ESPERS

Un projet d'équipe signé CryptoCoderz

White Paper

Écrit par l'équipe CryptoCoderz

20 Février 2018 (1e Version Publiée)

ESPERS

TABLE DES MATIÈRES

ESPERS

PRÉFACE

La plupart des mots techniques ont été traduits lors de leur première occurrence en Français et entre parenthèses. Pour des questions de lisibilité technique, ils seront cependant gardés en anglais au cours de la lecture.

ABSTRAIT

Avec l'apparition de la technologie blockchain (en Français « châine de blocs ») au début des années 2000, le monde s'est montré enthousiaste en observant son évolution. Bitcoin a notamment attiré l'attention de tout le monde comme étant une monnaie qui fonctionne sur la blockchain et d'autres communautés ont surgi dans la même vague. La nécessité d'une solution de blockchain avancée, sécurisée et décentralisée, pour les tâches quotidiennes utilisables par le fournisseur et l'utilisateur, n'a cependant pas encore été pleinement réalisée. Même celles qui ont actuellement des caractéristiques spécialisées ont souvent une mentalité de « loup solitaire », qui fait que les projets se battent entre eux et se fragmentent pour que les communautés se diluent et que le message de l'objectif soit perdu.

Espers est une blockchain hybride Proof-of-Work / Proof-Of-Stake (PoW / PoS, en Français Preuve de Travail / Preuve de participation), qui a été créée pour être une solution à la division et au manque d'utilisabilité actuellement attribués à la technologie blockchain, à la fois unifiante et évolutive. Les fonctionnalités implémentées telles que la messagerie sécurisée, l'interfaçage cross-chain, les sidechains modulaires, les sites Web sur la chaîne, le stockage de fichiers sur la chaîne, etc. sont ensuite intégrées via une interface universelle à laquelle tout projet lié à une monnaie peut participer. L'usage de la devise ESP (Espers), en tant que « carburant » ou catalyseur qui entraîne les services que la chaîne exploite, stimule l'intérêt de contribuer au traitement des blocs pour le réseau. Les mineurs / Stakers sont encouragés à participer, ce qui entraîne une génération de bloc cohérente et assure un réseau globalement rapide. Ce document est destiné à décrire en détail les différents systèmes qu'utilise le projet Espers et comment ils fonctionnent à l'unisson pour fournir à l'utilisateur final de toute communauté une expérience transparente et intuitive

ESPERS

BLOCKCHAINS

- **Les lacunes actuelles**

  Ce qui est attribué à la technologie blockchain à l'heure actuelle est simplement un système de fonctionnement ayant pour but unique de générer du revenu. Le créateur de Bitcoin avait espéré offrir une technologie vraiment unique ne se concentrant pas sur le revenu. Toutefois, la vision s'est mouillée pendant que des centaines de blockchains inondaient le monde. Malgré ce que les actualités et les médias aimeraient vous faire croire, les blockchains ne doivent pas seulement fournir une fonctionnalité. Malheureusement, les médias ne se concentrent que sur les pertes et les gains, de sorte que toute personne ordinaire soit considérablement découragée par toute blockchain qui ne s'occupe que de fournir des jetons ou « une devise ». Bien qu'étant individuellement des exploits technologiques, il n'y a pas de capacité de lier les blockchains basés sur Bitcoin ; même des alternatives telles que Ethereum ne fournissent pas une solution sans effort.

- **Implémentation et bénéfices actuels**

  Les blockchains peuvent être décrites comme « un grand livre (comptable) numérique dans lequel les transactions effectuées via Bitcoin, ou dans une autre crypto-monnaie, sont enregistrées chronologiquement et publiquement » (Google). Bien que cela soit plus ou moins vrai, en déclarant que le livre numérique d'une blockchain est utilisé pour enregistrer l'historique des transactions, on peut mentalement restreindre ce que l'on croit pouvoir faire avec. En principe, les blockchains sont en effet utilisées pour distribuer à grande échelle un grand livre numérique décentralisé, qui stocke les données de chaque transaction pour l'ensemble du système, permettant à toute personne d'accéder à ses comptes et à ses informations en toute sécurité. En l'absence de point de défaillance central (étant décentralisées), les blockchains, telles que Bitcoin, sont très résistantes à toute forme de démontage ou d'attaque contre le système. Les grands livres de compte distribués fournissent également une transparence permettant à toute personne de voir des informations générales. Ceci est fait tout en conservant plus de valeurs et d'informations privées sous le verrou d'une clé privée, dont chaque utilisateur dispose d'une version unique. Les informations sur les transactions sont stockées dans des blocs d'informations appelés « blocs ». Les blocs sont générés par des « mineurs », des personnes qui minent ou jalonnent, ce qui est une forme de contribution pour chiffrer un bloc d'informations et le transmettre au réseau. Comme une chaîne de blocs génère des blocs, elle peut également manipuler leur taille, facilitant la possibilité de stocker différents types de données dans des volumes de données plus importants qui sont ensuite fournis aux utilisateurs finaux. Cela empêche le besoin de développer la blockchain à moins que cela ne soit requis par les paramètres de cette dernière. Lorsqu'elle est assemblée, une blockchain est un système très performant en termes de devise, mais sa polyvalence ne s'arrête pas là.

- **Possibilités futures**

  Une blockchain peut être utilisée pour une pléthore de solutions logicielles en ce qui concerne la sécurité et la fiabilité supplémentaires offertes par un consensus distribué. La limite est sa propre imagination et créativité. Les communautés parlent de systèmes d'exploitation, de systèmes de messagerie, de systèmes de stockage de données fonctionnant tous sur la blockchain, améliorant considérablement nos protocoles actuels. Une fois que les communautés et les projets commenceront à s'éloigner de l'objectif monétaire et à se tourner davantage vers le développement des possibilités technologiques elles-mêmes, ils créeront une réelle rationalisation de la sécurité et de la fiabilité de nos tâches quotidiennes.

ESPERS

CONSENSUS ET MÉCANISME DE RÉCOMPENSE

Espers utilise une blockchain hybride Proof-of-Work / Proof-Of-Stake (PoW / PoS) qui affecte directement la façon dont le système gère la production de blocs et stimule l'intérêt à le faire.

