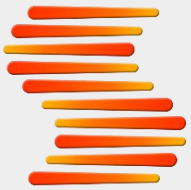


SECURE SWAP WHITEPAPER

Grey Matter Technologies

[Email address]

SECURE SWAP WHITEPAPER

CONTENTS

PRESENTATION OF SECURE SWAP

The summary and strong points are directed to the ones who do not want to read the whole document, or for the ones who want to have a previous idea of the project, before reading it in detail.

SUMMARY

Secure Swap, a new generation of exchanger:

It can function without an operating society support, because of its p2p architecture and the absence of central servers.

It is open source.

Its technology is highly modular, allowing the ones who want to add services (cryptocurrency support, fiat exchange support), turning them into actors.

It allows its users to find in it a source of income, supporting its community functioning.

Its technology inspired by the exchanges of Torrent files protects the system heart from regulations and brutal ban on cryptocurrencies, which can be a risk for the ones who have them, according to their residence, and always presents a possible exit.

It is completely anonymous (if the exchanged cryptocurrency allows it) when cryptocurrencies are exchanged.

Nevertheless, when it's about exchanging cryptocurrencies with fiat money, its allows to fully respect the regulations in use, because of its modular aspect and the clear separation between the systems exchanging fiat money and the cryptocurrencies from the other exchanges.

With that last aspect, the ones who want to can operate, using a legal structure, a professional exchange activity of cryptocurrency to fiat money, in the desired currencies.

Its protocol of operation integrates systems to detect malfunctions, leading to the automatic stop of the exchanges on the cryptocurrencies threatened by an intent of hacking.

Its trading client offers a level of comfort and ergonomics that can be compared with the best trading software on classical markets.

STRONG POINTS

SECURITY

- System secured by concept, with hacking intents detection, alarm and automatic stop of the concerned parts.
- Decentralized system, where the users stay in possession of their cryptocurrencies until they need to make an exchange.
- Being completely decentralized, no trusted third-party, no grasp for regulators to prohibit its use.
- No concentration of cryptocurrency, which is a first-choice target for hackers in the centralized and “decentralized” exchangers, the architecture of which implying the concentration of cryptocurrencies or tokens.
- An open system that allows everyone to control the code, functioning and security.

AVAILABILITY

- Highly redundant system, assuring résistance to breakdown, therefore a high availability of service, including with important charge.

CONTROLLED AND COMMUNITY LED EXCHANGE

- Its distributed and community aspect makes the service independent from the existence of the society that created it and it doesn’t require it to function.

EXTENSIBLE EXCHANGE

- By its open source and modular nature, the users who want can add the cryptocurrency support to the exchanger and also cryptocurrency exchanges to the fiat money of their choice.

AN INCOME FOR THOSE WHO SUPPORT ITS OPERATION

- Those who support the service process by operating parts of the system (link to a specific cryptocurrency, conversion nodes to fiat money), are rewarded with part of the expenses paid by the users on the exchanges.
- It allows to initiate a commercial activity of cryptocurrency to fiat money everywhere where it is legal in the world (conversion nodes to fiat money).

A GLOBAL EXCHANGER

- Beside the fact that the red is accessible anywhere in the world for the cryptocurrencies exchanges, the community additions of the fiat money will progressively make the service international for fiat money as well.

MARKET CONDITION

CENTRALIZED EXCHANGERS

Centralized exchange platforms are frequently hacked, which leads to cryptocurrency stealing. When that happens, it affects a lot of traders present on the platforms, and important amounts are stolen because of the concentration of funds.

In fact, a centralized exchange platform literally owns the cryptocurrencies that it received. The exchanger holds the private keys of traders' wallets. Therefore, the users must trust it, regardless of the risks of hacking and bankruptcy that might result. On the other hand, those exchangers present the advantage of having a centralized order book, therefore a better liquidity and faster orders execution, unlike most of decentralized platforms.

DECENTRALIZED EXCHANGERS

The decentralized exchangers often present a setback ergonomics in comparison with the centralized platforms, and often a reduced liquidity for being decentralized, in exchange for a better security (or at least a security depending entirely of the user), and a lack of trusted third-party, since the users stay in possession of their cryptocurrencies (wallets private keys).

They present also a limited choice in exchangeable cryptocurrencies, since their technologies depend on the interoperability of the exchanged cryptocurrencies, or the availability of the Atomic Swap on those, and so on. Few decentralized platforms allow the exchange of a wide number of different cryptocurrencies, and when they do, a small part of their systems is often not decentralized (centralized tokens used as counterparts to the exchanges, or as guarantee of liquidity for example). Which is a risk comparable to the classical centralized exchangers, although it is not the user who takes the risk but the operator of the exchanger.

Because of the lack of confidence about the security of centralized platforms in comparison to the risks of pirating, many users do not dare to leave their cryptocurrencies on these platforms. They remove them as soon as they finish to trade, and they put them back to trade again, which brings more transactions costs and delays.

Such lack of security also makes useless classical orders such as stop-loss, trigger file tracks, OCO (order cancels order), since many users do not leave their cryptocurrencies on the exchange platforms. The traders do not take the risk to leave their cryptocurrencies on a platform anymore, even with a stop-loss, and prefer to remove them and not taking the risk to have them stolen.

OTHER ASPECTS

The existing exchange platforms are frequently victims of loading problems that could lead to the interruption of services during periods of intense activity, which are often the periods when their users need them most (panic on the markets).

Besides, many existing platforms, centralized or not, present uncomfortable ergonomics of use (although recent exchangers improve it), some sites being real headache, even for an expert trader.

The users learned to deal with these problems, but such situations bother most of them to adopt cryptocurrencies. This remains complicated, risky and difficult to apprehend.

SOLUTIONS BROUGHT BY SECURE SWAP

A DECENTRALIZED, MODULAR, OPEN AND COMMUNITY EXCHANGE PLATFORM

To solve the identified problems, Secure Swap offers the advantages of centralized and decentralized exchanges: good liquidity, **reinforced security "by design"**, no intermediaries to trust with users' cryptocurrencies and ergonomics inspired by the best software of broker trading. Besides, nodes p2p technology guarantees a load capacity and redundancy assuring a reliable and available service.

Secure Swap is also an open system allowing everyone to control the code, functioning and security, and to participate in its operation with bridge nodes toward cryptocurrencies. **The exchange costs are totally redistributed** to those who operate this type of nodes, in proportion to the SSW token they have. Therefore, it is a source of income for all the ones who want and invert in the SSW token.

