LIBRO BLANCO SECURE SWAP

Grey Matter Technologies

[Email address]

LIBRO BLANCO SECURE SWAP

CONTENTS

PRESENTACIÓN DE SECURE SWAP

Las secciones “resumen” y “destacados” son para aquellos que no desean leer el documento completo en detalle, o para aquellos que desean obtener una idea preliminar rápida de este proyecto antes de leer más.

RESUMEN:

Secure Swap, una nueva generación de Exchanges:

Puede funcionar sin el apoyo de una compañía operadora debido a su arquitectura p2p y la ausencia de servidores centrales.

Es open source.

Su tecnología es altamente modular, lo que permite agregar servicios (soporte de criptomoneda, soporte de Exchange fiat) por quienes lo desean y, por lo tanto, convertirse en participantes del sistema.

Permite a sus usuarios obtener una fuente de ingresos al respaldar el funcionamiento comunitario.

Su tecnología inspirada en el sistema de intercambio de archivos Torrent, hace que el sistema esté protegido ante regulaciones y prohibiciones súbitas de cripto-monedas, ofreciendo una posibilidad de salida siempre disponible.

Es completamente anónimo, al menos tanto como lo permiten las criptomonedas intercambiadas.

Sin embargo, gracias a su sistema modular se permite una clara separación de exchanges cripto monedas con monedas fiat ,permitiendo respetar plenamente las regulaciones vigentes.

Este último aspecto también permite a quienes lo deseen ejercer legalmente una actividad profesional de intercambio de criptomonedas hacia divisas fiat.

Integra sistemas de detección de anomalías que detienen automáticamente los intercambios en las criptomonedas afectadas por un intento de pirateo, gracias a su protocolo operativo.

Su aplicación trading ofrece un nivel de comodidad y ergonomía comparable al mejor software de trading en los mercados clásicos.

PUNTOS FUERTES:

SEGURIDAD:

- Sistema asegurado por diseño, con detección de intentos de piratería, alerta y detención automáticas de las partes implicadas.
- Sistema realmente descentralizado, los usuarios permanecen en posesión de sus criptomonedas hasta el momento de un intercambio.
- Por su naturaleza totalmente descentralizada sin intermediarios, es libre de las presiones de los reguladores que intentan prohibir su uso.
- No hay concentración de criptomonedas, que es un objetivo de elección para los piratas informáticos en los exchanges centralizados y descentralizados que concentran criptomonedas para funcionar.
- Un sistema abierto que permite a cada utilizador controlar el código, el funcionamiento y la seguridad.

DISPONIBILIDAD:

- Sistema altamente redundante, que garantiza una resistencia a la avería, por lo tanto, una alta disponibilidad del servicio, incluso con una carga de funcionamiento.

CONTROL Y OPERACIÓN DE INTERCAMBIO 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.

EXCHANGE EXTENSIBLE:

- Por su naturaleza Open Source y modular, los usuarios que lo deseen pueden agregar el soporte de otras criptomonedas al exchange y también agregar las divisas fiduciarias de su elección.

UNA FUENTE DE INGRESO PARA LOS QUE APOYAN SU FUNCIONAMIENTO:

- Aquellos que apoyan la operación del servicio, operando partes del sistema (puertas de acceso a criptomonedas específicas), son recompensados ganando parte de las tarifas pagadas por los usuarios en los intercambios.
- Permite iniciar una actividad legal y profesional de intercambio de criptomonedas a moneda fiduciaria en lugares donde está permitido legalmente (nodos de conversión a divisas fiat).

UN EXCHANGE MUNDIAL:

- Las participaciones de la comunidad en diferentes divisas fiat, permitirá progresivamente, que el servicio sea mundial.

ESTADO DEL MERCADO

Exchanges centralizados

Las plataformas de exchanges centralizadas con frecuencia son víctimas de la piratería, con el consecuente robo de criptomonedas. Cuando esto sucede, muchos de sus usuarios son víctimas, con grandes sumas robadas por la concentración de fondos.

Además, una plataforma de exchange centralizada posee literalmente todas las criptomonedas que se le han enviado. De hecho, es el exchange que posee las llaves privadas de los wallets de los usuarios, los cuales deben confiar en él por completo, a pesar de los riesgos de piratería y bancarrota que puedan surgir.

Por otro lado, estos exchanges tienen la ventaja de tener un libro de órdenes centralizado, y por lo tanto una mejor liquidez y velocidad de ejecución de órdenes, que la mayoría de las plataformas descentralizadas no tienen.

Exchanges descentralizados

Las plataformas de exchange descentralizadas tienen a menudo una menor ergonomía en comparación con los exchanges centralizados y una menor liquidez, pero tienen a su favor una mayor seguridad, no necesitan intermediarios y los usuarios siempre tendrán el control y posesión de sus criptomonedas.

A menudo tienen una selección limitada de criptomonedas disponibles debido a que sus tecnologías dependen de la interoperabilidad de las criptomonedas intercambiadas, o a la disponibilidad del Atomic Swap.

Pocas plataformas descentralizadas permiten el intercambio de muchas criptomonedas diferentes y cuando se realiza hay a menudo una parte de sus sistemas que no son descentralizados (por ejemplo: tokens centralizados sirviendo como contrapartes de los exchanges o de garantía de liquidez). Esto representa un riesgo comparable al de los exchanges centralizados convencionales, con la diferencia de que no es el usuario quien toma este riesgo sino el operador del exchange.

La falta de confianza en la seguridad de las plataformas centralizadas en relación con los riesgos de piratería hace que muchos de los usuarios no se atrevan a dejar sus criptomonedas en estas plataformas y las retiren tan pronto sea posible mientras no las intercambian. Después deben regresar a la plataforma para operar de nuevo, lo que significa costos de transacción y demoras adicionales.

En vista que muchos utilizadores retiran sus criptomonedas de las plataformas centralizadas, se vuelven inútiles las órdenes clásicas como stop-loss, órdenes condicionadas y OCO. Los usuarios no se arriesgan a dejar sus monedas encriptadas en una plataforma, incluso con stop-loss, sino que prefieren almacenarlas en frío y no correr el riesgo de que se las roben.

Las plataformas de negociación existentes sufren frecuentemente de problemas de carga, incluso con interrupción de sus servicios durante períodos de alta actividad lo que a menudo corresponde a momentos en que sus usuarios presentan una mayor necesidad (pánico en los mercados).

Por otra parte, muchas plataformas existentes, ya sean centralizadas o no, tienen una ergonomía de uso incómoda (propiedad que ha mejorado en los exchanges recientes), algunos sitios son realmente acertijos a resolver, incluso para un utilizador experimentado en herramientas informáticas.