Proof-of-Work ou (PoW) comme on l'appelle souvent, est la méthode de consensus la plus notable, car c'est aussi la plus commune parmi les projets blockchain depuis son utilisation par Bitcoin. PoW fonctionne en invitant les participants à la puissance de calcul sous une forme appelée « hash » ou « hachage », en référence au hachage d'un bloc de la blockchain. Les participants sont récompensés pour les blocs correctement soumis qui sont acceptés par la blockchain / réseau et ensuite confirmés, car le bloc vieillit en assurant la génération ultérieure (extraction) des futurs blocs en gardant l'intérêt des participants. En outre, plusieurs participants regroupent généralement leurs ressources en utilisant un « pool de minage » : au lieu d'opposer la compétition entre mineurs simples, ce type de service permet même à ceux qui ont une faible puissance de calcul de recevoir une compensation pour ce qu'ils fournissent, plutôt que d'essayer de battre une entité avec beaucoup plus de puissance de hachage. Cette méthode de distribution est loin d'être parfaite, car il est possible d'attaquer la blockchain en contrôlant quelles informations sont dans les blocs étant minés et soumis. Ceux-ci sont connus sous le nom de « blocs défectueux » qui sont des blocs avec des informations invalides qui ne seraient normalement pas acceptées, et même en séparant la blockchain en deux versions d'elle-même (forking) qui rivalisent pour la validité et l'acceptation du réseau, des énormes quantités de courant auxquelles la majorité n'a pas accès seraient requises.

Proof-Of-Stake ou (PoS) est une nouvelle méthode de génération de blocs, mais sans doute l'une des méthodes de distribution les plus sûres, qui n'est pas aussi facilement accessibles aux nouveaux arrivants qui montent à bord d'une communauté / d'un projet. Ceci est dû au fait que le PoS utilise le montant de monnaie que possède et détient un participant pour générer un bloc. Par conséquent, posséder plus de pièces de monnaie et les jalonner donnent au participant une plus grande possibilité de générer le bloc suivant. Le jalonnement consiste à permettre à son portefeuille / client de rester en ligne, afin de soutenir le réseau en rendant temporairement indisponible aléatoirement un montant pré établi pendant que le portefeuille / client forge un bloc et compense ensuite le participant avec un intérêt gagné sur le montant utilisé. Plus longtemps le montant est rendu disponible, plus il accumule du poids et plus les chances de forger le bloc suivant sont élevées. Une fois le bloc trouvé, le poids de la pièce est réinitialisé pour permettre aux autres participants d'exploiter un bloc. Cette méthode est considérée comme plus sûre, car si elle est correctement distribuée, les participants invalideront la plupart des attaques qui abusent du pouvoir de hachage afin de prendre le contrôle d'une blockchain. Toutefois, il faut d'abord obtenir de la monnaie, qui, selon sa valeur, peut être coûteuse et cela est globalement dissuasif pour le projet si c'est la seule méthode disponible.

PoW / PoS Hybride, connu généralement comme une méthode de distribution « hybride », mélange à la fois PoW et PoS sur la même blockchain. Les systèmes hybrides sont encore relativement nouveaux, car peu de blockchains utilisent un algorithme de difficulté assez robuste qui ajuste l'intervalle de temps entre les blocs générés pour PoW ou PoS et dans ceci à l'unisson pour les deux. Un algorithme de re-ciblage de difficulté personnalisé connu sous le nom de « VRX » a été créé pour Espers, afin de permettre un mélange correct des types de blocs générés dans une chaîne de blocs hybride complète. Ce faisant, la sécurité d'Espers est considérablement augmentée, car PoW et

PoS se complètent mutuellement, ce qui permet à la blockchain d'avoir une longueur d'avance significative sur une opération particulière concernant une méthode particulière.

La structure de Consensus et de Récompense, au moment de la rédaction de ce document pour le projet Espers, est définie ci-dessous :

- **Temps par bloc (Après l'implémentation de VRX)**
  Espacement forcé minimum : 3.5 minutes par bloc
  Espacement ciblé : 5 minutes par bloc
  Maximum (limite logicielle) : 7 minutes par bloc

- **Proof-of-Work / PoW**

Bloc 0-10 :	0 ESP par bloc	(*Blocs de départ**)
Bloc 11-365 :	50.000.000 ESP par bloc	(*Blocs réservés**)
Bloc 366+ :	5.000 ESP par bloc + frais de réseau	(*Blocs standard*)

- **Proof-of-Stake / PoS**

Bloc 2125-20,000 :	250 % intérêt annuel	(*erreur de calcul sur 2 jours**)
Bloc 20.001- 2.000.800 :	25 % intérêt annuel	(*phase standard*)
Bloc 2.000.801- 3.000.300 :	5 % intérêt annuel	(*Phase de réduction 1**)
Bloc 3.000.300+ :	1 % intérêt annuel	(*Phase de réduction 2**)

- **Approvisionnement maximum d'Espers Coin**
  Total de : 50.000.000.000 ESP (*50 Milliards d'ESP**)

Blocs de départ* : Se réfère à la définition d'une récompense par bloc de « 0 », pour que les premiers blocs de la chaîne puissent être analysés pendant qu'ils sont extraits sans générer de récompense pour le mineur.

Reserved blocks* : Initialement, le projet Espers a distribué 20 % de la blockchain totale avec un processus connu sous le nom de « Air-Drop » à tous ceux qui voulaient participer gratuitement, tout en réservant un 5 % réparti également entre les six membres de l'équipe pour financer le développement en cours. Cela a été fait en avril 2016 lors du lancement et exécuté à nouveau lors du changement de blockchain qui a été effectué peu de temps après.

Erreur de calcul sur 2 jours* : Lors du lancement du PoS pour Espers, il y avait initialement une entrée de valeur erronée pour l'équation de pourcentage annuel qui calcule les récompenses de jalonnement d'un utilisateur. Cela s'est traduit par une surcompensation sur deux jours (48 heures) des primes de participation générées par le PoS, mais cela n'a eu aucun impact majeur sur l'offre / la fonction globale et a été rapidement résolu. Vingt mille blocs ont été traités, car c'était avant la mise en œuvre de VRX et la chaîne avait été en train de générer des blocs à cette période.

