatement toute nouvelle signature en anneau possédant une image clé en double. Cela n'identifiera pas l'utilisateur qui essaie de frauder, mais empêche toute tentative de double dépense, qu'elle provienne d'intentions malveillantes ou d'erreurs logicielles.

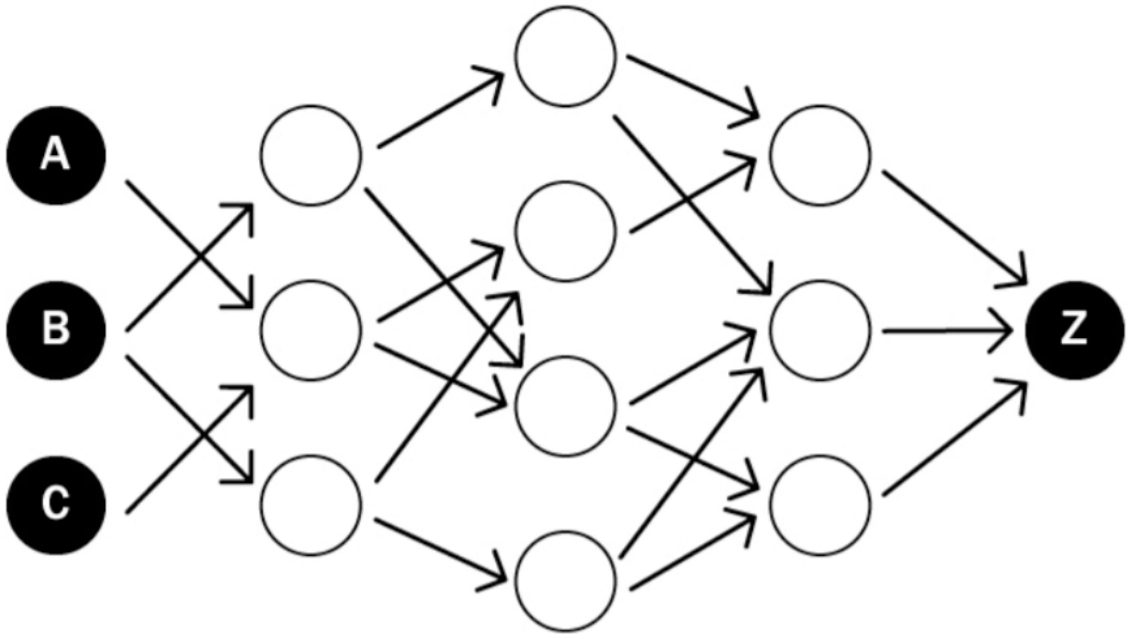


Résistance à l'analyse de la blockchain

Il existe de nombreux articles académiques consacrés à l'analyse de la blockchain du Bitcoin. Leurs auteurs retracent le flux de monnaie, identifient les propriétaires des pièces, déterminent les soldes des portefeuilles, etc. La possibilité d'effectuer une telle analyse est due au fait que tous les transferts entre adresses sont transparents : chaque entrée dans une transaction se réfère à une sortie unique. De plus, les utilisateurs réutilisent souvent leurs anciennes adresses, recevant et envoyant des pièces de monnaie plusieurs fois sur celles-ci, ce qui simplifie le travail de l'analyste. Cela arrive involontairement: si vous avez une adresse publique (par exemple, pour les dons), vous êtes assuré d'utiliser cette adresse dans de nombreuses entrées et transactions.

Le CryptoNote d'uPlexa est conçu pour réduire les risques associés à la réutilisation des clés et au traçage d'une entrée à une sortie. Chaque adresse utilisée pour un paiement est une clé unique, dérivée des données de l'expéditeur et du destinataire. Cette clé peut apparaître deux fois avec une probabilité de collision de 256 bits. Dès que vous utilisez une signature en anneau dans votre entrée, cela implique une incertitude : quelle sortie vient d'être dépensée ?

Si on essaie de dessiner un graphique avec des adresses aux sommets et des transactions sur les bords, on obtiendra un arbre : un graphique sans cycles (car aucune clé/adresse n'a été utilisée deux fois). De plus, il y a des milliards de graphiques possibles, puisque chaque signature en anneau produit de la confusion. Ainsi, vous ne pouvez pas être certain de savoir depuis quel expéditeur possible la transaction-bordure arrive à l'adresse-sommet. Selon la taille de l'anneau, vous obtenez une probabilité de deviner de "un sur deux" à "un sur mille". Chaque transaction subséquente augmente l'entropie et crée des obstacles supplémentaires pour les analystes.



Transaction CryptoNote standard

Une transaction standard uPlexa CryptoNote est générée par la séquence décrite ci-dessous.