Los usuarios han aprendido a lidiar con estos problemas, pero estas situaciones dificultan la utilización de criptomonedas por parte de la mayoría de personas pues sigue siendo algo percibido como complicado, arriesgado y difícil de comprender.

SOLUCIONES PROPORCIONADAS POR SECURE SWAP

UNA PLATAFORMA DE EXCHANGE DESCENTRALIZADA, MODULAR, ABIERTA Y COMUNITARIA:

Para responder a estos problemas identificados, Secure Swap ofrece los beneficios de los exchanges centralizados y descentralizados: buena liquidez, **seguridad mejorada "por diseño"**, sin tener que confiar en intermediarios que guarden las criptomonedas de los usuarios y una ergonomía inspirada en los mejores softwares de trading bursátiles. Además, la tecnología de nodo p2p asegura una capacidad de alta carga y redundancia garantizando la confiabilidad y disponibilidad del servicio.

Secure Swap es también un sistema abierto que permite a cada utilizador controlar el código, el funcionamiento y la seguridad además de participar en su funcionamiento al admitir nodos de puerta de enlace a las criptomonedas. **Las tarifas de intercambio se redistribuyen en su totalidad** a quienes operan este tipo de nodo, en proporción a los tokens SSW que poseen. Por lo tanto, es una fuente de ingresos para todos aquellos que desean e invierten en el token SSW.

Secure Swap es un ecosistema de intercambio de criptomonedas, construido en torno a un servicio descentralizado, una aplicación cliente para trading, y micro servicios opcionales para aprovechar las nuevas opciones que ofrece esta nueva red. Estos micro servicios son nodos especializados como nodos de conexión a diferentes blockchains, nodos de conexión a procesadores de pago para exchanges con divisas fiats, nodos de arbitraje, etc.

La aplicación cliente y los nodos se comunican entre sí a través de la tecnología Peer to Peer (p2p), constituyendo así un servicio descentralizado.

La seguridad y la atomicidad de los exchanges están garantizados por contratos inteligentes (uno por blockchain) dedicados a esta tarea, inicialmente en la blockchain de Ethereum. Se llevará a otras blockchains que admiten contratos inteligentes como EOS, para garantizar la seguridad / atomicidad de los intercambios. Esto permite aumentar el número de transacciones realizadas por segundo, al agregar la capacidad de ejecución de cada blockchain. El conjunto de contratos inteligentes en cada blockchain forma una distribución de aplicaciones DAPP, asegurando la interoperabilidad entre blockchains, para los intercambios

Solo la aplicación del cliente Secure Swap conoce las claves privadas de los wallets del usuario. De este modo, puede firmar contratos destinados a las diferentes blockchains (firma fuera de línea). Como resultado, nadie puede firmar las transacciones en lugar de la aplicación cliente si hay un intento de robar las propiedades de los usuarios. El usuario sigue siendo el propietario de sus criptomonedas, a diferencia del uso de una plataforma de exchange centralizada, donde este último posee las criptomonedas almacenadas allí, mediante la posesión de las claves privadas.

Tan pronto como el usuario se desconecta del servicio de intercambio, deja el software cliente, las claves privadas de sus wallets, que están almacenadas localmente en su computadora se encuentran fuera de línea (equivalente a un "almacenamiento en frío"). Las claves privadas de sus wallets nunca serán transmitidas por Internet, ya que nunca han salido de la aplicación cliente.

Además, si el usuario tiene wallets de hardware (ledger, Trezor ...), las claves privadas correspondientes a estas carteras nunca se almacenan en su computadora, sino que permanecen seguras en sus wallets de hardware.

Tan pronto como el usuario conecta el cliente en la red p2p, está listo para operar / intercambiar sus criptomonedas, sin costos innecesarios de transferencias previo a un exchange, mientras tiene una seguridad comparable a un almacenamiento de sus coins en una billetera privada en almacenamiento en frio (‘cold storage’).

La aplicación cliente ofrece facilidad de uso y ergonomía comparable con los mejores softwares de trading disponible en los mercados clásicos (mercados de valores, contratos futuros, Forex ...). En particular, la aplicación cliente ofrecerá órdenes llamadas "avanzadas", tales como órdenes con rangos de activación, órdenes condicionales de rango múltiple, órdenes OCO ...así como también trading en el gráfico con órdenes condicionales al cruzar líneas horizontales o pendientes, en indicadores, etc.

Como Secure Swap agrega las órdenes de clientes a través de nodos p2p, esto permite conservar las ventajas de los intercambios centralizados: liquidez y velocidad de ejecución. Para reforzar la liquidez, un mecanismo de arbitraje (nodo de arbitraje) es responsable de garantizar esto, en el caso de un déficit interno, mediante el uso de una reserva de criptomonedas que pertenece a la sociedad y mediante el uso de libros de órdenes de otros exchanges a través de sus APIs.

ARQUITECTURA Y OPERACIÓN DEL EXCHANGE

La arquitectura de la red distribuida se basará en un núcleo (Core) de aplicación Java Scipt (base común p2p), que servirá para los diferentes módulos del ecosistema: cliente de trading, nodos p2p de pasarelas a blockchains, nodo p2p de arbitrajes (responsable de garantizar la liquidez del exchange), nodos de intercambio cripto / fiat, nodo que indica el estado de la red.

La aplicación cliente emite las órdenes dadas por el usuario a los nodos conectados, lo que les permite consolidarse. Los nodos propagan todas las órdenes recopiladas de nodo a nodo siempre que haya un cambio, de modo que cada nodo tenga el libro de órdenes completo. Como la aplicación cliente también es un nodo, ella recibe la totalidad de la orden emitida en la red p2p.

Cada aplicación cliente realiza el matching de sus propias órdenes, contra el libro de órdenes completo, con el fin de encontrar contrapartes a los órdenes que ha emitido.

Cuando se encuentra un matching (contraparte), la aplicación cliente informa a los nodos p2p conectados. Los nodos pasarelas a las blockchains implicadas en el exchange, informarán al contrato inteligente de cada blockchain que valida una solicitud de envío de criptomonedas a cada cliente implicado, a fin de recibir los fondos involucrados en el intercambio. Los contratos inteligentes de cada blockchain involucrada, una vez que los fondos fueron recibidos en los wallets que sirven para gestionar el intercambio y después de la validación de la atomicidad de cambio por un mecanismo específico (*), envían estas criptomonedas a los wallets destinatarias del intercambio. Si no se reciben todos los fondos involucrados en un intercambio después de un cierto período de tiempo, el intercambio se cancela y los fondos se devuelven a sus respectivos propietarios. Esto asegura la atomicidad de los intercambios. Después de completado el intercambio, las aplicaciones clientes retiran las órdenes que han sido efectuadas. cada aplicación cliente retira sus propias órdenes, lo cual actualiza el libro de órdenes global.