Phase de réduction 1* : Une fois la phase de récompense standard du PoS terminée, environ 48 milliards d'ESP ont été générés.

Scale down phase-2* : Plus tard, une réduction finale allant jusqu'à 1 % est réalisée à l'approche de l'approvisionnement maximum de monnaie.

50-Billion ESP* : L'approvisionnement maximum de monnaie est estimé à ~ 30 ans après le lancement (2016-2046 après J.-C.)

TERMINAL VELOCITY RATEX (VRX)

VRX ou Terminal Velocity RateX est un système de ré-ciblage de difficulté blockchain qui, en utilisant un scan de profondeur de plusieurs blocs, adapte rapidement les niveaux de difficulté de minage ou de jalonnement de blockchain / altcoin pour assurer une fenêtre étroite autour du temps du bloc désiré. Permettant bien sûr certaines incohérences dans l'espacement des blocs en raison d'augmentations ou de diminutions significatives du hachage / jalonnement suivant si la blockchain est basée sur Proof-of-Work, Proof-of-Stake ou Hybrid, le système VRX garantit que les blocs soient générés à un rythme uniforme et régulier. En outre, pour les blockchains hybrides, les blocs sont correctement mélangés dans un rapport de 50/50, ce qui permet aux deux types de consensus d'avoir une chance égale.

Autrement dit, VRX indexe un nombre de blocs prédéfini (les implémentations de référence typiques sont définies sur les six blocs précédents), puis les compare les uns par rapport aux autres, déterminant ainsi l'espacement entre ces blocs. Le système prend alors l'espacement de bloc déterminé et le compare à l'espacement de bloc désiré dans ce que l'on appelle « Check Round ». Ce tour de contrôle est similaire aux autres systèmes de retarget disponibles mais s'ajuste sur une courbe différente qui s'adapte rapidement aux changements importants dans le hashrate de la blockchain, en veillant également à ne pas trop ajuster pour ne pas « bloquer » la blockchain. Il y a un tour de contrôle par paire de blocs indexés ; donc, en utilisant une profondeur d'index de six blocs, VRX donnera cinq tours de contrôle. Une fois que VRX a effectué ses vérifications, il détermine s'il doit changer la difficulté vers le haut ou vers le bas, selon que le temps de blocage désiré a été dépassé ou précipité, la gravité étant limitée à un maximum de deux. Enfin, une moyenne est calculée entre les différents changements de difficulté, de sorte que le changement de difficulté le plus logique se produise au mieux pour la blockchain et est ensuite enregistré par le système Espers. Veuillez vous reporter au diagramme fonctionnel de la page suivante qui décrit la fonction réelle.

Les versions plus récentes des systèmes VRX (tels que celui utilisé) présentent un problème de difficulté PoW / PoS unique dans lequel les systèmes hybrides biaisent la difficulté sur une courbe, en faveur du type de bloc le moins souvent trouvé. Cela garantit qu'aucun type de bloc ne peut l'emporter sur l'autre et que les mineurs et les stakers peuvent bénéficier de la blockchain de manière égale. VRX a été conçu pour interagir directement avec le système de contrainte « Velocity block » d'Espers, qui est discuté plus longuement dans la section suivante. Ceci, parce qu'aucune autre méthode de retarget de difficulté n'était compatible avec elle, puisque la difficulté de bloc joue un rôle important dans le système de Velocity lui-même.

(Diagramme de fonctionnement d'exemple)

[Cherche block précédent-1**]** → **[**Heure du block : p. ex. 07:00**]**

- Espacement du bloc de 7 minutes (mbs1)

[Cherche block précédent-2**]** → **[**Heure du block : p. ex. 07:07**]**

- Espacement du bloc de 9 minutes (mbs2)

[Cherche block précédent-3**]** → **[**Heure du block : p. ex. 07:16**]**

- Espacement du bloc de 8 minutes (mbs3)

[Cherche block précédent-4**]** → **[**Heure du block : p. ex. 07:24**]**

- Espacement du bloc de 5 minutes (mbs4)

[Cherche block précédent-5**]** → **[**Heure du block : p. ex. 07:29**]**

- Espacement du bloc de 5 minutes (mbs5)

[Cherche block précédent-6**]** → **[**Heure du block : p. ex. 07:34**]**

Espacement cible = Espacement du bloc de 5 minutes (mbsT)

[Check-round-1**]** → **[**mbs1 > mbsT**]** → **[**Décrémenter**]**

[Check-round-2**]** → **[**mbs2 > mbsT**]** → **[**Décrémenter**]**

[Check-round-3**]** → **[**mbs3 > mbsT**]** → **[**Décrémenter**]**

[Check-round-4**]** → **[**mbs4 = mbsT**]** → **[**Aucun ajustement**]**

[Check-round-5**]** → **[**mbs5 = mbsT**]** → **[**Aucun ajustement**]**

Comparez les actions, puis sélectionnez la plus haute action choisie

Décrémenter = 3
Pas de décrémentation = 2
Décrémenter > Pas de décrémentation

VRX ajuste le minage de blockchain / génération des difficultés pour atteindre l'espacement cible

SYSTÈME DE CONTRAINTE VELOCITY BLOCKCHAIN

- **Fonctionnalité globale des fonctionnalités**

Velocity est une fonctionnalité réécrite, à l'origine trouvée dans Frycoin (un ancien altcoin basé sur Bitcoin). En trébuchant sur cette fonctionnalité, il devint rapidement évident que bien que des parties significatives du code aient besoin d'être refaites, la fonctionnalité elle-même avait une bonne base globale en termes de sécurité et de stabilité de chaîne, ce qui la rendait très souhaitable. La fonctionnalité a été réécrite avec succès malgré quelques petits revers et bugs dans les versions antérieures qui n'affectent pas réellement la stabilité de la chaîne ou le fonctionnement de la monnaie d'une autre manière que celle prévue. Plus tard dans le développement, des systèmes supplémentaires ont été créés qui n'ont jamais fait partie de la fonctionnalité originale de la fonction pour une opération de blockchain globale correcte.

