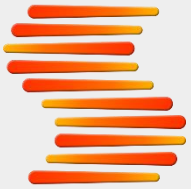


SECURE SWAP
LIVRE BLANC

Grey Matter Technologies

www.secure-swap.com

SECURE SWAP
LIVRE BLANC

MENTIONS LEGALES

L'objectif du présent Livre Blanc est de présenter le projet Secure Swap aux détenteurs potentiels de jetons dans le cadre du projet de lancement de cette ICO. Les informations présentées ci-dessous peuvent ne pas être exhaustives et n'impliquent aucun élément d'une relation contractuelle. Son seul but est de fournir des informations pertinentes et raisonnables aux détenteurs potentiels de jetons afin qu'ils puissent déterminer s'ils doivent entreprendre une analyse approfondie de l'entreprise dans le but d'acquérir des jetons SSW.

Aucune disposition du présent Livre Blanc n'est réputée constituer un prospectus de quelque nature que ce soit ou une sollicitation d'investissement, ni ne se rapporte de quelque manière que ce soit à une offre ou à la sollicitation d'une offre d'achat de titres dans un territoire quelconque. Le présent document n'est pas rédigé conformément aux lois ou règlements d'un territoire quelconque qui visent à protéger les investisseurs et n'est pas assujetti à ceux-ci.

Certaines déclarations, estimations et informations financières contenues dans le présent Livre Blanc constituent des déclarations ou informations prospectives. Ces déclarations ou informations prospectives comportent des risques et incertitudes connus et inconnus qui peuvent faire en sorte que les événements ou résultats réels diffèrent sensiblement des estimations ou des résultats implicites ou exprimés dans ces déclarations prospectives.

Les simulations évoquées dans le présent Livre Blanc ne peuvent être considérées comme une promesse de profit et/ou comme une prévision garantie de la croissance du jeton SSW. Les calculs fournis sont uniquement basés sur des lois mathématiques fondamentales.

Ce livre Blanc en Français est la principale source officielle d'information sur le jeton SSW. Les informations contenues dans le présent document peuvent être traduites dans d'autres langues ou peuvent être utilisées dans le cadre de communications écrites ou verbales, avec des membres actuels ou potentiels de la communauté, des partenaires, etc. Au cours d'une telle traduction ou d'une telle communication, et malgré nos efforts de relecture, une partie de l'information contenue dans ce document peut être perdue, corrompue ou déformée. L'exactitude de ces communications complémentaires ne peut être garantie. En cas de conflit ou d'incohérence entre ces traductions et communications et le présent Livre Blanc officiel en français, les dispositions du document original en langue française prévaudront.

TOUTE PERSONNE ACHETANT DES JETONS SSW RECONNAÎT ET DÉCLARE EXPRESSEMENT QU'ELLE A SOIGNEUSEMENT EXAMINÉ CE LIVRE BLANC ET A BIEN COMPRIS LES RISQUES, LES COÛTS ET LES AVANTAGES ASSOCIÉS A L'ACHAT DE JETONS SSW.

SOMMAIRE

TABLE DES MATIÈRES

PRÉSENTATION DE SECURE SWAP

INTRODUCTION

« Un échangeur de plus ? Le marché en est saturé ! »

Non, Secure Swap n'est pas qu'un échangeur décentralisé (DEX) de plus. Ses caractéristiques le rendent unique ! Il réunit les avantages des échangeurs centralisés et décentralisés : liquidités, rapidité d'exécution, absence de tiers de confiance, résistant au piratage, résistant aux interdictions et régulations hostiles aux crypto-monnaies.

La plate-forme Secure Swap est open source et sans serveur central. Elle est opérée par la communauté, et ne nécessite donc pas de société opérante pour fonctionner.

Son architecture est fortement modulaire, permettant d'ajouter des services (support de crypto-monnaies, support d'échanges fiat et intégration de moyens de paiement (cash-in/cash-out), support de fournisseur de liquidités). Les développeurs et les entrepreneurs peuvent ainsi rejoindre et étendre la communauté Secure Swap.

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

Son architecture rend le cœur du système à l'abri de régulations et d'interdictions brutales des crypto-monnaies. Suivant leur lieu de résidence, ces régulations peuvent représenter un risque pour ceux qui possèdent des crypto-monnaies. Secure Swap offre une porte de sortie toujours disponible.

Pour les devises digitales qui le permettent, Secure Swap respecte totalement l'anonymat lorsque l'on échange des crypto-monnaies entre elles.

Néanmoins, grâce à sa modularité et à la nette séparation des différents systèmes d'échange, Secure Swap permet aussi de respecter totalement les règlementations locales en vigueur dès qu'il s'agit d'échanger des crypto-monnaies avec des devises fiat.

L'ouverture de Secure Swap aux échanges crypto-fiat 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. Secure Swap est open-source et fournit des modèles de nodes prêts à être adaptés aux réglementations locales.

Son protocole de fonctionnement intègre des systèmes de détection d'anomalies. Chaque anomalie entraine la déconnexion du réseau de la partie défaillante et l'utilisation, si nécessaire, de la garantie en jetons SSW pour terminer un échange en cours. Ces anomalies peuvent être causées soit par une tentative de piratage ou soit par le dysfonctionnement de certains nodes.

Son application client de trading, Secure Trade, offre un niveau de confort et d'ergonomie comparables aux meilleurs logiciels de trading sur les marchés boursiers classiques (ordres sur graphique, « money management », aide au « scalping », module de trading automatique programmable…).

Notre objectif est de construire un échangeur de nouvelle génération qui, pour la première fois, réunira toutes ces caractéristiques. Et c'est seulement en les réunissant toutes, qu'un DEX peut prétendre détrôner les échangeurs centralisés.

ÉTAT DU MARCHÉ

Principales caractéristiques des échangeurs centralisés et décentralisés :

ÉCHANGEURS CENTRALISÉS

Avantages :

- Une bonne liquidité, voire très bonne pour les plus gros échangeurs. Cela assure d'y trouver une grande profondeur de marché et un « slippage[1] » des prix limités.
- Une bonne rapidité d'exécution des ordres, grâce à un carnet d'ordre centralisé ainsi qu'à la liquidité disponible.
- Un large choix de crypto-monnaies échangeables.
- Pour certains la possibilité de trader sur marge.

Inconvénients :

- Transfert de la propriété des actifs digitaux à ces échangeurs, qui servent de tiers de confiance.
- Cette centralisation des actifs est très attractive pour les pirates. Cela rend le piratage très dommageable, tant pour la société opérant l'échangeur que pour ses clients.
- Risque de fermeture soudaine, rendant inaccessibles les actifs qui y sont déposés. Ces fermetures peuvent être causées soit par une faillite de l'opérateur de l'échangeur, ou soit par une régulation étatique hostile aux crypto-monnaies.
- Fréquente indisponibilité des services lors des périodes de panique de marché.
- Le retrait des avoirs implique un double coût : les frais habituels de réseau, ainsi que les frais ajoutés par l'échangeur pour le retrait.

ÉCHANGEURS DÉCENTRALISÉS

Avantages :

- Pas de tiers de confiance.
- Pas de centralisation d'actifs, donc peu attractif pour les pirates et également plus difficile à pirater.
- Certains sont résistants à la faillite de leurs opérateurs et aux risques de régulation, mais ils sont peu nombreux[2].

Inconvénients :

- Liquidité insuffisante pour assurer la présence de contrepartie. Cela provoque également un fort risque de « slippage » sur les prix, ainsi qu'une lenteur d'exécution des ordres.
- La lenteur d'exécution des ordres est directement causée par leur modèle d'architecture distribuée et par le fonctionnement de leurs carnets d'ordres et système de « matching ».
- La plupart présentent un choix de crypto-monnaies échangeables limité. Beaucoup se limitent à n'effectuer des échanges qu'au sein du réseau Ethereum (Ether et Jetons).
- Les carnets d'ordres et le « matching » des ordres exécutés par des « smart contracts » (On-Chain) coûtent des frais de réseau (gaz sur Ethereum) même si les ordres ne sont pas exécutés. Pire, l'annulation et la modification d'ordres impliquent également des frais.

Ce qui découle de cette comparaison :

On constate que les DEXs ne sont pas sans inconvénients face aux échangeurs centralisés, ce qui limite leur intérêt.

L'insuffisance de liquidité est la raison principale de la non-adoption massive des DEXs, les utilisateurs jugeant la profondeur de marché des échangeurs centralisés préférable aux avantages des DEXs.

La lenteur d'exécution des ordres est également une des raisons de cette situation, mais c'est une cause moins importante que l'insuffisance de liquidité.

L'absence de trading sur marge est aussi une raison de la désaffection des DEXs, du moins pour les traders qui pratiquent ce type de trading sur les crypto-monnaies.

Aucun DEX actuel ne présente ces deux caractéristiques réunies (liquidité et rapidité). Ceux qui le font et prétendent être des DEXs, font reposer leurs liquidités sur le fait que la société opérante est la contrepartie intermédiaire des échanges. La société échange les crypto-monnaies contre ses jetons, à des taux décidés par elle-même. C'est la société opérante qui choisit en général le taux de change de ses jetons contre toutes les crypto-monnaies disponibles, parfois via une formule ad hoc, parfois en simulant même un mécanisme de « slippage » des prix, totalement à leur avantage, ce qui induit des frais cachés.

Ces jetons qui servent de contreparties intermédiaires constituent alors également une concentration d'actifs. Ces échangeurs supportent donc le même risque de piratage que les échangeurs centralisés (exemple : Bancor, qui a d'ailleurs été piraté, avec comme résultat le vol de 1/3 de ses jetons-contreparties).

---

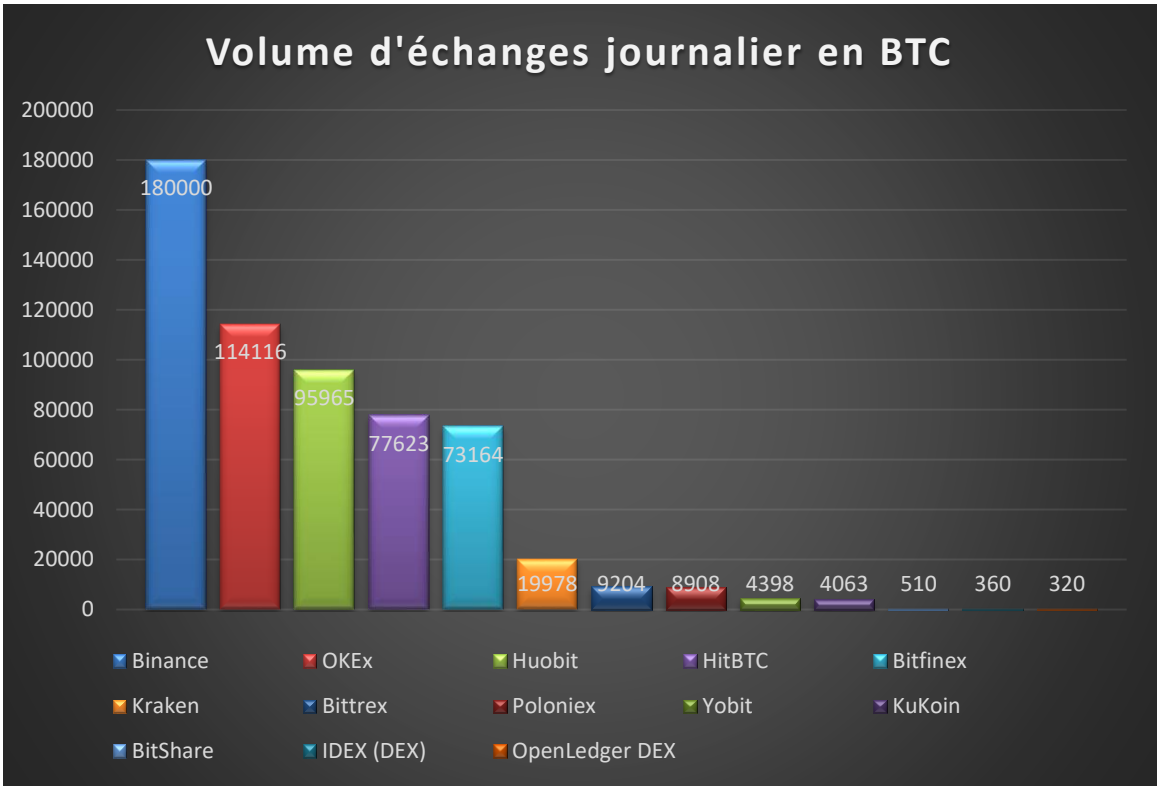
[1] Le « slippage » est le décalage de prix entre le cours auquel vous souhaitez acheter ou vendre, et le cours auquel votre ordre est exécuté sur une plateforme de trading.

[2] Pour qu'un DEX soit résistant à la faillite de son opérateur et aux risques d'interdiction, il faut que son architecture soit décentralisée, autonome ou avec une gouvernance décentralisée. Mais, et c'est un point souvent oublié, il faut que son système de passage d'ordres soit lui aussi résistant. Ce qui n'est absolument pas le cas de tous les DEXs utilisant un site web pour leur passage d'ordres. Ces sites peuvent être interdits ou fermés suite à un changement de régulation ou une faillite de la société opérant le site web, voir être inaccessibles à cause d'une simple attaque DDOS. Seuls les DEXs décentralisés, autonomes et avec une application client servant au passage d'ordres répondent à ce critère. Ils ne sont pas nombreux (Altcoin.IO, BarterDex, Bisq, Stellar Dex pour les principaux), et ils sont aussi sujets aux problèmes de liquidités.

COMPARAISON DES PARTS DE MARCHÉ

Malgré leurs avantages respectifs, une étude des parts de marché montre que les DEXs sont largement en retrait, en volumes échangés, en comparaison des échangeurs centralisés.

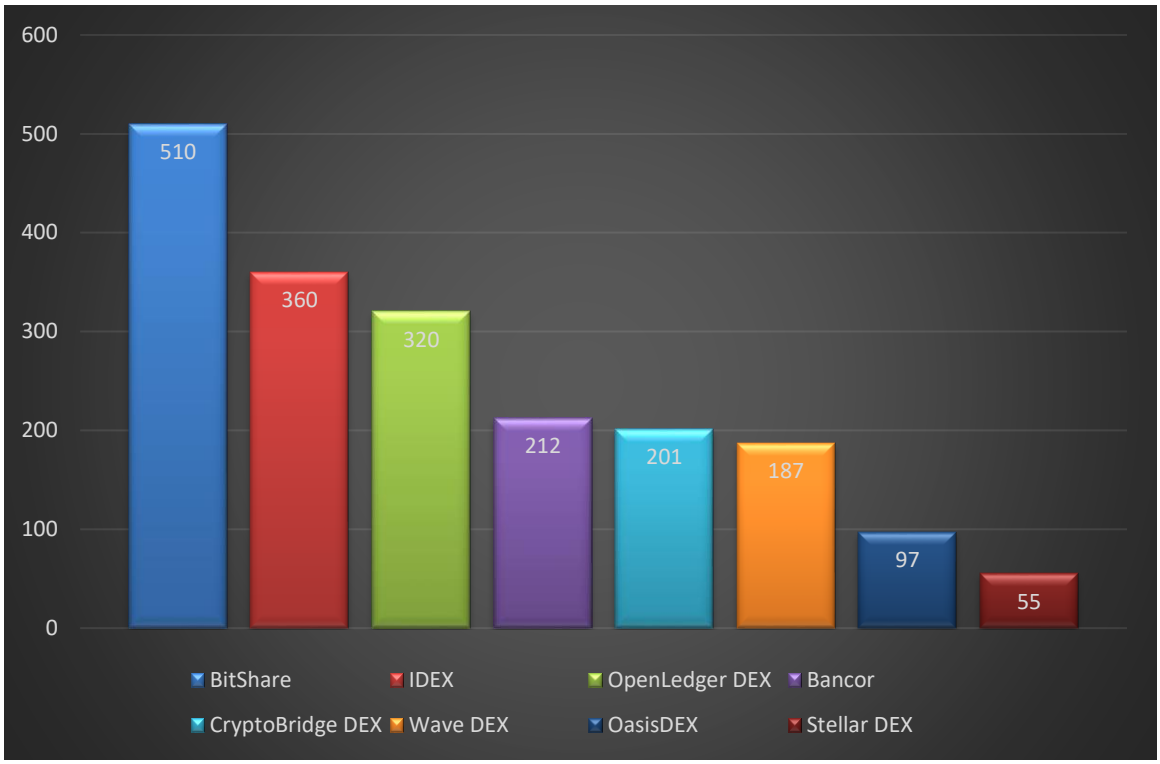
Volume d'échanges journalier comparé des échangeurs centralisés et décentralisés :



Ce graphique montre les volumes d'échange pour quelques échangeurs centralisés, et pour les trois échangeurs décentralisés qui ont le plus de volume.

