



SECURE SWAP LIBRO BLANCO

Grey Matter Technologies
www.secure-swap.com



Libro Blanco Secure Swap

SECURE SWAP LIBRO BLANCO



MENCIONES LEGALES

El objetivo de este Libro Blanco es presentar el proyecto Secure Swap a los interesados en adquirir tokens del proyecto de lanzamiento de esta ICO. La información presentada a continuación puede no ser exhaustiva y no implica ningún elemento de relación contractual. Su único propósito es proporcionar información pertinente y razonable a los potenciales titulares de tokens, para que puedan determinar si deben realizar un análisis profundo de la empresa con el fin de adquirir los tokens SSW.

Ningún contenido en este Libro Blanco se considerará como un documento publicitario o una solicitud de inversión, ni se referirá en modo alguno a una oferta o solicitud de una oferta de compra de valores en ninguna jurisdicción. Este documento no está escrito, de acuerdo o sujeto, a las leyes o regulaciones de ninguna jurisdicción que tenga la intención de proteger a los inversionistas ni está sujeto a esto.

Ciertas declaraciones, estimaciones e información financiera contenida en este Libro Blanco constituyen declaraciones o información a futuro. Dichas declaraciones o información a futuro implican riesgos e incertidumbres conocidos y desconocidos que pueden hacer que los eventos o resultados reales difieran materialmente de las estimaciones o resultados expresados o implícitos en dichas declaraciones a futuro. Dichas declaraciones o información a futuro no constituyen una promesa ni una obligación.

Los acontecimientos futuros descritos en este Libro Blanco no pueden considerarse como una promesa de beneficios y/o como una previsión garantizada de crecimiento del token SSW. Los cálculos proporcionados se basan únicamente en leyes matemáticas fundamentales.

Este Libro Blanco en español es una traducción del documento de referencia que está escrito en francés. La versión francesa es la fuente oficial de información sobre el token SSW. Durante esta traducción, y a pesar de nuestros esfuerzos por corregirla, parte de la información contenida en este documento puede perderse o distorsionarse. La exactitud de esta traducción no puede ser garantizada. En caso de conflicto o incoherencia entre esta traducción y el Libro Blanco en francés, prevalecerán las disposiciones del documento original en francés.

CUALQUIER PERSONA QUE COMPRE TOKENS SSW RECONOCE Y DECLARA EXPRESAMENTE QUE HA REVISADO CUIDADOSAMENTE ESTE LIBRO BLANCO Y QUE HA COMPRENDIDO PERFECTAMENTE LOS RIESGOS, COSTOS Y BENEFICIOS ASOCIADOS CON LA COMPRA DE TOKENS SSW.



CONTENTS

MENCIONES LEGALES.....	2
PRESENTACIÓN DE SECURE SWAP	5
Introducción.....	5
ESTADO DEL MERCADO.....	6
Exchanges centralizados	6
Exchanges descentralizados.....	6
Comparación de las cuotas de mercado	9
Ejemplos de soluciones a la falta de liquidez propuestas por diferentes DEX.....	11
SOLUCIONES PROPORCIONADAS POR SECURE SWAP	12
Resumen de los puntos fuertes de Secure Swap	13
Liquidez	13
Rapidez.....	13
Seguridad	13
Disponibilidad:	13
Una plataforma controlada y operada por una comunidad:	14
Plataforma extensible:	14
Una fuente de ingreso para los que apoyan su funcionamiento:	14
Una plataforma mundial:	14
Avanzadas ergonomía y herramientas de trading	14
Una plataforma con costos ventajosos para el usuario	14
ARQUITECTURA Y OPERACIÓN DE LA PLATAFORMA	16
Sistema de arbitraje que garantiza la disponibilidad de liquidez.....	18
Requisitos para conectar un nodo de arbitraje a la red.....	18
Funcionamiento de un nodo de arbitraje	18
Nodos pasarelas y nodeowners	20
Pre requisitos para poder conectar un nodo de pasarela a la red p2p.....	20
Seguridad de los intercambios, utilización de tokens ssw puestos como garantía y retribución a los nodesowners.....	20
Nodo margen de trading.....	24
Requisitos para poder conectar un nodo de margen de trading a la red p2p	24
Funcionamiento del nodo de margen de trading	25
Nodo de cambio a moneda fiduciaria	29
Sistema de detección de anomalías o intentos de piratería informática	30
Sistema que garantiza la atomicidad y la seguridad de los intercambios.....	33
Rendimiento del intercambiador	35



Libro Blanco Secure Swap

Indicación del estado del intercambiador.....	36
Indicaciones mostradas por la aplicación cliente.....	36
Indicaciones accesibles desde los nodos pasarelas	36
Comercio seguro, la aplicación cliente de trading	37
Connexion	37
Los wallets.....	37
Gráficos, datos en tiempo real	38
La cartera de órdenes	38
Herramientas de trading.....	39
Margen de trading	39
Trading automático.....	39
¿CÓMO COMPENSAR LA FALTA DE LIQUIDEZ INICIAL ?.....	41
UNA PLATAFORMA CON CÓDIGO ABIERTO	42
PROGRAMA DE BUG BOUNTY	43
ASPECTO FINANCIERO DE TOKEN	44
Datos utilizados para esta proyección:	44
Proyección de la rentabilidad de la inversión en token ssw:	45
Conclusiones:	47
ICO, EL TOKEN ERC-20 SECURE SWAP (SSW)	48
¿Por qué un ico y la creación de un token erc-20?	48
Datos del ICO.....	48
ASIGNACIÓN DE FONDOS:	50
Soft cap alcanzado:	50
Hard cap alcanzado:.....	51
ROADMAP	53
Roadmap ICO	53
Roadmap Secure Swap.....	54
TEAM:.....	55
Miembros fundadores.....	55
Equipo	56
Consultores	58
ASPECTOS LEGALES	59
Implicaciones legales con tokens ssw	59
LA COMPAÑÍA QUE EXPLOTA LA PLATAFORMA	60
FAQ.....	61
FAQ Secure Swap:	61



PRESENTACIÓN DE SECURE SWAP

INTRODUCCIÓN

¿Una plataforma de intercambio más? ¡El mercado está saturado con ellas!

No, Secure Swap no es sólo otra plataforma de intercambio descentralizada (DEX). ¡Sus características lo hacen único! Combina las ventajas de los intercambiadores centralizados y descentralizados: liquidez, rapidez de ejecución, no requiere de confianza en terceros, resistencia a la piratería, resistencia a las prohibiciones y regulaciones contra las criptomonedas.

La plataforma Secure Swap es de código abierto (open source) y sin servidor central. Es operada por la comunidad, y por lo tanto no requiere de una compañía operadora para funcionar.

Su arquitectura es altamente modular, lo que permite añadir servicios (soporte de criptomoneda, soporte de intercambio de fiat e integración de medios de pago (cash-in/cash-out), soporte de proveedores de liquidez). De este modo, los desarrolladores y empresarios pueden unirse y ampliar la comunidad Secure Swap.

Gracias a su funcionamiento comunitario, Secure Swap permite a los NodeOwners (usuarios que operan uno o más nodos de pasarela) obtener una fuente de ingresos.

Su arquitectura protege el corazón del sistema de las regulaciones y las prohibiciones súbitas de las criptomonedas. Dependiendo de su lugar de residencia, estas regulaciones pueden ser un riesgo para aquellos que poseen criptomonedas. Secure Swap ofrece una puerta de salida que está siempre disponible.

Para las divisas digitales que lo permiten, Secure Swap respeta plenamente el anonimato al intercambiar criptomonedas entre ellas. Sin embargo, gracias a su modularidad y a la clara separación de los diferentes sistemas de intercambio, Secure Swap también permite cumplir plenamente la normativa local a la hora de cambiar criptomonedas por monedas fiduciarias.

La apertura de Secure Swap a los intercambios cripto-fiat también permite, a quienes deseen operar desde una estructura legal, una actividad profesional de intercambio de criptomonedas a divisas fiduciarias, en las monedas de su elección. Secure Swap es de código abierto y proporciona modelos de nodos listos para ser adaptados a la normativa local.

Su protocolo de funcionamiento incluye sistemas de detección de anomalías. Cada anomalía provoca la desconexión de la red de la parte que falla y el uso, si es necesario, de la garantía de token SSW para poner fin a un intercambio en curso. Estas anomalías pueden ser causadas por un intento de piratería o por el mal funcionamiento de algunos nodos.

Su aplicación cliente de trading, Secure Trade, ofrece un nivel de comodidad y ergonomía comparable al mejor software de trading de los mercados de valores tradicionales (órdenes gráficas, money management, asistencia en el scalping, módulo de trading automático programable, etc.).



Libro Blanco Secure Swap

Nuestro objetivo al proponer "un intercambiador más" es construir una plataforma de nueva generación que, por primera vez, combine todas estas características. Y es sólo reuniendo todas estas características antes mencionadas, que un DEX puede pretender destronar los intercambiadores centralizados.

ESTADO DEL MERCADO

Principales características de las plataformas de exchanges centralizadas y descentralizadas:

PLATAFORMAS CENTRALIZADOS

Ventajas:

- Buena liquidez, incluso muy buena en las más grandes plataformas. Lo cual garantiza una alta profundidad de mercado y un "slippage¹" de precios limitados.
- Una buena velocidad de ejecución de las órdenes, gracias a una cartera de órdenes centralizada y a la liquidez disponible.
- En su mayor parte, una amplia gama de criptomonedas intercambiables.
- Para algunas personas la posibilidad de operar con márgenes en el trading.

Desventajas:

- Transferencia de la propiedad de los activos digitales a estas plataformas que sirven como terceros de confianza.
- Esta centralización de activos es muy atractiva para los hackers. Esto hace que la piratería sea muy perjudicial, tanto para la empresa que opera la plataforma, como para sus clientes.
- Riesgo de cierre repentino, haciendo inaccesibles los activos depositados allí. Estos cierres pueden ser causados por una bancarrota del operador de la plataforma o por una regulación estatal hostil a las criptomonedas.
- Frecuente indisponibilidad de servicios durante períodos de pánico en los mercados.
- El retiro de los activos implica un doble costo: las tarifas habituales de la red, más las tarifas añadidas por la plataforma por el retiro.

PLATAFORMAS DESCENTRALIZADOS

Ventajas:

- No hay terceros de confianza.
- No hay centralización de los activos, por lo tanto, no es muy atractivo para los hackers, y también más difícil de piratear.
- Algunos son resistentes a la quiebra de sus operadores y a los riesgos de regulación, pero son pocos².

Desventajas:

- Insuficiente liquidez para asegurar la presencia de una contraparte. Esto también causa un alto riesgo de slippage de los precios y una ejecución lenta de las órdenes.
- La lentitud en la ejecución de las órdenes se debe directamente a su modelo de arquitectura distribuida, al funcionamiento de sus carteras de órdenes y de su sistema de matching.
- La mayoría de ellos tienen una selección limitada de criptomonedas intercambiables. Muchos se limitan a intercambiar sólo dentro de la red Ethereum (Ether y tokens).



Libro Blanco Secure Swap

- Las carteras de órdenes y el matching de órdenes ejecutadas mediante contratos inteligentes (On-Chain), significan costos de tarifas de red (gas en Ethereum) incluso si estas órdenes no se ejecutan. Peor aún, también hay costos asociados con la cancelación y la modificación de órdenes.

Lo que resulta de esta comparación:

Puede verse que los DEXs no están exentos de desventajas en comparación con las plataformas centralizadas, lo cual limita su utilización.

La falta de liquidez es la principal razón de la no adopción masiva de DEXs, y los usuarios consideran que la profundidad del mercado de las plataformas centralizadas es más atractiva que los todos los beneficios de los DEXs.

La lenta ejecución de las órdenes es también una de las razones de la no adopción masiva de DEXs, pero es una causa menos importante que la falta de liquidez.

La ausencia de márgenes en el trading es también una razón de no elección de DEXs, al menos para los traders que practican este tipo de trading en criptomonedas.

Ningún DEX actual tiene estas dos características juntas (liquidez y rapidez). Aquellos que lo hacen y afirman ser DEXs, basan su liquidez en el hecho de que la empresa operadora es la contraparte intermediaria de las plataformas. La empresa intercambia las criptomonedas por sus tokens según la tarifa de intercambio que ella misma decide. Es la empresa operadora la que generalmente elige el tipo de cambio de sus tokens frente a todas las criptomonedas disponibles, a veces mediante una fórmula ad hoc, a veces simulando incluso un mecanismo de slippage de precios, totalmente a su favor, lo que induce costos ocultos.

Estos tokens, que sirven como contrapartidas intermedias, también constituyen una concentración de activos. Por lo tanto, estos intercambiadores corren el mismo riesgo de ser pirateados que los intercambiadores centralizados (ejemplo: Bancor, que ha sido pirateado, lo que resultó en el robo de 1/3 de sus tokens de contraparte).

¹ Slippage es la diferencia de precio entre el precio al que desea comprar o vender y el precio al que se ejecuta su orden en una plataforma de trading.

² Para que un DEX sea resistente a la quiebra de su operador y a los riesgos de prohibición, su arquitectura debe ser descentralizada, autónoma o con un gobierno descentralizado. Pero, y este es un punto que a menudo se olvida, su sistema de entrega de órdenes también debe ser resistente. Este no es en absoluto el caso de todos los DEXs que utilizan un sitio web para realizar sus entregas de órdenes. Estos



Libro Blanco Secure Swap

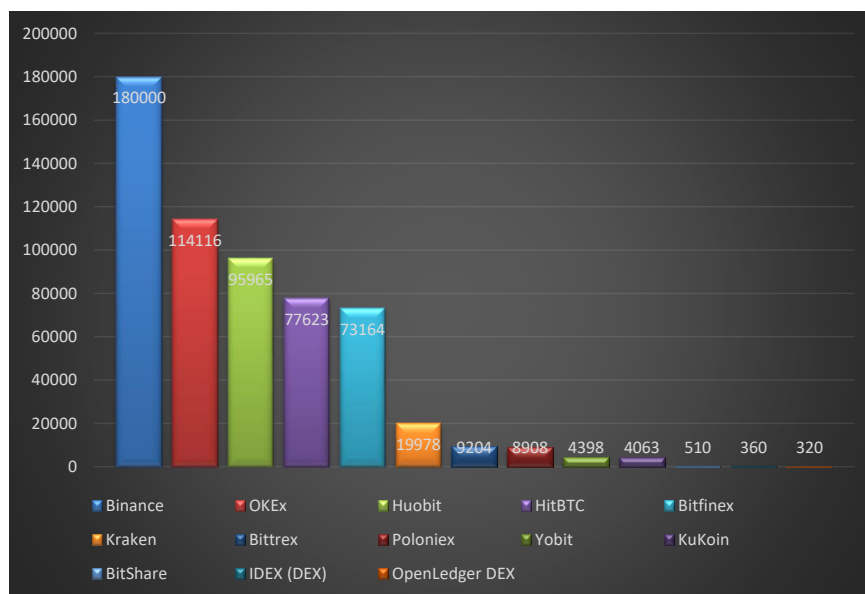
sitios pueden ser prohibidos o cerrados después de un cambio regulatorio o la bancarrota de la compañía que opera el sitio web; o incluso ser inaccesibles debido a un simple ataque de DDOS. Sólo los DEXs descentralizados, autónomos y con una aplicación cliente para entregar las órdenes, cumplen este criterio. Estos DEXs no son numerosos (Altcoin.IO, BarterDex, Bisq, Stellar Dex entre los principales), y ellos también están sujetos a problemas de liquidez.



COMPARACIÓN DE LAS CUOTAS DE MERCADO

A pesar de sus respectivas ventajas, un estudio de las cuotas de mercado muestra que los DEXs son significativamente inferiores en términos de volumen intercambiado en comparación con las plataformas centralizadas.