Le rôle clé de Velocity est de contraindre la chaîne avec les paramètres déjà définis dans le code, au lieu d'avoir l'espacement du bloc et d'autres propriétés se comportant comme une réaction au fonctionnement de la chaîne. D'autres implémentations de la technologie blockchain, une augmentation soudaine du hashrate, qui peut indiquer une éventuelle attaque, restent une vulnérabilité malgré la meilleure difficulté de retarget des systèmes mis en place pour contrôler l'espacement du bloc. Les frais de réseau, d'éventuels problèmes d'équilibrage invalide lors de l'envoi de transactions et d'autres parties de la blockchain sont contrôlés par un double contrôle. Cependant, ils sont toujours susceptibles d'être attaqués, que ce soit une attaque temporaire ou une double dépense confirmée en causant des pertes aux utilisateurs du réseau, ce qui est inacceptable.

La question de l'exploitation éventuelle des paramètres est résolue par le système Velocity étant une « triple vérification ». Même si un bloc pendant la génération a apparemment satisfait toutes les exigences et est ensuite généré, il n'est plus simplement accepté. Au lieu de cela, il est vérifié une fois de plus pour les incohérences et d'autres possibles exploits. Les utilisateurs verront notamment les blocs rejetés pendant la phase de mining ou de staking (ou les deux en fonction des propriétés de la pièce). En dépit de la tendance à supposer qu'il y a quelque chose qui ne va pas dans la chaîne, car elle rejette les blocs, c'est en fait une opération tout à fait normale et bien accueillie.

L'étape suivante vérifie qu'auparavant le client qui a envoyé une transaction (s'il en a envoyé une dans le bloc précédent) a envoyé une transaction valide en comparant le solde précédent au solde courant avec les frais payés et le minimum requis pour payer le bloc en attente d'être accepté. Si l'un de ces paramètres n'est pas respecté (attention, il s'agit de paramètres de chaîne standard et rien d'extravagant), le bloc est rejeté bien qu'il ait été généré avec succès. Ainsi, ce système sécurise la chaîne, la rend plus stable, prévisible et fiable dans son ensemble, ce qui instaure la confiance que les blocs acceptés sont effectivement des blocs propres.

Cette fonctionnalité est toujours en phase de prototypage. Sa mise en œuvre dans la blockchain d'Espers (qui est un système entièrement hybride utilisant à la fois PoW et PoS) a causé de petits problèmes avec le système de retarget original, qui ont été résolus en passant au système de retarget VRX mentionné précédemment. Ces problèmes consistaient à faire en sorte que la difficulté atteigne son minimum jusqu'à ce qu'un système de retarget approprié puisse être utilisé. Cela étant dit, les blocs acceptés sont maintenant espacés de façon constante à un minimum de 3,5 minutes, ce qui permet à la chaîne d'avancer en douceur. Ensuite, la vérification de transaction et

les vérifications de solde précédentes sont actuellement désactivées jusqu'à ce que les vérifications deviennent irréprochables. La mise en œuvre de ces contrôles spécifiques est encore en cours de développement pour correctement déterminer ces sections des paramètres de la chaîne.

- **Analyse de sécurité**

Les mineurs peuvent également être en mesure de créer des seuils automatiques pour le système afin de ne pas gaspiller de l'énergie, alors que les blocs ne sont tout simplement pas acceptés par la chaîne, créant deux exploits possibles. Tout d'abord, les utilisateurs disposant de systèmes de minage avancés peuvent être en mesure de préminer efficacement un bloc pendant que la chaîne n'accepte pas les blocs et de les empêcher de les soumettre jusqu'à ce que le délai minimum soit écoulé. Si le système utilisait alors un contrôle de sécurité qui vérifie l'horodatage du bloc pour voir si un mineur avait retenu un bloc pour soumission, un autre exploit consisterait à définir un bloc supprimé à créer avec un horodatage valide tant que le mineur connaissait chaque fenêtre de temps valide.

Ces deux exploits sont résolus, d'abord en ayant la méthode précédemment mentionnée du système pour s'assurer que l'horodatage du bloc ne provient pas de l'extérieur de la fenêtre de bloc autorisée. Cela décourage les attaques en créant plus d'étapes pour que l'attaquant puisse passer avant d'avoir une chance de succès. Ensuite, l'implémentation de VRX pénalise le temps de blocage minimum, augmentant la puissance requise pour maintenir une attaque possible (même en injectant un horodatage valide) exponentiellement jusqu'à après quelques blocs générés et la difficulté est si grande qu'un temps minimum ne peut plus être atteint et un autre mineur / participant peut simplement trouver le prochain bloc. Cela annule rapidement tout progrès possible dans l'attaque. Bien sûr, le système Velocity exige que tous les paramètres soient respectés et pas seulement le temps de blocage pour accepter ce qui semble être un bloc généré valablement.

Le système peut être étendu pour inclure plus de vérifications et une implémentation encore plus stricte qui peut s'adapter à tout type de fonctionnalités ajoutées ou supprimées. Cela rend le système d'Espers très adaptable et moins pénible à travailler, car il peut se développer avec de la monnaie et comme il devient plus raffiné et mature, cette nouvelle fonctionnalité de sécurité est appelée Velocity.

