EXPREAD：通过处理去中心化交易和统一流动性为加密交易所提供白标服务

白皮书 版本 2.1

摘要 EXPREAD 为加密交易所提供扩容性强的白标解决方案，以降低准入门槛，减少加密交易机构的垄断。EXPREAD 的流动性模型可无缝聚合市场深度，从统一的流动池获得协同价值。系统可协助完成订单，允许交易所采取以社区为基础的目标营销策略，更有效地利用各自网络积累的的人脉和声誉。EXPREAD 生态系统的内部框架是联盟式的网络拓扑结构，集成了（由区块链技术支撑的）支付通道协议，把握好去中心化和可扩容性的平衡。该系统是一种综合模式，有效地结合了去中心化和中心化加密货币交易所的优势。

关键词：加密货币交易所，商业网络模型，白标，面向社区的营销，DEX，支付通道，点对点，分布式治理，区块链技术

目录

1.加密货币交易所的当前系统及其缺陷

加密货币的出现是为了推动交易和数据系统的去中心化。然而，当前加密经济的基础设施和执行却朝着更为中心化的方向发展。就增加市场的流动性、协助代币价格收敛到其基本价值（长远目标）以及推广主流接受代币方面，加密货币交易所至关重要。在过去 7 年里，数百种中心化和去中心化交易所层出不穷，但是效率似乎很不理想，因为越多新的交易所进入这个领域，潜在流动性和市场债务就越分散。再者，当前大部分交易所系统容易出现重大风险和故障，偶然故障、欺诈活动或是底层协议设计不佳都可能带来问题。

中心化交易所和所有中心化系统都存在同样的漏洞：单点故障、中心化控制和治理（透明度低、非法预先交易、价格操纵等等）。这些交易所都容易受到攻击（单点故障），且攻击的方式多种多样，包括服务暂停和服务器无响应（比如 DoS 攻击）、重大安全漏洞和在地址中聚集的大量加密资产被盗。近几年来，中心化加密货币交易所系统故障带来了不少问题，诈骗、安全协议漏洞、管理效率低下和不合理的内部控制造成的损失高达 20 亿美元。上述故障起因有二：过分依赖系统安全（单个故障可能导致系统瘫痪）；缺少充分的制衡机制来识别信任方作弊行为。

除此之外，交易所的系统之间缺乏互联性和流动性，流动池被孤立。市场债务也被分散，导致价格回升缓慢、套利价格差异和大交易所（因为价格波动）执行费用高昂。然而，当前用来连接不同平台的流动性聚合器还很稀缺，仅有小部分交易所（一些大交易所）通过聚合器合作。而这些聚合器助推了大交易所的垄断，提高了流动性门槛，新交易所难以进入这个领域。

既然中心化交易所存在这么多问题，那么理论上来说，完全去中心化的加密货币交易所是个好选择。然而，实际应用的时候也会出现严重的故障。取消中间人的角色可能会降低交易所的功能效用，去中心化交易所通常成本更高、交易引擎更慢、功能也较为有限。最早尝试去中心化的有以太坊的智能合约，但是运行和匹配链上订单簿的成本非常高昂（由于所需的燃料）。后来，其他配置更好的协议问世，如 0x 和 Swap，结合了链下订单簿和链上交易结算。这些协议虽然运行成本较低，但它们的交易引擎较慢，而且无法接受“真正的”市场单或限价单。一次性的 P2P 加密货币交易可能还可以接受，但无法满足对日间交易或投机买卖感兴趣的用户群。