Aparte de los costos específicos a cada red blockchain, pagadas por los usuarios, los contratos inteligentes de intercambio recogen en cada exchange un pequeño porcentaje que será distribuido a los titulares de tokens SSW que operarán un / los nodos conectados a blockchains en prorrata de los tokens que posean, versus el número total de tokens asignados a cada blockchain. Ejemplo: Un usuario opera un nodo P2P que está conectado a la blockchain Ethereum (pasarela a Ethereum) se le asignarán 100 tokens entre aquellos que tiene para el funcionamiento de este nodo (a través de un wallet dedicado, pero sus tokens siguen siendo de su propiedad). Si otros usuarios también operan nodos P2P conectados a la blockchain Ethereum, y que todos estos nodos se han asignado 1.000 tokens para esto, entonces nuestro usuario recibirá un 10% (100/1000) de los cargos producto de todos los intercambios que implican Ethereums. Si tiene otros tokens de SSW y ejecuta otros nodos que se conectan a otras blockchains, también recibirá una parte de los cargos de cambio de otras blockchains. Este sistema de asignación por blockchain, ayuda a motivar a los usuarios para operar los nodos para conectar el exchange a las blockchains donde hay pocos nodos en funcionamiento, lo que tiende a reforzar la redundancia, así como la disponibilidad del sistema y su seguridad.

(*) Consulte la descripción detallada en la sección “Sistema de validación de la atomicidad de los exchanges”.

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: 50%

Creemos que algunos compradores de tokens de SSW no harán funcionar los nodos pasarelas a criptomonedas por lo que no podrán recibir la parte correspondiente de los cargos por exchange pagados por los usuarios, ellos sólo los comprarán por razones de especulación de precios de token. Incluso esta proyección del 50% de utilización de nodos pasarela, ya parece optimista y la realidad podría estar más cerca del 30%. Cuanto menor sea la proporción de tokens asignados al funcionamiento del nodo pasarela, mayor será el rendimiento de los tokens para aquellos que las hacen funcionar.

La siguiente información proviene de CoinMarketCap, tomada a fines de julio de 2018:

Al finalizar un período de caída de precio de criptomonedas, podemos esperar un aumento de los volúmenes de exchanges a niveles más altos, lo que aumentará la rentabilidad de los tokens utilizados para operar los nodos pasarela.

Repartición de la distribución de exchanges entre criptomonedas durante 24 horas:

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

Aquí tenemos las 3 criptomonedas más negociadas y 2 criptomonedas con menos exchanges.

Volumen de exchanges de diferentes plataformas durante 24 horas según su clasificación en CoinMarketCap:

Plataforma en el ranking 100: 3.000.000 $USD

Plataforma en el ranking 75: 10.000.000 $USD

Plataforma en el ranking 50: 20.000.000 $USD

PROYECCIÓN DE LA RENTABILIDAD DE LA INVERSIÓN EN TOKEN SSW:

Consideramos que los tokens asignados al funcionamiento de los nodos pasarela son proporcionales al volumen de intercambio de cada criptomoneda. La sobreasignación de tokens en nodos pasarela de una criptomoneda reduciría la rentabilidad de los tokens para esta criptomoneda. Por el contrario, la sub-asignación de tokens para otras criptomonedas aumentaría la rentabilidad de esta última. Esto implica que aquellos que ejecutarán nodos pasarela tenderán a asignar sus tokens a las criptomonedas más rentables, lo que reducirá su rentabilidad y aumentará la de los demás. Esto tendría como efecto la alineación de la distribución de tokens hacia los volúmenes de intercambio entre las criptomonedas.

Fórmula para calcular la rentabilidad de tokens SSW:

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.

RENTABILIDAD TOKEN SSW = ((∑ VE × FEC ÷ FRTC × T) / (TTOK × FTAP)) / PX

Vemos que si FEC = FRTC, obtenemos:

RENTABILIDAD = ((∑ VE × T) / (TTOK × FTAP)) / PX

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

-Si tiene un volumen de negociación de 3M $ USD por día (como la plataforma en ranking 100 de CoinMarketCap) vemos:

Al año: ∑ VE = 365*3M = 1.095 M$USD

Los costos del intercambio son: T = 0.15%

Por lo tanto, tenemos

Rentabilidad = ((1.095.000.000 * 0.0015) / (100000000 * 0.5)) / 0.45 = **7.3%** rendimiento anual

-Si tiene un volumen de negociación de 10M$ USD diarios (ranking 75 de CoinMarketCap)

Rentabilidad = ((10.000.000 * 365 * 0.0015) / (100000000 * 0.5)) / 0.45 = **24.33%** rendimiento anual

-Si tiene un volumen de negociación de 20M$USD diarios (ranking 50 de CoinMarketCap)

Rentabilidad = ((20.000.000 * 365 * 0.0015) / (100000000 * 0.5)) / 0.45 = **48.67%** rendimiento anual

CONCLUSIONES:

Al estudiar las diferentes plataformas en CoinMarketCap, podemos verificar que aquellas clasificadas sobre el ranking 100, son plataformas que rápidamente son abandonadas por los usuarios, teniendo un volumen muy pequeño de intercambios.

Creemos que, debido a sus ventajas, tan pronto como el número de criptomonedas intercambiables sea suficiente, Secure Swap no tendrá problemas para clasificarse en el ranking de las 100 principales plataformas.

Además, tan pronto como los NodeOwners (quienes hacen funcionar los nodos pasarela) tengan el soporte de sus criptomonedas en Secure Swap, ellos no tendrán ningún interés en usar otras plataformas de exchange; por lo que llegar al top de los 50 no nos parece una meta irreal.

Como resultado, a medida que los usuarios adopten Secure Swap, el rendimiento de los tokens SSW puede evolucionar del 7% al 48% anual. Si buscamos una situación intermedia con un volumen de operaciones correspondiente a las plataformas en el ranking de los 75 principales de CoinMarketCap, podemos esperar un rendimiento anual del 24% para los inversionistas que participarán en el ICO. Para aquellos que compren tokens SSW más tarde, dependerá del precio de compra. A menor precio de compra mayor el rendimiento, por el contrario, un precio de compra más elevado lo hará bajar.