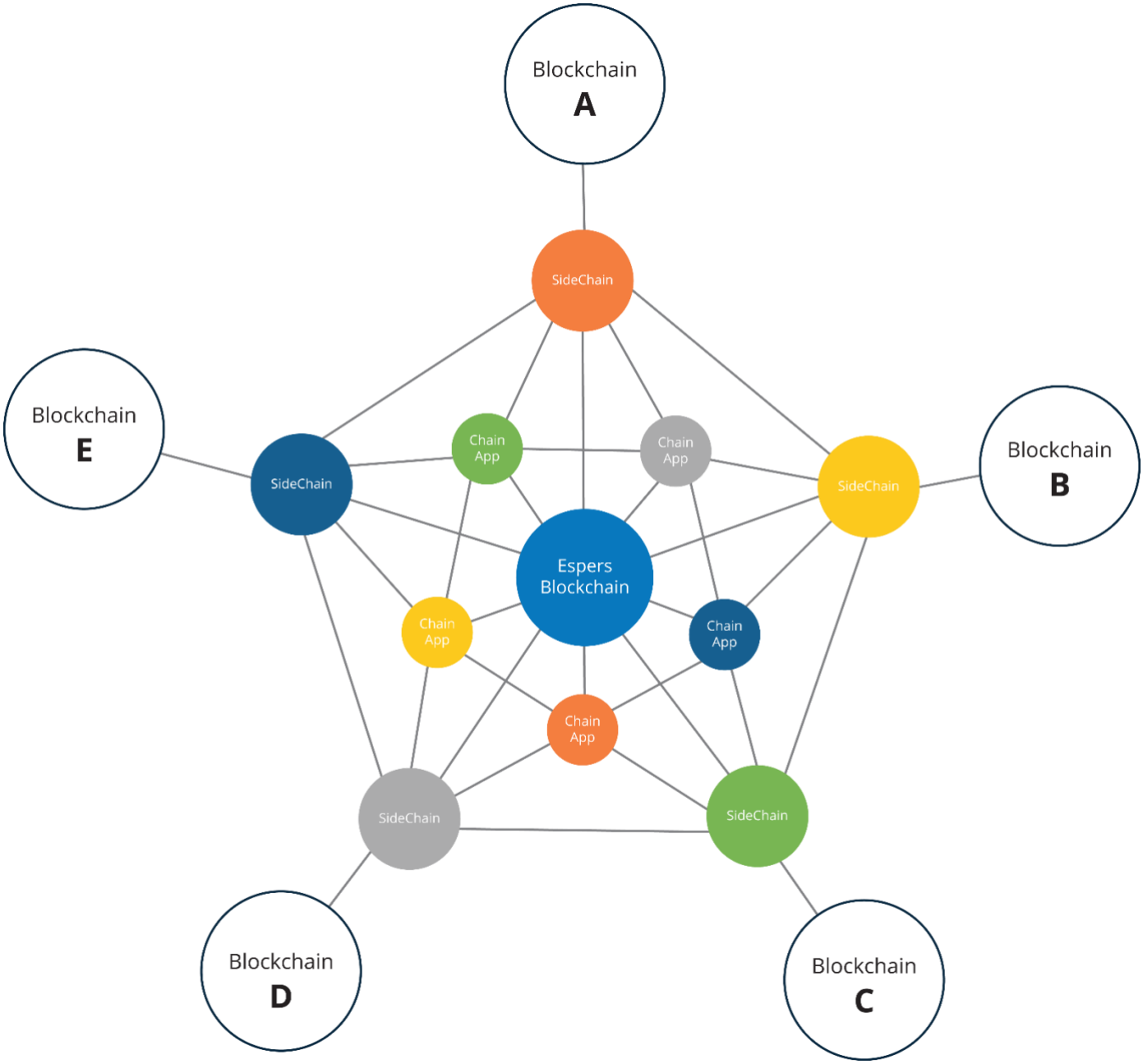
ESPERS

INTERFAÇAGE SIDECHAINS & CROSS-CHAIN

Alors qu'une seule blockchain est capable de traiter de grandes quantités d'informations, de nouvelles méthodes sont apparues où un système blockchain utilise des blockchains plus petites qui dépendent de la chaîne parente qui l'a créée, appelées sidechains (en français chaîne latérale). Ceci permet de traiter simultanément plus de données, tout en allégeant la charge du réseau à partir d'une chaîne quelconque. Certaines approches exigent que la chaîne principale s'interface directement avec les sidechains, en ayant la sidechain entièrement dépendant de la chaîne principale. L'approche d'Espers consiste à faire en sorte que les sidechains restent capables de fonctionner complètement indépendamment. Ces sidechains, une fois créées, continuent à fonctionner sans que l'exigence de la chaîne Espers existe. L'utilisation d'une interface à chaîne croisée, pour transmettre des données d'une chaîne de blocs à une autre, permettra à chaque chaîne de partager des charges de travail tout en restant complètement indépendante. Cette indépendance signifie que, indépendamment de toute défaillance ou tout problème avec une chaîne donnée, le reste du réseau restera intact et opérationnel au lieu de subir un effondrement complet. L'utilisation de ce système permet même d'interagir entièrement avec d'autres projets et communautés, ce qui permet à plusieurs projets de se lier et de profiter les uns des autres si les communautés choisissent de le faire.

Par exemple, si un projet capable de messagerie chiffrée et de distribution de monnaie traite uniquement des données de transaction pour une monnaie avec la blockchain « A » pendant que le traitement des données de texte de message soit effectué sur la blockchain « B », chaque blockchain doit seulement traiter leurs services respectifs. Ensuite, en utilisant l'interfaçage entre chaînes, les produits peuvent partager des données entre eux, fournissant ainsi aux utilisateurs finaux un système fluide, intuitif, rapide, sécurisé et fiable. Pour développer cet exemple, si la blockchain « A » était hypothétiquement compromise, la blockchain « B » resterait fonctionnelle et ses services continueraient également à fonctionner, en permettant aux utilisateurs de continuer à utiliser les services dont ils ont besoin, même si un ou plusieurs éléments peuvent ne plus être accessibles. Ce type de système permet également à un projet blockchain de se libérer d'un simple type de service.

Consulter l'image A pour une illustration visuelle du système proposé.


Blockchain
A
SideChain
Blockchain
E
SideChain
Chain
App
Chain
App
SideChain
Blockchain
B
Espers
Blockchain
Chain
App
Chain
App
Chain
App
SideChain
SideChain
Blockchain
D
Blockchain
C

(Figure A)

ESPERS

MESSAGERIE SECURISÉE

Il y a eu plusieurs tentatives différentes pour implémenter -Secure Messaging (en français Messagerie sécurisée)- dans des projets blockchain. Malheureusement, peu d'entre elles utilisent l'algorithme de la chaîne pour chiffrer les messages. Pour assurer une livraison rapide, le message ne s'attache pas réellement à la blockchain mais plutôt à une clé privée, où le contenu du message est envoyé et à partir duquel il peut être lu. Permettre des relais très rapides des messages sans avoir besoin d'ajouter de la charge au réseau blockchain est une solution intelligente. Cependant, une implémentation correcte de la messagerie sécurisée aurait besoin de diffuser les messages à travers les nœuds à travers la blockchain elle-même, tout comme un bloc miné le ferait normalement.

