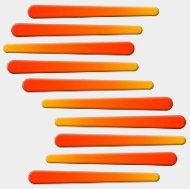


SECURE SWAP 白皮书

Grey Matter 科技

SECURE SWAP 白皮书

目录

SECURE SWAP 介绍

概要和优点针对那些不想阅读整篇文档的人，或者是想要在详细阅读文档前对项目有初步了解的人。

概要

Secure Swap，新一代交易所：

由于它的 P2P 架构和无中央服务器，它可以在无社会运营支持的情况下运行。

它是开源的。

其技术高度模块化，允许想要增加服务（加密货币支持，法定交易支持）的人员变成参与者。

它允许其节点所有者在其中发现收入来源、支持其社区功能。

其技术受 P2P 网络（作为 Torrent 文件）的启发，可以保护系统中心不受法规和加密货币的残酷禁令的影响，这些对拥有加密货币的人来说构成风险（根据其居住地），且总有可能使其退出。

交易不同的加密货币时是完全匿名的（如果交易的加密货币允许）。

然而，当涉及到使用法定货币兑换加密货币时，它允许完全遵守在用法规，这是由于它的模块化特性，以及与从其他交易所用加密货币兑换法定货币的系统间的明确分离。

这种能力允许商业人员创建专业的活动来为他们选定的法定货币兑换加密货币。当然他们需要有一个法律架构。

其操作协议集成了故障检测系统，可以自动终止被黑客的任意攻击威胁的加密货币交易。

它的交易客户端应用兼顾舒适性和人体工学，可与传统股票市场上的最佳交易软件相媲美。

优势

安全性

- 系统设计安全，具有入侵检测、报警及相关部件自动停止功能。
- 真正的分散式系统，在用户需要进行兑换前，加密货币仍然属于用户。
- 完全去中心化，没有可信赖的第三方，没有禁止其使用的监管机构的控制。
- 不集中加密货币，这是黑客在中心化交易所和传统的“去中心化”交易所的首选目标，它们的架构意味着加密货币或代币的集中。
- 一个开放的系统，允许每个人控制代码、功能和安全性。

可用性

- 高度冗余的系统，确保防止崩溃，即便是重要荷载下也可提供高可用性服务。

社区控制和实施的交易

- 它的分布式和社区方面使得服务独立于创建它的公司的存在，不依赖其即可运行。

可扩展的交易

- 凭借其开源和模块化特性，用户可以为交易所增加对新的加密货币的支持，还可以将加密货币兑换成他们所选的法定货币。

支持其运营的人的收入来源

- 通过系统的运营部分（到特定加密货币的网关，到法定货币的转换节点）来支持服务（节点所有者）的人，会获得交易者在 Secure Swap 交易所中支付的部分费用。
- 它允许在世界上任何合法的地方（到法定货币的转换节点）开展将加密货币兑换成法定货币的商业活动。

全球性交易所

- 除了网络在世界上任何地方都可以访问以进行加密货币交易的事实外，社区支持的新法定货币也将逐渐使法定货币的服务国际化。

市场行情

中心化交易所

中心化交易平台经常遭到黑客攻击，导致加密货币被盗。这种情况发生时，由于这种平台集中了交易者的资金，大量资金被窃取，影响平台当前的众多交易者。

事实上，一个中心化的交易平台实际上拥有发送给它的加密货币。交易所持有交易者钱包的私钥。因此，无论可能导致的攻击或者破产风险如何，用户都必须要信任它。另一方面，与大多数去中心化平台不同，这些交易所拥有集中订单记录的优势，因此具有更好的流动性和更快的订单处理速度。

与黑客攻击的风险相比，对中心化平台的安全性信心的缺乏，导致许多交易者不敢把他们的加密货币留在这些平台上。一旦交易完成，他们会立刻转移加密货币，交易时再重新放回，这导致交易成本和延迟的增加。

由于许多用户不会把他们的加密货币留在交易平台上，这种安全性的缺乏也会产生无用的经典订单，例如止损、条件订单、OCO（选择性委托单）。即使在止损的情况下，这些交易者也不再冒险将加密货币留在平台上，他们宁愿将其转移而不是冒其被盗的风险。

去中心化交易所

与中心化平台相比，去中心化交易平台通常呈现出失败的人体工程学，并且经常会降低分散的流动性，以换取更高的安全性（或者至少是完全取决于用户的安全性），以及缺乏可信赖的第三方，因为用户持有其加密货币（钱包私钥）。

他们还在可兑换的加密货币中提供了有限的选择，因为他们的技术依赖于兑换的加密货币的互操作性，或者这些加密货币的原子交换的可用性等等。很少有去中心化平台允许兑换大量不同的加密货币，当他们这样做时，他们的系统中通常有一部分并非是去中心化的（例如，集中式代币用作兑换的对等物，或作为流动性的保证）。这是可与传统的中心化交易所相比拟的风险，尽管冒险的是交易所的操作员而非交易者。

其他方面

现有的交易平台经常成为过载问题的受害者，这些问题会导致业务紧张时期的服务中断，此时通常是用户最需要他们的时候（市场恐慌）。

另外，许多现有的平台，无论是否中心化，都在使用中表现出令人不舒服的人体工程学（尽管交易所最近改进了它）。有些站点确实令人头痛，即使对专业交易者来说也是如此。

用户学会了处理这些问题，但是这种情形困扰了他们中的大多数人去使用加密货币。这仍然是复杂、有风险且难以理解的。

SECURE SWAP 带来的解决方案

一个去中心化、模块化、开放和社区交易的平台

为解决已发现的问题，Secure Swap 提供了中心化和去中心化的交易的优势：良好的流动性，“设计”增强的安全性，没有可信赖的中间人拥有交易者的加密货币以及受最佳交易软件启发的人体工程学。此外，P2P 节点技术保证了更好的可伸缩性和冗余性，确保了可靠和可用的服务。