Secure Swap is a cryptocurrencies exchange ecosystem, articulated around a decentralized service, a client application for trading and optional micro services to take advantage of the new options offered by this network. These micro-services are specialized nodes, such as connection nodes to different blockchains, connection nodes to payment processors to exchange to fiat money, arbitration nodes, and so forth.

The client application and the nodes communicate via Peer to Peer technology (p2p), forming a decentralized service.

The exchanges security and atomicity are covered by smart contracts (one in each blockchain) dedicated to this duty, initially on the blockchain Ethereum. It will be applied to other blockchains supporting smart contracts such as EOS, to guarantee the security/atomicity of exchanges on those. This allows also to increase the number of feasible transactions by second, adding execution capacities on each blockchain. The total of smart contracts on each blockchain forms a distribution of applications DAPP, insuring interoperability between the blockchains, for the exchanges.

Only the client application Secure Swap knows the user's wallets private keys, so it can sign contracts toward the blockchains (offline signature). Which means nobody can sign transactions instead of the client application while trying to steal the traders' assets. That way, the trader remains owner of his cryptocurrencies, unlike when using centralized exchanges platform, on which the trader transmits his stored cryptocurrencies, because these platforms own the private keys, therefore the stored cryptocurrencies.

As soon as the user disconnects himself from the exchanger and leaves the client software, his wallets private keys, locally stored on his computer, are offline (like a ‘cold storage’). His wallets private keys are never transmitted on Internet and never leave the client’s application.

Besides, if the user owns hardware wallets (Ledger, Trezor…), the private keys corresponding to these wallets are never stored on his computer but stay secured on his hardware wallets.

As soon as the user connects the client to the p2p network, he is ready to trade/exchange his cryptocurrencies, without useless costs to transfer before on an exchanger, while enjoying a security comparable to putting away his coins on a private wallet in ‘cold storage’.

The client application allows user-friendliness and ergonomics comparable to the best existing trading software (stock markets, future contracts, Forex...). The client application will offer client ‘advanced’ orders, trigger level orders, such as conditional orders with multiple tracks, OCO orders, as well as trading on graphics with conditional orders on crossing horizontal or down trendlines, on indicators, etc.

Besides, since Secure Swap incorporates the clients’ orders via p2p nodes, that allows to keep the advantages of centralized exchanges: liquidity and fast execution. To reinforce liquidity, an arbitration mechanism (arbitration node) must provide it, in case of internal lack, by using a reserve of cryptocurrencies belonging to the society and order books from the other exchangers via their APIs.

EXCHANGER ARCHITECTURE AND FUNCTIONING

The network architecture will be based on the application core Java Script (common basis p2p), that will be used by different modules of the ecosystem: trading client, p2p nodes of bridges to blockchains, arbitration p2p node insuring the exchanger liquidity, exchanges crypto/fiat nodes, node indicating the state of the network.

The client application sends orders given by the user to the connected nodes, which allows to consolidate them. The nodes spread all the collected orders from node to node every time there is a modification, so that each node has a complete order book. Since the client application is also a node, it receives also all the orders emitted on the p2p network.

Each client application realizes its own orders matching, versus the complete order book, to find counterparts about the orders that the trader emitted.

When a matching (counterpart) is found, the client application informs the p2p nodes which are connected. The bridge nodes to the blockchains involved in the exchange will inform the exchange smart contract of each blockchain which validates a request to send cryptocurrency to each involved client, to receive the funds involved in the exchange. The smart contracts of each blockchain, once the funds are received on the wallet managing the exchange, and after the exchange atomicity is validated by a specific mechanism (*), send those cryptocurrencies to the wallets recipient of the exchange. If all the funds involved in an exchange are not received after a time, the exchange is cancelled, and the funds are returned to their owners, which guarantees the exchange atomicity. Once the exchange is done, the client applications withdraw the orders that have been answered, each client application withdrawing its own orders, which puts the whole book in order.

Except for the network costs corresponding to each blockchain, which are paid by the traders, the exchange smart contracts collect a small percentage on each exchange, which will be redistributed to the owners of SSW tokens that will be needed for the operation of one or more nodes connected to blockchains, in proportion to the owned tokens and the total number of tokens allocated to each blockchain.

Example: a client uses a p2p node connected to the blockchain Ethereum (bridge towards Ethereum), he allocates 100 tokens from the ones he owns for the functioning of the node (via a dedicated wallet, the tokens remaining his property). If on the other hand, other clients use p2p nodes connected to the blockchain Ethereum, and all the nodes have 1000 tokens allocated to that, then our client will receive 10% (100/1000) of the collected costs on all the exchanges in which Ethereum are implicated.

If there are other SSW tokens, and other nodes are functioning and connected to other blockchains, he will also receive the part corresponding to him from the exchange costs on the other blockchains. Such a system of allocation by blockchain allows to encourage the clients to use nodes to connect the exchanger to blockchains where few nodes are in use, which reinforce the redundancy, thus the system availability and security.

(*) See detailed description in the paragraph “Validation system of exchanges atomicity”.

FINANCIAL ASPECT OF THE TOKEN

DATA USED FOR THIS PROJECTION

- Total tokens issued: 100.000.000
- Price of issue: 0.45$ USD
- Percentage of tokens affected to the nodes bridges: 50%

We believe that part of the SSW tokens acquirers will not use bridge nodes toward cryptocurrencies, losing the corresponding part of the exchange costs paid by traders, but will buy them only for speculation reasons on the token price. This projection seems optimistic, the truth could be closer to 30%. The smallest the part of tokens affected to bridge nodes functioning, the highest the output of the tokens for the users.

The following information comes from CoinMarketCap, end of July 2018.

The exchanges volumes correspond to a period of end of cryptocurrency crash. We can expect that later on, the volumes will raise, which will increase the profitability of tokens owning to activate bridge nodes.

Examples of distribution of exchanges between cryptocurrencies in 24h.

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

We have here the 3 cryptocurrencies most exchanged and one cryptocurrency less exchanged.

Volume of exchanges in the platforms during 24h according to their ranking in CoinMarketCap:

Rank 100: 3.000.000 $USD

Rank 75: 10.000.000 $USD

Rank 50: 20.000.000 $USD

PROJECTION OF THE PROFITABILITY OF INVESTMENT IN SSW TOKEN

We consider that the tokens affected to the bridge nodes functioning are proportionate to the volume of exchange of each cryptocurrency. An excessive allocation of tokens on bridge nodes of a cryptocurrency would lower the tokens rentability for this cryptocurrency. On the contrary, a low allocation of tokens for other related cryptocurrencies would increase their rentability. Which means that the ones who use nodes bridges will tend to affect their tokens to the most profitable cryptocurrencies, and those will become less profitable while the others will become more profitable. Therefore, the repartition of tokens relates to the volume of exchanges between cryptocurrencies.

