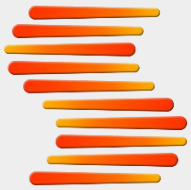


LIVRE BLANC SECURE SWAP

Grey Matter Technologies

www.secure-swap.com

LIVRE BLANC SECURE SWAP

SOMMAIRE

PRÉSENTATION DE SECURE SWAP

La partie résumé et points forts s'adresse à ceux qui ne voudraient pas lire en détail tout le document, ou pour ceux qui veulent se faire une idée préalable rapide de ce projet, avant d'en faire une lecture plus approfondie.

RÉSUMÉ

Secure Swap, une nouvelle génération d'échangeur :

L'Echangeur peut fonctionner sans le support d'une société opérante, du fait de son architecture p2p et de l'absence de serveurs centraux.

Il est open source.

Sa technologie est fortement modulaire, permettant d'ajouter des services (support de crypto-monnaies, support d'échanges fiat) par ceux qui le désirent et ainsi, d'en devenir acteur.

Il permet aux NodeOwners (utilisateurs faisant fonctionner un ou des nodes passerelles) d'en tirer une source de revenu, en supportant son fonctionnement communautaire.

Sa technologie inspirée des échanges de fichiers type P2P comme BitTorrent, rend le cœur du système à l'abri de régulations et d'interdictions brutales des crypto-monnaies. Ces régulations peuvent représenter un risque pour ceux qui en détiennent, suivant leur lieu de résidence. Secure Swap offre une porte de sortie toujours disponible.

Il est totalement anonyme (du moins autant que le permettent les crypto-monnaies échangées) lorsque l'on échange des crypto-monnaies entre elles.

Néanmoins, dès qu'il s'agit d'échanger des crypto-monnaies avec des devises fiat, il permet de respecter totalement les règlementations en vigueur, du fait de son aspect modulaire et de la nette séparation des systèmes échangeant des devises fiat avec les crypto-monnaies du reste des échanges.

Ce dernier aspect permet aussi à ceux qui le souhaitent d'opérer, à partir d'une structure légale, une activité professionnelle d'échange de crypto-monnaies vers devises fiat, dans les devises de leur choix.

Son protocole de fonctionnement intègre des systèmes de détection d'anomalies entrainant l'arrêt automatique des échanges sur les crypto-monnaies concernées par une tentative de hacking.

Son client de trading offre un niveau de confort et d'ergonomie comparables aux meilleurs logiciels de trading sur les marchés boursiers classiques.

POINTS FORTS

SÉCURITÉ

- Système sécurisé par conception, avec détection des tentatives de hacking, alerte et arrêt automatique des parties concernées.
- Système réellement décentralisé, les utilisateurs restent en possession de leurs crypto-monnaies jusqu'au moment d'effectuer un échange.
- Par sa nature totalement décentralisée, pas de tiers de confiance, pas de prise pour les régulateurs pour empêcher son utilisation.
- Pas de concentration de crypto-monnaies, ce qui est une cible de choix pour les hackers dans les échangeurs centralisés. Mais aussi dans les échangeurs dits décentralisés mais dont l'architecture implique la concentration des crypto-monnaies ou de tokens.
- Un système ouvert qui permet à chacun d'en contrôler le code, le fonctionnement et la sécurité.

DISPONIBILITÉ

- Système fortement redondant, garantissant une résistance à la panne, donc une grande disponibilité du service, même en cas de charge importante.

UN ÉCHANGE CONTRÔLÉ ET OPÉRÉ PAR UNE COMMUNAUTÉ

- Son aspect distribué et communautaire rend le service indépendant de l'existence de la société qui l'a créé et n'a pas besoin d'elle pour fonctionner.

UN ÉCHANGE EXTENSIBLE

- De par sa nature open source et modulaire, les utilisateurs qui le désirent peuvent ajouter à l'échangeur le support de nouvelles crypto-monnaies ainsi que des échanges de crypto-monnaies vers devises fiat de leur choix.

UNE SOURCE DE REVENU POUR CEUX QUI SUPPORTENT SON FONCTIONNEMENT

- Ceux qui supportent le fonctionnement du service (NodeOwners), en faisant fonctionner des parties du système (passerelle vers une crypto-monnaie spécifique), sont récompensés en gagnant une partie des frais payés par les traders sur les échanges.
- Permet de développer une activité commerciale d'échange de crypto-monnaies vers devises fiat partout où cela est légal dans le monde (nodes de conversion vers devise fiat).

UN ÉCHANGEUR MONDIAL

- Outre le fait que le réseau est de fait accessible de partout dans le monde pour les échanges de crypto-monnaies, le support de nouvelles devises fiat par la communauté rendront progressivement le service mondial, pour les devises fiat également.

ÉTAT DU MARCHÉ

ÉCHANGEURS CENTRALISÉS

Les plateformes d'échanges centralisées sont fréquemment soumises au piratage, entrainant le vol de crypto-monnaies. Lorsque cela se produit, un grand nombre de traders présents sur ces plateformes en sont victimes, avec des sommes dérobées importantes, puisque ces plateformes concentrent les fonds des traders.

En effet, une plateforme d'échanges centralisée possède littéralement les crypto-monnaies qui y ont été envoyées. C'est l'échangeur qui détient les clefs privées des wallets des traders. Les utilisateurs doivent donc lui faire totalement confiance, malgré les risques de piratage et de faillite qui peut en découler. D'un autre côté, ces échangeurs ont l'avantage d'avoir un carnet d'ordres centralisé, et donc une meilleure liquidité et une meilleure rapidité d'exécution des ordres, contrairement à la plupart des plateformes décentralisées.

Le manque de confiance sur la sécurité des plateformes centralisées par rapport aux risques de piratage fait que beaucoup de traders n'osent pas laisser leurs crypto-monnaies sur ces plateformes. Ils les retirent dès qu'ils ne tradent plus et doivent les renvoyer sur la plateforme pour trader de nouveau, ce qui entraine des frais de transactions et des délais supplémentaires.

Ce manque de sécurité rend aussi assez inutile les ordres classiques comme les stop-loss, les ordres à plage de déclenchement, les ordres OCO (order cancels order), vu que beaucoup de traders ne laissent pas leurs crypto-monnaies sur les plateformes d'échanges. Les traders ne prennent plus le risque de laisser leurs crypto-monnaies sur une plateforme, même avec un stop-loss, et préfèrent les retirer et ne plus risquer de se les faire dérober.

ÉCHANGEURS DÉCENTRALISÉS

Les plateformes d'échanges décentralisées présentent souvent une ergonomie en retrait par rapport aux plateformes centralisées, et souvent une liquidité moindre de par leur nature décentralisée, contre une meilleure sécurité (ou du moins une sécurité qui dépend entièrement de l'utilisateur), et une absence de tiers de confiance, les utilisateurs restant en possession de leur crypto-monnaies (clefs privées des wallets).

Elles présentent aussi souvent un choix limité en crypto-monnaies échangeables, du fait que leurs technologies dépendent de l'interopérabilité des crypto-monnaies échangées, ou de la disponibilité de l'Atomic Swap sur ces dernières etc. Peu de plateformes décentralisées permettent l'échange d'un grand nombre de crypto-monnaies différentes, et quand elles le font, il y a souvent une partie de leurs systèmes qui ne sont pas décentralisés (tokens centralisés servant de contreparties aux échanges, ou de garantie de liquidité par exemple). Ce qui représente un risque comparable aux échangeurs centralisés classiques, à la différence que ce n'est pas le trader qui prend ce risque, mais l'opérateur de l'échangeur.

AUTRES ASPECTS

Les plateformes d'échanges existantes sont très fréquemment victimes de problèmes de charge, allant jusqu'à l'interruption de leurs services lors des périodes de grosse activité, alors que cela correspond souvent aux moments où les traders en ont le plus besoin (panique sur les marchés).

Par ailleurs, beaucoup de plateformes existantes, qu'elles soient centralisées ou pas, présentent une ergonomie d'utilisation peu confortable (biens que cela s'améliore avec les échangeurs récents), certains sites étant des casse-têtes à utiliser, même pour un trader confirmé.

Les utilisateurs ont appris à composer avec ces problèmes mais ces situations gênent l'adoption des crypto-monnaies par le plus grand nombre. Cela reste perçu comme compliqué, risqué et difficile à appréhender.