Comparación de volumen de intercambio diario entre plataformas centralizadas y descentralizadas:

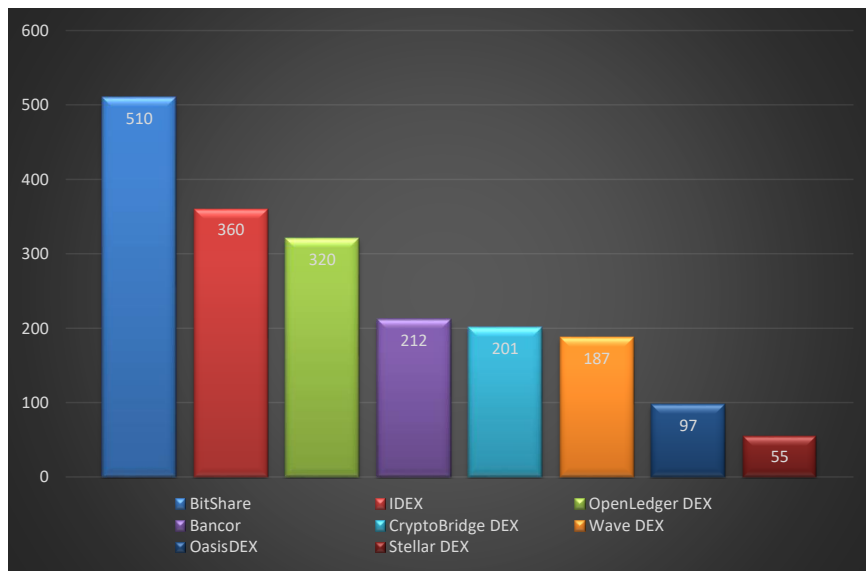


Este gráfico muestra los volúmenes de intercambio de algunas plataformas centralizadas y de las tres plataformas descentralizadas que presentan el mayor volumen.

Los volúmenes de DEXs BitShare, IDEX y OpenLedger son muy pequeños en comparación con las plataformas centralizadas y no son visibles en el gráfico.



Comparación de volumen de intercambio entre plataformas descentralizadas:



Conclusión:

¡Esta comparación entre intercambiadores centralizados y descentralizados es incuestionable!

¿Cuál es la principal diferencia, responsable de esta situación, y compartida por todos los DEXs?

No tienen la suficiente liquidez. Cualesquiera que sean sus ventajas, esta falta de liquidez los condena a desempeñar un papel anecdótico.

Algunos tratan de superar este problema de liquidez, como Bancor y otros, pero sus soluciones o bien no proporcionan realmente liquidez o bien transforman a DEX en un «market maker¹» que impone sus tasas de cambio, de modo que los usuarios pierden el control sobre el precio de sus transacciones.

¹ Un intermediario financiero que hace precios, ofrece un precio de compra y venta sobre un activo financiero.



EJEMPLOS DE SOLUCIONES A LA FALTA DE LIQUIDEZ PROPUESTAS POR DIFERENTES DEX

Altcoin IO:

Proporciona un sistema para compartir la liquidez entre DEXs a través de una API. Este sistema puede convertirse en una muy buena solución a largo plazo, cuando los DEXs tengan liquidez para compartir....

Para Altcoin IO, ésta solución no proporciona liquidez inmediata.

Bancor:

"Market Maker" utiliza sus tokens como contrapartida de todos los intercambios. Esto ofrece una liquidez siempre disponible, fijando las tasas de cambio e incluso añadiendo un slippage artificial de los precios durante el intercambio en función del volumen negociado. ¿El problema de liquidez está resuelto, pero a qué precio?: los usuarios ya no tienen el control sobre el precio de cambio de sus transacciones. Además, el sistema de fijación de tasas de cambio no es transparente y puede convertirse rápidamente en sospechoso.

BarterDex (Komodo platform):

Esta plataforma utiliza un sistema artificial de creación de liquidez ineficaz: la liquidez de la cartera de órdenes se multiplica por el hecho de que las criptomonedas implicadas en una orden en espera de ser ejecutada, siguen disponibles para otras órdenes. Esto crea una profundidad de la cartera de órdenes ficticia que no existe en la práctica. Tan pronto una orden es ejecutada, todas las órdenes basadas en estas mismas criptomonedas, que ya no están disponibles en cantidades suficientes, son canceladas. Lo que igualmente anula esta liquidez artificialmente creada....

Esto induce a errores a los usuarios en cuanto a la liquidez real de disponer.

Estos tres ejemplos describen la mayoría de las soluciones implementadas para tratar de resolver el problema de liquidez, siendo la solución de Bancor la más utilizada: los tokens del proyecto sirven como contrapartida, con o sin una blockchain específica, con las implicaciones antes descritas.



SOLUCIONES PROPORCIONADAS POR SECURE SWAP

La solución de Altcoin.IO será interesante a considerar cuando los DEXs tomen la delantera sobre las plataformas centralizadas, compartiendo su liquidez.

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

Secure Swap tiene previsto implementar la API de Altcoin.IO para compartir su liquidez, con la idea de que esto sea beneficioso para ambas plataformas como para aquellos que se unan a nosotros más adelante.

Mientras tanto, Secure Swap debe tener una forma de obtener liquidez tan pronto como se ponga en servicio. Por eso vamos a buscar liquidez donde está, en las plataformas centralizadas, explotando sus APIs. Nuestro sistema de arbitraje está dedicado a esta tarea. De esta manera, podremos explotar la liquidez de varias plataformas centralizadas, ofreciendo así una liquidez mayor a una sola plataforma centralizada.

¿Por qué esta simple idea no es utilizada por otros DEXs? Porque presenta un inconveniente: requiere un bloqueo significativo de fondos en criptomonedas para cada una de las plataformas centralizadas cuya liquidez se explota. Con este fin, una parte importante de los fondos recaudados en el ICO se dedicará a los nodos de arbitraje.

La velocidad de la correspondencia de las órdenes se obtiene de forma sencilla: todos los nodos de la red (incluyendo la aplicación cliente Secure Trade que también es un nodo), comparten las actualizaciones de la cartera de órdenes.

Cuando un operador añade/borra/modifica una orden a través de Secure Trade, este cambio se transmite a todos los nodos de uno a otro. Al ser una transmisión de diferencia, esto representa muy pocos datos a propagar, lo que hace que globalmente todos los nodos están permanentemente actualizados (un poco como nodos que validan bloques en las blockchains, excepto que aquí el volumen de datos transmitidos es insignificante).

Cada nodo de Secure Trade, efectúa la correspondencia de sus propias órdenes con la cartera de órdenes completa, por lo que obtenemos un rápido "matching" de órdenes (podemos considerarlo como instantáneo), ya que cada nodo de Secure Trade compara sólo una pequeña parte de las órdenes (las pocas órdenes del usuario) con la cartera de órdenes completa. Destacamos que estas operaciones son totalmente gratuitas.

En cuanto a la gama de criptomonedas disponibles, Secure Swap no se limita al ecosistema Ethereum, por lo que podemos ofrecer un gran número de ellas. Su aspecto comunitario, así como la disponibilidad de modelos de nodos de pasarelas (hacia criptomonedas, divisas fiduciarias, nodo de arbitraje) permite a la comunidad Secure Swap añadir soporte para las criptomonedas (y monedas fiduciarias) de su elección.

Secure Swap también permite márgenes de trading, a través de nodos dedicados a esta tarea.

En resumen, Secure Swap es un ecosistema de intercambio de criptomonedas, construido alrededor de un servicio descentralizado, una aplicación de cliente para el trading y micro servicios opcionales para aprovechar las nuevas oportunidades que ofrece esta nueva red. Estos micro servicios son nodos especializados, tales como los nodos de conexión a diferentes blockchains, nodos de conexión a procesadores de pagos para intercambios con monedas fiduciarias, nodos de arbitraje y los nodos de márgenes de trading.

Más detalles se presentan en la sección «ARQUITECTURA Y OPERACIÓN DE».



RESUMEN DE LOS PUNTOS FUERTES DE SECURE SWAP

LIQUIDEZ

- Como acabamos de ver, Secure Swap asegura una liquidez muy elevada, proporcionada por las plataformas centralizadas, gracias a nuestro sistema de arbitraje.
- En el futuro, la liquidez también se verá respaldada ya que las carteras de órdenes entre las plataformas DEXs podrán ser compartidas.

RAPIDEZ

- Cada aplicación cliente realiza la correspondencia de sus órdenes con la cartera de órdenes completa. Esto, combinado con la liquidez disponible, nos asegura una velocidad de ejecución comparable a la de las plataformas centralizadas.
- Su arquitectura y funcionamiento hacen que Secure Swap no dependa de la velocidad de ejecución de los contratos inteligentes en las diferentes blockchains (ver explicaciones en "ARQUITECTURA Y OPERACIÓN DE"). Por lo tanto, Secure Swap es tan rápido como una plataforma centralizada en carga nominal, y probablemente más rápido a alta carga. Secure Swap es sin duda el más rápido de todos los DEXs existentes.

SEGURIDAD

- Sistema asegurado por diseño, con detección de intentos de piratería o mal funcionamiento, y desconexión automática de las partes implicadas.
- Un sistema verdaderamente descentralizado, los usuarios permanecen en posesión de sus criptomonedas hasta el momento de un intercambio.
- Por su naturaleza totalmente descentralizada, Secure Swap no tiene terceros de confianza, y es una DAO ("Organización Autónoma Descentralizada"). Por lo tanto, no hay forma de que los reguladores impidan su uso.
- No hay concentración de criptomonedas. Este es un objetivo principal para los hackers en las plataformas centralizadas, pero también en las llamadas plataformas descentralizadas cuya operación implica la concentración de criptomonedas o tokens.
- El trader tiene la garantía de recibir su contraparte después de un intercambio, incluso si una parte del sistema es defectuosa o pirateada.
- Un sistema abierto y de código abierto que permite a todos controlar su código, funcionamiento y seguridad.

DISPONIBILIDAD:

- Sistema altamente redundante, que garantiza una resistencia a las fallas, por lo tanto, una alta disponibilidad del servicio incluso con una carga importante de órdenes.



UNA PLATAFORMA CONTROLADA Y OPERADA POR UNA COMUNIDAD:

- Su aspecto distribuido y comunitario, hace que el servicio sea independiente de la existencia de la sociedad que lo creó y no necesita de ella para funcionar.

PLATAFORMA EXTENSIBLE:

- Por su naturaleza “open source” y modular, los usuarios que lo deseen pueden agregar a la plataforma el soporte de otras criptomonedas y también agregar intercambios de otras divisas fiduciarias o añadir los medios de pago de su elección.

UNA FUENTE DE INGRESO PARA LOS QUE APOYAN SU FUNCIONAMIENTO:

- Aquellos que apoyan el funcionamiento del servicio (NodeOwners), haciendo funcionar partes del sistema (nodos pasarelas a criptomonedas específicas), son recompensados ganando parte de las tarifas pagadas por los usuarios en los intercambios.
- Aquellos que operan nodos de márgenes de trading también se benefician de esta fuente de ingresos.
- Del mismo modo, los nodos de arbitraje también pueden ser una fuente de ingresos, explotando las diferencias de precios entre las plataformas.
- Gracias a su código abierto, los empresarios podrán desarrollar una actividad comercial de intercambio de criptomonedas por monedas fiduciarias e incluso ofrecer métodos de pago donde sea legal (nodos de conversión a moneda fiduciaria).

UNA PLATAFORMA MUNDIAL:

- El hecho de que la red es accesible desde cualquier parte del mundo para los intercambios de criptomonedas, el apoyo de nuevas monedas fiduciarias y los nuevos métodos de pago añadidos por la comunidad, extenderá gradualmente el servicio a todo el mundo.

AVANZADAS ERGONOMÍA Y HERRAMIENTAS DE TRADING

- Su aplicación cliente, Secure Trade, ofrece herramientas avanzadas de trading que son comunes en el mundo del trading tradicional (mercados de valores, mercados de futuros...).
- Las principales herramientas son: la colocación de órdenes en el gráfico, la asistencia en el «money management», la asistencia en el scalping, un módulo de trading automático programable, por no mencionar la amplia gama de indicadores disponibles y otros modos de representación gráfica.
- Además, Secure Swap ofrece márgenes de trading, que actualmente es casi único para un DEX.

UNA PLATAFORMA CON COSTOS VENTAJOSOS PARA EL USUARIO

- Secure Swap utiliza los contratos inteligentes sólo en caso de anomalías.
- Un intercambio que se efectúa sin fallas ni piratería no va a utilizar los contratos inteligentes.
- Como resultado de la ejecución de órdenes, sus modificaciones y sus cancelaciones de no significan ningún costo para el usuario, a diferencia de la mayoría de los DEXs.



Libro Blanco Secure Swap

- Del mismo modo, la ejecución de una orden no genera ningún costo relacionado con una operación con un contrato inteligente.
- La plataforma tampoco cobra comisiones de retiro, ya que no posee los wallets. Con un cargo único del 0,15% sobre la ejecución de una orden, que puede reducirse en función de criterios de volumen, Secure Swap será tan competitiva como las plataformas centralizadas.

En conclusión, Secure Swap es un ecosistema que proporciona una respuesta eficaz a los problemas de las plataformas centralizadas y descentralizadas. Al igual que los proyectos Omise GO o Stellar Lumens, también ofrece el intercambio de criptomonedas a monedas fiduciarias y la integración simple de métodos de pago a través de un SDK (kit de desarrollo) que permite pagos en monedas fiduciarias y en criptomonedas.

A diferencia de los proyectos que ofrecen estas soluciones globales, no depende del éxito de desarrollos en curso como Plasma, Lightning Network, Sharding o Atomic Swap para proporcionar una funcionalidad equivalente.



ARQUITECTURA Y OPERACIÓN DE LA PLATAFORMA

Para abordar los problemas identificados, Secure Swap aplica soluciones que proporcionan las ventajas de las plataformas centralizadas y descentralizadas, sin las desventajas que estas presentan.

Secure Swap dispone de una seguridad reforzada "**por diseño**".

La arquitectura de los nodos asegura una posibilidad de aumento de capacidad y redundancia, garantizando el funcionamiento y disponibilidad del servicio.

Secure Swap no presenta ninguna de las desventajas de las plataformas centralizadas o descentralizadas.

Secure Swap es también un sistema abierto que permite a todo el mundo controlar su código, el funcionamiento, la seguridad, como también de participar en su funcionamiento dando soporte a los nodos de pasarela a las criptomonedas.

Las comisiones de intercambio se redistribuyen en su totalidad a quienes operan este tipo de nodos (NodeOwners), en proporción a los tokens SSW que poseen. Por lo tanto, es una importante fuente de ingresos para todos aquellos que deseen invertir en el token SSW.

La arquitectura de red distribuida se basa en un núcleo de aplicación JavaScript basado en Node.JS. Constituye la base común para la comunicación p2p², que se utilizará para los distintos módulos del ecosistema: aplicación cliente de trading, nodos pasarelas a blockchains, nodos de arbitraje responsables de asegurar la liquidez de la plataforma, nodos de intercambio cripto/fiat.

Secure Trade y los nodos se comunican entre sí a través de la tecnología Peer to Peer (p2p), lo que constituye un servicio descentralizado.

Sólo Secure Trade conoce las claves privadas de los wallets de los usuarios. De este modo, puede firmar las transacciones destinada a la blockchain (firma "offline"). Como resultado, nadie puede firmar transacciones en lugar de Secure Trade. El usuario sigue siendo el propietario de sus criptomonedas, a diferencia de las plataformas centralizadas en las que el trader les transfiere sus criptomonedas almacenadas haciendo que estas plataformas se conviertan así en los verdaderos propietarios de las claves privadas y criptomonedas almacenadas.

En cuanto el usuario se desconecta del servicio de intercambio, sale de la aplicación cliente. Las claves privadas de sus wallets, que se almacenan localmente en su computador, están realmente desconectadas (equivalente a un "cold storage"). Las claves privadas de sus wallets nunca se transmiten por Internet y nunca han salido de la aplicación cliente.

Además, si el usuario tiene wallets de hardware (Ledger, Trezor, etc.), las llaves privadas correspondientes a sus wallets nunca se almacenan en su computador, sino que permanecen seguras en sus wallets de hardware.