Secure Swap 也是一个开放的系统，允许每个人控制代码、功能和安全性并通过支持面向加密货币的网关节点参与其操作。根据拥有的 SSW 代币的比例，**交易成本完全重新分配**给操作这类节点的人。因此，对于所有想要投资 SSW 代币的人来说，这是一个重要的收入来源。

Secure Swap 是一个加密货币交易生态系统，围绕分散式服务，它是用于交易的客户端应用和可选的微服务，以利用这个新网络提供的新选项。这些微服务是专用节点，例如到不同区块链的连接节点，到支付处理器的连接节点（以交换到法定货币），仲裁节点等等。

客户端应用和节点通过点对点（P2P）技术交互，形成了去中心化的服务。

交易安全性和原子性由智能合约（每区块链一个）覆盖。智能合约专司此职，最初是用在以太坊（Ethereum）区块链上。它将被用到其他支持智能合约的区块链上，如 EOS，以保证其交易中的安全性、原子性。这样就允许按秒来增加可行事务的数量，在每个区块链上增强执行能力。每个区块链上的全部智能合约形成了去中心化应用（DApp）的分布，确保了区块链之间交易的互操作性。

只有 Secure Swap 客户端应用知道用户的钱包私钥。因此它可以签订对区块链的合约（离线签名）。这就意味着试图窃取交易者的资产时，没人可以签署交易而不是客户端应用签署。这样，交易者仍然拥有自己的加密货币，而不像使用中心化交易平台时交易者在其上传输存储的加密货币。因为这些平台拥有私钥，也就是拥有了存储在其上的加密货币。

一旦用户从交易所断开他自己的连接并且离开了客户端软件，他的钱包私钥-存储在他的计算机本地-就离线了（像是“冷储存”）。他的钱包私钥永远不会在互联网上传输，也从未离开过客户端应用。

另外，如果交易者拥有硬件钱包（Ledger, Trezor…），与他的钱包相对应的私钥永远不会存储在他的计算机上而是安全地保留在他的硬件钱包上。

一旦用户将客户端连接到 P2P 网络，他就可以交易/兑换他的加密货币，而不需要在交易所进行之前的不必要成本的传输，这样的安全性可以比拟将他的 coins 存入私有钱包“冷储存”。

客户端应用兼具用户友好性和人体工程学，可与现有的最佳交易软件（股票市场，未来合约，外汇…）相媲美。客户端应用将为客户提供“高级”订单，触发级别订单，例如多轨条件订单，OCO 订单，以及跨水平或趋势线、指标等条件订单的图形交易。

此外，由于 Secure Swap 通过 P2P 节点整合了客户订单，因此可以保留中心化交易所的优势：流动性和快速执行。为了加强流动性，仲裁机制（仲裁节点）通过使用属于公司的加密货币储备和利用从其他交易所 API 接口获取的订单簿，负责确保流动性。

交易所架构和功能

该网络架构基于 JavaScript 应用内核（通用基础 P2P），将被用于生态系统中的不同模块：交易客户端、区块链网关的 P2P 节点、确保交易所流动性的仲裁 P2P 节点，加密货币/法定货币交易节点、以及指示网络状态的节点。

客户端应用将用户给出的订单发送到连接的节点，这些节点允许合并订单。每次修改时，节点将所有收集到的订单从一个节点扩散到另一个节点，这意味着每个节点都有完整的订单簿。由于客户端应用也是一个节点，它还接收 P2P 网络上发出的所有的订单。

每个客户端应用实现自己的订单匹配，而不是完整的订单簿，以便查找交易者发出的订单的对应方。

当找到匹配（对应）时，客户端应用通知连接的 P2P 节点。交易中涉及到的区块链的网关节点将通知每个区块链的交易智能合约，该合约验证向每个相关客户端发送加密货币到并接收交易中涉及的资金的请求。每个涉及的区块链的智能合约，一旦在管理交易的钱包上接收到资金，并通过特定机制(*)验证了交易原子性之后，就会将这些加密货币发送给交易的钱包接收者。如果交易中涉及的所有资金在一段时间后没有收到，该交易就会取消，资金会返还给各自的所有者。这就保证了交易原子性。一旦交易完成，客户端应用撤销已响应的订单，每个客户端应用撤销自己的订单，这样就更新了全局订单。

除了交易者支付的每个区块链对应的网络成本外，交易智能合约收取每笔交易的一小部分，重新分配给连接到区块链上的一个或多个节点的操作所需的 SSW 代币的所有者，与拥有的代币和分配给每个区块链的代币总数成正比。

示例：节点所有者操作一个 P2P 节点，连接到以太坊（Ethereum）区块链（通往以太坊的网关），他从自己的代币中分配 100 个代币用于节点运作（通过专属钱包，代币仍是其财产）。另一方面，如果其他节点所有者操作连接到以太坊区块链的 P2P 节点，并且所有的节点有为此分配的 1000 个代币，那么我们的节点所有者会在涉及到以太坊的所有交易中获得收取到的成本的 10%（100/1000）。

如果他拥有其他 SSW 代币，且运营连接到其他区块链的其他节点，节点所有者也将从其他区块链的交易成本中收到与他相对应的部分。这样按区块链分配的系统，可以激励用户操作节点，以将交易所连接到少有节点运行的区块链，增加冗余，从而增强系统可用性和安全性。

(*) 详见 “交换原子性验证系统”。

代币的财务方面

用于此预测的数据

- 代币发行总数: 100,000,000
- 代币发行价格: 0.45 美元
- 分配给网关节点的代币百分比: 50%

我们认为部分 SSW 代币的收单方不会操作面向加密货币的网关节点，从而损失交易者支付的响应的部分交易成本，但是他们会因对代币价格的投机而购买代币。这一预测对我们来说是乐观的，现实可能接近于 30%。分配给网关节点操作的代币部分越少，操作网关节点的人的代币业绩越好。