En stockant du texte brut sur un bloc, de façon similaire au bloc de genèse de Bitcoin qui contient le titre de texte d'un titre d'article sur les blocs de genèse, les messages peuvent alors être plus sécurisés que simplement être cryptés et envoyés au destinataire. Ceci est dû, non seulement au cryptage du message via un algorithme de cryptage, mais aussi via la capacité de confirmer que le message envoyé / reçu est bien valide. Permettre au message de confirmer sa validité, de la même manière qu'une transaction, confirme sa validité dans la blockchain, garantit que les messages reçus et envoyés contiennent uniquement ce qu'ils étaient destinés à contenir. Les messages de spam falsifiés ou autres sont considérablement réduits voire annulés dans certains cas.

Alors que le contenu des messages reste privé, pour des raisons de transparence, la blockchain signale toujours quand un message est envoyé et à quelle clé publique. Cependant, le destinataire et l'expéditeur sont les seuls à avoir accès au contenu car, publiquement, seule une note sur la chaîne indique qu'un message a été envoyé, ainsi que les clés publiques déjà disponibles. La transparence est requise pour tout type de transfert de données, qu'il s'agisse de monnaie ou d'un autre type de service. En effet, sans transparence, il devient très compliqué de vérifier que le destinataire a effectivement reçu le service prévu car la chaîne ne parvient pas à enregistrer correctement les actions prises.

Au-delà du simple ajout de texte dans le contenu d'un message, le système de messagerie d'Espers est également conçu pour traiter et distribuer tout, des images de base aux fichiers compressés aux documents, permettant à ses utilisateurs d'aller au-delà des limitations textuelles. Pour accomplir ces derniers, le système Side-chain et l'interface cross-chain sont utilisés. Espers étant le catalyseur du traitement des données textuelles, ses autres sidechains interagissent directement avec la blockchain mère d'Espers ainsi qu'avec les autres sidechains individuelles, afin de pouvoir traiter simultanément d'autres données tout en conservant la vitesse du réseau. Ceci est fait pour supprimer un point de défaillance central du système tout en permettant une plus grande flexibilité des services. Par exemple, si l'utilisateur « A » envoie un message à l'utilisateur « B » sur la blockchain Espers qui contient des données textuelles stylisées ainsi que quelques images, le message sera divisé et traité simultanément en différentes sections.

Premièrement, la chaîne Espers elle-même traiterait et relayerait les données de message textuel, y compris le code de style, qu'elle interprétera ensuite côté client lors de la réception, en maintenant le traitement des données au plus bas. Deuxièmement, les images que l'utilisateur « A » a envoyées sont ensuite traitées dans une sidechain qui notifie la chaîne Espers d'une pièce jointe d'image à un message envoyé. Une fois le message confirmé, l'utilisateur

« B » est capable de visualiser le contenu du message, les images sont affichées en face de la chaîne locale et le texte du message est rendu nativement à partir de la chaîne locale, garantissant encore une fois que si un quelconque aspect, tel que la défaillance de la sidechain pour les images se produise, le message soit de même réceptionné peu importe l'état de ce dernier. L'inverse est également vrai. Si la chaîne traitant le texte posait un problème, la châine traitant les images relaierait et restituerait les images à l'utilisateur « B », bien que le texte ne soit pas visible. Cela crée un système beaucoup plus robuste que de tenter d'avoir un seul point pour traiter de telles charges de données.

Au-delà de la chaîne Espers, en utilisant l'interfaçage de chaîne, le système peut également interagir directement avec d'autres projets et leurs communautés, en les unissant en permettant aux utilisateurs d'une communauté d'interagir directement avec l'autre. Si deux utilisateurs de deux blockchains différentes mais participantes le souhaitent, ils peuvent envoyer un message depuis leur porte-monnaie / client local au portefeuille / client de l'autre utilisateur, qu'il s'agisse de la même chaîne, communauté ou projet. Cela brise la séparation entre les communautés et permet une plus grande possibilité d'utilisation réelle des systèmes qui existent actuellement et qui sont encore en cours de création. Chaque chaîne traite les messages avec des frais payés à leurs réseaux respectifs, gardant leurs communautés intéressées par le traitement des blocs.

Un avantage clé est de savoir comment cela affecte l'objectif du système Espers. Des entités individuelles telles que des sociétés peuvent gérer de manière pratique et efficace des blockchains autonomes pour leurs propres besoins, comme la messagerie inter-entreprises et le traitement de données dont l'entité a besoin pour rester sécurisée / cryptée. Cette communication inter-chaîne permet une interaction avec un autre département ou une entité entièrement différente, tout en conservant la confidentialité et la sécurité individuelle.

SITE-ON-CHAIN

Les protocoles Internet actuels, y compris SSL et TLS, laissent toujours à désirer. Les sites Web, les serveurs et même les ordinateurs personnels sont compromis presque chaque jour, même avec les meilleures pratiques mises en œuvre et le protocole de sécurité suivi. En effet, une grande partie du trafic qui circule sur Internet n'est ni cryptée ni sécurisée. Les sites Web et entreprises les plus réputés veillent à utiliser un cryptage du trafic avec leurs sites Web. Toutefois, même un serveur ou un réseau compromis peut entraîner la perte de tout le système, compromettant potentiellement les informations clientes, les informations commerciales et autres données sensibles.

En réponse à cette situation, le projet Espers propose que les sites Web et autres services liés à Internet soient exploités / stockés / hébergés via la chaîne de blocs, évitant ainsi toute attaque potentielle des sites Web et autres services Internet, sans jamais nuire à la convivialité. En utilisant la blockchain en tant que protocole Internet, vous ajoutez efficacement une couche de protection presque impénétrable à tout type de service, en particulier les sites Web. Au-delà du simple ajout d'une couche de sécurité, un site web blockchain n'a aucune possibilité de subir une

attaque DDOS, car il n'y a pas de serveurs ou de datacenters à compromettre, pas de fichiers à pirater, pas d'inquiétude, pas de problèmes de stockage, pas de données à intercepter, et ainsi de suite. Afin d'atteindre ce noble objectif, les fonctionnalités précédemment discutées sont toutes utilisées à l'unisson pour amener un site Web correctement rendu à n'importe quel utilisateur à travers quelconque blockchain / projet participant.