Tan pronto como el usuario conecta Secure Trade a la red p2p, está listo para operar/intercambiar sus criptomonedas, sin costos innecesarios de transferencia a una plataforma previamente, al tiempo que dispone de una seguridad comparable al de almacenaje de sus activos en un "cold storage".

² Peer 2 Peer: El peer-to-peer es un modelo de red informática similar al modelo cliente-servidor, pero donde cada cliente es también un servidor. Los peer-to-peer pueden ser centralizados o descentralizados. Se puede utilizar para compartir archivos de igual a igual, al cálculo distribuido o a la comunicación.



Libro Blanco Secure Swap

La aplicación cliente Secure Trade ofrece facilidad de uso y ergonomía comparable con el mejor software de trading existentes (mercados de valores, contratos de futuros, Forex, etc.). Secure Trade ofrecerá, en particular, las llamadas órdenes "avanzadas", como las órdenes de rango de activación, las órdenes condicionales de múltiples rangos, las órdenes OCO, etc., así como la negociación en el gráfico con órdenes condicionales al cruzar líneas horizontales o pendientes, órdenes sobre indicadores, un módulo de apoyo al money management, así como un módulo automático de trading programable y, por último, los márgenes de trading.

Cada aplicación cliente envía las órdenes generadas por el usuario a los nodos conectados, lo que permite su consolidación. Los nodos propagan todas las órdenes recogidas de un nodo a otro cada vez que hay un cambio, de modo que cada nodo tiene la cartera de órdenes completa. Como Secure Trade también es un nodo, también recibe todas las órdenes emitidas en la red p2p. Esta propagación de actualizaciones de la cartera de órdenes sólo transmite las diferencias, modificaciones, supresiones y agregar nuevas órdenes. Es muy rápida y parece instantánea desde el punto de vista del cliente.

Cada aplicación de cliente compara sus propias órdenes con la cartera de órdenes completa para encontrar las contrapartes de las órdenes que el operador ha emitido.

Cuando se encuentra una coincidencia, Secure Trade informa a los nodos a los que está conectado. Los nodos validarán la coincidencia, lo que desencadenará el proceso de intercambio (ver explicación detallada más adelante).

Para la seguridad de los intercambios, un sistema de garantía descrito en el capítulo "Nodos pasarelas y nodeowners", así como el control de las operaciones de todos los nodos, permiten garantizar el buen funcionamiento de los distintos nodos de la red, así como la seguridad de los intercambios en un entorno « trustless³ ».

Por último, Secure Swap se basa completamente en tecnologías existentes, funcionales y probadas. Por lo tanto, el proyecto no soporta el riesgo de fallo de las tecnologías en curso como, por ejemplo, el plasma. Esto reduce en gran medida el riesgo de fracaso del proyecto debido a las tecnologías de terceros que han fallado.

³ Las partes relacionadas no necesitan tener confianza entre ellas, ni requieren de un tercero de confianza, ya que toda la información procesada en la red se verifica de forma independiente.



SISTEMA DE ARBITRAJE QUE GARANTIZA LA DISPONIBILIDAD DE LIQUIDEZ

El sistema de arbitraje consiste en un conjunto de nodos de arbitraje. Como son nodos, tienen la cartera de órdenes Secure Swap actualizada, como todos los demás nodos.

Cada nodo de arbitraje está especializado en el uso de la API de la plataforma centralizada al que está destinado.

Estas especializaciones se refieren a la implementación de la API específica de la plataforma y a sus reglas específicas de uso (como el tiempo mínimo entre dos llamadas a la API...).

REQUISITOS PARA CONECTAR UN NODO DE ARBITRAJE A LA RED

Para poder operar este tipo de nodos es necesario disponer de un capital distribuido en todas las criptomonedas cuyo nodo de arbitraje asegure liquidez a Secure Swap.

Este capital debe repartirse a partes iguales entre las wallets gestionadas por el nodo de arbitraje de la red Secure Swap, y entre las wallets de la plataforma centralizada, cuya liquidez quiere ser explotada.

También requiere una máquina confiable y segura que dispone de una conexión estable a Internet.

Igualmente, es necesario obtener la aplicación de nodo de arbitraje adaptada a la plataforma que se desea explotar, o eventualmente haber desarrollado una especialización propia basada en el modelo de nodo proporcionado en "Open Source".

FUNCIONAMIENTO DE UN NODO DE ARBITRAJE

El nodo de arbitraje recupera y actualiza la cartera de órdenes de la plataforma centralizada que ella explota, para todas las criptomonedas que gestiona, y busca posibles contrapartidas entre las dos carteras de órdenes.

Tan pronto como se encuentra una coincidencia entre las dos carteras de órdenes, el nodo de arbitraje reserva la orden correspondiente de la cartera de órdenes Secure Swap. Una vez confirmada la reserva, realiza una operación inversa sobre la plataforma centralizada que la explota.

Ejemplo: si en la cartera de órdenes Secure Swap hay una orden de intercambio de 1 BTC por 30 ETH, y en la cartera de órdenes de la plataforma centralizada que la explota hay una orden de intercambio de 32 ETH por 1 BTC, entonces el nodo de arbitraje emitirá una orden de intercambio de 1 BTC por 32 ETH en esa plataforma centralizada.

Para esta transacción, Secure Swap utiliza las reservas de criptomonedas que se encuentran en la wallets de la plataforma centralizada, que pertenecen al operador del nodo de arbitraje.



Libro Blanco Secure Swap

Una vez realizada esta operación en esta plataforma centralizada, el nodo de arbitraje enviará una orden de intercambio de 30 ETH por 1 BTC en la cartera de órdenes de Secure Swap, lo que provocará el intercambio en Secure Swap con la orden previamente reservada, utilizando las reservas de criptomonedas que se mantienen en las wallets del nodo de arbitraje en Secure Swap, las que también pertenecen al operador del nodo.

Así, al final de la operación, se ejecutó la orden que no tenía contrapartida en nuestra cartera de órdenes (1 BTC contra 30 ETH). Las wallets del nodo de arbitraje en Secure Swap tienen 1 BTC más y 30 ETH menos. Las wallets del nodo de arbitraje en el lado de la plataforma centralizada que la explota, tiene 1 BTC menos y 32 ETH más. En general, el nodo de arbitraje ganó 2 ETH en esta operación.

Estas potenciales ganancias:

- Se utilizan para pagar a quienes van a hacer funcionar este tipo de nodo.
- Compensan los riesgos de tipo de cambio asumidos por el operador de un nodo de arbitraje.
- Compensan los costos operativos de este tipo de nodo (tarifas de servidor, Internet).
- Permiten el pago de comisiones en la plataforma centralizada que la explota y en Secure Swap.

Por lo tanto, no hay costos adicionales para el trader cuando su orden ha sido ejecutada a través del aporte de liquidez externo por vía nodo de arbitraje. Cualquier ganancia generada por una diferencia de precio entre las plataformas, beneficia al operador del nodo de arbitraje.

Un nodo de arbitraje también puede realizar intercambios sin ganancia para él, esto se puede establecer en las opciones de configuración del nodo de arbitraje.

Regularmente, el nodo de arbitraje debe equilibrar sus wallets en Secure Swap con las gestionadas por la plataforma centralizada para así mantener una buena distribución de las criptomonedas disponibles. La frecuencia del rebalanceo depende del stock de criptomonedas disponibles para el funcionamiento del nodo, y también de la tendencia de las transacciones a compensarse o no.

Este reequilibrio se llevará a cabo automáticamente sobre la base de criterios de cantidad mínima de reserva para cada criptomoneda, y se llevará a cabo mediante la realización de operaciones de transferencia con la plataforma externa. Estos criterios serán configurables a nivel de nodo de arbitraje.

Cabe señalar que un operador de nodos de arbitraje no necesita hacer funcionar un nodo de blockchains, sino que depende enteramente de la red Secure Swap y de la API de la plataforma externa, cuya liquidez se explota de este modo.

Un nodo de arbitraje puede operar con reservas de criptomonedas relativamente modestas, pero su eficiencia económica y su capacidad para proporcionar liquidez aumenta con las reservas de criptomonedas disponibles (frecuencia del balance requerida, capacidad para procesar grandes transacciones de valor en cada criptomoneda).

Grey Matter Technologies SpA operará los nodos de arbitraje a las plataformas centralizadas programadas utilizando sus API con una reserva suficiente de criptomonedas para garantizar un funcionamiento óptimo. También proporcionaremos un modelo de nodos listo para ser adaptado a otras plataformas, así como nodos de arbitraje listos para usarse en código abierto.

Es en este modelo de nodo de arbitraje, adaptado para la utilización de la API de Altcoin.IO, donde Secure Swap compartirá su liquidez con las plataformas que también implementarán esta API para compartir liquidez entre DEXs.



NODOS PASARELAS Y NODEOWNERS

Los nodos pasarelas son los nodos que proporcionan comunicación entre la red p2p Secure Swap y los nodos de blockchains.

Hay un tipo de nodo pasarela por blockchain (uno para la blockchain Ethereum, otro para Neo, otro para Bitcoin, etc.).

Para que se permitan los intercambios, el comercio seguro requiere que al menos dos nodos de pasarela para activar una blockchain en la red. Si este no es el caso, entonces el trading en la criptomoneda correspondiente será desactivado.

Los NodeOwners son las personas o entidades que eligen hacer funcionar los nodos pasarela, convirtiéndose así en miembros activos de la comunidad Secure Swap.

Grey Matter Technologies SpA actuará como NodeOwner, sin ningún privilegio particular, al igual que cualquier miembro de la comunidad que decida asumir este rol.

PRE REQUISITOS PARA PODER CONECTAR UN NODO DE PASARELA A LA RED P2P

Para que un nodo pasarela se conecte a la red p2p, debe tener tokens SSW, por un valor de preferencia equivalente a 1.5 veces el valor promedio de una transacción de la criptomoneda correspondiente. Este valor promedio será indicado por las estadísticas mantenidas por los nodos pasarelas y se mostrará en la interfaz de usuario del nodo pasarela.

El NodeOwner también debe tener una máquina fiable, segura y una conexión estable a Internet. Para ello, se recomienda utilizar un servidor físico o una máquina virtual en un operador de Cloud.

También debe haber obtenido la aplicación nodo pasarela correspondiente a la criptomoneda que desea operar, o posiblemente haber desarrollado su propia especialización basada en el modelo de nodo proporcionado en código abierto para añadir el soporte de una criptomoneda, y tener acceso a un nodo en la blockchain correspondiente.

SEGURIDAD DE LOS INTERCAMBIOS, UTILIZACIÓN DE TOKENS SSW PUESTOS COMO GARANTÍA Y RETRIBUCIÓN A LOS NODEOWNERS

Una vez configurado el nodo para conectarse a la blockchain correspondiente, su puesta en marcha lo conecta a los otros nodos p2p de la red Secure Swap. De este modo, se asigna al nodo un identificador único en la red. Sin embargo, en esta etapa de la puesta en marcha, ningún otro nodo acepta ni envía todavía solicitudes.

Para que este nodo pasarela sea plenamente operativo, su operador debe enviar su prueba de participación y garantía (consistente en tokens SSW) al wallet asociado al "contrato inteligente" que lo gestiona en la red Ethereum, así como el identificador único del nodo. Esto se hará fácilmente a través de la interfaz de usuario



Libro Blanco Secure Swap

del nodo. Esta transacción, firmada por el nodo pasarela, será transmitida por la red p2p a otro nodo pasarela de la blockchain Ethereum, que a su vez la transmitirá al nodo Ethereum al que está conectada.

Los tokens se envían a la wallet gestionada por este "contrato inteligente". Cuando el contrato inteligente valida la recepción de los tokens, emite la autorización del nodo con su nivel de garantía. La autorización se propagará a todos los nodos de la red, los cuales aceptarán operar con ella.

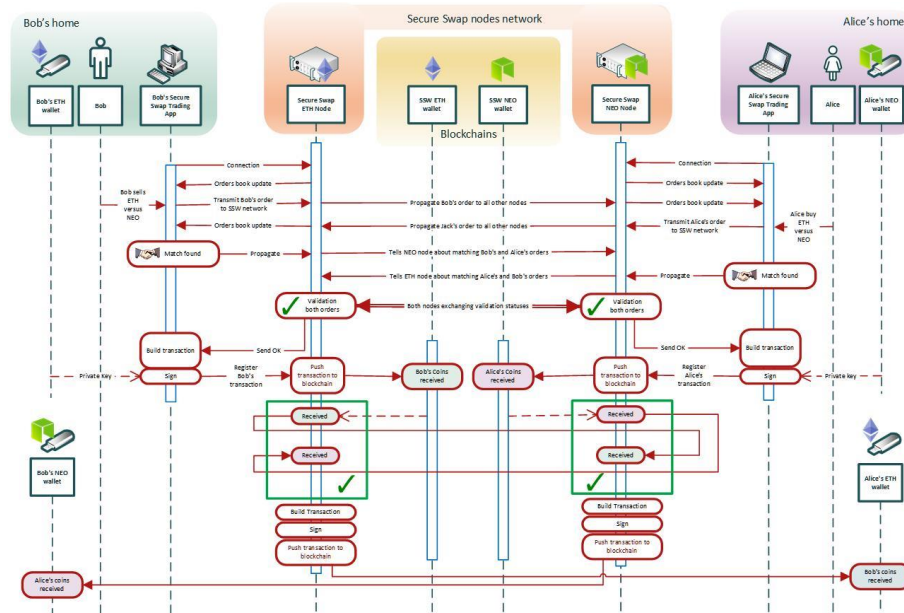
Por lo tanto, la prueba de participación también se utiliza como garantía, dada por el NodeOwner, para el funcionamiento de su nodo de pasarela. Esta prueba de participación también define el importe máximo de cada transacción que este nodo puede gestionar, que es como máximo 2/3 del valor de la prueba de participación.

El nodo pasarela también debe tener indicado, a través de su configuración, un wallet correspondiente a la criptomoneda que gestiona (wallet EOS para un nodo pasarela EOS).

Este wallet se utiliza para recibir la parte que le corresponde al NodeOwner de las comisiones pagadas por el trader. Esto va en proporción a los tokens que ha puesto en garantía en relación a todos aquellos comprometidos para la criptomoneda gestionada por el nodo.

Este wallet también se utiliza para recibir la contrapartida de los intercambios en los que interviene la criptomoneda gestionada por el nodo, antes de enviarla al destinatario final. Esto asegura la atomicidad de los intercambios (de modo que un trader no reciba ninguna contrapartida de un intercambio sin haber enviado la suya).

FLUJO DE COMUNICACIÓN DURANTE UNA TRANSACCIÓN SIN INCIDENTES



Este esquema está simplificado para la facilidad de comprensión y no representa las seguridades constituidas para la validación de las operaciones para todos los nodos de una blockchain.



Libro Blanco Secure Swap

En el funcionamiento normal (sin incidentes), durante las operaciones de intercambio entre criptomonedas, las contrapartes se encaminan a través de los nodos pasarelas de la criptomoneda correspondiente (monedas NEO que pasan por las pasarelas NEO). Para cada operación, las contrapartes son enviadas a uno de los wallets gestionados por los nodos de la pasarela elegibles, seleccionados aleatoriamente. Este sorteo aleatorio se pondera por la proporción de tokens SSW puestos en garantía en el nodo, en comparación con el número total de tokens SSW en garantía en todos los nodos que operan con la misma criptomoneda. De este modo, el nodo puede mantener directamente las comisiones de cambio (0,15% inicialmente) impuestas a la contraparte antes de enviarlas al destinatario.

Tenga en cuenta que sólo son elegibles los nodos con una garantía de 1,5 veces el valor de la transacción, en forma de tokens SSW y pueden participar en el sorteo de los nodos asignados para recibir contrapartes.

Esto evita una división excesiva de la remuneración a distribuir entre todos los nodos de pasarelas, a la vez que garantiza que con el tiempo cada nodo de pasarela reciba la parte que le corresponde. Y también evita costos adicionales de red por la repartición de las remuneraciones entre nodos.

