BROUILLON

Cette traduction est une version préliminaire. Si vous voyez des erreurs et souhaitez contribuer, contactez notre équipe avec une version mise à jour!

Livre blanc Zen

Robert Viglione,
Rolf Versluis,
et Jane Lippencott.

Mai 2017

RÉSUMÉ

Zen est un système crypté de bout à bout, doté d'une technologie à divulgation sans connaissance (zero-knowledge technology) sur laquelle les communications, les données ou la valeur peuvent être transmises et stockées en toute sécurité. C'est une combinaison de technologies révolutionnaires qui créent un système sur lequel l'innovation peut s'accélérer en combinant trois fonctions traditionnellement réalisées séparément:

1) transactions 2) communication et 3) gouvernance compétitive. Cela se fait de manière sécurisée et anonyme, en utilisant une chaîne de blocs (blockchain) et une infrastructure informatique réparties dans le monde entier. Le système intègre plusieurs technologies de premier ordre afin de former une plate-forme ouverte pour l'innovation sans permission et qui évolue d'après les préférences de l'utilisateur..

Les auteurs peuvent être contactés à rob@zensystem.io, rolf@zensystem.io, et jane@zensystem.io, respectivement. Nous tenons également à remercier Jake Tarren pour les commentaires et les suggestions, ainsi que l'ensemble des communautés Zclassic et Zen pour nous avoir aidé à développer ces idées et à rendre ce mouvement possible.

CONTENU

media@zensyster

OBJECTIF

“Critiquer en créant.” - Michelangelo Buonarroti

Nous vivons dans un monde hyper-réglementé et surveillé où des milliers d’individus sont privés de droits humains fondamentaux, tels que la propriété, la vie privée, la libre-association et l’accès à l’information. La technologie existe désormais pour résoudre certains de ces problèmes, et la mise en œuvre anticipée de Zen accomplira exactement cela.

Zen est une collection de produits, de services et d’entreprises construits autour d’un ensemble de technologies habilitantes qui utilisent des preuves sans divulgation de connaissance et un ensemble de valeurs fondamentales. En tant que système de chaîne de blocs distribués tirant parti des dernières techniques d’élimination de la censure, des communications entièrement chiffrées et d’un modèle social et de gouvernance conçu pour une viabilité à long terme, Zen contribuera au droit à la vie privée et fournira l’infrastructure de réseautage nécessaire pour que chacun puisse collaborer et construire de manière sécurisée dans un écosystème sans bornes. Notre mission est d’intégrer les dernières technologies disponibles post-Satoshi avec un ensemble décentralisé, volontaire et pacifique de structures sociales pour améliorer la vie de tous ceux qui veulent participer. Nous croyons que le temps de cette idéologie est venu.

Le cadre de Zen est une infrastructure sécurisée et axée sur la vie privée dotée d'un système de gouvernance structuré pour permettre aux participants d'étendre leurs fonctionnalités de façon collaborative dans de nombreux aspects. Les opportunités incluent : l'hébergement de données d'identification individuelle, de preuves sélectives de titre de propriété, les services bancaires décentralisés, l'échange d'actifs p2p / b2b de protection de la vie privée, les sociétés d'entraide, l'assurance p2p, les mécanismes d'aide humanitaire décentralisés ou l'utilisation purement comme une unité de valeur anonyme.

Ces fonctions peuvent être utilisées pour servir les populations privées de droit actuellement exclues des services vitaux tels que les services bancaires et de santé en raison du manque d'identification, de capital et de réseaux de distribution sécurisés. Elles peuvent également être exploitées par des personnes qui souhaitent garder le contrôle de leurs données privées, ou, par exemple, par des communautés entreprenantes qui souhaitent élaborer un système d'appel d'offres concurrentiel sur l'énergie solaire générée en interne. Les implémentations uniques sont illimitées, le lien commun étant la conviction que la décentralisation est le moteur du progrès moral et que les solutions participatives sont les plus créatives et durables.

HISTOIRE

Zen s'appuie sur l'héritage des meilleures crypto-monnaies, l'architecture de réseau et les systèmes de partage distribués en incorporant des fonctionnalités existantes et nouvelles pour produire une base solide conçue pour une viabilité à long terme. Tout aussi important que notre plate-forme technologique, nous nous appuyons sur les dernières idées en matière de consensus distribué et de gouvernance compétitive. Certains des fondements de notre projet viennent de Bitcoin, Dash, Decred et Seasteading.

Zcash a étendu Bitcoin avec des transactions blindées totalement anonymes, de sorte que les utilisateurs puissent choisir entre des adresses Bitcoin (adresses t) classiques ou des adresses blindées résistantes à l'analyse de corrélation du traffic (adresses z). Par la suite, nous avons créé Zclassic, un clone de Zcash qui a changé certains paramètres clés que notre communauté a estimés importants: nous avons supprimé à la fois la récompense aux fondateurs de 20% et le démarrage ralenti (slow start) de l'offre monétaire. Depuis le lancement de Zclassic, nous avons formé une communauté open source dynamique désireuse de faire avancer la technologie dans une direction particulière. Certaines accomplissements antérieurs comprennent l'élaboration d'une application open source pour Zcash et Zclassic, ainsi que des portefeuilles Windows et Mac.

Notre équipe s'est rendue compte que Zclassic pourrait être étendu comme un réseau entièrement chiffré avec un modèle économique et de gouvernance novateur qui s'harmonise mieux avec la vision originale de Satoshi d'une communauté globale décentralisée. Nous considérons Zclassic comme un projet de crypto-monnaie open-source fondamentalement pur, basé sur le volontariat, tandis que Zen s'étend à une plate-forme avec un financement interne pour faciliter un ensemble plus large de communications, de partage et d'activités économiques.

SPÉCIFICATIONS AU LANCEMENT

Zen est le système global sur lequel les jetons ZenCash se diffusent, similaire à des projets tels qu'Ethereum et son jeton Éther. ZenCash est conçu comme une bifurcation de Zclassic et sera étendu avec les fonctionnalités supplémentaires suivantes.

1. Date de sortie: 8PM EDT, 23 mai 2017 en tant que bifurcation de ZClassic (0:00 UTC).

2. Algorithme « Equihash » de hachage, qui est un algorithme d'extraction de mémoire et de démonstration basé sur le problème « Birthday » généralisé et l'algorithme de Wagner. Equihash a été créé par Alex Biryukov et Dmitry Khovratovich de l'Université du Luxembourg.

3. Récompense de bloc: 12.5 ZenCash.

4. Production de blocs: 2,5 minutes.

5. Taille du bloc: 2 Mo.

6. Algorithme d'ajustement contextuel: Digishield V3, ajusté pour utiliser la fenêtre suivante de difficulté moyenne :

   Difficulté suivante = Difficulté précédente × Racine carrée (150 secondes / Dernier temps de résolution)

7. Division de chaque récompense en bloc PoW et frais de transaction entre mineurs et autres parties prenantes:

   (a) 88% pour les mineurs.

   (b) 5% à un ou plusieurs DAO.

   (c) 3,5% pour les opérateurs de nœuds sécurisés.

   (d) 3,5% à l'équipe de base.