Calculation of tokens profitability:

TTOK: Total of tokens emitted at ICO
FTAP = Percentage of tokens affected to nodes bridges
VE = Volume of exchange, in $USD
FEC = Percentage of exchange of cryptocurrency in relation with the total exchanged
FRTC = Percentage of distribution of tokens for the cryptocurrency bridge nodes
PX = Purchase price of token, in $USD
T = Fees covered by the platform for the exchanges.

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

We see that if FEC = FRTC, we obtain:

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

THEREFORE, THE PROFITABILITY IS THE SAME FOR ALL THE CRYPTOS IF FEC = FRTC, REGARDLESS OF THEIR VOLUME OF EXCHANGE.

If we have a volume of exchange of 3M$ USD per day (exchanger rank 100 on CoinMarketCap)

Annually we will have: ∑ ve = 365*3M = 1.095 M $USD

The exchange cost being of T = 0.15%, on a :

Profitability = ((1.095.000.000 * 0.0015) / (100000000 * 0.5)) / 0.45 = **7.3%** of annual profitability

If we have a volume of exchange of 10M$ USD per day (exchanger rank 75 sur CoinMarketCap)

Profitability = ((10.000.000 * 365 * 0.0015) / (100000000 * 0.5)) / 0.45 = **24.33%** of annual profitability

Il we have a volume of exchange of 20M$USD per day (exchanger rank 50 sur CoinMarketCap)

Profitability = ((20.000.000 * 365 * 0.0015) / (100000000 * 0.5)) / 0.45 = **48.67%** of annual profitability

CONCLUSIONS

Studying the classification of the exchangers on CoinMarketCap, we can verify that the exchangers under the top 100 are exchangers that the users abandon very soon, meaning they have a low volume of exchanges.

We believe that considering its advantages, as soon as the number of exchangeable coins will be sufficient, Secure Swap will easily be ranked among the top 100 exchangers.

Also, as soon as the coins they want to exchange are supported by Secure Swap, the node owners using bridge nodes will not be interested in other exchange platforms. Therefore, it seems realistic to aim at the top 50.

Consequently, as Secure Swap is adopted by users, the SSW tokens productivity could grow from 7% per year to 48 % per year. Aiming at an intermediate situation with a volume of exchange corresponding to the top 75 of CoinMarketCap, we can hope **an annual productivity of 24%** for the investors participating in the ICO. For the ones who would buy SSW tokens later, it will depend on their purchase price. A lower purchase price increases the productivity, a higher one decreases it.

Besides, we must notice that these exchanged volumes apply to a period following long months of crash of the cryptocurrencies last bubble. We can assume that during the next months, the cryptocurrencies market will set off again, which will increase the exchanged volumes, therefore the token profitability.

VALIDATION OF EXCHANGES ATOMICITY

FOR THE EXCHANGES IN THE ETHEREUM ECOSYSTEM (ETH AND TOKENS ERC-20/ERC-720)

The exchange atomicity is assured by a smart contract on the Ethereum blockchain.

Such smart contract can, without external intervention, verify the reception of ETH/tokens and send them back to the recipients.

This type of exchange will be improved with the integration of Plasma/Lighning Network when these second level solutions will be operational and mature. Which will improve significantly the speed of exchanges within the Ethereum ecosystem.

FOR THE EXCHANGES BETWEEN INTEROPERABLE BLOCKCHAINS

For the exchanges between interoperable blockchains (for example between Litecoin and Decred, or Ethereum and Omisego): such interoperability is not effective yet at this time, and when it is, it will use technologies like Plasma or Lightning Network. Meanwhile, Secure Swap considers these blockchains as uninteroperable.

FOR THE EXCHANGES BETWEEN UNINTEROPERABLE BLOCKCHAINS

In this case, our exchanger will treat these cryptocurrencies as interoperable via its p2p network.

CASES IN WHICH THE CRYPTOCURRENCIES INVOLVED IN THE EXCHANGE SUPPORT THE SMART CONTRACTS

All the cryptocurrency bridge nodes verify that the smart contracts (one by blockchain) validate the arrival of coins on the wallets before sending to the recipients, to guarantee the exchange atomicity.

They send on the p2p network the validation of reception of the coins to the other smart contract (counterpart smart contract).

When the two smart contracts involved in an exchange have the validation of reception of the coins, those are sent to the final recipients for the smart contracts to conclude exchange themselves.

To protect themselves from nodes hacking or malicious nodes, the smart contracts only validate the coin reception if all the bridge nodes of the corresponding cryptocurrency indicate that the coins have been received.

In case of disagreement between the bridge nodes (which means hacked nodes /malicious node), the majority answer wins (one bridge node voice = number of SSW tokens associated to this node), all the bridge nodes in disagreement are disconnected and black-listed (ip address on black list, preventing the reconnection of those nodes to the p2p network).

Every time a node is disconnected because the response is incorrect, it sends to the p2p network the information of disconnection for non-compliance to all the clients and all the nodes. Each client receiving the information disactivates the trading on that cryptocurrency and cancels all the orders implying that cryptocurrency, all the nodes of the network memorize the trading status of each cryptocurrency. Consequently, a client who was not connected during the hacking attempt and would connect after would immediately be informed of the trading disactivating on that cryptocurrency. For the trading to start again on that cryptocurrency, the qualified majority (>=60%) of the clients formerly selected for that (volunteer delegates) reactivate the trading on that cryptocurrency.

The result of this protocol is a consensus by proof of stakes. To try to hack the p2p network and steal the coins of an exchange (therefore not to send the counterpart while receiving the coins from another user), it would be necessary to have more than half of the total of the SSW tokens affected to the link nodes of a cryptocurrency.

Which means that to try to steal an exchange, it is necessary to bring into play an important amount of SSW tokens. The effect on the exchanger's fame, in case it worked, would provoke a fall of the SSW token value, implying a loss for the hacker that would be much more important than what he would gain stealing a transaction.

Besides, since there surely were some honest nodes on the network before the hackers took control, those, as they were disconnected, sent a trading deactivation on that cryptocurrency that all the nodes (clients and others) received. Which also leads to the cancellation of the transaction in process and the restitution of the concerned coins to their users by the smart contracts.