Un mecanismo cambiará la ponderación de cada nodo en función del retraso o adelanto que hubiera hecho en la recaudación de comisiones en función de la parte que va a recibir. Este cálculo, realizado por los propios nodos, tiene en cuenta todas las comisiones cobradas por todos los nodos de una criptomoneda. Esto asegura que los nodos de pasarelas que sólo han transitado por pequeñas transacciones no estén en desventaja en comparación con otros que habrían transitado por grandes transacciones de valor.

Si por cualquier motivo (piratería informática, robo, caída, mal funcionamiento, pérdida de la red eléctrica o de Internet, etc.), un nodo de pasarela no envía al destinatario los activos que ha recibido cuando tiene que hacerlo, entonces los tokens de SSW que sirven de garantía serán cargados por el valor equivalente a la contrapartida que falta. Estos tokens se convertirán automáticamente al precio de mercado para el intercambio de la criptomoneda que falta, y estos activos se enviarán al destinatario de la bolsa que no haya recibido su contraparte.

Esta operación de finalización de una transacción interrumpida, utilizará todas las fuentes de liquidez disponibles incluida la liquidez de los intercambiadores externos conectados a través de nodos de arbitraje, con posibles conversiones múltiples, con el fin de que pueda llevarse a cabo lo más rápidamente posible, incluso si los costos resultantes son superiores.

La contraparte no enviada por el nodo pasarela pasa a ser propiedad del NodeOwner.

Todos los costos inherentes a esta operación de reemplazo son responsabilidad del NodeOwner que opera el nodo defectuoso de pasarela, y se descuentan de sus tokens SSW de garantía, los cuales se convertirán en la criptomoneda utilizada para pagar estos costos (Ether por ejemplo, para pagar los costos de gas correspondientes).

Toda esta operación la llevan a cabo los demás nodos de la red y el "smart contract" encargado de esta tarea en el marco de la conservación de las garantías de los nodos pasarelas.

El nodo pasarela defectuoso se desconecta, si aún estaba conectado, y sus tokens SSW en garantía restantes se devuelven al wallet del NodeOwner que los envió (menos los gastos de envío).

En el caso de una desconexión inesperada del nodo, éste tiene un retraso permitido de algunos minutos para volver a conectarse con el mismo identificador antes de que se active el procedimiento descrito anteriormente. Esto es para darle al nodo la oportunidad de reanudar sus actividades normales en caso de una falla en la



Libro Blanco Secure Swap

comunicación o un fallo inoportuno, pero a corto plazo. Durante este tiempo, la garantía del nodo (en tokens SSW) será obviamente retenida por el contrato inteligente.

Este procedimiento se utiliza tanto para garantizar al operador que recibirá su contraparte después de un intercambio, como para incentivar a los NodeOwner a asegurarse de que su nodo pasarela funcione en una máquina confiable, sin posibilidad de que se bloquee, pierda su conexión a Internet o sea pirateada. El NodeOwner asume estos riesgos.

Los tokens SSW en garantía también se devuelven al NodeOwner (menos los gastos de envío) cuando el nodo de pasarela se detiene normalmente.

Por lo tanto, un NodeOwner tiene como fuente de ingreso una parte de los gastos pagados por los traders lo cual va en proporción a los tokens SSW que ha puesto en garantía para la operación de su nodo, frente al número total de tokens SSW asignados a todos los nodos de pasarela para esta divisa criptográfica.

Este paga una tarifa por iniciar y detener su nodo correspondiente al envío inicial y a la devolución de los tokens SSW dejados como garantía (tarifas de red).

En el caso de un mal funcionamiento de su nodo lo que origine un falta de entrega de una contraparte, el NodeOwner también pagará los costos incurridos por el sistema descrito anteriormente, esto con el objetivo de garantizar la entrega de la contraparte al trader, y asumirá el riesgo de cambio de sus tokens SSW que ya no tiene y que son sustituidas por un valor equivalente en la criptomoneda gestionada por su nodo, y pagadas al wallet vinculado al nodo (los activos no enviados al destinatario).

Una vez que el nodo pasarela se detiene, todos los activos presentes en el wallet vinculado al nodo son propiedad del NodeOwner. Proceden de la remuneración del nodo y posiblemente de contrapartes que no han sido devueltas, pero que han sido pagadas por el propietario del nodo a través de sus tokens SSW.

Durante su operación, el nodo también muestra la cantidad de activos pertenecientes al NodeOwner, en caso de que éste desee transferirlos sin detener la operación de su nodo.

Los nodos pasarelas proporcionan una descentralización completa del acceso a la blockchain, sin un punto único de fallo.

Ellos aportan una redundancia significativa tanto para la conexión a las blockchains como para los intercambios.

Esta alta redundancia también permite absorber períodos de alta carga y si es necesario se pueden añadir nodos adicionales muy fácilmente, sin interrumpir la operación de Secure Swap.

Este sistema operativo de nodo seguro, así como los tokens SSW puestos en garantía en cada nodo de pasarela, garantizan que las contrapartes sean recibidas por los traders, independientemente de lo que suceda en la red Secure Swap.

Los nodos pasarelas también permiten que Secure Swap sea criptoagnóstico, es decir, que funcione con todas las criptomonedas, sin depender de tecnologías en desarrollo como Plasma o Lightning Network, al tiempo que tiene un rendimiento similar en sus capacidades de procesamiento de intercambio.



NODO MARGEN DE TRADING

Los nodos de margen de trading permiten a la red Secure Swap ofrecer operaciones de margen.

Este tipo de nodos también se distribuirán en código abierto, siendo cada uno de ellos libre de ejecutar uno.

Sin embargo, hay que tener en cuenta que la ejecución de este tipo de nodos es bastante exigente. Además de disponer de un número suficiente de tokens SSW para proporcionar una garantía a los traders, también es necesario disponer de un capital en forma de criptomonedas correspondiente a aquellas en las que se permite el margen de trading.

Grey Matter Technologies SpA actuará como operador de este tipo de nodos, sin ningún privilegio particular.

REQUISITOS PARA PODER CONECTAR UN NODO DE MARGEN DE TRADING A LA RED P2P

Al igual que con otros nodos, usted necesita una máquina confiable y segura con una conexión estable a Internet, preferiblemente un servidor dedicado exclusivamente a este uso.

Es necesario tener una reserva de tokens SSW equivalente al doble de la suma de los márgenes de las posiciones que el nodo autorice. En otras palabras, la cantidad de tokens SSW puestos en garantía, determina la cantidad de margen que se puede utilizar en las posiciones tomadas por los traders. Como corolario, la cantidad de tokens SSW utilizadas como garantía limita la altura de las posiciones que pueden tomarse al mismo tiempo en el nodo, en una proporción de 2:1.

Estos tokens se asegurarán mediante un contrato inteligente encargado de esta función, similar a los nodos de pasarela.

También es necesario tener suficiente capital de criptomonedas para que las posiciones que el nodo autoriza puedan ser tomadas por el trader, ya que el nodo adelanta la diferencia entre el tamaño de una posición y el margen disponible en el wallet del trader, dentro del límite del apalancamiento autorizado.

Ejemplo: el nodo permite operar con margen en Bitcoin, el trader quiere intercambiar 100 Bitcoins por otra criptomoneda, el apalancamiento máximo permitido es 5.

- El margen inicial del trader debe ser de al menos 20 Bitcoins.
- El margen mínimo del trader es de 15 Bitcoins (umbral de llamada de margen igual a $0,75 * \text{el margen inicial}$, por ejemplo).
- La garantía simbólica SSW (para garantizar la devolución de los activos del comerciante) debe ser equivalente en valor a 40 Bitcoins (el doble del margen de garantía).
- Y el número de bitcoins disponibles en el capital a nivel de nodo debe ser de un mínimo de 80 bitcoins, lo que, sumado al margen de 20 bitcoins del trader, permite tomar una posición de 100 bitcoins (realizar una transacción de intercambio de 100 Bitcoins contra otra criptomoneda).

Esto multiplicado por el número de posiciones equivalentes que el nodo permite.



FUNCIONAMIENTO DEL NODO DE MARGEN DE TRADING

El administrador del nodo tendrá que indicar, por cada par de criptomonedas que él decida autorizar para el margen de trading:

- El nivel máximo de apalancamiento permitido.
- El umbral mínimo de margen por debajo del cual la posición desencadena un ajuste de márgenes.
- Las tarifas de entrada y salida que cobra.
- La tasa de interés horaria tomada para la posición de margen.

De forma muy similar a los nodos pasarelas, el nodo de margen de trading se conecta a la red Secure Swap una vez configurado; él obtiene su identificador único y sólo puede operar una vez que ha recibido la autorización de los otros nodos, tras enviar su garantía en tokens SSW al contrato inteligente especializado en la gestión de nodos de margen de trading.

A continuación, el nodo informa a la red Secure Swap de sus capacidades de margen de trading, en función de sus reservas disponibles en criptomonedas y actualizadas en función de las transacciones realizadas, para que las aplicaciones cliente puedan ofrecer esta negociación a través de su interfaz. La información relevante también se transmitirá a las aplicaciones de los clientes, como el nivel máximo de apalancamiento permitido por par de criptomonedas, las comisiones de mantenimiento de posiciones (intereses sobre el avance realizado por el nodo).

La aplicación cliente Secure Trade presenta al trader las oportunidades disponibles para el margen de trading. El trader realiza su orden en Secure Trade la cual se transmite a través de la red Secure Swap p2p al nodo margen de trading correspondiente. Si la orden es aceptada, o sea cumple los criterios de margen, apalancamiento máximo, etc, el nodo solicitará recibir el margen del trader. Una vez recibido el margen, el nodo inicia una posición para este trader, que consiste en memorizar el préstamo concedido al trader y añadir una orden de intercambio correspondiente a la transacción deseada por el trader en la cartera de órdenes de Secure Swap.

Una vez que la orden de intercambio se ha ejecutado en la red Secure Swap, el nodo de margen de trading conserva la contraparte del intercambio y monitorea cualquier eventual pérdida latente de la transacción realizada.

Si las pérdidas latentes (convertidas en la criptomoneda original al tipo del mercado) causan que el margen mínimo para mantener la posición sea excedido, entonces la posición se cierra automáticamente por medio de una llamada de margen.

La posición también puede cerrarse a petición del trader a través de Secure Trade.

Cuando se cierra una posición, el nodo de margen de trading efectúa una conversión inversa de la primera al precio de mercado, utilizando la contrapartida que ha sido conservada. Una vez finalizado el canje, se retira el préstamo realizado previamente, y luego envía el saldo al trader restando del saldo todos los costos de la operación.

Ejemplo:

Un trader desea operar con un margen de cambio de 5 BTC frente a 150 ETH, el nodo pasarela permite un apalancamiento máximo de 5, y por lo tanto requiere un margen inicial de 1 BTC mínimo para esta transacción.



Libro Blanco Secure Swap

El margen mínimo antes del llamado de márgenes es 0,75 veces el margen inicial, este nodo activa un llamado de márgenes si el margen disponible cae por debajo de 0,75 BTC.

El trader, a través de Secure Trade, da la orden de tomar esta posición.

El nodo pone a disposición 4 BTC para esta posición, y enviará la orden de intercambio de 5 BTC contra 150 ETH en la red Secure Swap. Por lo tanto, el tipo de cambio es de 30 ETH para 1 BTC.

Si la orden se ejecuta, el nodo de margen de trading recibirá la contrapartida de 150 ETH frente a los 5 BTC de los cuales 1 BTC pertenece al trader y representa su margen disponible (menos todos los costos), y 4 BTC son los prestados por el nodo.

Si el tipo de cambio se mueve favorablemente para el trader y éste decide cerrar la posición cuando el precio se convierte en 1 BTC frente a 20 ETH, el nodo de margen de trading que recibe la orden de cerrar la posición, publicará una orden de intercambio por los 150 ETH que tiene para esa posición frente a BTC a precio de mercado.

Para este ejemplo, el intercambio se lleva a cabo en 1 BTC para 20 ETH. El nodo recibe 7.5 BTC. Este recupera los 4 BTC que había prestado para esta operación y, por lo tanto, envía el saldo de 3,5 BTC al trader, menos los costos asociados.

Si el precio cambia desfavorablemente para el trader, y de repente pasa a 1 BTC por 35 ETH, entonces tenemos una demanda de margen. El nodo cierra automáticamente la posición y, por lo tanto, realiza una orden de intercambio de 150 ETH para BTC, al precio de mercado.

El intercambio que se lleva a cabo para este ejemplo es de 1 BTC contra 35 ETH, el nodo recibe 4,28 BTC, recupera el anticipo de 4 BTC y envía el saldo de 0,28 BTC al trader, menos los costos. Por lo tanto, el trader incurre en una pérdida de 0,72 BTC más comisiones.

Para simplificar estos ejemplos, no hemos calculado las comisiones de posición, de cambio y de red, que son pagadas por el trader y cargadas a su margen disponible durante el mantenimiento de la posición, y deducidas del saldo enviado al cliente al cierre de la posición.

Del mismo modo, los costos derivados de los intereses tomados por el nodo se deducen del margen disponible cuando se mantiene la posición, y se deducen del saldo devuelto al trader.

El correcto funcionamiento de los nodos de margen de trading, está garantizado por los nodos pasarelas que lo controlan, cada uno de ellos en función de la criptomoneda que gestionan.

Si el nodo de margen de trading ha alcanzado un número máximo de posiciones globales (el doble de la suma total de los márgenes utilizados por los traders corresponde al nivel de valor materializado por los tokens del nodo colateral), entonces los nodos de pasarela ya no le permiten ofrecer otras posiciones de margen a las aplicaciones de los clientes. Sólo queda disponible la anulación de las posiciones ocupadas hasta que se restablezca un nivel suficiente de seguridad disponible.

Si el nodo ya no tiene suficientes fondos en una criptomoneda para el anticipo concedido al tomar una posición, entonces los nodos de pasarela sólo le permiten desbloquear posiciones en esta criptomoneda hasta que se restauren los fondos suficientes.



Libro Blanco Secure Swap

Si un nodo de margen de trading se desconecta, se cuelga, etc., tiene unos minutos para volver a estar operativo. Después de este período, el contrato inteligente dedicado a la gestión de estos nodos iniciará las operaciones de intercambio de tokens SSW con el fin de reembolsar a los clientes que mantengan posiciones de margen gestionadas por el nodo infractor. Este proceso:

- Calcula la posición del cliente en el momento de la desconexión del nodo infractor.
- Determina los beneficios/pérdidas no realizados.
- Los integra en el margen depositado por el cliente en el nodo infractor.
- Y devuelve el saldo menos los costes (red, cambios, intereses) correspondientes a una liquidación inmediata de las posiciones mantenidas.

Estos tokens SSW serán convertidos a través de la liquidez disponible en Secure Swap y proporcionados por los nodos de arbitraje mediante órdenes de conversión a precio de mercado con el fin de entregar a los traders en las criptomonedas correspondientes a sus posiciones, siendo todas estas operaciones gestionadas por los nodos pasarelas.

Todos los costes derivados de estas operaciones de intercambio y el envío de tokens SSW se cargarán al nodo de margen de trading infractor, deducidos de los tokens SSW puestos como garantía, cuyo saldo le será devuelto al final de dichas operaciones.

Como la distribución de las criptomonedas de los fondos de reserva se ha modificado a raíz del mal funcionamiento del nodo de margen de trading, el riesgo de tipo de cambio ya no es el mismo que en un principio. El operador del nodo asume el riesgo, y debe eventualmente reequilibrar su distribución en criptomonedas de los fondos utilizados para operar su nodo.

Si un nodo de margen de trading, sin estar desconectado, no envía al propietario las criptomonedas que le pertenecen cuando éste ha cerrado una posición, se activa el procedimiento descrito anteriormente, sólo para esa posición.