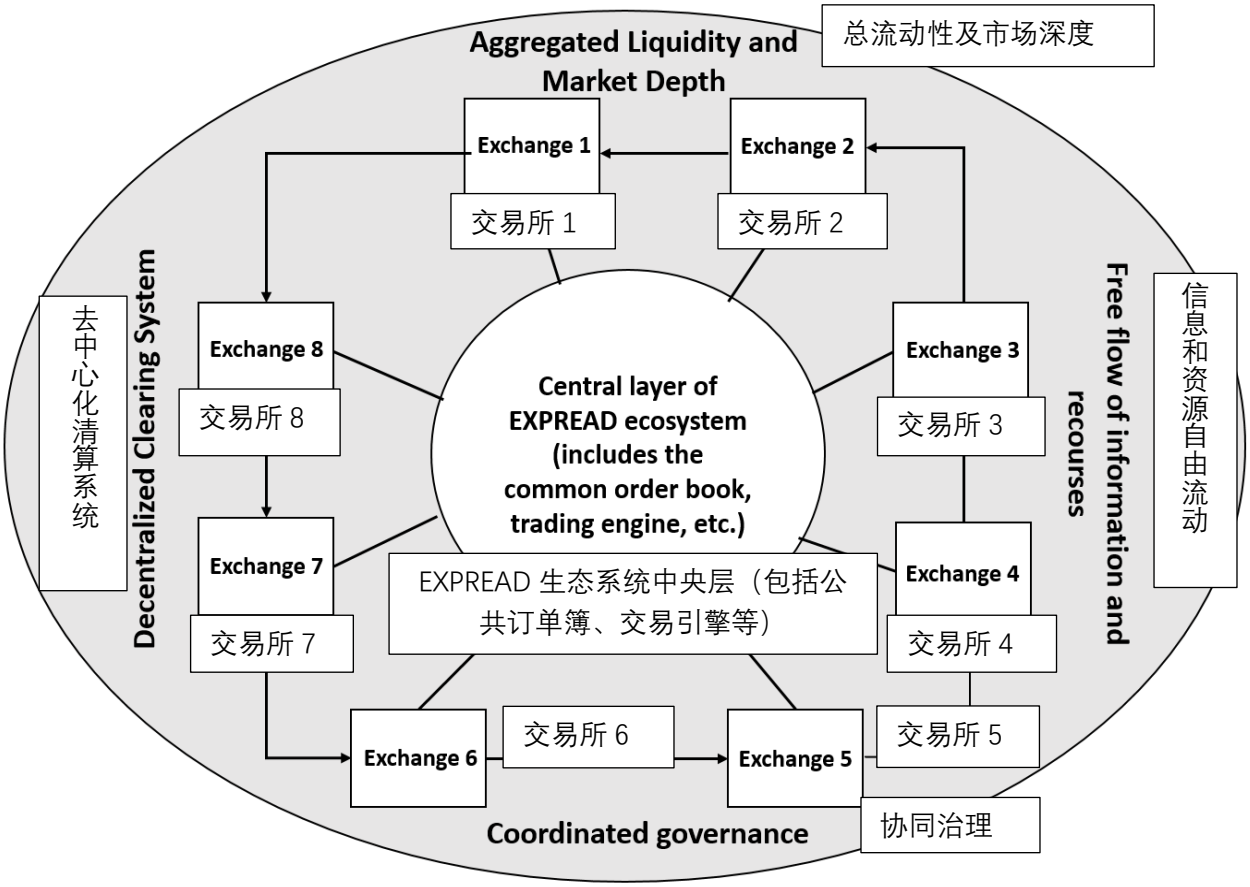
另外，去中心化系统没办法从根本上解决流动性孤立的问题。在这块领域还没有技术标准，而且目前提出来的去中心化交易协议的配置过程和设计都不同，所以它们之间的互联性差。因此，使用这些协议的交易所面临着内部协调和区块链互操作性的问题，进一步孤立了市场的流动池。

此白皮书会详细介绍 EXPREAD 交易系统。EXPREAD 交易系统是一个综合的解决方案，结合了中心化系统（功能高级、交易引擎高效）和去中心化系统（安全性更高、操作完全透明可审计、共同治理）的优点。提出 EXPREAD 是为了完全实现加密交易的去中心化和自由化（准入门槛非常低），真正实现所有人都能开放自己的交易节点，同时把流动性都聚集在 EXPREAD 生态系统里。创建这个系统是为了更好地利用多方交易所的协同价值（给予合适的经济奖励）并发挥市场统一的优势。

2. EXPREAD 的设计介绍

EXPREAD 是为加密货币交易所提供白标服务的生态系统，具有共享订单簿、交易引擎和流动池。EXPREAD 建立在交易所服务实现共享经济的基础上，把多个场所（节点、交易所）的流动性、技术成本和各自的专业知识都集中起来，形成网络效应并从中获得协同价值。此外，整个系统的设计能够分配池中储备资产的流动性，避免单点故障。每个节点（交易所）提供足够的内部控制，实现交易系统的全面可审计性。

图 2.1 EXPREAD 生态系统构成



EXPREAD 生态系统下的交易所发起的每个订单都会发送到整个系统，提高了订单执行的概率。这与当前以内部订单流为主的中心化交易所有着质的差别。如果中心化和去中心化交易系统各自缺乏持续大量的流动性，系统就会停止运作。而 EXPREAD 生态系统联通多间交易所的设计能加快用户增长速度，让系统里新开的交易所从市场债务中获益。

EXPREAD 系统是三层复合结构。生态系统的中心是 EXPREAD 基金会，用以确保统一的订单簿和交易引擎能正常运作。基金会建设的唯一目标就是为 EXPREAD 生态系统提供技术、安全性、商业咨询和其他服务，也会以中央管理员的身份为 EXPREAD 网络的发展创造更多激励机制。

订单簿会在系统内所有交易所广播更新，这就是第二层。为方便白标交易所所有者开展内部管理，EXPREAD 提供自定义界面、功能、可交易代币选择及其他工具。交易所是终端用户参与到 EXPREAD 系统的网关，接受的订单会登记在内部订单簿上，同时也会登记在 EXPREAD 基金会维护的统一账本上。内部订单簿不会和中央订单簿有任何的交集，中央订单簿可用于事后审计。