With such protocol, it's unlikely for an attempt of taking of control to succeed, and even if it did, there would be nothing to steal (disactivated trading), for an important engagement in SSW tokens, which would make such operation unprofitable and very expensive.

For this security to be efficient, the bridge nodes in a blockchain must be abundant enough and all the bridge nodes together had an amount of allocated SSW tokens much higher than the average value of an exchange, to constitute an acceptable proof of stakes.

Therefore, the client refuses to make an exchange with a cryptocurrency, if the number of active bridges for it is under two, which is the bare minimum.

CASES IN WHICH ONE OF THE CRYPTOCURRENCIES INVOLVED IN THE EXCHANGE (OR BOTH) DO NOT SUPPORT THE SMART CONTRACTS

In this case, the part normally plaid by the cryptocurrency smart contract is covered by a specialized node, by cryptocurrency, under control and with guaranteed security of Gray Matter Technologies.

Since there is no support of smart contract on a cryptocurrency, it is necessary to have a reliable third party. Therefore, this specialized node will assure the reception of the coins from an exchange different part before sending to the recipient, to secure the atomicity of the exchanges without smart contract.

For those exchanges without smart contract, this specific Secure Swap service will not need to take possession of the trader's cryptocurrencies, only during the transaction time, contrary to the centralized exchanges where the trader must transmit his assets for a long period of time.

Also, in this case, there is no cryptocurrency central stock, just a temporary counterparts stockage, the time to validate the exchange atomicity. Therefore, there is not much to gain for a hacker.

INDICATION OF THE EXCHANGER STATUS

INDICATIONS COMING FROM THE CLIENT

The client will indicate with a color code the bridge nodes availability for each cryptocurrency:

- Black: attempt of hacking detected on that cryptocurrency bridge nodes, trading disactivated for that cryptocurrency.
- Red: no bridge available for that cryptocurrency => no possible exchanges.
- Orange-Red: only one bridge available for that cryptocurrency => exchanges prohibited.
- Yellow: two bridges available for that cryptocurrency => exchange ok, but resistance to hacking not optimal.
- Green: minimum three bridges available for that cryptocurrency => exchange ok, optimal resistance to hacking.

INDICATION COMING FROM THE STATISTICAL NODE

A statistical node will analyze permanently the network in order to produce information for the node owners and the traders. It will allow, for example:

- To give a chart of advanced statistics on the nodes,
- To evaluate the expected remuneration according to the SSW tokens allocated to a node bridge,
- To verify volumes of exchanges on a period by cryptocurrency,
- etc.

EXCHANGER PERFORMANCE

At this time, the blockchain Ethereum is limited to about 10/15 transactions per second. Our smart contract managing the exchanges on the blockchain Ethereum will also suffer these limitations.

Nevertheless, developments are in process to greatly increase the number of transactions per second that the blockchain Ethereum will be able to do. The increase we are talking about is several thousand or even millions per second, with technologies such as Plasma, the sharding, the lightning network.

Although the first layer improvements, such as sharding, will increase the number of exchanges/second that can be performed by our smart contract, it shouldn't be the same for the second layer improvements such as Plasma/Lightning network (except for the consequent charge diminution on the first layer operations).

It is planned to have a smart contract managing the exchanges on each blockchain supporting smart contracts, like EOS and others, to combine the execution capacities from several blockchains (beside insuring the exchanges atomicity via the smart contracts of each blockchain). That way, the exchanger will not be linked to an only blockchain, and its capacity to manage exchanges is not limited to the execution capacities of the smart contracts of a blockchain, and a blockchain doesn't limit the exchange capacities on other faster ones.

We prefer the option to use exchanges smart contracts on several blockchains, rather than developing our own cryptocurrency with an execution capacity of sufficient smart contract. Better to build on existing and/or developing solutions, rather than to reinvent the wheel here.

HOW TO OVERCOME THE LACK OF INITIAL LIQUIDITY?

When launched, the exchangers obviously have liquidity problems: their order books are empty, which is not encouraging for the first traders. Liquidity problems might also exist on cryptocurrencies with small volume of exchange.

An arbitration service, relying both on order books and on other sites of exchanges, on the internal Secure Swap order book, and on the reserve funds in cryptocurrencies specific to our platform, will be able to guarantee a replacement liquidity.

This arbitration service will work as a client (i.e. it will emit orders in our order book) using cryptocurrencies belonging to the society. That service will be constituted of a p2p node specialized in this task. Like all the nodes of the network, it will receive the updates from the order book. Being aware of our order book, it will be able to identify the missing counterparts and complete them with transactions with other exchangers.

Part of the society available operating funds will be mobilized through a repartition in several cryptocurrencies used by arbitration mechanisms.

For example, if our order book contains an exchange order of 1 BTC against 12 ETH, but no exchange order of ETH against BTC at the solicited price or quantity, and on an external exchange platform that we use as replacement liquidity, such an order exists, then we will use the society ETH reserved for the arbitration service to do the exchange and buy back the ETH spent on our exchange platform against BTC owned on another exchanger's platform. In the end, we consider that the ETH that we had and used for the exchange to guarantee the liquidity of that transaction end up with an external exchanger, and the BTC that we had with an external exchanger end up on our internal wallets.

To rebalance our various external (on other exchangers) and internal (local to our exchanger) wallets, we will rebalance the amounts of held coins once a day (to limit the costs), to keep the diversity of cryptocurrencies in reserve. If necessary, a rebalance can be started during the day by the arbitration service in case of lack of liquidities in some cryptocurrencies, in order to keep functioning.

Such arbitration will act only in case of lack of liquidity on our order book (therefore orders without counterparts), and only if the operation is not a loss for our exchanger (minimum neutral). It can also generate profits, even if it's not its first destination.

AN EXCHANGER UNDER OPEN SOURCE LICENCE

Most of the exchanger nodes types are distributed in Open source.

This means that besides the client application used by all the traders, everybody will have a chance to support the exchanger functioning by using nodes connected to blockchains.

The node owners doing that and owning SSW tokens emitted during the ICO, will collect their part of costs, deducted during the exchanges at the prorate of the tokens allocated to a node bridge to a blockchain, in relation with the total of SSW tokens allocated to the bridge nodes to the same functioning blockchain.

The society Grey Matter Technologies will work the same way and will collect its part of the exchange costs at the prorate of the SSW tokens it will own at the end of the ICO and that it will keep for each node bridge to a functioning blockchain.