Les volumes des DEXs BitShare, IDEX et de OpenLedger sont tellement faibles en comparaison des échangeurs centralisés qu'ils ne sont même pas visibles sur le graphique…

Volume d'échange comparé des échangeurs décentralisés uniquement :



Conclusion :

Cette comparaison entre échangeurs centralisés et décentralisés est sans appel !

Quelle est la principale différence, responsable de cet état de fait, et partagée par tous les DEXs ?

Ils sont défaillants quant à la liquidité dont ils disposent. Quels que soient leurs avantages, ce manque de liquidité les condamne à jouer un rôle anecdotique parmi les échangeurs.

Certains essayent de pallier ce problème de liquidité, comme Bancor et d'autres, mais leurs solutions soit n'apportent pas réellement de liquidité, soit transforment le DEX en un «market maker[3]» qui impose ses taux de change, les utilisateurs perdent alors le contrôle du prix de leurs transactions.

[3] Intermédiaire financier qui fait les prix, qui propose un cours acheteur et un cours vendeur sur un actif financier.

EXEMPLES DE SOLUTIONS AU MANQUE DE LIQUIDITÉ PROPOSÉES PAR DIFFÉRENTS DEX

Altcoin IO :

Propose un système de partage de liquidités entre DEXs via une API. Ce système peut devenir une très bonne solution à long terme, quand les DEXs auront de la liquidité à partager…

Pour Atlcoin IO, cette solution n'apporte pas de liquidité de façon immédiate.

Bancor :

« Market Maker » utilisant ses jetons comme contrepartie de tous les échanges. Il propose ainsi une liquidité toujours disponible, en fixant les taux de change, et en ajoutant même un « slippage » de prix artificiel lors des échanges en fonction du volume échangé. Le problème de liquidité est solutionné, mais à quel prix : les utilisateurs n'ont plus le contrôle du prix d'échange de leurs transactions. De plus le système de fixation des taux de change est opaque et peut vite devenir suspect.

BarterDex (Komodo platform) :

Cette plateforme emploie un système de création artificiel de liquidité assez fumeux : la liquidité du carnet d'ordres est multipliée par le fait que les crypto-monnaies impliquées dans un ordre en attente d'être servi restent disponibles pour d'autres ordres. Cela crée une profondeur du carnet d'ordre fictive qui n'existe pas concrètement. Dès qu'un ordre est servi, tous les ordres basés sur ces mêmes crypto-monnaies, qui ne sont plus disponibles en quantité suffisante, sont alors annulés. Ce qui annule également cette liquidité artificiellement créée…

Cela n'apporte rien d'autre pour les utilisateurs que de les induire en erreur quant à la liquidité réelle disponible.

Ces trois exemples couvrent la plupart des solutions mises en œuvre pour essayer de solutionner le problème de liquidité, la plus couramment utilisée étant la solution de Bancor : les jetons du projet servent de contrepartie, avec ou sans blockchain spécifique, avec les implications qui en découlent.

SOLUTIONS APPORTÉES PAR SECURE SWAP

La solution de Altcoin.IO deviendra intéressante quand les DEXs auront pris le leadership face aux échangeurs centralisés, partageant ainsi leurs liquidités.

https://blog.altcoin.io/why-decentralized-exchanges-need-a-liquidity-strategy-51dfd75876eb

Secure Swap compte mettre en œuvre l'API de Altcoin.IO pour partager sa liquidité, dans l'idée que cela sera bénéfique aux deux échangeurs, ainsi qu'à ceux qui nous rejoindront plus tard.

En attendant, Secure Swap doit avoir un moyen d'obtenir de la liquidité dès sa mise en service. C'est pour cela que nous allons chercher la liquidité là où elle est, chez les échangeurs centralisés, en exploitant leurs APIs. Notre système d'arbitrage est dédié à cette tâche. Ainsi nous pourrons exploiter la liquidité de plusieurs échangeurs centralisés, proposant ainsi une liquidité potentiellement supérieure à chacun d'eux.

Pourquoi cette idée simple n'est pas utilisée par les autres DEXs ? C'est qu'elle a un revers : elle nécessite de bloquer des fonds importants en crypto-monnaies pour chacun des échangeurs centralisés dont on exploite la liquidité. C'est à cette fin qu'une partie importante des fonds levés lors de l'ICO sera consacrée aux nodes d'arbitrages.

La rapidité de « matching » des ordres est obtenue simplement : tous les nodes du réseau (y compris Secure Trade, l'application client, qui est également un node), partagent les mises à jour du carnet d'ordres.

Quand un trader ajoute/supprime/modifie un ordre via Secure Trade, cette modification est transmise à tous les nodes de proche en proche. Comme il s'agit d'une transmission de différence, cela représente très peu de données à propager, ce qui fait que globalement, tous les nodes sont à jour en permanence (un peu comme les nodes validant des blocks sur les blockchains, sauf qu'ici le volume de données transmis est négligeable).

Chaque node Secure Trade, effectue le « matching » de ses propres ordres versus le carnet d'ordres complet, donc on obtient un « matching » des ordres très rapide (on peut le considérer comme instantané), car chaque node Secure Trade n'effectue le « matching » que d'une petite partie des ordres (les quelques ordres de l'utilisateur) versus le carnet d'ordres complet. À noter que ces opérations sont totalement sans frais.

Concernant l'éventail des crypto-monnaies disponibles, Secure Swap n'est pas limité à l'écosystème Ethereum, nous pouvons donc en proposer un grand nombre. Son aspect communautaire ainsi que la mise à disposition de modèles de node passerelle (vers crypto-monnaies, vers devise fiat, vers node d'arbitrage) permet à la communauté Secure Swap d'ajouter le support des crypto-monnaies (et devises fiat) de son choix.

Secure Swap permet aussi le trading sur marge, via des nodes dédiés à cette tâche.

En résumé, 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, tels 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'arbitrage et des nodes de trading sur marge.

De plus amples détails sont présentés dans la section « Architecture et fonctionnement de l'Échangeur ».

SYNTHÈSE DES POINTS FORTS DE SECURE SWAP

LIQUIDITÉ

- Comme on vient de le voir, Secure Swap assure une liquidité très importante, apportée par celle des échangeurs centralisés, ceci grâce à notre système d'arbitrage.
- Dans le futur, la liquidité sera aussi soutenue par le partage des carnets d'ordres entre échangeurs DEXs.

RAPIDITÉ

- Chaque application client effectue le « matching » de ses ordres versus le carnet d'ordres complet. Ceci, allié à la liquidité disponible, nous assure une rapidité d'exécution comparable aux échangeurs centralisés.
- Son architecture et son fonctionnement font que Secure Swap n'est pas tributaire de la vitesse d'exécution des « smart contracts » sur les différentes blockchains (voir explications dans « Architecture et fonctionnement de l'Échangeur »). Ainsi, Secure Swap est aussi rapide qu'un échangeur centralisé en charge nominale, et sans doute plus rapide lors de fortes charges. Secure Swap est certainement le plus rapide des DEXs existants.

SECURITÉ

- Système sécurisé par conception, avec détection des tentatives de piratage ou de dysfonctionnements, et déconnexion 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, Secure Swap n'a pas de tiers de confiance, et est une DAO (« Decentralized Autonomous Organisation » : une organisation décentralisée autonome). Ainsi il n'existe aucun moyen pour les régulateurs d'en empêcher son utilisation.
- Pas de concentration de crypto-monnaies. Ce qui est une cible de choix pour les pirates dans les échangeurs centralisés, mais également dans les échangeurs dits décentralisés et dont le fonctionnement implique la concentration de crypto-monnaies ou de jetons.
- Le trader a la garantie de recevoir sa contrepartie suite à un échange, même si une partie du système est défaillante ou piratée.
- Un système ouvert et open-source 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 ÉCHANGEUR CONTRÔLÉ ET OPÉRÉ PAR UNE COMMUNAUTÉ

- Son caractère 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 ÉCHANGEUR EXTENSIBLE

- De par sa nature open source et modulaire, les utilisateurs souhaitant avoir un rôle actif peuvent ajouter à l'échangeur le support de nouvelles crypto-monnaies ainsi que des échanges de crypto-monnaies vers devises fiat ou encore le support de moyens de paiement de leur choix.

UNE SOURCE DE REVENUS POUR CEUX QUI SUPPORTENT SON FONCTIONNEMENT

- Ceux qui supportent le fonctionnement du service (NodeOwners), en faisant fonctionner des parties du système (nodes passerelles vers des crypto-monnaies spécifiques), sont récompensés en recevant une partie des frais payés par les traders sur les échanges.
- Ceux qui opèrent des nodes de trading sur marge profitent aussi de cette source de revenus.
- De même les nodes d'arbitrage peuvent également être source de revenu, par l'exploitation des différences de cotations entre échangeurs.
- Grâce à son caractère open source, les entrepreneurs pourront développer une activité commerciale d'échange de crypto-monnaies vers devises fiat et même proposer des moyens de payements 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 depuis le monde entier pour les échanges de crypto-monnaies, le support de nouvelles devises fiat ainsi que de nouveaux moyens de payements ajoutés par la communauté, étendront progressivement le service au monde entier pour les devises fiat également.

UNE ERGONOMIE ET DES OUTILS DE TRADING AVANCÉS

- Son application client, Secure Trade, propose des outils de trading avancés, qui sont communs dans le monde du trading traditionnel (marchés boursiers, marchés des futurs…).
- Les principaux outils sont : le passage d'ordres sur le graphique, l'aide au « money management », l'aide au « scalping », un module de trading automatique programmable, sans parler de la panoplie d'indicateurs disponibles et autres modes de représentation graphiques.
- En outre, Secure Swap propose le trading sur marge, ce qui est actuellement quasi unique pour un DEX.

UNE PLATEFORME AVEC DES COÛTS AVANTAGEUX POUR L'UTILISATEUR

- Secure Swap ne fait intervenir les « smart contracts » qu'en cas d'anomalies.
- Un échange se déroulant sans dysfonctionnement ni piratage ne fait pas intervenir les « smart contracts ».

- Il en résulte que les passages d'ordres, modifications d'ordres, annulations d'ordres n'engendrent aucun coût pour l'utilisateur, contrairement à la plupart des DEXs.
- De même l'exécution d'un ordre n'engendre aucun coût lié à une opération avec un « smart contract ».
- La plateforme ne prend pas non plus de frais de retrait, puisqu'elle ne possède pas les wallets. Il en découle qu'avec ses frais uniques de 0.15% sur l'exécution d'un ordre, pouvant être réduits sur critères de volume, elle sera aussi compétitive que les échangeurs centralisés.

En conclusion, Secure Swap est un écosystème apportant une réponse efficace aux problèmes des échangeurs centralisés et décentralisés. A l'instar des projets Omise GO ou Stellar Lumens, il propose aussi l'échange de crypto-monnaies vers les devises fiat ainsi que l'intégration simple de moyens de paiements via un SDK (kit de développement) permettant les paiements en devises fiat et en crypto-monnaies.

Contrairement aux projets proposant ces solutions globales, il ne dépend pas de la réussite de développements en cours comme Plasma, le Lightning Network, le Sharding, ou l'Atomic Swap pour proposer des fonctionnalités équivalentes.

ARCHITECTURE ET FONCTIONNEMENT DE L'ÉCHANGEUR

Pour répondre aux problèmes identifiés, Secure Swap applique des solutions procurant à la fois les avantages des échanges centralisés et décentralisés, sans aucun de leurs inconvénients respectifs.

Secure Swap dispose d'une **sécurité renforcée « by design ».**

L'architecture des nodes assure une capacité de montée en charge et de redondance, garantissant la fiabilité et la disponibilité du service.

Secure Swap ne souffre d'aucun des inconvénients des échangeurs centralisés ou décentralisés.

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'échange sont redistribués en totalité à ceux qui font fonctionner ce type de nodes (NodeOwners), au prorata des jetons SSW qu'ils détiennent. Il constitue donc pour tous ceux qui le désirent, et investissent dans le jeton SSW, une source de revenu majeure.

L'architecture réseau distribuée est basée sur un cœur applicatif en JavaScript s'appuyant sur Node.JS. Il constitue la base commune de communication Peer to Peer (p2p[4]), qui servira aux différents modules de l'écosystème : client de trading, nodes passerelles vers les blockchains, nodes d'arbitrage chargés d'assurer la liquidité de l'échangeur, nodes d'échanges crypto/fiat.

Secure Trade et les nodes communiquent entre eux via la technologie p2p, constituant ainsi un service décentralisé.

Seule Secure Trade a connaissance des clefs privées des wallets de l'utilisateur. Elle est ainsi à même de signer les transactions à destination des blockchains (signature « offline »). De ce fait, personne ne peut signer les transactions à la place de Secure Trade. Les moyens de vol des avoirs des traders utilisés sur les plateformes centralisées sont ici caducs. Le trader reste propriétaire de ses crypto-monnaies, contrairement aux plateformes d'échanges centralisées sur lesquelles le trader transmet ses crypto-monnaies qui y sont entreposées, et qui deviennent ainsi les réels propriétaires des clefs privées et des crypto-monnaies entreposées.

Dès que l'utilisateur se déconnecte du service d'échange, 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.

[4] Peer to Peer : Le pair à pair ou pair-à-pair est un modèle de réseau informatique proche du modèle client-serveur mais où chaque client est aussi un serveur. Le pair à pair peut être centralisé ou décentralisé. Il peut servir au partage de fichiers en pair à pair, au calcul distribué ou à la communication.

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

L'application client Secure Trade permet d'offrir un confort d'utilisation et une ergonomie comparable aux meilleurs logiciels de trading existants (marchés boursiers, contrats futurs, Forex...). Secure Trade 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 de pentes, ordres sur indicateurs, un module d'aide au « money management », ainsi qu'un module programmable de trading automatique et enfin le trading sur marge.

Chaque 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 Secure Trade est également un node, elle reçoit donc aussi la totalité des ordres émis sur le réseau p2p. Cette propagation des mises à jour du carnet d'ordres ne transmet que les différences, les modifications, les suppressions et ajouts d'ordres. Elle est très rapide et paraît instantanée du point de vue du client.

Chaque application client effectue le « matching » de ses propres ordres, contre le carnet d'ordres complet, afin de trouver des contreparties aux ordres que le trader a émis.

Quand un « matching » (contrepartie) est trouvé, Secure Trade en informe les nodes auxquels il est connecté. Les nodes vont valider le « matching », ce qui va provoquer le déroulement du processus d'échange (voir explication détaillée plus bas).

Pour la sécurité des échanges, un système de garantie décrit au chapitre « Nodes Passerelles et NodeOwners », ainsi qu'un contrôle des opérations par l'ensemble des nodes, permettent de s'assurer du fonctionnement conforme des différents nodes du réseau, ainsi que de la sécurité des échanges dans un environnement « trustless[5] ».

Dernier point important, Secure Swap est entièrement basé sur des technologies existantes, fonctionnelles et éprouvées. Le projet n'est donc pas exposé au risque d'un éventuel échec des technologies en cours de développement telles que le Plasma par exemple. Cela réduit grandement le risque d'échec du projet Secure Swap en raison de technologies tierces qui pourraient échouer.

[5] Les parties en relation n'ont pas besoin de se faire confiance entre elles ni de requérir un tiers de confiance puisque toutes les informations traitées sur le réseau sont vérifiées de manière indépendante.

SYSTÈME D'ARBITRAGE ASSURANT LA DISPONIBILIÉ DE LIQUIDITÉ

Le système d'arbitrage est constitué d'un ensemble de nodes d'arbitrage. Comme il s'agit de nodes, ils disposent du carnet d'ordres de Secure Swap à jour, comme tous les autres nodes.

Chaque node d'arbitrage est spécialisé pour utiliser l'API de l'échangeur centralisé pour lequel il est destiné.

Ces spécialisations concernent la mise en œuvre de l'API spécifique de l'échangeur, et les règles d'utilisation spécifiques de l'échangeur (comme par exemple le délai minimum entre deux appels de l'API…).

PRÉREQUIS POUR CONNECTER UN NODE D'ARBITRAGE AU RÉSEAU

Pour pouvoir opérer ce type de node, il faut avoir un capital réparti dans toutes les crypto-monnaies dont le node d'arbitrage va assurer un apport de liquidité à Secure Swap.

Ce capital doit être réparti de façon égale entre des wallets gérés par le node d'arbitrage sur le réseau Secure Swap, et entre les wallets de l'échangeur centralisé, dont on veut exploiter la liquidité.

Il faut également une machine fiable, sécurisée, disposant d'une connexion Internet stable.