Finalmente debe tenerse en cuenta que estas cifras de volúmenes de exchanges, sobre las cuales hemos realizado nuestra proyección, se encuentran en un período que sigue a la caída de la última burbuja de criptomonedas. Podemos suponer que, en los próximos meses, el mercado de criptomonedas comenzará a crecer nuevamente, lo que aumentará los volúmenes de intercambio y, por lo tanto, la rentabilidad del token.

SISTEMA DE VALIDACIÓN DE LA ATOMICIDAD DE LOS EXCHANGES

PARA INTERCAMBIOS DENTRO DEL ECOSISTEMA ETHEREUM (ETH Y TOKENS):

La atomicidad del intercambio está garantizada por completo por un contrato inteligente en la blockchain Ethereum.

Este contrato inteligente tiene la posibilidad, sin intervención externa, de verificar la recepción de los ETH / tokens y enviarlos de vuelta a los destinatarios.

Este tipo de intercambio se mejorará con la integración de Plasma / Lightning Network cuando estas soluciones de segundo nivel estén operativas y más desarrolladas. Esto aumentará significativamente la velocidad del exchange dentro del ecosistema de Ethereum.

PARA LOS INTERCAMBIOS ENTRE BLOCKCHAINS INTERCAMBIABLES:

Para los exchanges entre blockchains interoperables (por ejemplo, entre Litecoin y Decred, o Ethereum y Omisego): esta interoperabilidad aún no es efectiva actualmente y cuando lo sea, utilizará tecnologías como Plasma o Lightning Network. Mientras tanto, Secure Swap trata estas blockchains como no interoperables.

PARA LOS INTERCAMBIOS ENTRE BLOCKCHAINS NO INTEROPERABLES:

En este caso, nuestro exchangeur logrará la interoperabilidad entre estas criptomonedas a través de su red p2p.

CASOS DONDE LAS CRYPTO-MONEDAS QUE SON PARTE DEL EXCHANGE SOPORTAN LOS CONTRATOS INTELIGENTES:

Todos los nodos pasarelas de una criptomoneda verifican que los contratos inteligentes (uno por blockchain) validan la llegada de coins en los wallets antes de enviarlos a los destinatarios para garantizar la atomicidad del intercambio.

Envían en la red p2p la validación de la recepción de los coins a otro contrato inteligente (contrato inteligente de la contraparte).

Cuando los dos contratos inteligentes que participan en un intercambio han tenido la validación de la recepción de los coins, estos se envían a los destinatarios finales, a fin de concluir el intercambio por los propios contratos inteligentes.

Para protegerse contra la piratería de nodos o de nodos maliciosos, los contratos inteligentes validan la recepción de los coins de la contraparte sólo si todos los nodos pasarela de la criptomoneda correspondiente indican la recepción de los coins.

En caso de desacuerdo entre los nodos pasarela (por lo tanto, nodos pirateados / maliciosos), la respuesta mayoritaria gana (peso de voto de un nodo pasarela = número de tokens de SSW asociados con este nodo). Todos los nodos pasarelas que dan una respuesta no conforme son desconectados y quedan en una lista negra (dirección IP en lista negra, evitando la reconexión de estos nodos a la red p2p).

Cada vez que un nodo se desconecta por una respuesta no conforme, envía a la red p2p la información de esta desconexión por falta de conformidad, lo que se propaga a todos los clientes y a todos los nodos. Cada cliente que recibe esta información desactiva la negociación en esta criptomoneda y cancela todas sus órdenes que implican esta misma. Todos los nodos de la red memorizan el estado de trading de cada criptomoneda, por lo que un cliente que no haya estado conectado durante el intento de pirateo y que luego inicie sesión, será informado inmediatamente de la desactivación del trading en esta criptomoneda. Para que se reinicie el trading con esta criptomoneda, se necesita que la mayoría calificada (> = 60%) de los clientes previamente designados para esto (delegados voluntarios) hayan reactivado la negociación en esta criptomoneda.

Lo que se consigue con este protocolo es un consenso por prueba de participación (Proof of Stake).

Para intentar piratear la red P2P y tratar de robar los coins sobre un exchange (no enviar la contraparte, pero recibir los coins del otro usuario), sería necesario poseer más de la mitad del total de tokens SSW asignados a los nodos pasarelas de una criptomoneda.

Esto significa que, para tratar de robar un exchange, hay poner en juego una gran cantidad de tokens SSW. El efecto en la reputación del exchangeur, si el intento tiene éxito, causaría una caída en el valor del token SSW lo cual implicaría pérdidas para el hacker mucho más importantes que las ganancias obtenidas por el robo de una transacción.

Por otra parte como habían algunos nodos honestos en la red antes del ataque de los piratas, cuando estos son desconectados envían la desactivación de las operaciones para esta criptomoneda a todos los nodos (clientes y nodos otros) recibidos. Esto también provoca la cancelación de la transacción en curso y la devolución de los coins correspondientes a sus usuarios mediante contratos inteligentes.

Este protocolo hace improbable el éxito de un intento de toma de control, e incluso si sucede, no habría nada que robar (negociación desactivada), además que para ello se debería utilizar una cantidad importante de tokens SSW, por lo que esta tentativa de ataque definitivamente no es rentable e incluso muy costosa.

Para que esta seguridad sea efectiva, es necesario que los nodos de puerta de enlace de una cadena de bloques sean lo suficientemente numerosos y que el conjunto de nodos de puerta de enlace tenga una cantidad de testigos SSW asignados mucho más altos que el valor promedio de una central para constituir una prueba de un problema válido.

Esta es la razón por la cual la aplicación cliente se niega a realizar un intercambio con una criptomoneda, si el número de pasarelas activas para ella es inferior a dos, que es un mínimo estricto.

CASOS DONDE UNA DE LAS CRIPTO-DIVISAS (O AMBAS) QUE SON PARTE DEL EXCHANGE NO SOPORTAN LOS CONTRATOS INTELIGENTES:

En este caso la función normalmente operada por el contrato inteligente de la criptomoneda, es realizada por un nodo especializado por criptomoneda, controlado y con una seguridad garantizada por la empresa Grey Matter Technologies.

En ausencia de soporte de contrato inteligente en una criptomoneda, no podemos prescindir de Intermediarios de confianza. Es así que este nodo especializado garantizará la recepción de coins de cada parte de un intercambio antes de enviarlo al destinatario, con el objetivo de garantizar la atomicidad de los intercambios sin un contrato inteligente.

Para estos intercambios sin soporte de contratos inteligentes, este servicio específico que otorga Secure Swap necesita tomar posesión de las criptomendas de los trader solamente durante el tiempo necesario de la transacción. Lo que lo diferencia de los exchanges centralizados donde el trader debe transmitir sus activos por un largo período de tiempo.

