Zelcash

Innovant | Intuitif | Intelligent

Whitepaper version deux

Table des matières

Introduction 3
Mission, vision et valeurs 4
Aperçu 5
Avertissement : déclarations prospectives 5
1.0 Bitcoin 6
  1.5 Zcash 6
2.0 Ethereum 7
3.0 Zel 8
4.0 Fonctions de base ZelCash 8
  4.1 T_transactions 8
  4.2 Z_transactions 9
  4.3 Proof-of-Work 11
  4.4 Récompense de bloc 12
  4.5 Zelnodes 13
  4.6 Economie Zelnode 14
5.0 Double économie 16
6.0 Technologies Zel 16
  6.1 ZelTreZ 17
  6.2 Zel ID 17
  6.3 ZelPay 18
  6.4 ZelDev 19
  6.5 ZelChains 19
  6.5 ZelDex 19
  6.7 Dapp Store 20
7.0 Directions et contributions au livre blanc 20
8.0 Le futur de Zel 21
9.0 Glossaire 22
Ressources 24

Introduction

La technologie blockchain va changer le monde d'une manière qui n'aurait pas pu être imaginée il y a cinq ans. MarketsandMarkets prévoit un taux de croissance annuel de 61,5% sur au moins 2021, et le rapport du Forum économique mondial prévoit que d'ici 2027, 10% du PIB mondial sera stocké sur des technologies liées à la blockchain. [1] [2]

La transparence, l'immuabilité et la désintermédiation de la blockchain éliminent le besoin d'un tiers, réduisant les frais, améliorant la sécurité et éliminant le risque de contrepartie. Il offre une simplicité : les opérations sont ajoutées à un seul registre public, ce qui évite l'encombrement, le chaos et les maux de tête généralement associés à plusieurs registres.

Le plus important est peut-être que la blockchain permet aux personnes de mieux contrôler leurs transactions et leurs interactions avec les informations et les transactions financières (sans parler de leurs propres données).

Clairement, la blockchain offre un formidable potentiel pour redéfinir la confidentialité et la sécurité et, idéalement, transformer l'économie mondiale.

Mais seulement idéalement, à ce stade. Le manque d'accessibilité et l'utilisation ont bloqué l'adoption. Les problèmes d'évolutivité abondent. Parmi les autres défis, citons les attaques par déni de service distribué (DDoS), les plateformes d'échanges en panne, le manque de passerelles fiduciaires et, en particulier pour l'utilisateur moyen, un système déconcertant d'adresses hexadécimales. Le résultat : des écosystèmes cloisonnés, des vulnérabilités de sécurité et des barrières à l'entrée élevées, parfois insurmontables.

Comme indiqué dans ce document, nous prévoyons de traiter voire de résoudre ces problèmes.

Notre plate-forme offre une expérience intuitive et sans friction, facilitant les transactions inter-chaînes dans une interface simple et propre pour les utilisateurs et les développeurs. Avec Zel, nous avons créé un environnement complet et standardisé qui permet aux développeurs de concentrer leurs efforts sur les solutions de blockchain. Cela favorisera la création gratuite de DApp et de contrats intelligents ouverts à tous.

La vision articulée et les solutions décrites dans ce livre blanc représentent les premières étapes vers la démolition des barrières, l'adoption d'une blockchain mondiale et une transformation perturbatrice.

---

[1] "Blockchain Technology Market--Global Forecast to 2021" MarketsandMarkets research *Blockchain Daily News*

[2] Deep Shift Technology Tipping Points and Societal Impact --World Economic Forum www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

Mission, vision et valeurs

L'équipe de ZelCash a été fondée par des personnes partageant les mêmes idées qui croient que la technologie peut faire de grandes choses pour le développement de l'humanité. Nous croyons en la vision d'un monde décentralisé, pour l'amélioration de tous. En tant qu'équipe, nous nous sommes fixés comme objectif de devenir le **leader du développement frontal et de la confidentialité de la blockchain**. Notre communauté est ce qui conduira le projet, avec l'inspiration des autres dans l'espace. Notre objectif est d'être des leaders dans l'industrie de la blockchain et de laisser la technologie conduire le projet avec la participation de la communauté. ZelCash vise à créer les outils nécessaires aux développeurs pour développer la puissance impressionnante de la technologie de la blockchain, menée par notre équipe et notre communauté, afin de fournir une technologie puissante disponible pour tous.

Le point culminant de Zel s’efforce d’être un réseau mondial de calcul entièrement décentralisé et évolutif, permettant aux développeurs d’utiliser la puissance de l’Internet sans attaches, de fournir des instruments de transaction faciles à utiliser par les personnes du monde entier qui ont été presque oubliée par les institutions monétaires traditionnelles et étendre le potentiel apparemment infini de la technologie de la blockchain.

Aperçu

Le but de cet article est de fournir des informations détaillées sur les technologies et les fonctionnalités de Zel publiées ou en attente de publication. Nous voulons que ce document soit clair et accessible à tous, tout en veillant à ce que les technologies clés soient discutées. Il ne fournira pas de détails techniques approfondis sur les produits non publiés tant que Zel Technologies n'aura pas publié - ou sera sur le point de le publier - les produits du domaine public. Cela garantira que le développement de Zel Technologies ne sera pas copié avant la version actuelle.

Bien que certains produits et services de Zel (tels que ZelTreZ) soient des sources fermées, ils seront "contrôlés par le code" par un tiers indépendant. L'équipe de Zel croit fermement en l'open source ; Nous veillerons toujours à ce que nos logiciels et technologies soient disponibles en open source, avec les détails techniques.

À cette fin, ce livre blanc n’est pas conçu comme une référence technique ou un prospectus, mais comme un moyen de révéler ce que nous avons accompli jusqu’à présent et de communiquer notre vision et nos projets alors que nous travaillons à réaliser le véritable potentiel de Zel. Dans cet esprit, veuillez prendre note de l'avertissement suivant :

Avertissement : déclarations prospectives

Les informations contenues dans ce livre blanc sont purement descriptives et non contraignantes. Veuillez noter que ce document comprend des prédictions, des déclarations d'intention, des discussions sur des plans, des estimations et d'autres informations susceptibles d'être considérées comme prospectives. Bien que ces déclarations prospectives représentent notre jugement et nos attentes quant à l'avenir, il ne s'agit pas d'une offre ou d'une sollicitation d'achat de produits, de biens, de services ou de sécurité. Toutes les déclarations sont soumises à des risques et à des incertitudes susceptibles d’entraîner des différences substantielles avec les résultats réels du développement de ZelCash. Aucune information contenue dans ce livre blanc n'a été examinée ou approuvée par une autorité de réglementation.