第三层的基础是为支持 EXPREAD 设计而创建的支付通道协议，并由以太坊区块链作支撑。这个平台采用全新的加密资金储存方式，实现了不同交易所间账目核对的去中心化。总的来说，存入交易所（由终端用户进行交易）的加密资金会被储存在需要多重签名的地址上，每个交易所都会有这样的地址。交易所所有者和 EXPREAD 基金会共同控制并持有私钥。所以，为公正起见，这个系统对储存的所有资金采取分布式控制，确保交易所所有者和 EXPREAD 基金会均无法独自获取资金（制衡层）。EXPREAD 基金会和任何交易所之间因资金而产生的冲突会由系统中的纠纷调解机构解决。

EXPREAD 的状态通道协议集成了同行确认系统，所以 EXPREAD 生态系统通过交易所之间周期性的对账（每两个小时一次）支持基金的运作。整个对账的过程（第 4 节会详细阐述）能确保所有节点都获取完整、独立、从网关开始的订单流信息，也能迅速检测到任何操纵订单簿和交易引擎的行为。区块链上会储存交易所之间的资金流和最终结算信息，事后可用于审计。

总的来说，EXPREAD 有效地对系统中储存的资金实行去中心化管理，随着交易所数量增加，集中系数会下降。维护中心化的订单簿和交易引擎让交易所能运行高级复杂的交易工具、执行速度快（满足高频交易者的需求）而且扩容性高。同时，通过链下同行验证匹配和在链上操作，事后可对整个交易系统进行事后审计。

3. EXPREAD 模型的经济原因和协同价值

流动性聚合带来的巨大协同价值是 EXPREAD 诞生的灵感和基础，而目前加密交易所的搭建和运行模型并没有发掘出流动性聚合的巨大潜力。底层框架无法支持合作，催生了数以百计、独立存在的交易所，各自的流动性很小，竞争力不高而且难以满足大量交易的要求。当前模型的缺陷造成价值损失的原因有二：交易所运行效率低下以及消费者无法以市场上的最优价格执行订单。

EXPREAD 是开源生态系统，为搭建交易所提供白标服务和统一的交易引擎技术，由无需许可的区块链作支撑。网络内的交易所（联盟的一员）仍然是不同的个体。每个交易所会给生态系统带来各自的资源和流动性，从而进一步提高整个网络的竞争力。协同价值体现在为更多终端用户带来更多的冲销订单、更好的市场深度、有效的价格发现和更低的买卖价差。此外，互通订单流会提高 EXPREAD 交易所的交易速度，短期盈利和长期增长率都会有更好的业务前景。

除了解决流动性问题之外，EXPREAD 还极大地降低了准入门槛，交易所所需的创办资本（用于开发加密交易协议）更低，而且他们不需要担心交易所安全方面的技术问题。EXPREAD 负责处理大部分与技术相关的功能，这能帮助交易所创业者们把精力集中在遵守规则和市场推广上，事实证明，把这些领域做好对交易所的发展更为重要。由于 EXPREAD 交易所的内部运转不要求在买和卖两个终端都有大量的用户，交易所可在多场所结构的系统里采取以当地社区和小众市场为目标的营销策略。换句话说，交易所所有者可以专注于利用好自己的口碑、网络、社区和现有的客户群来开展加密交易活动[1]。

交易所可以选取不同的目标人群，同时也可以自定义交易费用、界面、可交易代币选择和功能等，吸引新消费者，实现 EXPREAD 生态系统的良性竞争。由于加密市场飞速扩张、当前交易所竞争力不断变化，我们相信 EXPREAD 生态系统需要花大量时间才能使内部达到帕雷托最优状态。因此，我们预测新交易所会给整个生态系统带来协同价值

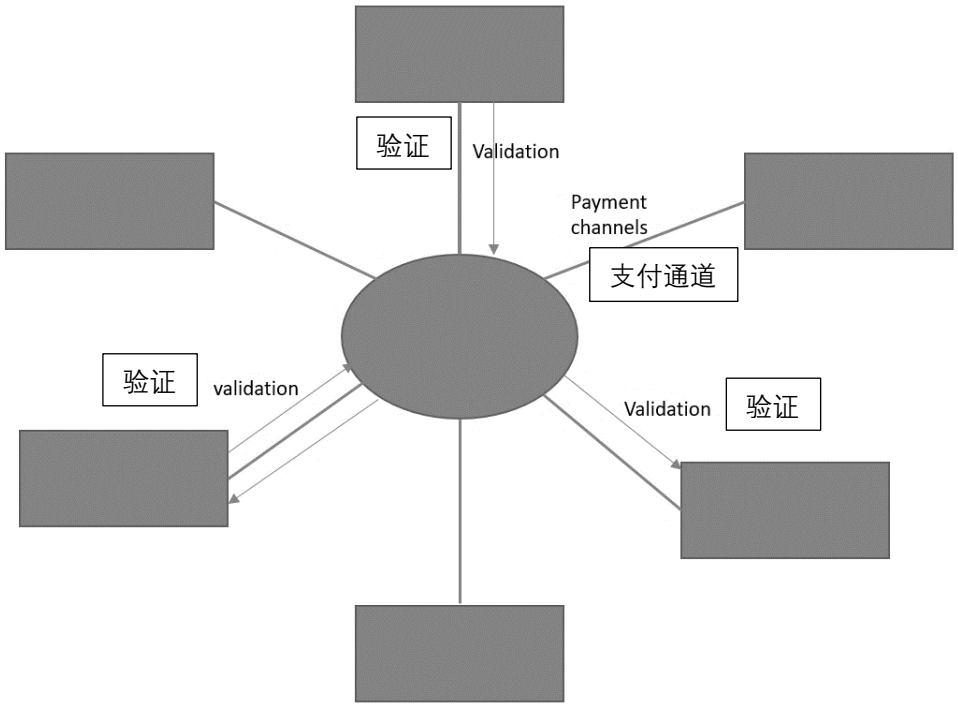
[1] 交易所所有者手握多重签名地址两把私钥中的其中一把（获取资金需要两把私钥），因此交易所的可信度与它们自身的声誉以及 EXPREAD 基金会的声誉密切相关。