SOLUTIONS APPORTÉES PAR SECURE SWAP

UNE PLATEFORME D'ÉCHANGE DÉCENTRALISÉE, MODULAIRE, OUVERTE ET COMMUNAUTAIRE

Pour répondre aux problèmes identifiés, Secure Swap procure à la fois les avantages des échanges centralisés et décentralisés : bonne liquidité, **sécurité renforcée « by design »**, pas d'intermédiaires de confiance détenant les crypto-monnaies des traders et une ergonomie inspirée des meilleurs logiciels de trading boursiers.
De plus, la technologie p2p des nodes assure une capacité de montée en charge et de redondance, garantissant la fiabilité et la disponibilité du service.

Secure Swap est aussi un système ouvert qui permet à chacun d'en contrôler le code, le fonctionnement et la sécurité, et de participer à son fonctionnement en supportant des nodes passerelles vers les crypto-monnaies. **Les frais d'échanges sont redistribués en totalité** à ceux qui font fonctionner ce type de nodes, au prorata des tokens SSW qu'ils détiennent. Il constitue donc pour tous ceux qui le désirent, et investissent dans le token SSW, une source de revenu majeure.

Secure Swap est un écosystème d'échange de crypto-monnaies, articulé autour d'un service décentralisé, d'une application client pour le trading et de micro services optionnels pour tirer parti des nouvelles opportunités offertes par ce nouveau réseau. Ces micro-services sont des nodes spécialisés, tel que les nodes de connexion à différentes blockchains, des nodes de connexion à des processeurs de paiement pour les échanges avec les devises fiat, des nodes d'arbitrages, etc.

L'application client et les nodes, communiquent entre eux via la technologie Peer to Peer (p2p), constituant ainsi un service décentralisé.

La sécurité et l'atomicité des échanges sont assurés par des smart contrats (un par blockchain) dédiés à cette tâche, initialement sur la blockchain Ethereum. Il sera porté sur d'autres blockchains supportant les smart contrats tels que EOS, afin d'assurer la sécurité/atomicité des échanges sur ces dernières. Cela permet aussi d'augmenter le nombre de transactions par seconde réalisables, par agrégation des capacités d'exécution de chaque blockchain. L'ensemble des smart contrats sur chaque blockchain formant une distribution d'applications DAPP, assurant l'interopérabilité entre les blockchains, pour les échanges.

Seule l'application client Secure Swap a connaissance des clefs privées des wallets de l'utilisateur. Elle est ainsi à même de signer les contrats à destination des blockchains (signature offline). De ce fait, personne ne peut signer les transactions à la place de l'application client, lors d'une tentative de vol des avoirs des traders. Le trader reste ainsi propriétaire de ses crypto-monnaies, contrairement aux plateformes d'échanges centralisées, sur lesquelles le trader transmet ses crypto-monnaies qui y sont entreposées, ces plateformes étant propriétaires des clefs privées, donc des crypto-monnaies entreposées.

Dès que l'utilisateur se déconnecte du service d'échanges, donc quitte le logiciel client, les clefs privées de ses wallets, qui sont stockées localement sur son ordinateur, se retrouvent de fait offline (équivalent à un 'cold storage'). Les clefs privées de ses wallets ne sont jamais transmises sur Internet et n'ont jamais quitté l'application client.

De plus, si l'utilisateur possède des wallets hardware (Ledger, Trezor…), les clefs privées correspondant à ses wallets ne sont même jamais stockées sur son ordinateur mais restent en sécurité sur ses wallets hardware.

Dès que l'utilisateur connecte le client au réseau p2p, il est prêt à trader/échanger ses crypto-monnaies, sans frais inutiles de transferts préalables sur un échangeur, tout en ayant une sécurité comparable à un stockage de ses coins sur un wallet privé, en 'cold storage'.

L'application client permet d'offrir un confort d'utilisation et une ergonomie comparable aux meilleurs logiciels de trading existants (marchés boursiers, contrats futurs, Forex...). L'application client proposera notamment des ordres dits 'avancés', comme les ordres à plages de déclenchement, les ordres conditionnels à pattes multiples, les ordres OCO…, ainsi que le trading sur le graphique avec des ordres conditionnels sur franchissement de droites horizontales ou pentes, sur indicateurs, etc.

Par ailleurs comme Secure Swap agrège les ordres des clients via les nodes p2p, cela permet de conserver les avantages des échanges centralisés : liquidité et rapidité d'exécution. Pour renforcer la liquidité, un mécanisme d'arbitrage (node d'arbitrage) est chargé d'assurer celle-ci, par l'utilisation d'une réserve de crypto-monnaies appartenant à la société et par l'exploitation des carnets d'ordres des autres échangeurs, via leurs APIs.

ARCHITECTURE ET FONCTIONNEMENT DE L'ÉCHANGEUR

L'architecture réseau distribuée est basée sur un core applicatif Javascript (base commune p2p), qui servira aux différents modules de l'écosystème : client de trading, nodes p2p de passerelles vers les blockchains, node p2p d'arbitrage chargé d'assurer la liquidité de l'échangeur, nodes d'échanges crypto/fiat, node indiquant l'état du réseau…

L'application client émet les ordres donnés par l'utilisateur vers les nodes connectés, ce qui permet de les consolider. Les nodes propagent la totalité des ordres collectés de node en node chaque fois qu'il y a un changement, si bien que chaque node dispose du carnet d'ordres complet. Comme l'application client est également un node, elle reçoit donc aussi la totalité des ordres émis sur le réseau p2p.

Chaque app-client effectue le matching de ses propres ordres, contre le carnet d'ordres complet, afin de trouver des contreparties concernant les ordres que le trader a émis.

Quand un matching (contrepartie) est trouvé, l'app-client en informe les nodes p2p connectés. Les nodes passerelles vers les blockchains concernées par l'échange vont en informer le smart contrat d'échange de chaque blockchain qui valide alors une demande d'envoi de crypto-monnaies à chaque client concerné pour recevoir les fonds impliqués dans l'échange. Les smart contrats de chaque blockchain impliquée, une fois les fonds reçus sur le wallet qui lui sert à gérer l'échange, et après validation de l'atomicité de l'échange par un mécanisme spécifique [(*)], envoient ces crypto-monnaies aux wallets destinataires de l'échange. Si la totalité des fonds impliqués dans un échange n'est pas reçue après un certain délai, l'échange est annulé et les fonds sont restitués à leurs propriétaires respectifs. Cela assure l'atomicité des échanges. Une fois l'échange effectué, les app-clients retirent les ordres qui ont été servis, chaque app-client retirant ses propres ordres, ce qui met à jour le carnet d'ordres global.

Hormis les frais réseau propres à chaque blockchain, payés par les traders, les smart contrats d'échange collectent sur chaque échange un petit pourcentage, qui sera redistribué aux possesseurs de tokens SSW qui feront fonctionner un/des nodes connectés à des blockchains, au prorata des tokens possédés et du nombre total de tokens alloués à chaque blockchain.

Exemple : un NodeRunner fait fonctionner un node p2p qui est connecté à la blockchain Ethereum (passerelle vers Ethereum), il a alloué 100 tokens parmi ceux qu'il possède pour le fonctionnement de ce node (via un wallet dédié, les tokens restant sa propriété). Si par ailleurs, d'autres NodeOwners font aussi fonctionner des nodes p2p connectés à la blockchain Ethereum, et que l'ensemble de ces nodes ont 1000 tokens alloués pour cela, alors notre NodeRunner recevra 10% (100/1000) des frais collectés sur tous les échanges impliquant des Ethereums.

S'il a d'autres tokens SSW, et qu'il fait fonctionner d'autres nodes se connectant à d'autres blockchains, le NodeRunner recevra aussi la part lui revenant des frais d'échanges concernant ces autres blockchains. Ce système d'allocation par blockchain, permet d'inciter les utilisateurs à faire fonctionner des nodes pour connecter l'échangeur à des blockchains où peu de nodes sont en fonctionnement, ce qui tend à renforcer la redondance, donc la disponibilité du système et sa sécurité.

[(*)] Voir description détaillée au paragraphe « Système de validation de l'atomicité des échanges »

ASPECT FINANCIER DU TOKEN

DONNÉES UTILISÉES POUR CETTE PROJECTION

- Nombre de tokens total émis : 100.000.000
- Prix d'émission du token : 0.45$ USD
- Pourcentage de tokens effectivement assignés aux nodes passerelles : 50%

Nous pensons qu'une partie des acquéreurs de tokens SSW ne feront pas fonctionner de nodes passerelles vers des crypto-monnaies, perdant ainsi la part correspondante des frais d'échanges payés par les traders, mais les achèteront uniquement pour des motifs de spéculation sur le prix du token. Cette projection nous semble optimiste, la réalité pourrait être plus proche des 30%. Plus la part des tokens assignés au fonctionnement des nodes passerelles est faible, plus le rendement des tokens pour ceux qui le font est grand.