En outre, nous avons l'intention d'utiliser la blockchain de Zel comme plate-forme de développement open-source, en utilisant ces technologies sous licence pour améliorer la société, sans nous concentrer uniquement sur le profit de toute personne associée au projet. Par conséquent, ne vous fiez pas indûment, en particulier dans toute décision financière, à ces déclarations prospectives, qui sont sujettes à modifications.

Ce livre blanc et ses versions précédentes et futures sont et seront disponibles sur zel.cash/whitepaper. Le livre blanc original est écrit en "The Queen's English". Remarque : Ce document sera fréquemment mis à jour, parfois sans préavis. Veuillez confirmer que la version que vous lisez est la version actuelle.

1.0 Bitcoin

Janvier 2009 marque la sortie de Bitcoin de Satoshi Nakamoto. En tant que première devise sans support central ni émetteur et sans soutien physique, elle a représenté une révolution radicale dans la façon dont les systèmes financiers fonctionnent. La technologie sur laquelle elle reposait était sans doute beaucoup plus importante que la simple transaction de marchandises. Blockchain, également développé par Nakamoto, a permis l'utilisation d'un consensus distribué et décentralisé. En supprimant un émetteur ou un contrôleur centralisé, la « trésorerie électronique » permettrait des transactions entre pairs sans le consensus ou la confirmation d'une organisation tierce de confiance.

Bitcoin n'était pas le premier argent électronique ; Le b-money de Dei et d'autres existaient avant Bitcoin. Leur problème était de parvenir à un consensus. Il fallait un mécanisme pour contrer un acteur infâme qui tenterait de doubler ses dépenses sur le réseau. En utilisant la preuve de travail pour vérifier les blocs sur la blockchain Bitcoin - de la même manière que le Hashcash d'Adam Back - un consensus pouvait être atteint entre les nœuds, permettant la confirmation des transactions.

La blockchain a évolué depuis. Le développement de divers projets - notamment Ethereum - a montré de nouvelles possibilités et utilisations pour la blockchain, élargissant ainsi son potentiel.

1.5 Zcash

Zerocash (2014), qui deviendra plus tard le projet Zcash (2016), utilisa les zk-SNARKs (Zeroknowledge Succinct Non-interactive ARguments of Knowledge) pour générer des transactions peer-to-peer véritablement anonymes. S'appuyant sur Bitcoin, Zcash a amélioré Zerocash avec des correctifs et des ajustements de sécurité, ainsi que des fonctionnalités et des performances améliorées. De même que Bitcoin est devenu la première monnaie électronique largement adoptée, Zcash est devenue la première monnaie électronique anonyme largement adoptée.

En outre, Zcash a entamé une lutte contre la centralisation dans le processus d'exploitation minière provoquée par les ASIC SHA-256 qui avaient frappé le réseau Bitcoin ; Cela (sans doute) a permis de centraliser le réseau. L'implémentation d'Equihash, un algorithme de preuve de travail de mémoire pour l'exploitation minière, a entraîné un retour à l'exploitation décentralisée, avec des processeurs et des processeurs graphiques. Bien que des ASIC aient récemment été développés pour Equihash 200,9 de Zcash, d'autres projets maintiennent ce mécanisme décentralisé de consensus de Zelcash avec le développement de Equihash et ProgPOW modifiés, ainsi que de nouveaux concepts tels que la preuve de travail utile.

Les zk-SNARK permettent l'exécution d'une opération - telle qu'une diffusion de transaction sur un réseau de blockchain, et l'origine de la transaction, le montant et le destinataire de la transaction – complètement masqués.

Le développement continu de Zcash, tel que la récente mise à niveau du réseau Overwinter et le développement de transactions z sur le portefeuille mobile (léger), apportent des améliorations qui garantissent la confidentialité dans le commerce de la même manière que la monnaie fiduciaire mais avec les commodités des monnaies digitales et l'avantage de ne pas être émis ou contrôlé par une autorité centrale.

2.0 Ethereum

Ethereum a également élargi les possibilités des applications décentralisées et de son utilisation de la chaîne de blocs, permettant aux développeurs d'accéder à une plate-forme ouverte pour le développement d'applications, de contrats intelligents et bien plus encore.

Extrait du livre blanc Ethereum :

> *Ce que Ethereum a l'intention de fournir est une blockchain avec un langage de programmation Turing-complet intégré qui peut être utilisé pour créer des "contrats" pouvant être utilisés pour encoder des fonctions de transition d'état arbitraires, permettant aux utilisateurs de créer n'importe lequel des systèmes décrits ci-dessus, ainsi que beaucoup d'autres que nous n'avons pas encore imaginé, simplement en écrivant la logique en quelques lignes de code.*

Avec cette vision, Ethereum a joué un rôle moteur dans de nombreux aspects du développement de la chaîne de blocs et du secteur des cryptomonnaies. Elle offre un potentiel pour un monde où la plupart des systèmes, sinon tous, pourraient bénéficier de la technologie de la chaîne de blocs et des fonctionnalités qui en découlent. Qu'il s'agisse de la tokenisation d'actifs ou de la possibilité d'exécuter des collectes de fonds ICO, elle a permis aux utilisateurs de créer un nouvel Internet, ce que nous aurions pu imaginer à peine quelques années auparavant.

Malgré cela, les problèmes d'évolutivité et les préoccupations concernant la manière dont Ethereum les abordera persistent. Limité à environ 15 à 20 transactions par seconde, il est tout simplement trop lent de transformer sa vision en réalité.

Comme nous le décrirons dans ce livre blanc, Zel vise à résoudre le problème de l'extensibilité et à transformer la vision d'Ethereum en réalité. Nous avons créé un écosystème de produits et d'applications pour atteindre cet objectif, en mettant l'accent sur l'accessibilité et la convivialité.

3.0 Zel

Les technologies de Zel fonctionnent dans des relations symbiotiques entre elles et avec des technologies en dehors de l'écosystème de Zel. Zel est conçu comme un système ouvert en partenariat avec des technologies à source fermée. Voir la section 4.0 pour les fondements spécifiques de Zel.

4.0 Fonctions de base ZelCash

À sa surface, Zelcash est une monnaie numérique exploitable basée sur les fondements technologiques de la crypto-monnaie Zcash (anciennement Zerocash), basée sur Bitcoin. Zelcash utilise des preuves Zeroknowledge, inventées pour la première fois dans une monnaie numérique par Zcash et utilisées par de nombreux autres projets de monnaie privées. Ce fait fournit un réseau relativement important de développeurs pour différentes équipes fournissant, au fil du temps, des améliorations au protocole pour renforcer les fonctionnalités de base de la technologie blockchain et de la base de protocole Zeroknowledge.