（增加市场深度），好处远比同行竞争多。与此同时，系统的内部治理机制能确保 EXPREAD 交易所不大量扎堆[2]（详见第 8 节）。

4. 应用于去中心化内部清算的状态通道协议

由于区块链技术对彻底的链上订单处理和订单流冲销有限制（交易成本高、扩容性低等），应用链下广播、抵销交易的周期性聚合和链上订单核对是应对这些限制的最佳方案。为了实现冲销订单的分布式处理，EXPREAD 应用了独特的支付通道协议。它的结构虽与以太坊的雷电网络（Raiden Network）和比特币的闪电网络（Lighting network）相似，但我们应用一个全新概念的网络拓扑结构来实现不同交易所间的去中心化互动。EXPREAD 基金会是系统中的超级节点，能快速地选择路径并增强所有交易所的支付通道之间的互联性，这与我们强调的商业模式高度契合。链下状态转换系统也可在两个交易所之间反复处理小额的冲销订单，如果每个订单都单独执行的话会导致高昂的成本和明显的时间延迟。

图 4.1 EXPREAD 网络拓扑结构



[2] 第 6 节将进一步阐述。

为了能在链下处理跨交易所的冲销订单，系统中的每个交易所都和 EXPREAD 基金会形成双重支付通道。为了支撑支付通道，资金通过网关（场所）储存在 2-2 多重签名地址（其中一个地址在通道内），私钥会分发到交易所和 EXPREAD 基金会。所以 EXPREAD 基金会实际上一直是系统中所有场所的中间人，不间断地工作。超级节点 EXPREAD 基金会的运作也有重要的实际意义，它把支付通道的数量限制在 N（系统中的交易所数量）。如果网络拓扑结构的分布结构更为分散的话，将产生N^2个开放的直接支付通道（所有场所之间互相开放），就系统管理和规划最低储存金额而言不太可行。此外，应用稀疏图（如闪电网络）不一定可行，因为两个参与者边缘间很可能一直都存在通路，为对账提供足够的执行能力。若资金被不同通道分散了，那么来自不寻常合作伙伴的大型订单很有可能耗尽通道，打断系统的正常运作。

除了分配交易所间的支付通道以外，EXPREAD 在生态系统里还有验证的功能。总的来说，交易所间任何对账和货币冲销行为都需要三方验证（即交易所双方和 EXPREAD 基金会），而终端用户从交易所撤回资金则需要双方验证（即交易所和 EXPREAD 基金会）。因此，此机制可确保就算交易所作弊，EXPREAD 仍然有审计和验证的权力，能及时阻止系统出现故障。

4.1 支付通道系统运作细节

整个支付流程可以分成三个主要阶段，包括通道开放、链下结算和链上执行/解决冲突。

通道开放阶段是个不断重复的过程（接着是重新开放通道和关闭通道取款）。每个交易所都有两层多重签名地址 :一层用于储存（或提取）用户的数字货币，另一层用于支付通道。这两个地址是相互关联的，资金从其中一个地址流入另一个地址，以确保在每个结算周期之前，支付通道有足够的资金满足已通过安全验证的对手方核对账目的需求。同时，基金会与交易方有单向支付通道（EXC 代币存款），万一基金会出现问题，该通道可确保交易所有能力补偿损失（详见下文）。

链下对账系统能实时传输已签名的信息，并支持跨场所的抵销交易，实现了流程能在链下安全执行。这种冲销机制意味着生态系统里所有交易所共享一个复制状态机。交易所和

EXPREAD 基金会之间的沟通是通过点对点的消息传递，信息由白标交易所所有者（场所）和基金会双方签名。因此，在对账期间，基金会可以以中间人的身份确保链上货币安全流通。从设计上来说，这个系统的确像是由区块链支撑的清算所，交易所没有逃避承诺的余地。