以下数据来自 CoinMarketCap 在 2018 年 7 月底的消息。

这些交易量对应于加密货币崩溃结束的一段时间。我们可以预期，稍后，为了操作网关节点，交易量会升到通常水平，这将增加持有代币的盈利能力。

24 时内加密货币之间交易的分布示例：

比特币（Bitcoin）:	33%
Tether:	20%
以太坊（Ethereum）:	11%
EOS:	4.5%
OmiseGo:	0.45%

我们这里有 3 种交易最多的加密货币和两种交易量少的加密货币。

根据他们在 CoinMarketCap 的排名，24 小时内交易所的交易数量：

排名 100：3,000,000 美元

排名 75：10,000,000 美元

排名 50：20,000,000 美元

SSW 代币投资的盈利能力预测

我们认为分配给网关节点功能的代币与每个加密货币的交易量成比例。在加密货币的网关节点上过度分配代币会降低该加密货币的代币盈利能力。相反，为其他相关的加密货币分配较少代币可以增加其盈利能力。这就意味着运营网关节点的人将会把他们的代币分配给最能盈利的加密货币，这些就会变得不那么能盈利，而其他的就会变得更能盈利。因此，代币的分布自然会与加密货币的交易量分布保持一致。

代币利润率计算公式:

TTOK:在 ICO 发行的代币总数
FTAP = 分配给网关节点的代币的百分比
VE =交易额，以美元（$USD）计算
FEC = 加密货币交易与交易总额的百分比
FRTC = 加密货币网关节点的代币分布百分比
PX =代币购买价格，以美元计算
T = 平台收取的交易费用

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

我们看到，如果 FEC=FRTC，我们得到：

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

因此，如果 FEC = FRTC，无论交易量如何，所有加密货币的盈利能力都是一样的。

例如：

假设我们每天有 300 万美元的交易额（CoinMarketCap 上排名第 100 位的交易所）

每年我们会有：∑ VE = 365*300 万 = 10.95 亿美元

交易成本 T=0.15%，我们有：

利润率（Profitability）= ((1,095,000,000 * 0.0015) / (100000000 * 0.5)) / 0.45 = **7.3%** 的年度业绩。

如果我们每天的交易额是 1000 万美元（CoinMarketCap 上排名第 75 位的交易所）：

利润率（Profitability）=((10,000,000 * 365 * 0.0015) / (100000000 * 0.5)) / 0.45 = **24.33%** 的年度业绩。

如果我们每天有 2000 万美元的交易额（CoinMarketCap 上排名第 50 位的交易所）：

利润率（Profitability）=((20,000,000 * 365 * 0.0015) / (100000000 * 0.5)) / 0.45 = **48.67%** 的年度业绩。

结论

通过对 CoinMarketCap 上交易所排名的研究，我们可以验证排名在 100 位之外的交易所很快就会被用户抛弃，就是说他们的交易量很低。

我们相信，考虑到 Secure Swap 的优势，只要可交易的代币数量足够，Secure Swap 的会很容易成为位列前 100 名的交易所。

另外，只要 Secure Swap 支持他们希望交易的代币，运营网关节点的节点所有者就不会对其他交易平台感兴趣。因此，瞄准前 50 名似乎是现实的。

因此，只要用户接受 Secure Swap，SSW 代币的业绩可能会从每年 7%增长到每年 48%。我们以交易额相当于 CoinMarketCap 前 75 位的中间情况为目标，希望参与 ICO 的投资者的**年度业绩能达到 24%**。对于想要晚些购买 SSW 代币的人，业绩将取决于他们的购买价格。低价购入会提高业绩，高价购入则降低业绩。

此外，应该注意的是，作为预测依据的这些交易量，是最近的，是在加密货币泡沫破裂数月以后的时期。我们可以假设，在接下来的数月，加密货币市场将再次启动，这将增加交易量从而提升代币的盈利能力。

交易原子性验证系统

用于以太坊生态系统中的交易（ETH 和代币 ERC-20/ERC-720）

交易原子性是完全由以太坊区块链上的智能合约来处理。

这样的智能合约可以在没有外部干预的情况下，验证 ETH、代币的接收并将其发送给接收者。

当 Plasma/闪电网络这些二级解决方案运作和成熟时，这种类型的交易将会通过它们的集成而得到改进，这将显著提高以太坊生态系统的交易速度。

对于可互操作的区块链之间的交易

对于可互操作的区块链之间的交易（例如 Litecoin 和 Decred 之间，或者 Ethereum 和 Omisego 之间）：这样的互操作性目前还不起作用，当起作用时，它将使用像 Plasma 或闪电网络这样的技术。同时，Secure Swap 认为这些区块链是不可互操作的。

对于不可互操作的区块链之间的交易

在这种情况下，我们的交易所将通过 P2P 网络实现这些加密货币的互操作性。

交易中涉及的加密货币支持智能合约的情况

在发送给接收者之前，智能合约（每区块链一个）验证币是否到达钱包，所有的加密货币网关节点都会这样做，以确保交易原子性。

他们在 P2P 网络上向另一个智能合约（对应的智能合约）发送收到币的验证。

当一个交易中涉及的两个智能合约拥有币接收的确认时，币就会被发送给最终的接收者，以完成智能合约本身的交易。

为了保护他们自己免受节点黑客或恶意节点的攻击，如果相应的加密货币的所有网关节点都确认币已收到，智能合约仅验证币收据。

假如网关节点之间存在不一致的情况（意味着被攻击的节点或恶意节点），多数的应答获胜（一个网关节点的声音=关联到该节点的 SSW 代币数量），所有给出错误响应的网关节点都会切断连接并进入黑名单（IP 地址在黑名单上，防止这些节点重新连接到 P2P 网络）。