8. Total éventuel du nombre de jetons : 21 millions.

9. Récompense réduite de moitié chaque 4 ans environ, par comme avec Bitcoin .

10. Transactions protégées obscurcissent l'expéditeur, le récepteur et le montant de la chaîne de bloc.

11. Les transactions transparentes publient l'expéditeur, le destinataire et le montant sur la chaîne de bloc.

12. Champ de message sécurisé par transaction z avec 1024 octets de caractères:

   (a) Publication sécurisée sur les sites GNUnet et / ou IPFS.

   (b) Messages courts entre les utilisateurs.

   (c) Publiablesez sur les canaux pouvant être consultés par n'importe qui avec un portefeuille capable de créer incluant des fonctionnalités de support des canaux.

13. Les nœuds sécurisés exécutent des fonctions d'infrastructure:

   (a) Assurer que toutes les communications réseau sont cryptées entre les

nœuds.

(b) Maintenir la chaîne de bloc ZenCash complète..

(c) Fournir des connexions de cryptage basées sur des certifications pour les applications de portefeuille ZenCash.

14. Les nœuds sécurisés répondant aux exigences reçoivent des récompenses sous forme de jetons.

15. Service de réception de domaine pour les transactions z à l'aide d'un CDN commercial.

16. Gouvernance par un ou plusieurs DAO. (Voir la section Gouvernance).

17. Zen DAO responsables des opérations et l'amélioration continue du système. Ils vont construire et opérer:

They will build and operate:

(a) La diffusion de l'information Zen (Web, wiki, blog, média).

(b) Le système de proposition et système de vote.

(c) Systèmes de rapports et de surveillance.

18. L'Équipe de base:

(a) Incluts les fondateurs de Zen.

(b) Leur mission est de guider le lancement, la croissance et le développement.

(c) Financent les dépenses importantes pour le développement et la maintenance.

(d) Opèrent au croisement des systèmes Zen et traditionnels.

FEUILLE DE ROUTE

“La liberté, c’est (l’apprentissage) par (le processus) d’essai et erreur (trial & error). »(Taleb, 2012)

Zen est lancé comme l’intégration de technologies révolutionnaires pour créer un système sur lequel l’innovation peut s’accélérer. Nous structurons une décentralisation optimale et une concurrence persistante afin que le système évolue constamment et n’atteigne jamais un plateau de confort. La feuille de route initiale couvre une fenêtre de développement de 12 à 18 mois pour permettre au système de fonctionner de manière autonome. La clé en est l’établissement du principal ensemble d’intégrations avec notre propre réseau de noeuds sécurisés, un système de stockage de données distribué comme GNUnet et l’écosystème plus large d’échanges, de pools d’exploration et de communauté d’utilisateurs. ZenCash doit être pleinement opérationnel, facilement disponible et utile à un ensemble varié d’intervenants.

Notre feuille de route rappelle l’accent sur ZenCash comme notre premier et plus important produit dans le portefeuille Zen.

1. Développer de portefeuilles améliorés.
   (a) Windows pour transactions t et z, messagerie, publication GNUnet.
   (b) Linux pour les transactions t et z, messagerie, publication GNUnet.
   (c) Mac pour les transactions t et z, messagerie, publication GNUnet.
   (d) Mobile (Android et iOS) pour les transactions t et z.
   (e) Matériel pour transactions t et z, messagerie, publication GNUnet.
   (f) Portefeuille Web pour transactions t, z, messagerie et édition GNUnet.

2. Service de réception de domaine pour les transactions z à l'aide d'un CDN commercial.

3. Serveurs de systèmes Zen dans une configuration résiliente de centres de données multiples.

4. Test d'élasticité d'infrastructure, résultats et améliorations.

5. Mise en place du « Segregated Witness »

6. Gérer les livrables de Recherche & Développement liés aux aspects de gouvernance, y compris le système opérationnel entièrement testé (voir la section Gouvernance):

   (a) Rapport de recherche.

   (b) Constitution.

   (c) Système de vote testé et mis en place.

   (d) Premières élections se déroulaent au moins sur un DAO, l'équipe de base de transition.

ÉLÉMENTS FONCTIONNELS

Zen rassemble de nombreux éléments différents pour former un ensemble de travail. Au lieu de nœuds réguliers, Zen nécessite des noeuds sécurisés, ce qui garantit que les nœuds maintiennent un niveau de sécurité et de performance de base pour s'assurer que le système reste distribué, résilient et sécurisé. En imposant la communication cryptée entre les nœuds, et entre les nœuds et les portefeuilles, Zen protège contre les interférences et les attaques de type « man-in-the-middle ».

Zen s'attaque également à la faiblesse des métadonnées d'autres crypto-monnaies. Par exemple, en communiquant de manière potentiellement compromise, puis en envoyant des Bitcoins, les participants à une transaction Bitcoin sont potentiellement exposés à l'identification par des corrélateurs de transaction. ZenCash intégrera des messages sécurisés dans des transactions blindées, afin que les utilisateurs puissent accepter la transaction, l'envoyer, puis vérifier leur réception. Ces éléments fonctionnels se manifesteront dans les systèmes suivants:

ZenTalk - Un nouveau type de réseau de communication sécurisé qui permet une communication à un ou plusieurs en utilisant la chaîne de blocs pour stocker des messages de manière permanente.

ZenPub - Une plate-forme de publication de documents anonymes utilisant GNUnet ou IPFS.

ZenHide - La possibilité d'éviter le blocage du crypto-commerce à l'aide de l'interface de domaine.

5.1 T transactions

Les transactions T sont les transactions traditionnelles enregistrées sur une chaîne de-blocs contrôlées par une clé privée dans un porte-monnaie. Celles-ci sont dérivées de Bitcoin et permettent une compatibilité rapide avec les échanges, les portefeuilles et d'autres applications écosystémiques dérivées de Bitcoin.

5.2 Z transactions

Il s'agit de transactions envoyées à des adresses blindées, telles qu'elles sont transmises par Zcash et Zclassic. Les soldes dans les adresses blindées sont privés. Si vous dépensez pour une ou plusieurs adresses blindées, la valeur reste privée, mais toutes les adresses transparentes à l'extrémité réceptrice déprotègeront le jeton et révéleront la valeur reçue sur la chaîne de bloc. Les adresses blindées d'entrée et le fait que la valeur ait été envoyée d'une ou deux d'entre elles restent confidentiel lorsqu'elles sont désolidarisées. Le protocole Zcash décrit ce processus en détail:

> La valeur dans Zcash est soit transparente, soit protégée. Les transferts de valeur transparente fonctionnent essentiellement comme dans Bitcoin et ont les mêmes propriétés de confidentialité. La valeur protégée est portée par des messages, qui précisent un montant et une clé de paiement. La clé de paiement fait partie d'une adresse de paiement, qui est une destination à laquelle les messages peuvent être envoyés. Comme dans Bitcoin, cela est associé à une clé privée qui peut être utilisée pour passer des messages envoyées à l'adresse; dans Zcash, cela s'appelle une clé de dépenses.
>
> À chaque message, l'engagement de message est associée cryptographiquement et un annulateur (nullifier) 1 (de sorte qu'il existe une relation 1: 1: 1 entre les messages, les engagements de message et les annulateurs). Le calcul de l'annulateur nécessite la clé de dépenses privée associée. Il est impossible de déduire l'engagement de message avec l'annulateur correspondant sans avoir au moins reconnu cette clé de dépenses. Un message

valide non dépensé, à un point donné de la chaîne des blocs, est celui pour lequel l'engagement du message a été révélé publiquement sur la chaîne de blocs avant ce point, mais l'annulateur n'a pas été dévoilé.