Il faut aussi se procurer l'application de node d'arbitrage adaptée à l'échangeur que l'on veut exploiter, ou éventuellement avoir développé sa propre spécialisation à partir du modèle de node fourni sous licence Open-Source.

FONCTIONNEMENT D'UN NODE D'ARBITRAGE

Le node d'arbitrage récupère et maintient à jour le carnet d'ordres de l'échangeur centralisé qu'il exploite, pour toutes les crypto-devises qu'il gère, et recherche des contreparties possibles entre les deux carnets d'ordres.

Dès qu'un « matching » entre les deux carnets d'ordres est trouvé, le node d'arbitrage réserve l'ordre concerné du carnet d'ordres de Secure Swap. Une fois la réservation confirmée, il effectue une transaction inverse sur l'échangeur tiers.

Exemple : si dans le carnet d'ordres de Secure Swap existe un ordre échangeant 1 BTC contre 30 ETH, et que sur le carnet d'ordres de l'échangeur tiers existe un ordre échangeant 32 ETH contre 1 BTC, alors le node d'arbitrage va émettre un ordre d'échange de 1 BTC contre 32 ETH sur l'échangeur tiers.

Pour cette transaction, Secure Swap utilise les réserves en crypto-monnaies détenues sur les wallets de l'échangeur tiers, qui appartiennent à l'opérateur du node d'arbitrage.

Une fois cette opération effectuée sur l'échangeur tiers, le node d'arbitrage va envoyer un ordre d'échange de 30 ETH contre 1 BTC sur le carnet d'ordres de Secure Swap, ce qui va provoquer l'échange sur Secure Swap avec l'ordre précédemment réservé, en utilisant les réserves en crypto-monnaies détenues sur les wallets servant au node d'arbitrage coté Secure Swap, appartenant également à l'opérateur du node.

Ainsi, à l'issue de l'opération, l'ordre qui n'avait pas de contrepartie sur notre carnet d'ordre (1 BTC contre 30 ETH) a été servi. Les wallets du node d'arbitrage coté Secure Swap ont 1 BTC de plus et 30 ETH de moins. Les wallets du node d'arbitrage coté échangeur tiers ont 1 BTC de moins et 32 ETH de plus. Au global le node d'arbitrage a gagné lors de cette opération 2 ETH.

Ces gains qui peuvent survenir :

- Servent à rémunérer ceux qui feront fonctionner ce type de node.
- Compensent les risques de change qu'assume l'opérateur d'un node d'arbitrage.
- Compensent les frais de fonctionnement de ce type de node (frais serveur, internet).
- Permettent de payer les frais sur l'échangeur tiers et sur Secure Swap.

Il n'y a donc pas de frais supplémentaires pour le trader quand son ordre est servi grâce à l'apport de liquidité externe via le node d'arbitrage. Tout gain généré par une différence de cotation entre les échangeurs est au profit de l'opérateur du node d'arbitrage.

Un node d'arbitrage peut également effectuer des échanges sans gain pour lui, ceci est paramétrable dans les options de réglages du node d'arbitrage.

Régulièrement, le node d'arbitrage doit opérer un équilibrage de ses wallets coté Secure Swap avec ceux gérés coté échangeur tiers afin de conserver une bonne répartition des crypto-monnaies disponibles. La fréquence de rééquilibrage dépend du stock de crypto-monnaies disponible pour le fonctionnement du node, et aussi en fonction de la tendance des transactions à se compenser entre elles ou pas.

Ce rééquilibrage sera effectué automatiquement sur des critères de minimum de quantité de réserve pour chaque crypto-monnaie, et sera effectué en exécutant des opérations de transfert avec l'échangeur externe. Ces critères seront paramétrables au niveau du node d'arbitrage.

Il est à noter qu'un opérateur de node d'arbitrage n'a pas besoin de faire fonctionner des nodes de blockchains, il s'appuie entièrement sur le réseau Secure Swap et sur l'API de l'échangeur externe dont la liquidité est ainsi exploitée.

Un node d'arbitrage peut opérer avec des réserves en crypto-monnaies relativement modestes, mais son efficacité économique et sa capacité à apporter de la liquidité augmente avec les réserves en crypto-monnaies disponibles (fréquence des équilibrages nécessaires, capacité à traiter des transactions importantes en valeur sur chaque crypto-monnaie).

Grey Matter Technologies SpA opérera des nodes d'arbitrage vers des échangeurs centralisés dont elle aura implémenté l'API avec une réserve de crypto-monnaies suffisante pour en garantir le fonctionnement optimal. Nous fournirons aussi un modèle de node prêt à être adapté à d'autres échangeurs, ainsi que des nodes d'arbitrage prêts à l'emploi sous licence Open-Source.

C'est sur ce modèle de node d'arbitrage, adapté pour cet usage et agrémenté de l'API de Altcoin.IO, que Secure Swap partagera sa liquidité avec les échangeurs qui implémenteront également cette API pour le partage de liquidité entre DEXs.

NODES PASSERELLES ET NODEOWNERS

Les nodes passerelles sont les nodes assurant la communication entre le réseau p2p de Secure Swap et les nodes des blockchains.

Il y a un type de node passerelle par blockchain (un pour la blockchain Ethereum, un pour Neo, un pour Bitcoin, etc.)

Pour que les échanges soient autorisés, Secure Trade demande qu'au minimum deux nodes passerelles pour une blockchain soient actifs sur le réseau. Si ce n'est pas le cas, alors le trading sur la crypto-monnaie correspondante est désactivé.

Les NodeOwners sont les personnes, physiques ou morales, qui choisissent de faire fonctionner des nodes passerelles, devenant ainsi des membres actifs de la communauté Secure Swap.

La société *Grey Matter Technologies SpA* agira en tant que NodeOwner, sans privilège particulier, au même titre que tout membre de la communauté qui choisirait d'assumer ce rôle.

PRÉREQUIS POUR POUVOIR CONNECTER UN NODE PASSERELLE AU RÉSEAU P2P

Pour qu'un node passerelle puisse se connecter au réseau p2p, il doit avoir des jetons SSW, pour une valeur de préférence équivalente à 1.5 fois la valeur moyenne d'une transaction de la crypto-monnaie correspondante. Cette valeur moyenne sera indiquée par les statistiques maintenues par les nodes passerelles, et affichée dans l'interface utilisateur du node passerelle.

Le NodeOwner doit également disposer d'une machine fiable, sécurisée, et d'une connexion Internet stable. Pour cela, il est conseillé d'utiliser un serveur physique ou une machine virtuelle chez un opérateur Cloud.

Il doit également s'être procuré l'application « node passerelle » correspondant à la crypto-monnaie qu'il veut opérer, ou éventuellement avoir développé sa propre spécialisation à partir du modèle de node fourni sous licence Open-Source afin d'ajouter le support d'une crypto-monnaie, et disposer d'un accès à un node de la blockchain correspondante.

SECURITÉ DES ÉCHANGES, UTILISATION DES JETONS SSW MIS EN GARANTIE, RÉTRIBUTION DES NODEOWNERS

Une fois le node configuré pour qu'il se connecte à la blockchain correspondante, sa mise en service le connecte aux autres nodes p2p du réseau Secure Swap. Le node se voit ainsi attribué un identifiant unique sur le réseau. Mais, à cette étape de la mise en service, aucun autre node n'accepte encore les requêtes provenant de ce node et aucun autre node ne lui en envoie.

Pour que ce node passerelle soit pleinement opérationnel, son opérateur doit envoyer sa preuve d'enjeu et de garantie (constituée de jetons SSW) au wallet associé du « smart contract » gérant cela sur le réseau

Ethereum, ainsi que l'identifiant unique du node. Cela se fera aisément via l'interface utilisateur du node. Cette transaction, signée par le node passerelle, va être transmise par le réseau p2p jusqu'à un autre node passerelle vers la blockchain Ethereum qui va, à son tour, la transmettre au node Ethereum auquel il est connecté.

Les jetons sont ainsi envoyés sur le wallet géré par ce « smart contract ». Quand le « smart contract » valide la réception des jetons, il émet l'autorisation du node avec son niveau de garantie. L'autorisation va être propagée à tous les nodes du réseau, qui accepteront alors d'opérer avec lui.

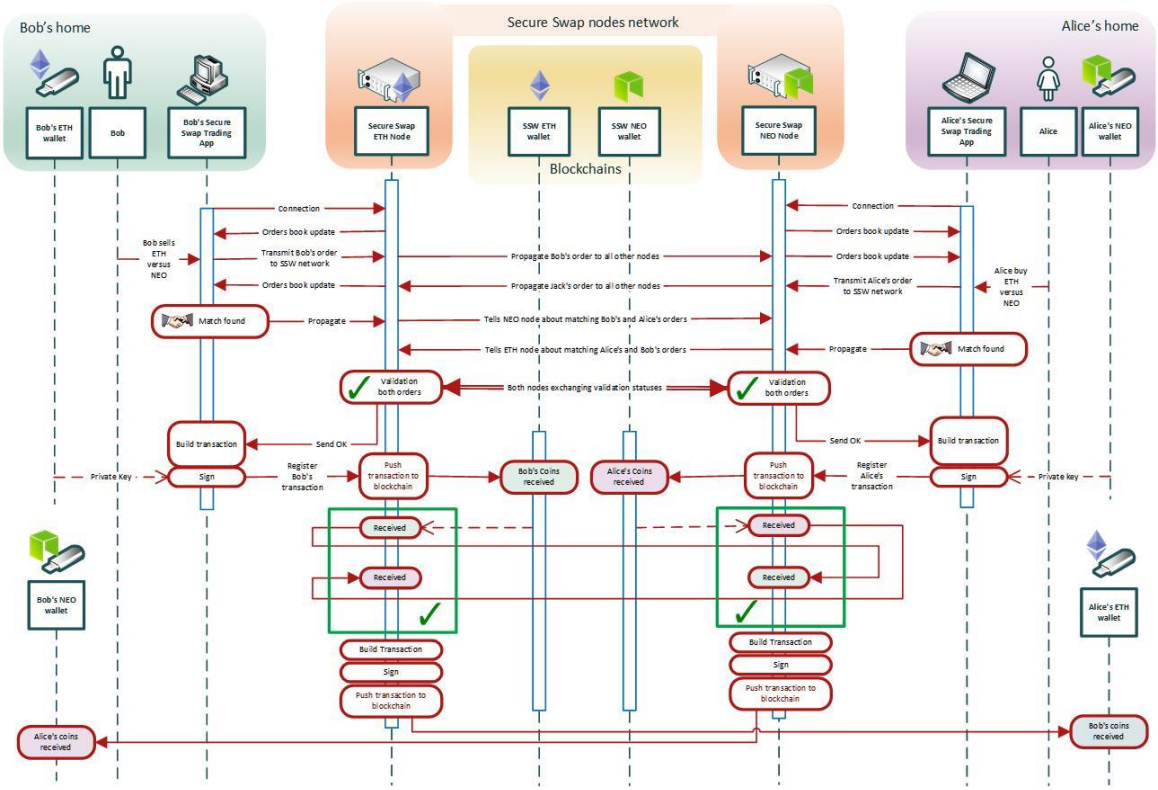
La preuve d'enjeu sert donc aussi de garantie, donnée par le NodeOwner, pour le fonctionnement de son node passerelle. Cette preuve d'enjeu définit également le montant maximum de chaque transaction que peut gérer ce node, qui est au maximum de 2/3 de la valeur de la preuve d'enjeu.

Le node passerelle doit aussi avoir indiqué, via sa configuration, un wallet correspondant à la crypto-monnaie qu'il gère (wallet EOS pour un node passerelle EOS).

Ce wallet sert à recevoir la part des frais payés par le trader qui revient au NodeOwner, au prorata des jetons qu'il a engagés par rapport à tout ceux engagés pour la crypto-monnaie gérée par le node.

Ce wallet sert aussi à recevoir la contrepartie des échanges impliquant la crypto-monnaie gérée par le node, avant envoi au destinataire final. Cela assure l'atomicité des échanges (pour qu'un trader ne reçoive pas une contrepartie d'un échange sans avoir envoyé la sienne).

FLUX DES COMMUNICATIONS LORS D'UNE TRANSACTION SANS INCIDENT



Ce schéma est simplifié pour la facilité de compréhension, et ne représente pas les sécurités constituées par la validation des opérations par tous les nodes d'une blockchain.

En fonctionnement normal (sans incident), lors d'opérations de change entre crypto-monnaies, les contreparties sont acheminées par les nodes passerelles de la crypto-monnaie correspondante (coins NEO passant par les passerelles NEO). Pour chaque transaction, les contreparties sont envoyées sur un des wallets gérés par les nodes passerelles éligibles, choisis aléatoirement. Ce tirage aléatoire est pondéré par le ratio de jetons SSW mis en garantie sur le node, comparé au total des jetons SSW mis en garantie sur l'ensemble des nodes opérant la même crypto-monnaie. Le node peut ainsi conserver directement les frais de change (0.15% initialement) prélevés sur la contrepartie avant de l'envoyer au destinataire.

A noter, seuls les nodes ayant une garantie de 1.5 fois la valeur de la transaction, sous forme de jetons SSW, sont éligibles et peuvent participer au tirage au sort désignant les nodes chargés de recevoir les contreparties.

Ceci permet d'éviter un fractionnement trop important des rémunérations à répartir entre tous les nodes passerelles, tout en garantissant que, sur la durée, chaque node passerelle reçoive la part qui lui est due. Et cela évite aussi des frais réseau supplémentaires pour répartir les frais entre les nodes.

Un mécanisme modifiera la pondération de chaque node en fonction du retard ou de l'avance qu'il aurait pris dans la perception des frais en fonction de la part qu'il doit recevoir. Ce calcul, assuré par les nodes eux-mêmes, prend en compte la totalité des frais perçus par tous les nodes d'une crypto-monnaie. Cela permet de ne pas pénaliser les nodes passerelles qui n'auraient fait transiter que des petites transactions par rapport à d'autres qui auraient fait transiter des transactions importantes en valeur.

Si pour une raison quelconque (piratage, vol, crash, dysfonctionnement, perte de réseau électrique ou internet, etc…), un node passerelle n'envoie pas au destinataire les actifs qu'il a reçus lorsque qu'il doit le faire, alors les jetons SSW en garantie vont être débités du montant équivalent à la contrepartie manquante. Ces jetons vont alors faire l'objet d'un ordre automatique de conversion au prix du marché pour échange contre la crypto-monnaie manquante, et ces actifs vont ensuite être envoyés au destinataire de l'échange qui n'avait pas reçu sa contrepartie.

Cette opération de terminaison d'une transaction interrompue utilisera toutes les sources de liquidités disponibles, ce qui inclut les liquidités des échangeurs externes connectés via les node d'arbitrage, avec d'éventuelles conversions multiples, afin d'être réalisée au plus vite, même si les frais qui en découlent sont plus élevés.

La contrepartie non envoyée par le node passerelle devenant alors la propriété du NodeOwner.

Tous les frais inhérents à cette opération de remplacement sont à la charge du NodeOwner opérant le node passerelle fautif, et sont prélevés sur ses jetons SSW en garantie, qui seront convertis dans la crypto-monnaie permettant de payer ces frais (Ether par exemple pour payer les frais correspondants en Gaz).

Toute cette opération est réalisée par les autres nodes du réseau et par le « smart contract » en charge de cette tâche dans le cadre de la conservation des garanties des nodes passerelles.

Le node passerelle fautif est ensuite déconnecté, s'il était encore connecté, et ses jetons SSW restant en garantie sont retournés au wallet qui les avait envoyés (moins les frais d'envois), donc au NodeOwner.

En cas de déconnexion inopinée du node, ce dernier dispose d'un délai (quelques minutes) pour se reconnecter avec le même identifiant avant que la procédure décrite ci-avant ne s'active. Ceci afin de laisser une chance au node de reprendre ses activités normales en cas de coupure de communication ou de crash intempestif mais de courte durée. Durant ce temps, la garantie du node (en jetons SSW) sera évidemment conservée par le « smart contract ».

Cette procédure sert à la fois à garantir au trader qu'il recevra sa contrepartie suite à un échange, mais aussi à inciter le NodeOwner à s'assurer que son node passerelle fonctionne sur une machine fiable, non susceptible de planter, de perdre sa connexion Internet ou d'être piraté. C'est le NodeOwner qui assume ces risques.

Les jetons SSW en garantie sont également retournés au NodeOwner (moins frais d'envois) lors de l'arrêt normal de son node passerelle.

Un NodeOwner a donc une entrée de valeurs (gains) sous forme d'une part des frais payés par les traders, au prorata des jetons SSW qu'il a mis en garantie pour le fonctionnement de son node, versus le total de jetons SSW affectés à l'ensemble des nodes passerelles pour cette crypto monnaie.

