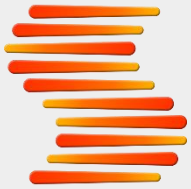


# SECURE SWAP
# WHITE PAPER

Grey Matter Technologies

www.secure-swap.com

# SECURE SWAP
# WHITE PAPER

## LEGAL MENTIONS

The purpose of this White Paper written by *Grey Matter Technologies SpA* (the "Company") is to present the Secure Swap project and its SSW token to potential token holders as part of the project to launch this ICO. The information presented below may not be exhaustive and does not imply any element of a contractual relationship. The sole purpose of this White Paper is to provide relevant and reasonable information to potential token holders. Holders of SSW Token are invited to undertake a thorough analysis of the company and to understand the current or potential future values of any acquired SSW tokens.

Nothing in this White Paper shall be deemed to constitute a prospectus of any kind or an investment solicitation, nor shall it relate in any way to an offer or solicitation of an offer to purchase securities in any jurisdiction. This document is not composed in accordance with, and is not subject to, laws or regulations of any jurisdiction which are designed to protect investors.

Certain statements, estimates and financial information contained in this White Paper constitute forward-looking statements or information. Such forward-looking statements or information involve known and unknown risks and uncertainties that may cause actual events or results to differ materially from the estimates or results expressed or implied by such forward-looking statements. Such forward-looking statements or information do not constitute a promise or any obligation.

The simulations contained in this White Paper cannot be considered as a promise of profit and/or a guaranteed forecast of the growth of the SSW token. The calculations provided are based solely on fundamental mathematical laws.

This white paper in English is a translation of the reference document in French. The French version is the main official source of information on the SSW token. During this translation, and despite our efforts to proofread, some of the information contained in this document may be lost, corrupted or distorted. The accuracy of this translation cannot be guaranteed. In the event of any conflict or inconsistency between this translation and the White Paper in French, the provisions of the original document in French shall prevail.

ANY PERSON PURCHASING SSW TOKENS EXPRESSLY ACKNOWLEDGES AND DECLARES THAT HE OR SHE HAS CAREFULLY REVIEWED THIS WHITE PAPER AND HAS FULLY UNDERSTOOD THE RISKS, COSTS AND BENEFITS ASSOCIATED WITH THE PURCHASE OF SSW TOKENS.

## SUMMARY

## TABLE OF CONTENTS

# PRESENTATION OF SECURE SWAP

## INTRODUCTION

"One more exchanger? The market is saturated with them!"

No, Secure Swap is not just another decentralized exchanger (DEX). Its characteristics make it unique! It combines the advantages of both centralized and decentralized exchangers: liquidity, speed of execution, no need of trusted third parties, resistance to hacking, resistance to prohibitions and regulations against crypto-currencies.

The Secure Swap platform is open source and without any central server. It is operated by the community, and therefore does not require an operating company to function.

Its architecture is highly modular, allowing services to be added (crypto-currency support, fiat exchange support and payment systems integration (cash-in/cash-out), liquidity provider support). Developers and entrepreneurs can thus join and extend the Secure Swap community.

Thanks to its community operation, Secure Swap allows NodeOwners (users operating one or more gateway nodes) to draw a source of income from it.

Its architecture protects the heart of the system from regulations and brutal bans on crypto-currencies. Depending on where they live, these regulations can be a risk for those who own crypto-currencies. Secure Swap offers an exit door that is always available.

For digital currencies that allow it, Secure Swap fully respects anonymity when exchanging crypto-currencies between them.

Nevertheless, thanks to its modularity and the clear separation of the different exchange systems, Secure Swap also makes it possible to fully comply with local regulations when it comes to exchanging crypto-currencies with fiat currencies.

The opening of Secure Swap to crypto-fiat exchanges also allows those who wish to do so to operate, from a legal structure, a professional activity of exchanging crypto-currencies into fiat currencies, in the currencies of their choice. Secure Swap is open-source and provides node models that are ready to be adapted to local regulations.

Its operating protocol includes anomaly detection systems. Each anomaly results in disconnection from the network of the failing ~~party~~ item and the use, if necessary, of the SSW tokens kept in guarantee to terminate an ongoing exchange. These anomalies can be caused either by a hacking attempt or by the malfunction of some nodes.

Its trading client application, Secure Trade, offers a level of comfort and ergonomics comparable to the best trading software on traditional stock markets (graphic orders, money management, scalping assistance, programmable automatic trading module, etc.).

Our objective ~~in proposing "one more exchanger"~~ is to build a new generation exchanger that will, for the first time, combine all these characteristics. And it is only by bringing them all together that a DEX can claim to dethrone the centralized exchangers.

## MARKET STATUS

Main characteristics of centralized and decentralized exchangers:

### CENTRALIZED EXCHANGERS

Advantages:

- Good liquidity, even very good for the largest exchangers. This ensures a high market depth and limited price slippage[1].
- A good speed of execution of orders, thanks to a centralised order book and the available liquidity.
- ~~For the most part, a~~A wide choice of exchangeable crypto-currencies.
- For some people the possibility of ~~leverage~~ margin ~~-~~trading.

Disadvantages:

- Transfer of ownership of digital assets to these exchangers, which serve as trusted third parties.
- This centralization of assets is very attractive for hackers. This makes hacking very damaging, both for the company operating the exchanger and for its customers.
- Risk of sudden closure, making the assets deposited there inaccessible. These closures can be caused either by a bankruptcy of the exchanger operator or by State regulation hostile to crypto-currencies.
- Frequent unavailability of services during periods of market panic.
- The withdrawal of assets involves a double cost: the usual network charges, ~~plus~~ and the charges added by the exchanger for the withdrawal.

### DECENTRALIZED EXCHANGERS

Advantages:

- No need for trusted third parties.
- No centralization of assets, therefore not very attractive for hackers, and also more difficult to hack.
- Some are resistant to the bankruptcy of their operators and regulatory risks, but there are few of them[2].

Disadvantages:

- Insufficient liquidity to ensure the presence of a counterparty. This also causes a high risk of price slippage and slow execution of orders.
- The slow execution of orders is directly caused by their distributed architecture model and by the way their order books and matching systems work.
- Most of them have a limited choice of exchangeable crypto-currencies. Many are limited to exchanging only within the Ethereum network (Ether and Tokens).

- Order books and matching of orders executed by smart contracts (On-Chain) cost network fees (gas on Ethereum) even if the orders are not executed. Moreover, there are also costs associated with cancelling and changing orders.

What results from this comparison:

It can be seen that DEXs are not without disadvantages compared to centralised exchangers, which limits their interest.

Insufficient liquidity is the main reason for the massive non-adoption of DEXs, with users finding the market depth of centralized exchangers preferable to the benefits of DEXs.

Slow order execution is also one of the reasons for this situation, but it is a less important cause than insufficient liquidity.

The absence of ~~leverage~~ margin trading is also a reason for the disaffection of DEXs, at least for traders who practice this type of trading on crypto-currencies.

No current DEX has these two characteristics combined (liquidity and speed). Those who do and claim to be DEXs are relying on the fact that the operating company is the intermediate counterparty to the exchanges to ensure their liquidity. The company exchanges the crypto-currencies for its tokens, at rates decided by itself. It is the operating company that generally chooses the exchange rate of its tokens in regard to all available crypto-currencies, sometimes via an ad hoc formula, sometimes even by simulating a price slippage mechanism, totally to their advantage, which induces hidden costs.

These tokens, which serve as intermediate counterparties, also constitute a concentration of assets. These exchangers therefore face the same risk of hacking as centralized exchangers (example: Bancor, which has been hacked, resulting in the theft of 1/3 of its counterpart tokens).

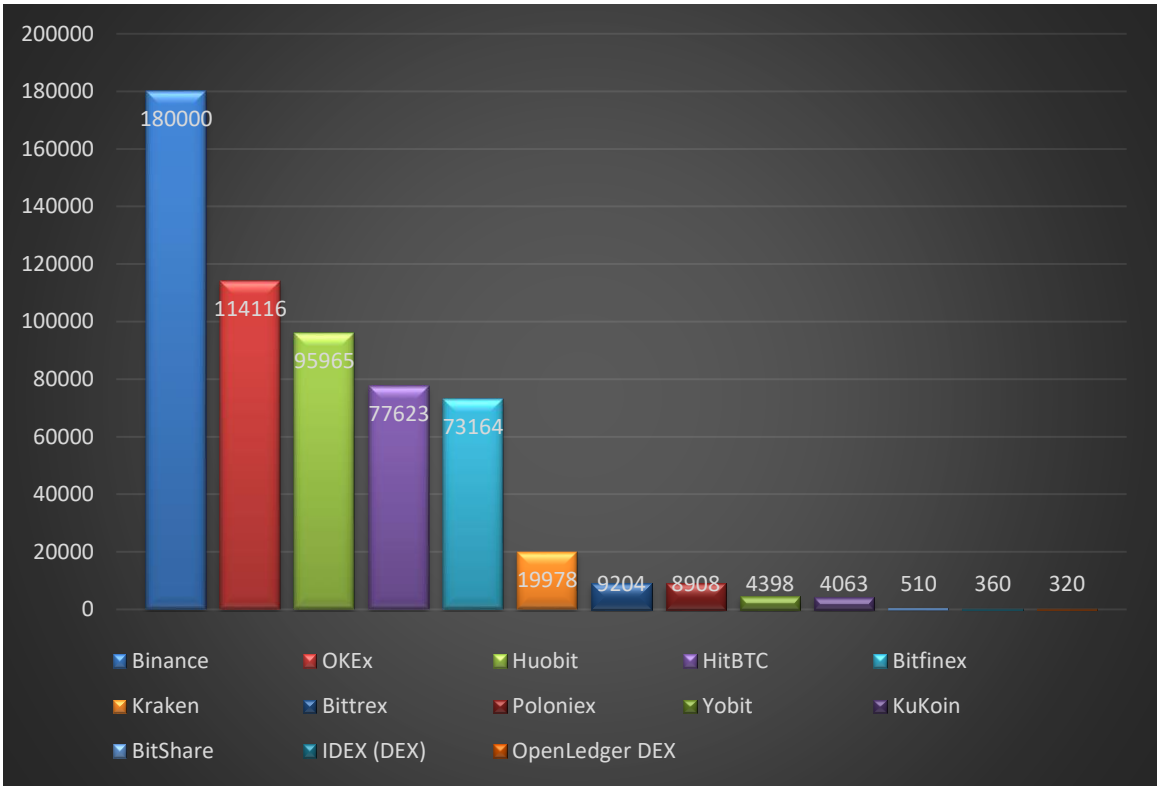
[1] Slippage is the price difference between the price at which you want to buy or sell, and the price at which your order is executed on a trading platform.

[2] For a DEX to be resistant to the bankruptcy of its operator and the risks of prohibition, its architecture must be decentralized, autonomous or with decentralized governance. But, and this is a point that is often forgotten, its ordering system must also be resistant. This is absolutely not the case for all DEXs using a website for their order placement. These sites may be banned or closed following a regulatory change or bankruptcy of the company operating the website, or even be inaccessible due to a simple DDOS attack. Only decentralized, autonomous DEXs with a client application for placing orders meet this criterion. They are not numerous (Altcoin.IO, BarterDex, Bisq, Stellar Dex for the main ones), and they are also subject to liquidity problems.

## COMPARISON OF MARKET SHARES

Despite their respective advantages, a study of market shares shows that DEXs are significantly lower in terms of volumes traded compared to centralized exchangers.

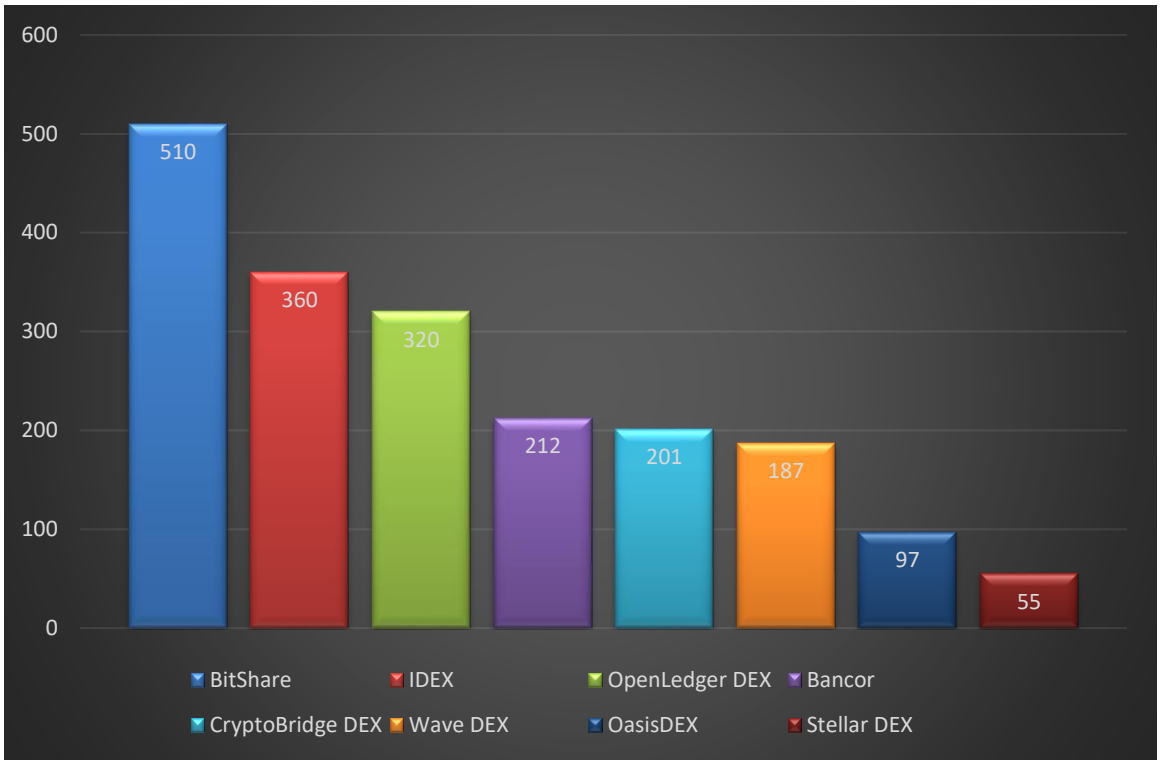
Daily exchanges volume compared to centralized and decentralized exchangers:




This graph shows the exchanges volumes for a few centralized exchangers, and for the three decentralized exchangers that have the highest volume.

The volumes of BitShare, IDEX and OpenLedger DEXs are so small compared to centralized exchangers that they are not even visible on the graph....

Comparative exchanges volume of decentralised exchangers only:




Conclusion:

This comparison between centralized and decentralized exchangers is irrefutable!

What is the main difference, responsible for this situation, and shared by all DEXs?