Cada vez que se activa este procedimiento, sin desconectar el nodo, se reduce la cantidad de tokens SSW utilizados como garantía para el nodo de margen de trading, lo que afecta a su capacidad de tomar otras posiciones de margen. Cuando el valor de los tokens SSW en garantía es inferior al doble del conjunto de márgenes correspondientes a las posiciones actuales, entonces ya no puede aceptar otras órdenes, esto está prohibido para él por los nodos de pasarela, sus posibilidades de negociación no están disponibles en el nivel de Secure Trade para este nodo de márgenes de trading.

Cuando una posición causa un ajuste de márgenes (el margen está por debajo del nivel de margen necesario para mantener la posición), el nodo reduce automáticamente la posición hasta que vuelve a un nivel de margen igual al margen inicial normal de una posición. Si no se puede restablecer el nivel de margen reduciendo la posición, entonces la posición está completamente cerrada.

Por lo tanto, un trader de un nodo de negociación de margen paga una tarifa de puesta en marcha y cierre (costes de red relacionados con el envío y recuperación de tokens SSW como garantía del contrato inteligente).

Asume todos los riesgos de pérdidas relacionadas con un mal funcionamiento de su nodo o una mala configuración que resulta en una toma de riesgos inadecuada, como por ejemplo:

- Un nivel de margen mínimo excesivamente bajo antes de la liquidación, lo que causaría una pérdida mayor que el margen del cliente al liquidar la posición.
- O una palanca autorizada que es demasiado grande.
- O la autorización para operar con margen para un par de criptomonedas que son demasiado volátiles.



Libro Blanco Secure Swap

Sus ganancias provienen de las comisiones de entrada y salida de posiciones, así como de los intereses sobre las posiciones de margen, que cobra.

Es importante que un operador de este tipo de nodo evalúe adecuadamente los riesgos asociados a esta actividad. La configuración del nodo debe permitir un cierre de posición causado por una llamada de margen sin causar que el nodo entre en un balance negativo, lo que si esto sucede constituye una pérdida para el operador del nodo. Esto depende tanto del nivel de margen requerido para mantener una posición, como de la volatilidad del par de criptomonedas que forman la posición.



NODO DE CAMBIO A MONEDA FIDUCIARIA

Los nodos de cambio a monedas fiduciarias son los puntos de conexión entre las criptomonedas y las finanzas tradicionales (monedas fiduciarias).

Estos nodos no son anónimos. Exigen el cumplimiento de las reglas de KYC ("Know Your Customer - Conozca a su cliente"). Serán gestionados por unidades jurídicas, cada una de las cuales ofrecerá su propia lista de pares fiat-cripto intercambiables.

Para cumplir con las reglas de KYC, los usuarios deberán abrir una cuenta en estos tipos de nodos antes de poder utilizarlos.

Estos nodos funcionan como bolsas de intercambio. Los usuarios que hayan transferido previamente monedas fiduciarias (cash in) podrán cambiarlas por las criptomonedas de otros usuarios que deseen vender sus criptomonedas por monedas fiduciarias (cash-out).

Además del servicio de intercambio fiat-cripto, estos nodos soportan la integración de métodos de pago, gracias al suministro de un kit de desarrollo (SDK) que permite la integración sencilla de los métodos de pago en los sitios web de los comerciantes, en las aplicaciones o en los métodos de pago móviles (smartphones).

Este SDK ofrecerá la integración de métodos de pago basados en monedas fiduciarias, pero también en pagos directamente en criptomonedas.

Grey Matter Technologies SpA planea operar este tipo de nodos, con un primer paso en la zona sudamericana (Chile, Perú, Argentina para empezar), y luego en las zonas USD y Euro.

Para ello, creará tantas empresas independientes como áreas en las que opere con monedas fiduciarias, con el fin de no extender los riesgos operativos a todo el Secure Swap.

Se proporcionará un nodo estándar en código abierto, adaptable a los diferentes métodos de pago, regulaciones locales y moneda fiduciaria a los que está destinado. Esto permitirá a aquellos que deseen llevar a cabo una actividad profesional de este tipo, ofrecer apoyo a las monedas fiduciarias y a los medios de pago de sus regiones.



SISTEMA DE DETECCIÓN DE ANOMALÍAS O INTENTOS DE PIRATERÍA INFORMÁTICA

PROTOCOLO DE COMUNICACIÓN PARA NODOS SWAP SEGUROS

Este protocolo de comunicación se utiliza cuando los datos esperados por un nodo receptor son sensibles y requieren validación.

Este protocolo permite la resolución en un solo paso del consenso bizantino (https://en.wikipedia.org/wiki/Byzantine_fault_tolerance) en entornos distribuidos y asíncronos.

Este proceso es posible gracias a ~~que Secure Swap porque~~ la red Secure Swap no necesita que los datos se reciban en un orden determinado, y porque puede contar con un mecanismo de pruebas de participación y ~~de~~ compromiso, ~~lo cual que~~ simplifica su implementación.

Descripción del protocolo:

Cada nodo ~~conoce~~ el número de nodos que pueden responder a una petición. Este número se actualiza cada vez que ~~un nodo~~ aparece o desaparece ~~un nodo~~ en la red.

Cuando se espera una respuesta, se asigna una ventana de tiempo de hasta 30 segundos para recibir las respuestas. Cada nodo receptor memoriza y cuenta las respuestas.

Tan pronto como el número de respuestas recibidas corresponda ~~n~~ al 60% de los nodos susceptibles de responder, y todas las respuestas sean idénticas, ~~entonces~~ la respuesta recibida será validada y se considerará exacta.

Si, por el contrario, una o más respuestas difieren o el número de respuestas recibidas no alcanza el 60% de los nodos susceptibles de responder, entonces se utiliza la ventana de 30 segundos para permitir que se reciba el máximo número de respuestas.

Cuando la ventana de tiempo para recibir respuestas ha expirado y, por lo tanto, la respuesta aún no ha sido validada, se califica cada una de las respuestas recibidas. Esta ~~calificación~~ se calcula sumando el número de tokens SSW en garantía ~~para el funcionamiento la operación~~ de cada nodo que proporcionó la misma respuesta. Es en este contexto que los tokens de SSW se utilizan como prueba de participación.

La respuesta con la puntuación más alta se considera la respuesta correcta. Los nodos que han respondido de forma diferente quedan excluidos de la red Secure Swap (enviando una solicitud de desconexión e invalidando la autorización de ~~funcionamiento operación~~), lo que puede dar lugar a la activación del mecanismo de garantía para los nodos en cuestión (intercambios en curso).

Este protocolo asegura el correcto funcionamiento de la red en caso de fallas, ~~e~~ si al menos el 60% de los nodos responden a una solicitud en el tiempo asignado y todos dan la misma respuesta, o si la respuesta correcta es la ~~que es~~ mayoritaria en términos de prueba de ~~participación~~ ~~misión~~ entre ~~aquellas~~ recibidas en el tiempo asignado.

Este protocolo permite que Secure Swap sea ~~resistente~~ ~~tolerante~~ a las fallas, incluso cuando la falla es causada por un intento de piratería, sin dejar de ser eficiente.



En el caso de que no se produzca ning~~una~~^{ún} fall~~o~~^e, la respuesta de sólo el 60% de los nodos afectados valida la información~~respuesta~~. En caso de fall~~o~~^e, la respuesta se valida tras un retraso de 30 segundos.

Puede haber tantos procesos de validación en curso como respuestas a la espera de validación. Estas validaciones se realizan en paralelo, por lo que no hay tiempo de espera adicional para validar una respuesta que sería causada por la espera de otro proceso de validación de una respuesta anterior.

APLICACIÓN DEL PROTOCOLO DE COMUNICACIÓN

Cuando se realiza una operación sensible, ya sea la comprobación de la recepción de activos en un wallet, o cualquier otra transmisión de información a través de nodos, clientes o pasarelas, esta información es verificada por todos los nodos, de acuerdo con el protocolo de comunicación anteriormente descrito.

Ejemplo: Si Secure Trade informa de haber enviado tal cantidad de activos en dicha billetera, todos los nodos de pasarela a la criptomoneda relevante pueden verificar la existencia de la transacción, verificar que se está llevando a cabo y que los activos están siendo recibidos por la billetera indicada.

Cada nodo en cuestión transmite esta información a los otros nodos, si los nodos tienen respuestas contradictorias, entonces la respuesta válida es la de los nodos que acumulan el mayor número de tokens SSW en garantía, que se convierte en la respuesta mayoritaria. Los nodos que dan respuestas minoritarias se desconectan de la red. Sus tokens SSW como garantía, en el caso de nodos de pasarela, son devueltos (posiblemente reducidos por la contraprestación retenida por el nodo si retiene uno).

Con este sistema, los tokens SSW que ya sirven como garantía para el funcionamiento de los nodos de pasarela también tienen un papel como prueba de participación.

Esto afecta a todas las operaciones sensibles, que están bajo la supervisión de toda la red.

- Incluye el anuncio por parte de un cliente de Secure Trade de un matching. Si ningún otro Secure Trade indica un matching complementario, o si los nodos de pasarela no validan el matching, se desconecta el Secure Trade defectuoso.
- Se aplica a los matching realizados por los nodos de arbitraje.

En el caso de los nodos de pasarela, si uno de ellos indica que no ha recibido la contrapartida de un cliente durante una operación de intercambio o si no envía la contrapartida al cliente receptor indicando que lo ha hecho o no, entonces esto será detectado por los otros nodos. Se desconectará el nodo de pasarela defectuoso y se le devolverán sus tokens SSW tras restarle la parte necesaria para completar el intercambio, tal y como se describe en el apartado "Nodos de pasarela y NodeOwners".

Para evitar que un nodo distorsione las estadísticas, este sistema de validación también se utiliza en los nodos pasarelas y se aplica a:

- El valor de un token SSW expresado en cada criptomoneda soportada.
- El estado estadístico de la distribución de la remuneración entre los nodos pasarela para el sistema de asignación aleatoria ponderada del siguiente nodo pasarela que gestionará una contrapartida de una bolsa.
- Etc.

Mis en forme : Taquets de tabulation : 14,45 cm, Gauche + Pas à 8 cm



Libro Blanco Secure Swap

En resumen, todos los datos sensibles son verificados por todos los nodos, tan pronto como pueden hacerlo (por ejemplo, un nodo pasarela Ethereum no puede comprobar la recepción de Bitcoins en un wallet, pero todos los nodos pasarela de Bitcoins pueden hacerlo).

Este sistema de multicontrol, junto con la entrega de tokens SSW de los nodos pasarela conectados, garantiza la seguridad de los intercambios, la detección de anomalías de cualquier tipo (hacking, mal funcionamiento...) y la desconexión de las partes fallidas.

Este sistema implica que las partes que funcionan normalmente no se ven perjudicadas, y que las partes que incumplen asumen la responsabilidad de sus posibles pérdidas.



SISTEMA QUE GARANTIZA LA ATOMICIDAD Y LA SEGURIDAD DE LOS INTERCAMBIOS

Cuando una contraparte es detectada por una aplicación cliente, emite una reserva de la orden correspondiente, que se propaga en los nodos de la red Secure Swap. De este modo, el pedido queda bloqueado e inalterable para el cliente de Secure Trade que lo ha emitido. El cliente contrario de Secure Trade también encontrará la contraparte adicional, procedente del primer cliente, y la reservará también.

Ejemplo: Bob puso un pedido de 2 BTC contra 60 ETH, Alice puso un pedido de 32 ETH contra 1 BTC.

El matching es encontrado por ambos clientes.

Secure Trade (en Bob's) bloquea la orden de Alice a 32 ETH contra 1 BTC.

Secure Trade (en Alice's) bloquea el pedido de Bob de 1 BTC a 30 ETH (1 BTC a 30 ETH permanece en la cartera de órdenes de Bob).

Una vez que ambas contrapartes están bloqueadas, los nodos pasarelas iniciarán y gestionarán el proceso de intercambio.

Es importante recordar que todos los nodos pasarela correspondientes a las contrapartes (aquí en el ejemplo: nodos de la pasarela BTC y nodos de la pasarela ETH) comprobarán todos los pasos del proceso. Esto se refiere a:

- La validez de las direcciones de los wallets transmitidos (posesión de la contraparte por el emisor de la orden).
- La recepción efectiva de las contrapartidas mediante nodos pasarelas seleccionadas aleatoriamente.
- La remisión, por parte de los nodos pasarela que actúan como intermediarios, de las contrapartes a los destinatarios adecuados.
- La buena recepción de sus homólogos por parte de las aplicaciones Secure Trade de Bob y Alice.

En caso de desacuerdo entre los nodos, la respuesta válida es la correspondiente a la respuesta dada por los nodos con la mayor cantidad de tokens SSW en garantía juntos (prueba de participación), tal y como se describe en el capítulo "Sistema de detección de anomalías o intentos de piratería informática". Este mecanismo permite que el intercambiador funcione en un entorno "sin confianza".

Se designará un nodo pasarela en BTC para recibir esta parte del intercambio, de forma aleatoria descrita en el capítulo "Nodos de pasarelas y NodeOwners". Se designará un nodo pasarela ETH de acuerdo con el mismo principio.

Una vez recibidos los nodos de recepción de las entidades de contrapartida designadas, sus direcciones de wallet se transmiten a las dos aplicaciones de negociación segura que reciben la validación del envío de las entidades de contrapartida.

Ambas aplicaciones de Secure Trade envían sus contrapartidas a los nodos pasarelas designados. Una vez que ambos nodos pasarelas han confirmado que han recibido a estas contrapartes, los nodos envían los activos a las aplicaciones Secure Trade de los destinatarios finales, con lo que se concluye el intercambio.

Usando nuestro ejemplo, Bob envió 1 BTC y recibió 32 ETH a cambio, todavía tiene una orden de intercambio de 1 BTC por 30 ETH activos. Alice envió 32 ETHs y recibió 1 BTC a cambio.



Libro Blanco Secure Swap

En caso de incidencia durante el intercambio (desacuerdos entre nodos), se desconectan los nodos minoritarios y se continúa el intercambio con los nodos restantes, lo que puede dar lugar a una designación aleatoria de nodos que sirvan de intermediarios para el intercambio.

Si un nodo pasarela retiene una contrapartida, por una de las siguientes razones:

- No lo envía a su destinatario en un plazo de tiempo normal (retraso de bloqueo).
- Había recibido una contraparte antes de desconectarse o después de un desacuerdo entre los nodos.
- Se desconecta o ya no responde a las peticiones de red.

la contraparte retenida por el nodo se entregará al operador de acuerdo con las condiciones descritas en "Nodos pasarelas y nodeowners".

Así, la multi-verificación y puesta en garantía de los tokens SSW entrega seguridad a las transacciones en el entorno "trustless" Secure Swap.



RENDIMIENTO DEL INTERCAMBIADOR

Hemos visto anteriormente que la plataforma no depende de las capacidades de una blockchain para su velocidad de funcionamiento. Ya sea para la gestión de la cartera de órdenes, la gestión de transacciones y todos los otros sistemas. Por supuesto, un intercambio en sí mismo no puede completarse más rápido de lo que permite una blockchain, pero ellas no limitan el número de transacciones por segundo que la plataforma puede transmitir.

El número de transacciones que pueden ser operadas se estima en alrededor de mil transacciones por blockchain por segundo. Como la velocidad de funcionamiento de la red p2p es independiente a la de cada blockchain, la capacidad total de la plataforma se multiplica por el número de bloques gestionados, lo que puede representar desde unas pocas decenas hasta cientos de miles de transacciones por segundo en total.

Así, sin depender de tecnologías aún en desarrollo, Secure Swap ofrece, con tecnología propia, prestaciones similares a las de Plasma o Lightning Network.

Si consideramos una blockchain en particular, la velocidad de la plataforma está limitada por la capacidad de blockchain en cuestión para minar/validar transacciones.

Actualmente la blockchain Ethereum está limitada a unas 10/15 transacciones por segundo.