Tout d'abord, la partie d'hébergement télécharge son site Web via le client Espers, qui convertit rapidement les fichiers en code brut et les stocke dans des blocs indexés sur la blockchain. Les sidechains individuelles sont utilisées pour stocker chaque type d'information afin que les types de code, les images, les vidéos et autres données ne saturent aucune chaîne donnée. Lorsque l'hébergeur soumet son site Web sur la blockchain, il paie également un petit montant pour traiter les données avec cette dernière, tout comme il le ferait en payant des frais de transaction pour l'envoi d'une transaction. Cette taxe est d'un montant fixe, et est simplement destiné à conserver une compensation raisonnable à tout mineur ou jalonneur qui aurait pu traiter le bloc. Une fois les données traitées et confirmées sur un bloc, ce dernier devient disponible pour toute la communauté en utilisant le système Espers et toutes les autres parties participantes. Lors de la recherche de sites Web, le client d'Espers interroge chaque chaîne pour son type de données prédéterminé et le restitue en direct du côté client pour que l'utilisateur puisse interagir avec ce dernier. Cela signifie que tout type de navigation Web est toujours basé sur une session et non visible par une autre entité ou une tierce partie. Toute information traitée entre le site Web et l'utilisateur est ensuite également sécurisée avec toutes les informations vues par l'utilisateur avec l'accès à la chaîne de rapports et d'autres variables d'utilisation à stocker à des fins analytiques. Ce faisant, un service de navigation Web, tel que Google, pourrait soumettre son propre navigateur qui explorerait alors la chaîne pour les sites Web hébergés sur celui-ci, offrant dans un sens aucune différence de transition entre notre système Internet actuel et ce que l'on peut appeler « Internet 3.0 », tout en maintenant une expérience sécurisée, intuitive et fluide.

En utilisant le système d'interface croisée, Espers peut être jumelé avec de futurs projets similaires afin que l'utilisateur puisse parcourir les sites stockés dans le système d'un autre projet à partir du système client et du système blockchain, tout en restant complètement indépendant sans encourir de risque de défaillance de la chaîne d'un projet indépendant affectant le système actuellement utilisé par un utilisateur. Cela encourage l'unité en permettant une standardisation, ce qui élimine le besoin d'un système propriétaire.

ESPERS

BLOCKCHAIN 《 LÉGÈRE 》/MOBILE

Au fur et à mesure que la blockchain se développe, elle devient « plus lourde » dans le sens qu'elle stocke en permanence des informations sans tenir compte des limitations éventuelles du matériel ou du service pour l'utilisateur final. Afin de contourner une telle préoccupation pour les utilisateurs mobiles ou les utilisateurs qui ne peuvent tout simplement pas stocker la chaîne entière à ce moment / indéfiniment, il est important d'offrir une alternative à ce qu'on appelle un client « complet ». Les clients standard ou « complets », de manière générale, stockent et vérifient l'ensemble de la blockchain qui permet une redondance et un soutien significatifs lorsque les membres de la communauté utilisent le système. Un« Lightweight » (en français « Léger ») ou « Blockchain Mobile » agit comme un portail d'accès, interrogeant la blockchain et tirant des données de celle-ci, plus comme un navigateur de blocs plutôt que de stocker le système localement.

En ne stockant pas la majorité des fichiers localement, le système Espers peut plus facilement être utilisé en pleine échelle sur un appareil mobile ou par un utilisateur ayant des capacités réseau / stockage limitées. Bien qu'une grande partie de ce qui rend ce système léger soit simplement en train d'explorer la blockchain, il a aussi la possibilité de soumettre des données à la blockchain pour qu'elles soient traitées dans le prochain bloc avec ou sans synchronisation de la blockchain. Chaque système devrait permettre la personnalisation par l'utilisateur qui l'utilise et, en tant que tel, la Blockchain Lightweight / Mobile est également capable de se synchroniser partiellement ou entièrement. Si l'option est sélectionnée, le système se synchronisera à partir du dernier point de contrôle et « assumera » que les transactions précédentes, signalées par les chaînes hébergées par les nœuds, sont valides. Une autre option consiste à exécuter une synchronisation complète « silencieuse » où, après la fin de la semi-synchronisation depuis le dernier point de contrôle, le client commence à synchroniser le reste de la blockchain en arrière-plan, permettant à l'utilisateur de toujours prendre en charge le réseau à leur discrétion.

CHAIN APPS

Comme le système de blockchain d'Espers est conçu pour utiliser des sidechains et des fonctionnalités modulaires, les « Chain Apps » (en français « Applications sur chaîne ») se rapportent à la capacité du projet à brancher n'importe quel type d'application fonctionnant en blockchain et à développer ses capacités. Certaines de ces applications en chaîne proviennent des fonctionnalités votées par X-Node (voir plus loin dans la section suivante), tandis que d'autres proviennent de tierces parties vérifiées avant leur mise en œuvre dans le système. Les chain apps, créées par l'utilisateur, peuvent être soumises à tout moment via le client du système et sont ensuite traitées rapidement pour se voir attribuer un sidechain unique à utiliser.

ESPERS

X-NODES

Les X-Nodes ne doivent pas être confondus avec les Masternodes, qui sont un système centralisé dans lequel les utilisateurs verrouillent un montant spécifique pour participer à d'autres fonctionnalités du réseau et les supportent, récompensant ensuite le participant avec une partie de la monnaie générée du bloc suivant si qualifié. Au lieu de cela, les X-Nodes sont complètement « opt-in », ce qui signifie que n'importe quel membre de la communauté peut participer au système indépendamment de leur solde actuel ou de leur expérience antérieure. Cela garantit que l'aspect décentralisation du projet Espers et des blockchains en général ne soit pas perdu, renforçant une fois de plus le réseau global.