闪电网络协议面临的主要挑战就是在链下、链上操作的时候可能会运行中断。这是由于系统在链上执行的时候，不能开展链下交易，这种情况对 EXPREAD 平台而言是不可持续的。为了解决这个障碍，我们应用了 Sprites 通道协议提供的增量式储存系统（A. Miller 和 I. Bentow 等），实现在支付通道里部分提款和存款。

支付通道系统的界面操作简便，白标所有者可轻松使用，不需要有专业技术背景。EXPREAD 基金会成立的目的是服务和支持所有信息传输过程和最终结算，所以系统有专门的确认界面，用于订单的分布式验证和管理链上所验证的信息。交易所可以将链内公布交易的验证功能委托给第三方，以确保他们交易操作中的相互制衡。

总而言之，整个系统的核心在于用适度的内部控制实现基金流的安全运作。为了避免整个生态系统出现故障，如有交易所因某种原因而掉线（无法进行验证），处理对账和转账的要求超过一定时间即视为无效。

从博弈论来看，这个系统的独特性使其对于所有参与方而言都是不可信任的。因为一旦有一方作弊，所有交易所和基金会都有可能影响交易价值。

1. $(\mathbf{E1(X1 \ggg F) \cup E2(X2 \ggg F)} \rightarrow F(X2 \ggg \mathbf{E1, X1} \ggg \mathbf{E2}) \rightarrow OK$

2. $(\mathbf{E1(X1 \ggg F) \cup E2((X2\text{-}1) \ggg F)} \rightarrow F(E2(X2) \ggg \mathbf{F)} \rightarrow F(X2 \ggg \mathbf{F1, X1} \ggg \mathbf{F2}) \rightarrow OK$

3. $(\mathbf{E1((X1\text{-}1) \ggg F) \cup E2((X2) \ggg F)} \rightarrow F(E1(X1) \ggg \mathbf{F)} \rightarrow F(X2 \ggg \mathbf{F1, X1} \ggg \mathbf{F2}) \rightarrow OK$

4. $(\mathbf{E1((X1) \ggg F) \cup E2((X2) \ggg F)} \rightarrow F((X2 - 1) \ggg \mathbf{F1, (X1\text{-}1)} \ggg \mathbf{F2})$
$\rightarrow E1((F(T) \ggg \mathbf{E1) \text{ and } E2}((F(T) \ggg \mathbf{E2})$

5. $(\mathbf{E1((X1) \ggg F) \cup E2((X2) \ggg F)} \rightarrow \mathbf{F((X1),(X2))} \ggg \mathbf{Z}) \rightarrow (T, T) \ggg \mathbf{E1,E2}$

在公式里：（）内广播函数
***F*代表基金会、E 代表交易所、Z 代表第三方地址**
⋙代表发送交易
→前往下一步
T 代表基金会储存的资金（EXC 代币）

这个系统充分利用了闪电支付通道的链上纠纷解决程序。由于交易代码中包含时标，若一方广播了错误的输出信息（信息传输赋予了参与方这一功能），对手方（这里指交易所和基金会）有时间改变交易输出。同时，若基金会作弊，交易所可以单向广播 EXC 代币转到

它们地址的过程。因此，整个系统是个闭路循环，所有参与方都没有作弊的动机，有效地把整个过程去中心化。

5. 订单簿和交易引擎的事后可审计性

为确保 EXPREAD 基金会不能因为偏袒任何一交易所而操控订单记录，实现各个交易所能够全面追溯订单记录和交易引擎至关重要，是安全措施的关键一环。整个过程都很直接，每位用户均可查看公布订单簿上的所有记录，每家交易所从各自的渠道也可全权查看订单流。正因为每家交易所能从各自终端查看全面的订单信息，获取订单准确性、时间等待审计认定项都很方便。系统上的每一笔交易都有一个独一无二的 ID，交易所可以轻松检索交易相关信息，如这笔交易在统一的订单记录上是否存在、数额和时间是否正确。其他认定项比如订单记录虚高、“流动性黑洞”问题、交易引擎的运作也会通过内部的审计程序来保证交易所的良好运营。软件有两大审计功能：第一是核查订单记录的完整性（订单记录虚高情况不考虑在内）；第二是回测交易匹配引擎的有效运转。

为了检查审计认定项并同时保证各个交易所门户订单流的保密性，EXPREAD 将可能应用 Enigma 引擎（https://www.enigma.co/）或中心化的云计算系统，后者相对来说没那么安全。每个交易所将会向 Enigma 平台（去中心化的数据计算）提交各自加密货币带时间戳的订单信息，系统将运用 EXPREAD 基金会编写的算法处理。该算法具有简洁性、系统性的优势，而且完全开源。正式审计针对的两个认定项是订单记录的完整性和交易引擎的准确性。

完整性方面，审计过程保证所有交易所提交的订单都在公共订单簿上有记录。检查订单簿的一种方法是通过订单时刻（moments）来表征出其频数分布（可独立买卖的订单大小）。如果订单大小序列有时刻生成函数，则只需执行简单的计算。该功能在不同阶段可能会改变，也是提供给白标交易所拥有者的统计信息的一部分。交易所可全权查看公布公开的订单簿，可以轻松验证这些信息。