Une transaction peut contenir des entrées, des sorties et des scripts transparents, qui fonctionnent tous comme Bitcoin [Bitcoin-Protocol]. Il contient également une séquence de zéros ou plus de descriptions JoinSplit. Chacun d'eux décrit un transfert JoinSplit qui prend une valeur transparente et jusqu'à deux messages d'entrée, et produit une valeur transparente et jusqu'à deux messages de sortie. Les annulateurs des messages d'entrée sont révélés (les empêchant d'être dépensés à nouveau) et les engagements des messages de sortie sont révélés (ce qui leur permet de passer à l'avenir). Chaque description JoinSplit comprend également une preuve zk-SNARK fonctionnant en calcul, ce qui prouve que toutes les valeurs suivantes sont présentes sauf avec une probabilité négligeable:

La balance des valeurs d'entrée et de sortie (individuellement pour chaque transfert JoinSplit).

Pour chaque message de saisie de valeur non nulle, il existe un engagement de message révélé pour ce message.

Les prouveurs connaissaient les clés de dépenses privées des messages d'entrée. Les annulateurs et les engagements de message sont calculés correctement.

Les clés de dépenses privées des messages d'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 connaissait pas ces clés privées.

Chaque message de sortie est généré de telle sorte qu'il est impossible de faire en sorte que son annulateur entre en collision avec l'annulateur de tout autre message.

En dehors de zk-SNARK, il est également vérifié que les annulateurs pour les messages d'entrée n'avaient pas encore été révélés (c'est-à-dire qu'ils n'avaient pas déjà été dépensés).

Une adresse de paiement comprend deux clés publiques: une clé payante correspondant à celle des messages envoyés à l'adresse et une clé de transmission pour un schéma de chiffrement asymétrique à clé-privée. « Clé privée» signifie que les chiffrages ne révèlent pas l'information sur la clé à laquelle ils ont été chiffrés, sauf pour le titulaire de la clé privée correspondante, qui est appelée la clé de visualisation dans ce contexte. Cette installation permet de communiquer une sortie de messages cryptées sur la chaine de blocs à leur destinataire prévu, qui peuvent utiliser la touche de visualisation pour analyser la chaîne de blocs pour les messages qui leur sont adressées, puis décrypter ces messages.

La base des propriétés de protection de la vie privée de Zcash est que lorsqu'un message est dépensé, le décideur prouve seulement qu'un certain engagement a été révélé, sans révéler lequel. Cela implique qu'un message dépensé ne peut pas être liée à la transaction dans laquelle elle a été créée. C'est-à-dire, du point de vue d'un adversaire, l'ensemble des possibilités d'une entrée de message donnée à une transaction, son ensemble de traçabilité de message, comprend tous les messages précédents que l'adversaire ne contrôle pas ou ne sait pas avoir été dépensé. Cela contraste avec d'autres propositions pour les systèmes de paiement privés, tels que CoinJoin ou CryptoNote, qui sont basées sur le mélange d'un nombre limité de transactions et qui ont donc des ensembles de traçabilité de messages plus petits.

Les annulateurs sont nécessaires pour éviter les dépenses doubles: chaque message n'a qu'un annulateur valide, et donc essayer de passer un message deux fois révélerait l'annulateur deux fois, ce qui entraînerait le rejet de la deuxième transaction.

5.3 ZenTalk

Les transactions Z dans ZenCash ont la possibilité d'incorporer des messages textuels, qui sont cryptés et inclus dans la chaîne de blocs. Il existe une limite de 1024 caractères pour ces messages, et ils améliorent la capacité des utilisateurs à effectuer un commerce sécurisé. Au lieu de discuter de la transaction dans d'autres canaux moins sûrs qui peuvent ne pas avoir le même niveau d'amélioration de la vie privée que Zen, les utilisateurs peuvent communiquer via les messages ZenTalk avec l'autre partie ou les parties avant et après le transfert blindé avec une très petite transaction z. Ces messages peuvent être envoyés directement d'une adresse z à l'autre, et ils peuvent également être envoyés à un canal. En générant une adresse z à partir du hachage d'un nom de chaîne, les utilisateurs peuvent s'abonner à la chaîne et lire tout ce qui a été publié par quelqu'un sur le canal.

Par exemple, les annonces de la chaîne #ZenCash hacheraient zXXXXXXXXXXXX, permettant à tout utilisateur d'envoyer un message anonyme au canal. Chaque message coûterait un montant minimal de ZenCash à envoyer, car il est contenu dans des transactions z, réduisant ainsi la quantité de messages non utiles sur les canaux communs. Les annonces officielles seraient signées par clé privée et ne seraient affichées que si elles étaient jugées valides. En outre, des messages de groupe essentiellement privés peuvent être publiés à l'aide de transactions z en créant un nom de chaîne complexe, puis en chiffrant le contenu du message avec des clés souhaitées que les destinataires détiennent. Les messages ZenTalk seraient chiffrés avec des algorithmes tels que AES-256 avec Perfect Forward Secrecy (PFS), correspondant aux normes actuelles de cryptage pour une communication sécurisée.

5.4 ZenPub

Zen a la possibilité de publier des documents sur IPFS ou GNUnet. Cela se fait en publiant une adresse IPFS ou GNUnet dans le champ texte de l'adresse z. Le système préféré de publication de documents en ce moment est GNUnet, car il

fournit l'infrastructure requise pour l'édition anonyme et maintient une base de données active de documents. Le système est également extensible à IPFS ou à tout autre système d'archivage de distribution futur. En créant une couche de messagerie anonyme en conjonction avec une couche de publication anonyme, ZenPub permet la création de publications vraiment anonymes qui peuvent être rapidement distribuées aux lecteurs intéressés.

5.5 ZenHide

Il est possible pour les régulateurs dans les pays hostiles au crypto-commerce de bloquer les crypto-monnaies traditionnelles comme Bitcoin et même Zcash. Zen utilise le Domain Fronting (front de domaine) pour étendre la capacité à compléter les transactions dans les environnements de réseau conflictuel, comme expliqué dans la communication résistante au blocage par le biais du résumé concernant le Domain Fronting :

> Nous décrivons le « domain fronting » comme une technique de contournement de censure polyvalente qui masque le point de terminaison distant d'une communication. Le front de domaine fonctionne sur la couche d'application, en utilisant HTTPS, pour communiquer avec un hôte interdit tout en communiquant avec un autre hôte, autorisé par le censeur.
>
> L'idée clé est l'utilisation de différents noms de domaine à différentes couches de communication. Un domaine apparaît sur l'extérieur d'une requête HTTPS - dans la demande DNS et l'indicateur de nom de serveur TLS, tandis qu'un autre domaine apparaît sur l'intérieur - dans l'en-tête du hôte HTTP, invisible à la censure sous cryptage HTTPS.
>
> Un censeur, incapable de distinguer le trafic frontal et non frontal, doit choisir entre permettre le contournement et bloquer entièrement le domaine, ce qui entraîne des dommages collatéraux coûteux.
>
> Le front de domaine est facile à déployer et à utiliser et ne nécessite pas de coopération spéciale par les intermédiaires de réseau. Nous identifions

un certain nombre de services Web difficiles à bloquer, tels que les réseaux de distribution de contenu, qui prennent en charge les connexions aux domaines et sont utiles pour le contournement de la censure.