每当一个节点因为错误响应被断开连接，它就会因不符合规则向 P2P 网络发送断开连接的信息，并传播到所有的客户端和所有节点。每个接收到该信息的客户端就会停用该加密货币的交易并取消他关联该加密货币的所有订单。网络所有节点会记住每个加密货币的交易状态。因此，在黑客攻击尝试期间未连接并在之后连接的客户端将立即被告知该加密货币的交易失效。为了让该加密货币重新开始交易，之前为其（志愿者代表）选择的合格的多数（>=60%）的客户端将重新激活该加密货币上的交易。

该协议的结果是通过股权证明（proof of stake）达成共识。为了试图破解 P2P 网络并窃取交易中的币（因此从其他用户接收币时不发送相应的币），有必要将一半以上的 SSW 代币分配给加密货币的网关节点。这意味着要试图窃取交易，就有必要引入相当大量的 SSW 代币。假如其有效，交易所名声的影响会引起 SSW 代币价值的降低，这意味着黑客的损失会比窃取交易的收益更重要。

此外，由于在黑客控制之前，网络上必然存在一些诚实的节点，因此，这些节点断开连接时，会对所有节点（客户端和其他节点）已经收到的加密货币发送交易失效的通知。这也导致正在进行中的交易被取消，相关的币通过智能合约归还给用户。

有了这样的协议，尝试取得控制权就不太可能成功，即使成功了，也没什么可以窃取（交易已停用），SSW 代币的重要约定使得此类操作无利可图且成本高昂。

为了使这种安全性更有效，区块链中的网关节点必须足够充足，且所有的网关节点加在一起所分配的 SSW 代币要比交易的平均值要高得多，以构成可接受的股权证明。

因此，如果客户端的活动网关的数量低于 2，客户端将拒绝与加密货币进行交易，这是最低限度。

交易中涉及的加密货币之一（或两者）不支持智能合约的情况

在这种情况下，通常由加密货币智能合约覆盖的部分由一个专用节点覆盖，通过加密货币，在 Grey Matter 科技的安全保障和控制之中。

由于一种加密货币没有智能合约的支持，有必要拥有一个可靠的地方。因此，该专用节点要确保在发送给接收者之前，从交易的每一方接收到币，以确保没有智能合约的情况下交易的原子性。

对于没有智能合约的交易所，这种特殊的 Secure Swap 服务不需要占用交易者的加密货币，只是在交易时间内占用，与交易者必须将其资产转移较长时间的中心化交易所正相反。

此外，在这种情况下，没有加密货币中心库存，只有交易双方的临时存储，只是验证交易原子性的时间。因此，对黑客来说没有多大收获。

交易状态的指示

来自客户端的指示

客户端使用颜色代码表示每个加密货币的网关节点的可用性：

- 黑色：在加密货币的网关节点上检测到攻击尝试，该加密货币的交易停用。
- 红色：该加密货币没有网关可用=>没有可能的交易。
- 橙红色：该加密货币只有一个网关可用=>禁止交易。
- 黄色：该加密货币有两个网关可用=>交易正常，但对攻击的抵抗非最佳状态。
- 绿色：加密货币有三个或以上的网关可用=>交易正常，攻击抵抗处于最佳状态。

来自统计节点的指示

统计节点永久分析网络，以便为借点所有者和交易者提供不同的信息。它允许，例如：

- 提供关于节点的高级统计信息的仪表板，
- 根据分配给网关节点的 SSW 代币来评估预期报酬，
- 通过加密货币验证一段时期内的交易量，
- 等等。

交易所性能

如今，以太坊区块链的每秒事务数被限制在 10/15 左右。我们的智能合约在以太坊区块链的交易管理上也会遇到这些限制。

然而，开发工作正在进行之中，以大大增加以太坊区块链每秒能够完成的事务数量。我们正在讨论，通过诸如 Pasma，分片，闪电网络等技术，使该增长达到每秒几千甚至几百万。

虽然第一层改进，例如分片，将会增加我们的智能合约可以执行的每秒交易次数，但它与第二次改进例如 Plasma/闪电网络不应该是相同的（除了第一层操作的后续费用降低）。

按计划，在每个支持智能合约的区块链上有一个智能合约来管理交易，像 EOS 和其他，以联合多个区块链的执行能力（另外通过每个区块链的智能合约确保交易的原子性）。这样，交易者就不会仅与一个区块链的未来联系在一起，并且其管理交易的能力也不限于一个区块链的智能合约的执行能力，一个区块链不会限制其他更快的区块链的交易能力。

我们更倾向于在几个区块链上使用交易智能合约，而不是开发我们自己的具有足够的智能合约执行能力的加密货币。在现有的并且/或者正在开发的解决方案上构建，而不是在这里进行重复工作。

如何克服原始流动性不足？

发行时交易者显然会面对流动性问题：刚开始时，他们的订单簿是空的，这对第一批交易者来说是不利的。交易量较小的加密货币上也可能存在流动性问题。

仲裁服务能保证替代流动性，它依赖于订单簿和其他交易网站，依赖于 Secure Swap 内部订单簿以及我们平台特有的加密货币储备基金。

该仲裁服务将作为客户端（即，它在我们的订单簿中发出订单）使用属于公司的加密货币。这项服务由专门执行此任务的 P2P 节点组成。像网络上的所有节点一样，它从订单簿中接收更新。它能够在觉察到我们的订单簿时识别缺失的相应部分和完成他们与其他交易者的交易。