They are lacking in terms of the liquidity they have. Whatever their advantages, this lack of liquidity condemns them to play an anecdotal role among exchangers.

Some are trying to overcome this liquidity problem, such as Bancor and others, but their solutions either do not really provide liquidity, or transform DEX into a market maker[3] that imposes its exchange rates, users then lose control of the price of their transactions.

[3] A financial intermediary that makes prices, offers a bid and ask price on a financial asset.

## EXAMPLES OF SOLUTIONS TO THE LACK OF LIQUIDITY PROPOSED BY DIFFERENT DEXS

***Altcoin IO:***

Provides a system for sharing liquidity between DEXs via an API. This system can become a very good long-term solution, when DEXs have liquidity to share...

For Atlcoin IO, this solution does not provide immediate liquidity.

***Bancor:***

Market Maker using its tokens as counterpart to all trades. It thus offers liquidity that is always available, by fixing exchange rates and even adding an artificial price slippage during trading based on the volume traded. The liquidity problem is solved, but at what price: users no longer have control over the exchange price of their transactions. In addition, the exchange rate setting system is opaque and can quickly become suspect.

***BarterDex (Komodo platform):***

This platform uses a rather smoky artificial liquidity creation system: the liquidity of the order book is multiplied by the fact that the crypto-currencies involved in an order waiting to be served remain available for other orders. This creates a depth of the fictitious order book that does not exist in practice. As soon as an order is served, all orders based on these same crypto-currencies, which are no longer available in sufficient quantities, are then cancelled. This also cancels out this artificially created liquidity....

This provides nothing more for users than misleading them as to the actual liquidity available.

These three examples cover most of the solutions implemented to try to solve the liquidity problem, the most commonly used being Bancor's solution: the project tokens serve as a counterpart, with or without a specific blockchain, with the resulting consequences.

## SOLUTIONS PROVIDED BY SECURE SWAP

Altcoin.IO's solution will become interesting when DEXs take the lead over centralized exchangers, sharing their liquidity.

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

Secure Swap plans to implement Altcoin.IO's API to share its liquidity, with the idea that this will be beneficial to both exchangers, as well as to those who will join us later.

In the meantime, Secure Swap must have a way to obtain liquidity as soon as it is operational. That is why we are going to find liquidity where it is, in the centralized exchangers, by using their APIs. Our arbitration system is dedicated to this task. In this way, we will be able to exploit the liquidity of several centralized exchangers, thus offering a liquidity potentially greater than each of them.

Why is this simple idea not used by other DEXs? It has a downside: it requires blocking significant funds in crypto-currencies for each of the centralized exchangers whose liquidity is exploited. To this end, a significant portion of the funds raised at the ICO will be devoted to arbitration nodes.

The speed of matching orders is achieved simply: all nodes in the network (including Secure Trade, the client application, which is also a node), share order book updates.

When a trader adds/deletes/modifies an order via Secure Trade, this change is transmitted to all nodes from one to the next. As it is a differential transmission, it represents very little data to propagate, which means that globally all nodes are permanently updated (a bit like nodes validating blocks on blockchains, except that here the volume of data transmitted is negligible).

Each Secure Trade node matches its own orders versus the complete order book, so we obtain a very fast matching of orders (we can consider it as instantaneous), because each Secure Trade node matches only a small part of the orders (the user's few orders) versus the complete order book. Please note that these operations are totally free of charge.

Regarding the range of available crypto-currencies, Secure Swap is not limited to the Ethereum ecosystem, so we can offer a large number of them. Its community aspect as well as the availability of gateway node models (to crypto-currencies, fiat currency, arbitration node) allows the Secure Swap community to add support for the crypto-currencies (and fiat currencies) of its choice.

Secure Swap also allows ~~leverage~~ margin-trading, via nodes dedicated to this task.

In summary, Secure Swap is a crypto-currency exchange ecosystem, built around a decentralized service, a client application for trading and optional micro services to take advantage of the new opportunities offered by this new network. These micro-services are specialized nodes, such as connection nodes to different blockchains, connection nodes to payment processors for exchanges with fiat currencies, arbitration nodes, ~~leverage~~ margin-trading nodes.

Further details are presented in the section “Architecture and operation of the exchanger”.

## SUMMARY OF SECURE SWAP STRENGTHS

### LIQUIDITY

- As we have just seen, Secure Swap ensures a very high liquidity, provided by the centralized exchangers, thanks to our arbitration system.
- In the future, liquidity will also be supported by the sharing of order books between DEXs exchanges.

### SPEED

- Each client application performs the matching of its orders versus the complete order book. This, combined with the available liquidity, ensures us a speed of execution comparable to centralized exchangers.
- Its architecture and operation make Secure Swap not dependent on the speed of execution of smart contracts on the various blockchains (see explanations in “Architecture and operation of the exchanger”). Thus, Secure Swap is as fast as a centralized exchanger at nominal load, and probably faster at high loads. Secure Swap is certainly the fastest of all existing DEXs.

### ~~SÉCURITY~~SECURITY

- System secured by design, with detection of hacking attempts or malfunction, and automatic disconnection of the concerned sections.
- A truly decentralized system, users remain in possession of their crypto-currencies until the exchange occurs.
- By its totally decentralized nature, Secure Swap has no trusted third parties, and is a DAO (Decentralized Autonomous Organisation). Thus, there is no way for regulators to prevent its use.
- No concentration of crypto-currencies. This is a prime target for hackers in centralized exchangers, but also in so-called decentralized exchangers whose operation involves the concentration of crypto-currencies or tokens.
- The trader is guaranteed to receive his counterparty following an exchange, even if part of the system is defective or hacked.
- An open and open-source system that allows everyone to control its code, operation and security.

### AVAILABILITY

- Highly redundant system, guaranteeing failure resistance and therefore high service availability, even under heavy load.

### AN EXCHANGER CONTROLLED AND OPERATED BY A COMMUNITY

- Its distributed and community nature makes the service independent of the existence of the company that created it and does not need it to function.

## AN EXTENSIBLE EXCHANGER

- Due to its open source and modular nature, users who wish to do so, can add to the exchanger the support of new crypto-currencies as well as exchanges of crypto-currencies to fiat currencies or the support of payment methods of their choice.

## A SOURCE OF INCOME FOR THOSE WHO SUPPORT ITS OPERATION

- Those who support the operation of the service (NodeOwners), by running parts of the system (nodes gateways to specific crypto-currencies), are rewarded by receiving a share of the fees paid by traders on the exchanges.
- Those who operate ~~leverage~~ margin-trading nodes also benefit from this source of income.
- Similarly, arbitration nodes can also be a source of revenue, by exploiting differences in quotations between exchangers.
- Thanks to its open source nature, entrepreneurs will be able to develop a commercial activity of exchanging crypto-currencies for fiat currencies and even offer payment methods wherever it is legal in the world (conversion nodes to fiat currency).

## A WORLDWIDE EXCHANGER

- In addition to the fact that the network is accessible from anywhere in the world for crypto-currency exchanges, support for new fiat currencies as well as new payment methods added by the community, will gradually extend the service to the whole world for fiat currencies as well.

## ADVANCED AND ERGONOMICS TRADING TOOL

- Its client application, Secure Trade, offers advanced trading tools, which are common in the world of traditional trading (stock markets, futures markets...).
- The main tools are: order placement on the chart, money management assistance, scalping assistance, a programmable automatic trading module, not to mention the wide range of available indicators and other graphic representation modes.
- In addition, Secure Swap offers ~~leverage~~ margin-trading, which is currently unique for a DEX.

## A PLATFORM WITH ATTRACTIVE COSTS FOR THE TRADER

- Secure Swap only uses smart contracts in the case of anomalies.
- An exchange that takes place without malfunctioning nor hacking, do not involve smart contracts.
- As a result, order placing, order modifications, order cancellations do not have any cost for the user, unlike most DEXs.
- Also, the execution of an order does not generate any cost related to a transaction with a smart contract.
- The platform also does not take withdrawal fees, since it does not have wallets. As a result, with its single 0.15% charge on the execution of an order, which can be reduced on the basis of volume criteria, it will be as competitive as centralized exchangers.

In conclusion, Secure Swap is an ecosystem that provides an effective response to the problems of centralized and decentralized exchangers. Like the OmiseGO or Stellar Lumens projects, it also offers the exchange of crypto-currencies into fiat currencies as well as the simple integration of payment methods via an SDK (development kit) allowing payments in fiat currencies and crypto-currencies.

Unlike projects offering these global solutions, it does not depend on the success of ongoing developments such as Plasma, Lightning Network, Sharding, or Atomic Swap to provide equivalent functionality.

## ARCHITECTURE AND OPERATION OF THE EXCHANGER

To address the identified problems, Secure Swap applies solutions that provide both the advantages of centralized and decentralized exchanges, with none of their respective disadvantages.

Secure Swap has **enhanced by-design security**.

The architecture of the nodes enables scalability and redundancy, guaranteeing the reliability and availability of the service.

**Secure Swap does not suffer from any of the disadvantages of centralized or decentralized exchangers.**

Secure Swap is also an open system that allows everyone to control its source code, operation and security, and to participate in its operation by supporting gateway nodes to crypto-currencies.

**The exchange fees are fully redistributed** to those who operate this type of node (NodeOwners), in proportion to the SSW tokens they hold. It is therefore a major source of income for all those who wish to invest in the SSW token.

The distributed network architecture is based on a JavaScript application core based on Node.JS. It forms the common basis for peer to peer (p2p[4]) communications, which will be used for the various modules of the ecosystem: trading client, gateway nodes to blockchains, arbitration nodes to ensure the liquidity of the exchanger, crypto/fiat exchange nodes.

Secure Trade and nodes communicate with each other via p2p technology, thus constituting a decentralized service.

Only Secure Trade knows the private keys of the user's wallets. It is thus able to sign contracts for blockchains (offline signature). As a result, no one can sign transactions instead of Secure Trade. Attempts to steal traders' assets on centralized platforms are no longer relevant here. The trader remains the owner of his crypto-currencies, unlike the centralized trading platforms on which the trader transmits his crypto-currencies stored there, which thus become the real owners of the private keys and stored crypto-currencies.

As soon as the user disconnects from the exchange service, thus quitting the client software, the private keys of his wallets, which are stored locally on his computer, are in fact offline (equivalent to a cold storage). The private keys of its wallets are never transmitted over the Internet and have never left the client application.

Moreover, if the user has hardware wallets (Ledger, Trezor...), the private keys corresponding to his wallets are never even stored on his computer, but remain secure on his hardware wallets.

As soon as the user connects Secure Trade to the p2p network, he is ready to trade/exchange his crypto-currencies, without unnecessary prior transfer costs to an exchanger, while having a security comparable to storing his assets on a private wallet, in cold storage.

[4] Peer ~~2~~ to Peer or peer-to-peer is a computer network model similar to the client-server model but where each client is also a server. Peer-to-peer can be centralized or decentralized. It can be used for peer-to-peer file sharing, distributed computing or communication.

The Secure Trade client application offers user-friendliness and ergonomics comparable to the best existing trading software (stock markets, futures contracts, Forex...). Secure Trade will offer so-called advanced orders, such as trigger range orders, multi-legged conditional orders, OCO orders, etc., as well as trading on the chart with conditional orders on crossing horizontal lines or slopes, indicator orders, a money management support module, as well as a programmable automatic trading module, and finally ~~leverage~~ margin-trading.

Each client application sends user orders to the connected nodes, which allows them to be consolidated. Nodes propagate all collected orders from node to node each time there is a change, so that each node has the complete order book. As Secure Trade is also a node, it also receives all orders issued on the p2p network. This propagation of order book updates only transmits differences, modifications, deletions and additions of orders. It is very fast and appears instantaneous from the customer's point of view.

Each client application matches its own orders versus the complete order book for finding counterparties to the orders that the trader has issued.

When a matching is found, Secure Trade informs the nodes to which it is connected. The nodes will validate the matching, which will trigger the exchange process (see detailed explanation below).

For the security of exchanges, a guarantee system described in the chapter “Gateway nodes and NodeOwners”, as well as a control of operations by all nodes, make it possible to ensure the proper functioning of the various nodes of the network, as well as the security of exchanges in a trustless[5] environment.

Finally, Secure Swap is entirely based on existing, functional and proven technologies. The project is therefore not exposed to the risk of a possible failure of technologies under development such as Plasma for example. This greatly reduces the risk of failure of the Secure Swap project due to third-party technologies that may fail.

[5] The related partners do not need to trust each other or require a trusted third party since all information processed on the network is independently verified.

## ARBITRATION SYSTEM ENSURING THE AVAILABILITY OF LIQUIDITY

The arbitration system consists of a set of arbitration nodes. As these are nodes, they have the current Secure Swap order book, like all other nodes.

Each arbitration node is specialized in using the API of the centralized exchanger for which it is intended.

These specializations concern the implementation of the specific API of the exchanger, and the specific rules of use of the exchanger (such as the minimum time between two API calls...).

### REQUIREMENTS TO CONNECT AN ARBITRATION NODE TO THE NETWORK

To be able to operate this type of node, it is necessary to have a capital distributed in all the crypto-currencies whose arbitration node will provide liquidity to Secure Swap.

This capital must be divided equally between wallets managed by the arbitration node on the Secure Swap network, and between the wallets of the centralized exchanger, whose liquidity is to be exploited.

It also requires a reliable, secure machine with a stable Internet connection.

It is also necessary to obtain the arbitration node application appropriate to the exchanger you want to operate, or possibly to have developed your own specialization based on the node model provided in Open Source.

### OPERATION OF AN ARBITRATION NODE

The arbitration node retrieves and updates the order book of the centralized exchanger it operates, for all the crypto-currencies it manages, and searches for possible counterparties between the two order books.

As soon as a matching between the two order books is found, the arbitration node reserves the relevant order from the Secure Swap order book. Once the reservation has been confirmed, it carries out a reverse transaction on the third-party exchanger.

Example: if in the Secure Swap order book there is an order exchanging 1 BTC for 30 ETH, and on the order book of the third party exchanger there is an order exchanging 32 ETH for 1 BTC, then the arbitration node will issue an exchange order of 1 BTC for 32 ETH on the third party exchanger.

For this transaction, Secure Swap uses the crypto-currency reserves held on the wallets of the third-party exchanger, which belong to the operator of the arbitration node.

Once this operation has been carried out on the third-party exchanger, the arbitration node will send an exchange order of 30 ETH for 1 BTC on the Secure Swap order book, which will cause the exchange on Secure

Swap with the previously reserved order, using the crypto-currency reserves held on the wallets used for the arbitration node on the Secure Swap side, also belonging to the node operator.

Thus, at the end of the transaction, the order that had no counterpart in our order book (1 BTC for 30 ETH) was served. The wallets of the arbitration node on the Secure Swap side have 1 more BTC and 30 less ETH. The wallets of the arbitration node on the third-party exchanger side have 1 BTC less and 32 ETH more. Overall, the arbitration node won 2 ETH during this operation.