Il paye des frais de mise en fonctionnement et d'arrêt de son node, correspondant à l'envoi initial et à la restitution des jetons SSW laissés en garantie (frais réseau).

En cas de dysfonctionnement de son node aboutissant au défaut de livraison d'une contrepartie, il paye les frais engagés par le système décrit plus haut (qui assure la livraison de la contrepartie au trader), et il assume le risque de change de ses jetons SSW qu'il n'a plus et qui sont remplacés par une valeur équivalente dans la crypto-monnaie gérée par son node, et versée au wallet lié au node (les actifs non envoyés au destinataire).

Une fois le node passerelle arrêté, tous les actifs présents dans le wallet lié au node sont la propriété du NodeOwner. Ils proviennent de la rémunération du node et éventuellement des contreparties qui n'ont pas été renvoyées, mais qui ont été payées par le NodeOwner via ses jetons SSW.

Le node affiche aussi pendant son fonctionnement la quantité d'actifs appartenant au NodeOwner, pour le cas où ce dernier voudrait les transférer sans stopper le fonctionnement de son node.

Les nodes passerelles apportent une décentralisation complète d'accès aux blockchains, sans point de défaillance unique.

Ils apportent une redondance importante à la fois pour la connexion aux blockchains et pour le traitement des échanges.

Cette forte redondance permet aussi d'absorber les périodes de forte charge, permettant si besoin d'ajouter des nodes supplémentaires très facilement, sans interrompre le fonctionnement de Secure Swap.

Ce système de fonctionnement sécurisé des nodes, ainsi que les jetons SSW mis en garantie sur chaque node passerelle, garantissent la réception des contreparties aux traders, quoi qu'il arrive sur le réseau Secure Swap.

Les nodes passerelles permettent également à Secure Swap d'être crypto-agnostique, c'est-à-dire d'opérer avec toutes les crypto-monnaies, sans dépendre de technologies en développement comme Plasma ou Lightning Network, tout en ayant des performances comparables dans ses capacités de traitement des échanges.

NODE DE TRADING SUR MARGE

Les nodes de trading sur marge permettent au réseau Secure Swap de proposer le trading sur marge.

Ce type de nodes sera aussi distribué sous licence Open Source, chacun étant libre d'en faire fonctionner un.

Cependant, il faut noter que faire fonctionner ce type de nodes est assez exigeant. Il faut non seulement avoir un nombre de jetons SSW suffisants afin de constituer une garantie pour les traders, mais également avoir un capital sous forme de crypto-devises correspondant à celles où l'on autorise le trading sur marge.

La société *Grey Matter Technologies SpA* agira en tant qu'opérateur de ce type de nodes, sans privilège particulier.

PRÉREQUIS POUR POUVOIR CONNECTER UN NODE DE TRADING SUR MARGE AU RÉSEAU P2P

Comme pour les autres nodes, il faut une machine fiable, sécurisée et avec une connexion Internet stable, donc ici encore, de préférence un serveur dédié.

Il faut disposer d'une réserve de jetons SSW équivalente à deux fois la somme des marges des positions que le node va autoriser. Dit autrement, la quantité de jetons SSW mis en garantie détermine la quantité de marge qui peut être utilisée dans les positions prises par les traders. En corolaire, la quantité de jetons SSW mis en garantie limite la hauteur des positions qui peuvent être prises en même temps sur le node, dans un rapport de 2 pour 1.

Ces jetons seront mis en garantie via un « smart-contract » dédié, de façon similaire aux nodes passerelles.

Il faut aussi disposer d'un capital en crypto-monnaies suffisant pour que les positions que le node autorise puissent être prises par le trader, puisque le node fait l'avance de la différence entre la taille d'une position et la marge disponible sur le wallet du trader, dans la limite du levier autorisé.

Exemple : le node autorise le trading sur marge sur Bitcoin, le trader veut échanger 100 Bitcoins contre une autre crypto-monnaie, le levier maximum autorisé est de 5.

- La marge initiale du trader devra être alors de 20 Bitcoins minimum.
- La marge minimale du trader est de 15 Bitcoins (seuil d'appel de marge égale à 0.75 * la marge initiale par exemple)
- La garantie en jetons SSW (pour garantir le retour des avoirs du trader) devra être d'une valeur équivalente à celle de 40 Bitcoins (deux fois la marge en garantie).
- Et le nombre de bitcoins disponibles en capital au niveau du node devra être d'un minimum de 80 bitcoins, ce qui, ajouté aux 20 bitcoins de marge du trader, permet de prendre une position de 100 bitcoins (effectuer une opération de change de 100 Bitcoins contre une autre crypto-monnaie).

Ceci multiplié par le nombre de positions équivalentes que permet le node.

FONCTIONNEMENT DU NODE DE TRADING SUR MARGE

L'administrateur du node va devoir, pour chaque paire de crypto-monnaie pour laquelle il décide d'autoriser le trading sur marge, indiquer :

- Le niveau de levier maximum autorisé.
- Le seuil de marge minimum en deçà duquel la position provoque un appel de marge.
- Les frais d'entrée et de sortie de position qu'il prélève.
- Le taux d'intérêt horaire pris pour la position sur marge.

De manière tout à fait similaire aux nodes passerelles, une fois configuré, le node de trading sur marge se connecte au réseau Secure Swap. Il envoie sa garantie en jetons SSW au « smart contract » spécialisé dans la gestion des node de trading sur marge. Il obtient alors son identifiant unique qui va l'autoriser à fonctionner.

Le node informe alors le réseau Secure Swap de ses capacités de trading sur marge, dépendant de ses réserves disponibles en crypto-monnaies et actualisées en fonction des opérations effectuées, afin que les applications clients puissent proposer ce trading via leur interface. Les informations pertinentes seront aussi transmises aux applications clients, comme le niveau de levier maximum autorisé par paire de crypto-monnaies, les frais de maintien des positions (intérêts sur l'avance faite par le node).

L'application client Secure Trade présente ainsi au trader les possibilités de trading sur marge disponibles. Le trader passe son ordre sur Secure Trade, l'ordre est transmis via le réseau p2p de Secure Swap jusqu'au node de trading sur marge concerné, qui, si l'ordre est accepté (s'il remplit les critères de marge, de levier max, etc.), va alors demander de recevoir la marge du trader. Une fois la marge reçue, le node initie une position pour ce trader, ce qui consiste à mémoriser le prêt consenti au trader et à ajouter un ordre d'échange correspondant à l'opération voulue par le trader au carnet d'ordres de Secure Swap.

Une fois l'ordre d'échange exécuté sur le réseau Secure Swap, le node de trading sur marge conserve la contrepartie de l'échange et surveille les pertes latentes éventuelles de l'opération d'échange effectuée.

Si les pertes latentes, converties dans la crypto-monnaie de départ, au cours du marché, font que la marge minimale de maintien de la position est dépassée, alors la position est fermée automatiquement, par appel de marge.

La position peut aussi être fermée à la demande du trader via Secure Trade.

Lors de la fermeture d'une position, le node de trading sur marge effectue une conversion inverse de la première, au cours du marché, en utilisant la contrepartie qui était conservée. Une fois l'échange effectué, il en déduit l'avance effectuée précédemment, puis envoie le solde au trader, après avoir soustrait du solde tous les frais de l'opération.

Exemple :

Un trader veut effectuer une opération sur marge de change de 5 BTC contre 150 ETH, le node passerelle autorise un levier de 5 maximum, et donc demande une marge initiale de 1 BTC minimum pour cette opération. La marge minimum avant appel de marge étant de 0.75 fois la marge initiale, ce node déclenche un appel de marge si la marge disponible tombe en dessous de 0.75 BTC.

Le trader, via Secure Trade, donne l'ordre de prendre cette position.

Le node va avancer 4 BTC pour cette position, et va envoyer l'ordre de change de 5 BTC contre 150 ETH sur le réseau Secure Swap. Le taux de change est donc de 30 ETH pour 1 BTC.

Si l'ordre est exécuté, le node de trading sur marge va recevoir la contrepartie de 150 ETH contre les 5 BTC, 1 BTC appartient au trader et représente sa marge disponible (moins tous les frais), 4 BTC étant prêtés par le node.

Si le taux de change évolue favorablement pour le trader, et qu'il décide de fermer la position quand le taux devient 1 BTC contre 20 ETH, alors le node de trading sur marge qui reçoit l'ordre de clôture de la position va poster un ordre de change des 150 ETH qu'il détient pour cette position contre des BTC au prix du marché.

L'échange s'effectue, pour l'exemple, à 1 BTC contre 20 ETH. Le node reçoit donc 7.5 BTC. Le node récupère les 4 BTC qu'il avait prêté pour cette opération, et envoie donc le solde de 3.5 BTC au trader, diminué des frais.

Si le taux évolue de façon défavorable pour le trader, et qu'il passe brusquement à 1 BTC pour 35 ETH, on a alors un appel de marge. Le node passe automatiquement en fermeture de la position, et donc passe un ordre de change des 150 ETH pour des BTC, au prix du marché.

L'échange s'effectuant pour l'exemple à 1 BTC contre 35 ETH, le node reçoit donc 4.28 BTC, récupère l'avance de 4 BTC et envoie le solde de 0.28 BTC au trader moins les frais. Le trader accuse donc une perte de 0.72 BTC augmentée des frais.

Pour simplifier ces exemples, nous n'avons pas calculé les frais de prise de position, de change et de réseau, qui sont payés par le trader et sont imputés à sa marge disponible pendant le maintien des positions, et déduits du solde envoyé au client à la clôture de la position.

De même, les frais venant des intérêts pris par le node sont déduits de la marge disponible lors du maintien de la position, et déduits du solde retourné au trader.

Le bon fonctionnement des nodes de trading sur marge est assuré par les nodes passerelles, qui contrôlent les node de trading sur marge, chacun selon la crypto-monnaie qu'il gère.

Si le node de trading sur marge a atteint un nombre de positions globales maximum (le double de la somme totale des marges utilisées par les traders correspond au niveau de valeur matérialisé par les jetons du node en garantie), alors les nodes passerelles ne lui permettent plus de proposer aux applications clients d'autres prises de positions sur marge. Seul le débouclage des positons détenues reste disponible, jusqu'à rétablissement d'un niveau de garantie disponible suffisant.

De même, si le node ne dispose plus de suffisamment de fonds dans une crypto-monnaie pour l'avance consentie lors d'une prise de position, alors les nodes passerelles ne lui autorisent plus que le débouclage des positions sur cette crypto monnaie, jusqu'à rétablissement de fonds suffisants.

Si un node de trading sur marge se déconnecte, crash etc., il a un délai de quelques minutes pour redevenir opérationnel. Passé ce délai le « smart-contract » dédié à la gestion de ces nodes va commencer les opérations d'échange de jetons SSW afin de rembourser les clients détenant des positions sur marge gérés par le node fautif. Ce processus :

- Calcule la position du client au moment de la déconnexion du node fautif.
- Détermine les gains / pertes latentes.

- Les intègre à la marge déposée par le client sur le node fautif.
- Et lui retourne le solde moins les frais (réseau, d'échanges, d'intérêts) correspondant à un débouclage immédiat des positions détenues.

Ces jetons SSW seront convertis via les liquidités disponibles sur Secure Swap et apportées par les nodes d'arbitrage, par des ordres de conversion au prix du marché, afin de livrer les traders dans les crypto-monnaies correspondant à leurs positions, toutes ces opérations étant gérées par les nodes passerelles.

Tous les frais engendrés par ces opérations de change et d'envoi des jetons SSW sont imputés au node de trading sur marge fautif, déduits des jetons SSW en garantie, dont le solde lui sera retourné à l'issue de ces opérations.

La répartition des crypto-monnaies des fonds de réserve étant modifiée suite au dysfonctionnement du node de trading sur marge, le risque de change n'est plus le même qu'initialement. L'opérateur du node en assume le risque, et doit éventuellement rééquilibrer sa répartition en crypto-monnaies des fonds servant au fonctionnement de son node.

Si un node de trading sur marge, sans qu'il soit déconnecté, n'envoie pas au propriétaire les crypto-monnaies qui lui reviennent, quand ce dernier à débouclé une position, la procédure décrite ci-dessus se déclenche, uniquement pour cette position.

Chaque déclenchement de cette procédure, sans déconnexion du node, implique une réduction de la quantité de jetons SSW en garantie pour le node de trading sur marge, ce qui impacte sa capacité à prendre d'autres positions sur marges. Quand les jetons SSW en garantie deviennent inférieurs en valeur à deux fois l'ensemble des marges correspondant aux positions en cours, alors il ne peut plus accepter d'autres ordres, cela lui est interdit par les nodes passerelles, ses possibilités de trading sont rendues indisponibles au niveau de Secure Trade, pour ce node de trading sur marge.

Quand une position provoque un appel de marge (la marge est en deçà du niveau de marge demandé pour maintenir la position), le node réduit automatiquement la position jusqu'à retrouver un niveau de marge égal à la marge initiale normale pour une position. Si le niveau de marge ne peut être rétabli par la réduction de la position, alors celle-ci est totalement fermée.

Un opérateur d'un node de trading sur marge paye donc des frais de mise en fonctionnement et d'arrêt (frais réseau liés à l'envoi et récupération des jetons SSW en garantie auprès du « smart-contract »).

Il assume tous les risques de pertes liés à un dysfonctionnement de son node ou à un mauvais paramétrage entraînant une prise de risque inadéquate, comme :

- Un niveau de marge minimum avant liquidation trop faible, qui causerait une perte supérieure à la marge du client lors de la liquidation de la position.
- Ou bien d'un levier autorisé trop grand.
- Ou l'autorisation de trading sur marge pour une paire de crypto-monnaies trop volatiles.

Ses gains proviennent des frais d'entrée et sortie de position, ainsi que des intérêts sur les positions sur marge, qu'il prélève.

Il est important qu'un opérateur de ce type de node évalue bien les risques liés à cette activité. Le paramétrage du node doit permettre une fermeture de position provoquée par un appel de marge sans entraîner le passage en solde négatif, qui si cela arrive constitue une perte pour l'opérateur du node. Cela dépend à la fois du niveau de marge demandé pour garder une position, mais aussi de la volatilité de la paire de crypto-monnaies formant la position.

NODE D'ECHANGE VERS LES DEVISES FIAT

Les nodes d'échange vers les devises fiat sont les points de connexion entre les crypto-monnaies et la finance traditionnelle (devises fiat étatiques).

Ces nodes ne sont pas anonymes. Ils nécessitent de se conformer aux règles KYC ("Know Your Customer"). Ils seront opérés par des unités juridiques, chacune proposant sa liste de paires fiat-crypto échangeables.

Pour se conformer aux règles KYC, les utilisateurs devront ouvrir un compte sur ce type de nodes avant de pouvoir les utiliser.

Ces nodes fonctionnent comme des bourses d'échange. Les utilisateurs y ayant transféré des devises fiat au préalable (cash-in) pourront les échanger contre les crypto-monnaies des autres utilisateurs souhaitant vendre leurs crypto-monnaies contre des devises fiat (cash-out).

En plus du service d'échange fiat–crypto, ces nodes supportent l'intégration de moyens de paiements, grâce à la mise à disposition d'un kit de développement (SDK) permettant l'intégration simple de moyens de payement sur des sites web marchants, sur des applications ou bien sur des moyens de payements mobiles (smartphone).

Ce SDK proposera l'intégration de moyens de paiement basés sur des devises fiat, mais aussi sur des payements directement en crypto-monnaies.

La société *Grey Matter Technologies SpA* prévoit d'opérer ce type de nodes, avec une première étape sur la zone sud-américaine (Chili, Pérou, Argentine pour commencer), et ensuite sur les zones USD et Euro.

A cette fin, elle créera autant de sociétés indépendantes que de zones où elle opérera des échanges vers les devises fiat, afin de ne pas propager les risques opérationnels à l'ensemble de Secure Swap.

Un node type sera fourni sous licence Open-Source, adaptable à différents moyens de paiement, aux régulations locales, et devises fiat auxquelles il est destiné. Cela permettra à ceux qui désirent exercer une telle activité professionnelle, de proposer le support des devises fiats et de moyens de paiement de leurs régions.

SYSTÈME DE DÉTECTION D'ANOMALIES OU DE TENTATIVE DE PIRATAGE

PROTOCOLE DE COMMUNICATION DES NODES DE SECURE SWAP

Ce protocole de communication est engagé lorsque la donnée attendue par un node récepteur est sensible et nécessite une validation.

Ce protocole permet la résolution en une passe du consensus byzantin (https://en.wikipedia.org/wiki/Byzantine_fault_tolerance) en environnement distribué et asynchrone.