公司的部分可用运营资金将通过仲裁机制使用的几种加密货币的再分配来筹集。

例如，如果我们的订单簿包括 1BTC 兑 12ETH 的交易订单，但没有 BTC 兑 ETH 的请求价格或数量的交易订单，以及我们用作替代流动性的外部交易平台，存在一个这样的订单，那么我们会使用公司为仲裁服务保留的 ETH 做这个兑换，并回购在我们的交易平台上花费的 ETH 与另一个交易者平台拥有的 BTC 兑换。最后，我们认为我们在交易上拥有和使用以保证交易流动性的 ETH 最终会产生一个外部交易者，并且我们拥有的与外部交易者兑换的 BTC 最终会出现在我们的内部钱包上。

为了重新平衡我们的不同外部（在其他交易者）和内部（我们的交易者本地）钱包，我们将每天重新平衡持有的币数量（以限制成本），以保持加密货币储备的多样性。如果有必要，为保持正常运转，仲裁服务会在白天启动再平衡机制，以防某些加密货币缺乏流动性。

此类仲裁仅在我方订单簿缺乏流动性（因此订单没有对应方），以及操作对我们的交易者没有损失（最小中性）的情况下才会起作用。它也能产生利润，即使这不是它的首要目的。

开源许可证下的交易所

大多数交易所节点类型都分布在开源下。

这意味着除了所有交易者使用的客户端应用，每个人都有机会通过操作连接到区块链的节点来支持交易所的运营。

节点所有者这样做并且拥有在 ICO 期间发行的 SSW 代币，在交易期间根据他们分配给网关节点的代币的比例收取费用、代币中他们的部分，并与分配给有相同功能的区块链的网关节点的 SSW 代币的整体相关。

Grey Matter 科技公司将以同样的方式工作，并在 ICO 结束时按照它拥有的 SSW 代币的比例收取交易成本中自己的那部分，这将为每个网关节点保留一个正常运转的区块链。

我们也将在开放源码中提供一个计划用于法定货币兑换的节点的样本模板，以及连接到银行支付处理器的接口。因为这种活动受到严格控制，需要同时适应每一种情况（地方性法规和所使用的支付监管机构的接口），并开始运营合法活动（通过公司），我们将在开放源码中提供的节点模板会适用于每个特定的情况。

Grey Matter 科技也将在南美地区运营此类节点。我们计划运营节点来将下列货币转换为法币：智利比索，阿根廷比索，秘鲁比索，可能还会有其他。

因此，这种交易所将逐步转为大范围的法定货币和世界区域。

仲裁节点不会在开放源码中发布，因为我们保留它的使用权。当然，我们不能阻止那些想要开发自己的仲裁解决方案的人。无论如何，这种类型的服务需要大约 10 万美元的加密货币最低可用资金，或者更现实一点，大约一百万美元，才能与若干交易所一起运作。

BUG 程序赏金

ICO 期间募集的资金将用于资助漏洞赏金活动。奖项会颁发给参与这些计划并向我们的团队报告未知错误或安全故障的人。

活动开始于开发期间的每个阶段，以确保第一个投入运营的平台版本可以得到充分分析。

然后，还会计划季度活动，以跟踪事态的持续发展。

ICO，代币 ERC-20 SECURE SWAP (SSW)

为什么 ICO？为什么创建代币 ERC ERC-20？

我们需要为这个项目筹集资金

给额外的员工雇佣提供资金，支付活跃团队的工资。这是主要费用。

我们还必须在平台发布前为广告筹集资金，以便让其众所周知。

对于仲裁系统，我们还需要以加密货币计价的营运资金。

最后，我们必须为 Bug 赏金活动提供资金。

ICO 期间所有未售出的代币将归公司所有，以收取相应部分的兑换成本。因此，ICO 越成功，参与交易所运营的投资者收到的因交易产生的收入越多，因为公司持有的 SSW 币会很少。

相反，ICO 认购越少，公司持有的代币越多，并且还获得产生的收入中可观的一部分。考虑到公司在 ICO 期间筹集的资金，会确保我们对收入进行重新分配似乎是正确的，这将允许我们的支持投资者获得回报。