También en este caso, no existe un stock central de criptomonedas, solo un almacenamiento temporal de contrapartes el tiempo necesario para validar la atomicidad del intercambio. Así que no hay mucho que el hacker pueda ganar.

INDICACIONES DE STATUS DEL EXCHANGE

INDICACIONES PROVENIENTES DEL CLIENTE

La aplicación cliente indicará, mediante un código de colores, la disponibilidad de nodos pasarela para cada criptomoneda:

- Negro: Intento de pirateo detectado en los nodos pasarelas de esa criptomoneda, trading desactivado para esta.
- Rojo: No hay pasarelas disponibles para esta criptomoneda => no hay exchanges posibles.
- Naranja-Rojo: Sólo hay una pasarela disponible para esta criptomoneda => exchanges prohibidos.
- Amarillo: Dos pasarelas disponibles para esta criptomoneda => exchange ok, pero protección no óptima contra pirateo.
- Verde: A partir de tres pasarelas disponibles para esta criptomoneda => exchange ok, óptima protección contra pirateo.

INDICACIÓN PROVENIENTE DE UN NODO ESTADÍSTICO

Un nodo estadístico analiza permanentemente la red con el objetivo de producir diferentes informaciones para los NodeOwners y los traders. Esto permitirá:

- Proporcionar un tablero de estadísticas avanzadas en los nodos.
- Evaluar la remuneración esperada en función de los tokens SSW asignados a un nodo pasarela.
- Verificar los volúmenes de exchanges de un período por criptomoneda.
- Entre otros

RENDIMIENTO DE LA PLATAFORMA

Actualmente, la blockchain Ethereum está limitada a alrededor de 10/15 transacciones por segundo. Nuestro contrato inteligente que gestiona los intercambios en esta blockchain, también tendrá estas limitaciones.

Sin embargo, se está trabajando en aumentar en gran medida la cantidad de transacciones por segundo que la blockchain Ethereum podrá realizar. Estamos hablando de un aumento de unos cientos de miles o incluso millones de transacciones por segundo, a través de tecnologías como Plasma, Sharding y Lightning Network.

Las mejoras de primera capa, como Sharding, sin duda aumentarán el número de intercambios / segundo alcanzables mediante nuestro contrato inteligente. Este no es el caso de las mejoras de segunda capa como Plasma / Lightning Network (excepto por la disminución de carga inducida en las operaciones de primera capa).

Está previsto tener un contrato inteligente que administre los intercambios en cada blockchain que soporte contratos inteligentes, como EOS y otros, para agregar las capacidades de ejecución de varias blockchains (además de garantizar la atomicidad de los intercambios a través de los contratos inteligentes de cada blockchain). Por lo tanto, la plataforma no está vinculada al futuro de una sola blockchain y además su capacidad para gestionar intercambios no se limita a las capacidades de ejecución de los contratos inteligentes de una blockchain, y a su vez una blockchain no limita la capacidad de intercambio de otras blockchains más rápidas.

Preferimos la opción de implementar contratos inteligentes de exchange en varias blockchains, en lugar de desarrollar nuestra propia criptomoneda con una adecuada capacidad de ejecución de contrato inteligente.

Nos enfocamos en utilizar soluciones existentes que crear una nueva criptomoneda.

¿CÓMO SOLUCIONAR LA FALTA DE LIQUIDEZ INICIAL?

Al iniciarse una plataforma inevitablemente se presentan problemas de liquidez: cuando se inicia el servicio, sus libros de órdenes están vacíos, lo cual no es alentador para los primeros usuarios. Los problemas de liquidez también pueden existir en criptomonedas con bajo volumen de intercambio.

El servicio de arbitraje (basado en los libros de órdenes de otras plataformas, el libro de órdenes interno de Secure Swap y en los fondos de reserva en criptomoneda propias de nuestra plataforma), podrá garantizar una liquidez de reemplazo.

Este servicio de arbitraje actuará como una aplicación cliente (en el sentido de que emitirá órdenes en nuestro libro de órdenes) utilizando las criptomonedas pertenecientes a la compañía. Este servicio consistirá en un nodo p2p especializado en esta tarea. Al igual que todos los nodos de la red, recibirá las actualizaciones del libro de órdenes. Al conocer nuestro libro de órdenes, este servicio podrá identificar las contrapartes que faltan y completarlas con transacciones con otras plataformas.

Una parte de los fondos operativos disponibles de la compañía, se repartirá en varias criptomonedas utilizadas por los mecanismos de arbitraje.

Por ejemplo: si nuestro libro de órdenes contiene una orden de intercambio de 1 BTC por 12 ETH pero no hay ninguna orden de intercambio de ETH contra BTC por el precio o las cantidades solicitadas. Si esta orden existe en otra plataforma de intercambio externa, ella nos sirve como una liquidez de reemplazo. Utilizaremos los ETH de nuestra compañía reservados para el servicio de arbitraje para poder realizar este intercambio y nosotros recuperamos los ETH gastados efectuando el intercambio de los 12 ETH por 1 BTC en la plataforma de otro exchangeur.

Este sistema de arbitraje solo actuará en caso de falta de liquidez de nuestro libro de órdenes y solamente si la operación no significa una pérdida para nuestra plataforma. Incluso nos puede generar ganancias si el exchange de la otra plataforma es favorable a nuestra operación, pero este no es el objetivo principal del sistema.

UNA PLATAFORMA OPEN SOURCE

La mayoría de los tipos de nodos serán distribuídos en Open Source.

Esto significa que, además de la aplicación cliente que sirve a todos los traders, todos tendrán la oportunidad de apoyar el funcionamiento de la plataforma operando nodos conectados a blockchains.

Los NodeOwners que apoyan este sistema y que poseen tokens de SSW emitidos en el ICO, recibirán una parte de los cargos cobrados por los intercambios en proporción a los tokens asignados a un nodo pasarela de un blockchain, esto será en relación a todos los tokens SSW asignados a los nodos pasarela de la blockchain en funcionamiento.

Grey Matter Technologies operará de la misma manera y recibirá su parte de las tarifas de intercambios en proporción a los tokens de SSW que posea al final de ICO y que reservará para cada nodo pasarela que tenga en funcionamiento.

Proporcionamos, en Open Source, una estructura tipo de nodo para el intercambio a monedas fiduciarias, con interfaces para conectarse a los procesadores de pagos bancarios. Como esta actividad está muy regulada ello requerirá de adaptaciones para cada caso (regulaciones locales e interfaces a los procesadores de pago utilizados).