通过当前的时刻生成函数，时刻的数量是有限的，可通过以下方式计算：

$$\mathrm{E}[\mathrm{X}^{\mathrm{n}}] = \frac{d^n F_x(m)}{dt^n}\Big|_{\boldsymbol{m=0}}$$

$F_x(m)$为关于 m 的时刻生成函数函数，

$\frac{d^n F_x(m)}{dt^n}\Big|_{\boldsymbol{m=0}}$n-th 为 m=0 时$F_x(m)$的导数

即使在没有时刻生成函数的情况下（比如由于时刻未定义），前 6 个时刻应该涵盖分布的主要内容。因此，如果这些公共订单簿上的时刻和联合分布的计算时刻相匹配（单独分布的数据由交易所提交至 Enigma 系统），我们可以合理判定订单簿是完整的。

举个例子，我们可以用学生 F 分布来表征这个系列（鉴于订单大小不可为负而且可能小数点右边还有很多位，这还是比较相近的）。这个分配没有时刻生成函数，那么分布函数可以表示为：

$$F_x(x) = \frac{1}{B(\frac{n_1}{2},\frac{n_2}{2})}\int_{-\infty}^{k_1 x/k_2} s^{n_1/2-1}(1+s)^{-\frac{k_1}{2}-\frac{k_2}{2}}\,ds$$

k_1和k_2是（卡方分布的）自由度

所以整个算法可表示为：

$$if$$

$$E[X] = \frac{k_2}{k_2-2} \quad \text{for } k_2 > 2$$

$$(E[X^2] = Var[X] = \frac{2k_2^2(k_1+k_2)-2)}{k_1(k_2-2)^2(k_2-4)}\ for\ k_2 > 4)\ !=(\begin{matrix} Moment\ 1 \\ Moment\ 2\ to \\ Moment\ 6 \end{matrix}) \rightarrow$$

Complete Order Book

完整订单簿

…… …… …… …… …… …… …… ……

$$E[X^n] = \left(\frac{k_2}{k_1}\right)^n \frac{\Gamma(\frac{k_1}{2}+n)}{\Gamma(k_1/2)}\frac{\Gamma(\frac{k_2-2n}{2})}{\Gamma(k_2/2)}$$

*时刻 3-6 也代入以上方程中

为保证交易引擎的准确性，这个系统可能随机抽取任一订单（系统中每个订单都有独一无二的 ID），然后跟踪抵消订单是否在时间和价格方面是系统中最好的订单。样本量确定如下：

$$n = \frac{Nz^2 * 0.25}{\left[d^2 * [N-1]\right] + [z^2 * 0.25]}$$

n——所需样本量
N——人口规模
d——精确度
z——信心度的标准分数

所有的审计程序均嵌入软件中（对所有交易所开源）并将自动和定期执行，无需过多操作。

6. 建立交易所的流程和 EXPREAD 白标解决方案的描述

EXPREAD 提供的白标解决方案是其新颖之处，有效地将 EXPREAD 定位为首家带有统一的流动性池的加密货币交易所白标提供商。EXPREAD 提供的是一种可扩容的技术，满足不同交易所的需求，允许交易所在我们现成技术的基础上打造自己的品牌。任一设备都可访问所有白标。交易所不仅可以使用我们提供的模版，也可以基于 EXPREAD 系统搭建自己的 UI。该解决方案为新的交易所提供了易集成的开放 API，可用于风险管理以及链下交易确认消息传送系统、用户入门、KYC 系统、审计线索等。在后端，白标附在交易引擎上，自动处理订单的分发、匹配和登记。交易所只需支付云托管的运营维护费，云托管主要靠备份和应急计划来实现。由于所有的图表解决方案和功能系统都是由 EXPREAD 基金会直接托管，可以保证集中快速的软件更新和维护。为了确保整个 EXPREAD 网络能流畅地运行，EXPREAD 基金会提供 24 小时 IT 服务台咨询。

另外，该系统根据交易所提交的订单收取交易手续费用作为白标交易所的收入来源，按交易所具体情况收费。交易功能的所有软件包（下一个章节会介绍）已经集成在白色标签中，定期更新，参与订阅计划便可激活。终端菜单栏的组成和布局可按客户需求定制。功能取决于交易所选择的付费计划，菜单栏显示有固定的布局，交易所可选择激活菜单栏中相应的功能特性。所有交易所都可轻松在平台上添加广告、教育或其他内容，来满足用户需求。

品牌灵活度也是该系统的主要关注点。系统提供给白标交易所的 UI 设计包含不同组件，可通过界面分别定制修改色彩方案及布局。如此一来，交易所便可灵活测试其品牌设计，打造对目标市场最具吸引力的品牌方案。