Sin embargo, se está trabajando para aumentar considerablemente el número de transacciones por segundo que blockchain Ethereum podrá realizar. Estamos hablando de un aumento de cientos de miles o incluso millones de transacciones por segundo, gracias a tecnologías como Plasma, Sharding y Lightning Network. Otras blockchains, basadas en la prueba de participación, son intrínsecamente más rápidas. Secure Swap tiene la capacidad de explotar la velocidad actual y futura de estas blockchains.

Utilizamos contratos inteligentes en la blockchain Ethereum para gestionar los tokens SSW puestos en garantía para la conexión de los diferentes servicios, lo cual es útil en caso de anomalías en estos y para autorizar su funcionamiento.

Por lo tanto, dependemos del futuro de la blockchain Ethereum para el funcionamiento de Secure Swap.

Sin embargo, nada nos impediría, si fuera necesario, cambiar el funcionamiento de estas partes dependientes del contrato inteligente, a otra blockchain, y distribuir los nuevos tokens en sustitución de los tokens SSW ERC-20 en circulación.

Una forma bastante sencilla de hacerlo sería cambiar el funcionamiento en la blockchain Tomochain, que puede considerarse como una bifurcación de Ethereum, totalmente compatible a nivel de token y contrato inteligente, pero que integra Sharding y Plasma desde el principio y que trabaja en una prueba de participación, haciéndola mucho más rápida que Ethereum. Sin embargo, será necesario reemplazar los tokens de todos los propietarios por los nuevos tokens de esta blockchain. Esto implicaría el funcionamiento paralelo en ambas blockchains de Secure Swap para contratos inteligentes y tokens hasta que todos los tokens SSW ERC-20 sean intercambiados por los de la nueva blockchain.

Sin embargo, no hay indicios de que tengamos razones para dudar del futuro de la blockchain Ethereum. Es por ello que nos parece una solución fiable la dependencia del funcionamiento de Secure Swap en la blockchain Ethereum a través de nuestros contratos inteligentes. Y si nos equivocamos en este punto, migraremos a otra blockchain, que simplemente consiste en migrar contratos inteligentes y tokens.



INDICACIÓN DEL ESTADO DEL INTERCAMBIADOR

Hemos visto en las explicaciones anteriores que los nodos pasarela, además de sus otras funciones, gestionan las estadísticas de la red Secure Swap.

Estas estadísticas serán utilizadas por las aplicaciones cliente de Secure Trade así como por otros nodos de la red p2p.

Indicaciones mostradas por la aplicación cliente

La aplicación Secure Trade indicará mediante un código de color, la disponibilidad de nodos pasarelas para cada criptomoneda:

- Rojo: no hay pasarela disponible para esta criptomoneda → no hay cambio posible.
- Rojo-Naranja: sólo una pasarela disponible para este criptomoneda → intercambios técnicamente posibles pero prohibidos.
- Amarillo: dos pasarelas disponibles para este criptomoneda → cambio ok.
- Verde: a partir de tres o más pasarelas disponibles para esta criptomoneda → cambio ok, la garantía de un funcionamiento óptimo.

Es posible, pero no recomendable, operar con una criptomoneda en la que sólo se utilizarían dos nodos pasarelas, lo que hace que la protección por prueba de participación sea potencialmente frágil (sistema que designa la respuesta correcta en caso de desacuerdo entre nodos).

En caso de desconexión de uno de los dos nodos pasarelas, sólo quedaría uno en servicio, lo que prohibiría el comercio de esta criptomoneda. No obstante, se concluiría un intercambio que estaría en curso en ese momento de forma normal o bien utilizando los tokens SSW de garantía por el nodo desconectado (si este último conservaba cualquier contraprestación recibida antes de la desconexión).

Para asegurar un inicio óptimo del servicio, *Grey Matter Technologie SpA* operará tres nodos pasarelas para cada criptomoneda gestionada inicialmente, hasta que la comunidad tome el relevo.

INDICACIONES ACCESIBLES DESDE LOS NODOS PASARELAS

Los nodos pasarelas mantendrán continuamente actualizadas las estadísticas de la red para producir información diversa para los NodeOwners, traders y operadores de nodos de operaciones de arbitraje y de margen de trading. Estas estadísticas permitirán entre otras cosas:

- Proporcionar un tablero de estadísticas avanzadas sobre los nodos.
- Evaluar la compensación esperada basada en los tokens SSW asignados a un nodo pasarela.
- Para comprobar los volúmenes de intercambios a lo largo de un período de tiempo por criptomoneda.
- Indique el tipo de cambio de los tokens SSW para cada criptomoneda, etc.



COMERCIO SEGURO, LA APLICACIÓN CLIENTE DE TRADING

Secure Trade, es una aplicación de trading que proporciona herramientas avanzadas y una cartera de múltiples wallets. Secure Trade se desarrollará principalmente para ordenadores con sistemas operativos Windows, Linux y MacOS, antes de ser portado a IOS y Android en su versión móvil.

CONNEXION

En el momento del lanzamiento, Secure Trade debe conectarse a un mínimo de tres nodos pasarelas antes de permitir las operaciones del usuario.

LOS WALLETS

Para la gestión de los diferentes tipos de billeteras, la aplicación Secure Trade utiliza un sistema de plugins que define una interfaz de programación común.

Los plugins de wallets gestionados por Secure Trade se instalarán desde los repositorios de plugins. Secure Trade gestionará una lista de depósitos que pueden ser actualizados. El usuario puede añadir una billetera para una criptomoneda y sólo tiene que seleccionar el plugin correspondiente de una lista el cual se instalará en Secure Trade.

Esto le permite agregar wallets para otras criptomonedas, descargando el plugin, sin tener que modificar la aplicación Secure Trade.

Por lo tanto, cuando añada una criptomoneda a Secure Swap, agregando un nodo pasarela a una blockchain, también debe proporcionar el correspondiente plugin de wallet para la aplicación Secure Trade.

Las carteras de hardware, como Trezor, Ledger, etc., también se gestionarán a través de sus respectivos plugins.

Si aparecen nuevas carteras de hardware en el mercado, bastará con desarrollar y añadir el plugin correspondiente.

La consulta del saldo de las carteras, la emisión de transacciones, etc. se realiza a través del soporte de nodos pasarela conectados a clientes Secure Trade. Si el nodo conectado no puede ejecutar una operación por sí mismo, dirige ésta a un nodo capaz de ejecutarla (la capacidad de ejecución depende de la blockchain afectada por la operación y de la blockchain a la que está conectado el nodo pasarela).



GRÁFICOS, DATOS EN TIEMPO REAL

Los datos del gráfico de precios para cada criptomoneda se derivan del historial de precios generado por las transacciones en Secure Swap.

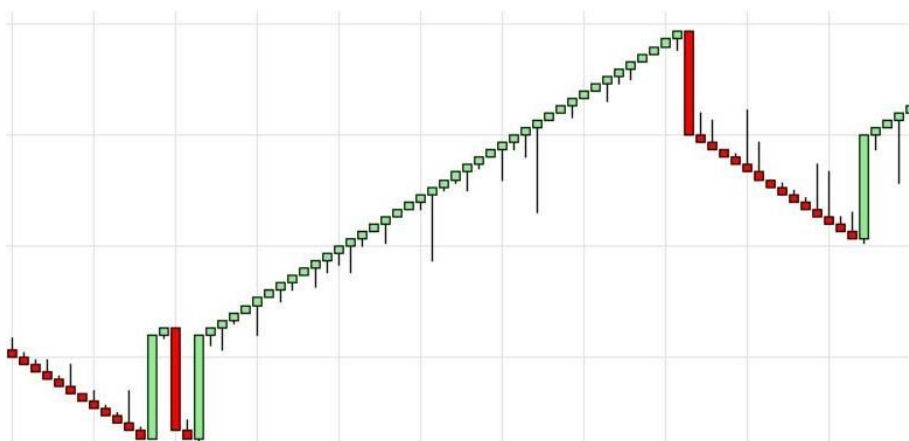
Nuevamente son los nodos pasarelas los que almacenan los historiales de precios, cada uno para la blockchain a la que está conectado. Cuando son puestos en marcha los nodos pasarelas, recuperan estos históricos de los nodos pasarelas ya conectados a la misma criptomoneda.

Secure Trade recibe los datos brutos de los nodos pasarelas marca por marca, es decir, transacción por transacción, y los representa según los parámetros elegidos por el trader.

Además de los clásicos gráficos temporales, en los que el trader puede elegir el período (marcas, segundos, minutos, etc.), Secure Trade también ofrece las representaciones Kagi, Renko, Line Break, Harmonic Bar (un Line Break mejorado), Point and Figure, Volume, Volume Filter, Range.

El estilo gráfico por defecto es el clásico candelabro, pero se puede cambiar al estilo LineOnClose, Hi Lo u OHLC.

Ejemplo de un gráfico de tipo Harmonic Bar (ruptura 28 y tendencia 2) y candelabro:



LA CARTERA DE ÓRDENES

Como se ha mencionado anteriormente, Secure Trade es un nodo como cualquier otro desde el punto de vista de la transmisión de datos de la cartera de órdenes, por lo que recibe actualizaciones constantemente.

El módulo de cartera de la aplicación Secure Trade indica los volúmenes por nivel de precios (profundidad de la cartera de órdenes), pero también la fuente de liquidez por código de color.

Por ejemplo, verde para los volúmenes de la cartera de órdenes de Secure Swap, naranja para los volúmenes de los nodos de arbitraje. La distinción del origen de la liquidez es importante porque la que proviene de los



Libro Blanco Secure Swap

los nodos de arbitraje puede conducir a un intercambio ligeramente más lento que los intercambios que utilizan la liquidez procedente directamente de la red Secure Swap.

HERRAMIENTAS DE TRADING

Además de las herramientas clásicas y los diferentes tipos de órdenes disponibles que existen:

- Orden a mercado,
- Orden limitada,
- Orden stop,
- Orden condicionada,
- Orden condicionada con límite,
- Orden OCO "order cancel order order",
- Múltiples órdenes condicionadas,

Secure Trade cuenta con módulos de soporte de scalping y money management, ejecutando órdenes semiautomáticas definidas de antemano.

MARGEN DE TRADING

Cada nodo de margen de trading disponible tiene sus propias condiciones de operación de margen:

- Pares de criptomonedas autorizados para el margen de trading,
- Comisiones de entrada y salida de posiciones de margen,
- Niveles de margen inicial y mínimo (activación de un ajuste de márgenes si el margen es insuficiente),
- Interés por hora en posiciones de margen,
- Nivel de apalancamiento máximo.

Secure Trade muestra la lista de nodos de margen de trading disponibles y sus configuraciones.

Secure Trade dispone de filtros para seleccionar los nodos de margen de trading según estos criterios. También indica, para cada nodo, su identificador y su duración en línea sin desconexión, para que el trader pueda evitar los nodos más poco fiables. Saber que una desconexión de un nodo de margen de trading implica el cierre de las posiciones del trader.

TRADING AUTOMÁTICO

Secure Trade tiene un módulo de operaciones automático.



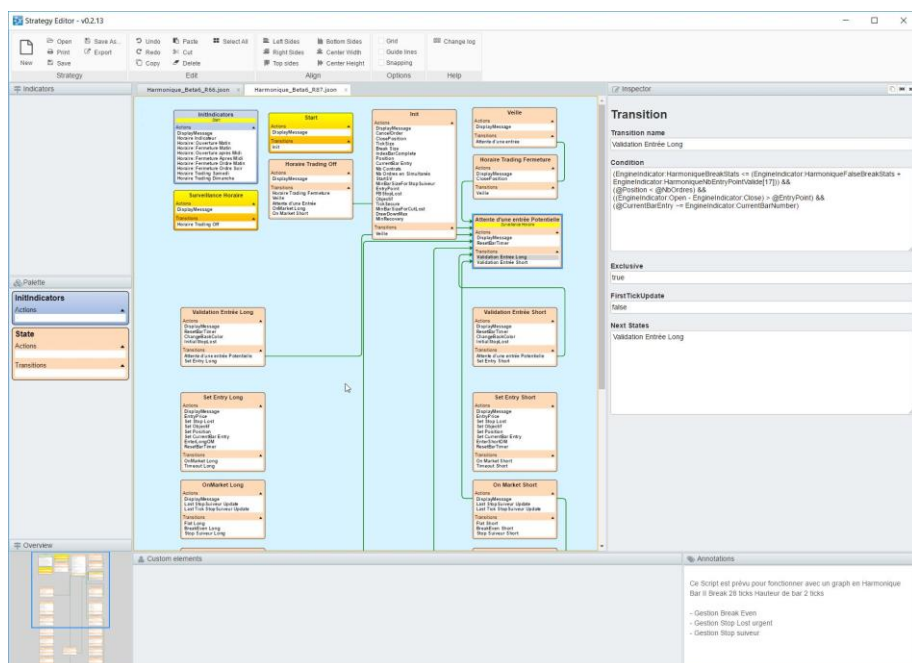
Libro Blanco Secure Swap

Este módulo consiste en una máquina jerárquica y competitiva (HCMS: Hierarchical Concurrency State Machines). Un lenguaje de programación simplificado, en la medida de lo posible, permitirá programar esta máquina de estados para ejecutar comandos de acuerdo con las condiciones programadas.

Estas condiciones pueden utilizar los resultados de todos los indicadores disponibles, así como los precios de los gráficos, el estado de los wallets, las indicaciones de money management, las indicaciones de tiempo, etc.

La programación de estas máquinas de estado se realiza a través de un editor gráfico, accesible incluso a personas que no tienen muchos conocimientos de programación.

La versión de desarrollo del editor de estrategias está en desarrollo:



Versión alfa del editor de estrategias.



¿CÓMO COMPENSAR LA FALTA DE LIQUIDEZ INICIAL?

Las plataformas tienen inevitablemente problemas de liquidez en su lanzamiento: cuando se ponen en servicio, sus carteras de órdenes están vacías, lo que no es alentador para los primeros traders. También pueden existir problemas de liquidez en las criptomonedas con bajos volúmenes de negociación.

En el momento de su puesta en marcha, Secure Swap no tendrá liquidez propia y tendrá que depender de la liquidez externa proporcionada por los nodos de arbitraje.

Para ello, *Grey Matter Technologies SpA* movilizará una parte de sus fondos. Estos fondos se dividirán en varias criptomonedas disponibles para los servicios de arbitraje (un nodo de arbitraje por plataforma de terceros). Inicialmente planeamos utilizar la liquidez de tres plataformas centralizadas.

Estos nodos de arbitraje serán operados por *Grey Matter Technologies SpA*, con fondos suficientes asignados a cada instancia conectada a una plataforma de terceros, para garantizar un funcionamiento eficiente en la provisión de liquidez.

Los miembros de la comunidad Secure Swap también podrán operar este tipo de nodos conectados a plataformas de terceros, lo que proporcionará aún más liquidez.



UNA PLATAFORMA CON CÓDIGO ABIERTO

Los diferentes tipos de nodos de la plataforma se distribuirán bajo licencia Open Source.

Esto significa que, además de servir a los traders, todos tendrán la oportunidad de apoyar el funcionamiento de la plataforma operando nodos conectados a blockchains, nodos de negociación a monedas fiduciarias, nodos de arbitraje (que proporcionan liquidez) y nodos de márgenes de trading.

Los NodeOwners de nodos pasarelas que operen y posean tokens SSW recibirán su parte de las tarifas cobradas durante los intercambios en proporción a los tokens que hayan asignado a un nodo pasarela de una blockchain, en proporción con el número total de tokens SSW asignados a los nodos pasarelas a la misma blockchain en funcionamiento.

Los otros tipos de nodos pueden generar sus propios ingresos de forma independiente, por lo que no están incluidos en este sistema de reparto de costos.

Grey Matter Technologies SpA operará de la misma manera y recibirá su parte de las tasas de cambio en proporción a los tokens SSW que poseerá al final de la ICO y que reservará para cada nodo pasarela a una blockchain.