Les données suivantes proviennent de CoinMarketCap, prise fin Juillet 2018.

Les volumes d'échanges correspondent à une période de fin de krach de crypto-monnaies, on peut espérer que par la suite les volumes d'échanges remontent à des niveaux plus habituels, ce qui augmentera la rentabilité de la détention de tokens, dans le but de faire fonctionner des nodes passerelles.

Exemples de répartition de la distribution des échanges entre crypto-monnaies sur 24h.

Bitcoin :	33%
Tether :	20%
Ethereum :	11%
EOS :	4.5%
OmiseGo :	0.45%

Nous avons ici les 3 crypto-monnaies les plus échangées ainsi que 2 crypto-monnaies moins échangées.

Volume d'échanges des échangeurs sur 24h suivant leur ranking de CoinMarketCap :

Rank 100: 3.000.000 $USD

Rank 75: 10.000.000 $USD

Rank 50: 20.000.000 $USD

PROJECTION DE LA RENTABILITE D'INVESTISSEMENT DANS LE TOKEN SSW

Nous considérons que les tokens qui sont assignés au fonctionnement des nodes passerelles le sont en proportion du volume d'échanges de chaque crypto-monnaie. Une sur-allocation de tokens sur des nodes passerelles d'une crypto-monnaie ferait baisser la rentabilité des tokens pour cette crypto-monnaie. À contrario, la sous-allocation de tokens pour d'autres crypto-monnaies qui en découlerait, ferait augmenter la rentabilité de ces dernières. Ceci implique que ceux qui feront fonctionner des nodes passerelles, auront tendance à assigner leur tokens aux crypto-monnaies les plus rentables, ce qui fera baisser la rentabilité de ces dernières et augmenter celle des autres. En conséquence, la répartition des tokens va naturellement s'aligner sur la répartition des volumes d'échanges entre crypto-monnaies.

Formule de calcul de rentabilité des tokens :

TTOK : Total tokens émis à l'ICO
FTAP = Pourcentage tokens assignés aux nodes passerelles
VE = Volume d'échanges, en $USD
FEC = Pourcentage d'échanges de la crypto-monnaie par rapport au total échangé
FRTC = Pourcentage répartition des tokens pour les nodes passerelles de la crypto-monnaie
PX = Prix d'achat du token, en $USD
T = Frais pris par la plateforme pour les échanges.

$$\text{RENTABILITÉ TOKEN} = ((\sum VE \times FEC \div FRTC \times T) / (TTOK \times FTAP)) / PX$$

On voit que si FEC = FRTC, nous obtenons :

$$\text{RENTABILITÉ} = ((\sum VE \times T) / (TTOK \times FTAP)) / PX$$

LA RENTABILITÉ EST DONC ALORS LA MEME POUR TOUTES LES CRYPTOS SI FEC = FRTC, INDEPENDAMMENT DE LEUR VOLUME D'ECHANGE.

Par exemple :

Imaginons un volume d'échanges de 3M$ USD journalier (échangeur rank 100 sur CoinMarketCap)

En annuel, cela nous fait : ∑ VE = 365*3M = 1.095 M $USD

Les frais de l'échange étant de T = 0.15%, nous avons alors :

Rentabilité = ((1.095.000.000 * 0.0015) / (100000000 * 0.5)) / 0.45 = **7.3%** de rendement annuel

Avec un volume d'échanges de 10M$ USD journalier (échangeur rank 75 sur CoinMarketCap)

Rentabilité = ((10.000.000 * 365 * 0.0015) / (100000000 * 0.5)) / 0.45 = **24.33%** de rendement annuel

Avec un volume d'échanges de 20M$USD journalier (échangeur rank 50 sur CoinMarketCap)

Rentabilité = ((20.000.000 * 365 * 0.0015) / (100000000 * 0.5)) / 0.45 = **48.67%** de rendement annuel

CONCLUSIONS

En étudiant le classement des échangeurs sur CoinMarketCap, on peut vérifier que les échangeurs en dessous du top 100 sont des échangeurs qui, très vite, sont délaissés des utilisateurs et ont par conséquent un faible volume d'échanges.

Nous pensons qu'au vu de ses avantages, dès que le nombre de coins échangeables sera suffisant, Secure Swap n'aura aucun mal à se classer dans le top 100 des échangeurs.

Par ailleurs, dès que les coins qu'ils veulent échanger sont supportés par Secure Swap, les NodeOwners, qui font fonctionner des nodes passerelles, n'auront pas intérêt à utiliser d'autres plateformes d'échanges. De ce fait, viser le top 50 ne nous parait pas irréaliste.

Par conséquent, au fur et à mesure de l'adoption de Secure Swap par les utilisateurs, le rendement des tokens SSW pourra évoluer de 7% annuel à 48 % annuel. En visant une situation intermédiaire avec un volume d'échanges correspondant au top 75 de CoinMarketCap, nous pouvons espérer **un rendement annuel de 24%** pour les investisseurs qui participeront à l'ICO. Pour ceux qui achèteraient des tokens SSW plus tard, cela dépendra de leur prix d'achat. Un prix d'achat moins cher augmente le rendement, un prix d'achat plus cher le fait baisser.

Par ailleurs, il faut remarquer que ces chiffres de volumes échangés, sur lesquels s'appuient cette projection, sont récents et collectés dans une période qui suit de longs mois de krach de la dernière bulle des crypto-monnaies. On peut supposer que dans les prochains mois, le marché des crypto-monnaies va repartir en croissance, ce qui augmentera les volumes échangés, et donc la rentabilité du token.

SYSTÈME DE VALIDATION DE L'ATOMICITE DES ÉCHANGES

POUR LES ÉCHANGES AU SEIN DE L'ECOSYSTÈME ETHEREUM (ETH ET TOKENS ERC-20/ERC-720)

L'atomicité de l'échange est entièrement assurée par un smart contrat sur la blockchain Ethereum.

Ce smart contrat a la possibilité, sans intervention extérieure, de vérifier la réception des ETH/tokens et de les renvoyer aux destinataires.

Ce type d'échange fera l'objet d'améliorations avec l'intégration de Plasma/Lightning Network quand ces solutions de deuxième niveau seront opérationnelles et matures. Ce qui augmentera sensiblement la rapidité des échanges au sein de l'écosystème Ethereum.

POUR LES ÉCHANGES ENTRE BLOCKCHAINS INTEROPÉRABLES

Pour les échanges entre blockchains interopérables (Par exemple entre Litecoin et Decred, ou Ethereum et Omisego) : cette interopérabilité n'est pas encore effective actuellement, et quand elle le sera, elle utilisera les technologies comme Plasma ou bien Lightning Network. En attendant, Secure Swap traite ces blockchains comme non-interopérables.

POUR LES ÉCHANGES ENTRE BLOCKCHAINS NON INTEROPÉRABLES

Dans ce cas, notre échangeur va réaliser l'interopérabilité entre ces crypto-monnaies via son réseau p2p.

CAS OÙ LES CRYPTO-MONNAIES FAISANT PARTIE DE L'ÉCHANGE SUPPORTENT LES SMART CONTRATS

Tous les nodes passerelles d'une crypto-monnaie vérifient que les smart contrats (un par blockchain) valident l'arrivée des coins sur les wallets avant envoi aux destinataires, afin de garantir l'atomicité de l'échange.

Ils envoient sur le réseau p2p la validation de la réception des coins à destination de l'autre smart contrat (smart contrat de la contrepartie).

Quand les deux smart contrats impliqués dans un échange ont eu la validation de la réception des coins, ils sont envoyés aux destinataires finaux, afin de conclure l'échange par les smart contrats eux-mêmes.

Pour se prémunir du hacking des nodes ou de nodes malicieux, les smart contrats ne valident la réception de coin de la part de la contrepartie uniquement si tous les nodes passerelles de la crypto monnaie correspondante confirment la réception des coins.