Ce processus est rendu possible dans le cadre de Secure Swap car le réseau Secure Swap n'a pas besoin que les données soient reçues dans un ordre particulier, et parce qu'il peut s'appuyer sur un mécanisme de preuve d'enjeu et de gage qui simplifient sa mise en œuvre.

Description du protocole :

Chaque node connaît le nombre de nodes susceptibles de répondre à une requête. Ce nombre est actualisé chaque fois qu'un node apparaît ou disparaît sur le réseau.

Quand une réponse est attendue, une fenêtre de temps de 30 secondes maximum est allouée pour la réception des réponses. Chaque node récepteur mémorise et comptabilise les réponses.

Dès que le nombre de réponses reçues correspond à 60% des nodes susceptibles de répondre, et que toutes les réponses sont identiques, alors la réponse reçue est validée et est réputée exacte.

Si, au contraire, une ou des réponses divergent ou que le nombre de réponses reçues n'atteint pas 60% des nodes susceptibles de répondre, alors la fenêtre de temps de 30 secondes est utilisée pour permettre la réception d'un maximum de réponses.

Quand la fenêtre de temps allouée pour la réception des réponses est écoulée, et donc que la réponse n'est pas encore validée, chaque réponse reçue reçoit alors une notation. Cette notation est calculée en additionnant le nombre de jetons SSW versés au fonctionnement de chaque node ayant fourni la même réponse. C'est dans ce cadre que les jetons SSW servent de preuve d'enjeu.

La réponse qui a la meilleure notation est réputée la réponse exacte. Les nodes qui ont répondu différemment sont écartés du réseau Secure Swap (envoi d'une demande de déconnexion et invalidation de l'autorisation de fonctionner), ce qui peut entraîner l'activation du mécanisme de la garantie pour les nodes concernés (échanges en cours).

Ce protocole assure le fonctionnement correct du réseau en cas de défaillance si au moins 60% des nodes répondent à une requête dans les temps impartis et qu'ils donnent tous la même réponse, ou bien que la réponse correcte soit celle qui est majoritaire en termes de preuve d'enjeu parmi celles reçues dans le temps imparti.

Ce protocole permet à Secure Swap d'être tolérant à la panne, y compris quand cette panne provient d'une tentative de piratage, tout en étant performant.

Dans le cas de non défaillance, la réponse de 60% seulement des nodes concernés valide la réponse. En cas de défaillance, la réponse est validée après un délai de 30s.

Il peut y avoir autant de processus de validation en cours qu'il y a de réponses en attente de validation. Ces validations se déroulent en parallèle, il n'y a donc pas d'attente supplémentaire pour valider une réponse qui serait provoquée par l'attente d'un autre processus de validation d'une réponse précédente.

MISE EN ŒUVRE DU PROTOCOLE DE COMMUNICATION

Quand une opération sensible a lieu, que ce soit la vérification de la réception d'actifs sur un wallet, ou toute autre transmission d'informations passant par les nodes, clients ou passerelles, ces informations sont vérifiées par tous les nodes, selon le protocole de communication précédemment décrit.

Exemple : si Secure Trade reporte avoir envoyé telle quantité d'actifs sur tel wallet, tous les nodes passerelles vers la crypto-monnaie concernée peuvent vérifier l'existence de la transaction, vérifier qu'elle est effectuée et que les actifs sont bien reçus par le wallet indiqué.

Chaque node concerné transmet ces informations aux autres nodes, si des nodes ont des réponses discordantes, alors la réponse valide est celle provenant des nodes cumulant ensemble le plus grand nombre de jetons SSW en garantie, qui devient la réponse majoritaire. Les nodes donnant les réponses minoritaires sont déconnectés du réseau. Leurs jetons SSW en garantie, s'il s'agit de nodes passerelles, sont restitués (éventuellement minorés de la contrepartie conservée par le node si ce dernier en conserve une).

Avec ce système, les jetons SSW qui servent déjà de garantie au fonctionnement des nodes passerelles ont aussi un rôle de preuve d'enjeu.

Ces mécanismes concernent toutes les opérations sensibles, qui sont ainsi sous la surveillance de l'ensemble du réseau.

- Cela inclut l'annonce par un client Secure Trade d'un « matching ». Si aucun autre Secure Trade n'indique le « matching » complémentaire, ou si les nodes passerelle ne valident pas le « matching », alors le Secure Trade fautif est déconnecté.
- Cela concerne également les « matchings » effectués par les nodes d'arbitrage.
- Les opérations effectuées par les nodes de trading sur marge.

Pour les nodes passerelles, si l'un d'eux indique ne pas avoir reçu la contrepartie d'un client pendant un échange, ou s'il n'envoie pas la contrepartie au client destinataire tout en indiquant l'avoir fait, ou pas, alors cela sera détecté par les autres nodes. Le node passerelle fautif sera déconnecté, et ses jetons SSW restitués après en avoir soustrait la partie nécessaire pour terminer l'échange, comme indiqué dans la section « Nodes Passerelles et NodeOwners ».

Pour qu'un node ne puisse pas fausser les statistiques, ce système de validation est employé aussi sur les nodes passerelles, et s'applique entre autres à :

- La valeur d'un jeton SSW exprimée dans chaque crypto-monnaie supportée.
- L'état statistique de répartition de la rémunération entre les nodes passerelles pour le système de tirage aléatoire, pondéré du prochain node passerelle qui va gérer une contrepartie d'un échange
- Etc.

En résumé, toutes les données sensibles sont multi-vérifiées par l'ensemble des nodes, dès que ceux-ci sont en capacité de le faire (un node passerelle Ethereum ne peut pas vérifier la réception de Bitcoins sur un wallet par exemple, mais tous les nodes passerelles vers Bitcoins le peuvent).

Ce système de multi-vérifications, plus la mise en gage des jetons SSW des nodes passerelles connectés, permet d'assurer la sécurité des échanges, la détection d'anomalies quelle qu'en soit la nature (piratage, disfonctionnement…) et la déconnexion des parties défaillantes.

Ce système implique que les parties qui fonctionnent normalement ne sont pas lésées, et que les parties défaillantes assument la responsabilité de leurs pertes éventuelles.

SYSTÈME GARANTISSANT L'ATOMICITÉ ET LA SÉCURITE DES ÉCHANGES

Lorsque qu'une contrepartie est trouvée par une application client, elle émet une réservation de l'ordre correspondant, qui est propagée sur les nodes du réseau Secure Swap. L'ordre devient ainsi verrouillé et non modifiable pour le client Secure Trade qu'il l'a émis. Le client Secure Trade adverse va également trouver la contrepartie complémentaire, venant du premier client, et la réserver aussi.

Exemple : Bob a mis un ordre de 2 BTC contre 60 ETH, Alice a mis un ordre de 32 ETH contre 1 BTC.

Le « matching » est trouvé par les deux clients.

Secure Trade (chez Bob) verrouille l'ordre d'Alice de 32 ETH contre 1 BTC.

Secure Trade (chez Alice) verrouille l'ordre de Bob de 1 BTC contre 30 ETH (1 BTC contre 30 ETH reste dans le carnet d'ordres pour Bob).

Une fois les deux contreparties verrouillées, les nodes passerelles vont initier et gérer le processus d'échange.

Ce ne sera pas répété ensuite, pour ne pas alourdir l'explication, mais tous les nodes passerelles correspondant aux contreparties (ici dans l'exemple : nodes passerelles BTC et nodes passerelles ETH) vont vérifier toutes les étapes du processus. Cela concerne :

- La validité des adresses des wallets transmises (possession de la contrepartie par le donneur d'ordre).
- La réception effective des contreparties par les nodes passerelles tirés au hasard.
- Le renvoi, par les nodes passerelles servant d'intermédiaires, des contreparties aux bons destinataires.
- La bonne réception de leurs contreparties par les applications Secure Trade de Bob et d'Alice.

En cas de désaccord entre les nodes, la réponse valide est celle qui correspond à la réponse donnée par les nodes ayant ensemble le plus de jetons SSW en garantie (preuve d'enjeu), comme décrit au chapitre « Nodes Passerelles et NodeOwners ». Ce mécanisme permet le fonctionnement de l'échangeur dans un environnement « trustless ».

Un node passerelle sur BTC va être désigné pour recevoir cette partie de l'échange, aléatoirement suivant un tirage pondéré décrit au chapitre « Nodes Passerelles et NodeOwners ». Un node passerelle ETH va être désigné suivant le même principe.

Une fois les nodes de réception des contreparties désignés, leurs adresses de wallets sont transmises aux deux applications Secure Trade qui reçoivent la validation d'envoi des contreparties.

Les deux applications Secure Trade envoient leurs contreparties aux nodes passerelles désignés. Une fois que les deux nodes passerelles ont confirmé avoir reçu ces contreparties, les nodes envoient les actifs aux applications Secure Trade des destinataires finaux, ce qui conclut l'échange.

En reprenant notre exemple, Bob a envoyé 1 BTC et reçu 32 ETH en échange, il lui reste un ordre d'échange de 1 BTC contre 30 ETH actif. Alice a envoyé 32 ETH et reçu 1 BTC en échange.

En cas d'incident survenant pendant l'échange (désaccords entre nodes), les nodes minoritaires sont déconnectés et l'échange est poursuivi avec les nodes restants, ce qui peut entrainer un nouveau tirage aléatoire de nodes servant d'intermédiaires pour l'échange.

Si un node passerelle conserve une contrepartie, pour une des raisons suivantes :

- Il ne l'envoie pas à son destinataire dans un délai normal (délai défini par blockchain).
- Il avait reçu une contrepartie avant sa déconnexion de son fait ou par mise en minorité, suite à un désaccord entre nodes.
- Il se déconnecte ou ne répond plus aux requêtes du réseau.

Alors, la contrepartie conservée par le node sera délivrée au trader suivant les modalités décrites dans « Nodes Passerelles et NodeOwners ».

Ainsi la multi-vérification et la mise en gage des jetons SSW permettent de garantir la sécurité des transactions dans l'environnement « trustless » de Secure Swap.

PERFORMANCE DE L'ÉCHANGEUR

Nous avons vu précédemment que l'échangeur n'est pas dépendant des capacités d'une blockchain pour sa vitesse de fonctionnement. Que ce soit pour la gestion du carnet d'ordres, la gestion des transactions et tous les autres systèmes. Bien sûr, un échange en lui-même ne peut pas être effectué plus rapidement que ne le permet une blockchain, mais les blockchains ne limitent pas le nombre de transactions par seconde que peut émettre l'échangeur.

Le nombre de transactions opérables est estimé à environ un millier de transactions par blockchain et par seconde. Le réseau p2p de Secure Swap est constitué de multiples sous-réseaux. Chacun de ces sous-réseau ne gère qu'une seule blockchain. Chaque sous-réseau est indépendant des autres réseaux et donc indépendant des autres blockchains. La capacité totale de l'échangeur est donc multipliée par le nombre de blockchains gérées, ce qui peut représenter quelques dizaines à centaines de milliers de transactions par seconde au total.

Ainsi, sans dépendances avec des technologies encore en développement, Secure Swap propose, avec sa propre technologie, des performances similaires à celles visées par Plasma ou le Lightning Network.

Si on considère une blockchain particulière, au final, la vitesse de l'échangeur est bien sûr limitée par la capacité de la blockchain en question à miner/valider les transactions.

Actuellement la blockchain Ethereum est limitée à environ 10/15 transactions par seconde.

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, grâce à des technologies comme Plasma, le Sharding, le Lightning network. D'autres blockchains, basées sur la preuve d'enjeu, sont nativement rapides. Secure Swap a la capacité d'exploiter la rapidité actuelle et future de ces blockchains.

Nous utilisons des « smart contracts » sur la blockchain Ethereum pour gérer les jetons SSW mis en garantie pour la connexion des différents services, garanties qui servent en cas d'anomalies sur ces services et d'autorisation de fonctionnement de ceux-ci.

Nous sommes donc dépendants de l'avenir de la blockchain Ethereum pour le fonctionnement de Secure Swap.

Cependant rien ne nous empêcherait, le cas échéant, de basculer le fonctionnement de ces parties dépendantes du « smart contract » sur une autre blockchain, et d'en distribuer les jetons en remplacement des jetons SSW ERC-20 en circulation.

Un moyen assez simple de faire cela serait par exemple de basculer le fonctionnement sur la blockchain Tomochain, qui peut être considérée comme un fork d'Ethereum, totalement compatible au niveau jetons et « smart contract », mais qui intègre dès l'origine le Sharding et Plasma et qui fonctionne sur une preuve d'enjeu, la rendant beaucoup plus rapide que Ethereum. Néanmoins, il faudra remplacer les jetons détenus par tous les propriétaires par les nouveaux jetons de cette blockchain. Ce qui impliquerait un fonctionnement de Secure Swap en parallèle, pour les « smart contracts » et jetons, sur les deux blockchains, le temps que tous les jetons SSW ERC-20 soient échangés pour ceux de la nouvelle blockchain.

Cependant, rien ne nous indique que nous aurions des raisons de douter de l'avenir de la blockchain Ethereum. Aussi la dépendance de fonctionnement de Secure Swap avec celle-ci, via nos « smart contracts » et jetons, nous semble une solution pérenne. Et si on se trompe sur ce point, nous migrerons sur une autre blockchain, ce qui consiste simplement à migrer les « smart contracts » et les jetons.

INDICATION DU STATUS DE L'ÉCHANGEUR

Nous avons vu dans les explications précédentes que les nodes passerelles, en plus de leurs autres fonctions, gèrent les statistiques du réseau Secure Swap.

Ces statistiques seront exploitées par les applications clients Secure Trade comme par les autres nodes du réseau p2p.

INDICATIONS AFFICHÉES PAR L'APPLICATION CLIENT

L'application Secure Trade indiquera via un code couleur la disponibilité des nodes passerelles pour chaque crypto-monnaie :

- Rouge : pas de passerelle disponible pour cette crypto-monnaie ➔ pas d'échange possible.
- Orange-Rouge : une seule passerelle disponible pour cette crypto-monnaie ➔ échanges techniquement possibles mais interdits.
- Jaune : deux passerelles disponibles pour cette crypto-monnaie ➔ échange ok.
- Vert : à partir de trois passerelles et plus disponibles pour cette crypto-monnaie ➔ échange ok, garantie de fonctionnement optimal.

Il est possible, mais déconseillé, de trader sur une crypto-monnaie ou seuls deux nodes passerelles seraient en service, cela rend la protection par preuve d'enjeu potentiellement fragile (système désignant la réponse correcte en cas de désaccord entre nodes).

En cas de déconnexion d'un des deux nodes passerelles, il n'en resterait plus qu'un en service, interdisant le trading pour cette crypto-monnaie. Néanmoins un échange qui serait en cours à ce moment-là serait conclu, soit normalement, soit par utilisation des jetons SSW mis en garantie par le node déconnecté (si ce dernier conservait la contrepartie éventuellement reçue avant déconnexion).

Pour assurer un démarrage du service dans des conditions optimales, *Grey Matter Technologie SpA* fera fonctionner trois nodes passerelles pour chaque crypto-monnaie gérée initialement, jusqu'à ce que la communauté prenne le relai.

INDICATIONS ACCESSIBLES DEPUIS LES NODES PASSERELLES

Les nodes passerelles maintiendront en permanence des statistiques à jour sur le réseau afin de produire différentes informations à destination des NodeOwners, des opérateurs des nodes d'arbitrages et de trading sur marge ainsi que pour les traders. Ces statistiques permettront, par exemple :

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

SECURE TRADE, L'APPLICATION CLIENT DE TRADING

Secure Trade, est une application de trading qui apporte à la fois des outils avancés et un portefeuille multi-wallets. Secure Trade sera développé en priorité pour des ordinateurs sous système d'exploitation Windows, Linux et MacOS, avant d'être portée sur IOS et Android dans sa version mobile.

CONNEXION

Au lancement, Secure Trade doit se connecter à un minimum de trois nodes passerelles, avant d'autoriser les opérations de l'utilisateur.

LES WALLETS

Pour gérer les différents types de wallets, l'application Secure Trade utilise un système de plugin, définissant une interface commune de programmation.

Les plugins des wallets gérées par Secure Trade seront installés à partir de dépôts de plugin. Secure Trade gèrera une liste de dépôts qui pourra être mise à jour. L'utilisateur, pour ajouter un wallet pour une crypto-monnaie, n'aura qu'à sélectionner le plugin correspondant depuis une liste, le plugin s'installera alors dans Secure Trade.

Cela permet d'ajouter des wallets pour d'autres crypto-monnaies, en téléchargeant le plugin, sans avoir à modifier l'application Secure Trade.