These gains that can occur:

- Remunerate those who will operate this type of node.
- Compensate for the exchange rate risks assumed by the operator of an arbitration node.
- Compensate for the operating costs of this type of node (server fees, Internet).
- Allow fees to be paid on the third-party exchanger and on Secure Swap.

There are therefore no additional costs for the trader when his order is served through the provision of external liquidity via the arbitration node. Any gain generated by a difference in price between the exchangers is made for the benefit of the operator of the arbitration node.

An arbitration node can also perform exchanges without gain for it, this can be configured in the arbitration node's settings options.

Periodically, the arbitration node must equilibrate its wallets on the Secure Swap side with those managed on the third-party exchanger side, in order to maintain a good distribution of the available crypto-currencies. The frequency of rebalancing depends on the stock of crypto-currencies available for the node's operation, and also on the propensity of transactions to clear each other or not.

This rebalancing will be carried out automatically on the basis of minimum reserve quantity criteria for each crypto-currency, and will be carried out by performing transfer operations with the external exchanger. These criteria will be configurable at the arbitration node level.

It should be noted that an arbitration node operator does not need to operate ~~a~~ blockchains nodes, ~~it~~ he relies entirely on the Secure Swap network and on the API of the external exchanger, whose liquidity is thus exploited.

An arbitration node can operate with relatively modest crypto-currency reserves, but its economic efficiency and ability to provide liquidity increases with the available crypto-currency reserves (frequency of balancing required, ability to process large transactions in value on each crypto-currency).

*Grey Matter Technologies SpA* will operate arbitration nodes to centralized exchangers for which it has implemented the API with a sufficient reserve of crypto-currencies to guarantee optimal operation. We will also provide a node model ready to be adapted to other exchangers, as well as ready-to-use arbitration nodes under Open Source license~~in open source~~.

It is on this arbitration node model, adapted for this use and enhanced with Altcoin.IO's API, that Secure Swap will share its liquidity with the exchangers who will also implement this API for liquidity sharing between DEXs.

## GATEWAY NODES AND NODEOWNERS

Gateway nodes are the nodes that provide communication between the Secure Swap p2p network and the blockchain nodes.

There is one type of gateway node per blockchain (one for the Ethereum blockchain, one for Neo, one for Bitcoin, etc.)

For exchanges to be allowed, Secure Trade requires at least two active gateway nodes for a blockchain on the network. If this is not the case, then trading in the corresponding crypto-currency is disabled.

NodeOwners are the individuals or entities that choose to operate gateway nodes, thus becoming active members of the Secure Swap community.

*Grey Matter Technologies SpA* will act as a NodeOwner, without any particular privilege, as will any member of the community who would choose to assume this role.

## REQUIREMENTS TO BE ABLE TO CONNECT A GATEWAY NODE TO THE P2P NETWORK

For a gateway node to connect to the p2p network, it must have SSW tokens for a value, preferably equivalent to 1.5 times the average value of a transaction of the corresponding crypto-currency. This average value will be indicated by the statistics maintained by the gateway nodes, and displayed in the gateway node user interface.

The NodeOwner must also have a reliable, secure machine and a stable Internet connection. For this purpose, it is recommended to use a physical server or a virtual machine from a Cloud operator.

He must also have obtained the gateway node application corresponding to the crypto-currency he wants to operate, or possibly have developed his own specialization based on the node model provided under Open Source license~~in open source~~ in order to add the support of a crypto-currency, and have access to a node in the respective blockchain.

## SECURITY OF EXCHANGES, USE OF SSW TOKENS PLACED IN GARANTEE, REMUNERATION OF NODEOWNERS

Once the node is configured to connect to the respective blockchain, its activation connects it to other p2p nodes on the Secure Swap network. The node is then given a unique identifier on the network. However, at this stage of start-up, no other node yet accepts requests from this node and no other node sends them to it.

For this gateway node to be fully operational, its operator must send his proof of stake and guarantee (made up of SSW tokens) to the associated wallet of the smart contract managing this on the Ethereum network, as well as the node's unique identifier. This will be done easily via the node's user interface. This transaction,

signed by the gateway node, will be transmitted by the p2p network to another gateway node to the Ethereum blockchain, which, in turn, will transmit it to the Ethereum node to which it is connected.

The tokens are then sent to the wallet managed by this smart contract. When the smart contract validates the receipt of the tokens, it issues the authorization of the node with its guarantee level. The authorization will be propagated to all nodes of the network, which will then agree to operate with it.

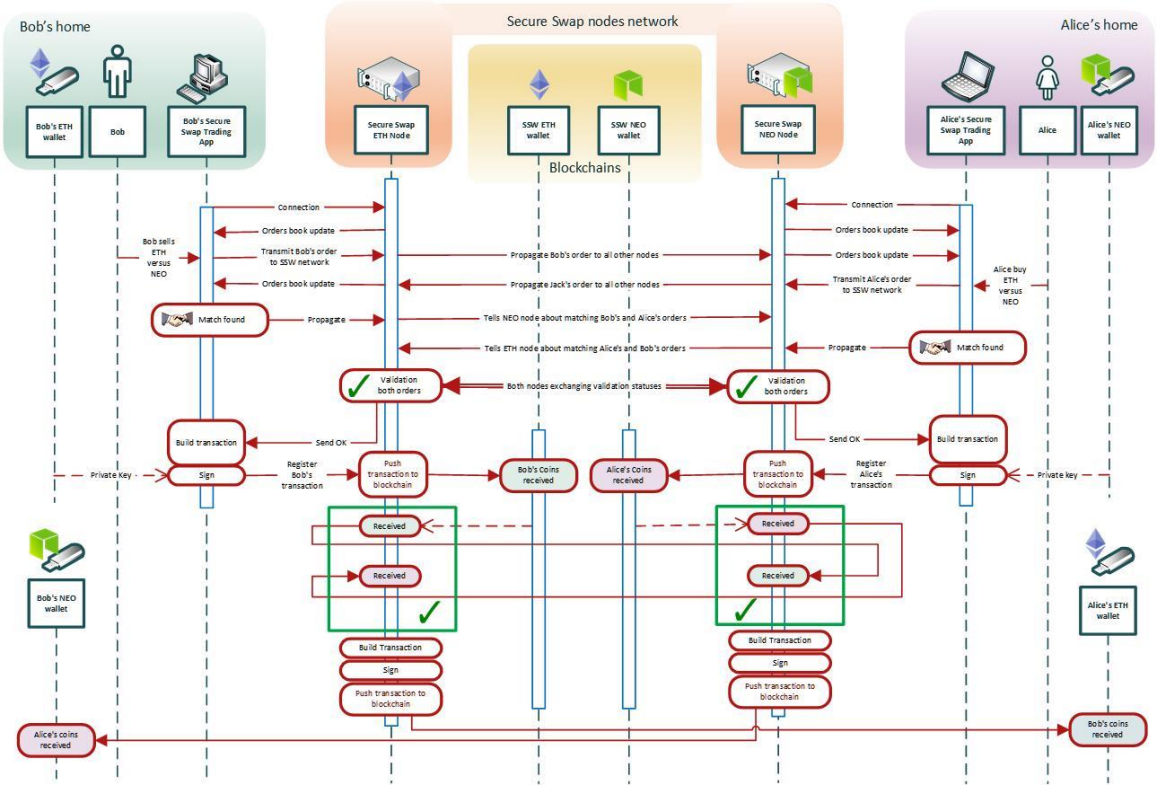
The proof of stake is therefore also used as a guarantee, given by the NodeOwner, for the operation of its gateway node. This proof of stake also defines the maximum amount of each transaction that this node can manage, which is at most 2/3 of the value of the proof of stake.

The gateway node must also have indicated, via its configuration, a wallet that matches the crypto-currency it manages (EOS wallet for an EOS gateway node).

This wallet is used to receive the NodeOwner's share of the fees paid by the trader, in proportion to the tokens he has committed in relation to all those committed for the crypto-currency managed by the node.

This wallet is also used to receive the counterpart of exchanges involving the crypto-currency managed by the node, before sending it to the final recipient. This ensures the atomicity of the exchanges (so that a trader does not receive any counterpart from an exchange without having sent his own).

## COMMUNICATION FLOW DURING A TROUBLE-FREE TRANSACTION




This diagram is simplified for ease of understanding, and does not represent the security provided by the validation of operations by all nodes of a blockchain.

In normal operation (without incident), during exchange operations between crypto-currencies, counterparties are routed through the gateway nodes of the corresponding crypto-currency (NEO coins passing through the NEO gateways). For each transaction, counterparties are sent to one of the wallets managed by the eligible gateway nodes, randomly selected. This random selection is balanced by the ratio of SSW tokens pledged on the node, compared to the total number of SSW tokens pledged on all nodes operating the same crypto-currency. The node can thus retain the exchange fees (0.15% initially) levied on the counterparty before sending it to the recipient.

Note that only nodes with a guarantee of 1.5 times the value of the transaction, in the form of SSW tokens, are eligible and can participate in the selection for the nodes responsible for receiving counterparties.

This avoids an excessive splitting of the remuneration to be distributed among all the gateway nodes, while ensuring that, over time, each gateway node receives the share due to it. And it also avoids additional network costs to spread the costs among the nodes.

A mechanism will change the weighting of each node based on the delay or advance it would have made in collecting fees based on the share it is to receive. This calculation, carried out by the nodes themselves, considers all the fees collected by all the nodes of a crypto-currency. This ensures that gateway nodes that would have only transited small transactions are not disadvantaged compared to others that would have processed transactions that are high in value.

If for any reason (hacking, theft, crash, malfunction, loss of power grid or Internet, etc...), a gateway node does not send the recipient the assets it has received when it has to do so, then the SSW guarantee tokens will be charged the same amount as the missing counterparty. These tokens will then be automatically converted, at market price, for exchange for the missing crypto-currency, and these assets will then be sent to the recipient of the exchange who had not received his counterparty.

This operation to recover an interrupted transaction will use all available sources of liquidity, including the liquidity of external exchangers connected via arbitration nodes, with possible multiple conversions, in order to be carried out as quickly as possible, even if the resulting costs are higher.

The counterpart not sent by the gateway node then becoming the property of the NodeOwner.

All costs involved in this replacement operation are charged to the NodeOwner who operates the faulty gateway node, and are deducted from its SSW guarantee tokens, which will be converted into the crypto-currency used to pay these costs (Ether for example to pay the corresponding gas costs).

All this operation ~~being~~ is carried out by the other nodes of the network and by the smart contract in charge of this task within the scope of the conservation of the guarantees of the gateway nodes.

The faulty gateway node is then disconnected, if it was still connected, and its SSW tokens remaining in guarantee are returned to the wallet that sent them (minus the shipping costs), therefore to the NodeOwner.

In the event of an unexpected disconnection of the node, the node has a delay (a few minutes) to reconnect with the same identifier before the procedure described above is activated. This will give the node a chance to resume normal activities in the event of a communication failure or an accidental but short-lived crash. During this time, the guarantee of the node (in SSW tokens) will obviously be retained by the smart contract.

This procedure is used both to ensure that the trader receives his counterparty following an exchange, and to encourage the NodeOwner to be sure that his gateway node works on a reliable machine that is not likely to crash, lose its Internet connection or be hacked. The NodeOwner assumes these risks.

SSW guarantee tokens are also returned to the NodeOwner (minus shipping costs) when its gateway node normally stops.

A NodeOwner has therefore an inflow of values (gains) in the form of a share of the fees paid by traders, in proportion to the SSW tokens he has pledged for the functioning of his node, versus the total number of SSW tokens allocated to all gateway nodes for this crypto-currency.

He pays fees to start and stop his node, corresponding to the initial sending and the return of SSW tokens left as guarantee (network fees).

In case of a malfunction of his node leading to the failure to deliver a counterparty, he pays the costs incurred by the system described above (which ensures the delivery of the counterparty to the trader), and he assumes the exchange risk of his SSW tokens that he no longer has and which are replaced by an equivalent value in the crypto-currency managed by his node, and paid to the wallet linked to the node (the assets not sent to the receiver).

Once the gateway node is stopped, all the assets present in the wallet linked to the node are the property of the NodeOwner. They come from the remuneration of the node and possibly from counterparties that have not been returned, but have been paid by the NodeOwner via his SSW tokens.

During its operation, the node also displays the quantity of assets belonging to the NodeOwner, in case he would like to transfer them without stopping the operation of his node.

Gateway nodes provide complete decentralization of blockchain access, with no single point of failure.

They provide significant redundancy both for connection to blockchains and for processing exchanges.

This high redundancy also allows to absorb periods of high load, allowing, if necessary, to add additional nodes very easily, without interrupting the operation of Secure Swap.

This secure node operating system, as well as the SSW tokens pledged on each gateway node, ensure that counterparties are received by traders, no matter what happens on the Secure Swap network.

Gateway nodes also allow Secure Swap to be crypto-agnostic, i.e. to operate with all crypto-currencies, without depending on emerging technologies such as Plasma or Lightning Network, while having comparable performance in its exchange processing capabilities.

## ~~LEVERAGE~~ MARGIN- TRADING NODE

~~Leverage~~ Margin-trading nodes allow the Secure Swap network to offer ~~leverage~~ margin-trading.

This type of nodes will also be distributed under Open Source license~~in open source~~, everyone being free to run one.

However, it should be noted that running this type of node is quite demanding. In addition to having a sufficient number of SSW tokens to provide a guarantee for traders, it is also necessary to have a capital in the form of crypto-currencies matching those in which ~~leverage~~ margin-trading is allowed.

*Grey Matter Technologies SpA* will act as the operator of this type of node, without any particular privilege.

### REQUIREMENTS TO BE ABLE TO CONNECT A MARGIN-~~LEVERAGE~~ TRADING NODE TO THE P2P NETWORK

As with other nodes, you need a reliable, secure machine with a stable Internet connection, so again, preferably a dedicated server.

It is necessary to have a reserve of SSW tokens equivalent to twice the sum of the margins of the positions that the node will authorize. In other words, the amount of pledged SSW tokens determines the amount of margin that can be used in positions taken by traders. Consequently, the quantity of SSW tokens used as a guarantee limits the height of the positions that can be taken at the same time on the node, in a ratio of 2:1.

These tokens will be secured via a dedicated smart-contract, similar to the gateway nodes.

It is also necessary to have sufficient crypto-currency capital so that the positions that the node authorizes can be taken by the trader, since the node advances the difference between the size of a position and the margin available on the trader's wallet, within the limit of the authorized leverage.

Example: the node allows margin-~~leverage~~ trading on Bitcoin, the trader wants to exchange 100 Bitcoins for another crypto-currency, the maximum leverage allowed is 5.