En cas de désaccord entre les nodes passerelles (donc présence de nodes hackés/malicieux), la réponse majoritaire l'emporte (voix d'un node passerelle = nombre de tokens SSW associés à ce node), tous les nodes

passerelles donnant une réponse non conforme sont déconnectés et black-listés (adresse ip sur liste noire, empêchant la reconnexion de ces nodes au réseau p2p).

Chaque fois qu'un node est déconnecté pour réponse non conforme, il envoie au réseau p2p l'information de cette déconnexion pour non-conformité, qui se propage ainsi à tous les clients et tous les nodes. Chaque client qui reçoit cette information désactive le trading sur cette crypto-monnaie et annule tous ses ordres impliquant cette crypto-monnaie. Tous les nodes du réseau mémorisent le statut de trading de chaque crypto-monnaie, par conséquent un client qui n'était pas connecté lors de la tentative de hacking et qui se connecterait ensuite, serait immédiatement informé de la désactivation du trading sur cette crypto-monnaie. Pour que le trading puisse reprendre sur cette crypto-monnaie, il faut que la majorité qualifiée (>=60%) des clients préalablement désignés pour cela (délégués volontaires) aient réactivé le trading sur cette crypto-monnaie.

Ce qui découle de ce protocole, c'est un consensus par preuve d'enjeu. Pour tenter de hacker le réseau p2p et tenter de voler les coins d'un échange (donc ne pas envoyer la contrepartie tout en recevant les coins de l'autre utilisateur), il faudrait posséder plus de la moitié du total de tokens SSW assignés aux nodes passerelles d'une crypto-monnaie.

Cela veut dire que pour tenter de voler un échange, il faut mettre en jeu une somme en tokens SSW importante. L'effet sur la réputation de l'échangeur, si la tentative réussissait, provoquerait une chute de la valeur du token SSW impliquant des pertes pour le hacker beaucoup plus importantes que les gains obtenus par le vol d'une transaction.

Par ailleurs, comme il y avait forcément quelques nodes honnêtes sur le réseau avant prise de contrôle des hackers, ces derniers, lorsqu'ils ont été déconnectés, ont envoyé une désactivation du trading sur cette crypto-monnaie que tous les nodes (clients et node autres) ont reçu. Cela provoque également l'annulation de la transaction en cours et la restitution des coins concernés à leurs utilisateurs par les smart contrats.

Ce protocole rend improbable le succès d'une tentative de prise de contrôle, et quand bien même cela arriverait, il n'y aurait rien à voler (trading désactivé), pour un engagement en tokens SSW très important, rendant cette opération assurément non rentable et même très coûteuse.

Pour que cette sécurité soit effective, il faut que les nodes passerelles d'une blockchain soient suffisamment nombreux et que l'ensemble des nodes passerelles aient une quantité de tokens SSW alloués nettement supérieure à la valeur moyenne d'un échange, pour constituer une preuve d'enjeu valable.

C'est pour cela que l'app client refuse de faire un échange avec une crypto-monnaie, si le nombre de passerelles actives pour celle-ci est inférieur à deux, qui est un strict minimum.

CAS OÙ L'UNE DES CRYPTO-MONNAIES (OU LES DEUX) FAISANT PARTIE DE L'ÉCHANGE NE SUPPORTE PAS LES SMART CONTRATS

Dans ce cas, le rôle opéré normalement par le smart contrat de la crypto-monnaie est effectué par un node spécialisé, par crypto-monnaie, sous le contrôle et avec une sécurité garantie par la société Grey Matter Technologies.

En absence de support de smart contrat sur une crypto-monnaie on ne peut pas se passer d'un tiers de confiance. Ainsi ce node spécialisé garantira la réception des coins de chaque partie d'un échange avant envoi vers le destinataire, afin d'assurer l'atomicité des échanges sans smart contrat.

Pour ces échanges sans smart contrat, ce service spécifique de Secure Swap n'aura besoin de prendre possession des crypto-monnaies du trader qu'uniquement pendant le temps nécessaire à la transaction. Contrairement aux échanges centralisés où le trader doit transmettre ses actifs pour une longue période de temps.

Dans ce cas également, il n'y a pas de stock central de crypto-monnaies, juste un stockage temporaire des contreparties, le temps de valider l'atomicité de l'échange. Il n'y a donc pas grand-chose à gagner à tenter de hacker cette partie.

INDICATION DU STATUT DE L'ÉCHANGEUR

INDICATIONS PROVENANT DU CLIENT

Le client indiquera via un code couleur la disponibilité des nodes passerelles pour chaque crypto-monnaie :

- Noir : tentative de hacking détectée sur les nodes passerelles de cette crypto-monnaie, trading désactivé pour cette crypto-monnaie.
- Rouge : pas de passerelles disponibles pour cette crypto-monnaie => pas d'échanges possibles.
- Orange-Rouge : une seule passerelle disponible pour cette crypto-monnaie => échanges interdits.
- Jaune : deux passerelles disponibles pour cette crypto-monnaie => échange ok, mais résistance au hacking non optimale.
- Vert : à partir de trois passerelles et plus disponibles pour cette crypto-monnaie => échange ok, résistance au hacking optimale.

INDICATION PROVENANT DU NODE STATISTIQUE

Un node statistique analysera en permanence le réseau afin de produire différentes informations à destination des NodeOwners et des traders. Il permettra par exemple :

- De fournir un tableau de bord des statistiques avancées sur les nodes,
- D'évaluer la rémunération attendue en fonction des tokens SSW alloués à un node passerelle,
- De vérifier les volumes d'échanges sur une période par crypto-monnaie,
- etc.

PERFORMANCE DE L'ÉCHANGEUR

Actuellement la blockchain Ethereum est limitée à environ 10/15 transactions par seconde. Notre smart contrat gérant les échanges sur la blockchain Ethereum subira également ces limitations.

Néanmoins, des développements sont en cours pour grandement augmenter le nombre de transactions par seconde que la blockchain Ethereum sera en mesure d'effectuer. On parle d'une augmentation de quelques centaines de milliers voire millions de transactions par seconde, via des technologies comme Plasma, le sharding, le lightning network.

Autant les améliorations de première couche, comme le sharding, augmenteront certainement le nombre d'échanges/seconde réalisables par notre smart contrat, autant cela ne devrait pas être le cas pour les améliorations de seconde couche comme Plasma/Lightning network (hormis la diminution de charge induite sur les opérations de première couche).

Il est prévu d'avoir un smart contrat gérant les échanges sur chaque blockchain supportant les smart contrats, comme EOS et d'autres, afin d'agréger les capacités d'exécution de plusieurs blockchains (en plus d'assurer l'atomicité des échanges via les smart contrats de chaque blockchain). Ainsi l'échangeur n'est pas lié à l'avenir d'une seule blockchain, et par ailleurs, sa capacité à gérer des échanges n'est pas limitée aux capacités d'exécution de smart contrats d'une blockchain, et une blockchain ne limite pas la capacité d'échange sur les autres blockchains plus rapides.

Nous préférons le choix de déployer des smart contrats d'échanges sur plusieurs blockchains, plutôt que de développer notre propre crypto-monnaie ayant une capacité d'exécution de smart contrat suffisante. Autant bâtir sur les solutions existantes et/ou en développement plutôt que de réinventer la roue dans ce domaine.

COMMENT PALLIER LE MANQUE DE LIQUIDITÉS INITIAL ?

À leur lancement, les échangeurs ont forcément des problèmes de liquidités : à leur mise en service, leurs carnets d'ordres sont vides, ce qui n'est pas encourageant pour les premiers traders. Des problèmes de liquidité peuvent aussi exister sur des crypto-monnaies à faible volume d'échange.

Un service d'arbitrage, s'appuyant à la fois sur les carnets d'ordres d'autres sites d'échanges, sur le carnet d'ordre interne de Secure Swap et sur les fonds de réserve en crypto-monnaies propres à notre plateforme, pourra assurer une liquidité de remplacement.

Ce service d'arbitrage agira comme un client (dans le sens où il émettra des ordres dans notre carnet d'ordres) en utilisant les crypto-monnaies appartenant à la société. Ce service sera constitué d'un node p2p spécialisé dans cette tâche. Comme tous les nodes du réseau, il recevra les mises à jour du carnet d'ordres. Ayant connaissance de notre carnet d'ordres, il sera capable d'identifier les contreparties manquantes et de les compléter par des transactions avec d'autres échangeurs.

Une partie des fonds de fonctionnement disponibles de la société seront mobilisés sous forme d'une répartition en diverses crypto-monnaies utilisées par les mécanismes d'arbitrage.