Ainsi quand on ajoute une crypto-monnaie à Secure Swap, en ajoutant un node passerelle vers une blockchain, il faut également fournir le plugin wallet correspondant pour l'application Secure Trade.

Les wallets hardware, comme Trezor, Ledger etc., seront aussi gérés via leurs plugins respectifs.

Si de nouveaux wallets hardware apparaissent sur le marché, il suffira de développer et d'ajouter le plugin correspondant.

La consultation du solde des wallets, l'émission de transactions, etc. se font via le support des nodes passerelles connectés aux clients Secure Trade. Si le node connecté ne peut exécuter une opération lui-même, il achemine l'opération vers un node en capacité de l'exécuter (la capacité d'exécution dépend de la blockchain concernée par l'opération et de la blockchain à laquelle est connecté le node passerelle).

LES GRAPHIQUES, LES DONNÉES TEMPS REEL

Les données des graphiques des prix pour chaque crypto-monnaie sont issues de l'historique des prix générés par les transactions effectuées sur Secure Swap.

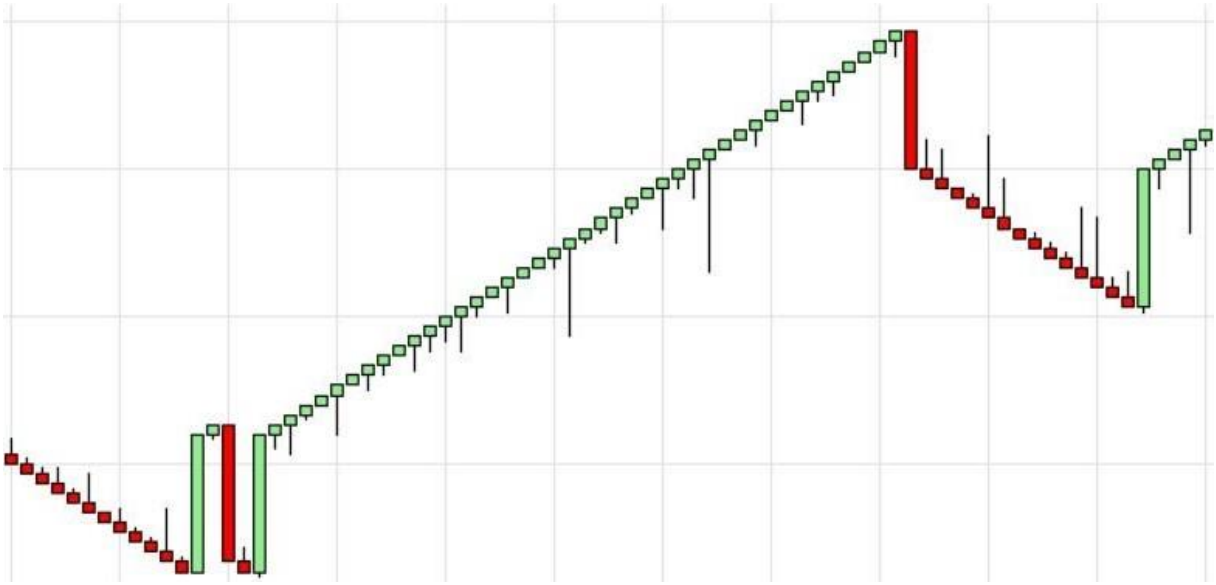
Ce sont à nouveau les nodes passerelles qui mémorisent les historiques de prix, chacun pour la blockchain à laquelle il est connecté. Les nodes passerelles, à leur mise en service, récupèrent ces historiques des nodes passerelles déjà connectés à la même crypto-monnaie.

Secure Trade reçoit les données brutes des nodes passerelles, tick par tick, c'est-à-dire transaction par transaction, et les représente selon les paramètres choisis par le trader.

Hormis les classiques affichages temporels, où le trader peut choisir la période (ticks, secondes, minutes etc.), Secure Trade propose aussi les représentations Kagi, Renko, Line Break, Harmonique Bar (un Line Break amélioré), Point and Figure, Volume, Volume Filter, Range.

Le style graphique par défaut est le classique chandelles (candlestick), mais peut être changé pour le style LineOnClose, Hi Lo, ou OHLC.

Exemple d'affichage en harmonique bar (break 28 et tendance 2) et candlestick :



LE CARNET D'ORDRES

Comme indiqué précédemment, Secure Trade est un node comme les autres du point de vue de la transmission des données du carnet d'ordres, il en reçoit donc les mises à jour.

Le module carnet d'ordres de l'application Secure Trade indique les volumes par niveau de prix (profondeur du carnet d'ordres), mais également la provenance de la liquidité par un code couleur.

Par exemple, vert pour les volumes provenant du carnet d'ordres Secure Swap et orange pour le volume provenant des nodes d'arbitrage. La distinction de la provenance de la liquidité est importante car celle venant des nodes d'arbitrage peut entrainer un échange un peu plus lent que les échanges utilisant la liquidité provenant directement du réseau Secure Swap.

LES OUTILS DE TRADING

Hormis les outils de trading classiques et les différents types d'ordres disponibles qui sont :

- Ordre au marché,
- Ordre limite,
- Ordre stop,
- Ordre à seuil de déclenchement,
- Ordre à seuil de déclenchement avec limite,
- Ordre OCO « order cancel order »,
- Ordres multiples,

Secure Trade possède des modules d'aide au « scalping » et au « money management », exécutant des ordres semi-automatiques définis à l'avance.

LE TRADING SUR MARGE

Chaque node de trading sur marge disponible propose ses propres conditions de trading sur marge :

- Paires de crypto-monnaies autorisées pour le trading sur marge,
- Frais d'entrée et sortie de position sur marge,
- Niveau de marge initiale et minimum (déclenchant un appel de marge si marge insuffisante),
- Intérêts horaires sur les positions sur marge,
- Niveau de levier maximum.

Secure Trade affiche la liste des nodes de trading sur marge disponibles et leurs configurations.

Secure Trade dispose de filtres pour sélectionner des nodes de trading sur marge suivant ces critères. Elle indique également, pour chaque node, son identifiant et sa durée online sans déconnexion, afin que le trader puisse éviter les nodes les moins fiables. Sachant qu'une déconnexion d'un node de trading sur marge implique la fermeture des positons du trader.

LE TRADING AUTOMATIQUE

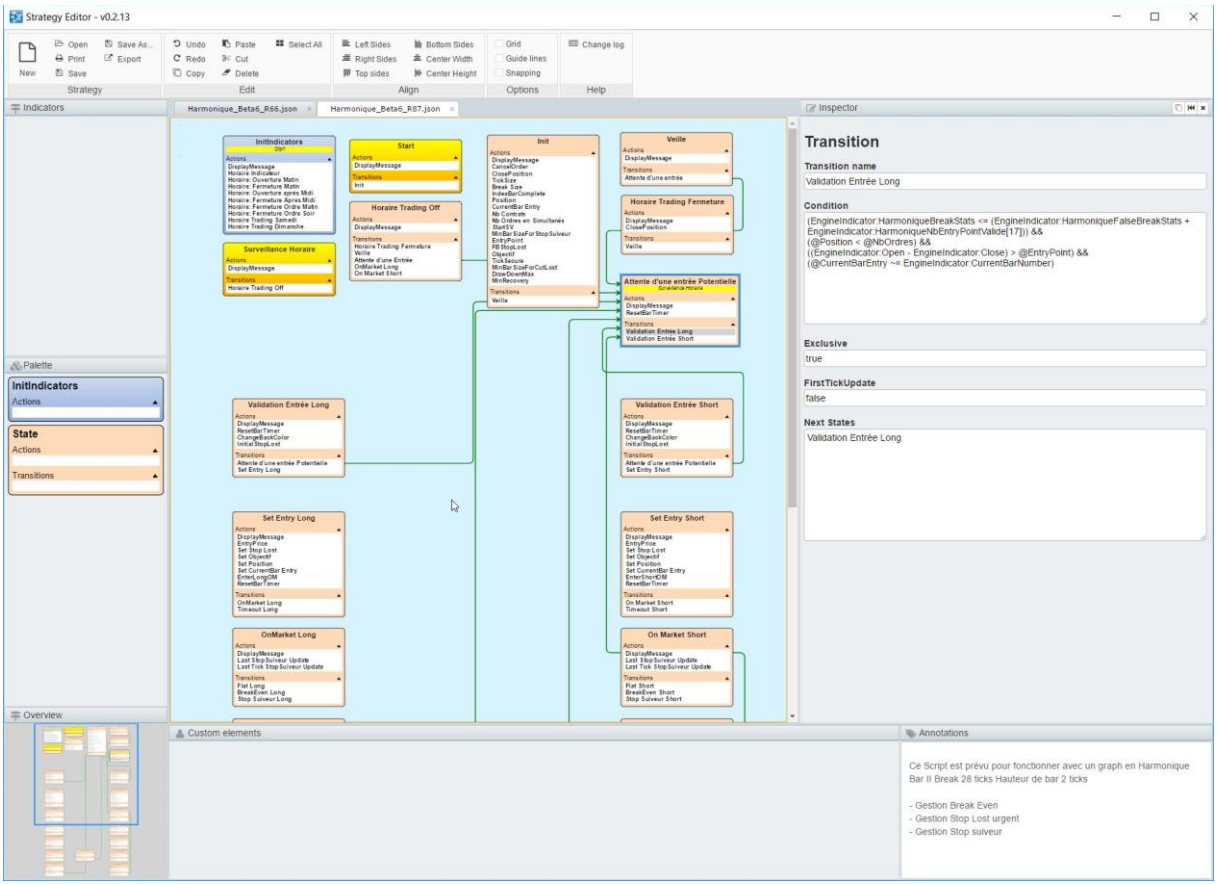
Secure Trade dispose d'un module de trading automatique.

Ce module est constitué d'une machine à états hiérarchique et à exécution parallèle (HCSM : Hierarchical Concurrency State Machines). Un langage de script, simplifié autant que possible, permettra de programmer cette machine à états pour lui faire exécuter des ordres en fonction de conditions programmées.

Ces conditions pourront utiliser les résultats de tous les indicateurs disponibles ainsi que les prix de graphiques, la situation des wallets, des indications de « money management », des indications horaires etc.

La programmation de ces machines à états se fait par l'intermédiaire d'un éditeur graphique, accessible même aux personnes qui n'ont pas de grandes connaissances en programmation.

Version en développement de l'éditeur de stratégies :



Version alpha de l'éditeur de stratégie.

COMMENT PALLIER AU MANQUE DE LIQUIDITÉS INITIAL ?

À leur lancement, les échangeurs ont forcément des problèmes de liquidité : 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.

Au démarrage, Secure Swap n'aura aucune liquidité propre et devra s'appuyer sur les liquidités externes fournies par les nodes d'arbitrages.

Pour cela la société *Grey Matter Technologies SpA* mobilisera une partie de ses fonds. Ces fonds seront répartis en diverses crypto-monnaies disponibles pour les services d'arbitrage (un node d'arbitrage par échangeur tiers). Nous prévoyons initialement d'utiliser les liquidités de trois échangeurs centralisés.

Ces nodes d'arbitrage seront opérés par la société *Grey Matter Technologies SpA*, avec des fonds suffisants assignés à chaque instance connectée à un échangeur tiers, afin d'en garantir un fonctionnement efficace dans l'apport de liquidité.

Les membres de la communauté Secure Swap pourront également faire fonctionner ce type de nodes connectés à des échangeurs tiers, ce qui apportera encore davantage de liquidité.

UN ÉCHANGEUR SOUS LICENCE OPEN SOURCE

Les différents types de nodes de l'échangeur seront distribués sous licence Open source.

Cela signifie qu'en plus de Secure Trade 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, des nodes d'échanges vers des devises fiat, des nodes d'arbitrages (apport de liquidité) et des nodes de trading sur marge.

Les NodeOwners faisant fonctionner des nodes passerelles et possédant des jetons SSW, percevront leur part des frais, prélevés lors des échanges au prorata des jetons qu'ils auront alloués à un node passerelle vers une blockchain, par rapport à la totalité des jetons SSW alloués aux nodes passerelles vers la même blockchain en fonctionnement.

Les autres types de nodes étant en mesure de générer leurs propres revenus indépendamment, ils ne sont pas inclus dans ce système de partage des frais.

La société *Grey Matter Technologies SpA* fonctionnera de la même manière et touchera sa part des frais d'échanges au prorata des jetons 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 modèle 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 modèle de node que nous fournirons en open source sera à adapter à chaque cas particulier.

La société *Grey Matter Technologies SpA* exploitera initialement ce type de nodes pour les régions d'Amérique du Sud, USA et Europe. Nous prévoyons d'exploiter des nodes de conversion en devises fiat pour les devises suivantes : Peso Chilien, Peso Argentin, Sol Péruvienne, USD et Euro puis éventuellement d'autres par la suite.

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

PROGRAMME DE BUG BOUNTY

Une partie des fonds récoltés lors de l'ICO sera utilisé pour financer un service de pentesting et des campagnes de bug bounty. Les récompenses seront décernées à ceux qui participeront à ces programmes bug bounty et auront signalé à nos équipes des bugs ou des failles de sécurité encore inconnus.

Le pentesting sera utilisé pendant les phases de développement, le bug bounty à partir des versions release candidates.

Une campagne bug bounty sera lancée à chaque étape de la phase de développement à partir de la release candidate, 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.

Nous étudierons la pertinence d'utiliser pour cela les services de Buglab, une plateforme sur le réseau Ethereum qui permet la mise en relation pour ce type de programme.

https://buglab.io/#about

ASPECT FINANCIER DU JETON

ÉLÉMENTS UTILISÉS POUR CETTE PROJECTION

- Nombre de jetons total émis : 100 000 000
- Prix d'émission du jeton : 0,45 $ USD
- Pourcentage de jetons effectivement assignés aux nodes passerelles : 30%

Nous pensons qu'une partie des acquéreurs de jetons SSW ne feront pas fonctionner de nodes passerelles vers des crypto-monnaies (et ainsi ne tireront pas profit de la part correspondante des frais d'échanges payés par les traders), mais les achèteront uniquement pour des motifs de spéculation sur le prix du jeton.

Une partie des jetons sera utilisée pour faire fonctionner des nodes de trading sur marge.

Par conséquent, nous pensons qu'au maximum 30% des jetons SSW seront effectivement alloués au fonctionnement de node passerelles. Plus la part des jetons assignée au fonctionnement des nodes passerelles est faible, plus grand est le rendement des jetons pour ceux qui font fonctionner des nodes.

Nous allons utiliser des données venant de CoinMarketCap pour le volume d'échange journalier des échangeurs et la distribution de volume entre crypto-monnaies, collectées fin Juillet 2018, afin d'évaluer le rendement possible des jetons SSW pour ceux qui acquerraient ces jetons au prix de l'ICO et feraient fonctionner des nodes passerelles avec.

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.

Pour évaluer une fourchette de rentabilité probable du jeton, nous allons considérer différents scénarios portant sur le volume d'échange journalier de Secure Swap.

PROJECTION DE LA RENTABILITÉ D'INVESTISSEMENT DANS LE JETON SSW

Nous considérons que les jetons, qui sont assignés au fonctionnement des nodes passerelles, le sont en proportion du volume d'échanges de chaque crypto-monnaie.

Une surallocation de jetons à des nodes passerelles d'une crypto-monnaie ferait baisser la rentabilité des jetons pour cette crypto-monnaie. À contrario, la sous allocation de jetons à d'autres crypto-monnaies, en ferait augmenter la rentabilité. Cela signifie que ceux qui exploitent des nodes passerelles auront tendance à allouer leurs jetons aux crypto-monnaies les plus rentables, ce qui réduira leur rentabilité et augmentera celle des autres crypto-monnaies. En conséquence, la répartition des jetons sur les nodes passerelles va naturellement tendre à correspondre à celle des volumes d'échanges entre crypto-monnaies.