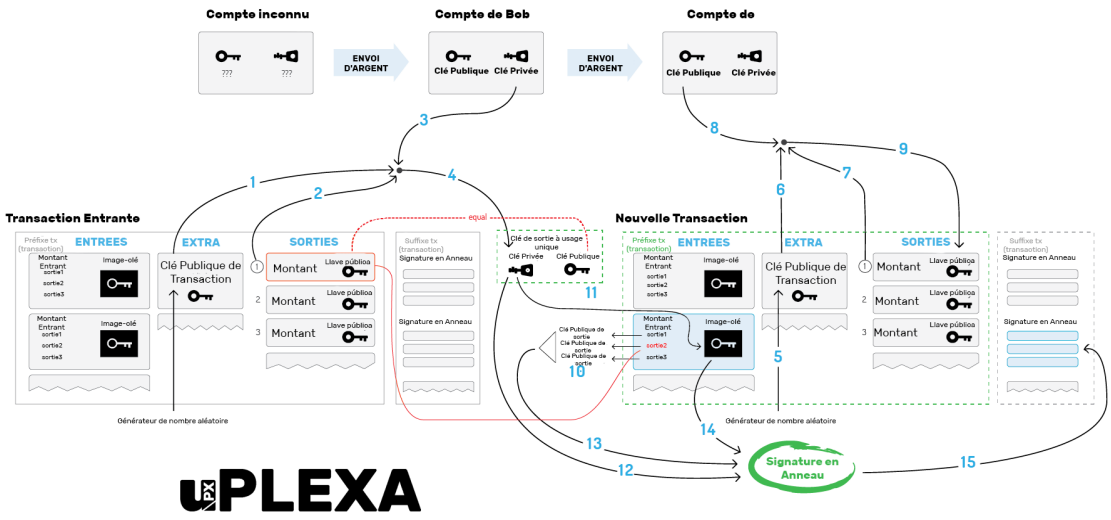
Bob décide de dépenser une sortie, qui a été envoyée à la clé publique à usage unique. Il a besoin de Extra (1), TxOutNumber (2), et sa clé de Compte privée (3) pour récupérer sa clé privée à usage unique (4).

Lors de l'envoi d'une transaction à Carol, Bob génère sa valeur Extra par tirage aléatoire (5). Il utilise Extra (6), TxOutNumber (7) et la clé de Compte publique de Carol (8) pour obtenir sa clé publique de sortie (9).

Dans l'entrée, Bob cache le lien vers sa sortie parmi les clés tierces (10).

Pour éviter les doubles dépenses, il envoie également l'Image Clé, dérivée de sa clé privée à usage unique (11).

Pour finir, Bob signe la transaction en utilisant sa clé privée à usage unique (12), toutes les clés publiques (13) et l'Image Clé (14). Il appose la signature en anneau qui en résulte à la fin de la transaction (15).



Limites adaptatives

Un système de paiement décentralisé ne doit pas dépendre des décisions d'une seule personne, même si cette personne est un des développeurs principaux. Les constantes dures et les nombres magiques dans le code entravent l'évolution du système et devraient donc être éliminées (ou du moins réduites au minimum). Chaque limite cruciale (telle que la taille maximale de bloc ou le montant minimal des frais) doit être recalculée en fonction de l'état antérieur du système. Par conséquent, cette limite change toujours de façon adaptative et indépendante, ce qui permet au réseau de se développer tout seul.

Le CryptoNote de uPlexa possède les paramètres suivants qui s'ajustent automatiquement à chaque nouveau bloc :

1. Difficult”. L'idée générale de notre algorithme est de faire la somme de tout le travail que les nœuds ont effectué au cours des 720 derniers blocs et de le diviser par le temps qu'ils ont passé pour l'accomplir. La mesure du travail est la valeur de difficulté correspondante pour chacun des blocs. L'heure est calculée comme suit : on trie tous les 720 horodatages et on retranche 20% des valeurs extrêmes. La plage des 600 valeurs restantes est le temps qui a été consacré pour 80% des blocs correspondants.

2. Taille Maximum de Bloc. Soit MN la valeur médiane des N dernières tailles de blocs. Dans ce cas, la "limite dure" pour la taille des blocs de validation est de 2*MN. Cela évite l’engorgement de la chaîne de blocage tout en permettant à la limite de croître lentement avec le temps, si nécessaire. La taille de la transaction n'a pas besoin d'être limitée explicitement. Elle est délimitée par la taille du bloc.

Émission en douceur

La limite supérieure du montant total de toutes les pièces numériques est également numérique

RéserveMax = 264 − 1 unité atomique

Il s'agit d'une restriction naturelle basée uniquement sur les limites de mise en œuvre, et non sur une intuition qui supposerait que "N pièces devraient suffire pour tout le monde". Pour faciliter le processus d'émission, CryptoNote d'uPlexa utilise la formule suivante pour les récompenses de bloc :

RécompenseDeBase = (RéserveMax − A) >> 18

Où A est le montant des pièces déjà générées. Cela permet une croissance prévisible de la masse monétaire sans aucun ralentissement.

Conclusion

uPlexa se concentre sur la production d'une monnaie anonyme avec une application complémentaire dans le commerce électronique et les paiements des fournisseurs de services. Ces applications domineront les couches de base du hachage de masse “IoT”, et des transactions hors chaîne.

References

Livre Blanc Cryptonote (EN) :
https://cryptonote.org/whitepaper.pdf

Cryptonote Inside :
https://cryptonote.org/inside

Livre Blanc Bitcoin (EN) :
https://bitcoin.org/bitcoin.pdf

Statistiques: Les équipements IoT connectés 2015-2025:
https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

PRISM (programme de surveillance):
https://en.wikipedia.org/wiki/PRISM_(surveillance_program)

uPLEXA