在用户信息管理以及用户身份详细资料的登记方面，该系统将会提供一个独立的操作系统，只有交易所所有者才有权限查看和管理全部信息。除了现金账户外，EXPREAD 同时也在考虑纳入新功能，允许新用户注册模拟交易账户，做出另外一部分运行 JavaScript 脚本的登记信息。这样一来，新用户可在测试模式下加深对加密市场运作的了解。

清算通知系统用于通知交易所所有者批准把链下签名信息发送给 EXPREAD 基金会，来支持链下支付渠道系统。消息传达通过文件传输来执行，附带高度的安全性和等待时间。

要启动 EXPREAD 交易所搭建程序，交易所团队应提交申请资料包到 EXPREAD 基金会。尽职调查是申请流程的主要环节，EXPREAD 基金会将浏览所有提交的文件，如团队背景简介、目标营销策略、运营交易所的合法执照（若某特定管辖区有要求）、股东名称等。第三方机构会参与到尽职调查中调查团队背景是否可信，这份调查是独立完成的，EXPREAD 基金会不会参与其中（关系审计），以有效降低交易所和基金会勾结的可能性。

如果一个团队顺利通过尽职调查，交易所建立程序将即刻启动。交易所团队会支付启动费用来搭建布局、连接云端、建立链上的清算协议并培训交易所团队使用技术系统等。交易所的申请通过后，交易所建立时间线将具体化，技术搭建工作启动。提交申请通常在两周内会有回复，技术上的搭建需要两周。因此整个过程历时不会超过一个月。从启动到执行，这个加密货币交易所搭建所需用时是当前市场上最短的。

7. EXPREAD 交易工具介绍

提供多种技术分析和自动化策略工具包是 EXPREAD 系统的主要价值主张之一。系统旨在为交易者提供在加密资产交易操作上的独到见解。订阅半年计划的交易所可以在他们的终端激活部分工具包，使用的工具越多，订阅费越高。虽然每家交易所都可以选择使用整套工具，但我们预计不同交易所会根据自身的目标市场，比如机构投资者或私人等，作出更具

战略性的选择。由于可以灵活选择功能，交易所可以根据用户群的增长和交易所的生命周期演变来规划并逐步为用户提供的更多使用功能。

标准套餐提供：(I) 强大的市场可视化；(II) 制图； (III) 多重时间维度和工具分析；(IV) 五种以上提前搭建的技术指标。全套的工具包提供以下工具和功能：

- 实时和定制的报价：通过高端的图表分布更为全面地展现价格、市场深度和波动状况的相关数据。
- 技术指标：为满足各类要求高的技术型交易者需求，我们提供超过 20 种技术指标。该套餐包括波动指标（每小时上升／下降比率、每 2 天的前进／下降比率趋势等），趋势指标（移动平均数、MACD 等）还有宽度指标（上升／下降量比率、强力指数等）。
- 个人会计：用户可以通过自己的账户访问微型会计系统，获取历史和当前实时表现情况的分析。系统提供的模型包括所有持仓的损益、平均最大有利变动幅度、平均最大不利变动幅度（提供图表）、所持资产（货币）、表现差异等。在风险级别窗口上，交易者可以通过不同属性，比如货币、公链、国家等来深度查看其累计曝光。
- 投资组合管理工具：高级投资组合管理工具箱，集成了投资组合创建、回测、优化工具。用户可以在系统里面创建实况或模拟投资组合，还可计算该投资组合在一定时间段内的表现（回报、变量、夏普比率、相关矩阵等）。优化工具会自动调整所选货币的仓位，来优化用户的投资组合（最高夏普比率、最低变量等）。优化向导也可以利用历史数据（已优化）推导出投资组合选择，并将其他历史数据用于策略效率测试当中。

  自定义智能订单：通过集成的交叉币和基于交易量的触发机制，可以通过高级功能设置自定义订单（包括市场价成交、限价成交、止损、止损订单）。除了常规的市场单和限价单之外，用户还可以根据其他货币的涨跌情况来设置买进或卖出另一种货币的触发点（利用货币之间的滞后关系）。用户也可以设置交易量触发点 （交易额达到一定的数量便可触发交易）。所有功能都是为常规用户设计的，操作简单，高度用户友好。
- 智能市场闹钟：设置自定义的提醒功能以识别交易触发点。该闹钟也可用于净暴露，协助交易者重新定位其投资组合以维持其投币目标范围。

- 分析门户：为加密分析师提供展示自己服务的平台，他们可以在这个特别的系统上收获订阅人群和出售报告。这个门户旨在让 EXPREAD 交易终端为用户提供一站式服务，让他们更便捷地学习并做出明智的投资选择。
- 新闻推送（只读）：在终端，交易者可从主要的加密新闻平台接受短消息。此外，交易所可通过系统聘用新闻作者和其他内容生产方来为用户提供更多的增值服务。该平台的交互式开放结构（配备多功能附加组件）能使白标交易所在竞争中脱颖而出。