La mise en œuvre spécifique du Domaine Fronting utilisée par Zen au lancement est avec un réseau de distribution de contenu commercial, mais comme dans tous les aspects de notre architecture, la flexibilité est conçue dès le début et le système peut s'étendre dans de nombreuses directions à mesure que la technologie évolue.

5.6 Noeuds sécurisés Zen

Les nœuds sont les principaux systèmes qui maintiennent la chaîne de blocs (blockchain), acceptent les transactions à partir de portefeuilles, valident les solutions des mineurs et agissent comme un système de calcul et de communication décentralisé pour les crypto-monnaies. Dans Zen, toutes les informations transmises vers et depuis les Nœuds sécurisés sont cryptées avec des certificats valides à l'aide de la version 1.3 de TLS et protégées de plus avec Perfect Forward Privacy (PFS). Dans le cadre de la fonctionnalité de Nœuds Sécurisés (Secure Nodes), l'application ZenCash améliore les fonctionnalités en:

Etendant RPC pour permettre aux données chiffrées avec AES de résider dans des transactions blindées

Etendant RPC pour permettre une poignée de main (handshake) utilisant Perfect Forward Privacy (PFS) entre les clés publiques

Les nœuds sécurisés (Secure Nodes) qui répondent à toutes les exigences seront récompensés par la partie « nœud sécurisé » du minage via une file d'attente. Les nœuds sécurisés doivent surveiller le canal #secure node. Le système de paiement Secure Node est destiné à être exploité de manière vérifiable avec des normes claires pour maximiser l'exploitation et minimiser les problèmes.

1. Fonctions d'infrastructure de base réalisées par Secure Nodes:

(a) S'assurer que toutes les communications réseau sont cryptées entre les nœuds.

(b) Maintenir une chaîne de blocs Zen complète.

(c) Fournir des connexions de cryptage basées sur des certifications pour les applications de portefeuille ZenCash.

2. Les nœuds sécurisés répondant aux exigences décrites ci-dessous reçoivent 3,5% de la récompense de la cotation des blocs d'une manière qui récompense le temps de disponibilité en opérant avec toutes les fonctionalités activées:

(a) Opérer un logiciel de nœud sur un système capable tel que spécifié par les exigences d'infrastructure.

La mémoire recommandée est supérieure à 4 Go.

(b) Maintenir la chaîne complète de blocs ZenCash sur le système.

(c) Fournir un certificat SSL valide au logiciel ZenCash Node à utiliser pour la communication avec d'autres nœuds et portefeuilles.

(d) Maintenir au moins 42 ZenCash sur le serveur dans une adresse t pour la participation.

(e) Surveiller le canal SecureNode pour les messages de défi de SecureNodeHQ environ toutes les 10 minutes (inclus dans un champ de message de transaction z).

(f) Répondre au défi avec l'information d'identification du nœud sécurisé.

(g) La réponse au défi sera une combinaison de deux éléments:

i. Envoi d'un message blindé à SecureNodeHQ contenant l'adresse publique t et l'emplacement du document GNUnet dans le

champ de message.

ii. Publier un document à GNUnet signé avec une adresse t privée incluant:

A. Adresse T publique de participation Zen, qui sera également utilisée pour le paiement de récompense.

B. Certificat SSL et adresse IP.

C. En-tête de bloc (block header) provenant de la chaîne de blocs (blockchain).

D. D'autres informations qui peuvent être nécessaires pour s'assurer qu'il s'agit d'un serveur unique.

(h) Chaque Nœud Zen Secure doit également être un pair sur les systèmes GNUnet pour publier la réponse au défi anonymement et soutenir les publications anonymes à partir d'autres éléments du système.

(i) D'autres besoins potentiels qui pourraient se présenter à l'avenir pour permettre au système ZenCash d'utiliser les Nœuds sécurisés pour un consensus et une puissance de calcul.

3. Système de paiement des Nœuds Sécurisés Zen (Z-SNPS):

(a) Z-SNPS exploité par un DAO Zen.

(b) Z-SNPS suivra les réponses au défi de chaque Nœud sécurisé.

(c) Les nœuds sécurisés seront suivis et publiés par leurs adresses t.

(d) Chaque bloc miné paiera une récompense de 3,5% au système ZC-SNPS, qui distribuera périodiquement les ZenCash aux Nœuds Sécurisés en fonction de leur temps de disponibilité pendant chaque période distincte.

Parce que Zen dispose d'un réseau informatique distribué sous la forme de Nœuds sécurisés compensés, ces nœuds peuvent être amenés à fournir d'autres services informatiques pour le réseau en fonction de l'évolution du consensus communautaire.

5.7 Noeuds Standard Zen

L'application ZenCash peut fonctionner sur n'importe quel serveur linux, Mac ou PC. Le client agit à la fois comme un nœud et un portefeuille. Bien qu'il ne dispose pas de la capacité de cryptage complète d'un noeud sécurisé, tous les noeuds aident le système à exécuter correctement ses fonctions tout en restant résilient aux attaques.

5.8 Logiciel de portefeuille ZenCash

Le logiciel ZenCash peut être utilisé comme un porte-monnaie. La version ligne de commande (command line) du portefeuille est la forme de base, mais des versions basées sur l'interface utilisateur graphique (GUI) existent déjà pour les systèmes d'exploitation bureau (desktop). Les versions Mobile, Web, Raspberry Pi et autres portefeuilles physiques font partie des tâches de développement hautement prioritaires pour améliorer l'expérience utilisateur et la sécurité des jetons ZenCash. Les portefeuilles peuvent être configurés pour utiliser n'importe quel nœud ZenCash disponible pour la communication, ou peuvent être configurés pour se connecter uniquement à des Nœuds Sécurisés afin de maintenir des normes élevées de sécurité de l'information.

5.9 Applications

Zen est ce que nous considérons comme un projet Open Source décentralisé de manière optimale, et nous nous attendons à ce que de de nombreuses parties tierces créent des applications et contribuent à l'écosystème. Beaucoup de ces contributions seront probablement offertes en mode open source libre, mais

nous nous attendons à ce qu'une communauté commerciale solide se développe également autour de la plate-forme. En outre, l'équipe de base dispose d'un plan de développement d'applications complet qui est déjà en cours. Cela inclut, mais sans s'y limiter:

Application de nœud
Pool de minage Open Source Equihash
Applications de Gouvernance
Systèmes de suivi et de rapports
Portefeuilles de tous types
Système de surveillance de nœud sécurisé
Système de paiement de nœud sécurisé

GOUVERNANCE

“Ainsi les idéologies ne tombent: non pas par la violence mais par des exemples démontrant une meilleure manière de faire » -Joe Quirk, Institut Seasteading.