La compañía Grey Matter Technologies, utilizará este tipo de nodos para Sudamérica. Proyectamos operar inicialmente con nodos de conversión de moneda fiduciaria para las siguientes divisas: peso chileno, peso argentino, sol peruano y posiblemente otras más posteriormente.

De este modo, gradualmente, esta plataforma podrá admitir conversiones a un gran número de monedas fiduciarias de distintas regiones del mundo.

El nodo de arbitraje no se publicará en Open Source. De hecho, nos reservamos su utilización.

PROGRAMA BUG BOUNTY

Parte de los fondos recaudados en el ICO se utilizarán para financiar campañas de Bug Bounty. Las recompensas se otorgarán a aquellos que participen en estos programas e informen a nuestros equipos sobre las fallas de seguridad desconocidas.

Se lanzará una campaña en cada etapa de la fase de desarrollo para asegurar que la primera versión de la plataforma haya sido bien analizada antes de su puesta en marcha.

Se planificarán campañas trimestrales para acompañar la continuidad del desarrollo de la plataforma.

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

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

NECESITAMOS FINANCIAMIENTO PARA ESTE PROYECTO:

Para:

- Financiar la contratación de personal adicional y los salarios del equipo ya activo. Este es el principal gasto de la sociedad.
- Financiar publicidad previa al lanzamiento de la plataforma para poder darla a conocer.
- Financiar un capital de trabajo en criptomonedas destinado al sistema de arbitraje.
- Financiar las campañas de Bug Bounty.

Todos los tokens que no se vendan en el ICO seguirán siendo propiedad de la empresa, a fin de reunir la parte correspondiente a las tarifas de cambio. Por lo tanto, cuanto más exitoso sea el ICO, más inversores que apoyen la operación del intercambio recibirán una parte significativa de los ingresos generados por los intercambios, la compañía tendrá menos tokens SSW.

Por otro lado, cuanto menos se suscriba al ICO, mayor será la propiedad de tokens de la sociedad al finalizar este último y recibirá una parte significativa de los ingresos generados. Esto garantiza una distribución equitativa de los ingresos, en función de lo que la empresa haya recaudado como capital en el ICO y permitirá recompensar a los inversionistas que nos hayan respaldado.

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 gerentes / animadores sociales de la campaña ICO: 3%

Reservado para socios: 4%

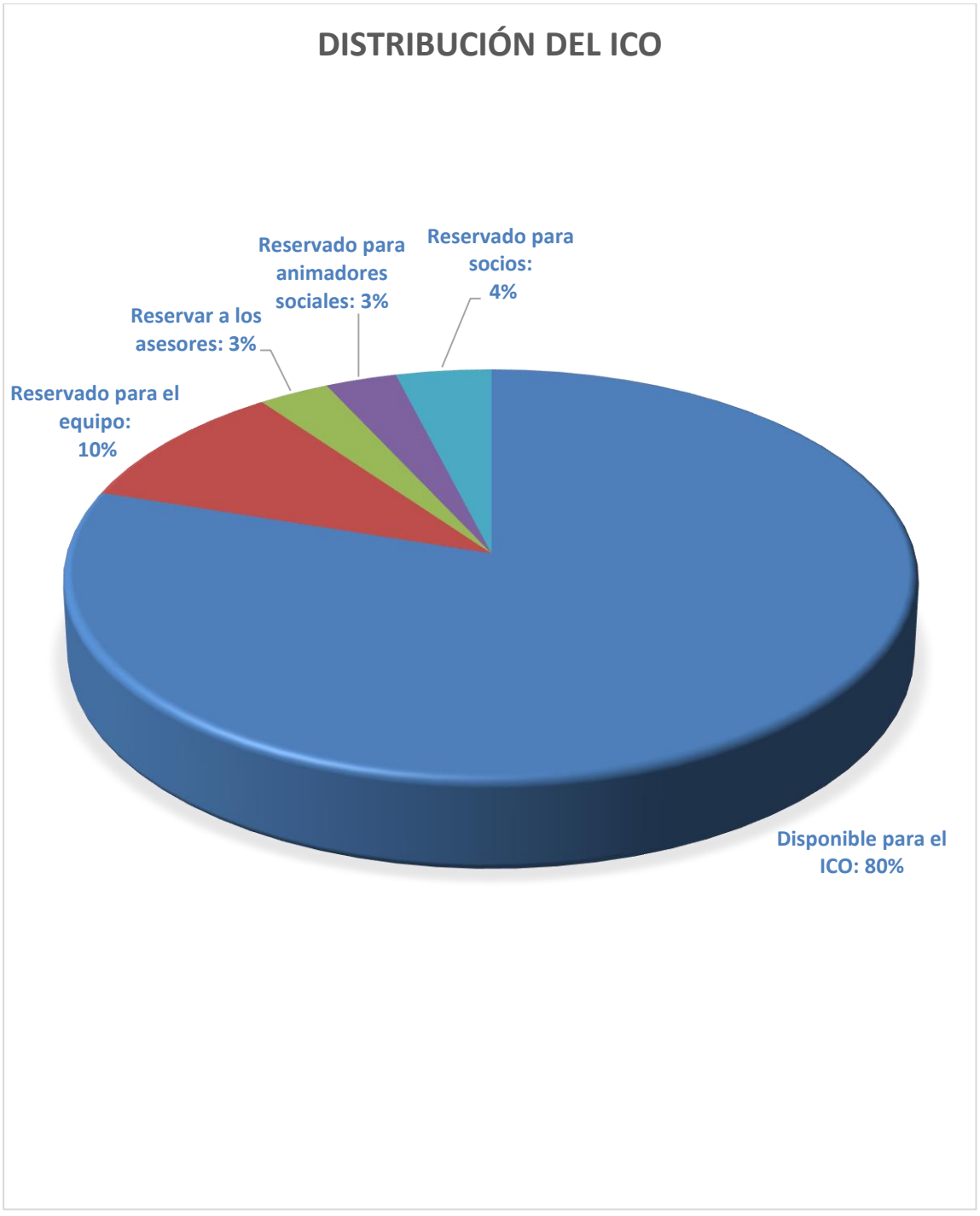
Disponible para el ICO: 80%

Soft Cap: 10 millones de tokens

Hard Cap: 80 millones de tokens

Todos los tokens sin vender siguen siendo propiedad de la empresa

ICO operado por la sociedad chilena Grey Matter Technologies



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:

HARD CAP ALCANZADO :