- The trader's initial margin must then be at least 20 Bitcoins.
- The minimum trader margin is 15 Bitcoins (margin call threshold equal to 0.75 * the initial margin for example)
- The SSW guarantee tokens (to guarantee the return of the trader's assets) must be equivalent in value to 40 Bitcoins (twice the guarantee margin).
- And the number of bitcoins available in capital at the node level must be a minimum of 80 Bitcoins, which, added to the trader's 20 Bitcoins margin, allows to take a 100 Bitcoins position (perform a 100 Bitcoin exchange transaction for another crypto-currency).

This multiplied by the number of equivalent positions that the node allows.

## OPERATION OF THE ~~LEVERAGE~~ MARGIN-TRADING NODE

For each pair of crypto-currencies for which he decides to allow ~~leverage~~ margin-trading, the node administrator will have to specify:

- The maximum leverage level allowed.
- The minimum margin threshold below which the position triggers a margin call.
- The entry and exit fees charged by the administrator.
- The hourly interest rate taken for the margin position.

In a very similar way to gateway nodes, once configured, the margin-trading node connects to the Secure Swap network. It sends its guarantee in SSW tokens to the smart contract specialized in the management of margin trading nodes. It then obtains its unique identifier that will allow it to operate.~~In a very similar way to gateway nodes, the leverage trading node connects to the Secure Swap network once configured, obtains its unique identifier and is only allowed to operate once it has received authorization from the other nodes, after sending its guarantee in SSW tokens to the smart contract specialized in leverage trading node management.~~

The node then informs the Secure Swap network of its ~~leverage~~ margin-trading capabilities, depending on its reserves available in crypto-currencies and updated according to the operations performed, so that clients applications can offer this trading via their interface. Relevant information will also be transmitted to client applications, such as the maximum leverage level allowed per pair of crypto-currencies, position holding fees (interest on the advance made by the node).

The Secure Trade client application thus presents to traders the available ~~leverage~~ margin-trading options. The trader places his order with Secure Trade, the order is transmitted via the Secure Swap p2p network to the relevant ~~leverage~~ margin-trading node, which, if the order is accepted (if it meets the criteria of margin, max leverage, etc.), will then request to receive the trader's margin. Once the margin is received, the node initiates a position for this trader, which consists of memorizing the loan granted to the trader and adding an exchange order corresponding to the transaction wanted by the trader to Secure Swap's order book.

Once the exchange order is executed on the Secure Swap network, the ~~leverage~~ margin-trading node retains the exchange counterparty, and monitors any unrealized losses on the exchange transaction.

If the unrealized losses, converted into the original crypto-currency, at the market rate, cause the minimum margin for maintaining the position to be exceeded, then the position is closed automatically, by margin call.

The position can also be closed at the trader's request via Secure Trade.

When closing a position, the ~~leverage~~ margin-trading node performs a reverse conversion of the first one, at the market price, using the counterpart that was held. Once the exchange is completed, it deducts the advance made previously, then sends the remainder to the trader, after subtracting from the remainder all the costs of the transaction.

Example:

A trader wants to trade on an exchange margin of 5 BTC for 150 ETH, the gateway node allows a maximum leverage of 5, and therefore requires an initial margin of 1 BTC minimum for this transaction. The minimum

margin before margin call being 0.75 times the initial margin, this node triggers a margin call if the available margin falls below 0.75 BTC.

The trader, via Secure Trade, gives the order to take this position.

The node will advance 4 BTC for this position, and will send the exchange order of 5 BTC for 150 ETH on the Secure Swap network. The exchange rate is therefore 30 ETH for 1 BTC.

If the order is executed, the ~~leverage~~ margin-trading node will receive the counterpart of 150 ETH for the 5 BTCs, 1 BTC belongs to the trader and represents his available margin (minus all costs), 4 BTCs being lent by the node.

If the exchange rate moves positively for the trader, and he decides to close the position when the rate becomes 1 BTC for 20 ETH, then the ~~leverage~~ margin-trading node that receives the order to close the position will post an exchange order for the 150 ETH it holds for that position for BTCs at market price.

For the example, the exchange is carried out at 1 BTC for 20 ETH. The node receives 7.5 BTC. The node recovers the 4 BTCs it had lent for this operation, and therefore sends the balance of 3.5 BTCs to the trader, minus the costs.

If the rate changes unfavourably for the trader, and it suddenly changes to 1 BTC for 35 ETH, then we have a margin call. The node automatically closes the position, and thus places an exchange order for 150 ETH for BTCs, at market price.

The exchange being carried out for the example at 1 BTC for 35 ETH, the node receives 4.28 BTC, recovers the advance of 4 BTC and sends the balance of 0.28 BTC to the trader minus the costs. The trader therefore suffers a loss of 0.72 BTC plus fees.

To simplify these examples, we have not calculated the position, exchange and network fees, which are paid by the trader and charged to his available margin during position holding, and deducted from the balance sent to the client at the closing of the position.

Similarly, the costs resulting from the interests taken by the node are deducted from the margin available when the position is held, and deducted from the balance returned to the trader.

The proper functioning of ~~leverage~~ margin-trading nodes is achieved by the gateway nodes, which control the margin-~~leverage~~ trading nodes, each according to the crypto-currency they manage.

If the ~~leverage~~ margin-trading node has reached a maximum number of global positions (twice the total sum of the margins used by traders is equivalent to the value level represented by the tokens of the guaranteeing node), then the gateway nodes no longer allow it to offer other margin positions to the client applications. Only the release of the positions held remains available, until a sufficient level of available guarantee is restored.

Similarly, if the node no longer has enough funds in a crypto-currency for the advance granted when taking a position, then the gateway nodes only allow it to release the positions on this crypto-currency until sufficient funds are restored.

If a ~~leverage~~ margin-trading node disconnects, crashes etc., it has a few minutes to become operational again. After this period, the smart contract dedicated to managing these nodes will start SSW tokens

exchange operations in order to refund customers holding margin positions managed by the faulty node. This process:

- Calculates the client's position at the time of disconnection of the faulty node.
- Determines unrealized gains/losses.
- Integrates them into the margin placed by the client on the faulty node.
- And returns the balance minus the costs (network, exchanges, interest) related to an immediate release of the positions held.

These SSW tokens will be converted via the liquidity available on Secure Swap and provided by the arbitration nodes, by conversion orders at market price, in order to provide traders with the crypto-currencies corresponding to their positions, all these operations being managed by the gateway nodes.

All costs incurred as a result of these exchange transactions and the sending of SSW tokens are charged to the faulty ~~leverage~~ margin-trading node, deducted from the SSW guarantee tokens, the balance of which will be returned to it at the end of these transactions.

As the distribution of the crypto-currencies of the reserve funds has been modified following the malfunction of the ~~leverage~~ margin-trading node, the exchange rate risk is no longer the same as initially. The operator of the node assumes the risk, and must possibly rebalance its distribution into crypto-currencies of the funds used to operate his node.

If a ~~leverage~~ margin-trading node, without being disconnected, does not send the owner the crypto-currencies that belong to him, when he has closed a position, the procedure described above is activated, only for that position.

Each time this procedure is triggered, without disconnection from the node, the quantity of SSW tokens used as guarantee for the ~~leverage~~ margin-trading node is reduced, which has an impact on its ability to take other margin positions. When the SSW guarantee tokens become lower in value than twice the sum of the margins corresponding to the current positions, then it can no longer accept other orders, this is prohibited to it by the gateway nodes, its trading capabilities are made unavailable within ~~at the~~ Secure Trade ~~level~~, for this ~~leverage~~ margin-trading node.

When a position causes a margin call (the margin is below the margin level required to hold the position), the node automatically reduces the position until it returns to a margin level equal to the normal initial margin for a position. If the margin level cannot be restored by reducing the position, then the position is completely closed.

An operator of a ~~leverage~~ margin-trading node therefore pays a start-up and shutdown fee (network costs related to sending and recovering SSW guarantee tokens from the smart contract).

He assumes all the risks of losses related to a malfunction of his node or a bad configuration resulting in inadequate risk management, such as:

- An excessively low minimum margin level before liquidation, which would cause a loss greater than the client's margin when liquidating the position.
- Or an authorized lever that is too large.
- Or the authorization to trade on margin for a pair of crypto-currencies that are too volatile.

His gains come from the position entry and exit fees, as well as interest on margin positions, which he charges.

It is important that an operator of this type of node properly assesses the risks associated with this activity. The configuration of the node must allow a position closure caused by a margin call without causing the node to go into negative balance, which, if this happens, constitutes a loss for the node operator. This depends both on the level of margin required to hold a position, but also on the volatility of the pair of crypto-currencies forming the position.

## NODE SPECIALIZED IN FIAT CURRENCIES EXCHANGES

The exchange nodes to fiat currencies are the connection points between crypto-currencies and traditional finance (state's fiat currencies).

These nodes are not anonymous. They require compliance with KYC ("Know Your Customer") rules. They will be operated by legal units, each offering its own list of exchangeable fiat-crypto pairs.

To comply with KYC rules, users will need to open an account on these types of nodes, with verification tiers, before they can use them.

These nodes function as trading exchanges. Users who have previously transferred fiat currencies to them (cash-in) will be able to exchange them for the crypto-currencies of other users wishing to sell their crypto-currencies for fiat currencies (cash-out).

In addition to the fiat-crypto exchange service, these nodes support the integration of payment methods, thanks to the release of a development kit (SDK) allowing the simple integration of payment methods on merchant websites, applications or mobile payment methods (smartphone).

This SDK will offer the integration of payment methods based on fiat currencies, but also on payments directly in crypto-currencies.

Grey Matter Technologies plans to operate this type of node, with a first step in the South American zone (Chile, Peru, Argentina to start with), and then in the USD and Euro zones.

To this end, it will create as many independent companies as there are areas where it will trade in fiat currencies, in order not to spread operational risks to the entire Secure Swap.

A node model will be provided under Open Source license~~in open source~~, adaptable to different payment methods, local regulations, and fiat currency for which it is intended. This will allow those who wish to carry out such a professional activity to offer support for the fiat currencies and methods of payment in their regions.

## ANOMALY DETECTION OR HACKING ATTEMPT DETECTION SYSTEM

When a sensitive operation takes place, whether it is checking the receipt of assets on a wallet, or any other transmission of information through nodes, clients or gateways, this information is verified by all nodes.

Example: If Secure Trade reports having sent such a quantity of assets on such a wallet, all gateway nodes to the relevant crypto-currency can verify the existence of the transaction, verify that it is being carried out and that the assets are being received by the indicated wallet.

Each node involved transmits this information to the other nodes, if nodes have conflicting responses, then the valid response is the one from the nodes that together combine the largest number of SSW guarantee tokens, which becomes the majority response. Nodes giving minority responses are disconnected from the network. Their SSW guarantee tokens, in the case of gateway nodes, are returned (possibly reduced by the counterpart retained by the node if the latter holds one).

With this system, the SSW tokens that already serve as a guarantee for the operation of gateway nodes also have a role as proof of stake.

This covers all sensitive operations, which are thus under the supervision of the entire network.

- This includes the matching announcement by a Secure Trade client. If no other Secure Trade indicates complementary matching, or if the gateway nodes do not validate matching, then the faulty Secure Trade is disconnected.
- This also includes the matching performed by arbitration nodes.

For gateway nodes, if one of them indicates that it has not received the counterparty from a client during an exchange, or if it does not send the counterparty to the recipient client while indicating that it has done so, or not, then this will be detected by the other nodes. The faulty gateway node will be disconnected, and its SSW tokens returned after subtracting the part necessary to complete the exchange, as described in the section "Gateway nodes and NodeOwners".

To prevent a node from falsifying statistics, this validation system is also used on gateway nodes, and applies to:

- The value of an SSW token expressed in each supported crypto-currency.
- The statistical state of distribution of the remuneration between the gateway nodes for the weighted random selection system of the next gateway node that will manage a counterpart of an exchange
- Etc.

In summary, all sensitive data are cross-checked by all nodes, as soon as they are able to do so (an Ethereum gateway node cannot check the reception of Bitcoins on a wallet for example, but all gateway nodes to Bitcoins can).

This cross-checking system, plus the pledge of SSW tokens of connected gateway nodes, ensures the security of exchanges, the detection of anomalies of any kind (hacking, malfunctioning...) and the disconnection of failed components.

This system implies that components that function normally are not prejudiced, and that defaulting components assume responsibility for their possible losses.

## COMMUNICATION PROTOCOL FOR SECURE SWAP NODES

This communication protocol is used when the data expected by a receiving node is sensitive and requires validation.

This protocol allows the one-step resolution of the Byzantine consensus (https://en.wikipedia.org/wiki/Byzantine_fault_tolerance) in a distributed and asynchronous environment.

This process is made possible by Secure Swap because the Secure Swap network does not need the data to be received in a specific order, and because it can rely on a proof of stake and pledge mechanism that simplifies its implementation.

Description of the protocol:

Each node knows the number of nodes that are expected to respond to a request. This number is updated each time a node appears or disappears on the network.

When a response is expected, a time window of up to 30 seconds is allocated for receiving the responses. Each receiving node memorizes and counts the responses.

As soon as the number of responses received corresponds to 60% of the nodes likely to respond, and all responses are identical, then the response received is validated and is considered accurate.

If, on the other hand, one or more answers are divergent, or the number of responses received does not reach 60% of the nodes likely to respond, then the 30 second time window is used to allow the maximum number of responses to be received.

When the time window for receiving responses has expired, and therefore the response is not yet validated, each response received is then rated. This rating is calculated by adding the number of SSW tokens allocated to the operation of each node that provided the same response. It is in this context that SSW tokens are used as proof of stake.

The answer with the highest rating is considered the correct answer. Nodes that have responded differently are excluded from the Secure Swap network (sending a disconnection request and invalidating the authorization to operate), which may result in the activation of the guarantee mechanism for the nodes concerned (exchanges in progress).

This protocol ensures the correct operation of the network in the event of a failure if at least 60% of the nodes respond to a request within the allotted time and all give the same response, or if the correct response is the one that is the dominant, in terms of proof of stakes, among those received within the time limit.

This protocol allows Secure Swap to be fault-tolerant, even when the failure is caused by a hacking attempt, while being efficient.

In the case of no failure, the response of only 60% of the nodes concerned validates the response. In case of failure, the answer is validated after a delay of 30s.

There can be as many validation processes in progress as there are responses waiting for validation. These validations take place in parallel, so there is no additional waiting time to validate a response that would be caused by waiting for another validation process of a previous response.

## IMPLEMENTATION OF THE COMMUNICATION PROTOCOL

When a sensitive operation occurs, whether it is checking the receipt of assets on a wallet, or any other transmission of information through nodes, clients or gateways, this information is verified by all nodes, according to the communication protocol described above.

Example: If Secure Trade reports having sent such a quantity of assets on such a wallet, all gateway nodes to the relevant cryptocurrency can verify the existence of the transaction, verify that it is being carried out and that the assets are being received by the specified wallet.