Zen est conçu avec un modèle de gouvernance décentralisé intégrant l’autonomisation des parties prenantes et l’aptitude à évoluer pour s’adapter de manière optimale à notre communauté. Fondamentalement, notre philosophie de gouvernance est que nous ne connaissons pas a priori la meilleure approche, mais nous avons des idées sur la façon d’initialiser le système et de lui permettre d’évoluer avec les besoins de la communauté. Nous croyons en la gouvernance en tant que service (GaaS) et visons à fournir une valeur efficace à nos acteurs directs, à la communauté élargie et au monde.

“Toute industrie qui offre un service médiocre pour un prix élevé mérite d’être perturbée » (Quirk, 2017), la gouvernance en est un exemple consommé. En solidarité avec d’autres projets et des idées enracinées dans le monde entier, nous rejetons la centralisation forcée et embrassons le volontarisme. Plutôt que de confier à une minorité de personnes le pouvoir, nous croyons que toutes les personnes ont le droit de se voir confier la liberté.

La philosophie de base de notre modèle de gouvernance est que la décentralisation du pouvoir maximise l’inclusion et la créativité. Les implémentations pratiques doivent reconnaître que la mise en commun des ressources et des ressources fournit des synergies qui devraient être équilibrées de manière optimale par rapport à la décentralisation totale; Les points optimaux variant en fonction du temps ou de l’état, étant idéalement déterminés par la participation volontaire et la sécession.

Il est important que nous mettions en œuvre un système où les DAO concurrentes peuvent émerger pour partager des ressources, voire compléter entièrement des versions moins efficaces ou impopulaires. Il ne devrait pas y avoir de structure de taille unique dans l'environnement, la fonction, la culture ou le temps ; Plutôt, les structures doivent être adaptées à des problèmes spécifiques et flexibles lorsqu'elles fonctionnent et se fanent en cas de défaillance par rapport aux alternatives. Un tel ensemble de systèmes évoluerait de manière dynamique de manière à ce qu'il soit insensible à des réactions concurrentielles.

Notre état de gouvernance objectif permettra d'équilibrer la décentralisation, l'efficacité de la mise en œuvre, la séparation des pouvoirs, l'autonomisation des parties prenantes et l'aptitude à l'évolution. Cet état initial sera le résultat d'au moins une étude de R & D de 12 à 18 mois dans la recherche de la théorie des jeux, de science politique et d'économie dans les mécanismes de vote optimal, couplé à des commentaires provenant de plusieurs implémentations test. Le projet sera l'un de nos premiers efforts financés avec des produits livrables, y compris un rapport de recherche complet et un code opérationnel intégré au réseau Zen. Dans les 6 mois suivant la mise en œuvre de la gouvernance, nous nous attendons à ce que les équipes de direction soient opérationnelles à partir de nos premières élections pleines et ouvertes.

6.1 Décentralisation optimale

"Un spectre hante le monde moderne, le spectre de la crypto - anarchie. » -Crypto Anarchist- Manifesto

En ce qui concerne la décentralisation, nous voulons dire que chacun a l'égalité des chances de participer, que nous sommes pleinement inclusifs et que l'autorité décisionnelle est utilisable au maximum, de sorte que le système résiste au contrôle. La décentralisation maximale théorique signifie que tout individu conserve une autorité égale pour influencer la prise de décisions. Il est cependant difficile d'implémenter en pratique la mise en commun de ressources pour collaborer sur un système commun. Même si elles sont mises en œuvre de manière

pure et simple, les décisions individuelles s'accumulent naturellement pour l'efficacité de la collaboration et les ressources s'accumulent auprès de certaines parties prenantes à des rythmes inégaux.

Nous ne pouvons pas arrêter ces forces naturelles, et il n'y a aucune raison de les considérer catégoriquement comme nuisibles dans chaque cas. Ce que nous pouvons faire, c'est de concevoir le système de telle sorte que toute participation soit volontaire, que le pouvoir décisionnel sur l'allocation des ressources soit équilibré dans un large éventail de types de parties prenantes et qu'il existe un mécanisme crédible pour évoluer avec des retours d'information. Une structure imprégnée de flexibilité est plus importante que d'abord concevoir le meilleur système en fonction de toutes les circonstances, d'autant plus que nous créons un mouvement tellement expansif qu'en prédire tous les développements est essentiellement impossible.

L'efficacité de la mise en œuvre est également une grande préoccupation pour les organisations décentralisées. La décentralisation pure pourrait être la paralysie de la prise de décision, l'apathie des électeurs ou l'hystérie de masse à l'extrême. C'est pourquoi nous nous éloignons d'un système de démocratie pure pour toute prise de décision et nous prenons le temps de rechercher des modèles concurrents et de les tester dans des conditions de stress variables. Notre système proposé de concurrence gratuite et ouverte pour les DAO est conçu pour encourager les groupes hautement performants d'experts et de professionnels pour chaque zone fonctionnelle à proposer leur leadership dans des domaines spécialisés afin que l'efficacité de notre système pour la conversion de ressources en produits finis ou services de grande valeur évolue continuellement pour répondre aux besoins et aux demandes des utilisateurs.

6.2 Mécanismes de séparation des pouvoirs

Une leçon clé tirée de l'histoire de l'humanité est que les pouvoirs sont les mieux séparés et les pôles de puissance concurrents devraient fournir un état d'équilibre des contrôles et des soldes. L'équilibrage doit être résistant à une croissance non contrôlée dans n'importe quel groupe de puissance unique, de sorte que tout le système succombe à une prise de contrôle. Pour se prévenir initialement de cette situation, Zen démarre avec une équipe de base (core team) qui contrôle 3,5% du financement de récompense de bloc, et un DAO initial composé de leaders de l'industrie contrôlant 5% des ressources. En outre, notre état objectif à mettre en œuvre après la phase de recherche et de développement de 12 à 18 mois comprendra un type hybride de vote multipartite, de sorte qu'une grande partie de la communauté conserve le pouvoir de prendre en compte les décisions et les affectations de ressources. Chaque aspect de notre structure de gouvernance sera finalement soumis à des commentaires et à des changements concurrentiels. Nous adoptons une approche évolutive qui commence par un modèle simple qui va croître avec la communauté.

DAO: Infrastructure, Propositions et Vote

Le système Zen aura au moins un DAO financé par une partie des récompenses minières et est régi par un système de vote qui rassemble les acteurs. Ce système de gouvernance permet de s'assurer que la mise en œuvre des changements, des améliorations et des intégrations minimise la contention et réduit les chances qu'un désaccord entraîne une bifurcation dans le projet. Au fur et à mesure que nous développons notre plan de gouvernance plus large issu de la R & D et des tests rigoureux, l'objectif est d'ouvrir le paysage de la gouvernance à la pleine concurrence; Cela signifie que nous pouvons voir plusieurs DAO concurrents émerger avec différentes équipes travaillant sur différents problèmes. Chaque DAO émergerait de sa propre structure, de ses processus et de ses objectifs proposés, ce qui garantira que ces attributs évoluent à travers la concurrence et que les mauvaises décisions organisationnelles initiales ne se perpétuent pas.