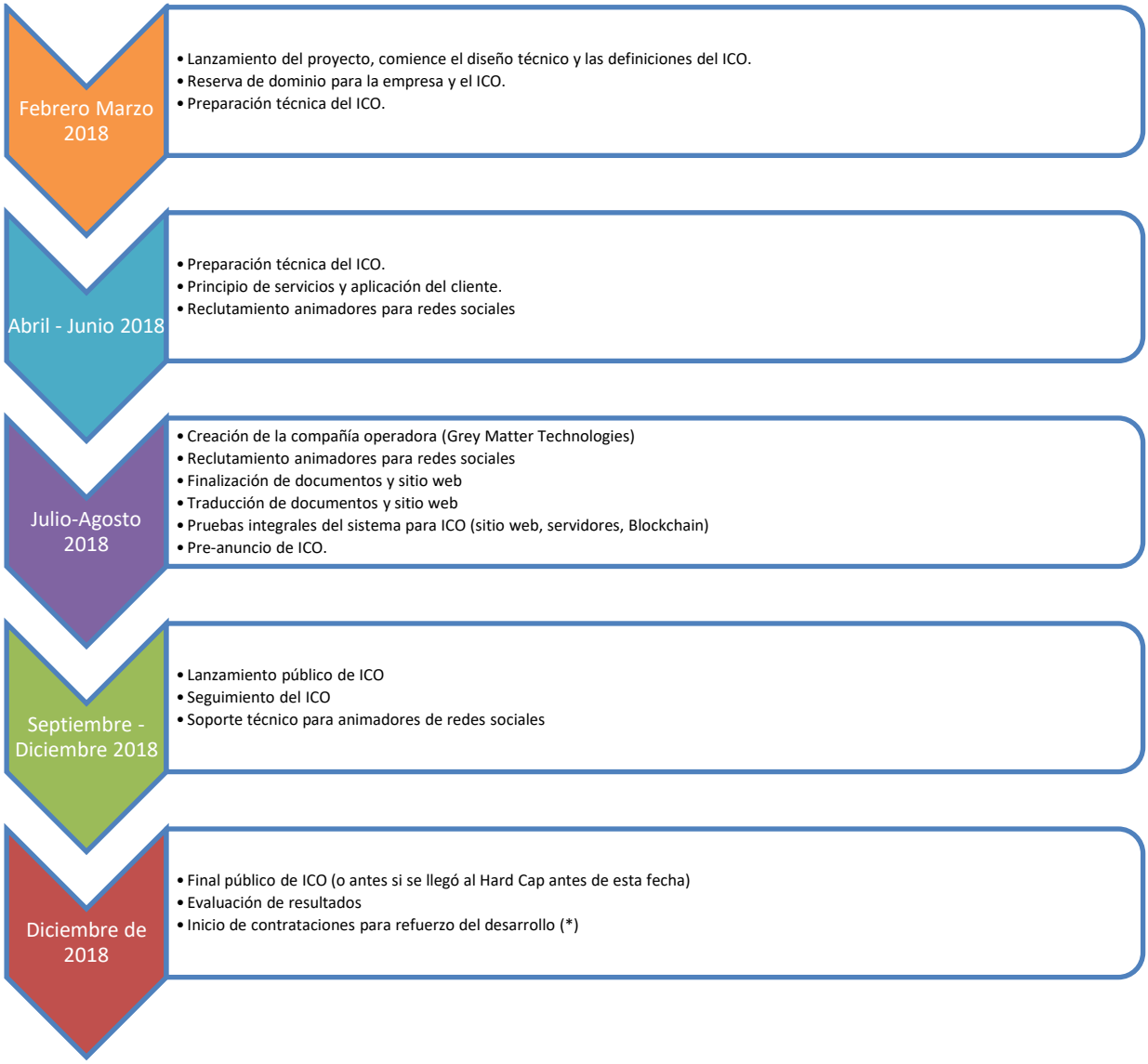
ROADMAP

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.

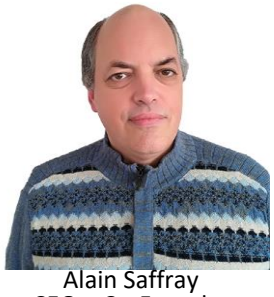
ROADMAP ICO



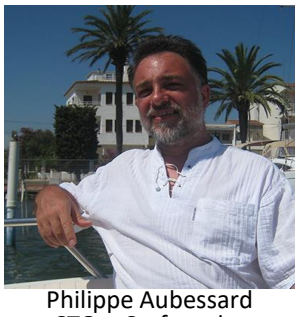
ROADMAP SECURE SWAP

TEAM:

MIEMBROS:



Alain Saffray
CEO – Co-Founder
Developer engineer



Philippe Aubessard
CTO – Co-founder
Developer engineer

Alicia Laura Poblete
Co-founder
Financial Director

Nadine Miotti
Co-founder
Marketing Director

Renaud Desportes
Business development
Executive

Rafael Romero Carmona
DevOps Engineer

Pierre Pretti
Security Infrastructure
Engineer

Aliaksandr Kharlamou
Blockchain Developer

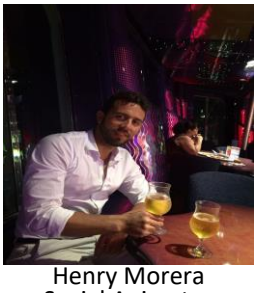
Victor Chukholskiy
Blockchain Engineer
Smart Contracts Specialist

Marc Rivoal
Software Architect
Engineer

Kevin Vanstaen
Social Animator
Blockchain enthusiast

Zhan Wei - 詹玮
Social Animator

Lulia Galea
Social Animator



Henry Morera
Social Animator

CONSULTORES:

Benoît Renard
Conseiller légal

SOCIOS:

Guillaume Krawczyk
GORIOUX GROUPE

Hatem Ben Abdallah
Art Director – Designer - Photographer

ASPECTOS LEGALES

IMPLICACIONES LEGALES CON TOKENS SSW

No podemos garantizar la evolución futura del precio del token SSW, ni su presencia en los listados de plataformas y la posibilidad de reventa. La posesión de Tokens no otorga ningún derecho de participación, control o decisión sobre la empresa Grey Matter Technologies. Cualquiera sea el resultado de la ICO, el token no es reembolsable. El inversionista o el especulador asume plenamente el riesgo de compra.

Debido al aspecto comunitario de Secure Swap y el hecho de que los exchanges entre criptomonedas forman parte de un sistema distribuido fuera de control de la sociedad Grey Matter Technologies, el token SSW es un token utilitario que sirve de prueba de participación (Proof of Stake) para asegurar los exchanges al interior de un sistema abierto. Esto permite obtener ganancias, tal como Ethereum con el minaje, pero en un sistema distribuido sin el control de una sociedad. Grey Matter Technologies sólo entrega las soluciones técnicas.