Each node concerned transmits this information to the other nodes. If nodes have conflicting responses, then the valid response is the one from the nodes that together cumulate the largest number of SSW tokens in guarantee, which becomes the dominant response. Nodes giving minority responses are disconnected from the network. In the case of gateway nodes, their SSW tokens as guarantee are returned (possibly reduced by the counterpart retained by the node if it retains one).

With this system, the SSW tokens that already serve as a guarantee for the operation of gateway nodes also have a role as proof of stakes.

These mechanisms cover all sensitive operations, which are thus under the supervision of the entire network.

- This includes the announcement by a Secure Trade app of a matching. If no other Secure Trade indicates complementary matching, or if the gateway nodes do not validate matching, then the faulty Secure Trade is disconnected.
- This also applies to matching carried out by arbitration nodes.
- As well as the operations carried out by margin trading nodes.

For gateway nodes, if one of them indicates that it has not received the counterparty from a client during an exchange, or if it does not send the counterparty to the recipient client while indicating that it has done so, or not, then this will be detected by the other nodes. The faulty gateway node will be disconnected, and its SSW tokens returned after subtracting the part necessary to complete the exchange, as described in the section "Gateway nodes and NodeOwners".

To prevent a node from skewing statistics, this validation system is also used on gateway nodes, and applies to:

- The value of an SSW token expressed in each supported cryptocurrency.
- The statistical state of distribution of the remuneration between the gateway nodes for the weighted random selection system of the next gateway node that will manage a counterpart of an exchange
- Etc.

In summary, all sensitive data is multi-checked by all nodes, as soon as they are able to do so (an Ethereum gateway node cannot check the reception of Bitcoins on a wallet for example, but all gateway nodes to Bitcoins can).

This multi-checking system, plus the pledge of SSW tokens of connected gateway nodes, ensures the security of exchanges, the detection of anomalies of any kind (hacking, malfunctioning...) and the disconnection of failed parties.

This system implies that parties that function normally are not penalized, and that failing parties assume responsibility for their possible losses.

## SYSTEM THAT GUARANTEES THE ATOMICITY AND SECURITY OF EXCHANGES

When a counterparty is found by a client application, it issues a reservation of the relevant order, which is propagated on the nodes of the Secure Swap network. The order thus becomes locked and unmodifiable for the Secure Trade client that has issued it. The opposite Secure Trade client will also find the additional counterpart, coming from the first client, and book it too.

Example: Bob put an order of 2 BTC for 60 ETH, Alice put an order of 32 ETH for 1BTC.

Matching is found by both clients.

Secure Trade (at Bob's) locks Alice's order at 32 ETH for 1 BTC.

Secure Trade (at Alice's) locks Bob's order from 1 BTC to 30 ETH (1 BTC to 30 ETH remains in the order book for Bob).

Once both counterparties are locked, the gateway nodes will initiate and manage the exchange process.

This will not be repeated later, to avoid burdening the description, but all the gateway nodes that match the counterparties (here in the example: BTC gateway nodes and ETH gateway nodes) will check all the steps in the process. This includes:

- The validity of the addresses of the wallets transmitted (possession of the counterparty by the trader).
- The effective reception of counterparties, by randomly selected gateway nodes.
- The return, through the gateway nodes acting as intermediaries, of counterparties to the right recipients.
- The good reception of their counterparts by Bob and Alice's Secure Trade applications.

In case of disagreement between the nodes, the valid answer is the one provided by the nodes with the most SSW guarantee tokens together (proof of stake), as described in the chapter: “Gateway nodes and NodeOwners”. This mechanism allows the exchanger to operate in a trustless environment.

A gateway node on BTC will be selected to receive this part of the exchange, randomly according to a weighted selection described in the chapter “Gateway nodes and NodeOwners”. An ETH gateway node will be selected according to the same method.

Once the reception nodes of the designated counterparties have been received, their wallet addresses are transmitted to the two Secure Trade applications that receive the validation of the counterparties' sending.

Both Secure Trade applications send their counterparts to the designated gateway nodes. Once both gateway nodes have confirmed that they have received these counterparties, the nodes send the assets to the Secure Trade applications of the final recipients, which concludes the exchange.

Using our example, Bob sent 1 BTC and received 32 ETH in exchange, he still has an exchange order of 1 BTC for 30 active ETH. Alice sent 32 ETHs and received 1 BTC in exchange.

In case of an incident during the exchange (disagreements between nodes), the minority nodes are disconnected and the exchange is continued with the remaining nodes, which can lead to a new random selection of nodes that serve as intermediaries for the exchange.

If a gateway node holds a counterpart, for one of the following reasons:

- It does not send it to its recipient within a normal time frame (blockchain delay).
- It had received a counterpart before it disconnects itself, or by outvoting, following a disagreement between nodes.
- It is disconnected or no longer responds to network requests.

Then, the counterparty held by the node will be delivered to the trader according to the terms described in section “Gateway nodes and NodeOwners”.

Thus, the cross-verification and pledge of SSW tokens guarantees the security of transactions in the trustless Secure Swap environment.

## EXCHANGER PERFORMANCE

We have seen previously that the exchanger is not dependent on the capacities of a blockchain for its operating speed. Whether it is for order book management, transactions management and all other systems. Of course, an exchange itself cannot be completed faster than a blockchain allows, but the blockchains do not limit the number of transactions per second that the exchanger can transmit.

The number of transactions that can be operated is estimated at about a thousand transactions per blockchain per second. The p2p network is made up of multiple sub-networks. Each of these sub-networks manages only one blockchain. Each sub-network is independent of the other sub-networks and therefore independent of the other blockchains. This means that the total capacity of the exchanger is multiplied by the number of blockchains managed, which can represent a few tens to hundreds of thousands of transactions per second in total.

Thus, without dependence on technologies still in development, Secure Swap offers, with its own technology, performances similar to those targeted by Plasma or Lightning Network.

If we consider a particular blockchain, in the end, the speed of the exchanger is of course limited by the ability of the blockchain in question to mine/validate transactions.

Currently the Ethereum blockchain is limited to about 10/15 transactions per second.

Nevertheless, developments are underway to greatly increase the number of transactions per second that the Ethereum blockchain will be able to perform. We are talking about an increase of a few hundred thousand or even millions of transactions per second, thanks to technologies such as Plasma, Sharding and the Lightning network. Other blockchains, based on proof of stake, are natively fast. Secure Swap has the ability to exploit the current and future speed of these blockchains.

We use smart contracts on the Ethereum blockchain to manage the SSW tokens pledged for the connection of the various services, which are used in case of anomalies on these services, and to authorize the operation of the various services.

We are therefore dependent on the future of the Ethereum blockchain for the functioning of Secure Swap.

However, nothing would prevent us, if necessary, from switching the operation of these modules dependent on the smart contract to another blockchain, and distributing these tokens in replacement of the SSW ERC-20 tokens in circulation.

A fairly simple way to do this would be to switch the operation to the Tomochain blockchain, which can be considered as a fork of Ethereum, fully compatible at the token and smart contract level, but which integrates Sharding and Plasma from the beginning and which works on a proof of stake, making it much faster than Ethereum. Nevertheless, it will be necessary to replace the tokens held by all owners with the new tokens of this blockchain. This would imply a parallel Secure Swap operation, for smart contracts and tokens, on both blockchains, until all SSW ERC-20 tokens are exchanged for those of the new blockchain.

However, there is no indication that we would have any reason to doubt about the future of the blockchain Ethereum. Thus, the dependence of Secure Swap's operation on it, via our smart contracts and tokens, seems to us to be a long-term solution. And if we are wrong on this point, we will migrate to another blockchain, which simply means migrating smart contracts and tokens.

## INDICATION OF THE STATUS OF THE EXCHANGER

We have seen in the previous sections that gateway nodes, in addition to their other functions, manage the statistics of the Secure Swap network.

These statistics will be used by Secure Trade client applications as well as by other nodes in the p2p network.

### INDICATIONS DISPLAYED BY THE CLIENT APPLICATION

The Secure Trade application will indicate via a colour code the availability of gateway nodes for each crypto-currency:

- Red: no gateway available for this crypto-currency → no exchange possible.
- Orange-Rouge: only one gateway available for this crypto-currency → exchanges technically possible but forbidden.
- Yellow: two gateways available for this crypto-currency → exchange ok.
- Green: from three gateways and more available for this crypto-currency → exchange ok, ensuring optimal operation.

It is possible, but not recommended, to trade on a crypto-currency where only two gateway nodes would be in use, this makes protection by proof of stake potentially fragile (system designating the correct answer in case of disagreement between nodes).

In case of disconnection of one of the 2 gateway nodes, only one node would remain in service, prohibiting trading for this crypto-currency. Nevertheless, an exchange that would be in progress at that time would be concluded, either normally or by using the SSW tokens pledged by the disconnected node (if it kept any counterpart received before disconnection).

To ensure an optimal launch of the service, *Grey Matter Technologie SpA* will operate three gateway nodes for each crypto-currency initially managed, until the community takes over.

### INDICATIONS ACCESSIBLE FROM GATEWAY NODES

The gateway nodes will continuously maintain up-to-date network statistics to produce various information for NodeOwners, arbitration and ~~leverage~~ margin-trading node operators and traders. These statistics will allow, for example:

- Provide a dashboard of advanced statistics about nodes.
- Evaluate the expected remuneration according to the SSW tokens allocated to a gateway node.
- To check the volumes of exchanges over a period of time by crypto-currency.
- Indicate the exchange rate of SSW tokens for each crypto-currency, etc.

## SECURE TRADE, THE TRADING CLIENT APPLICATION

Secure Trade, is a trading application that provides both advanced tools and a multi-wallet portfolio. Secure Trade will be developed primarily for computers running Windows, Linux and MacOS operating systems, before being ported to IOS and Android in its mobile version.

### CONNECTION

At launch, Secure Trade must connect to a minimum of three gateway nodes before allowing user operations.

### WALLETS

To manage the different types of wallets, the Secure Trade application uses a plugin system, defining a common programming interface.

The wallet plugins managed by Secure Trade will be installed from plugin repositories. Secure Trade will manage a list of repositories that can be updated. In order to add a wallet for a crypto-currency, the user only has to select the corresponding plugin from a list, the plugin will then install itself in Secure Trade.

This allows you to add wallets for other crypto-currencies, by downloading the plugin, without having to modify the Secure Trade application.

So, when you add a crypto-currency to Secure Swap, by adding a gateway node to a blockchain, you must also provide the corresponding wallet plugin for the Secure Trade application.

Hardware wallets, such as Trezor, Ledger etc., will also be managed through their respective plugins.

If new hardware wallets appear on the market, it will be only necessary to develop and add the corresponding plugin.

The consultation of the balance of the wallets, the issuing of transactions, etc. are done via the support of gateway nodes connected to Secure Trade clients. If the connected node cannot execute an operation itself, it routes the operation to a node capable of executing it (the execution capacity depends on the blockchain concerned by the operation and the blockchain to which the gateway node is connected).

## CHARTS, REAL TIME DATA

The price-chart data for each crypto-currency is taken from the price history generated by transactions made on Secure Swap.

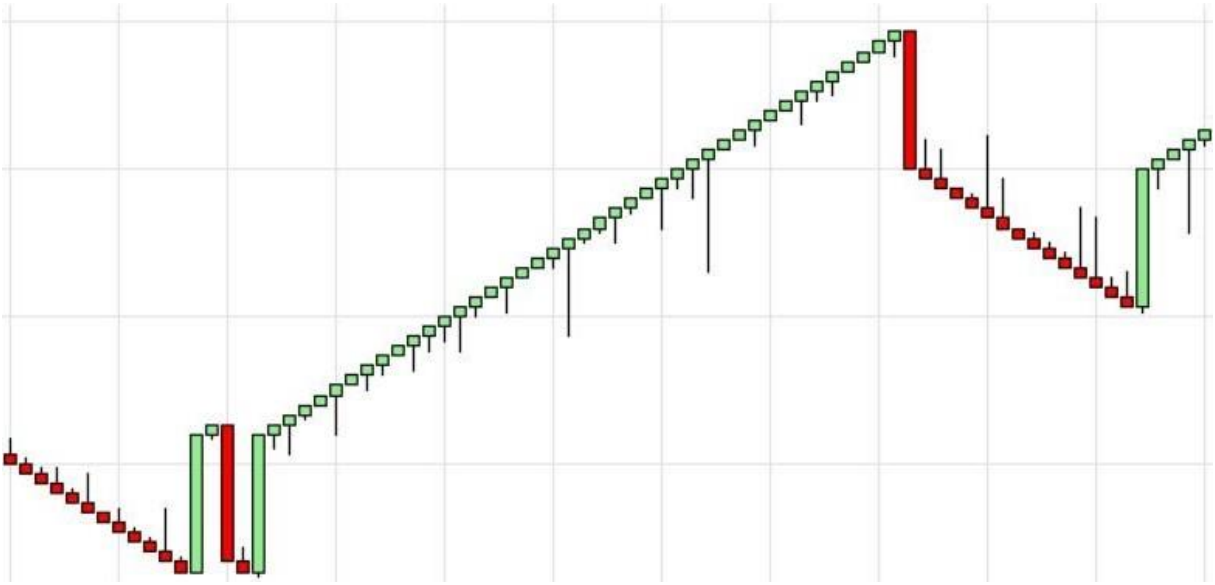
It is again the gateway nodes that store the price historical data, each for the blockchain to which it is connected. The gateway nodes, when they are activated, retrieve these historical data from the gateway nodes already connected to the same crypto-currency.

Secure Trade receives the raw data from the gateway nodes, tick by tick, i. e. transaction by transaction, and represents them according to the parameters chosen by the trader.

In addition to the classic time displays, where the trader can choose the period (ticks, seconds, minutes etc.), Secure Trade also offers the Kagi, Renko, Line Break, Harmonic Bar (an improved line break), Point and Figure, Volume, Volume Filter, Range representations.

The default graphic style is the classic candlestick, but can be changed to the LineOnClose, Hi Lo, or OHLC style.

Example of a bar harmonic display (break 28 and trend 2) and candlestick:



## THE ORDER BOOK

As mentioned above, Secure Trade is a node like any other from the point of view of the transmission of order book data, so it receives updates from them.

The order book module of the Secure Trade application indicates volumes by price level (depth of the order book), but also the source of liquidity by a colour code.

For example, green for volumes from the Secure Swap order book, orange for volumes from arbitration nodes. The distinction of the origin of liquidity is important because the one coming from the arbitration nodes can lead to a slightly slower exchange than exchanges using liquidity coming directly from the Secure Swap network.

## TRADING TOOLS

Apart from the classic trading tools and the different types of orders available which are:

- Market order,
- Limit order,
- Stop order,
- Trigger threshold order,
- Trigger threshold order with limit,
- OCO Order (order cancels order),
- Multiple orders,

Secure Trade has scalping and money management support modules, executing semi-automatic orders defined in advance.