Contrairement à Bitcoin dont les revendications d'anonymat ont été réfutées ces dernières années, Zcash garantit l'anonymat des utilisateurs via le protocole zk-SNARK (décrit dans la section 4.2). L'anonymat des utilisateurs finaux d'une transaction étant un principe fondamental de la vision originale de Bitcoin, les améliorations et l'évolution générale de l'idée de protection de la vie privée devraient être bien accueillies par les détenteurs de pièces et les utilisateurs. Zel a choisi d'utiliser les fonctionnalités de confidentialité de Zcash pour appliquer cette vision de l'anonymat et pour augmenter l'adoption d'un tel ensemble de fonctionnalités via un vaste réseau évolutif.

Zelcash offre une incitation économique à notre réseau de nœuds décentralisé, ZelNodes, pour offrir un réseau de développement de chaînes de blocs décentralisé et véritablement évolutif. Cette incitation est créée par une partie des récompenses globales et, éventuellement, par différents modèles économiques tels que les frais de transaction ou les tarifs d'exploitation pour DApps, afin de soutenir notre vision d'un réseau de nœuds puissant et décentralisé pour permettre des blockchains séparées, des applications, des jetons, des contrats intelligents et bien plus encore.

4.1 T_transactions

T_transactions sont des transactions traditionnelles enregistrées par la blockchain Bitcoin. Celles-ci sont effectuées entre des adresses appelées adresses transparentes ou des adresses t dérivées initialement de Bitcoin. Ceux-ci sont le plus couramment utilisés tous les jours entre les portefeuilles et les échanges. En effet, ils ont besoin de moins de puissance de calcul pour exécuter la transaction et peuvent être envoyés depuis des appareils mobiles et d'autres appareils portables.

4.2 Z_transactions

Les Z_transactions sont protégées ou privées. Celles-ci sont envoyées entre les adresses Z, également appelées adresses blindées. Zelcash les a héritées de Zcash et a donc bénéficié de tous les progrès et développements techniques réalisés par l'équipe Zcash pendant le développement de Zcash et de ses protocoles, tels que les mises à niveau réseau comme le fork Overwinter.

Si elle est envoyée depuis une ou plusieurs adresses protégées, la valeur de la ou des transactions reste confidentielle. Ce n'est que lorsqu'il y aura une adresse transparente à la réception que les pièces seront défigurées (et que la transaction ne sera plus privée). Cela permettra, par conséquent, de révéler la valeur reçue uniquement à cette adresse spécifique sur la blockchain. Les adresses d'origine ou l'adresse d'entrée, ainsi que la valeur envoyée, restent privées lorsqu'elles sont protégées de cette manière. Le protocole Zcash décrit ce processus en détail :

La valeur dans Zcash est soit transparente soit protégée.

- Les transferts de valeurs transparentes fonctionnent essentiellement comme Bitcoin et ont les mêmes propriétés de confidentialité.
- La valeur blindée est portée par des notes, qui spécifient un montant et une clé de paiement. La clé de paiement fait partie d'une adresse de paiement, qui est une destination vers laquelle les notes peuvent être envoyées. Comme avec Bitcoin, cela est associé à une clé privée qui peut être utilisée pour dépenser des notes envoyées à l'adresse ; dans Zcash, cela s'appelle une clé de dépense.

Chaque note a un engagement de note associé à la cryptographie et un nullificateur unique (de sorte qu'il existe une relation 1 : 1 : 1 entre les notes, les engagements de note et les nullificateurs). Le calcul du nullificateur nécessite la clé de dépense privée associée. Il est impossible d'établir une corrélation entre l'engagement de la note et le nullificateur correspondant sans connaître au moins cette clé de dépense. Une note valide non dépensée, à un point donné de la blockchain, est une note pour laquelle l'engagement de la note a été révélé publiquement sur la blockchain avant ce point, mais non le nullifier.

Une transaction peut contenir des entrées, des sorties et des scripts transparents, qui fonctionnent tous comme dans Bitcoin [Protocole Bitcoin]. Il contient également une séquence de zéro ou plusieurs descriptions JoinSplit. Chacune d'elles décrit un transfert JoinSplit qui intègre une valeur transparente et jusqu'à deux notes d'entrée et produit une valeur transparente et jusqu'à deux notes de sortie.

Les nullificateurs de notes d'entrée sont révélés (empêchant leur réutilisation) et les engagements des notes de sortie sont révélées (leur permettant d'être passées dans le futur). Chaque description JoinSplit comprend également une preuve zk-SNARK solide sur le plan des calculs, ce qui prouve que tous les éléments suivants sont valables, sauf avec une probabilité négligeable :

- Les valeurs d'entrée et de sortie sont équilibrées (individuellement pour chaque transfert JoinSplit).
- Pour chaque note d'entrée de valeur non nulle, un engagement de note révélée existe.
- Le prouveur connaissait les clés de dépense privées des notes d'entrée.
- Les nullificateurs et les engagements de note sont calculés correctement.

- Les clés de dépense privées des notes en entrée sont cryptographiquement liées à une signature sur l'ensemble de la transaction, de telle sorte que la transaction ne peut être modifiée par une partie qui ne connaît pas ces clés privées.
- Chaque note de sortie est générée de telle manière qu'il est impossible que son nullificateur entre en collision avec le nullificateur d'une autre note.

En dehors de zk-SNARK (adresses blindées), il est également vérifié que les nullificateurs des notes d'entrée n'ont pas déjà été révélés (c'est-à-dire qu'ils n'ont pas déjà été dépensés).

Une adresse de paiement comprend deux clés publiques :

1. Une clé de paiement correspondant à celle des notes envoyées à l'adresse, et
2. Une clé de transmission pour un schéma de chiffrement asymétrique clé-privé.

"Clé privée" signifie que les cryptogrammes ne révèlent pas d'informations sur la clé sur laquelle ils ont été cryptés, sauf pour le détenteur de la clé privée correspondante, appelée dans ce contexte la clé d'affichage. Cette clé unique est utilisée pour communiquer les notes de sortie chiffrées sur la blockchain à leur destinataire, qui peut utiliser la clé de visualisation pour analyser la chaîne de blocs pour les notes qui lui sont adressées, puis déchiffrer ces notes.