Nos DAO seront responsables de la construction, du maintien et de l'amélioration de l'infrastructure qui maintient le système. Il est également responsable de la mise en œuvre des modifications apportées aux applications logicielles Zen et est assez flexible pour répondre à d'autres priorités communautaires telles que la sensibilisation communautaire, le marketing, la formation, etc.

Au fur et à mesure que le système Zen grandit, les structures de support pour les utilisateurs, les mineurs, les opérateurs de Noeuds Sécurisés et les partenaires de l'écosystème devront également croître et varier. Les structures DAO auront des fonds, alloués par des projets et des propositions, afin d'aider à la croissance et au soutien.

La communauté est encouragée à participer à la contribution au Zen de toutes manières. Les DAO sont chargées de coordonner les contributions de la communauté et disposent de fonds pour aider à définir les dépenses engagées par la communauté. L'un des buts des propositions est de rembourser les membres de la communauté pour leurs dépenses dans le soutien du système.

Au lancement, Zen aura un programme DAO avec des professionnels respectés qui couvrent les industries concernées. Lorsque le plan de gouvernance sera prêt à être mis en œuvre, ce DAO sera un regroupement proposé soumis à une concurrence sur le marché pour les personnes qui pourraient souhaiter résister à leurs propres structures de gouvernance; La communauté élargie prendra cette décision.

7.1 Infrastructure Zen Opérée par DAO

Le système DAO maintiendra les serveurs et les services d'applications, y compris:

Serveur (s) de validation de nœud sécurisé.

Serveur (s) du forum.

Modération de Slack.

Sites Internet.

Blogs.

Système de proposition.

Système de vote.

Référentiels binaires.

Les DAO sont responsables du support suivant:

Aiderz le public s gens à utiliser ZenCash ou d'autres fonctionnalités du système.

Aiderz les opérateurs Node sécurisé.

Résoudre les problèmes de récompense des nœuds.

Résoudre les problèmes du système de vote.
Fournir un processus d'escalade pour le support.
Fournir une décision rapide et finale.

DAO distribue ZenCash aux propriétaires de proposition après un vote réussi et l'expiration de la période de veto.

Il y aura initialement 3-5 représentants DAO, mais cela finira par être illimité. Les clients peuvent être anonymes, mais ce n'est pas une exigence. En fait, déclarer ouvertement l'identité a l'avantage que les réalisations professionnelles antérieures et la force du caractère sont naturellement importées dans le système Zen.

Il y aura des conflits et, par conséquent, des mécanismes de résolution doivent être développés pour juger de manière équitable et équitable. Une idée qui sera explorée dans le projet de R & D en matière de gouvernance sera d'établir un système judiciaire et un jury.

7.2 Présentation et vote des propositions

Chaque DAO aura sa propre structure, ses processus et ses priorités, mais un mécanisme cohérent sera un système de soumission de propositions gratuites et ouvertes pour le travail et un processus d'évaluation et d'attribution. Il n'y a aucune raison de préciser comment cela se produit, seulement que cela se produise. Il s'agit d'une communauté ouverte à toute l'humanité, donc il ne devrait y avoir aucun obstacle à la participation. Une méthode proposée pour notre DAO initial est la suivante:

1. Voter tous les deux mois. Date limite de soumission des propositions deux semaines avant le vote. Dates de vote: 31 janvier, 31 mars, 31 mai, 31 juillet, 31 septembre, 31 novembre.

2. La soumission de la proposition ouvre le jour après le vote.

3. Veto - l'équipe de base peut opposer son veto à une proposition dans les 7 jours suivant un vote avec un veto d'équipe à l'unanimité (cela ne devrait presque jamais être fait).

4. Les propositions peuvent être financées dans l'équivalent ZenCash en devise locale à la date du vote (pour prévenir tout problème tel qu'avec Dash lié à la montée rapide de prix conduisant au rejet du projet).

5. Vote effectué avec des jetons. 1440 jetons de vote distribués 1 mois avant le vote.

6. La plupart des décisions prises à la majorité des voix> 720 détenteurs de jetons votent oui.

7. Quelques décisions par vote de super-majorité> 1080 détenteurs de jetons votent oui.

7.3 Processus de vote

Plan de distribution de jetons - {fait pour chaque période de vote, 1440 jetons au total:

1. 360 jetons à la vente {permet aux utilisateurs et aux détenteurs de ZenCash afin d'acheter des votes.
   (a) 1-30: 1 ZenCash
   (b) 31-60: 2 ZenCash
   (c) 61-90: 3 ZenCash
   (d) etc. jusqu'à 12 ZenCash par jeton pour le dernier groupe de 30

2. 240 - développeurs de projets ZenCash.

Attribué par des engagements, des demandes de tirage ou d'autres mesures raisonnables de contribution.

L'objectif est d'habiliter les développeurs de logiciels et systèmes.

3. 60 – Marchés d'échange qui gèrent du ZenCash.

(a) Le Top 6 par volume reçoit 10 jetons chacun.

4. 60 - Propriétaires de Pool miniers.

5. 360 – Nœuds Sécurisés.

(a) 1 jeton décerné tous les 40 blocs jusqu'à ce que tous les 360 soient décernés.

6. 120 - Officiers DAO, réparti équitablement entre les officiers DAO.

7. 240 - Équipe de base, répartie équitablement parmi les membres de l'équipe de base.

Communauté Zen: Forte et Vibrante

Zen évolue symbiotiquement avec le projet Zclassic, avec notre communauté combinée autour de 1000 membres du forum, développeurs, mineurs, commerçants, investisseurs à long terme, organisations partenaires, places de marché, blogueurs, etc. En tant que projet entièrement ouvert et inclusif, tous les types de contributions et de soutien ont convergé du monde entier dans Zen, et ce collectif impromptu mais cohérent est l'une de nos fonctionnalités en tant que système. Notre communauté a déjà une histoire durable non seulement des relations positives et des interactions amicales, mais aussi du soutien spontané et de l'engagement qui émergent pour prévenir ou résoudre des problèmes divers.

8.1 L'éthique de l'Open Source

Les projets open source peuvent prendre une évolution de l'éthique, mais leurs fondateurs espèrent garder la communauté centrée sur les principes de zen, d'où notre nom. Nous développons un système que nous espérons être utilisé pour une collaboration pacifique, une innovation sans autorisation et une inclusion maximale. Nous espérons que notre héritage offrira un bénéfice massivement positif pour la société, et nous rejetons personnellement le travail avec toute personne vouée à un préjudice, physique ou frauduleux.

8.2 Support Zen

Zen Support se réfère à une communauté de Développeurs Zen et à d'autres professionnels informatiques distribués qui s'engagent à faire progresser la technologie et à fournir une assistance de base aux utilisateurs. Ce réseau sera financé par le DAO et servira à rendre la technologie Zen plus intuitive et plus facile à utiliser dans l'écosystème. Le support Zen sera également constitué d'un réseau de contributeurs de diverses industries qui s'engagent à servir d'ambassadeurs, de conseillers et de soutien aux contributeurs Zen. Prière de se référer aux sections ultérieures de la Communauté Zen. Zen Support s'engage à ce que Zen soit structuré pour favoriser l'intégration, la collaboration et l'aide collective, et que les cadres supérieurs, les ambassadeurs Zen, les Entrepreneurs Zen Vérifiés ou tout représentant de la communauté Zen sera une source de collaboration pour les contributeurs.