## ~~LEVERAGE~~ MARGIN-TRADING

Each available ~~leverage~~ margin-trading node has its own ~~leverage~~ margin-trading conditions:

- Pairs of crypto-currencies authorized for ~~leverage~~ margin-trading,
- Margin position entry and exit fees,
- Initial and minimum margin level (triggering a margin call if insufficient margin),
- Hourly interest on margin positions,
- Maximum leverage level.

Secure Trade displays the list of available arbitration nodes and their configurations.

Secure Trade has filters to select arbitration nodes according to these criteria. It also indicates, for each node, its identifier and its online duration without disconnection, so that the trader can avoid the most unreliable nodes. Considering that a disconnection from an arbitration node implies the closing of the positions of the trader.

## AUTOMATION TRADING

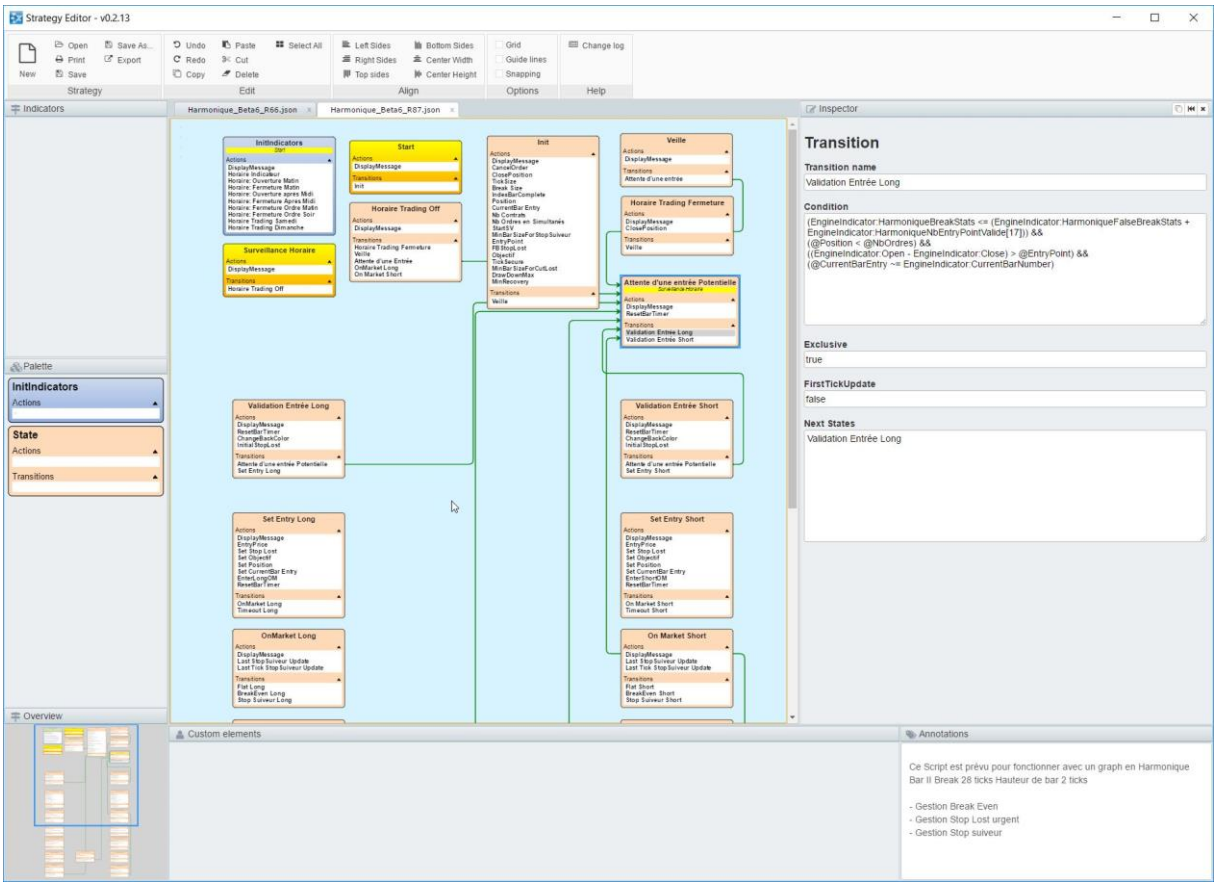
Secure Trade has an automatic trading module.

This module consists of a hierarchical and Concurrency ~~competitive~~ Sstate ~~machine~~ Machine (~~HCMS~~HCSM: ~~Hierarchical Concurrency State Machines~~). A simplified scripting language as much as possible will make it possible to program this states machine to execute commands according to programmed conditions.

These conditions may use the results of all available indicators as well as price-charts, wallet status, money management indications, time indications, etc.

The programming of these states machines is done through a graphical editor, accessible even to people who do not have much programming knowledge.

Version of the strategy editor under development:




Alpha version of the strategy editor.

## HOW TO OVERCOME THE INITIAL LACK OF LIQUIDITY?

When they are launched, exchangers inevitably have liquidity problems: when they are put into service, their order books are empty, which is not an incentive for the first traders. Liquidity problems may also exist on crypto-currencies with low trading volumes.

At start-up, Secure Swap will have no liquidity of its own and will have to rely on external liquidity provided by the arbitration nodes.

For this purpose, *Grey Matter Technologies SpA* will mobilize a part of its funds. These funds will be divided into various crypto-currencies available for arbitration services (one arbitration node per third party exchanger). We initially plan to use the liquidity of three centralized exchangers.

These arbitration nodes will be operated by *Grey Matter Technologies SpA*, with appropriate funds allocated to each instance connected to a third-party exchanger, in order to ensure that they operate efficiently in providing liquidity.

Members of the Secure Swap community will also be able to operate this type of node connected to third-party exchangers, which will provide even more liquidity.

## AN EXCHANGER UNDER OPEN SOURCE LICENSE

The different types of nodes of the exchanger will be distributed under Open Source license.

This means that, in addition to Secure Trade serving all traders, everyone will have the opportunity to support the functioning of the exchanger by operating nodes connected to blockchains, trading nodes to fiat currencies, arbitration nodes (providing liquidity) and ~~leverage~~ margin-trading nodes.

NodeOwners operating gateway nodes and owning SSW tokens will receive their share of the fees, charged during exchanges, in proportion to the tokens they have allocated to a gateway node to a blockchain, compared to the total number of SSW tokens allocated to the gateway nodes to the same blockchain in operation.

The other types of nodes are able to generate their own revenues independently, so they are not included in this cost-sharing system.

*Grey Matter Technologies SpA* will operate in the same way and will receive its share of the exchange fees in proportion to the SSW tokens it will own at the end of the ICO and which it will reserve for each gateway node to a blockchain that it will operate.

We will also provide an open source node model for exchange to fiat currencies, with interfaces to connect to bank payment processors. Since this activity is highly regulated, and requires both adaptation for each case (local regulations and interfaces to the payment processors used) and starting a legal activity to be operated (via a company), the node model that we will provide under Open Source license ~~in open source~~ will have to be adapted to each particular case.

*Grey Matter Technologies SpA* will initially operate this type of node for the regions of South America, USA and Europe. We plan to operate fiat currency conversion nodes for the following currencies: Chilean Peso, Argentine Peso, Peruvian Sol, USD and Euro and possibly others later on.

Thus, gradually, this exchanger will be able to support conversions to a large number of fiat currencies and regions of the world.

## BUG BOUNTY PROGRAM

A part of the funds raised during the ICO will be used to finance a pen-testing service and bug bounty campaigns. Rewards will be given to those who participate in these bounty bug programs and have reported bugs or security breaches to our teams that are still unknown.

Pen-testing session will be run at each stage of the development phases, so that the first version of the platform put into production has already been well analysed.

Quarterly Bug bounty campaigns are planned from the first release candidate version, to support the continuity of developments.

We will study the relevance of using the services of Buglab, a platform on the Ethereum network that allows the connection for this type of program.

https://buglab.io/#about

## SSW TOKEN - FINANCIAL ASPECT

### DATA USED FOR THIS PROJECTION

- Total number of tokens issued: 100,000,000
- Token Issuing Price: 0.45 $ USD
- Percentage of tokens actually allocated to gateway nodes: 30%

We believe that some SSW tokens purchasers will not operate gateway nodes to crypto-currencies (and thus will not benefit from the corresponding share of the exchange fees paid by traders), but will only purchase them for speculative purposes on the token's price.

And some of the tokens will be used to operate ~~leverage~~ margin-trading nodes.

Therefore, we believe that a maximum of 30% of SSW tokens will actually be allocated to the operation of gateway nodes. The lower the proportion of tokens allocated to the operation of gateway nodes, the higher the token efficiency for those who operate nodes.

We will use data from CoinMarketCap to collect daily exchange volume of exchangers and volume distribution between crypto-currencies, gathered at the end of July 2018, to evaluate the possible yield of SSW tokens for those who would acquire these tokens at the ICO price and operate gateway nodes with them.

| Examples of the distribution of exchanges between crypto-currencies over 24 hours: | |
|---|---|
| Bitcoin : | 33% |
| Tether : | 20% |
| Ethereum : | 11% |
| EOS : | 4.5% |
| OmiseGo : | 0.45% |

We have here the 3 most exchanged crypto-currencies and also 2 less exchanged crypto-currencies.

To assess a realistic range of token profitability, we will consider different scenarios for the daily trading volume of Secure Swap:

## PROJECTION OF THE RETURN ON INVESTMENT IN THE SSW TOKEN

We consider that the tokens, which are allocated to the operation of gateway nodes, are allocated in proportion to the volume of exchanges of each crypto-currency.

An over-allocation of tokens to gateway nodes of a crypto-currency would lower the profitability of the tokens for that crypto-currency. On the other hand, the under-allocation of tokens to other crypto-currencies would increase their efficiency. This means that those who operate gateway nodes will tend to allocate their tokens to the most profitable crypto-currencies, which will reduce their profitability and increase the profitability of the other crypto-currencies. As a result, the distribution of tokens on gateway nodes will naturally tend to be in line with the distribution of exchange volumes between crypto-currencies.

Formula for the evaluation of token profitability:

| | |
|---|---|
| P | Profitability of the token |
| TTOK | Total tokens issued to the ICO |
| PTAN | Percentage of tokens allocated to gateway nodes |
| TV | Trading volume over a period, in USD |
| PEC | Percentage of exchanges of crypto-currency compared to the total exchanged |
| PRTC | Percentage of tokens distribution for crypto-currency gateway nodes |
| PPT | Purchase price of the token, in USD |
| F | Fees taken by the platform for exchanges |

Token profitability: $$P = \frac{(\frac{\sum TV \times PEC}{PRTC} \times F)/(TTOK \times PTAN)}{PPT}$$

We see that if PEC = PRTC, we get:

Token profitability: $$P = \frac{(\sum TV \times F)/(TTOK \times PTAN)}{PPT}$$

**THE PROFITABILITY IS THEREFORE THE SAME FOR ALL CRYPTOS IF PEC = PRTC, REGARDLESS OF THEIR EXCHANGE VOLUME.**

For example:

Let's take a trading volume of $3 million USD daily (rank 100 exchanger on CoinMarketCap)

In a year, that gives us: ∑ TV = 365*3 = $1,095 million USD

The exchange fees being F = 0.15%, we then have:

Profitability = ((1,095,000,000 * 0.0015) / (100,000,000 * 0.3)) / 0.45 = **12.2%** annual return

With a trading volume of $10 million USD daily (rank 75 exchanger on CoinMarketCap)

Profitability = ((10,000,000 * 365 * 0.0015) / (100,000,000 * 0.3)) / 0.45 = **40.6%** annual return

With a trading volume of $20 million USD daily (rank 50 exchanger on CoinMarketCap)

Profitability = ((20,000,000 * 365 * 0.0015) / (100,000,000 * 0.3)) / 0.45 = **81.1%** annual return

And if, despite its advantages, Secure Swap did not do better in terms of volume traded than the average DEXs, at least in the first year, by the time it is massively embraced, it would still generate about $1.2 million to be exchanged per day (approximately the volume of Bancor, Crypto Bridge and Wave DEX), the return would still be:

Profitability = ((1,200,000 * 365 * 0.0015) / (100,000,000 * 0.3)) / 0.45 = **4.8**% annual return

## CONCLUSION

We believe that with its advantages, Secure Swap will quickly reach the trading volumes of the most active DEXs, such as Bitshare, IDEX and OpenLedger.

This represents approximately 400 BTCs of daily exchange, i.e. with a BTC quotation at USD $6,000, **an annual return of approximately 10% of SSW tokens**.

In the future, we believe that Secure Swap is able to capture significant market shares from centralized exchangers, which will further increase the profitability of holding SSW tokens in order to operate gateway or ~~leverage~~ margin-trading nodes.

We have not quantified the profitability of ~~leverage~~ margin-trading activity, as it depends too much on the configuration choices made by their operators and the volume of ~~leverage~~ margin-trading.

Likewise, we have not quantified the profitability of an arbitration node or a fiat currency exchange node, which depends on too many parameters currently unknown, such as the volume of liquidity provided and actually used on the Secure Swap network, the opportunity to benefit from price differences between exchanges, the trading volume to each fiat currency, and so forth.

These projections show us that the profitability of SSW tokens increases rapidly with the daily volumes exchanged. If Secure Swap actually takes market shares from centralized exchangers, which is what it was designed for, and what is its objective, then the SSW token could become very popular and profitable.

# SECURE SWAP ICO AND ERC20 TOKEN (SSW)

## WHY CREATE AN ERC20 TOKEN?

The SSW token, in addition to being used to collect funds at the ICO, will serve as proof of stake and guarantee allowing the safe operation of the exchanger, as well as the distribution of the fees paid by traders and collected during the exchanges.