La base des propriétés de confidentialité de Zcash est la suivante : lorsque la note est dépensée, le dépensier prouve seulement que certains engagements ont été révélés sans révéler lesquels. Cela signifie qu'une note dépensée ne peut pas être liée à la transaction dans laquelle elle a été créée.

D'un point de vue contradictoire, l'ensemble des possibilités pour une note donnée et son ensemble de traçabilité des notes, comprend toutes les notes précédentes, que l'adversaire ne contrôle ni ne sait avoir été dépensé. Cela contraste avec d'autres propositions de systèmes de paiement privés, tels que CoinJoin ou CryptoNote, qui reposent sur le mélange d'un nombre limité de transactions et qui ont donc des ensembles de traçabilité des notes plus petites.

Les nullificateurs sont nécessaires pour éviter les doubles dépenses : chaque note ne possède qu'un seul nullificateur valide. Tenter de dépenser deux fois une note révélerait le nullificateur deux fois, ce qui entraînerait le rejet de la seconde transaction.

4.3 Proof-of-Work

Comme Nakamoto a amélioré le travail d'Hashcash d'Adam Back, il a créé un système de validation qui repose sur le hachage cryptographique plutôt que sur la confiance d'un système centralisé. À la suite de l'utilisation de SHA-256 par Nakamoto pour Bitcoin, Litecoin a implémenté Scrypt, suivi de Dash et Ethereum utilisant respectivement X11 et Ethash. Les développements récents (élargissant l'idée de X11, qui est une séquence d'algorithmes de hachage où la sortie de l'un devient l'entrée du suivant) sont venus avec le développement de X13, X15 et X17.

BTC était destiné à être exploité par des unités de traitement informatique (CPU) faisant référence au hachage et au vote avec les CPU. Mais des solveurs pour les cartes graphiques (GPU) ont été développés. Au fur et à mesure que la valeur de Bitcoin augmentait et que l'incitation au minage devenait plus élevée ; il est devenu viable d'utiliser le matériel programmable tel que les FPGA pour l'exploitation de Bitcoin. Celles-ci avaient un avantage sur les processeurs et les GPU. Après le développement des FPGA, le développement de matériel minier spécialement conçu, les ASICs ont rapidement dominé le réseau Bitcoin, ce qui signifie que de la même manière qu'il est devenu peu rentable de miner avec des CPUs quand les GPU ont été développés, le même destin est attendu pour les GPUs avec les FPGAs.

Construit sur l'idée de chaîner de nombreux algorithmes ensemble dans une séquence qui a été implémentée pour la première fois dans X11, suivi de X13, X15, X17. Celles-ci fonctionnent de la même façon mais avec plus d'algorithmes, ce qui signifie qu'il est plus difficile pour les machines spécialement conçues de hacher ces algorithmes.

Zelcash était basé sur Zcash pour ses technologies de confidentialité et les avantages obtenus grâce à ces technologies. Mais comme beaucoup de cryptomonnaies basées sur Zcash hérité de sa méthode et de son algorithme de consensus POW, il est devenu économiquement viable de créer des ASIC pour Equihash 200_9. Comme beaucoup de cryptomonnaies, BTCZ, BTG, SAFE et autres sont passées à un ensemble différent de paramètres N, K, 144_5, ils ont commencé à faire preuve de résilience face à ces fabricants d'ASIC.

L'équipe de développement de Zel a décidé d'échanger X16R pour Equihash 200_9 comme algorithme de hachage POW pour Zelcash. Le développement était déjà bien avancé, intégrant zk-SNARK dans l'algorithme de hachage et permettant de commencer le testnet, lorsque des rumeurs crédibles révélèrent que des FPGA / ASIC étaient en cours de développement pour X16R.

Alors que nous luttons contre les ASIC, les récents développements dans le matériel FPGA présentent un autre défi potentiel. Bien que CPU PoW serait l'idéal, nous comprenons que la plupart des communautés minières utilisent actuellement des GPU et qu'en fin de compte, nous avons tous une sorte d'affection pour les GPU. Le jeu se prête donc à la lutte contre les ASIC et à la préservation de l'exploitation des GPU.

Le développement sur l'algorithme X16R pour Zelcash a donc été arrêté. La quantité de travail nécessaire pour intégrer les fonctions de confidentialité dans X16R et ne toujours pas résister aux ASIC était trop élevée.

Pour ces raisons, Zelcash va échanger les algorithmes de hachage pour modifier Equihash avec des valeurs N, K de 144 et 5, la même approche que les autres monnaies confidentielles ont été utilisées récemment. Ce sera un "point d'arrêt" pour rester résistant aux ASIC et aux FPGA et laisser le temps d'explorer un chemin plus permanent. Des solutions sont constamment développées pour maintenir l'exploitation minière du GPU et conserver ainsi un écosystème décentralisé massif de puissance de hash. Une de ces idées est progPOW, qui sera étudiée et discutée par l'équipe de Zel dans les prochaines semaines. Une description approfondie des futurs algorithmes et stratégies sera décrite dans les prochaines versions de ce livre blanc.

Zel ayant pour objectif de créer un réseau décentralisé, il est logique de conserver la distribution de Zelcash elle-même, ce qui permet la création du réseau ZelDev, décentralisé et le plus distribué possible. Nous continuerons d'appliquer notre position de résistance aux ASIC. La mise à niveau de l'algorithme POW sera terminée fin juillet 2018.

Enfin, notre algorithme de difficulté passera de l'ancien Digishield V3 au LWMA de Zawy. La moyenne mobile pondérée linéairement de Zawy (LWMA) apporte une cohérence beaucoup plus grande aux temps de blocage et s'ajuste beaucoup plus rapidement que Digishield V3 à de grandes augmentations de hachage. Lors de nos tests, le LWMA de Zawy est plus de dix fois plus rapide lors du reciblage de blocs que Digishield V3. Le nouvel algorithme de difficulté permettra d'atténuer la puissance de hachage et les attaques d'horodatage, car Zel libère davantage de produits et apporte probablement davantage de puissance de hachage au réseau à mesure que le projet se développe. Ce déménagement sera également effectué dans le cadre de la mise à niveau du réseau Zelcash en juillet 2018.

4.4 Récompense de bloc

Au lancement, Zelcash a connu un démarrage lent de 5 000 blocs, après que le fonds de développement ait été miné, puis à partir du bloc 5 000, la récompense globale a été de 150 zelcash pour les mineurs. Au fur et à mesure que le développement de ZelNodes se développera, nous le modifierons pour prendre en compte l'incitation à la propriété des nœuds et, à ce titre, nous verrons un changement dans les récompenses. Ceci doit être guidé par l'équipe et décidé par la communauté au cours des prochaines semaines à partir de la publication de cet article.