Par exemple, si notre carnet d'ordre contient un ordre d'échange de 1 BTC contre 12 ETH, mais qu'aucun ordre n'échange des ETH contre des BTC au prix ou quantités demandés, mais que sur une plateforme d'échange externe, qui nous sert de liquidité de remplacement, un tel ordre existe, alors nous allons utiliser les ETH de la société réservés pour le service d'arbitrage pour faire l'échange, et racheter les ETH dépensés sur notre plateforme d'échange en effectuant l'échange de 12 ETH contre 1 BTC sur la plateforme d'un autre échangeur. Au final, de notre point de vue, les ETH que nous avions et que l'on a utilisé pour l'échange afin d'assurer la liquidité de cette transaction se retrouvent chez un échangeur externe, et les BTC que nous possédions sur un échangeur externe se retrouve sur nos wallets internes.

Pour rééquilibrer nos différents wallets externes (sur d'autre échangeurs) et internes (locaux à notre échangeur), nous effectuerons un rééquilibrage des montants de coins détenus, une fois par jour (pour limiter les frais), ceci afin de garder une bonne diversité de réserve de crypto-monnaies. Si nécessaire, un rééquilibrage peut être déclenché en cours de journée par le service d'arbitrage s'il venait à manquer de liquidités dans certaines crypto-monnaies pour pouvoir continuer à fonctionner.

Ce système d'arbitrage n'agira qu'en cas de manque de liquidité sur notre carnet d'ordres (donc présence d'ordres sans contreparties), et seulement si l'opération n'est pas perdante pour notre échangeur (à minima neutre). Il peut donc aussi générer des gains même si cela n'est pas sa destination première.

UN ÉCHANGEUR SOUS LICENCE OPEN SOURCE

La plupart des types de nodes de l'échangeur seront distribués en Open source.

Cela signifie, qu'en plus de l'application client servant à tous les traders, tout le monde aura l'opportunité de soutenir le fonctionnement de l'échangeur en faisant fonctionner des nodes connectés à des blockchains.

Les NodeOwners faisant cela et possédant des tokens SSW émis lors de l'ICO, toucheront leur part des frais, prélevés lors des échanges au prorata des tokens qu'ils auront alloués à un node passerelle vers une blockchain, par rapport à la totalité des tokens SSW alloués aux nodes passerelles vers la même blockchain en fonctionnement.

La société Grey Matter Technologies fonctionnera de la même manière et touchera sa part des frais d'échanges au prorata des tokens SSW qu'elle possèdera à l'issue de l'ICO et qu'elle réservera pour chaque node passerelle vers une blockchain qu'elle fera fonctionner.

Nous fournirons également en open source un squelette type de node prévu pour l'échange vers des devises fiat, avec des interfaces pour se connecter aux processeurs de paiement bancaires. Comme cette activité est fortement réglementée, et nécessite à la fois d'être adaptée pour chaque cas (réglementations locales et interfaces vers les processeurs de paiements utilisés) et de démarrer une activité légale pour être exploitée (via une société), le squelette de node que nous fournirons en open source sera donc à adapter à chaque cas particulier.

La société Grey Matter Technologies, exploitera également ce type de nodes pour les régions d'Amérique du sud. Nous prévoyons d'exploiter des nodes de conversion en devises fiat pour les devises suivantes : Peso Chilien, Peso Argentin, Sol Péruvienne et éventuellement d'autres.

Ainsi, progressivement, cet échangeur pourra supporter les conversions vers un grand nombre de devises fiat et régions du monde.

Le node d'arbitrage ne sera pas publié en Open Source. En effet, nous nous en réservons l'utilisation. Bien sûr nous ne pouvons pas empêcher ceux qui le désirent de développer leurs propres solutions d'arbitrage. De toute façon, ce type de service nécessite la disponibilité de fonds en crypto-monnaies de l'ordre de 100k USD au minimum, et de façon plus réaliste, de l'ordre du million de dollars USD, pour fonctionner avec plusieurs échangeurs.

BUG BOUNTY PROGRAMME

Une partie des fonds récoltés lors de l'ICO seront utilisés pour financer des campagnes de Bug Bounty. Les récompenses seront décernées à ceux qui participeront à ces programmes et auront signalé à nos équipes des bugs ou des failles de sécurité encore inconnus.

Une campagne sera lancée à chaque étape de la phase de développement, de façon à ce que la première version de la plateforme mise en exploitation ait déjà été bien analysée.

Des campagnes trimestrielles seront ensuite planifiées pour accompagner la continuité des développements.

L'ICO, LE TOKEN ERC-20 SECURE SWAP (SSW)

POURQUOI UNE ICO ET LA CRÉATION D'UN TOKEN ERC-20 ?

NOUS AVONS BESOIN D'UN FINANCEMENT POUR LA RÉALISATION DE CE PROJET

Pour financer l'embauche de personnels supplémentaires et le paiement des salaires de l'équipe déjà active. C'est le poste de dépense principal.

Nous devons également financer de la publicité peu avant le lancement de la plateforme, afin de la faire connaître.

Nous devons aussi financer un fond de roulement en crypto monnaies, servant au système d'arbitrage.

Et enfin financer les campagnes de Bug Bounty.

Tous les tokens non vendus lors de l'ICO resteront la propriété de la société, afin de collecter la part correspondante des frais d'échanges. Ainsi, plus l'ICO sera un succès et plus les investisseurs supportant le fonctionnement de l'échangeur toucheront une part importante des revenus générés par les échanges, la société possédant alors peu de tokens SSW.

A contrario, moins l'ICO sera souscrite, et plus la société possédera de tokens à l'issue de cette dernière et touchera une part importante des revenus générés. Cela nous assure une répartition des revenus qui nous parait juste, en fonction de ce que la société aura levé comme capital lors de l'ICO, et permettra de récompenser les investisseurs qui nous auront soutenus.