## TOKENOMICS

| | |
|---|---|
| Token name: | Secure Swap |
| Ticket: | SSW |
| Quantity created: | 100 million tokens |
| Initial token price: | 0.45 $ USD |
| Reserved for the team: | 10% |
| Reserved for the advisors: | 3% |
| Reserved for social animators: | 3% |
| Reserved for partners: | 4% |
| Available for the ICO: | 80% |
| Soft Cap: | 10 million tokens |
| Hard Cap: | 80 million tokens |

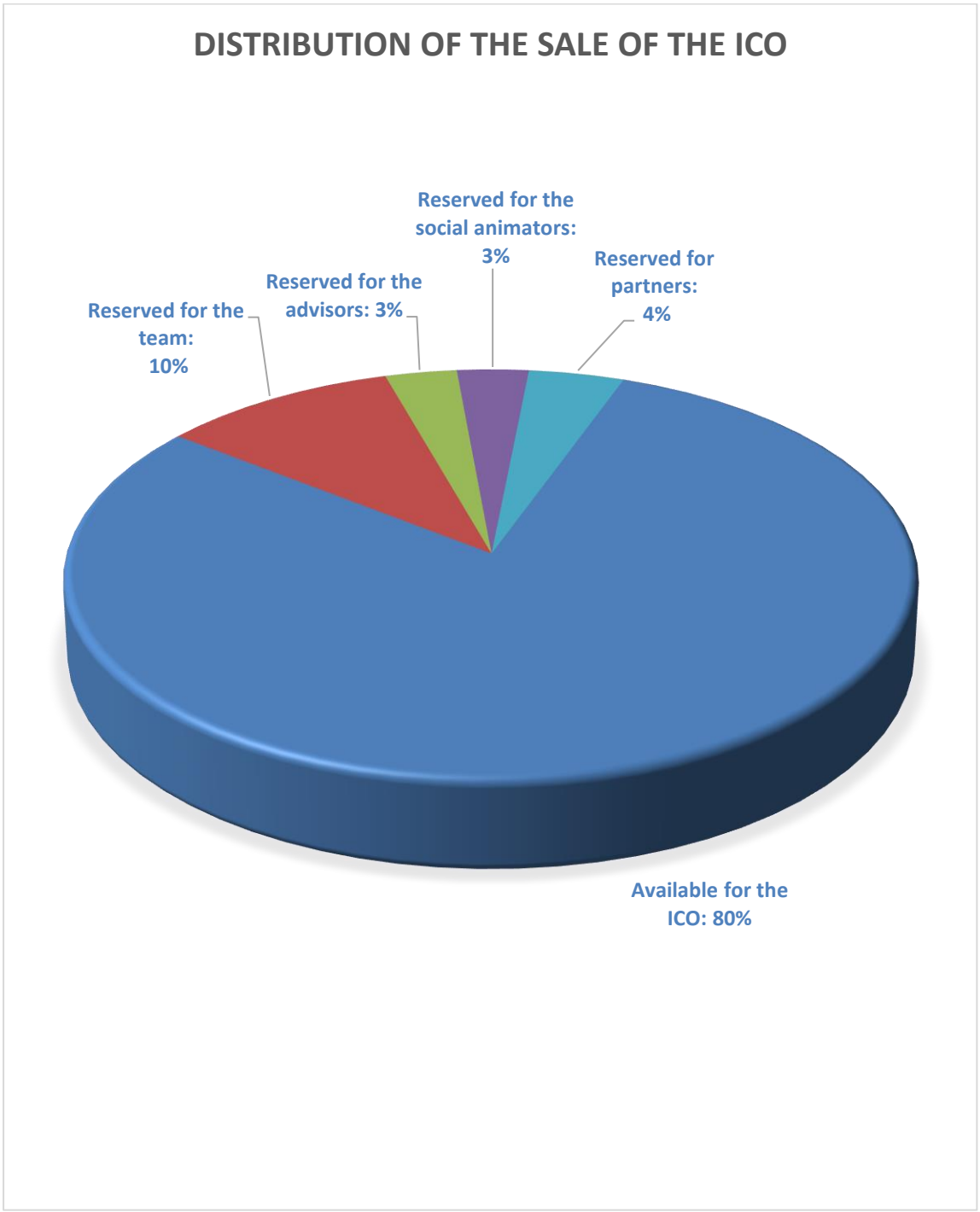
All unsold tokens remain the property of *Grey Matter Technologies SpA* in order to serve as proof of stake and guarantee in the operation of the gateway nodes that will be operated by the company.

There is no way that the team can recover the unsold tokens, this would constitute a misuse of company assets.

These tokens will remain the property of the Company, in order to use them as proof of stake and guarantee to operate nodes, the Company acting as a NodeRunner(s) and as an operator of ~~leverage~~ margin-trading nodes.

This will be the company's main source of income. Other revenues will come from fees collected on fiat exchanges as well as profits made with arbitration nodes.

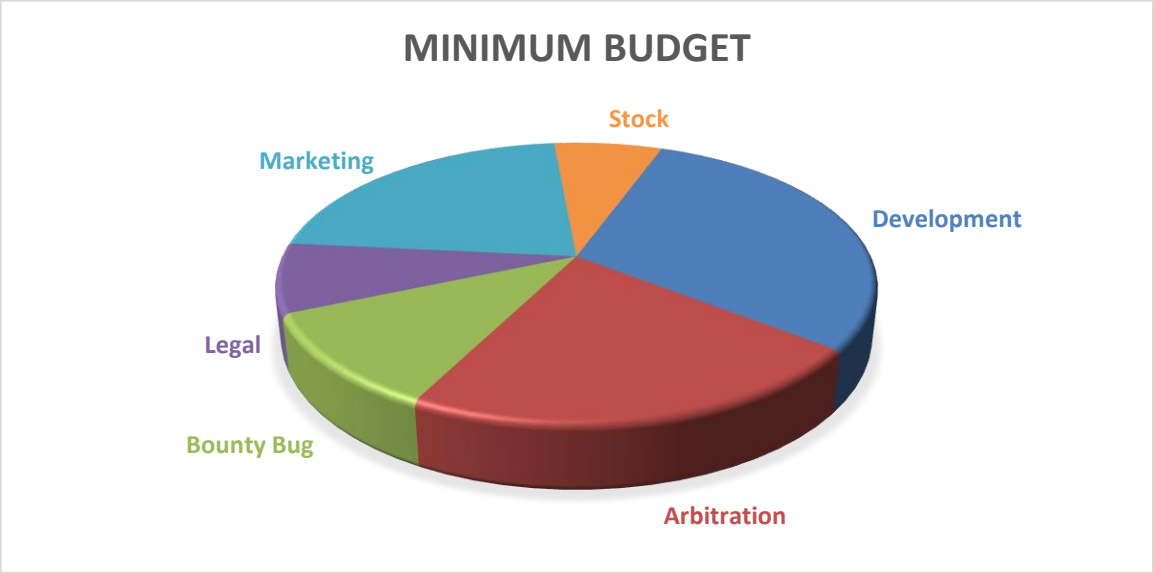
The *Grey Matter Technologies SpA* company reserves itself the right to redeem the SSW tokens allocated to the team and other collaborators (advisors, social workers, and partners), in order to increase its revenue from the gathering of fees paid by traders.


DISTRIBUTION OF THE SALE OF THE ICO
Reserved for the social animators: 3%
Reserved for partners: 4%
Reserved for the advisors: 3%
Reserved for the team: 10%
Available for the ICO: 80%

## USE OF FUNDS RAISED

Here, we are going to give details about the distribution of funds, in 2 extreme cases: soft cap reached and hard cap reached.

### SOFT CAP REACHED




The soft cap is the budget necessary to develop the minimum viable product.

It represents US$ 4.5 million.

Development budget: ..... 1.35 Million $USD

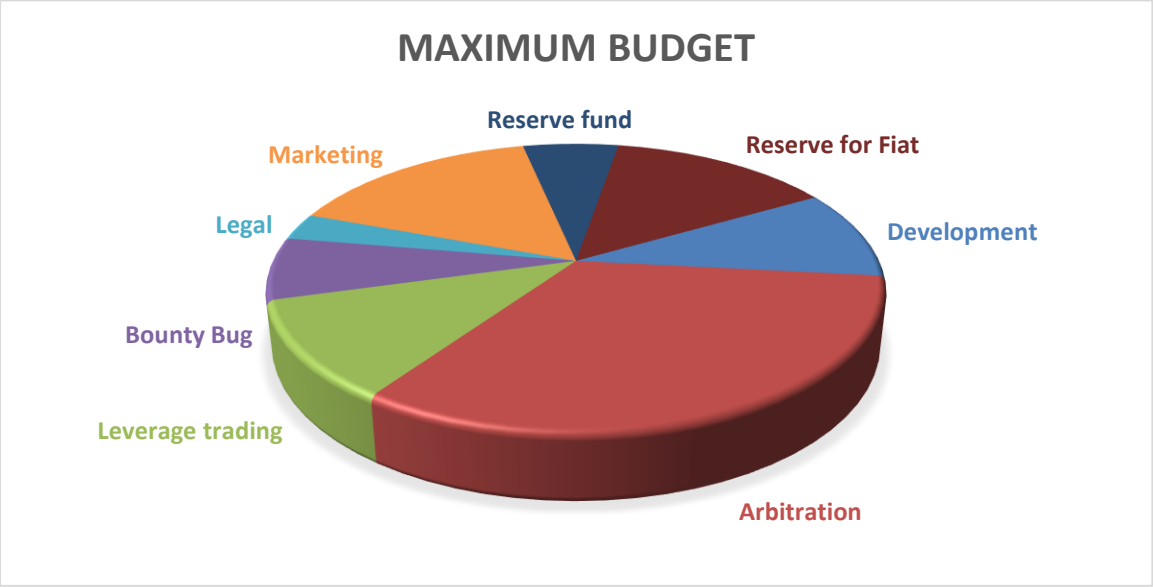
- Secure Trade simplified trading client application (Blockchain Ethereum trading only): ..... 400 K $USD
- Gateway node model + smart contract without controls on ~~leverage~~ margin trading nodes: ..... 450 K $USD
- Specialization of the gateway node model for the Ethereum blockchain + Tokens: ..... 100 K $USD
- Arbitration node model: ..... 350 K $USD
- Specialization of the arbitration node model for a third-party exchanger: ..... 50 K $USD

Operation of the arbitration node by *Grey Matter Technologies SpA*:
Required cash stock:..... 1 Million $USD

- 70 % Ethereum
- 30 % spread out in tokens ERC-20 / ERC-223 / ERC-777

Bug Bounty Program: ..... 500 K $USD
Marketing: ..... 1 Million $USD
Legal: ..... 350 K $USD
Reserve fund: ..... 300 K $USD

## HARD CAP REACHED




The hard cap is the budget needed to make the product with all the features.

It represents US$ 36 million.

Development budget: .....3.7 Millions $USD

- Complete Secure Trade trading client application: .....800k $USD
  - Trading on all Blockchains
  - ~~Leverage~~ Margin-trading
  - Order placement on the graph
  - Money management support module
  - Programmable automatic trading module

  Gateway node model + ~~leverage~~ margin-trading controls
  + smart contract: .....700k $USD
- Specialization of the gateway node model
  - For Ethereum blockchain + Tokens: .....100k $USD
  - For Bitcoin blockchain: .....50k $USD
  - For Tether blockchain:.....50k $USD
  - Ripple:.....50k $USD
  - Bitcoin Cash: .....50k $USD
  - EOS: .....50k $USD
  - Litecoin: .....50k $USD
  - Stellar Lumen:.....50k $USD
  - Monero:.....50k $USD
  - Dash:.....50k $USD
  - Neo: .....50k $USD
  - Zcash:.....50k $USD
- ~~Leverage~~ Margin-trading Node + SC (smart contract):.....750k $USD
- Arbitration node model:.....350k $USD

  Specialization of the arbitration node model
  for three third-party exchangers: 3*50k = .....150k $USD
- Model of exchange node to fiat currency + SDK: .....300k $USD

Operation of three arbitration nodes by *Grey Matter Technologies SpA*: 3 x 4M $USD:..... 12 Million $USD

Distribution by arbitration node:

- Bitcoin ..... 1,3 Million $USD
- Tether..... 1 Million $USD
- Ethereum and Tokens ..... 1 Million $USD
  (70% Ethereum, 30% Tokens ERC-20 / ERC-223 / ERC-777)
- Ripple ..... 300 K $USD
- Other crypto-currencies..... 400 K $USD

Operation of a ~~leverage~~ margin-trading node by *Grey Matter Technologies SpA*: ..... 4 Million $USD

Distribution of funds between crypto-currencies similar to an arbitration node, but reduced to a part of the crypto-currencies on the basis of volatility criteria.

Opening and operation of five legal units for the exploitation of conversions into fiat currencies and payment services, USD, EUR, CPL (Chilean pesos), SOL (Peruvian sol), ARS (Argentine pesos): 5 * 1M $USD ..... 5 Million $USD

By unit: 1M $USD

- Legal: .....400 K $USD
- Structure (company creation, staff…): ..... 200 K $USD
- Technical platform: ..... 100 K $USD
- Specialization of the exchange model to fiat currency: .....100 K $USD
- Marketing:..... 100 K $USD
- Reserve:..... 100 K $USD

We prefer to have independent units for the exploitation of payment methods and exchanges between crypto-currencies and fiat currencies in order to guarantee a clear legal separation between Secure Swap / *Grey Matter Technologies SpA* and fiat exchanges, in order to protect *Grey Matter Technologies SpA* and the core of Secure Swap from regulations risks associated with fiat exchanges.

Bug Bounty Program: ..... 2,5 Million $USD

Marketing: ..... 6 Million $USD

Legal: ..... 1 Million $USD

Reserve Fund:..... 1.8 Million $USD

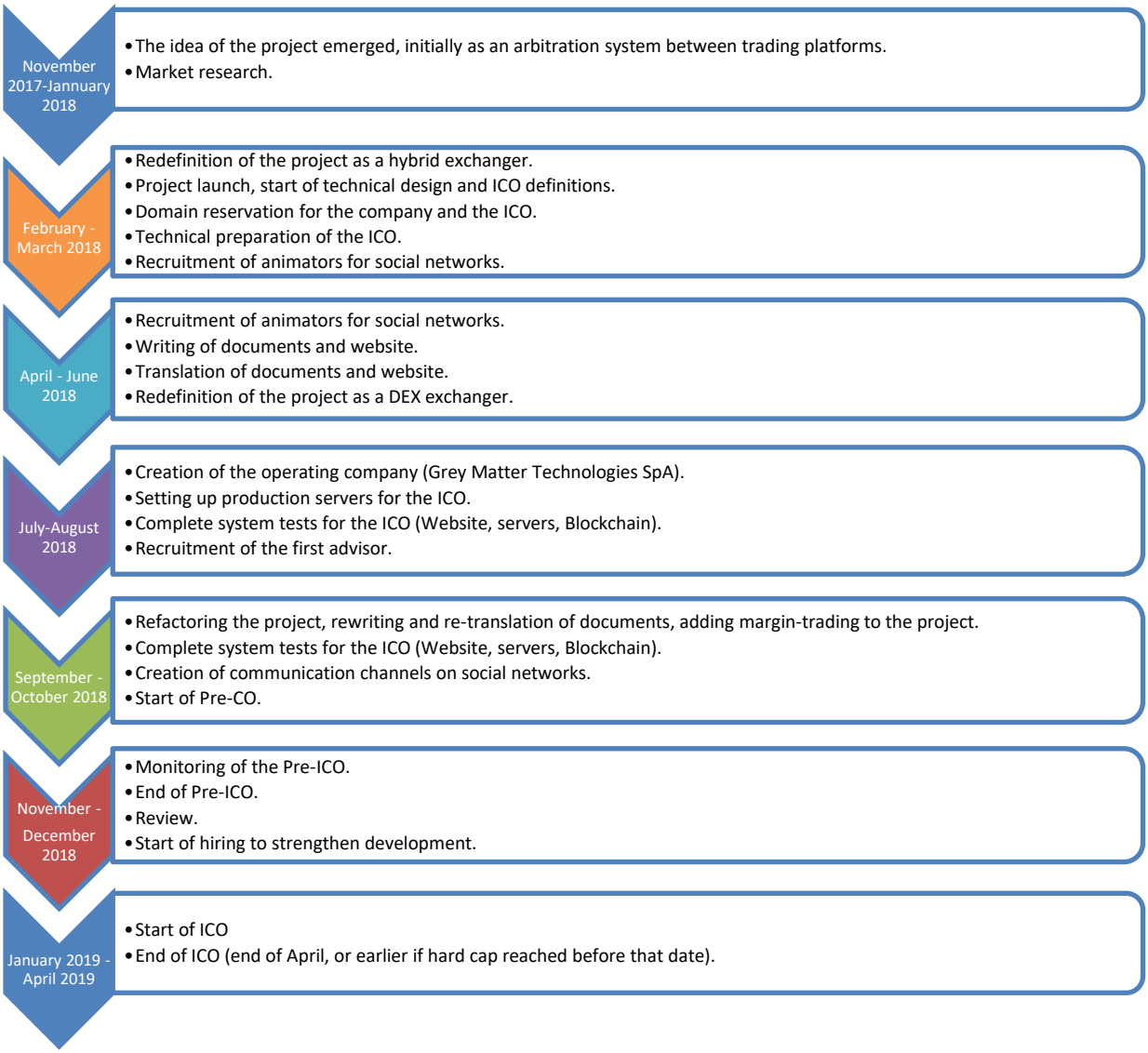
## ROADMAP

This roadmap is the one planned if the ICO Hard Cap is reached. Otherwise, the project is designed as stand-alone modules. The development of each module may be postponed until the revenues generated allow the self-financing of the realization of these functionalities.