L'intention des systèmes de récompense par blocs ajustés sera de garantir la valeur à la fois à la communauté minière basée sur PoW et à la propriété de ZelNode. Cette échelle sera glissante et donc ajustée au besoin pour garantir un modèle de récompense approprié pour tous.

La récompense de bloc sera réduite de moitié tous les 2 ans et demi, à compter de la date du bloc de la genèse.

4.5 Zelnodes

Le concept de ZelNodes est né d'une discussion sur la manière d'élargir une plate-forme, un réseau d'applications, de développement et de contrats intelligents décentralisés, tels que Ethereum. Des projets tels que Lisk, Neo et d'autres ont pu le faire. Cependant, ils courent le risque de s'éloigner de la décentralisation, offrant plutôt les avantages de la technologie blockchain d'une manière quelque peu accessible.

Ethereum est décentralisé, il fait donc face à des problèmes de mise à l'échelle, comme tous les réseaux décentralisés semblent le faire. Avec les DApps telles que Crypto Kitties, qui mettent le réseau Ethereum à genoux, le résultat est que les transactions coûteuses sont lentes et qu'elles augmentent le coût d'interaction avec les contrats intelligents opérant sur son réseau.

Ce n'est pas seulement une question de coût ; Cela pourrait causer des problèmes dans les DAO et dans de nombreuses autres applications fonctionnant sur le réseau, ce qui le rend inacceptable dans le monde connecté dans lequel nous vivons. En créant un réseau incitatif, dans la même veine que DASH, Zelcash nous permet de créer un réseau de nœuds véritablement décentralisé et distribué. Cela permettrait un réseau évolutif, similaire à Ethereum, avec un débit transactionnel beaucoup plus élevé. Utilisant ZelChains (sidechains) permettant plus de transactions par seconde.

Cela est nécessaire si nous voulons passer à un Internet décentralisé. Ethereum ne peut actuellement pas s'adapter à ces exigences. Uber fournit un exemple concret : avec 12 trajets par seconde, le réseau saturerait, ce qui signifie qu'un concurrent tel que Lyft ne pourrait pas opérer sur le même réseau. Bien que la vision de Vitalik Buterin visât potentiellement 1 million de transactions par seconde (TPS), il est actuellement de 15-20. Avec des concepts tels que le sharding en cours de développement, il est toutefois possible qu'Ethereum puisse atteindre de tels nombres.

Nous ne sommes pas enclins à donner un nombre aléatoire sans preuves tangibles, mais théoriquement basé sur un POC (proof of concept). Le réseau Zel pourra atteindre un TPS plus élevé qu'Ethereum en moins de temps. Avec l'évolutivité apportée par ZelNodes, nous pourrions théoriquement faire correspondre le TPS du réseau VISA. Notez que cette estimation de plus de 1000 TPS n'est que cela, une estimation. Nous aimons prouver notre technologie avant d'offrir des chiffres susceptibles de changer, mais nous considérons que c'est une estimation prudente.

Nous ne spéculerons pas sur le vrai TPS tant que Mainnet ne sera pas lancé et approuvé pendant plusieurs mois, afin que nous puissions livrer un nombre réaliste qui n'est pas hyperbolique ou non testé.

4.6 Economie Zelnode

Les nœuds incentivisés utilisés pour sécuriser le réseau et le processus de transaction d'une monnaie existent depuis la création de DASH, une monnaie électronique. Depuis lors, de nombreux projets ont ajouté la plate-forme de Masternodes (MNs) comme moyen d'inciter les détenteurs de monnaies à bloquer l'approvisionnement en pièces et de dynamiser le commerce actif et l'exploitation minière. Certains projets ont réussi à intégrer les MN, tandis que certaines nouvelles monnaies de micro-capitalisations ont utilisé l'allure des MN et des rendements massifs et irréalistes pour obtenir une croissance rapide de la communauté et des augmentations de capital, pouvant conduire à des arnaques, des baisses de ROI, etc. Pour créer un réseau de développement robuste et décentralisé de MN, nommé ZelNodes pour ce projet, la garantie et les récompenses doivent être conçues pour être réalistes et considérées comme un investissement à long terme.

ZelNodes sera une structure de noeud à trois niveaux, nécessitant trois niveaux différents de collatéralisation et de spécifications matérielles du système, et générant trois niveaux de récompenses. Les récompenses ZelNode seront distribuées aux détenteurs de nœuds à partir d'un bloc de chaque bloc miné dans un rapport de 25% à ZelNodes, 75% aux mineurs du PoW, et constituent une échelle mobile pour la croissance et les incitations futures, ce qui signifie que le rapport peut être ajusté légèrement au besoin pour maintenir un vaste réseau décentralisé de puissance de calcul (voir section 4.5 pour les cas d'utilisation). Un ZelNode nécessitera également une haute disponibilité, donc une disponibilité très stable est nécessaire pour recevoir la récompense du nœud ; le pourcentage de disponibilité requis sera publié plus près de la publication de ZelNodes.

Configuration matérielle requise pour le système ZelNode :

Spec. Type	**Zelnode basic**	**Zelnode super**	**Zelnode BAMF**
CPU	2 vCores	4 vCores	8 vCores
RAM	4GB	8GB	32 GB
Espace disque	50GB	150GB	600GB
Bande passante	2.5TB	4TB	6TB

Pour l'instant, les trois niveaux ZelNode sont nommés ZelNode Basic (collatéral le plus bas requis), ZelNode Super et ZelNode BAMF (garantie la plus élevée requise). Chaque niveau ZelNode a des exigences système VPS, ce qui se traduit par un niveau de service VPS plus coûteux. Tous les ZelNodes auront également une exigence de disponibilité, de sorte que les exigences de temps et de spécification du système seront testées par Zel pour garantir la conformité aux règles et que la distribution des récompenses est à juste titre méritée.

Structure de garantie et de récompense proposée :

Tier Level	**Collateral (ZEL)**	**Récompense % (de 25% de chaque bloc)**
ZelNode Basic	10,000	15%
ZelNode Super	25,000	25%
ZelNode BAMF	100,000	60%

Le large éventail de dimensions de la garantie permet à un grand nombre de personnes de participer au système ZelNode si elles le souhaitent, et la garantie / récompense de mise à l'échelle non linéaire est requise pour que, par exemple, 10 nœuds de base ne puissent pas gagner plus d'un nœud BAMF. Le modèle économique a été développé avec un prix de pièce estimé à 1 USD pour Zel à la fin de 2018. En tant qu'investissement à long terme, le coût associé à l'utilisation d'un ZelNode est relativement insignifiant et est supposé être de nature spéculative s'apparentant à l'extraction spéculative de GPU, où le profit instantané n'est pas la seule exigence de l'investisseur.