DONNÉES DE L'ICO

Nom du token : Secure Swap

Ticket SSW

Quantité créée : 100 millions de tokens

Prix initial du token : 0,45$ USD

Réservé à l'équipe : 10%

Réservé pour les advisors : 3%

Réservé pour les social managers/animateurs de la campagne ICO : 3%

Réservé pour les partenaires : 4%

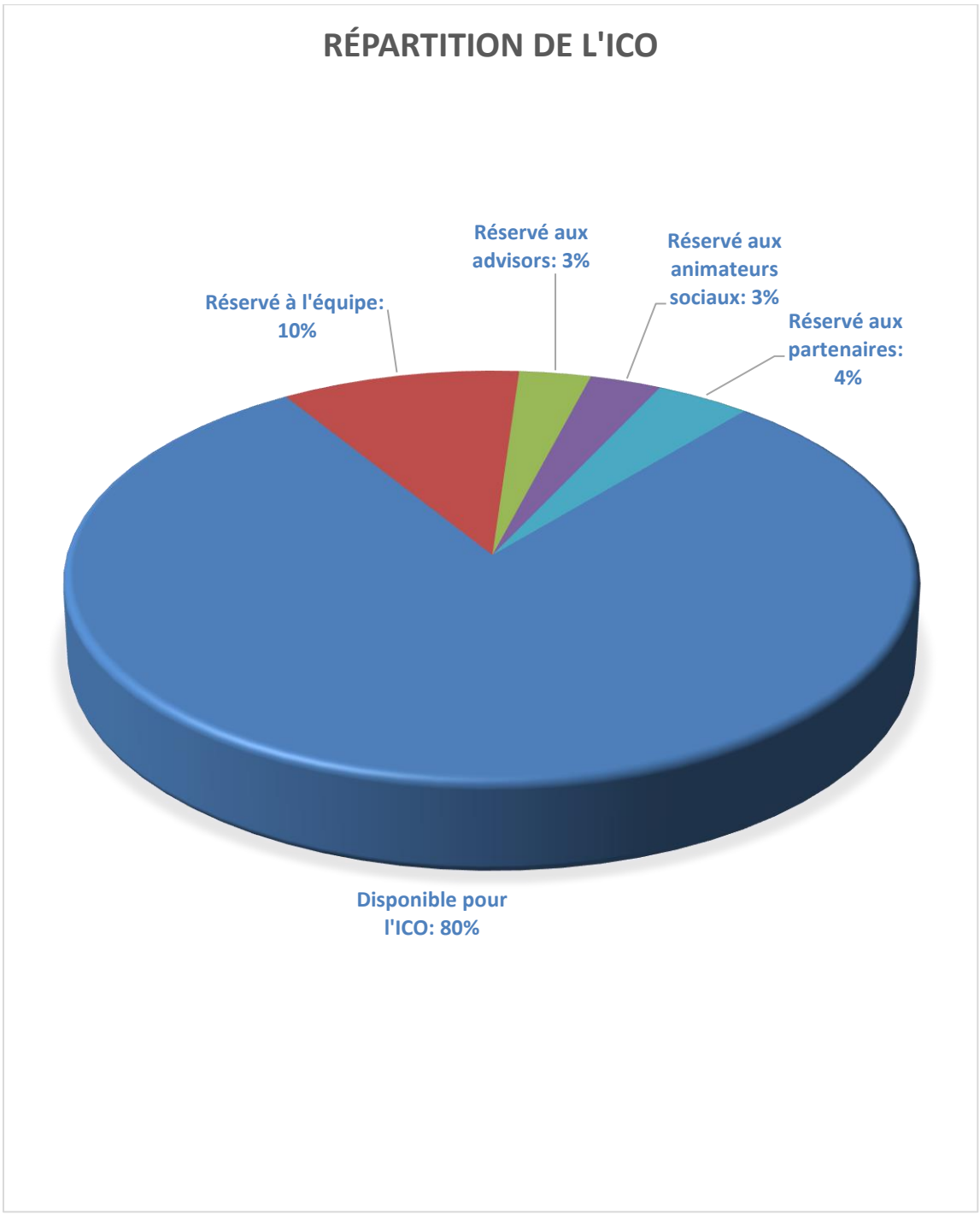
Disponible pour l'ICO : 80%

Soft Cap : 10 millions de tokens

Hard Cap : 80 millions de tokens

Tous les tokens invendus restent la propriété de la société

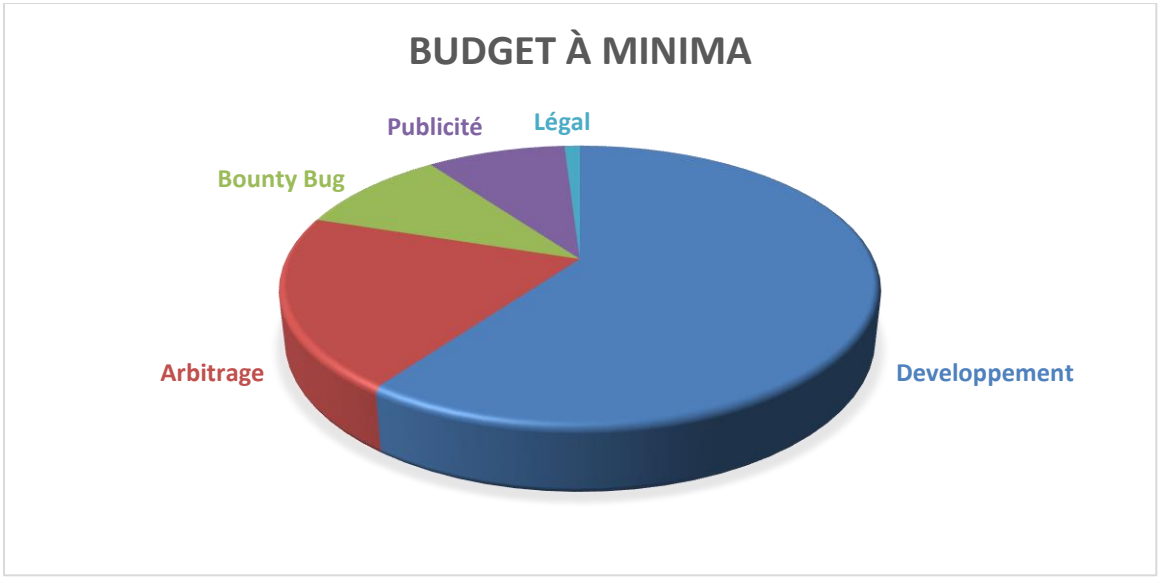
ICO opérée par la société Grey Matter Technologies SA (Société Chilienne)



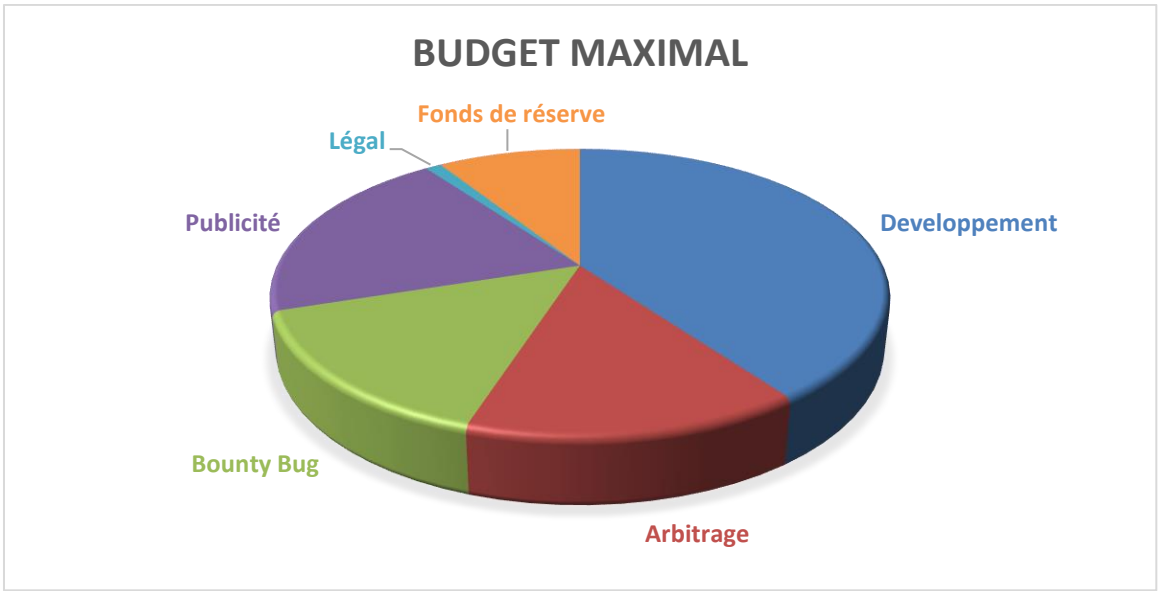
AFFECTATION DES FONDS

Nous allons indiquer ici l'affectation des fonds suivant deux cas extrêmes : Soft Cap atteint et Hard Cap atteint.