We will also provide in Open Source a skeleton type node planed for the exchange to fiat money, with interfaces to connect to the bank payments processors. Since this activity is highly controlled and needs at the same time to be adapted to each case (local regulations and interfaces to the payments regulators used) and to start a legal activity to be operated (via a society), the skeleton node we will provide in Open Source will be adapted to each case.

Grey Matter Technologies will also operate this type of nodes in regions of South America. We plan to operate nodes for conversion to fiat money for the following currencies: Chilean peso, Argentinian peso, Peruvian sol and maybe others.

So, progressively, this exchanger will convert to a wide number of fiat currencies and world regions

The arbitration node will not be published in Open Source because we reserve the right to use it. Of course, we can’t prevent the ones who want to develop their own arbitrating solutions. In any case, this type of service needs a minimum of available funds in cryptocurrencies of about 100k USD, or to be more realistic, of about a million of USD, to function with several exchangers.

BOUNTY BUG PROGRAM

Part of the funds collected during the ICO will be used to finance Bug Bounty campaigns. Awards will be given to those who will participate in these programs and reveal new bugs or security failures to our teams.

A campaign will start in each stage of the development phase, to make sure that the first version of the platform put in operation will be well analyzed.

Then, quarterly campaigns will be planned to follow the continuity of the developments.

THE ICO, THETOKEN ERC-20 SECURE SWAP (SSW)

WHY AN ICO AND WHY CREATING A TOKEN ERC-20 ?

WE NEED FINANCING FOR THIS POJECT

To finance additional employees hiring and to cover the salaries of the active team. This is the main expense.

We must also finance publicity a little before the platform launch, so that it is known.

We also need a working capital in cryptocurrencies, for the arbitration system.

And finally, we must finance the Bounty Bug campaigns.

All the unsold tokens during the ICO will stay property of the society, to collect the corresponding part of the exchange costs. So, the more the ICO succeeds, the more the investors involved in the exchanger functioning will receive parts if the incomes generated by the exchanges, since the society will have few SSW tokens.

On the contrary, the less the ICO is suscribed, the more the society will owe tokens and will receive an important part of the generated incomes. That assures us a repartition of income that seems correct, considering what the society will have raised during the ICO, and it will allow us to reward our supportive investors.