Avec la possibilité de modifier légèrement le taux de récompense des blocs, l'équipe de Zel a la capacité de maintenir un certain nombre de nœuds sur le réseau en augmentant la récompense si le nombre total de nœuds tombe en dessous d'un seuil situation. Cette fonctionnalité sera utilisée de manière extrêmement restreinte et est considérée comme un dernier effort pour maintenir l’adoption de ZelNode sur le réseau Zel.

5.0 Double économie

Zelcash est le mécanisme de transaction de la plate-forme Zeldev. Les processus, frais et services d'intégration seront directement liés à l'infrastructure de Zeldev et nécessiteront une pièce de monnaie Zel ; Cependant, nous étudions les évolutions possibles à long terme autour d'un "double modèle économique". Au fur et à mesure que les échanges décentralisés et les DApp sont développés, la vision d'une économie basée sur les services et d'une structure monétaire devra être développée.

Comprendre la nécessité d'un réseau solide de mineurs, de nœuds et de développeurs consolidera Zelcash et la plate-forme Zeldev. Au fur et à mesure que le développement de l'échange décentralisé (DEX) et de DApp prend de l'importance, il est essentiel de financer et de maintenir les développeurs. Comprenant que cela doit être considéré, un établissement de la Fondation est essentiel pour engager la communauté autour des modèles de financement à long terme.

6.0 Technologies Zel

Zel Technologies travaille sur divers projets et applications en plus de Zelcash. Celles-ci cohabitent et interagissent dans des relations symbiotiques au sein de l'écosystème de Zel.

Le projet a été fondé sur l'idée de créer un réseau de blockchains décentralisé composé d'une chaîne de type Ethereum, avec un débit transactionnel plus élevé grâce au consensus trouvé entre les opérateurs de ZelNode. La chaîne ZelDev sera lancée à partir de la chaîne de blocs principale Ethereumlike. ZelChains fonctionnera comme des chaînes latérales dans un environnement de type Lisk, permettant à ces chaînes de blocs de communiquer entre elles si nécessaire, tout en étant capable de gérer un débit transactionnel plus élevé et de bénéficier d'un fonctionnement réellement décentralisé.

Cela positionne Zel à :

- Résoudre les problèmes d'extensibilité auxquels Ethereum et les projets similaires sont confrontés ; et
- Permettre le développement évolutif des applications décentralisées, des contrats intelligents, des oracles décentralisés, des systèmes de vote, etc.

Avec cette initiative (lancée par Satoshi Nakamoto), nous nous éloignons d'Internet centralisé que nous connaissions tous il y a quelques années (et que nous utilisons encore aujourd'hui) pour créer un monde et un Internet décentralisé.

D'autres projets tels que ZelTreZ, ZelPay, Zel ID et d'autres nous permettent de créer cet écosystème pour développer des technologies pour l'avenir.

6.1 ZelTreZ

ZelTreZ est une plate-forme née du souhait de l'équipe de disposer d'une meilleure plateforme de portefeuille que celle offerte actuellement dans l'espace open source. Zel a commencé à développer un portefeuille léger et à nœud complet qui ne comprenait que Zelcash. Il a été conçu pour permettre aux utilisateurs de choisir les fonctionnalités dont ils ont besoin. Au début de ce développement, nous avons commencé à réaliser le potentiel de la plate-forme et, en tant que telle, l'idée s'est développée et s'est épanouie dans ce qu'elle est aujourd'hui. ZelTreZ est maintenant un portefeuille multi-actifs qui offre des options à la fois légères et complètes pour les utilisateurs.

Conçu pour être facile à utiliser avec une interface utilisateur nouvelle et légère, ZelTreZ est en train de devenir une passerelle pour le monde de la crypto-monnaie. Actuellement supportant ZEL, BTC, LTC, ZEC, ETH, BTCZ, RVN, BNB et HUSH, de nouveaux projets sont ajoutés toutes les deux semaines ainsi que des mises à jour et des améliorations de sécurité. ZelTreZ utilise le cryptage pour assurer la sécurité des utilisateurs ; Cela nous permet de créer des comptes sans stocker aucune information utilisateur à distance. Alors que le développement de Zel se poursuit, la mise en œuvre de ZelDev présentera notre réseau de développement décentralisé via ZelTreZ sous la forme de ZelDex, notre échange décentralisé qui sera proposé de manière native au sein de la plate-forme ZelTreZ.

En plus d'être une vitrine pour DApps, c'est aussi un portail pour les développeurs et les étudiants qui peuvent apprendre le développement de la blockchain et commencer à utiliser la plateforme ZelDev pour développer leurs propres applications DApps et blockchain. Actuellement disponible sous Windows, Linux et MacOS, ZelTreZ sera porté sur une application Web, le plug-in Chrome, Android et iOS, permettant des comptes et des connexions multi-périphériques sans stocker aucune information utilisateur sur notre infrastructure.

6.2 Zel ID

Zel ID est un système d'authentification conçu pour permettre aux utilisateurs de garder un contrôle total sur leurs identités numériques. Il permet potentiellement aux utilisateurs de conserver la propriété, les dossiers médicaux et d'autres informations sur un réseau décentralisé et crypté plutôt que sur papier ou sur des serveurs centralisés ; Cela donnera à l'utilisateur le contrôle de ses informations et de la confidentialité qui font défaut dans notre monde numérique actuel.

Zel ID est alimenté par les mêmes concepts de sécurité mis en avant par Authparty, un système d'authentification basé sur Bitcoin / Counterparty développé par Matthew Reichardt, membre de l'équipe Zel. Zel ID réalise une authentification sans épreuve en utilisant des signatures générées à partir des clés publiques et privées de votre portefeuille. Cela supprime pratiquement le besoin de 2FA, car l'authentification nécessite un accès de garde à votre portefeuille. Votre portefeuille, dans ce cas, ZelTreZ, serait aussi essentiel qu'un téléphone portable ou une connexion Internet.

Des identités d'authentification uniques, appelées Personas, sont ensuite générées et utilisées pour une authentification « zero-proof » avec des fournisseurs et des services tiers.

Le registre Zel fournit un accès API au protocole d'authentification Zel ID. Via une Persona générée, une nouvelle identité appelée Entity est alors générée et attachée au Persona. De cette façon, un service tiers s'authentifiant via Zel ID aurait trois degrés de séparation par rapport à votre identité de portefeuille réelle, ce qui permettrait différentes personnalités tout en offrant un potentiel d'anonymat.