También proporcionaremos un modelo de nodo de código abierto para el cambio a monedas fiduciarias, con interfaces para conectarse a procesadores de pagos bancarios. Dado que esta actividad está altamente regulada, y requiere tanto la adaptación para cada caso (normativas locales e interfaces con los procesadores de pagos utilizados) como el inicio de una actividad legal a explotar (a través de una empresa), el modelo de nodo que proporcionaremos en código abierto tendrá que adaptarse a cada caso particular.

Grey Matter Technologies SpA operará inicialmente este tipo de nodo para las regiones de América del Sur, Estados Unidos y Europa. Planeamos operar nodos de conversión de moneda fiduciaria para las siguientes monedas: peso chileno, peso argentino, sol peruano, USD y euro, y eventualmente otras divisas a futuro.

Así, gradualmente, esta plataforma podrá soportar conversiones a un gran número de monedas fiduciarias y regiones del mundo.



PROGRAMA DE BUG BOUNTY

Una parte de los fondos recaudados en el ICO se utilizará para financiar un servicio de pentesting y campañas de bug bounty. Las recompensas serán dadas a aquellos que participen en estos programas y que hayan reportado errores o violaciones de seguridad a nuestros equipos que aún son desconocidos.

Pentesting será utilizado durante las fases de desarrollo, bounty bug de las versiones candidatas a definitiva (RC).

En cada etapa de la fase de desarrollo se lanzará una campaña de bug bounty desde la versión candidata a definitiva, de modo que la primera versión de la plataforma de explotación haya sido bien analizada.

A continuación, se planificarán campañas trimestrales para apoyar la continuidad de los acontecimientos.

Estudiaremos la relevancia de utilizar los servicios de Buglab, una plataforma de la red Ethereum para este tipo de programas.

<https://buglab.io/#about>



ASPECTO FINANCIERO DE TOKEN

DATOS UTILIZADOS PARA ESTA PROYECCIÓN:

- Número total de tokens emitidos: 100,000,000
- Precio de emisión del token: \$ 0,45 USD
- Porcentaje de tokens realmente asignados a nodos pasarelas: 30%

Creemos que una parte de los compradores del token SSW, no operarán nodos pasarelas (y por lo tanto no se beneficiarán de la parte correspondiente de las tasas de cambio pagadas por los operadores) ya que sólo los comprarán por razones especulativas sobre el precio del token.

Una parte de los tokens se utilizará para operar los nodos de margen de trading.

Por lo tanto, creemos que un máximo del 30% de los tokens SSW se asignarán realmente a la operación de los nodos pasarelas. Cuanto menor sea la proporción de tokens asignados a la operación de estos nodos, mayor será el rendimiento de los tokens para aquellos que los operan.

Utilizaremos los datos de CoinMarketCap sobre volumen de intercambio diario de plataformas y la distribución de volumen entre criptomonedas, con datos recopilados a finales de julio de 2018 y así poder evaluar el posible rendimiento de los tokens de SSW para los compradores de estos al precio ICO y que operarán los nodos pasarelas con ellos.

Ejemplos de la repartición de la distribución de intercambios entre criptomonedas durante 24 horas:	
Bitcoin :	33%
Tether :	20%
Ethereum :	11%
EOS :	4.5%
OmiseGo :	0.45%

Tenemos aquí las 3 criptomonedas más intercambiadas, así como 2 criptomonedas menos intercambiadas.

Para evaluar un posible rango de rentabilidad probable, consideraremos diferentes escenarios para el volumen diario de operaciones de Secure Swap:



PROYECCIÓN DE LA RENTABILIDAD DE LA INVERSIÓN EN TOKEN SSW:

Consideramos que los tokens, que se asignan a la operación de los nodos pasarelas, se distribuirán en proporción al volumen de intercambios de cada criptomoneda.

Una sobreasignación de tokens a los nodos pasarelas de una criptomoneda reduciría la rentabilidad de los tokens para esa criptomoneda. Por otra parte, la sub asignación de tokens a otras criptomonedas aumentaría su rentabilidad. Esto significa que aquellos que operan nodos pasarelas tenderán a asignar sus tokens a las criptomonedas más rentables, lo que reducirá su rentabilidad y aumentará la de otras criptomonedas. Como resultado, la distribución de los tokens en los nodos pasarelas tenderá naturalmente a corresponder a la distribución de los volúmenes de intercambio entre las criptomonedas.

Fórmula para calcular la rentabilidad de tokens:

R	Rendimiento del token
TTOK	Total de tokens emitidos al ICO
FTAP	Porcentaje de tokens asignados a los nodos pasarelas
VE	Volumen de exchanges en \$ USD
FEC	Porcentaje de exchange de la criptomoneda en relación con el total intercambiado
FRTC	Porcentaje de repartición de tokens para nodos pasarela de la criptomoneda
PX	Precio de compra del token en \$ USD
T	Tarifas cobradas por la plataforma por los exchanges.

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

Vemos que si $FEC = FRTC$, obtenemos:

$$\text{Rentabilidad token: } R = \frac{(\sum VE \times T) / (TTOK \times FTAP)}{PX}$$

LA RENTABILIDAD ES POR LO TANTO PARA TODAS LAS CRIPTOMONEDAS SI $FEC = FRTC$, INDEPENDIENTEMENTE DE SU VOLUMEN DE INTERCAMBIOS.



Libro Blanco Secure Swap

Por ejemplo:

Tomemos un volumen de operaciones de 3 millones de dólares diarios (100º lugar en CoinMarketCap)

En un año, eso nos hace: $\sum VE = 365 * 3 = \$1,095$ millones USD

La comisión de cambio es $T = 0.15\%$, entonces tenemos:

Rentabilidad = $((1\,095\,000\,000 * 0.0015) / (100\,000\,000 * 0.3)) / 0.45 = 12.2\%$ de rendimiento anual

Con un volumen de operaciones de 10 millones de dólares diarios (75º lugar en CoinMarketCap)

Rentabilidad = $((10\,000\,000 * 365 * 0.0015) / (100\,000\,000 * 0.3)) / 0.45 = 40.6\%$ de rendimiento anual

Con un volumen de operaciones de 20 millones de dólares diarios (50º lugar en CoinMarketCap)

Rentabilidad = $((20\,000\,000 * 365 * 0.0015) / (100\,000\,000 * 0.3)) / 0.45 = 81.1\%$ de rendimiento anual

Y si, a pesar de sus ventajas, Secure Swap no lo hiciera mejor en términos de volumen negociado que el DEX promedio, al menos en el primer año en el momento en que se adopte masivamente, todavía estaría alrededor de 1,2 millones de dólares negociados al día (sobre el volumen de Bancor, Crypto Bridge y Wave DEX) y la rentabilidad sería:

Rentabilidad = $((1\,200\,000 * 365 * 0.0015) / (100\,000\,000 * 0.3)) / 0.45 = 4.8\%$ rendimiento anual



CONCLUSIONES:

Creemos que, con sus ventajas, Secure Swap alcanzará rápidamente los volúmenes de operaciones de los DEXs más activos, como Bitshare, IDEX y OpenLedger.

Esto representa alrededor de 400 BTCs de intercambio diario, es decir, con un BTC de \$6,000 USD, un retorno de alrededor del **10% por año en tokens SSW**.

Por lo tanto, consideramos que Secure Swap es capaz de ganar una significativa parte del mercado de las plataformas centralizadas, lo que aumentará la rentabilidad de los tokens SSW para hacer funcionar los nodos pasarelas o nodos de margen de trading.

No hemos cuantificado la rentabilidad de la actividad de margen de trading, ya que depende demasiado de las elecciones de configuración hechas por sus operadores y el volumen de margen.

Del mismo modo, no hemos cuantificado la rentabilidad de un nodo de arbitraje o de un nodo de cambio de divisa fiduciaria, que depende de demasiados parámetros actualmente desconocidos, como el volumen de liquidez proporcionada y realmente utilizada en la red Secure Swap, la posibilidad de beneficiarse de las diferencias de precio entre las plataformas, el volumen de los intercambios a cada divisa fiduciaria, etc.

Estas proyecciones nos muestran que la rentabilidad de los tokens SSW aumentan rápidamente con los volúmenes diarios intercambiados. Si Secure Swap toma una parte significativa del mercado de las plataformas centralizadas, que es objetivo para lo cual fue diseñado, entonces el token SSW podría llegar a ser muy popular y rentable.



ICO, EL TOKEN ERC-20 SECURE SWAP (SSW)

¿POR QUÉ UN ICO Y LA CREACIÓN DE UN TOKEN ERC-20?

El token SSW, además de ser utilizado para recaudar fondos en el ICO, servirá como prueba de participación y garantía de la seguridad operativa de la plataforma, así como de la distribución de las comisiones pagadas por los traders y recaudadas durante los intercambios.

DATOS DEL ICO

Nombre del token:	Secure Swap
Ticket:	SSW
Cantidad creada:	100 millones de tokens
Precio inicial del token:	0.45\$ USD
Reservado para el equipo:	10%
Reservado para asesores:	3%
Reservado para animadores sociales:	3%
Reservado para socios:	4%
Disponible para el ICO:	80%
Soft Cap:	10 millones de tokens
Hard Cap:	80 millones de tokens

Todos los tokens no vendidos son propiedad de *Grey Matter Technologies SpA* con el fin de servir como prueba de participación y garantía en el funcionamiento de los nodos pasarelas que serán operados por la empresa.

No es la idea que el equipo acumule los tokens no vendidos ya que esto constituiría un abuso de la propiedad social.

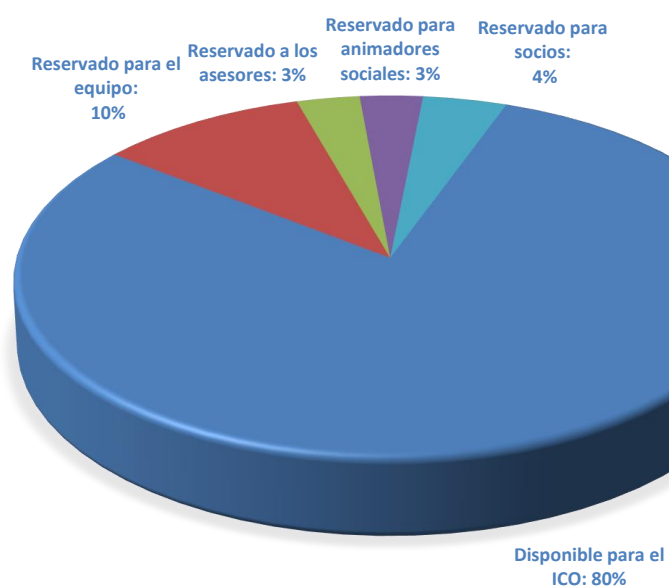
Estos tokens seguirán siendo propiedad de la Compañía, con el fin de utilizarlos como prueba de participación y garantía para operar los nodos, actuando la Compañía como NodeRunner(s) y operador de los nodos de margen de trading.

Esta será la principal fuente de ingresos de la empresa. Otros ingresos procederán de las tasas cobradas en las bolsas de fiat, así como de las ganancias obtenidas con los nodos de arbitraje.

Grey Matter Technologies SpA se reserva el derecho prioritario de readquirir los tokens SSW asignados al equipo y a otros colaboradores (asesores, animadores sociales y asociados) con el fin de aumentar su parte correspondiente a los costos pagados por los traders.



DISTRIBUCIÓN DEL ICO





Libro Blanco Secure Swap

ASIGNACIÓN DE FONDOS:

Indicaremos aquí la asignación de fondos de acuerdo con dos casos extremos: Soft Cap alcanzado y Hard Cap alcanzado.

SOFT CAP ALCANZADO:



El soft cap es el presupuesto necesario para desarrollar el producto mínimo viable.

Corresponde a US\$ 4,5 millones.

Presupuesto de desarrollo: US\$ 1,35 millones

- Secure Trade simplifica la aplicación de trading para clientes (Sólo para el trading en blockchain Ethereum): \$400K USD
- Modelo de nodo pasarela + contrato inteligente sin controles en los nodos de margen de trading: \$450K USD
- Especialización del modelo de nodo de pasarela para la blockchain Ethereum + tokens: \$100K USD
- Modelo de nodo de arbitraje: \$350K USD
- Especialización en modelos de nodos arbitraje para un tercero: \$50K USD

Funcionamiento del nodo de arbitraje por *Grey Matter Technologie SpA*:

Reserva en efectivo requerida: US\$ 1 millón

- 70% Ethereum
- 30% dividido en fichas ERC-20 / ERC-223 / ERC-777

Programa Bug Bounty: US\$ 500K

Publicidad: US\$ 1 millón

Legal: US\$ 350K

Fondo de reserva: US\$ 300K



HARD CAP ALCANZADO:



El hard cap es el presupuesto necesario para desarrollar el producto con todas sus funcionalidades, lo que corresponde a 36 millones de dólares USD.

Presupuesto de desarrollo:US\$ 3,7 Millones

- Aplicación cliente Secure Trade completa: US\$ 800k
 - Operar en todas las blockchains
 - Margen de Trading
 - Colocación de órdenes en el gráfico
 - Módulo de ayuda para el «money management»
 - Módulo de trading automático programable
- Modelo de nodo pasarela + controles de margen de trading + «smart contract»: US\$ 700k
- Especialización del modelo de nodo pasarela
 - Para blockchain Ethereum + Tokens: US\$ 100k
 - Para blockchain Bitcoin: US\$ 50k
 - Para blockchain Tether: US\$ 50k
 - Ripple: US\$ 50k
 - Bitcoin Cash: US\$ 50k
 - EOS: US\$ 50k
 - Litecoin: US\$ 50k
 - Stellar Lumens: US\$ 50k
 - Monero: US\$ 50k
 - Dash: US\$ 50k
 - Neo: US\$ 50k
 - Zcash: US\$ 50k
- Nodo de margen de trading + SC (smart contract): US\$ 750k
- Modelo de nodo arbitraje: US\$ 350k
- Especialización del esqueleto del nodo de arbitraje para tres plataformas de terceros: 3*50k = US\$ 150k
- Modelo de nodo de cambio a moneda fiduciaria + SDK: US\$ 300k



Libro Blanco Secure Swap

Funcionamiento de tres nodos de arbitraje por *Grey Matter Technologies SpA*: 3 x US\$ 4M:US\$ 12 Millones

Distribución por nodos de arbitraje:

- Bitcoin US\$ 1,3 millón
- Tether US\$ 1 millón
- Ethereum y tokens US\$ 1 millón
(70% Ethereum, 30% tokens ERC-20 / ERC-223 / ERC-777)
- Ripple US\$ 300 K
- Otra criptomonedas US\$ 400 K

Operación de un nodo de margen de trading por *Grey Matter Technologies SpA* :US\$ 4 Millones

Distribución de fondos entre criptomonedas similar a un nodo de arbitraje, pero reducida a una parte de las criptomonedas sobre la base de criterios de volatilidad.

Apertura y funcionamiento de cinco entidades jurídicas para operación de conversiones a monedas fiduciarias y servicios de pago,

USD, EUR, CPL (pesos chilenos), SOL (sol peruano), ARS (pesos argentinos): 5 * \$US 1M\$US 5 Millones

Por entidad: \$US 1 millón

- Legal: US\$ 400 K
- Estructura (creación de empresas, personal...): US\$ 200 K
- Plataforma técnica: US\$ 100 K
- Especialización del modelo de nodo de cambio a moneda fiduciaria: US\$ 100 K
- Publicidad: US\$ 100 K
- Fondo de reserva: US\$ 100 K

Preferimos tener entidades independientes para la explotación de los medios de pago y los intercambios entre las criptomonedas y las monedas fiduciarias con el fin de garantizar la clara separación legal entre Secure Swap / *Grey Matter Technologies SpA* y los intercambios fiduciarios, con el fin de proteger a *Grey Matter Technologies SpA* y al núcleo de Secure Swap de los riesgos regulatorios relacionados con los intercambios fiduciarios.

Programa Bug Bounty:US\$ 2,5 Millones

Publicidad:US\$ 6 Millones

Legal: US\$ 1 Millón

Fondo de reserva:US\$ 1.8 Millones



ROADMAP

Este roadmap es lo planificado si se alcanza el Hard Cap del ICO. Si esto no se cumple el proyecto está diseñado en módulos independientes. El desarrollo de cada módulo puede posponerse hasta que los ingresos generados permitan el autofinanciamiento de la realización de estas funcionalidades.