ICO DATA

Token name: Secure Swap

Ticket SSW

Quantity created: 100 million of tokens

Token initial price: 0,45$ USD

Reserved to the team: 10%

Reserved to the advisors: 3%

Reserved to the social managers/ICO campaign team leaders: 3%

Reserved to the partners: 4%

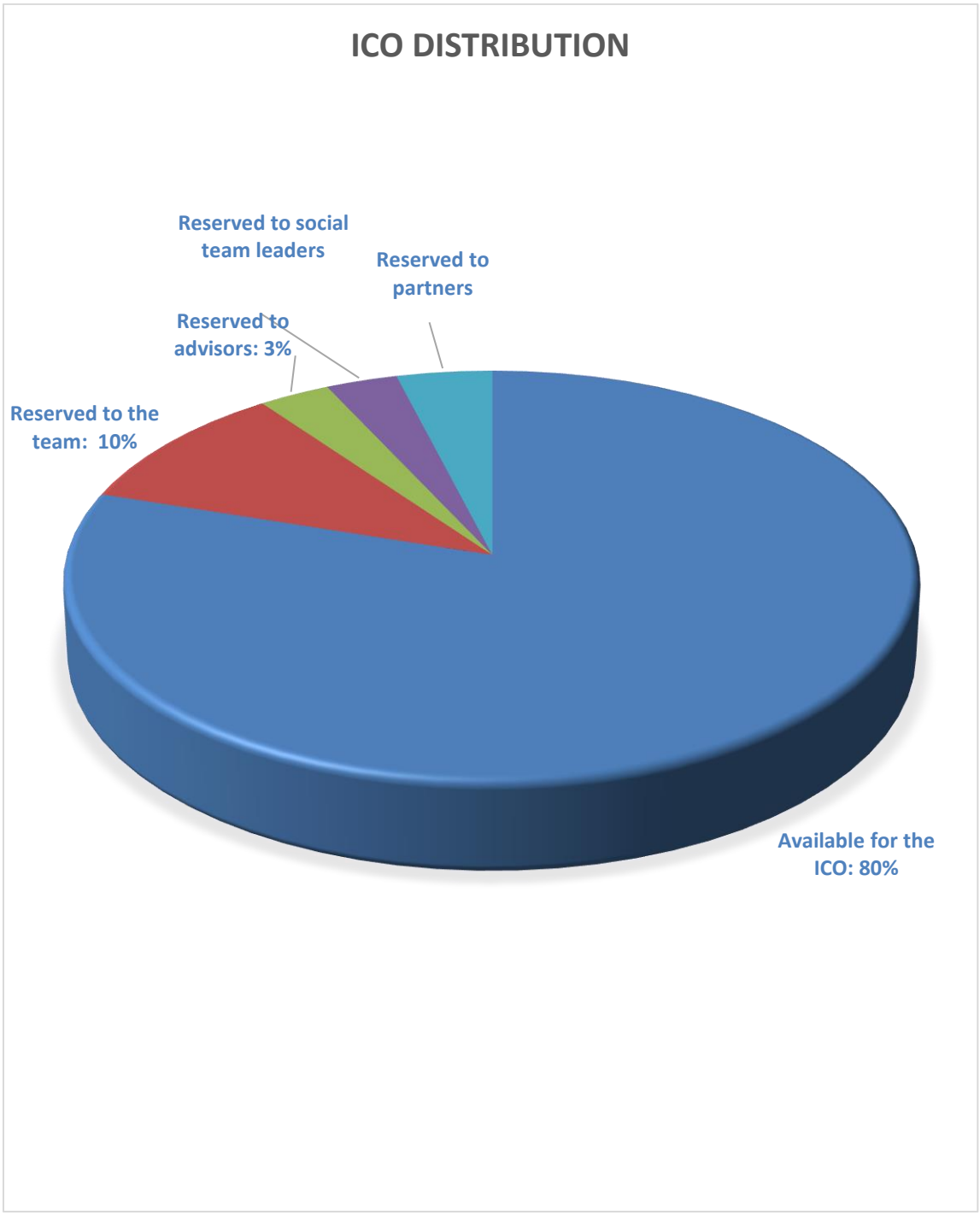
Available for the ICO: 80%

Soft Cap: 10 million of tokens

Hard Cap: 80 million of tokens

All the unsold tokens remain to the society

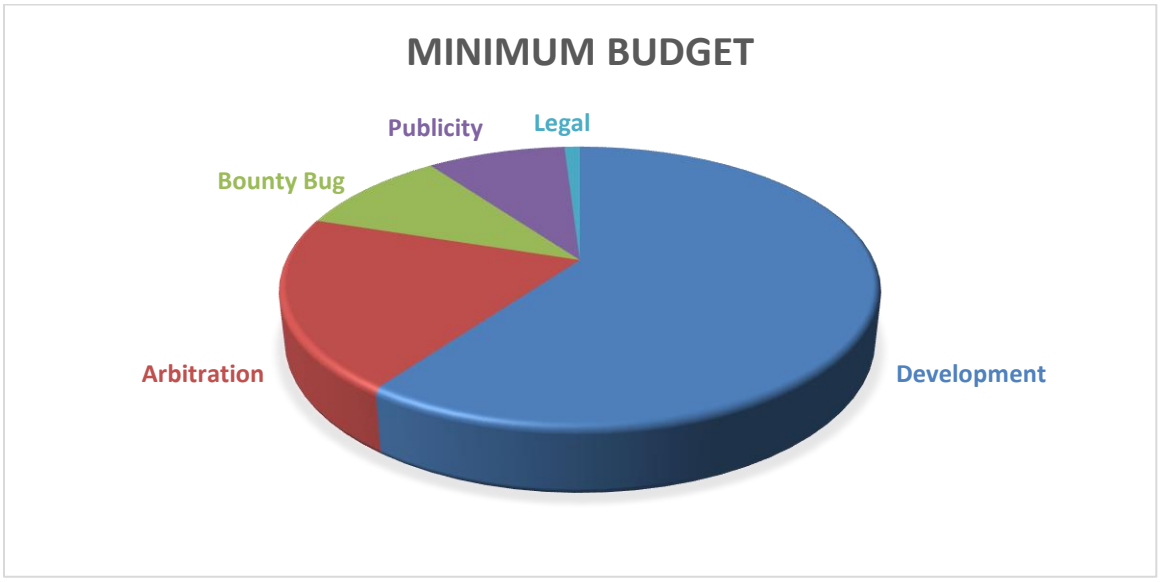
ICO operated by Grey Matter Technologies SA (Chilean society)



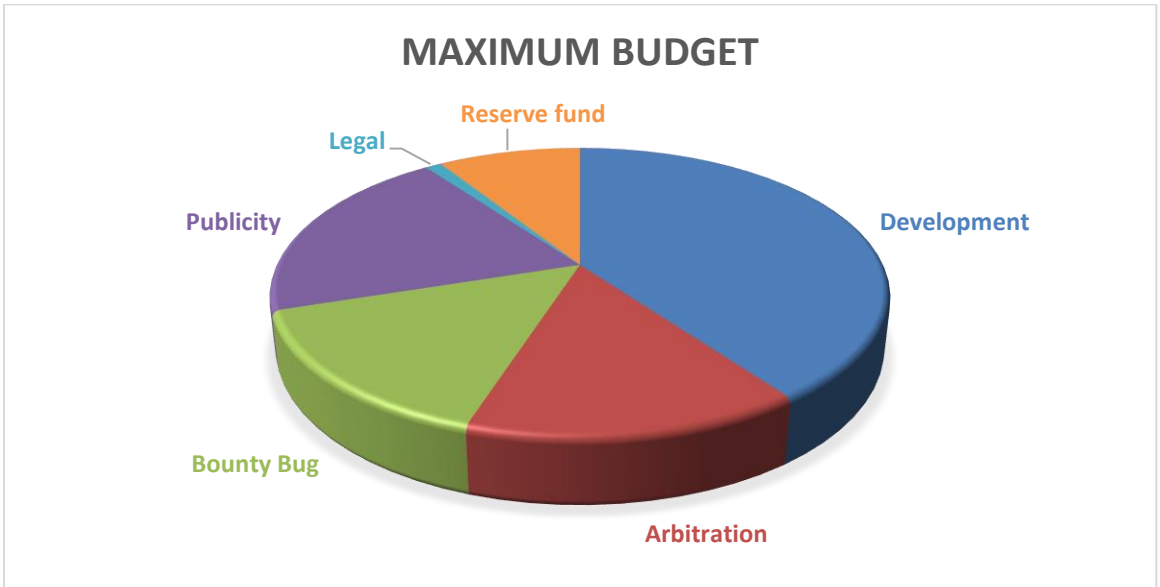
FUNDS ASSIGNATION

We are going to indicate here the funds assignation in two extreme cases: Soft Cap reached, and Hard Cap reached.