Le fonctionnement d'un X-Node consiste à faire en sorte qu'un participant s'inscrive lui-même sur le réseau en tant que processeur de données supplémentaire lui permettant de stocker des sidechains supplémentaires qui sont utilisées pour fournir des fonctionnalités attribuées à ces dernières. Comme pour un Masternode, un X-Node nécessite une connexion Internet permanente et pénalise de manière cohérente tout participant qui se déconnecte, afin d'éviter des connexions incohérentes ou des interruptions de service possibles pour les utilisateurs finaux. Plus un utilisateur participe au système, plus sa chance de faire partie des X-Nodes compensés est automatiquement votée par le réseau en fonction de la fiabilité et des données traitées. Un utilisateur participant peut alors également verrouiller n'importe quel montant de son solde qui deviendra effectivement gelé, car le participant ne pourra plus le jalonner tant qu'il ne sera pas déverrouillé du X-Node et, ce faisant, le solde agira comme un multiplicateur pour le taux de compensation fourni. Bien sûr, le multiplicateur se trouve sur une courbe et implémente plusieurs systèmes anti-abus, tels que la nécessité d'une période d'attente pour les pièces récemment verrouillées. Jusqu'à ce que l'attente soit terminée, un participant ne verra pas d'effet multiplicateur. Plus la quantité verrouillée est faible, plus l'utilisateur doit attendre pour le déblocage à un rythme exponentiel. Les soldes plus importants exigent que les utilisateurs attendent moins de temps pour les déverrouiller, tout en ayant le multiplicateur sur une courbe exponentielle. Ceci annule l'utilité de balances significativement plus grandes, en veillant à ce que les utilisateurs soient encouragés à verrouiller des montants plus importants pour être récompensés plus tôt, tout en pénalisant un éventuel blocage de « poussière » à un tel point que cela devienne impossible.

Un montant verrouillé sera toujours capable de trouver le bloc suivant dans la chaîne, mais toutes les pièces créées seront détournées (après que l'attente du blocage soit dépassée) au vote de fonctionnalité sélectionné du participant. Voter sur le réseau de cette manière est crucial pour établir un développement rapide des fonctionnalités par l'équipe du projet et augmenter le soutien de la communauté. Les participants peuvent également choisir de ne pas voter, mais l'aspect multiplicateur est à nouveau pénalisé, car cela crée une baisse de la prise en charge des nouvelles fonctionnalités du réseau. Tout participant peut soumettre une fonctionnalité demandée à voter par le réseau pour un développement futur, mais lorsque le tour de vote se termine, tout vote de fonctionnalité qui n'a pas été sélectionné est regroupé et divisé en deux sections qui sont ensuite utilisées de manière indépendante. La première moitié est divisée en sections qui sont ensuite réinjectées dans le réseau en tant que frais payés permettant aux mineurs et aux jalonneurs de recevoir un léger « bonus » jusqu'à ce que le solde soit épuisé, tandis que la seconde moitié est affectée aux caractéristiques gagnantes. Les utilisateurs peuvent débloquer leur solde à tout moment lorsqu'ils participent au système X-Node, même si le solde n'a pas terminé la période de récupération, ce qui donne

aux utilisateurs un contrôle total sur leur expérience. De même, si un participant se retire à un moment donné, tout comme lors de son inscription, le participant devra attendre entre la désactivation et le temps de réactivation permis. De plus, le système X-Node est intuitif et permet de supprimer, en un seul clic, les éventuelles erreurs de l'utilisateur qui se produisent souvent avec des fonctionnalités similaires telles que les Masternodes et de les remplacer par l'intérêt / l'immersion de l'utilisateur. Cela prend également une charge considérable à l'écart des besoins de support, des incohérences de réseau et des tracas d'exploitation ou de participation au système.

ESPERS

ROADMAP

Q4 2017

- Website Update
- PoW & PoS Revise
- Wallet Upgrade
- Marketing Campaign (active)

Q1 2018

- Whitepaper
- Mobile Wallet
- Lightweight Client

Q2 2018

- Xnodes
- Sidechains
- Mailing System

Q3 2018

- ChainApps
- CrossChain
- SiteOnChain

DISCLAIMER

This Roadmap is for informational purposes only, and not a binding commitment. Do not rely on this information in purchasing Espers coins/tokens as ultimately the development and timing remains at the sole discretion of the Espers/CryptoCoderz team.

ESPERS

MEET OUR TEAM

A PERFECT BLEND OF CREATIVITY AND DEVELOPMENT WIZARDRY.

CRYPTOCODERZ

Jonathan Zaretsky

Lead Project Manager

Developer

MONOXIDE

Assistant Project Manager

Public Relations

CTGIANT

Assistant Developer

BATYSTA

Antonio Batista

Project logistics

ARSONIC

Guillaume Huot

Lead Web Developer

Graphics Designer

BBOBB

Project logistics

ARCADE

Justin Cappellini

Public Relations

ESPERS

DIVULGATION

Ce Whitepaper (document) est à titre informatif seulement, et non un engagement contraignant. Ne comptez pas sur ces informations lorsque vous interagissez avec la monnaie Espers, car le développement et le timing restent à la seule discrétion de l'équipe d'Espers / CryptoCoderz.

Nous, l'équipe d'Espers / CryptoCoderz, n'entendons en aucun cas nuire à qui que ce soit, sous quelque forme que ce soit. Il n'y a jamais eu de crowdsale de monnaie, de prévente ou de toute autre méthode crowdfunding (en français, financement de foule) utilisée pour le projet Espers / CryptoCoderz ou ses développeurs. Merci de comprendre les risques liés à la technologie de blockchain cryptographique et leurs monnaies respectives. L'équipe d'Espers / CryptoCoderz ne peut être tenue responsable des fonds perdus, volés ou manquants de quelque nature que ce soit. Si vous n'êtes pas sûr ou avez des doutes sur ce projet, nous vous prions de NE PAS investir ou vous impliquer, car il s'agit d'un prototype de système technologique tel qu'indiqué dans de nombreux domaines et à utiliser à vos risques et périls.

Nous n'avons aucune affiliation avec le produit se trouvant sur Yobit appelé « Espers ». Ceci est un produit distinct uniquement exploité par Yobit.

CRÉDITS

Un grand merci à tous ceux qui ont contribué à la réalisation de ce projet, un merci spécial aux membres de la communauté (noms d'utilisateur) suivants qui ont contribué à la création et aux révisions de ce document :

Bit010
CafeConTiki
CryptoCarrot
cXplexus
Eugen
Gandalf86
IK
Tekna
Vin
Wolf