En el roadmap, las características que pueden esperar en el tiempo están marcadas con un asterisco (*).

Las mejoras en la plataforma, la incorporación de criptomonedas (nodos pasarelas) y otros, continuarán más allá de este roadmap.

ROADMAP ICO





Libro Blanco Secure Swap

ROADMAP SECURE SWAP





TEAM:

MIEMBROS FUNDADORES



Alain Saffray
CEO – Co fundador
Ingeniero de desarrollo

Más de 30 años de experiencia en desarrollo de softwares, Alain es un programador muy experimentado con sólidos conocimientos técnicos.
Su experiencia previa en varias industrias informáticas, que van desde la gestión, los videojuegos, el procesamiento de imágenes y el diseño de robots de comercio automático, le ha permitido cubrir muchos aspectos técnicos difíciles del desarrollo de software.
Todas estas experiencias le permiten gestionar cualquier proyecto con confianza y pragmatismo.
También es cofundador de Montmartre Spa, que se convirtió en el holding de Grey Matter Technologies.

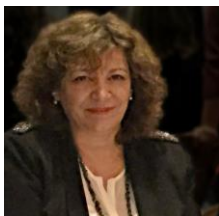
<http://www.viadeo.com/p/0021oc3uxefhcfu2>



Philippe Aubessard
CTO – Co fundador
Ingeniero de desarrollo

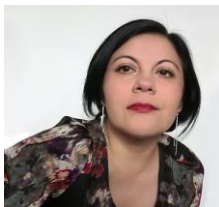
Con más de 35 años de experiencia en TI, Philippe cuenta con una amplia gama de experiencia y conocimientos técnicos.
Líder dinámico, ha desarrollado una serie de tecnologías innovadoras, desde la I+D hasta el mercado.
Fundador de muchos proyectos, trabajando con una docena de empresas de todos los tamaños y tipos, tiene una amplia experiencia en TI, I+D, desarrollo de productos, ingeniería y control de calidad.
Es un experto en seguridad informática, especialmente en el área móvil.

<http://www.viadeo.com/en/profile/philippe.a>



Nadine Miotti
Co fundadora

Más de 25 años de experiencia en negocios y relaciones públicas.
Ejecutivo de Grandes Cuentas para Empresas Financieras y Bancos.
“Una mirada constante a la innovación y al futuro - una persistencia que no teme a la adversidad, me acerco al mundo de las cripto-divisas con entusiasmo”.



Alicia Laura
Co fundadora

Como inversionista en varios proyectos, particularmente en el área salud, me entusiasma participar en este proyecto innovador y desafiante.

Co fundadora de Montmartre Spa, que se convirtió en el holding de Grey Matter Technologies.



EQUIPO



Victor Chukholskiy
Ingeniero de Blockchain
Especialista Smart Contract

Experto en tecnología Blockchain y contratos inteligentes con Solidity.
Su experiencia técnica le permite evaluar y abordar retos de programación complejos.



Rafael Romero Carmona
Cloud Arquitecto
Ingeniero DevOps

Totalmente apasionado en todo lo relacionado con la nube, la automatización y la optimización.

Feliz y curioso friki de todas las ciencias que puedas imaginar.



Zhan Wei - 詹玮
Ingeniero de
seguridad móvil

Líder Experto Anti-hack

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
Ingeniero
Arquitectura de Software

30 años de experiencia en informática empresarial, en el sector retail.

Definición de arquitecturas de software, modelado de procesos, modelado de datos, gestión de proyectos, diseño, etc.

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



Kevin Vanstaen
Animador Social

Productor de contenidos digitales desde 2013, me informo y participo a mi propia escala en la emancipación de la blockchain.



Henry Morera
Animador Social

Coach de desarrollo personal, también tengo curiosidad por todo lo relacionado con la tecnología.

Interesado en las criptomonedas, mi participación en este proyecto es una oportunidad para jugar un papel activo en este campo.



Sonia Montella
Animador Social

Qué oportunidad para participar en este ambicioso y necesario proyecto: ofrecer una plataforma confiable y ergonómica para finalmente operar con monedas criptográficas con confianza y a un menor costo.

Respondo a todas sus preguntas



Lulia Galea
Animador Social

Mi nombre es Valentina y estoy deseando conocerte. Me interesa la ciberseguridad, cómo se crean los espacios virtuales y cómo podemos protegerlos de los ciberataques.

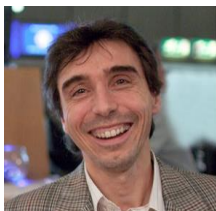
Mi curiosidad me lleva a adquirir diferentes habilidades técnicas, lo que me convierte cada día en un mejor experto.

Por eso estamos todos aquí, para crear y ofrecerte el lugar más seguro para tus transacciones.

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



CONSULTORES



Renaud Desportes
CEO de DoCaption
Director de Desarrollo

Más de 25 años de experiencia internacional en gestión de productos, incluyendo desarrollo de hardware y software.

Sólida experiencia en la construcción y mantenimiento de relaciones con los clientes: desarrollo de estrategias de ventas y marketing, expansión de redes de revendedores en todo el mundo, pre-ventas, soporte al cliente y formación.



Edouard Enault
Analista financiero
CEO de Aeroshot

Especialista en mercados financieros (analista de ventas) y fundador del especialista en filmación aérea Aeroshot (aeroshot.fr).

Entusiasta inversor de blockchain y criptografía desde 2016.



Richard Shibi
Advisor

Richard Shibi tiene más de 15 años de experiencia en la industria de TI. Se ha desempeñado como consultor de gestión senior y ejecutivo de cuentas regional para proyectos de TI desplegados a escala global en la industria de las telecomunicaciones (Norteamérica, Europa, Rusia, Oriente Medio, China y Sudáfrica).

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



ASPECTOS LEGALES

IMPLICACIONES LEGALES CON TOKENS SSW

No podemos garantizar cambios futuros en el precio del token SSW, su posible presencia en los listados de intercambiadores o la posibilidad de reventa. La posesión de los tokens no otorga ningún derecho de participación, control o decisión sobre Grey Matter Technologies SpA. Independientemente del resultado de la ICO, el token no es reembolsable. El inversor o especulador asume plenamente el riesgo de la compra.

Debido al aspecto comunitario de Secure Swap, y al hecho de que los intercambios entre criptomonedas forman parte de un sistema de gobierno distribuido y autónomo (DAO), fuera del control de Grey Matter Technologies SpA, el token Secure Swap es un token de "Seguridad", una clasificación por defecto según la SEC, utilizada como prueba de participación para asegurar los intercambios dentro del sistema abierto. Permite obtener beneficios y sirve principalmente como garantía para la seguridad de los intercambios.

Como Secure Swap es un intercambio abierto, distribuido y basado en la comunidad sin gobierno central, esto implica el anonimato de los usuarios, al menos tanto como lo permitan las criptomonedas intercambiadas. Por lo tanto, parece impensable pedir la identidad de los inversores o su prueba de residencia para verificar sus derechos de participación en esta ICO.

En consecuencia, **corresponde a los inversores asegurarse, dependiendo de su país de residencia, de la legalidad para participar en esta ICO**, y abstenerse de hacerlo en caso de ilegalidad o duda.

Cabe señalar que la participación en una ICO está actualmente totalmente prohibida en China y Corea del Sur, independientemente de la naturaleza del token.

Para los ciudadanos estadounidenses, es su responsabilidad **verificar con la SEC la legalidad de participar en esta ICO**. Debido a la naturaleza predeterminada de "Seguridad" del token SSW, sólo los inversores confirmados pueden participar en este ICO.

Para los ciudadanos europeos, al participar en este ICO, **usted declara que no es un consumidor en el sentido de la Directiva Europea 2011/83/EU de 25 de octubre de 2011 sobre derechos de los consumidores**.

Para los nacionales rusos y los de todos los demás países en general, **es su responsabilidad verificar con las autoridades reguladoras locales la legalidad de participar en esta ICO**.

Sobre los nodos de conversión de criptomonedas a monedas fiduciarias:

Este tipo de nodo implica una estructura legal y el cumplimiento de las leyes locales del lugar de operación, incluyendo **las regulaciones (KYC/AML/CFT/FCA) relativas al fraude, lavado de dinero o cualquier otra actividad delictiva**.



LA COMPAÑÍA QUE EXPLOTA LA PLATAFORMA

- *Grey Matter Technologies SpA* explotará la plataforma, es decir: los nodos pasarelas, el nodo de arbitraje y los nodos de conversión a la moneda fiduciaria.

www.greymattertechs.com

- *Grey Matter Technologies SpA* es una compañía bajo la jurisdicción chilena.

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

Fojax: 60729 n° 31132 año 2018



- Motivamos a todos los voluntarios a respaldar el sistema ejecutando sus propios nodos pasarelas y también a utilizar las conversiones a moneda fiduciaria por su propia cuenta, por supuesto con su total responsabilidad del cumplimiento de las leyes y reglamentaciones locales, correspondientes a la ubicación de la explotación de estos sistemas.



FAQ

FAQ SECURE SWAP:

Q1: ¿Qué es Secure Swap?

R1: Secure Swap es una plataforma descentralizada (DEX), con un aspecto comunitario. Es desarrollada por la sociedad Grey Matter Technologies, ubicada en Chile con un equipo fundador francés.

Q2: ¿Qué criptomonedas admite?

R2: Potencialmente, todas las monedas digitales pueden intercambiarse. Inicialmente funcionará con las criptomonedas más populares y las otras serán añadidas progresivamente.

Q3: ¿Secure Swap soporta las conversiones con las divisas fiat?

R3: Si, este aspecto está previsto. En su inicio trabajará con monedas sud americanas.

Su aspecto comunitario permite a otras sociedades trabajar con intercambios de diferentes divisas fiat a criptomonedas.

Q4: ¿En qué consiste el aspecto comunitario de Secure Swap?

R4: El proyecto está bajo licencia Open Source. Su arquitectura se apoya en una red de nodos tipo p2p. Aquellos usuarios que estén interesados, pueden hacer funcionar estos nodos.

Q5: ¿Cuál es el interés de la comunidad en hacer funcionar estos nodos p2p?

R5: Los usuarios que hacen funcionar los nodos p2p, y que ayudan al funcionamiento del servicio, recibirán una parte de las comisiones pagadas por las plataformas de los traders. Por lo tanto, serán automáticamente remunerados a prorrata de tokens SSW que serán atribuidos a estos nodos.

Q6: ¿Cómo se atribuyen los tokens SSW a un nodo?

R6: En la configuración del nodo indicamos el wallet que contiene los tokens SSW que atribuimos a ese nodo. Este wallet es atribuido solamente a un nodo. Los tokens asignados al nodo son transferidos a un wallet administrado por un contrato inteligente, y serán devueltos cuando este nodo termine. Estos sirven de garantía de los intercambios.



Libro Blanco Secure Swap

Q7: ¿Cómo puedo obtener estos tokens de SSW?

R7: Grey Matter Technologies está lanzando esta ICO mediante la emisión de tokens SSW. Posteriormente, estos tokens pueden intercambiarse al menos en Secure Swap.

Q8: ¿Cómo se calcula la remuneración?

R8: Los nodos están especializados para cada blockchain. Proporcionan la conexión de la red p2p a blockchains, y se llaman "nodos pasarelas". Para cada blockchain hay varios nodos pasarelas, cada uno con tokens de SSW asignados.

Q9: ¿Cómo garantizará Grey Matter Technologies los beneficios con este sistema?

R9: Al igual que los NodeOwners, la compañía operará los nodos p2p asociando los tokens que tendrá al final de la ICO (los que no se venderán).

Q10: Y en caso de que la empresa venda todas sus fichas durante la ICO, ¿terminaría sin tokens de SSW?

R10: La compañía podrá generar ganancias a través de intercambios de criptomonedas a monedas fiduciarias, que no se comparten a través del sistema de tokens, sino que se devuelven por completo a los operadores de dichos intercambios. También puede eventualmente comprar tokens de SSW, una vez que el servicio funcione.

Q11: ¿La compañía Grey Matter Technologies se reserva intercambios a monedas fiduciarias?

R11: No, debido a su característica Open Source y a su aspecto de comunidad, Secure Swap permite a cualquiera que lo desee, hacer uso de las pasarelas de exchanges a monedas fiduciarias. Sin embargo, esto requiere de una estructura legal y cumplir con las regulaciones del lugar donde operan estos intercambios. Grey Matter Technologies proyecta comenzar a operar con monedas fiduciarias en Chile, Perú y Argentina.

Q12: ¿Cómo atrae Secure Swap a los traders?

R12: Secure Swap ofrece una aplicación cliente dedicada al trading basándose en una red de nodos pasarelas. Esta aplicación se beneficia de toda nuestra experiencia en el desarrollo de softwares de inversiones en la bolsa electrónica. Su ergonomía será mucho mejor que las plataformas actuales y ofrece un conjunto de herramientas innovadoras de trading.



Q13: En esta comunidad y sistema de código abierto, ¿cómo garantizar la seguridad de los exchanges?

R13: El conjunto de nodos pasarelas a una criptomoneda responden a la solicitud de las aplicaciones cliente que participan en un intercambio. Si los nodos responden de manera diferente, hay un intento de hackeo. En este caso, un sistema basado en una prueba de participación (Proof of Stake), eliminando los nodos no conformes y desconectándolos.

Q14: ¿Cómo funciona este sistema de prueba de participación?

R14: Cuando los nodos dan respuestas diferentes durante los pasos de validación de un intercambio, la respuesta de referencia se convierte en la respuesta mayoritaria en todos los nodos, cada uno de los cuales tiene un peso de voto correspondiente a los tokens SSW asignados a su operación. Los nodos que responden de forma diferente se desconectan. Por lo tanto, para intentar robar una transacción, sería necesario invertir una cantidad de tokens SSW que representen más de la mitad de los tokens asignados a los nodos de pasarelas de esta criptomoneda. Esto representa un valor más alto que el robo de una transacción. En cualquier caso, este robo no tiene ninguna posibilidad de éxito porque, tan pronto como se detecta una anomalía, se cancela la transacción. Además, si el operador de dicho nodo mantuviera a las contrapartes de las transacciones, sus valores se cargarían de los tokens SSW asignados como garantía en este nodo por una cantidad equivalente, convertidos en la criptomoneda esperada por el operador y enviados a este último. Si el pirata pusiera recursos significativos para tomar el control de todos los nodos pasarelas, esta operación sería en última instancia una pérdida para el pirata, probablemente muy costosa, dado el número de tokens que tendría que invertir para hacer esto y que se perderían. Para el pirata la operación consistiría en comprar todas las criptomonedas que desvía a precio de mercado, y en asumir todos los costos generados por estas operaciones. Los operadores siguen recibiendo las contrapartidas para sus operaciones según lo previsto.

Q15: Si los nodos son pirateados y quedan bajo control malicioso, ¿cómo se puede garantizar que este sistema de seguridad seguirá funcionando?

R15: Inicialmente, los nodos pasarelas no están corrompidos, lo sabemos porque nosotros mismos lanzaremos los primeros nodos cuando comience el servicio. Dado que Secure Trade espera la confirmación de todos los nodos pasarelas a una criptomoneda para enviar activos, si todos ellos no proporcionan la misma respuesta significa que existe un problema. Los clientes que participan en este intercambio cancelan la transacción e informan a toda la red p2p. Al final, el pirata paga por el desvío de las contrapartes, que por lo tanto siempre se entregan a los traders. Y su nodo estará desconectado de la red.

Q16: ¿Qué medidas se están tomando para luchar contra los piratas informáticos?

R16: Además de los protocolos descritos en las respuestas anteriores y que el proyecto Secure Swap está disponible para todos en Open Source, lanzamos campañas de Bug Bounty cada 3 meses con una recompensa para aquellos que encuentren un error en el sistema.