On the Roadmap, features that may be postponed are indicated by an asterisk (*).

Improvements to the exchanger, addition of crypto-currencies (nodes gateways) etc. will continue to be made beyond this roadmap.

## ROADMAP ICO



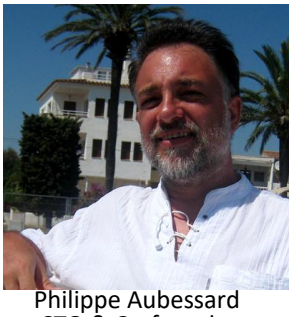
## ROADMAP SECURE SWAP

# TEAM

## FOUNDING MEMBERS

Alain Saffray
CEO & Co-founder

30+ years of experience in software development,
Alain is a very experienced programmer with solid technical knowledge. His previous experience in various computer industries, from management, video games, image processing, automatic trading robot design, has enabled him to cover many difficult technical aspects of software development.
All these experiences make him able to manage any project with confidence and pragmatism.
He is also co-founder of Montmartre SpA, now a holding company of Grey Matter Technologies SpA.
http://www.viadeo.com/p/0021oc3uxefhcfu2



Philippe Aubessard
CTO & Co-founder

35+ years of IT experience, Philippe has a wide range of experience and technical knowledge. Dynamic leader, he has developed a number of disruptive technologies, from R&D to the market. Founder of numerous projects, working with a dozen companies of all sizes and types, he has extensive expertise in IT, R&D, product development, engineering and QC. He is an expert in computer security, particularly in the mobile field. Philippe is also an early investor in crypto-currencies.
http://www.viadeo.com/en/profile/philippe.a

Nadine Miotti
Co-Founder

Over 25 years of experience in business and public relations. Account Executive for Financial Companies and Banks.
A constant look at innovation and at future - a persistence that does not fear adversity, I approach the world of crypto-currencies with enthusiasm!

Alicia Laura Poblete
Co-Founder

As an investor in various projects, particularly in the medical field, I am enthusiastic about participating in this innovative project.
Co-founder of Montmartre SpA, which became the holding company of Grey Matter Technologies SpA.

## TEAM

Victor Chukholskiy
Blockchain Engineer
Smart Contracts Specialist

Expert in blockchain technology and Smart Contracts with Solidity.

His technical expertise enables him to evaluate and tackle complex programming challenges.

Rafael Romero Carmona
Cloud Architect
DevOps Engineer

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

Happy and curious geek on every science you can imagine.

Zhan Wei - 詹玮
Mobile Security Engineer

Anti-hack Expert Lead

Senior Online Developer, Data Analyst at Mobile Game Company

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

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

Marc Rivoal
Software Architect
Engineer

30 years of experience in management information technology, in the retail sector.

Definition of software architectures, process modelling, data modelling, project management, design, ...

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

Kevin Vanstaen
Social Animator
Blockchain enthusiast

Digital content producer since 2013, I inform myself and I participate at my scale in the emancipation of the blockchain.

Henry Morera
Social Animator

Coach in personal development, I am also curious about everything to do with technology.

Interested by crypto-currencies, my participation in this project is an opportunity to have an active role in this field..

Sonia Montella
Social animator

What a chance to participate in this ambitious and necessary project: to offer a reliable and ergonomic platform to finally trade crypto-currencies with confidence and at a lower cost.

I answer all your questions.

See you soon on social networks!

Lulia Galea
Social Animator

My name is Valentina and I'm looking forward to meet you. I'm interested in cyber security; how virtual spaces are created and how we can protect them from cyber attackers.

My curiosity way of being, lead me to accomplish different technical skills, making me a better detective as days go by.

That's why we all gathered here, to create and offer you the safest place for your transactions.

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

## ADVISORS

Renaud Desportes
CEO at DoCaption.
Business Dev. Executive

25+ years of international experience, working in product management, including hardware and software development.

Strong experience at building and maintaining customer relationships: business and marketing strategies development, extension of worldwide reseller networks, pre-sales, customer support and training.

Edouard Enault
Financial Analyst
Aeroshot CEO

Financial market specialist (sell-side analyst) and founder of aerial shooting specialist Aeroshot (aeroshot.fr).

Blockchain enthusiast and crypto investor since 2016.

Richard Shibi
Advisor

Richard Shibi has more than 15 years of experience in the IT industry. He has served as a senior management consultant and a regional account executive for IT projects deployed at global scale in the Telecommunication industry (North America, Europe, Russia, Middle East, China & South Africa)

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

# LEGAL NOTICES

## LEGAL IMPLICATIONS WITH THE SSW TOKEN

We cannot ensure future changes in the price of the SSW token, nor its possible presence in the listings of exchangers, nor the possibility of reselling it. The possession of tokens does not give any right of participation, control or decision regarding *Grey Matter Technologies SpA*. Regardless of the outcome of the ICO, the token is not refundable. The investor or speculator fully assumes the purchase risk.

Due to the community aspect of Secure Swap, and to the fact that exchanges between crypto-currencies are part of a distributed autonomous governance (DAO) system, outside the control of *Grey Matter Technologies SpA*, the Secure Swap token is a Security token, a default classification according to the SEC, used as proof of stake to secure exchanges within the open system. It allows profits to be made and mainly serves as a guarantee for the security of exchanges.

As Secure Swap is an open, distributed, community-based exchange without central governance, this implies anonymity of users, at least as much as the crypto-currencies exchanged allow this anonymity. Therefore, it seems unthinkable to ask for the identity of investors or their proof of residence, in order to verify their participation rights in this ICO.

As a result, **it is up to investors to ensure, depending on their country of residence, that they are allowed to participate in this ICO**, and to avoid it in case of illegality or doubt.

**It should be noted that participation in an ICO is currently totally prohibited in China and South Korea**, regardless of the nature of the token.

**For US citizens**, it is their responsibility to **verify with the SEC the legality of participating in this ICO**. Due to the default Security nature of the SSW token, only experienced investors can participate in this ICO.

**For European citizens**, by participating in this ICO, you declare that **you are not a consumer within the meaning of the European Directive 2011/83/EU of 25 October 2011 relating to consumers' rights**.

**For Russian citizens** and those from all other countries in general, it is their responsibility to **check with local regulatory authorities about the lawfulness of participating in this ICO**.

About the conversion nodes from crypto-currencies to fiat currencies:

This type of node implies a legal unit and compliance with local laws of the place of operation, including **regulations (KYC/AML/CFT/FCA) relating to fraud, money laundering or any criminal activity**.

## THE COMPANY OPERATING THE EXCHANGER

- The exchanger, i.e. the gateway nodes, the arbitration nodes and the conversion nodes to fiat currencies, supported by us, will be operated by *Grey Matter Technologies SpA*:

  www.greymattertechs.com

- *Grey Matter Technologies SpA* is a company under Chilean jurisdiction.

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

  Fojax: 60729 n° 31132 año 2018

- We encourage all volunteers to support the system by operating their own gateway nodes, arbitration nodes, ~~leverage~~ margin-trading nodes, and also to exploit conversions to fiat currencies for their own benefit, obviously at their full responsibility for compliance with local regulations, corresponding to the locations where these systems are operated.

# FAQ

## FAQ SECURE SWAP

Q1 : What is Secure Swap?

R1 : Secure Swap is a community-based decentralized crypto-currency exchanger (DEX). It is developed by *Grey Mater Technologies SpA*, based in Chile, by a French founding team.

Q2 : Which crypto-currencies does it support?

R2 : Potentially all digital currencies can be exchanged. When launched, the service will support the most popular crypto-currencies, the others will be added as they are released.

Q3 : Does Secure Swap support conversions with fiat currencies?

R3 : Yes, this is planned. At its launch, South American currencies will be supported, as well as USD and EUR. The community nature of our platform will allow other companies to establish themselves in order to offer links to the fiat currencies of their country or region.

Q4 : What is the community nature of Secure Swap?

R4 : The project is under open source license. Its architecture is based on a network of P2P nodes. Those who find it interesting can operate these nodes.

Q5 : What is the interest for a community to operate these p2p nodes?

R5 : Those who operate gateway nodes, and therefore support the operation of the service, will receive, in proportion to the SSW tokens they have allocated to this node, their share of the exchange fees paid by the traders. They will therefore be automatically remunerated for this.

Q6 : How to allocate SSW tokens to a node?

R6 : In the configuration of the node, the wallet containing the SSW tokens that are allocated to this node is indicated. This same wallet can only be allocated to one node at a time. The tokens allocated to the node are transferred to a wallet managed by a smart contract, and will be returned when the node stops. They serve as a guarantee for exchanges.

Q7 : How can I get these SSW tokens?

R7 : *Grey Matter Technologies SpA* launches this ICO (Initial Coin Offering) by issuing these SSW tokens. Thereafter, these tokens may be exchanged, in particular on Secure Swap.

Q8 : How is the remuneration calculated?

R8 : Nodes are specialized for each supported blockchain. They connect the p2p network to the blockchains, and are called gateway nodes. For each blockchain there are a number of gateway nodes, each with SSW tokens allocated.

For example, if a gateway node is launched on the EOS blockchain, and a wallet containing 10 SSW tokens is allocated to it, and all the gateway nodes on the EOS blockchain together have 100 SSW tokens allocated, then the node owner receives a 10% (10/100) exchange fee, for all exchanges made with EOS crypto-currency automatically on the previously specified EOS wallet.

Q9 : How will *Grey Matter Technologies SpA* ensure benefits with this system?

R9 : Like NodeOwners, the company will operate p2p nodes by allocating to them the tokens it will have after the ICO (those that will not be sold).

Q10 : And if the company sells all its tokens during the ICO, would it end up without SSW tokens?

R10 : The company will be able to generate profits via the exchange of crypto-currencies into fiat currencies. The profits generated by exchanges are not shared via the token system, but are entirely returned to the operators of such exchanges. The company may also be able to buy back SSW tokens once the service is operational.

Q11 : So *Grey Matter Technologies SpA* reserves the exchange to fiat currencies for itself?

R11 : No, due to its open-source and community nature, Secure Swap allows anyone to use exchange gateways to fiat currencies. However, this requires a legal structure and compliance with the regulations of the country where the trade is carried out. *Grey Matter Technologies SpA* plans to start trading in fiat currencies in Chile, Peru and Argentina.

Q12 : How does Secure Swap plan to attract traders?

R12 : Secure Swap offers a client application, Secure Trade, dedicated to trading based on the network of gateway nodes. This application benefits from our experience in developing professional stock market software. Its ergonomics will be much better than current platforms, and offers a set of innovative tools and trading aids in the world of crypto-currencies.

Q13 : In such a community and open-source system, how can we ensure the security of exchanges?

R13 : All gateway nodes to a crypto-currency respond to a request from client applications participating in an exchange. If the nodes respond differently, it is because there is a hacking attempt or a malfunction. In this case, a system based on a proof of stake, eliminates non-compliant nodes by disconnecting them.

Q14 : How does this system of proof of stake work?

R14 : When nodes give different responses during the validation steps of an exchange, then the reference response is the one that is the majority on all nodes, each node having a voting weight corresponding to the SSW tokens allocated to its operation. Nodes responding differently are disconnected. Thus, to attempt to steal a transaction, it would be necessary to invest a quantity of SSW tokens representing more than half of the tokens allocated to the gateway nodes to this crypto-currency. This represents a higher value than the theft of a transaction. In any case, this robbery has no chance of success since, as soon as an anomaly is detected, the transaction is cancelled. In addition, if the operator of such a node kept the counterparties of the transactions, their values would be debited from the SSW tokens pledged as guarantee on this node for an equivalent amount, converted into the crypto-currency expected by the trader and sent to him. If the hacker put significant resources into it to take control of all the gateway nodes, this operation would ultimately be a loss for the hacker, probably very expensive, given the number of tokens he would have to commit to achieve this and which would be lost for him. The operation would consist for the hacker in buying all the crypto-currencies he diverts at market price, and in assuming all the costs generated by these operations. Traders are continuing to receive the counterparties for their trades as planned.

Q15 : If nodes are hacked and come under malicious control, how can we ensure that this security system remains operational?

R15 : Initially, the gateway nodes will be honest, we know this because we will launch the first nodes ourselves when the service starts. Since Secure Trade is waiting for confirmation of all gateway nodes to a crypto-currency to send assets, if not all gateway nodes provide the same answer, there is a problem. The applications involved in this exchange then cancel the transaction, and inform the entire p2p network. In the end, the hacker pays for the diversion of counterparties, which are therefore always delivered to traders.  And his node is disconnected from the network.

Q16 : What other measures are being taken to fight piracy?

R16 : In addition to the protocols described in the previous answers, and in addition to the fact that the entire Secure Swap project is available to everyone under Open Source license~~in Open Source~~, we launch Bug Bounty campaigns every 3 months with a reward for those who find a vulnerability in the system.