Formule de calcul de rentabilité des jetons :

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

Rentabilité Jeton : $$R = \frac{(\frac{\sum VE \times FEC}{FRTC} \times T)/(TTOK \times FTAP)}{PX}$$

On voit que si FEC = FRTC, nous obtenons :

Rentabilité Jeton : $$R = \frac{(\sum VE \times T)/(TTOK \times FTAP)}{PX}$$

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

Par exemple :

Prenons un volume d'échanges de 3 millions $ USD journalier (échangeur classé 100ème sur CoinMarketCap)

En annuel, cela nous fait : ∑ VE = 365*3 = 1 095 millions $ USD

Les frais de l'échange étant de T = 0,15%, nous avons alors :

Rentabilité = ((1 095 000 000 * 0,0015) / (100 000 000 * 0,3)) / 0,45 = **12,2%** de rendement annuel

Avec un volume d'échanges de 10 millions $ USD journalier (échangeur classé 75ème sur CoinMarketCap)

Rentabilité = ((10 000 000 * 365 * 0,0015) / (100 000 000 * 0,3)) / 0,45 = **40,6%** de rendement annuel

Avec un volume d'échanges de 20 millions $ USD journalier (échangeur classé 50ème sur CoinMarketCap)

Rentabilité = ((20 000 000 * 365 * 0,0015) / (100 000 000 * 0,3)) / 0,45 = **81,1%** de rendement annuel

Et si, malgré ce qu'il apporte comme avantages, Secure Swap ne faisait pas mieux en volume échangé que les échangeurs DEXs moyens, du moins la première année, le temps qu'il soit adopté en masse, cela ferait quand même de l'ordre de 1.2 millions de dollars échangés par jour (environ le volume de Bancor, Crypto Bridge et Wave DEX), la rentabilité serait quand même de :

Rentabilité = ((1 200 000 * 365 * 0,0015) / (100 000 000 * 0,3)) / 0,45 = **4.8%** de rendement annuel

CONCLUSION

Nous croyons qu'avec ses avantages, Secure Swap rejoindra rapidement les volumes d'échanges des DEXs les plus actifs, tel que Bitshare, IDEX et OpenLedger.

Cela représente environ 400 BTC d'échange journalier, soit avec un BTC à 6000 $ USD, **une rentabilité d'environ 10% annuel des jetons SSW**.

Par la suite, nous pensons que Secure Swap est en mesure de prendre des parts de marché conséquentes aux échangeurs centralisés, ce qui ne fera qu'augmenter la rentabilité de détenir des jetons SSW dans le but de faire fonctionner des nodes passerelles ou des nodes de trading sur marge.

Nous n'avons pas chiffré la rentabilité de l'activité de trading sur marge, car elle dépend trop des choix de paramétrage par leurs opérateurs et du volume de trading sur marge.

De même, nous n'avons pas chiffré la rentabilité d'un node d'arbitrage ou d'un node d'échanges vers devise fiat, qui dépendent de trop de paramètres inconnus actuellement, comme le volume de liquidité apporté et effectivement utilisé sur le réseau Secure Swap, la possibilité de bénéficier d'écarts de prix entre échangeurs, le volume d'échanges vers chaque devise fiat, etc.

Ces projections nous montrent que la rentabilité des jetons SSW augmente rapidement avec les volumes journaliers échangés. Si Secure Swap prend effectivement des parts de marché aux échangeurs centralisés, ce pour quoi il a été conçu et ce qui est son objectif, alors le jeton SSW pourrait devenir très demandé et très rentable.

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

POURQUOI LA CRÉATION D'UN JETON ERC 20 ?

Le jeton SSW, en plus de servir à la collecte des fonds lors de l'ICO, servira de preuve d'enjeu et de garantie permettant la sécurité de fonctionnement de l'échangeur, ainsi que la répartition des frais payés par les traders, et collectés lors des échanges.

DONNÉES DE L'ICO

Nom du jeton :	Secure Swap
Ticket :	SSW
Quantité créée :	100 millions de jetons
Prix initial du jeton :	0,45$ USD
Réservé à l'équipe :	10%
Réservé pour les conseillers :	3%
Réservé pour les animateurs sociaux :	3%
Réservé pour les partenaires :	4%
Disponible pour l'ICO :	80%
Soft Cap :	10 millions de jetons
Hard Cap :	80 millions de jetons

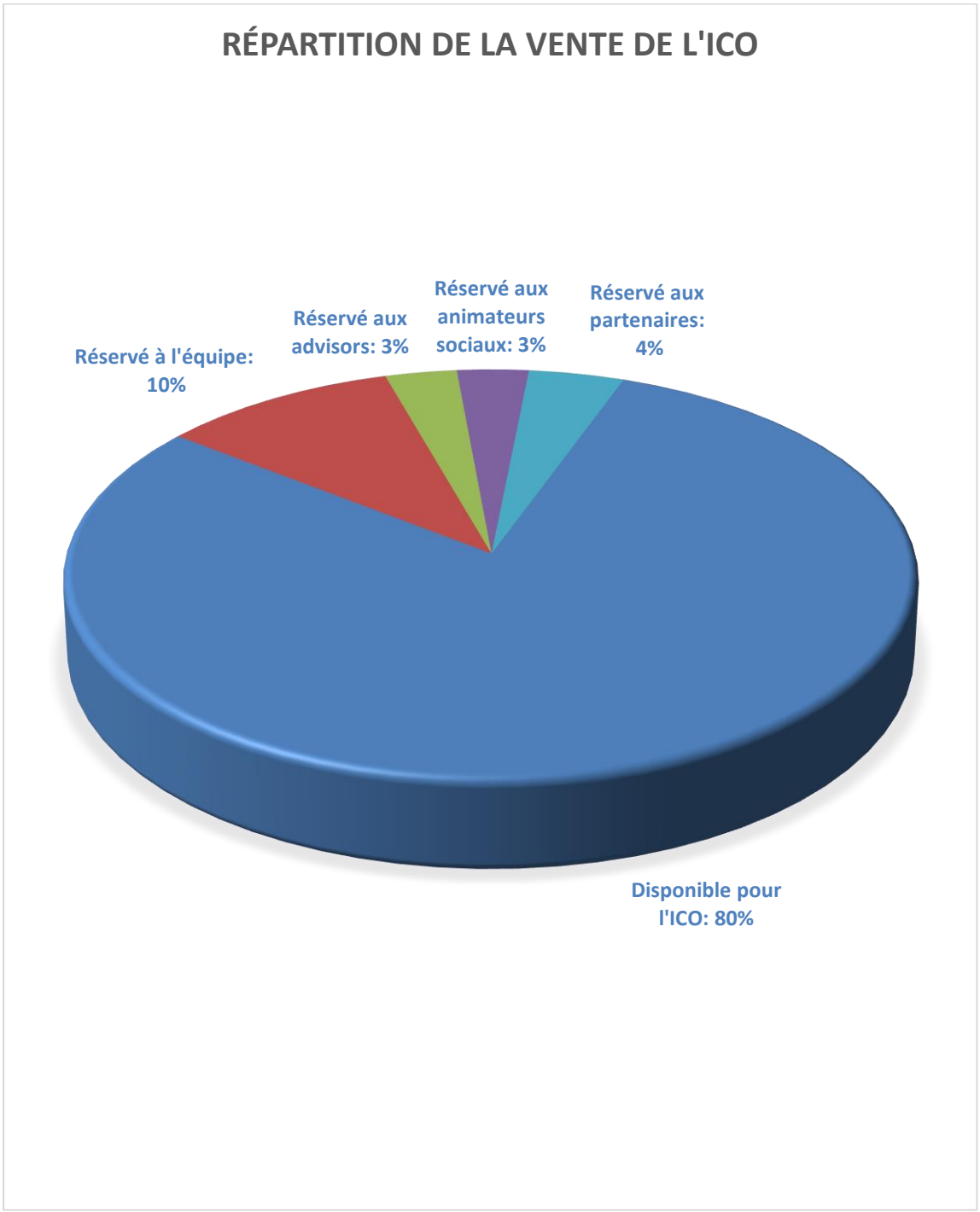
Tous les jetons invendus restent la propriété de la société *Grey Matter Technologies SpA* afin de servir de preuve d'enjeu et de garantie dans le fonctionnement des nodes passerelles qui seront opérés par la société.

Il ne s'agit pas que l'équipe récupère les jetons invendus, ce qui constituerait un abus de biens sociaux.

Ces jetons resteront la propriété de la société, afin de les utiliser comme preuve d'enjeu et garantie pour faire fonctionner des nodes, la société agissant comme un (des) NodeRunner(s) et comme opérateur de nodes de trading sur marge.

Cela constituera la principale source de revenus de la société. Les autres revenus proviendront des frais collectés sur les échanges fiat ainsi que les gains effectués avec les nodes d'arbitrage.

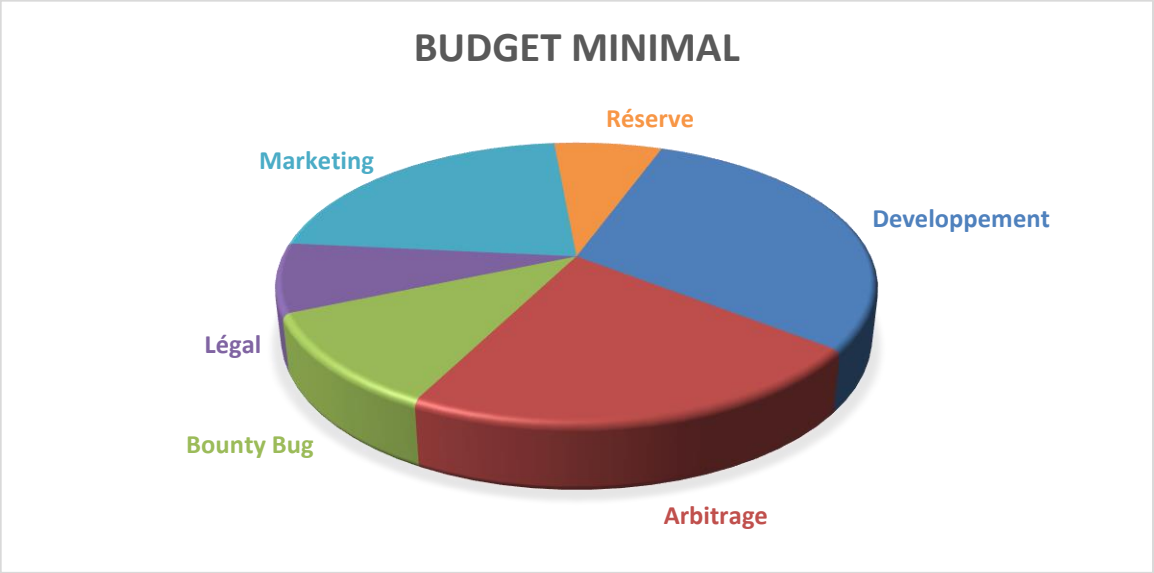
La société *Grey Matter Technologies SpA* se réserve le droit prioritaire de rachat des jetons SSW attribués à l'équipe ainsi qu'aux autres collaborateurs (conseillers, animateurs sociaux, et partenaires), afin de renforcer sa part de collecte des frais payés par les traders.


RÉPARTITION DE LA VENTE DE L'ICO
Réservé à l'équipe: 10%
Réservé aux advisors: 3%
Réservé aux animateurs sociaux: 3%
Réservé aux partenaires: 4%
Disponible pour l'ICO: 80%

UTILISATION DES FONDS COLLECTÉS

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

SOFT CAP ATTEINT



Le soft cap est le budget nécessaire pour développer le produit minimum viable.

Il correspond à 4.5 Millions de $USD.

Budget développement : ..... 1,35 Million $USD

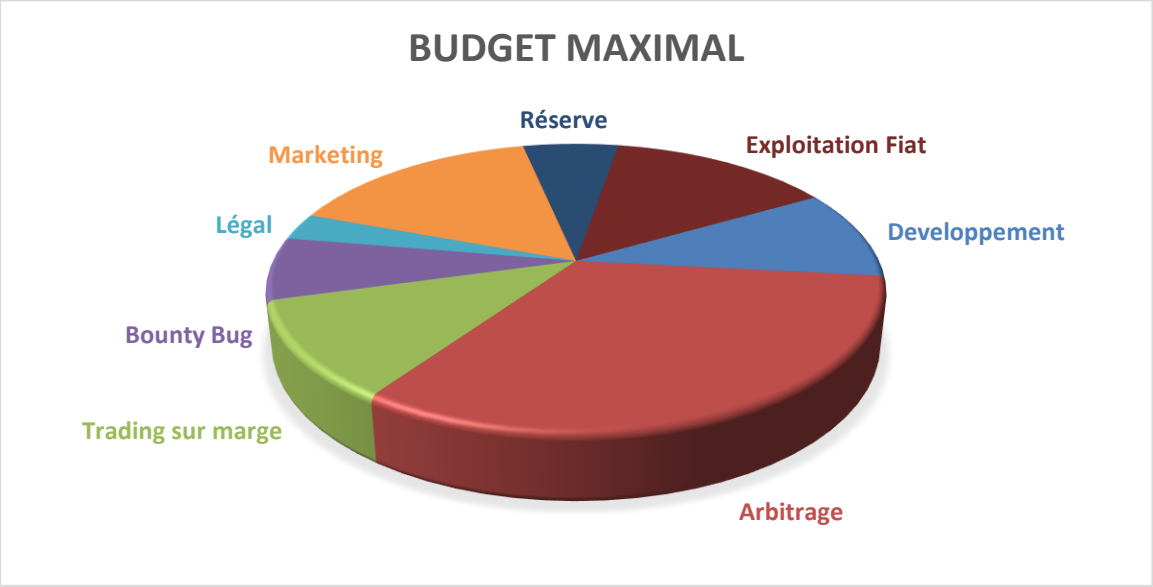
- Application client de trading simplifiée Secure Trade (Trading sur Blockchain Ethereum uniquement) : ..... 400 K $USD
- Modèle de node passerelle + « smart contract » sans contrôles des nodes de trading sur marge : ..... 450 K $USD
- Spécialisation du modèle de node passerelle pour la blockchain Ethereum + Jetons : ..... 100 K $USD
- Modèle de node d'arbitrage : ..... 350 K $USD
- Spécialisation du modèle de node d'arbitrage pour un échangeur tiers : ..... 50 K $USD

Exploitation du node d'arbitrage par *Grey Matter Technologie SpA* :
Réserve de fonds nécessaires : ..... 1 Million $USD

- 70 % Ethereum
- 30 % répartie en jetons ERC-20 / ERC-223 / ERC-777

Programme Bug Bounty : ..... 500 K $USD
Marketing : ..... 1 Million $USD
Légal : ..... 350 K $USD
Fond de réserve : ..... 300 K $USD

HARD CAP ATTEINT



Le hard cap est le budget nécessaire pour réaliser le produit avec toutes les fonctionnalités.

Il correspond à 36 Millions $USD.

Budget développement : .....3,7 Millions $USD

- Application client de trading Secure Trade complète : ..... 800k $USD
  - Trading sur toutes les Blockchains
  - Trading sur marge
  - Passage d'ordre sur le graphique
  - Module d'aide au « money management »
  - Module de trading automatique programmable
- Modèle de node passerelle + contrôles trading sur marge + « smart contract » : ..... 700k $USD
- Spécialisation du modèle de node passerelle
  - Pour la blockchain Ethereum + Jetons : ..... 100k $USD
  - Pour la blockchain Bitcoin : ..... 50k $USD
  - Pour la blockchain Tether : ..... 50k $USD
  - Ripple : ..... 50k $USD
  - Bitcoin Cash : ..... 50k $USD
  - EOS : ..... 50k $USD
  - Litecoin : ..... 50k $USD
  - Stellar Lumen : ..... 50k $USD
  - Monero : ..... 50k $USD
  - Dash : ..... 50k $USD
  - Neo : ..... 50k $USD
  - Zcash : ..... 50k $USD
- Node de Trading sur marge + SC (smart contract) : ..... 750k $USD
- Modèle de node d'arbitrage : ..... 350k $USD
- Spécialisation du squelette de node d'arbitrage pour trois échangeurs tiers : 3*50k = ... 150k $USD
- Modèle de node d'échange vers devise fiat + SDK : ..... 300k $USD

Exploitation de trois nodes d'arbitrages par *Grey Matter Technologies SpA* : 3 x 4M $USD : .....12 Millions $USD

Répartition par nodes d'arbitrage :

- Bitcoin ..... 1,3 Millions $USD
- Tether.....1 Million $USD
- Ethereum et Jetons .....1 Million $USD
  (70% Ethereum, 30% Jetons ERC-20 / ERC-223 / ERC-777)
- Ripple .....300 K $USD
- Autres crypto-monnaies.....400 K $USD

Exploitation d'un node de trading sur marge par *Grey Matter Technologies SpA* :.....4 Millions $USD

Répartition des fonds entre crypto-monnaies similaire à un node d'arbitrage, mais réduit à une partie des crypto-monnaies sur des critères de volatilité.