SOFT CAP REACHED



HARD CAP REACHED



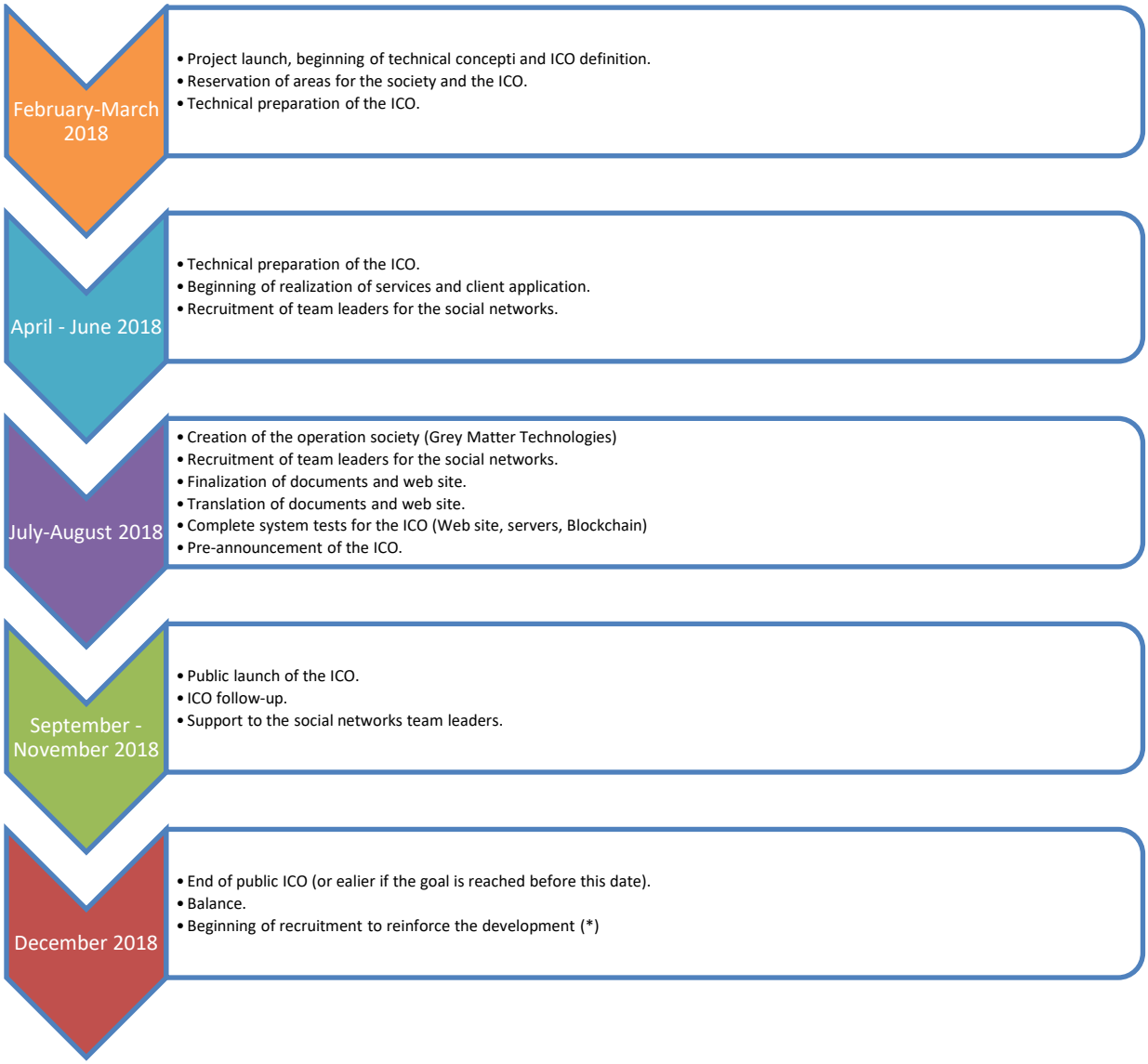
ROADMAP

This is the roadmap planned if the ICO Hard Cap is reached. Otherwise, the project is designed as drawer modules. The development of each module would be postponed until the income allows these features to finance themselves.

On the Roadmap, the features that could be postponed are marked with an asterisk (*).

Exchanger improvements, cryptocurrencies additions (bridge nodes), etc. will be made beyond this roadmap.

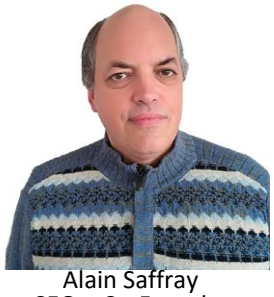
ICO ROADMAP



SECURE SWAP ROADMAP

TEAM

MEMBERS



Alain Saffray
CEO – Co-Founder
Developer engineer

Philippe Aubessard
CTO – Co-founder
Developer engineer

Alicia Laura Poblete
Co-founder
Financial Director

Nadine Miotti
Co-founder
Marketing Director

Renaud Desportes
Business development
Executive

Rafael Romero Carmona
DevOps Engineer

Pierre Pretti
Security Infrastructure
Engineer

Aliaksandr Kharlamou
Blockchain Developer

Victor Chukholskiy
Blockchain Engineer
Smart Contracts Specialist

Marc Rivoal
30 expérience
Definition of software architectures, process modelling, data modelling, project management, design

Zhan Wei - 詹玮
Social Animator

Kevin Vanstaen
Social Animator
Blockchain enthusiast

Lulia Galea
Social Animator

Henry Morera
Social Animator

CONSULTANTS

Benoît Renard
Legal adviser

LEGAL ASPECTS

LEGAL IMPLICATIONS WITH THE SSW TOKENS

We cannot guarantee the future evolutions of the SSW token price, nor its possible presence in the exchangers listings and the possibility to resell it. Owning tokens doesn't give any right of participation, control or decision about the society Grey Matter Technologies. Whatever the ICO issue is, the token is not refundable. The investor or the speculator fully assumes the purchase risk.

Because of the community aspect of Secure Swap, and because the exchanges between cryptocurrencies belong to a distributed system that Grey Matter Technologies does not control, the Secure Swap token is a utilitarian token, serving as proof of stakes to secure the exchanges in the open system. It allows to make profit, like Ethereum with the mining, but in system distribute without society governance, Grey Matter Technologies bringing only technical solutions.

Since Secure Swap is a distributed and community open exchanger, that means the users are anonymous, at least while the exchanged cryptocurrencies allow it, therefore it seems unthinkable to ask the investors' identities and proof of residence to check their right to participate in this ICO.

Then, **the investors should verify, according to their country of residence, if it is legal to participate to this ICO**, and to abstain in case of illegality or doubt.

Please note that the participation in an ICO is currently totally prohibited in China and South Korea, regardless of the token nature.

For the American nationals, they must **check with the SEC if the participation in this ICO is legal**.

For the European nationals, by participating in this ICO, you declare that **you are not a consumer in the meaning of the 2011/83/UE European Directive of October 25, 2011, on the consumers' rights**.

For the Russian nationals, they must **check with the authorities if the participation in this ICO is legal**.

Regarding the nodes to convert cryptocurrencies to fiat money:

This type of node implies a legal structure and conformity to the operation place local laws, in particular **the regulations (KYC/AML/CFT/FCA) about fraud, money laundering or any criminal activity**.

THE COMPANY OPERATING THE EXCHANGER

- The exchanger, meaning the bridge nodes, the arbitration node and the conversion nodes to fiat money, which we support, will be managed by the society Grey Matter Technologies: ww.greymattertechs.com
- The society Grey Matter Technologies is a Chilean jurisdiction society. (https://www.conservador.cl/portal/indice_comercio)
- We encourage any volunteer to support the system managing his/her own bridge nodes, and to operate the conversions to fiat money on his/her own, being of course responsible to observe local regulations, according to these systems place of exploitation.

FAQ

FAQ SECURE SWAP

Q1: What is Secure Swap?

A1: Secure Swap is a decentralized cryptocurrency exchanger (DEX), with community aspect. It is developed by the society Grey Mater Technologies, based in Chile, with a French founding team.

Q2: What cryptocurrencies does it function with?

A2: Potentially all the digital currencies can be exchanged. When it starts, the system will work with the most popular cryptocurrencies, the others will be added little by little.

Q3: Does Secure Swap accept the conversions with fiat currencies?