SOFT CAP ATTEINT



HARD CAP ATTEINT



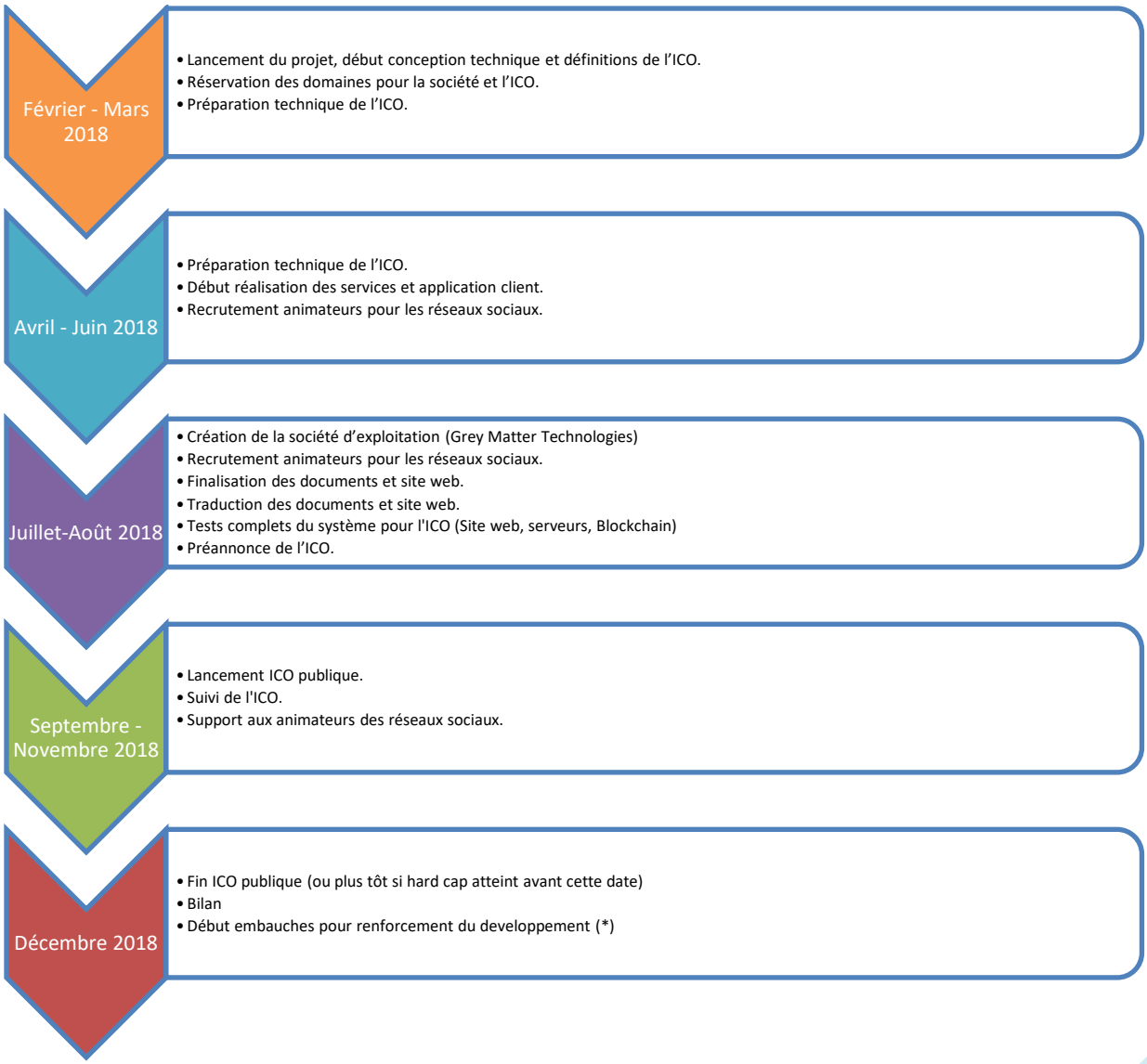
ROADMAP

Cette roadmap est celle prévue si le Hard Cap de l'ICO est atteint. Dans le cas contraire, le projet est conçu sous forme de modules à tiroirs. Le développement de chaque module pourra être repoussé jusqu'à ce que les revenus générés permettent l'autofinancement de la réalisation de ces fonctionnalités.

Sur la Roadmap, les fonctionnalités susceptibles d'être repoussées dans le temps sont signalées par un astérisque (*).

Des améliorations de l'échangeur, ajout de crypto-monnaies (nodes passerelles) etc. continueront d'être effectués au-delà de cette roadmap.

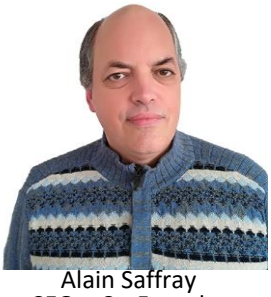
ROADMAP ICO



ROADMAP SECURE SWAP

TEAM

MEMBRES



Alain Saffray
CEO – Co-Founder
Developer engineer

Philippe Aubessard
CTO – Co-founder
Developer engineer

Alicia Laura Poblete
Co-founder
Financial Director

Nadine Miotti
Co-founder
Marketing Director

Renaud Desportes
Business development
Executive

Rafael Romero Carmona
DevOps Engineer

Pierre Pretti
Security Infrastructure
Engineer

Aliaksandr Kharlamou
Blockchain Developer

Victor Chukholskiy
Blockchain Engineer
Smart Contracts Specialist

Marc Rivoal
30 d'expérience
Définition d'architectures logicielles, modélisation de processus, modélisation de données, gestion de projet, conception

Zhan Wei - 詹玮
Social Animator

Kevin Vanstaen
Social Animator
Blockchain enthusiast

Lulia Galea
Social Animator

Henry Morera
Social Animator

CONSEILLERS

Benoît Renard
Conseiller légal

ASPECTS LÉGAUX

IMPLICATIONS LÉGALES AVEC LES TOKENS SSW

Nous ne pouvons garantir les évolutions futures du prix du token SSW, ni son éventuelle présence dans les listings des échangeurs et la possibilité de le revendre. La possession de tokens ne donne aucun droit de participation, contrôle ou décision concernant la société Grey Matter Technologies. Quelle que soit l'issue de l'ICO, le token n'est pas remboursable. L'investisseur ou le spéculateur en assume pleinement le risque d'achat.

De par l'aspect communautaire de Secure Swap, et le fait que les échanges entre crypto-monnaies font partie d'un système distribué, hors du contrôle de la société Grey Matter Technologies, le token Secure Swap est un token utilitaire, servant de preuve d'enjeu pour sécuriser les échanges au sein du système ouvert. Il permet certes de gagner des profits, comme Ethereum avec le mining, mais dans un système distribué sans gouvernance de société, Grey Matter Technologies se contentant de fournir les solutions techniques.

Comme Secure Swap est un échangeur ouvert distribué et communautaire, cela implique l'anonymat des utilisateurs, du moins autant que les crypto-monnaies échangées le permettent, et donc il parait inenvisageable de demander les identités des investisseurs et leurs justificatifs de résidence, afin de vérifier leurs droits de participations à cette ICO.

De ce fait, **il revient aux investisseurs de vérifier, selon leur pays de résidence, la légalité de participer à cette ICO**, et de s'en abstenir en cas d'illégalité ou de doutes.

À noter que la participation à une ICO est actuellement totalement interdite en Chine et en Corée du sud, quelle que soit la nature du token.

Pour les ressortissants Américains, il leur revient de **vérifier auprès de la SEC la légalité de participer à cet ICO**.

Pour les ressortissants Européens, en participant à cette ICO, vous déclarez **ne pas être un consommateur au sens de la Directive Européenne 2011/83/UE du 25 octobre 2011 relative aux droits des consommateurs**.

Pour les ressortissants Russes, il leur revient de vérifier **auprès des autorités régulatrices de la légalité de participer à cet ICO**.

À propos des nodes de conversion des crypto-monnaies vers les devises fiat :

Ce type de node implique une structure légale et une conformité aux lois locales du lieu d'exploitation, notamment **les réglementations (KYC/AML/CFT/FCA) relatives à la fraude, le blanchiment d'argent ou toute activité criminelle**.

L'ENTREPRISE EXPLOITANT L'ECHANGEUR

- L'échangeur, c'est-à-dire les nodes passerelles, le node d'arbitrage et les nodes de conversion vers les devise fiat, supportés par nous-même, sera exploité par la société Grey Matter Technologies: ww.greymattertechs.com
- La société Grey Matter Technologies est une société de juridiction Chilienne. (https://www.conservador.cl/portal/indice_comercio)
- Nous encourageons tout volontaire à soutenir le système en faisant fonctionner ses propres nodes passerelles, et également à exploiter les conversions vers les devises fiat pour son propre compte, ceci évidemment à son entière responsabilité quant au respect des réglementations locales, correspondant aux lieux d'exploitations de ces systèmes.

FAQ

FAQ SECURE SWAP

Q1 : Qu'est-ce qu'est Secure Swap ?

R1 : Secure Swap est un échangeur de crypto-monnaies décentralisé (DEX), avec un aspect communautaire. Il est développé par la société Grey Mater Technologies, basée au Chili, par une équipe fondatrice Française.

Q2 : Quelles crypto-monnaies supporte-t-il ?

R2 : Potentiellement toutes les devises digitales peuvent être échangées. À son lancement le service supportera les crypto-monnaie les plus populaires, les autres seront ajoutées au fur et à mesure.

Q3 : Secure Swap supporte-t-il les conversions avec les devises fiat ?

R3 : Oui, cela est prévu. À son lancement les monnaies sud-américaines seront supportées. L'aspect communautaire de notre plate-forme permettra à d'autres sociétés de s'installer afin de proposer les liens vers les monnaies fiat de leur pays ou région.

Q4 : En quoi consiste l'aspect communautaire de Secure Swap ?

R4 : Le projet est sous licence open source. Son architecture s'appuie sur un réseau de nodes type P2P. Ceux qui y trouvent un intérêt peuvent faire fonctionner ces nodes.

Q5 : Quel intérêt pour une communauté de faire fonctionner ces nodes p2p ?