ICO 数据

代币名称：Secure Swap

Ticket SSW

创建数量：一亿个代币

代币初始价格: 0.45 美元

团队预留：10%

顾问预留：3%

社区经理、ICO 活动团队负责人预留： 3%

合作伙伴预留：4%

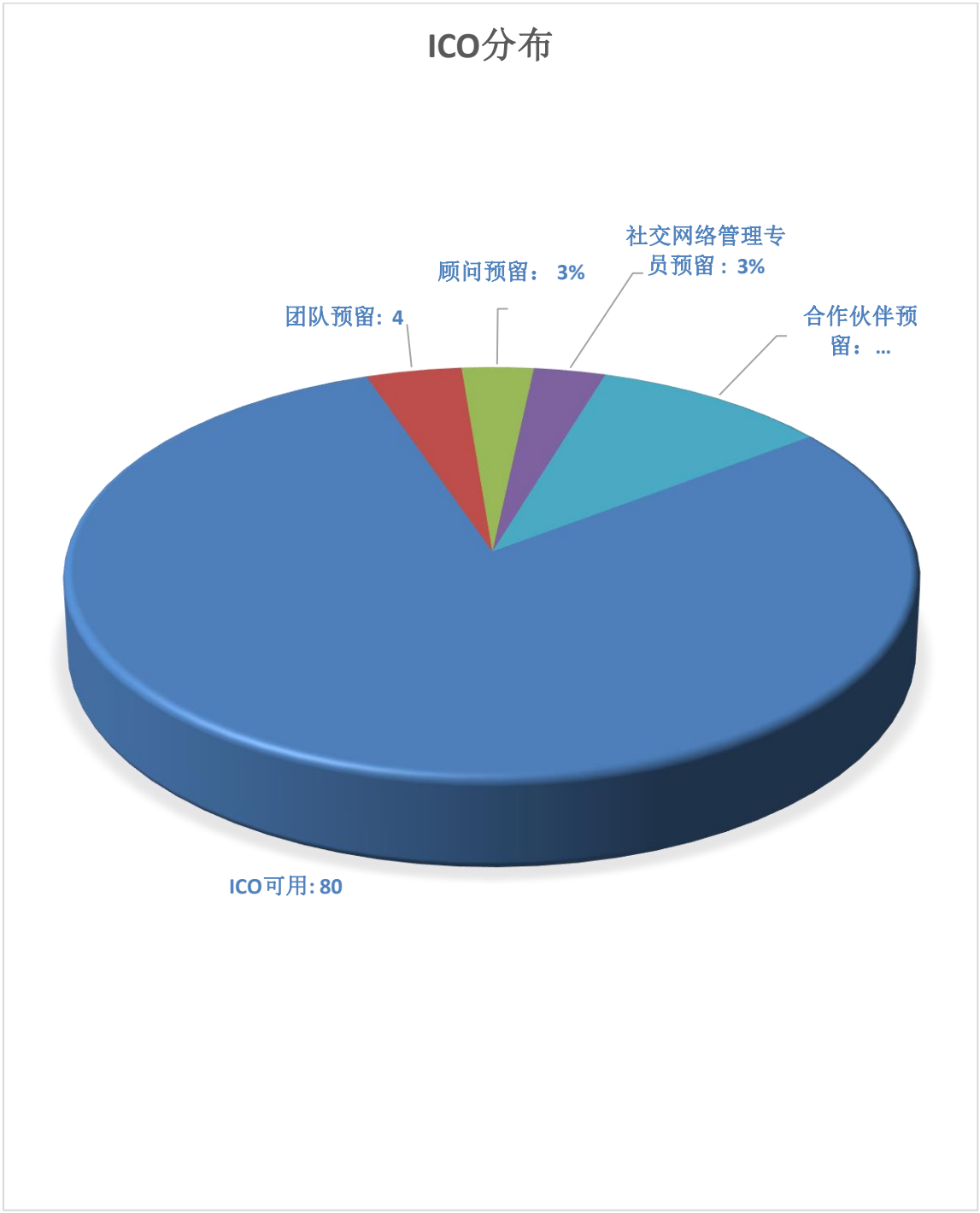
ICO 可用: 80%

软上限：1 千万代币

硬上限：8 千万代币

所有未售出的代币仍为公司的财产。

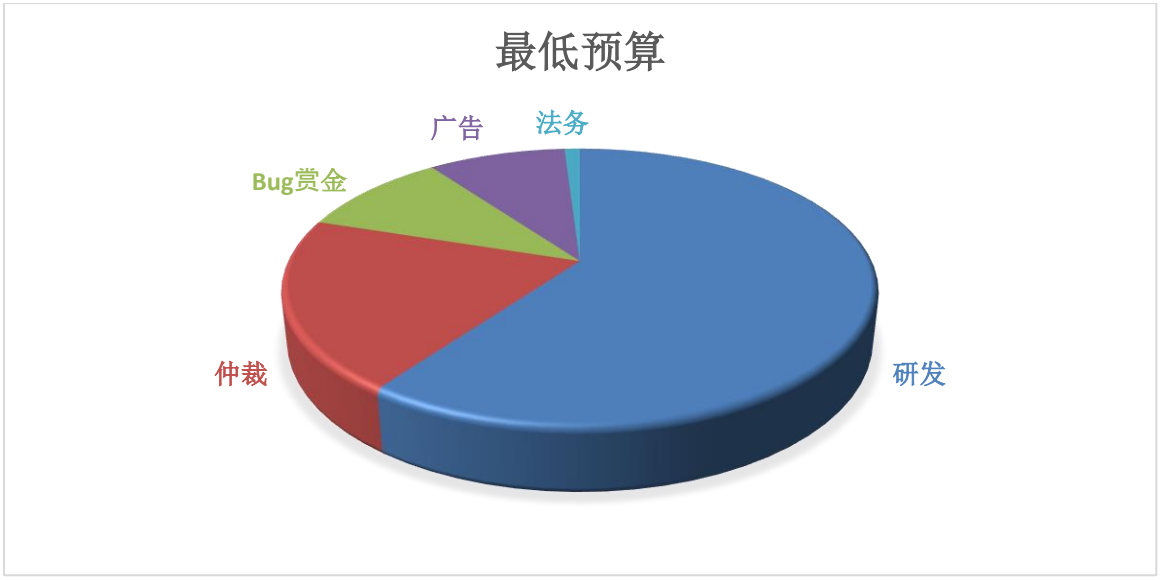
ICO 由 Grey Matter 科技（智利公司）运营。



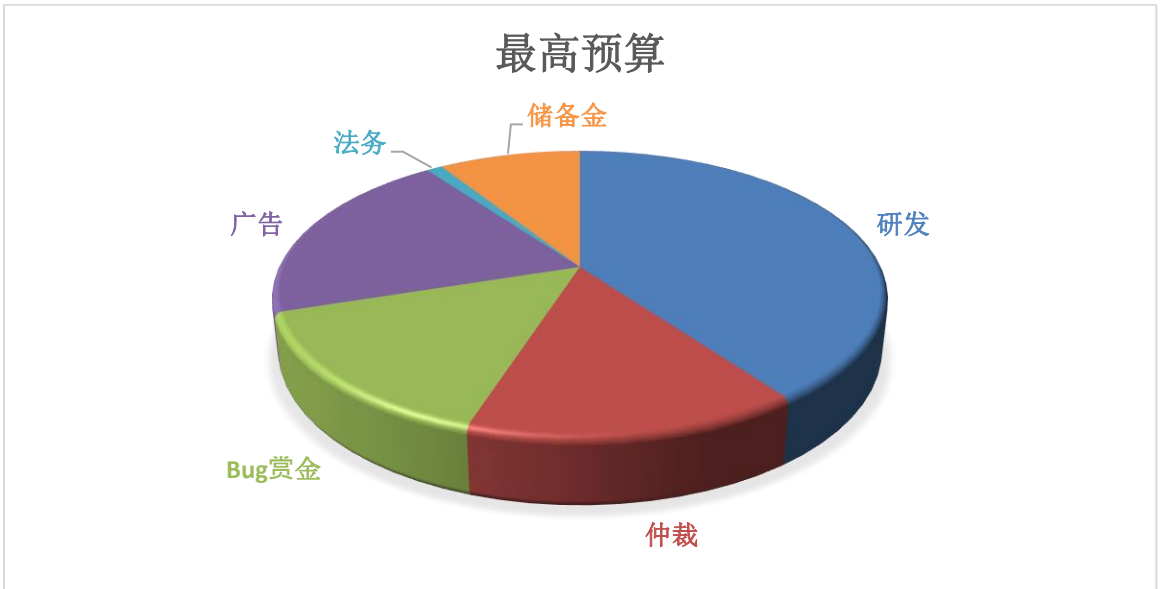
资金分配

我们将在这里指出两种极端情况下的资金分配：达到软上限，达到硬上限。

达到软上限



达到硬上限



路线图

这是在 ICO 硬上限达到时的计划的路线图。否则，该项目会被设计成抽屉模块（drawer modules）。每个模块的开发都可以推迟，直到收入允许这些功能自我融资。

在路线图中，可以推迟的特性以星号（*）标记。

交易所的改进，加密货币的添加（网关节点）等，将在此路线图之外进行。

ICO 路线图

SECURE SWAP 路线图

团队

成员

Alain Saffray
CEO – 联合创始人
研发工程师

Philippe Aubessard
CTO – 联合创始人
研发工程师

Alicia Laura Poblete
联合创始人
财务总监

Nadine Miotti
联合创始人
市场总监

Renaud Desportes
业务拓展经理

Rafael Romero Carmona
DevOps 工程师

Pierre Pretti
安全基础设施工程师

Aliaksandr Kharlamou
区块链工程师

Victor Chukholskiy
区块链工程师
智能合约专家

Marc Rivoal
30 年经验
软件体系结构的定义，过程建模，数据建模，项目管理，设计

Zhan Wei - 詹玮
社交管理专员

Kevin Vanstaen
社交管理专员
区块链爱好者

Lulia Galea
社交管理专员

Henry Morera
社交管理专员

顾问

Benoît Renard
法律顾问

法律方面

SSW 代币的法律含义

我们无法保证 SSW 代币价格的未来演变，也不能保证它出现在交易所列表的可能性和转售它的可能性。拥有代币并不意味着拥有 Grey Matter 科技公司的任何参与、控制或决策的权利。无论 ICO 发行如何，代币都不可退款。投资者或投机者完全承担购买风险。

由于 Secure Swap 的社区方面，并且由于加密货币之间的交易属于 Grey Matter 科技无法控制的分布式系统，因此 Secure Swap 代币是一种实用的代币，用作在开放系统中保护交易的股权证明。它允许盈利，就像拥有采矿技术的以太坊一样，但是在没有公司治理的分布式系统中，Grey Matter 科技只能带来技术解决方案。