A3: Yes, this is planned. When it starts, South American currencies will be accepted. The community aspect of our platform will allow other societies to offer links to the fiat currencies of their country or region.

Q4: What is Secure Swap community aspect?

A4: The project is under open source license. Its architecture relies on a p2p node type network. The ones who are interested can work with these nodes.

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

A5: Those who will use p2p nodes, therefore the service, will receive, in proportion to the SSW tokens that they will attribute to it, their part of the exchange costs paid by the traders. Therefore, they will be automatically remunerated for that.

Q6: How SSW tokens are attributed to a node?

A6: In the node configuration is indicated the wallet containing the SSW tokens attributed to this node. That same wallet can be attributed only to one node at a time. Only the wallet is indicated to the node, to verify the quantity of token contained, the tokens stay with the same owner.

Q7: How can we get these SSW tokens?

A7: The society Grey Matter Technologies send out this ICO (Initial Coin Offering) issuing these SSW tokens. Later, the tokens can be exchanged, particularly on Secure Swap.

Q8: How is the payment calculated?

A8: The nodes are specialized for each supported blockchain. They ensure the connection of the p2p network to the blockchains and are called “bridge node”. For each blockchain, there is a certain amount of bridge nodes, each one with SSW tokens attributed.

For example, if a bridge node is sent out on the blockchain EOS, and a wallet with 10 SSW tokens is associated to it, and if all the bridge nodes on the blockchain EOS have together 100 SSW tokens associated, then the owner of the node receives 10% (10/100) of the exchange costs, for all the exchanges done with the EOS cryptocurrency, automatically, on a formerly indicated EOS wallet.

Q9: How will Grey Matter Technologies guarantee its benefits with this system?

A9: As node owners, the society will put in function p2p nodes associated with the tokens it will own at the end of the ICO (the unsold ones).

Q10: And if the society sells all its tokens during the ICO, would it be running out of SSW tokens?

A10: The society could get benefits via the cryptocurrencies exchanges to fiat money, which are not shared via the tokens system, but come back entirely to the operators of such exchanges. It could also buy more SSW tokens once the service becomes operational.

Q11: Does that mean that Grey Matter Technologies keeps for itself the fiat money?

A11: No, because of its open-source and community aspect, Secure Swap allows anyone to use exchange bridges to fiat money. Yet, a legal structure is necessary, and it must observe the rules of the place where these exchanges are performed. The society Grey Matter Technologies plans to start doing exchanges to fiat money in Chile, Peru and Argentina.

Q12: How does Secure Swap plan to attract traders?

A12: Secure Swap offers a client application dedicated to trading and relies on the bridge nodes network. Such application takes advantage of our experience in broker software. Its ergonomics will be much better that the current platforms and offers a system of tools and support for the trading innovators.

Q13: In such a community and open-source system, how do you guarantee the exchanges security?

A13: All the bridge nodes to a cryptocurrency responds to the request from the client applications that participate in an exchange. If the nodes respond differently, that means there is a hacking attempt. In this case, a system based on a proof of stakes eliminates the non-compliant nodes by disconnecting and blacklisting them.

Q14: How does the proof of stakes work?

A14: When the nodes give different answers during an exchange validation steps, then the standard answer becomes majority on all the nodes, each node having a vote weigh corresponding to the SSW tokens associated to its function. The nodes that answer differently are disconnected and blacklisted. So, to steal a transaction, it would be necessary to invest a quantity of SSW tokens representing more than half the tokens assigned to the bridge nodes to that cryptocurrency. Which means a value superior to stealing a transaction, a hacking that will not be done since as soon as the problem is detected the transaction will be cancelled. If the hacker invested a sufficient amount to control all the bridge nodes, the exchanger would lose his reputation and the consequence would be a quick drop of the SSW tokens value; the operation would be a loss for the hacker, the number of tokens involved would make it very expensive. Besides, as soon as a problem is detected, the exchanges with that cryptocurrency are interrupted, and the hacker has no transaction to steal.

Q15: If the nodes are hacked and pass under control of the hacker, how can you guarantee that the security system keeps functioning?

A15: Initially, the bridge nodes will be honest, we know it because we ourselves will send the first nodes at the beginning of the service. Since the client application waits for the confirmation of all the bridge nodes to a cryptocurrency to send the coins, if all the bridge nodes do not give the same answer, that means there is a problem. The clients involved in that exchange cancel the transaction and inform all the p2p network that the exchanges on the cryptocurrency are disactivated, which will cancel all the waiting orders from all the clients connected for that cryptocurrency. There is no more exchanges, the hacker has no transaction to steal.

Q16: How do the exchanges start again a cryptocurrency, after been disactivated because of an anomaly?

A16: It needs a unanimous vote of a qualified majority (60%) of the representatives connected for that cryptocurrency, formerly selected, for the exchanges to start again. Those representatives are responsible to make sure that the nodes being active of the cryptocurrency comply before authorizing again the exchanges on that cryptocurrency.

Q17: How can the representatives make sure that the bridge nodes are honest before voting?

A17: By connecting themselves a node bridge or by verifying that their nodes are still connected. With only one reliable node connected, the problem will be detected if the nodes respond differently again. And again, the exchanges on that cryptocurrency would be suspended and cancelled.

If the trading restarts without incident, that means the exchanges are reliable and that the malicious nodes were cleaned. If malicious nodes are sleeping and function correctly while waiting to get into action, when they do so, they will be detected because of their different responses. Therefore, any intent of node corruption is detected and stealing a transaction is impossible.

Q18: How are the representatives designated?

A18: They are volunteers and qualify only if they have 100 times the amount of an average exchange, in equivalent value of SSW tokens. The volunteer sends the request through its node interface, and if qualified, all the nodes of the network memorize its status of “super node bridge”. The “super node bridge” is gratified with a 50% bonus on its remuneration, compared to what it would normally be considering the tokens allocated.

Q19: How can you prevent dishonest people to permanently connect defective nodes to block the service?

A19: The deviant nodes being blacklisted, beside disconnected, these dishonest people will quickly be running out of IP addresses to connect those nodes. Besides, such an IT sabotage action being illegal, its repetition will increase the chance to identify their authors, and Grey Matter Technologies with pursue these people to demand compensation.

Q20: What measures are taken to fight against the hackers?

A20: Beside the protocols described previously, and beside the fact that the whole Secure Swap project is available to everyone in Open source, we will have Bug Bounty campaigns every 3 months with awards for the ones who would find a breach in the system.