R5 : Ceux qui feront fonctionner des nodes p2p, et donc supporteront le fonctionnement du service, recevront, au prorata des tokens SSW qu'ils y auront attribués, leur part des frais d'échanges payés par les traders. Ils seront donc rémunérés automatiquement pour cela.

Q6 : Comment attribuer des tokens SSW à un node ?

R6 : Dans la configuration du node, on indique le wallet contenant les tokens SSW que l'on attribue à ce node. Ce même wallet ne peut être attribué qu'à un node à la fois. Seul le wallet est indiqué au node, pour vérification de la quantité de token détenus, les tokens ne changent pas de propriétaire.

Q7 : Comment peut-on se procurer ces tokens SSW ?

R7 : La société Grey Matter Technologies lance cette ICO (Initial Coin Offering) en émettant ces tokens SSW. Par la suite, ces tokens pourront être échangés, notamment sur Secure Swap.

Q8 : Comment est calculée la rémunération ?

R8 : Les nodes sont spécialisés pour chaque blockchain supportée. Ils assurent la connexion du réseau p2p aux blockchains, et sont appelés « nodes passerelles ». Pour chaque blockchain il y a un certain nombre de nodes passerelles, chacun ayant des tokens SSW attribués.

Par exemple, si un node passerelle est lancé sur la blockchain EOS, et qu'un wallet contenant 10 tokens SSW lui est associé, et que l'ensemble des nodes passerelles sur la blockchain EOS ont ensemble 100 tokens SSW associés, alors le propriétaire du node perçoit 10% (10/100) des frais d'échanges, pour tous les échanges faits avec la crypto-monnaie EOS automatiquement sur un wallet EOS préalablement indiqué.

Q9 : Comment la société Grey Matter Technologies va-t-elle s'assurer de bénéfices avec ce système ?

R9 : Comme les NodeOwners, la société fera fonctionner des nodes p2p en y associant les tokens qu'elle possédera à l'issue de l'ICO (ceux qui ne seront pas vendus).

Q10 : Et dans le cas où la société vendrait tous ses tokens pendant l'ICO, se retrouverait-elle sans tokens SSW ?

R10 : La société pourra dégager des bénéfices via les échanges crypto-monnaies vers devises fiat, qui ne sont pas partagés via le système des tokens, mais reviennent entièrement aux opérateurs de tels échanges. Elle pourra aussi éventuellement racheter des tokens SSW, une fois le service fonctionnel.

Q11 : La société Grey Matter Technologies se réserve donc les échanges vers les devises fiat ?

R11 : Non, de par son aspect open-source et communautaire, Secure Swap permet à qui le veut de faire fonctionner des passerelles d'échanges vers des devise fiat. Cela nécessite néanmoins une structure légale, et de se conformer aux réglementations du lieu où ces échanges sont opérés. La société Grey Matter Technologies prévoit de commencer à opérer des échanges vers les devises fiat au Chili, Pérou et Argentine.

Q12 : Comment Secure Swap compte séduire les traders ?

R12 : Secure Swap propose une application client dédiée au trading et s'appuie sur le réseau des nodes passerelles. Cette application profite de notre expérience en développement de logiciels boursiers. Son ergonomie sera bien meilleure que les plateformes actuelles, et propose un ensemble d'outils et d'aide au trading novateurs.

Q13 : Dans un tel système communautaire et open-source, comment assurer la sécurité des échanges ?

R13 : L'ensemble des nodes passerelles vers une crypto-monnaie répondent tous à une sollicitation des applications clientes participantes à un échange. Si les nodes répondent différemment c'est qu'il y a une tentative de hacking. Dans ce cas, un système basé sur une preuve d'enjeux, élimine les nodes non conformes en les déconnectant et en les blacklistant.

Q14 : Comment fonctionne ce système de preuve d'enjeu ?

R14 : Quand des nodes donnent des réponses différentes lors des étapes de validation d'un échange, alors la réponse de référence devient celle majoritaire sur l'ensemble des nodes, chaque node ayant un poids de vote correspondant aux tokens SSW, associés à son fonctionnement. Les nodes répondant différemment sont déconnectés et blacklistés. Ainsi, pour tenter de voler une transaction, il faudrait investir une quantité de tokens SSW représentant plus de la moitié des tokens assignés aux nodes passerelles vers cette crypto-monnaie. Ce qui représente une valeur supérieure au vol d'une transaction, vol qui n'a aucune chance de s'effectuer vu que, dès qu'il y a détection d'anomalies, la transaction est annulée. Si le hacker y mettait des moyens importants pour prendre le contrôle de tous les nodes passerelles, la perte de réputation de l'échangeur engendrerait une baisse rapide de la valeur des tokens SSW, rendant l'opération perdante pour le hacker, surement très couteuse, compte tenu du nombre de tokens qu'il devrait engager pour réaliser cela. Par ailleurs, dès la détection d'anomalies, les échanges avec cette crypto-monnaie sont interrompus, ne laissant au hacker aucune transaction à voler.

Q15 : Si les nodes sont hackés et passent sous contrôle malveillant, comment garantir que ce système de sécurité restera opérationnel ?

R15 : Initialement, les nodes passerelles seront honnêtes, nous le savons car nous lancerons nous-mêmes les premiers nodes au démarrage du service. Puisque l'application client attend la confirmation de tous les nodes passerelles vers une crypto-monnaie pour effectuer un envoi de coins, si les nodes passerelles ne fournissent pas tous la même réponse, c'est qu'il y a un problème. Les clients impliqués dans cet échange annulent alors la transaction, et informent l'ensemble du réseau p2p que les échanges sur la crypto-monnaie sont désactivés, provoquant l'annulation de tous les ordres en attente de tous les clients connectés pour cette crypto-monnaie. Il n'y a alors plus d'échanges, le hacker se retrouve sans transaction à voler.

Q16 : Comment sont relancés les échanges sur une crypto-monnaie, après avoir été désactivés, suite à une anomalie ?

R16 : Il faut un vote unanime, de la majorité qualifiée (60%) des représentants connectés pour cette crypto-monnaie, précédemment désignés, pour que les échanges puissent reprendre. Ces représentants ont alors la responsabilité de s'assurer que les nodes actifs sur la crypto-monnaie sont bien des nodes conformes, avant d'autoriser de nouveau les échanges sur cette crypto-monnaie.

Q17 : Comment ces représentants peuvent-ils s'assurer que les nodes passerelles sont honnêtes avant de voter ?

R17 : En connectant eux-mêmes un node passerelle ou en vérifiant que leurs nodes sont toujours connectés. Il suffit d'un seul node connecté fiable pour que le système détecte une anomalie si de nouveau des nodes répondent différemment. Ce qui provoquerait de nouveau la suspension et l'annulation des échanges sur cette crypto-monnaie.

Donc, si le trading reprend sans incident, c'est que les échanges sont de nouveau fiables et que les nodes malicieux ont été purgés. Si des nodes malicieux sont dormants et fonctionnent correctement en attendant d'entrer en action, quand ils le feront, ils seront détectés par leurs réponses différentes. Ainsi toute tentative de corruption de node est détectée et rend impossible le vol de transaction.

Q18 : Comment sont désignés ces représentants ?

Q18 : Ces représentants sont volontaires et ne sont qualifiés que s'ils possèdent 100 fois le montant d'un échange moyen, en valeur équivalente de tokens SSW. Le volontaire en fait alors la demande via l'interface de son node, et s'il est qualifié, l'ensemble des nodes du réseau mémorise son statut de « super node passerelle ». Le « super node passerelle » se voit gratifié d'un bonus de 50% sur sa rémunération, par rapport à ce qu'il toucherait normalement en vertu de ses tokens alloués.

Q19 : Comment empêcher des gens mal intentionnés de connecter en permanence des nodes défectueux, afin de paralyser le service ?

R19 : Les nodes déviants étant blacklistés, en plus d'être déconnectés, ces personnes mal intentionnées vont vite être à cours d'adresses IP permettant de connecter de tels nodes. Par ailleurs, une telle action de sabotage informatique étant illégale, sa répétition va augmenter la probabilité d'en découvrir leurs auteurs, et la société Grey Matter Technologies attaquera les responsables en justice afin de demander réparation.

Q20 : Quelles mesures sont prises pour lutter contre les hackers ?

R20 : Outre les protocoles décrits dans les réponses précédentes, et outre le fait que tout le projet Secure Swap est disponible à tous en Open source, nous lançons des campagnes de Bug Bounty tous les 3 mois avec récompense à la clé pour ceux qui trouveraient une faille dans le système.