6.3 ZelPay

Un logiciel simple mais essentiel, ZelPay pourrait être utilisé dans les terminaux de points de vente, dans les magasins ainsi qu'en tant que plugin de site web. ZelPay est conçu pour donner aux utilisateurs la facilité d'utilisation et la transparence, et pour offrir aux entreprises soit 0 frais soit 1% de frais sur les transactions.

L'avantage de ZelPay est une application unifiée qui offre une facilité d'utilisation en magasin et en ligne et permet aux propriétaires d'entreprise d'accéder à des niveaux élevés d'analyse et de détails des ventes pour les aider à grandir et à développer leur activité. ZelPay sera conçu pour permettre aux entreprises d'accepter non seulement toutes les devises cryptographiques de ZelTreZ, mais également les devises fiduciaires, dans une chaîne d'actifs diversifiée, soutenue par des USD, GBP, EUR, YEN ou de l'or et d'autres actifs. Cela permettrait un commerce plus libre et plus facile avec des capacités de TPS plus élevées que celles offertes par d'autres solutions de cryptomonnaie.

ZelPay proposera des options NFC (Near Field Communications) et QR-Code pour faciliter le paiement sans contact via l'application mobile ZelTreZ ainsi que les paiements e-commerce utilisant une méthode similaire, permettant une expérience transparente et rapide pour le client et le commerçant.

Une implémentation hypothétique pour ZelPay et d'autres applications de blockchain :

Nous avons déjà vu l'adoption de kiosques libre-service dans les épiceries, ce qui élimine le besoin de plusieurs commis humains. Au lieu de cela, un seul est nécessaire pour garantir le bon fonctionnement des machines et la vérification de l'identité pour ceux qui achètent de l'alcool. Pour approfondir cette idée, Amazon et d'autres sociétés testent des expériences de shopping sans personnel, et ces systèmes ont déjà été mis en œuvre dans certaines villes.

Ceci est réalisé grâce à un processus qui semble complexe mais qui, en fait, est aussi simple et naturel que l'utilisation d'un smartphone. Le client scanne un code QR pour entrer dans le magasin ; c'est leur panier. Lorsque le client entre, il choisit les articles qu'il souhaite et les place à la table de paiement. La table lit les autocollants RFID qui figurent sur les articles, génère un autre code QR ou autorise le paiement NFC, et le client est autorisé à partir avec ses produits. Ce système pourrait être amélioré, mais il constitue un excellent exemple de la manière dont la technologie peut améliorer l'expérience client et réduire les coûts pour les entreprises.

6.4 ZelDev

ZelDev sera conçu autour des développeurs pour rendre le travail avec la blockchain aussi facilement accessible que possible. Nous y parviendrons en donnant aux développeurs l'accès au ZelSDK et au BDK, ce qui facilitera l'adoption de la blockchain dans leurs projets nouveaux ou existants. Il y aura un template ZelChains pour aider les développeurs à démarrer et permettra aux développeurs d'interagir avec eux en utilisant Javascript. En outre, des modèles de contrat intelligents ainsi que des modèles de jetons seront disponibles, permettant également aux contrats intelligents d'être écrits en Javascript. Cela réduit la barrière à l'entrée pour les développeurs, car Javascript est le langage de programmation le plus utilisé. Pour gérer les transactions de jetons, celles-ci seront déchargées sur des chaînes de blocs distinctes qui, si nécessaire, communiquent avec la chaîne principale ZelDev. Cela permet également un débit transactionnel plus élevé et, par exemple, peut réduire l'impact lorsqu'une chaîne particulière est en maintenance.

Les détails techniques concernant la plate-forme ZelDev et les produits directement liés à celle-ci seront partagés ultérieurement.

6.5 ZelChains

La chaîne principale ZelDev avec ZelChains (chaînes latérales) sont des chaînes de blocs qui fonctionneront sur le réseau ZelNode. Cela permettra une véritable décentralisation de manière évolutive, car il est garanti que les ressources de calcul seront disponibles jusqu'au nombre total de ZelNodes associés sur le réseau Zelcash. Cela permet d'ouvrir d'autres chemins de ressource si un ou plusieurs ZelChains deviennent saturés et augmente considérablement le nombre total de transactions possibles par seconde que Zel peut traiter.

6.5 ZelDex

Actuellement, les échanges les plus importants pour les crypto-monnaies sont centralisés. Dans la plupart des cas, l'utilisateur ne possède pas ses clés privées sur les portefeuilles du commutateur et, à ce titre, ne possède pas la cryptomonnaie utilisée dans son « compte d'échange ».

Bien que les échanges centralisés offrent actuellement de bien meilleures expériences, de même que davantage de transactions par seconde, les échanges décentralisés s'améliorent. Avec de nouvelles offres permettant aux utilisateurs de contrôler leurs clés privées, nous sommes au début d'une révolution sur le marché des changes. Le principal problème qui freine l'adoption des échanges décentralisés est le problème de l'évolutivité due en partie à leur infrastructure.

ZelDex sera construit sur le réseau ZelDev comme une vitrine de ses capacités. L'interface sera conçue pour être simple à naviguer mais assez complexe pour les utilisateurs avancés. Avec une intégration directe dans ZelTreZ et une plate-forme autonome sur le Web et le mobile, ZelDex a pour objectif d'être le premier Dex avec une adoption massive.

De plus, les appels API ouverts permettront aux développeurs d'utiliser ZelDex dans leurs applications pour l'échange de jetons et de devises.

6.7 Dapp Store

Le magasin ZelDapp sera un hub central pour les applications décentralisées et certaines applications centralisées, avec un obstacle à l'entrée limité, et avec certaines règles et réglementations pour garantir la légalité. La boutique d'applications est conçue pour permettre aux développeurs d'accéder à une large base d'utilisateurs sur une solution multi-plateforme. ZelTreZ fonctionne comme un bac à sable pour ces Dapps, permettant un accès plus rapide et un temps de développement sans attendre l'approbation de certaines entreprises.

ZelDapps diffère des autres offres de blockchain par sa courbe d'apprentissage intrinsèquement faible. Le framework sera accessible via le SDK, qui sera probablement du langage Javascript, et éventuellement d'autres langages au fur et à mesure du développement de la plateforme. L'utilisation d'un langage de programmation extrêmement populaire garantit un accès facile aux outils de développement et à l'accessibilité à un large éventail de programmeurs professionnels et amateurs.