8.3 Sensibilisation au Zen

Notre feuille de route comprend des programmes de sensibilisation passionnants et sans précédent qui contribueront à renforcer notre engagement collectif et faciliter l'engagement avec des personnes de tous horizons. En bref, le zen n'a pas de «marché cible», comment pouvons-nous en définir un, lorsque les cas pratiques et les applications de notre technologie sont vastes et diversifiés? Nous n'avons pas l'intention de confiner Zen aux visions personnelles de nos membres de l'équipe de base, alors, nous allons lancer des programmes dès leur création conçus pour maximiser l'engagement avec Zen et permettre aux membres de la communauté d'adapter notre mission et nos initiatives au fur et à mesure que Zen évolue. Notre DAO initial est en passe de réserver des ressources pour financer des programmes expérimentaux et pour récompenser des contributions actives à notre communauté. Certaines de ces idées de programmes proposés sont expliquées ci-dessous.

Encore une fois, Zen est inclusif et agnostique, et notre présence mondiale reflètera ces valeurs fondamentales. Nous allons inclure des groupes d'intérêt tels que les entrepreneurs, les activistes, les développeurs, les universités, les entreprises et les personnes mal informées mais curieuses, toutes dotées de différents antécédents d'engagement avec l'univers des crypto-monnaies.

Grâce à notre programme d'ambassadeur Zen, les utilisateurs expérimentés, les leaders de la pensée et les membres de la communauté passionnés auront l'opportunité de représenter Zen, propageant notre vision aux personnes dans les coins du monde sans accès aux ressources, au capital et à la technologie nécessaires pour découvrir et rejoindre notre communauté individuellement. Les dirigeants de ce programme peuvent servir à plusieurs fins, en conseillant les startups Zen, au mentorat des Zen Chapters pour représenter Zen dans la presse.

En participant à notre programme Zen Youth, les mineurs mondiaux auront un programme intensif de codage et de développement commercial, et des occasions uniques d'engagement avec le collectif Zen. Cette initiative aura de multiples facettes, avec des résultats allant des compétitions mondiales de jeunes pour les startups financées par DAO construites sur la plateforme Zen aux loteries allouant des ressources pour couvrir les dépenses d'éducation de la jeunesse Zen. Ces jeunes pionniers seront également mobilisés pour recruter leurs pairs et engager leurs communautés.

Les entrepreneurs engagés dans la gestion de projets financés par DAO seront des Entrepreneurs Zen Vérifiés et auront accès à des avantages pertinents pour l'accélérateur de start-up, tels que l'accès à des mentors commerciaux établis, des canaux de marketing et d'acquisition d'utilisateurs, d'encadrement de développeurs open-source, de chaînes directes aux investisseurs et Venture capitalistes et des événements, des partenariats et des séminaires conçus pour résoudre de façon collaborative les problèmes

et favoriser l'innovation.

Les contributeurs individuels auront accès au contenu prêt à l'emploi conçu pour aider à engendrer des mouvements de base sous la forme de Zen Chapters faisant la promotion de la technologie, l'éthique et / ou la gouvernance zen, et en développant des projets à travers le monde. Ces chapitres Zen seront localisables et personnalisables, avec une grande importance selon les besoins de la région et de la communauté. Zen constituera une plate-forme fondamentale en ligne de ressources matérielles, allant de:

Contenu marketing et éducatif détaillant les origines, les spécificités, les différenciations et les objectifs de Zen.

Modèles et idées pour les groupes qui souhaitent créer des événements promotionnels ou éducatifs parrainés par Zen, des conférences et des compétitions.

Des modules, des discussions et des webinaires sur les principes de Zen et les sujets pertinents pour les participants à participer et à contribuer, tels que le codage, l'esprit d'entreprise, l'éthique de la décentralisation, les fondements de Blockchain, etc.

Base de données sur les plans d'affaires, les documents juridiques, les modèles de revenus, les tactiques d'acquisition d'utilisateurs, etc., afin de favoriser les objectifs des chapitres d'entreprendre une initiative de développement commercial ou d'amélioration de la communauté.

L'accès aux contributeurs et aux développeurs Zen pour obtenir de l'aide, des conseils, des conseils et de l'assistance via les canaux Zen.

Par exemple, un Zen Chapter aux Philippines, où seulement environ 30% de la population a accès aux services financiers, pourrait s'engager virtuellement avec le collectif international pour développer un projet FinTech répondant aux besoins particuliers des Philippins et des spécificités de la culture du pays et de son infrastructure. Un tel engagement évolutif pourrait réduire considérablement la friction qui a empêché historiquement les communautés de stimuler de façon autonome leurs propres économies à petite échelle et d'augmenter leur capacité à être compétitives.

L'interaction et la communication virtuelles sont un développement inestimable du 21ème siècle et seront le canal principal pour relier les personnes à des milliers de kilomètres afin de favoriser l'innovation et le développement Zen. Cela étant dit, nous reconnaissons à Zen qu'il y a quelque chose de sensationnel au sujet de l'interaction en face à face avec ceux qui se sont également consacrés et mobilisés autour d'un ensemble de principes et de vision commune. La Zen University (Université Zen) aura lieu chaque année pour récompenser et engager les contributeurs les plus actifs et à valeur ajoutée de Zen, les jeunes talents ainsi que les entrepreneurs exceptionnels. Il y aura également une loterie distribuant des billets au hasard à des nœuds Zen particulièrement compatibles et sécurisés. Le thème, le contenu et l'intention de cet événement varieront en fonction des préférences de la communauté Zen.

Nos ressources sont destinées à notre communauté Zen, qui englobe bien plus de catégories de participants et d'initiatives, et a beaucoup plus de valeur que les acteurs traditionnels d'un projet de crypto-monnaie. Nous espérons être autant d'un mouvement social que nous sommes un projet technologique, le but final pur d'aider à rendre la vie plus libre et plus gratifiante pour autant de personnes que possible.

ENVIRONNEMENT CONCURRENTIEL

“Nous croyons depuis longtemps que, au fil du temps, les entreprises ont tendance à se sentir à l’aise en faisant la même chose, en faisant des changements incrémentiels. Mais dans l’industrie de la technologie, où les idées révolutionnaires conduisent les prochains grands secteurs de croissance, vous devez être un peu mal à l’aise pour rester pertinent. »-Larry Page, Alphabet

La concurrence est gravée au cœur du projet Zen ; Par sa nature, c’est une nécessité de décentralisation optimale et un principe que nous croyons permettant une évolution sociale. Ce processus comprend également la concurrence dans l’environnement des crypto-monnaies pour ZenCash et pour notre système dans l’écosystème des plates-formes de blockchain.