Ouverture et exploitation de cinq entités juridiques pour l'exploitation des conversions vers devises fiat et services de moyens de paiement, USD, EUR, CPL (pesos chilien), SOL (sol péruvien), ARS (pesos argentin) : 5 * 1M $USD.....5 Millions $USD

Par entité : 1M $USD

- Légal : ..... 400 K $USD
- Structure (création société, personnel…) :..... 200 K $USD
- Plateforme technique : ..... 100 K $USD
- Spécialisation du Modèle de node d'échange vers devise fiat : 100 K $USD
- Marketing :..... 100 K $USD
- Réserve :..... 100 K $USD

Nous préférons avoir des entités indépendantes pour l'exploitation des moyens de paiement et échanges entre crypto-monnaies et devises fiat afin de garantir la nette séparation juridique entre Secure Swap / *Grey Matter Technologies SpA* et les échanges fiat, afin de préserver *Grey Matter Technologies SpA* et le cœur de Secure Swap des risques de régulations liés aux échanges fiat.

Programme Bug Bounty : .....2,5 Millions $USD

Marketing : .....6 Millions $USD

Légal :.....1 Millions $USD

Fonds de réserve : .....1.8 Millions $USD

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 autonomes. 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

Novembre 2017-Janvier 2018

- Emergence de l'idée du projet, initialement en tant que système d'arbitrage entre plateformes d'échanges.
- Etude de marché.

Février - Mars 2018

- Redéfinition du projet comme échangeur hybride.
- Lancement du projet, début conception technique et définitions de l'ICO.
- Réservation des domaines pour la société et l'ICO.
- Préparation technique de l'ICO.
- Recrutement animateurs pour les réseaux sociaux.

Avril - Juin 2018

- Recrutement animateurs pour les réseaux sociaux.
- Ecriture des documents et site web.
- Traduction des documents et site web.
- Redéfinition du projet en tant qu'échangeur DEX.

Juillet-Août 2018

- Création de la société d'exploitation (Grey Matter Technologies SpA).
- Mise en place des serveurs de production pour l'ICO.
- Tests complets du système pour l'ICO (Site web, serveurs, Blockchain).
- Recrutement premier advisor.

Septembre - Décembre 2018

- Refactoring du projet, réécriture et re-traduction des documents, ajout du trading sur marge au projet.
- Tests complets du système pour l'ICO (Site web, serveurs, Blockchain).
- Creation des channels de communications sur les reseaux sociaux.
- Annonce Pre-ICO sur les sites dédiés.
- Ouverture publique du site web

Janvier 2019 - Mai 2019

- Début Pré-ICO (1er Janvier 2019).
- Suivi de la Pré-ICO.
- Fin pré-ICO (28 février 2019).
- Bilan.
- Début embauches pour renforcement du developpement.
- Debut ICO (1er Mars 2019), période de trois mois renouvlables.

ROADMAP SECURE SWAP

Janvier - Avril 2019

- Réalisation d'un demonstrateur validant le principe de propagation du carnet d'ordres, des nodes passerelles, du client, du trading sur marge et de l'apport de liquidité par les nodes d'arbitrage.

Mai - Juin 2019

- Version Alpha du client et du node passerelle générique.
- Pentesting.

Juillet - Septembre 2019

- Version alpha du node d'arbitrage et du node squelette pour conversion fiat et SDK. (*)
- Version alpha du node de trading sur marge (*)
- Pentesting.

Octobre - Décembre 2019

- Version Beta de tous les composants de la plateforme.
- Spécialisation de nodes passerelles pour les premières crypto-monnaies supportées
- Pentesting.

Janvier - Mars 2020

- Version Release candidate du client.
- Version Release candidate des nodes passerelles vers les premières crypto-monnaies supportées.
- Lancement de nos propres serveurs faisant fonctionner des nodes passerelles.
- Version release candidate du node d'arbitrage et exploitation sur nos propres serveurs.
- Version release candidate du premier node d'échange vers devises fiat et SDK, création d'une entité juridique pour exploitation. (*)
- Première campagne Bug Bounty, sur version en exploitation.

Avril - Juin 2020

- Version release candidate du node de trading sur marge et exploitation sur nos propres serveurs. (*)
- Specialisation du node d'échange vers devises fiat pour une seconde devise, création d'une entité juridique pour exploitation. (*)
- Version Alpha des clients IOS et Android (*).
- Campagne Bug Bounty.
- Ajout de crypto-monnaies supportées par la plateforme (ajout de nodes passerelles spécialisés)

Juillet - Septembre 2020

- Version Beta des clients IOS et Android (*).
- Campagne Bug Bounty.
- Ajout de crypto-monnaies supportées par la plateforme (ajout de nodes passerelles spécialisés).
- Specialisation du node d'échange vers devises fiat pour une troisiéme devise, création d'une entité juridique pour exploitation. (*)

Octobre - Décembre 2020

- Version Release candidate des clients IOS et Android (*).
- Campagne Bug Bounty.
- Ajout de crypto-monnaies supportées par la plateforme (ajout de nodes passerelles spécialisés).
- Specialisation du node d'échange vers devises fiat pour deux autres devise, création des entités juridiques pour exploitation. (*)

Cycles itératifs de trois mois

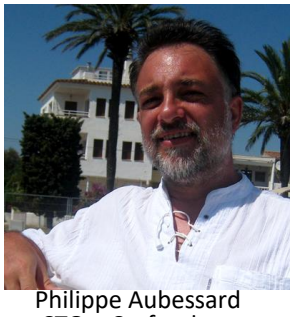
- Campagne Bug Bounty.
- Ajout de crypto-monnaies supportées par la plateforme (ajout de nodes passerelles spécialisés)
- Specialisation du node d'échange vers devises fiats, création d'entités juridiques pour exploitation. (*)

ÉQUIPE

MEMBRES FONDATEURS

Alain Saffray
CEO – Co-fondateur
Developer engineer

30+ ans d'expérience en développement logiciel,
Alain est un programmeur très expérimenté avec de solides connaissances techniques.
Ses expériences antérieures dans différentes industries de l'informatique, allant de la gestion, le jeu vidéo, le traitement d'images, la conception de robots de trading automatiques lui ont permis de couvrir de nombreux aspects techniques difficiles du développement de logiciels.
Toutes ces expériences font qu'il est capable de gérer n'importe quel projet avec confiance et pragmatisme.
Il est aussi co-fondateur de Montmartre Spa, devenue holding de Grey Matter Technologies.
http://www.viadeo.com/p/0021oc3uxefhcfu2



Philippe Aubessard
CTO – Co-fondateur
Developer engineer

35+ ans d'expérience en IT, Philippe possède une vaste gamme d'expérience et de connaissances techniques.
Leader dynamique, il a développé un certain nombre de technologies novatrices, de la R&D jusqu'au marché.
Fondateur de multiples projets, travaillant avec une douzaine d'entreprises de toutes tailles et de tous types, il possède une vaste expertise en IT, en R&D, en développement de produits, en ingénierie et QC.
Il est un expert en sécurité informatique, en particulier dans le domaine du mobile. Philippe est également un investisseur précoce dans les crypto-devises.
http://www.viadeo.com/en/profile/philippe.a

Nadine Miotti
Co-fondatrice

Plus de 25 ans d'expérience dans le commerce et les relations publiques. Chargée d'affaires Grands-Comptes pour des Entreprises financières et des Banques.
Un regard constant sur l'innovation et l'avenir - une persistance qui ne craint pas l'adversité, j'aborde le monde des crypto-monnaies avec enthousiasme.

Alicia Laura
Co-fondatrice

Investisseuse dans différents projets, notamment dans le domaine médical, c'est avec enthousiasme que je participe à ce projet novateur.

Co-fondatrice de Montmartre Spa, devenue holding de Grey Matter Technologies SpA.

ÉQUIPE

Victor Chukholskiy
Blockchain Engineer
Smart Contracts Specialist

Expert en technologie Blockchain et contrats intelligents avec Solidity.

Son expertise technique lui permet d'évaluer et de relever des défis de programmation complexes.

Rafael Romero Carmona
Cloud Architect
DevOps Engineer

Fully passionate in everything related to Cloud, automation and optimisation.

Happy and curious geek on every science you can imagine.

Zhan Wei - 詹玮
Mobile Security Engineer

Anti-hack Expert Lead

Senior Online Developer, Data Analyst at Mobile Game Company

PMP, ITPMP (by MHRSS PRC and MIIT, PRC)

https://www.viadeo.com/p/0021we33g798ou6g?consultationType=29

Marc Rivoal
Software Architect
Engineer

30 d'expérience dans l'informatique de gestion, dans le domaine du retail.

Définition d'architectures logicielles, modélisation de processus, modélisation de données, gestion de projet, conception, …

https://www.viadeo.com/p/00239wo68mpxnyl

Kevin Vanstaen
Social Animator
Blockchain enthusiast

Producteur de contenu digital depuis 2013, je m'informe et je participe à mon échelle à l'émancipation de la blockchain.

Henry Morera
Social Animator

Coach en développement personnel, je suis aussi curieux de tout ce qui touche aux technologies.

Intéressé par les crypto-monnaies, ma participation à ce projet est l'occasion d'avoir un rôle actif dans ce domaine.

Sonia Montella
Social animator

Quelle chance de participer à ce projet ambitieux et nécessaire : offrir une plateforme fiable et ergonomique pour enfin trader en toute confiance et à moindre coût les crypto-monnaies.

Je réponds à toutes vos questions

À très vite sur les réseaux sociaux!

Lulia Galea
Social Animator

Mon nom est Valentina et je suis impatiente de vous rencontrer.
Je m'intéresse à la cyber-sécurité, comment les espaces virtuels sont créés et comment nous pouvons les protéger contre les cybers attaquants.

Ma curiosité me conduit à acquérir différentes compétences techniques, ce qui fait de moi une meilleure experte de jours en jours.

C'est pourquoi nous sommes tous réunis ici, pour créer et vous offrir l'endroit le plus sûr pour vos transactions.

http://www.viadeo.com/p/002yt8g1ptm426v

CONSEILLERS

Renaud Desportes
PDG de DoCaption
Directeur du développement

Plus de 25 ans d'expérience internationale dans la gestion de produits, y compris le développement de matériel et de logiciels.

Forte expérience dans l'établissement et le maintien de relations avec les clients : développement de stratégies commerciales et marketing, extension des réseaux de revendeurs dans le monde entier, avant-vente, support client et formation.

Edouard Enault
Analyste financier
PDG d'Aeroshot

Spécialiste des marchés financiers (analyste sell-side) et fondateur du spécialiste du tournage aérien Aeroshot (aeroshot.fr).

Blockchain enthousiaste et investisseur crypto depuis 2016.

Richard Shibi
Advisor

Richard Shibi a plus de 15 ans d'expérience dans l'industrie des TI.

Il a été consultant senior en gestion et chargé de compte régional pour des projets informatiques déployés à l'échelle mondiale dans l'industrie des télécommunications (Amérique du Nord, Europe, Russie, Moyen-Orient, Chine et Afrique du Sud).

https://www.linkedin.com/in/richardshibi/

ASPECTS LEGAUX

IMPLICATIONS LÉGALES AVEC LE JETON SSW

Nous ne pouvons garantir les évolutions futures du prix du jeton SSW, ni son éventuelle présence dans les listings des échangeurs ni la possibilité de le revendre. La possession de jetons ne donne aucun droit de participation, contrôle ou décision concernant la société *Grey Matter Technologies SpA*. Quelle que soit l'issue de l'ICO, le jeton 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, de gouvernance autonome (DAO), hors du contrôle de la société *Grey Matter Technologies SpA*, le jeton Secure Swap est un jeton « Security », classification par défaut au sens de la SEC, servant de preuve d'enjeu pour sécuriser les échanges au sein du système ouvert. Il permet de réaliser des profits et sert principalement de garantie pour la sécurité des échanges.

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

De ce fait, **il revient aux investisseurs de s'assurer, selon leur pays de résidence, de 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 jeton.

Pour les ressortissants Américains, il leur revient de **vérifier auprès de la SEC la légalité de participer à cette ICO**. En raison de la nature « Security » par défaut du jeton SSW, seuls les investisseurs confirmés peuvent participer à cette 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 et ceux de tous les autres pays en général, il leur revient de **vérifier auprès des autorités régulatrices locales de la légalité de participer à cette ICO**.

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

Ce type de node implique une structure juridique 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'ÉCHANGEUR

- L'échangeur, c'est-à-dire les nodes passerelles, les nodes d'arbitrage et les nodes de conversion vers les devises fiat, supportés par nous-même, sera exploité par la société *Grey Matter Technologies SpA* : www.greymattertechs.com
- La société *Grey Matter Technologies SpA* est une société de juridiction Chilienne.

  https://www.conservador.cl/portal/indice_comercio

  Fojax: 60729 n° 31132 año 2018

- Nous encourageons tout volontaire à soutenir le système en faisant fonctionner ses propres nodes passerelles, les nodes d'arbitrage, les nodes de trading sur marge, 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'exploitation 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) communautaire. Il est développé par la société *Grey Mater Technologies SpA*, 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-monnaies 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, ainsi que l'USD et l'EUR. 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 passerelles, et donc supporteront le fonctionnement du service, recevront, au prorata des jetons SSW qu'ils auront assignés à ce node, leur part des frais d'échanges payés par les traders. Ils seront donc rémunérés automatiquement pour cela.

Q6 : Comment assigner des jetons SSW à un node ?

R6 : Dans la configuration du node, on indique le wallet contenant les jetons SSW que l'on assigne à ce node. Ce même wallet ne peut être assigné qu'à un node à la fois. Les jetons assignés au node sont transférés vers un wallet géré par un smart contract, et seront rendus à l'arrêt du node. Ils servent de garantie aux échanges.

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

R7 : La société *Grey Matter Technologies SpA* lance cette ICO (Initial Coin Offering) en émettant ces jetons SSW. Par la suite, ces jetons 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 jetons SSW assignés.

Par exemple, si un node passerelle est lancé sur la blockchain EOS, et qu'un wallet contenant 10 jetons SSW lui est assigné, et que l'ensemble des nodes passerelles sur la blockchain EOS ont ensemble 100 jetons SSW assignés, 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 le wallet EOS préalablement indiqué.

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

R9 : Comme les NodeOwners, la société fera fonctionner des nodes p2p en y assignant les jetons 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 jetons pendant l'ICO, se retrouverait-elle sans jeton SSW ?

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

Q11 : La société *Grey Matter Technologies SpA* 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 juridique, et de se conformer aux réglementations du lieu où ces échanges sont opérés. La société *Grey Matter Technologies SpA* 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, Secure Trade, dédiée au trading, qui s'appuie sur le réseau des nodes passerelles. Cette application profite de notre expérience en développement de logiciels boursiers professionnels. Son ergonomie sera bien meilleure que les plateformes actuelles, et propose un ensemble d'outils et d'aide au trading novateurs dans le monde des crypto-monnaies.

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 clients participantes à un échange. Si les nodes répondent différemment, c'est qu'il y a une tentative de piratage ou un dysfonctionnement. Dans ce cas, un système basé sur une preuve d'enjeu, élimine les nodes non conformes en les déconnectant.

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 jetons SSW assignés à son fonctionnement. Les nodes répondant différemment sont déconnectés. Ainsi, pour tenter de voler une transaction, il faudrait investir une quantité de jetons SSW représentant plus de la moitié des jetons assignés aux nodes passerelles vers cette crypto-monnaie. Ce qui représente une valeur supérieure au vol d'une transaction. Ce vol n'a de toutes façons aucune chance de réussir puisque, dès qu'il y a détection d'anomalie, la transaction est annulée. De plus, si l'opérateur d'un tel node gardait les contreparties des transactions, leurs valeurs seraient débitées des jetons SSW assignés en garantie sur ce node pour un montant équivalent, convertis dans la crypto-monnaie attendue par le trader et envoyés à ce dernier. Si le pirate y mettait des moyens importants pour prendre le contrôle de tous les nodes passerelles, cette opération serait finalement perdante pour le pirate, sûrement très couteuse, compte tenu du nombre de jetons qu'il devrait engager pour réaliser cela et qui seraient perdus pour lui. L'opération consisterait pour le pirate à acheter toutes les crypto-monnaies qu'il détourne au prix du marché et supporter tous les frais engendrés par ces opérations. Les traders, eux, continuent à recevoir les contreparties de leurs échanges tel que prévu.

Q15 : Si les nodes sont piratés 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 Secure Trade attend la confirmation de tous les nodes passerelles vers une crypto-monnaie pour effectuer un envoi d'actifs, 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. Au final, le pirate paye le détournement des contreparties qui sont par conséquent toujours délivrées aux traders. Et son node est déconnecté du réseau.

Q16 : Quelles autres mesures sont prises pour lutter contre les pirates ?

R16 : Outre les protocoles décrits dans les réponses précédentes, et outre le fait que tout le projet Secure Swap est disponible à tous sous Licence Open Source, nous lançons des campagnes de Bug Bounty tous les 3 mois avec récompenses à la clé pour ceux qui trouveraient une faille dans le système.