Chez Zel Technologies, nous pensons que les gens devraient pouvoir communiquer librement et sans restriction. À cette fin, un messager sera créé en tant que premier DApp. Il peut alors être suivi par une plate-forme de médias sociaux qui permet aux gens d'exprimer leurs opinions sans censure (dans le cadre de la loi).

Il y aura peu de frais sur le magasin ZelDApp. Il sera conçu pour être un marché libre et ouvert permettant aux développeurs d’atteindre les utilisateurs.

7.0 Directions et contributions au livre blanc

Fondateur – Miles Manley

Partenaire et développeur – Lumi Ibishi

Partenaire et développeur en chef – Tadeas Kmenta

Conseiller principal – Daniel Keller

Chef de projet et conseiller – Parker Honeyman

Respect à : 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

Pour le jour où il a été créé, Bitcoin a changé pour toujours la liberté financière pour ceux qui choisissent un chemin différent. La technologie est le meilleur niveleur, à tous ceux qui créent le futur, nous vous saluons!

-L’équipe Zel

8.0 Le futur de Zel

Zel sera un écosystème en développement continu. L'équipe est dédiée aux avantages mondiaux de la blockchain et de la crypto-monnaie. À cette fin, Zel s'engagera de manière proactive dans les technologies nouvelles et émergentes, les projets et le développement du leadership. Nous pensons que l'espace aura besoin de leaders pour introduire de nouvelles technologies, et nous aimerions être à l'avant-garde.

À l'avenir, l'équipe de Zel va :

- Continuer à développer de nouvelles technologies basées sur le modèle Zelcash dans les projets open source et privés.
- S'associer avec d'autres dans cet espace pour s'assurer que le projet est à l'avant-garde de l'espace crypto.
- Développer et encourager une communauté autour de la plateforme Zel qui guidera les valeurs et les livrables du modèle économique.
- Développer et promouvoir une branche caritative de la Fondation Zel pour l'amélioration de la qualité des autres grâce aux technologies émergentes.

9.0 Glossaire

Altcoin – Une cryptomonnaie autre que le Bitcoin

ASIC (application-specific integrated circuit) - Des puces en silicium spécialement conçues pour effectuer une seule tâche (hachage pour crypto). Dans le cas de Bitcoin, ils sont conçus pour traiter les problèmes de hachage SHA-256 pour miner de nouveau Bitcoin.

Technologie cross-chain - Permet à deux chaînes de blocs d'échanger des informations et des ressources cryptographiques en même temps.

DASH - Un type de crypto-monnaie basé sur le logiciel Bitcoin qui offre des fonctionnalités d'anonymat ; précédemment connu sous XCoin (XCO) et Darkcoin.

Monnaie Fiat - Les monnaies ayant une valeur intrinsèque minime ou nulle, mais définies comme monnaie légale par le gouvernement, telles que les billets et pièces.

JoinSplit - données incluses dans une transaction qui décrit un transfert JoinSplit, c'est-à-dire un transfert de valeur protégé. Ce type de transfert de valeur est l'opération principale spécifique à Zcash effectuée par les transactions.

Litecoin (LTC) - Cryptomonnaie créé par l'ancien employé de Google Charlie Lee en 2011. Il permet un traitement plus rapide à moindre coût.

NEO - Fait référence à la crypto-monnaie et au nom de la première chaîne de blocs open source de la Chine. Comme Ethereum, il peut exécuter des contrats intelligents ou des DApp, mais dans un environnement quelque peu centralisé.

Overwinter fork - Le tout premier fork de Zcash à adresser des mises à niveau de réseau et de performances, entre autres, afin de renforcer le protocole pour les futures mises à niveau du réseau.

Multi signature (multisig) - Les adresses multisig permettent à plusieurs parties d'exiger plus d'une clé pour autoriser une transaction. Les adresses multisig ont une plus grande résistance au vol.

Clé privée - Une clé privée est une chaîne de données qui confère un contrôle utilisateur à une clé publique et à une adresse pour autoriser les transactions de cryptomonnaie.

Proof of Stake ou preuve d'enjeu (POS) - Un algorithme qui récompense les participants qui résolvent des puzzles cryptographiques difficiles à atteindre pour parvenir à un consensus. Le PoS consomme moins d'énergie que le PoW.

Proof of word ou preuve de travail (POW) - Un algorithme qui récompense la première personne ou le premier groupe de personnes [pool] qui résout un problème de calcul pour parvenir à un consensus distribué.

Z-cash - Une des premières cryptomonnaies orientées confidentialité

Zel ID - Un système d'authentification qui crée une Persona en ligne pour l'utilisateur, à utiliser dans tous les aspects de la vie pour tout système de règles nécessitant la vérification et la validation d'une identité réelle.

ZelChains – Les chaînes secondaires qui s'exécuteront sur le réseau Zelcash fourniront une puissance de calcul et une évolutivité utilisable aux développeurs d'applications décentralisées.

ZelDev – La plate-forme permettant aux développeurs d'applications décentralisés d'interagir avec la chaîne de blocs Zelcash et ZelChains via des environnements SDK et BDK faciles à utiliser.

ZelDex – Un échange décentralisé créé par Zelcash pour fonctionner sur le réseau décentralisé et fourni via ZelTreZ et un portail Web autonome, ZelDex sera également une vitrine technologique pour ZelDev.

ZelNodes – Un réseau de puissance de calcul multi-niveaux et incitatif à utiliser par les développeurs Dapp et la propagation des jetons, robuste, évolutive et véritablement décentralisée.

ZelTreZ – La plate-forme frontale de Zelcash, ZelTreZ est un portefeuille chiffré multi-actifs, qui hébergera Dex, gérera les portefeuilles ZelNode et contiendra le Dapp Store.

Zk-SNARK – Un protocole de confidentialité mis au point dans la cryptomonnaie par Zcash qui permet des transactions protégées garantissant l'anonymat des utilisateurs finaux. (Voir le livre blanc Zcash pour une explication technique)

Ressources

[1] Nakamoto S. (2008) : Bitcoin : un système électronique peer-to-peer

[2] Daira Hopwood, Sean Bowe, Taylor Hornby, Nathan Wilcox. (2017) Protocole Zcash Spécification Version 2017.0-beta-2.5.

[3] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, et Madars Virza. (2014) Zerocash: les paiements anonymes décentralisés de Bitcoin

[4] Vitalik Buterin et le projet Ethereum : Un contrat intelligent de nouvelle génération et une plate-forme d'application décentralisée, Ethereum

[5] Tron Black et Joel Weight : Conception résistante aux ASIC X16R