ZenCash est directement en concurrence avec ZCash, Zclassic, Dash, Monero, ZCoin, Bytecoin, ShadowCash, Boolberry et d’autres crypto-monnaies axées sur la protection de la vie privée. La concurrence se présente sur plusieurs dimensions, mais du point de vue de la technologie, nous entrons en compétition directe avec les crypto-monnaies utilisant zk-SNARK. ZCash était le pionnier dans ce domaine, et notre technologie bénéficie directement de ses contributions novatrices. La protection de la vie privée en tant que fonctionnalité signifie également que ZenCash est en concurrence avec d’autres implémentations, telles que le protocole Zerocoin, CryptoMessage, RingCT et des mixeurs plus simples. Toutes ces monnaies répondent à une niche particulière axée sur la confidentialité dans la demande globale de crypto-monnaies.

Notre proposition de valeur est que nous incorporons des éléments que nous considérons de première qualité, ce qui commence par hériter la mise en œuvre

de ZCash du blindage à zéro connaissance via zk-SNARKs, mais nous prenons cet étape cruciale et renforçons notre réseau en cryptage de bout à bout tout en activant les services de messagerie à l'intérieur de l'infrastructure la plus sécurisée de notre marché. Il est important de noter que nous n'avons pas l'intention d'être bousculés, parce que nous sommes structurés de façon non seulement pour mettre à jour et rajeunir nos systèmes au fur et à mesure que la technologie sous-jacente avance, mais pour nous-mêmes être les innovateurs de l'espace.

Zen construit une architecture de système avec ZenCash comme un jeton de valeur ou un carburant de transaction. En tant que tel, nous sommes également en concurrence avec des projets plus larges de type plate-forme, tels que Ethereum, Ethereum Classic, NEM, Lisk et Synereo sur lesquels des applications décentralisées (dApps) peuvent être construites. Dans ce domaine, le langage de script simple de Zen hérité de Bitcoin et ZCash conserve une grande sécurité et une résilience à partir d'un large éventail de vecteurs d'attaque, mais limite également les degrés de liberté utiles aux exécutions complexes de code possibles pour les plates-formes avec des scripts Turing-complets améliorés, Ethereum et Ethereum Classic. Notre avantage dans cette arène concurrentielle est que les dApps peuvent être construites sur le réseau de crypto-monnaie le plus sécurisé au monde, et que nous sommes assez expérimentés pour opérer à travers diverses chaînes de blocs par des partenariats stratégiques.

Notre innovation unique dans la communauté de crypto-monnaies est notre modèle de gouvernance pleinement compétitif et évolutif qui donne du pouvoir à un large éventail d'intervenants dans un environnement de décentralisation optimale. Bitcoin a créé la brèche initiale dans le consensus distribué, mais d'autres projets ont depuis pris de l'ampleur avec divers mécanismes de vote. Ces projets vont de Dash avec son modèle simple de soumission de proposition et de vote communautaire jusqu'à Decred avec sa gouvernance communautaire intégrée; Chacun a contribué positivement à l'évolution du consensus décentralisé, mais Zen amène cela au niveau supérieur en supprimant des contraintes supplémentaires telles que notre système évolutif au fil du temps grâce à une concurrence perpétuelle entre les fournisseurs de services de gouvernance au sein de

l'écosystème. Nous mettons en œuvre un système autonome qui changera avec les réactions et les innovations résultant d'essais et d'erreurs sur la manière dont les systèmes décentralisés s'organisent pour résoudre des problèmes spécifiques. En ce sens, nous croyons que Zen est révolutionnaire dans la technologie sociale, pionnier d'un système qui n'a jamais été tenté à grande échelle.

D'un point de vue plus large, Zen rivalise avec les monnaies en place et les systèmes bancaires, ainsi que les start-ups émergentes FinTech avec un avantage particulier dans la prestation de services aux personnes privées de droits. Nous choisissons de contribuer à cet espace novateur, axé sur le bien-être social, en offrant une protection et une sécurité accrues. En tant que système sécurisé de messagerie et d'archivage des données distribuées, nous sommes en concurrence avec d'autres services tels que Signal, Telegram et Tor Project. Il existe également un certain nombre de projets potentiels qui peuvent être construits sur la plate-forme Zen, augmentant notre compétitivité de façon exponentielle.

Nous considérons la concurrence comme un processus propice à la croissance et nous sommes ouverts à la concurrence maximale. Nous préférerions vivre dans un monde avec de nombreux concurrents qui nous forcent à accélérer nos propres innovations qu'un monde statique dépourvu de progrès. Nous espérons que Zen ajoute positivement au bien-être humain en intégrant les grandes technologies et les communautés, en transformant la gouvernance en un service compétitif et en permettant à quiconque dans le monde de participer à notre système d'innovation sans permission, collaborative et décentralisée. Nous considérons également les opérateurs historiques et les futures startups dans cet espace comme des partenaires potentiels et des alliés au lieu de concurrents absolus.

L'AVENIR DE ZEN

Prévoir est un exercice difficile, mais nous voyons un avenir brillant pour Zen et l'écosystème paisible et productif que nous construisons. Nous croyons que l'organisation décentralisée, entièrement inclusive, volontaire et flexible que nous créons sera considérée comme évidemment supérieure à l'avenir par rapport à celles statiques, centralisées et à solution unique comme toutes les versions qui se sont perpétuées au XXe siècle. L'avènement de la cryptographie, de la philosophie volontaire et de la technologie blockchain rendent possible une telle chose, et nous croyons que beaucoup de gens partageront notre vision pour un monde meilleur; Surtout lorsqu'ils découvriront comment nous pouvons accélérer l'innovation et améliorer le bien-être humain en permettant à chacun d'exprimer ses valeurs.

Cette vision se concrétisera dans une ou deux années d'après notre planification initiale en exécutant notre feuille de route. Il y aura certainement des défis en cours de route, mais la flexibilité et la coopération pacifique remédieront systématiquement aux problèmes qui paraissaient insurmontables.

Nous avons la chance de vivre dans une époque d'incroyable innovation tant dans la technologie que dans les idées. Nous construisons au-dessus des épaules des géants proverbiels, certains d'entre eux énumérés ci-dessous, mais beaucoup d'autres ne sont pas nommés uniquement parce qu'ils sont si nombreux et les contributions aussi fondamentales.

RÉFÉRENCES

[1] Juan Benet. (2014) IPFS - Content Addressed,Versioned, P2P File System.

[2] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. (2014) Zerocash: Decentralized Anonymous Payments from Bitcoin.

[3] Evan Du eld, Kyle Hagan. (2014) Darkcoin: Peer-to-Peer Crypto Currency with Anonymous Blockchain Transactions and an Improved Proof-of-Work System.

[4] David Fi eld, Chang Lan, Rod Hynes, Percy Wegmann, and Vern Paxson. (2015) Blocking-resistant communication through domainfronting.

[5] Daira Hopwood, Sean Bowe, Taylor Hornby, Nathan Wilcox. (2017) ZCash Protocol Speci cation Version 2017.0-beta-2.5.

[6] May, T. (1992). The cryptoanarchist manifesto. High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace.

[7] Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system.

[8] Quirk, Joe, and Patri Friedman. (2017) Seasteading: How Floating Nations Will Re-store the Environment, Enrich the Poor, Cure the Sick, and Liberate Humanity from Politicians. Free Press.

[9] Taleb, NN (2012). Antifragile: Things that gain from disorder (Vol. 3). Random House.