Como Secure Swap es una plataforma abierta, distribuida y comunitaria, ello implica el anonimato de los usuarios, al menos tanto como las criptomonedas intercambiadas lo permiten, y por lo tanto no nos parece pertinente preguntar las identidades de los inversores y sus comprobantes de residencia para la ICO para verificar sus derechos de participación en esta ICO.

Corresponde a los inversionistas verificar, de acuerdo su país de residencia, la legalidad de participar en esta ICO y de abstenerse en caso de ilegalidades o de dudas.

Destacamos que la participación a una ICO actualmente está totalmente prohibida en el caso de China y Corea del Sur, sea la naturaleza del token.

Para los residentes en EEUU es su responsabilidad verificar en la SEC la legalidad de su participación en esta ICO.

Para los residentes de la Comunidad Europea que desean participar de esta ICO, ellos deben declarar no ser consumidores según la definición de la Directiva Europea 2011/83/UE del 25 de Octubre de 2011, relativa a los derechos de los consumidores.

Por los residentes de Rusia, es su responsabilidad verificar según sus autoridades reguladoras el marco legal de su participación en esta ICO.

Acerca de los nodos de conversión de criptomonedas a divisas fiduciarias:

Este tipo de nodo implica una estructura legal y el cumplimiento de las leyes locales del lugar de operación, sobre todo las reglamentaciones KYC/AML/CFT/FCA relacionadas con la lucha contra el fraude, el lavado de dinero y cualquier actividad delictual.

LA COMPAÑÍA QUE EXPLOTA LA PLATAFORMA

- Grey Matter Technologies explotará la plataforma es decir: los nodos pasarelas, el nodo de arbitraje y los nodos de conversión a la moneda fiduciaria.
- Grey Matter Technologies es una compañía bajo la jurisdicción chilena.

  (https://www.conservador.cl/portal/indice_comercio)
- Motivamos a todos los voluntarios a respaldar el sistema ejecutando sus propios nodos pasarela 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 un Exchange de criptomonedas descentralizado (DEX), con un aspecto comunitario. Es desarrollado 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 los exchanges de los utilizadores. 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 para verificación de la cantidad de tokens que él tiene. Los tokens no cambian de propietarios.

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 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, desconectándolos y colocándolos en una lista negra.

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

R14: Cuando los nodos dan respuestas diferentes durante los pasos de validación de un intercambio, entonces la respuesta de referencia se convierte mayoritaria sobre el conjunto de nodos, teniendo cada nodo un peso de votación correspondiente a los tokens SSW asociados con su funcionamiento. Los nodos que responden de manera diferente son desconectados y anotados en una lista negra. Por lo tanto, para tratar de robar una transacción, sería necesario invertir una cantidad de tokens SSW que representan más de la mitad de los tokens asignados a los nodos pasarelas a esa criptomoneda. Esto representa un valor superior al del robo de una transacción, robo que no tiene posibilidad de realizarse ya que, tan pronto como se detecten anomalías, la transacción se cancela.

Si el hacker utilizara muchos tokens para tomar el control de todos los nodos de pasarelas, la pérdida de la reputación de la plataforma conduciría a una rápida disminución en el valor de los tokens SSW haciendo que esta operación sea infructuosa para el hacker. Además, tan pronto como se detectan anomalías, los intercambios con esta criptomoneda se interrumpen, lo que deja al hacker sin transacción a robar.

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 serán honestos. Dado que la aplicación cliente espera la confirmación de todos los nodos pasarelas a una criptomoneda para el envío de coins, si los nodos pasarelas no proporcionan la misma respuesta, existe un problema. Los clientes involucrados en este intercambio cancelan la transacción e informan a toda la red p2p que los intercambios en la criptomoneda están deshabilitados, lo que provoca la cancelación de todas las órdenes pendientes de todos los clientes conectados para esta criptomoneda. No hay más intercambios, el hacker se encuentra sin transacción a robar.

Q16: ¿Cómo se retoman los intercambios en una criptomoneda, después de haber sido desactivados a consecuencia de una anomalía?

R16: Para reiniciar los intercambios, se requiere un voto unánime de la mayoría calificada (60%) de los representantes conectados a esta criptomoneda y que han sido previamente designados. Estos representantes tienen la responsabilidad de asegurarse de que los nodos activos en la criptomoneda sean nodos conformes, antes de volver a permitir los intercambios en esta criptomoneda.

Q17: ¿Cómo pueden estos representantes asegurarse de que los nodos pasarela sean honestos antes de votar?

R17: Al conectar ellos mismos su nodo pasarela o al verificar que sus nodos estén siempre conectados. Es suficiente la conexión de un sólo nodo conectado confiable u honesto para que el sistema detecte una anomalía si de nuevo los nodos responden de manera diferente. Esto causaría nuevamente la suspensión y anulación de los exchanges en esta criptomoneda.

Entonces, si el trading se reanuda sin incidentes, significa que los exchanges nuevamente son confiables y los nodos maliciosos han sido eliminados. Si los nodos maliciosos están inactivos y funcionan correctamente mientras esperan entrar en acción, cuando lo hacen, serán detectados por sus diferentes respuestas. Por lo que cualquier tentativa de corrupción de nodo se detecta y hace que el robo de la transacción sea imposible.

Q18: ¿Cómo se designan estos representantes?

Q18: Estos representantes son voluntarios, y solo están calificados si poseen 100 veces la cantidad de un intercambio promedio, en valor equivalente de tokens SSW. El voluntario luego lo solicita a través de la interfaz de su nodo, y si está calificado, todos los nodos de la red memorizan su estado como un "super nodo pasarela". Este super nodo pasarela se recompensa con una bonificación del 50% en su remuneración, en comparación con lo que normalmente recibiría con los tokens asignados.

Q19: ¿Cómo evitar que personas malintencionadas conecten permanentemente nodos defectuosos para paralizar el servicio?

R19: Los nodos defectuosos están en una lista negra, además de estar desconectados. Estas personas malintencionadas se quedarán sin direcciones IP para conectar sus nodos.

Una acción de sabotaje informático es ilegal, su repetición aumentará la probabilidad de descubrir a sus autores, y la empresa Grey Matter Technologies acudirá a la justicia para solicitar una indemnización.

Q20: ¿Qué medidas se están tomando para luchar contra los piratas informáticos?

R20: 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.