由于 Secure Swap 是分布式和社区开放式的交易所，这意味着用户可以匿名，至少在交易的加密货币允许的情况下可以，因此，询问投资者的身份和居住证明来检验他们参与此 ICO 的权利似乎是不可以想象的。

因此，投资者**应该根据其居住国家验证参与此 ICO 是否合法**，并在非法或存疑的情况下弃权。

请注意，目前中国和韩国完全禁止参与 ICO，无论代币性质如何。

对于美国公民，他们必须**向美国证券交易委员会（SEC）合适参与此 ICO 是否合法。**

对于欧洲公民，通过参与此 ICO，您声明了**您不是 2011 年 10 月 25 日关于消费者权利的 2011/83/UE 欧洲指令意义上的消费者。**

对于俄罗斯公民，他们必须**向当局核实参与此 ICO 是否合法。**

关于将加密货币兑换为法定货币的节点：

这种类型的节点意味着一种法律结构，并且符合运营地当地的发来吧，特别是**关于欺诈、洗钱或任何认罪活动的法规（KYC/AML/CFT/FCA）。**

公司经营交易所

- 交易所，即网关节点、仲裁节点和我们支持的法定货币的转换节点，将由 Grey Matter 科技公司管理：ww.greymattertechs.com
- Grey Matter 科技公司是一家智利公司(https://www.conservador.cl/portal/indice_comercio)。
- 我们鼓励任何志愿者支持系统管理他/她自己的网关节点，并且自己操作转换到法定货币，当然，根据这些系统的开发地点，有责任遵守当地法规。

FAQ 常见问题

SECURE SWAP 常见问题

问:1：Secure Swap 是什么？

答 1：Secure Swap 是一个去中心化的加密货币交易所（DEX），具有社区属性。它由位于智利的 Grey Mater 科技公司与一个法国创始团队共同开发。

问 2：它支持哪些加密货币？

答 2：可能所有数字货币都能够交易。开始时，系统使用最流行的加密货币来运作，其他的会逐步增加。

问 3：Secure Swap 是否接受使用法定货币的兑换？

答 3：是的，计划好了。开始时，它接受南美货币。我们平台的社区方面允许其他公司提供他们国家或地区的的法定货币的链接。

问 4：Secure Swap 社区方面是什么？

答 4：该项目处于开源许可之下。其架构依赖于 P2P 节点类型网络。感兴趣的人可以使用这些节点。

问 5：社区使用这些 P2P 节点的利益是什么？

答 5：运营 P2P 节点、因此支持该服务的人，会根据他们分配给该服务的 SSW 代币的比例，接收交易者支付的部分交易成本。

问 6：SSW 代币如何归属于节点？

答：节点配置中标示包含 SSW 代币的钱包归属于此节点。同一个钱包一次只能归属于一个节点。钱包在节点中标示，以验证所包含的代币的数量，代币为相同所有者持有。

问 7：我们如何获得这些 SSW 代币？

答 7：Grey Matter 科技公司启动 ICO（Initial Coin Offering，首次币发行）发行这些 SSW 代币。之后，代币可以交易，特别是在 Secure Swap 上。

问 8：付款如何计算？

答 8：节点对每个支持的区块链来说是专用的。它们确保 P2P 网络与区块链的连接，并被称为“网关节点”。每个区块链都有一定数量的网关节点，每个节点分配有 SSW 代币。

例如，如果在 EOS 区块链上发出一个网关节点，并且关联了有 10 个 SSW 代币的钱包，如果 EOS 区块链上所有的网关节点共有 100 个 SSW 代币被关联，那么对于在之前标示的 EOS 钱包上自动使用 EOS 加密货币进行的所有交易，节点所有者会收到交易成本的 10%（10/100）。

问 9：Grey Matter 科技如何通过这个系统保证其利益？

答 9：作为节点所有者，公司会将 ICO 结束时拥有的代币（未售出的代币）放置在功能 P2P 节点。

问 10：如果公司销售 ICO 期间的所有代币，SSW 代币会耗尽吗？

答：公司可以通过加密货币到法定货币的交易盈利，这不是通过代币系统共享的，而是完全回归这些交易的运营者。一旦服务开始运行，它还可以购入更多 SSW 代币。

问 11：这是否意味着 Grey Matter 科技为自己保留了法定货币？

答 11：不，由于它的开源和社区方面，Secure Swap 允许任何人使用到法定货币的交易网关。然而，法律架构是必须的，它必须保留遵守交易发生地的法规。Grey Matter 科技公司计划开始在智利、秘鲁和阿根廷进行与法定货币的交易。

问 12：Secure Swap 计划如何吸引交易者？

答 12：Secure Swap 提供了专用于交易的客户端应用，并且依赖于网关节点网络。这个应用利用了我们在经纪人软件方面的经验。它的人体工程学设计比现有的平台要好得多，它还为交易提供了工具和支持的系统，这是创新的。

问 13：在这样一个社区和开源系统中，你如何保证交易的安全？

答 13：加密货币的所有网关节点都响应来自参与交易的客户端应用程序的请求。如果节点的响应不同，就意味着存在黑客攻击尝试。在这种情况下，基于股权证明的系统通过断开并将其加入黑名单来清除不合规的节点。

问 14：股权证明如何运作？

答 14：当节点在交易验证步骤给出不同的应答时，而标准应答是在所有节点中占多数的那个，每个节点都有一个投票权重来对应与其功能相关联的 SSW 代币。应答不同的节点会被断开并加入黑名单。因此，为了窃取交易，有必要投资大量的 SSW 代币，即分配给该加密货币的网关节点的半数以上的代币，这意味着一个高于窃取交易的值、一次无法进行的攻击，因为一旦检测到问题，交易就会取消。如果黑客投入足够的资金来控制所有的网关节点，交易所就会失去信誉，导致 SSW 代币价值迅速下降；这项行动对黑客而言是一种损失，涉及到的代币数量会使其非常昂贵。此外，一旦检测到问题，那种加密货币的交易就会中断，黑客就没什么交易可以窃取了。

问 15：如果节点被黑客攻击并且处于黑客的控制之下，您如何保证安全系统能够正常运行？

答 15：最初，网关节点是诚实的，我们知道这一点是因为我们会在服务开始时自己运行第一个节点。因为客户端应用程序会等待所有网关节点的确认以向加密货币发送 coins，如果所有的网关节点没有给出相同的应答，就意味着存在问题。参与交易的客户端取消交易，并通知所有的 P2P 网络该加密货币上的交易停用，这将取消连接到该加密货币的所有客户端的所有等待的订单。没有交易了，黑客也就没有交易可以窃取。

问 16：因异常情况停用的加密货币，交易如何再次启动？

答 16：要让交易再次启动，需要获得与之前选定的加密货币相连接的代表中的合格的多数（60%）的一致投票。这些代表负责确保该加密货币的活跃节点在再次授权之前与该加密货币的交易相符。

问 17：这些代表如何确保在投票前网关节点是诚实的？

答 17：通过将它们自身连接到网关节点或验证它们的节点是否仍然连接。只有连接一个可靠节点，如果节点再次有不同响应，才能检测到问题。而且，该加密货币上的交易会再次被暂停并取消。

因此，如果没有事故交易就重新启动，这意味着交易可靠且恶意节点已被清除。如果恶意节点正在休眠并在等待付诸行动时正常运行，当它们这样做时，它们会因为不同的响应再次被检测出来。因此，节点损坏的任何尝试都可以检测到，窃取一笔交易是不可能的。

问 18：如何指定代表？

答 18：他们是志愿者，只有当他们拥有相当于所有节点 SSW 币值的平均交易量的 100 倍时才有资格。志愿者通过节点接口发送请求，如果合格，网络中的所有节点都会记住其“超级网关节点”的状态。与通常认为的分配的代币相比，“超级网关节点”的报酬会多出 50%的奖金。

问 19：如何防止不诚实的人永久连接有缺陷的节点以阻止服务？

答 19：被列入黑名单的异常节点，除了会断开连接，这些不诚实的人会迅速耗尽连接这些节点的 IP 地址来。另外，这样的 IT 破坏行为是非法的，它的重复会增加识别其作者的机会，和 Grey Matter 科技会搜寻这些人以要求赔偿。

问 20：采取什么措施来打击黑客？

答 20：除了之前描述的协议，以及整个 Secure Swap 项目在开放源码上对每个人来说都可用的事实，我们还有每 3 个月举行一次的 Bug 赏金活动来奖励在系统中发现漏洞的人。