8. EXPREAD 生态系统上交易所的商业模式

正如前几个部分所提到的，在加密货币交易平台推广上，面向社区的交易所作用明显，这样既可增加用户群也可提升系统的流动性。它能够在保证去中心化控制和治理原则的同时实现了更高的安全性和可扩容性。该模式解决了市场孤立的问题，创建了一个网络，将交易所协同联系起来，为 EXPREAD 生态系统的扩建提供支持和资源。EXPREAD 上推出的经济激励和治理机制旨在创建一个合作、透明和互联的社区，倡导合作并实现集体的成功。

收入来源方面，EXPREAD 系统为白标交易所提供多种定价模式，交易所可以根据自身市场环境、目标客户群和所在地地域特色及竞争情况来选择合适的模式。根据我们的预期，交易所在商业生命周期的不同阶段会采取不同的定价策略，以保持其竞争力并实现增长。所用定价会登记在 EXPREAD 系统，所有交易手续费都会基于订单来源的交易所提供的市场价格。如果能提前公布并及时推出的话，交易所是可以做到灵活更改手续费计划的。此外，该系统允许 EXPREAD 交易所采取不同的定价模型促进市场良性竞争（从现有的模式中选择）。当前交易所的定价模型包括固定费用、动态定价策略和灵活的费用调度（如根据百分比、交易量、分层订阅的模式）。系统允许交易所动态改变交易费，但是有一定限度的。从博弈论的角度来说，交易所不应该（和 EXPREAD）进行价格竞争，因为这会降低他们自己的收益。同时，他们应该聚合成一个生态系统，一起与外部的交易所竞争。

8.1 EXPREAD 生态系统贷款计划

除了生态系统的合作，EXPREAD 交易所之间的网络效应将通过内部的借贷计划得以加强，以巩固它们在市场上的地位，并促进新交易所的快速增长。内部借贷计划可以让 EXPREAD 网络的交易所可以在 EXPREAD 在线平台上直接实现交易所之间的借贷，无需任何外部金融机构的参与，但需满足以下条件：透明清晰，快速高效，可审计可预测。这样一来，EXPREAD 生态系统能够更好地发挥其集体优势并占据更多市场份额。这将为贷款方提供更高的风险调整回报，降低借款方的利息，实现更高效的技术利用和创新风险管理系统等。EXPREAD 生态系统内的借贷省去了中间多个操作支出，降低成本，节约下来的部分成本将通过降低利率和高收益率的方式让借贷双方都受惠。

作为提供资本的回报，贷款方将获得借款方（交易所）的部分交易费用。该结算将通过 EXPREAD 核心进行，以确保借款方合规。和外部借贷主要不同的是，内部借贷系统能帮助网络参与者在没有信用评级和抵押品的情况下筹集必要的基金。贷款方可查看借款方的业务细节（团队背景、执行计划、目前状况等）；此外，他们可以选择分多次提供资金或与其他有意愿的贷款方合作。基于拍卖的借贷机制可帮助借款人根据贷款条款寻得最佳报价。

- 费用低：EXPREAD 借贷计划不需要过多的管理费用和行政支出，直接实现生态内交易所之间的借贷。成功的交易所可以借款给刚起步的交易所，促进其启动或加速业务扩展，同时也可以使自身利益最大化。在规定的时期内，贷款者将从借款方的交易所获得未来交易费用的某个百分比，根据双方的协议 5%到 100%不等。

- 时间快：一旦内部贷款通过审查得到批准后，借款方将在几分钟或一天内将贷款转给借款人，实现快速处理和资金分发（利用 EXPREAD 基础设施）。

- 处理高效：平台不需要像传统的银行或信用社一样需要准备大量的文件，简化了借款流程，这点尤其方便了借款方。同时，平台也会保障事后的可审计性，让贷款人对透明度安心。

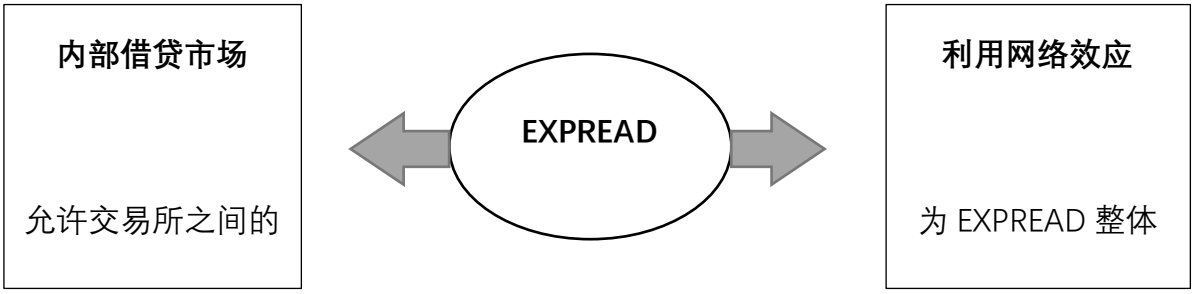
- 可审计性：提供资金的贷款方有权要求 EXPREAD 基金会对借款方交易所进行外部审计，以检查资金分配的效率和初始协议的执行情况。

- 系统透明公开：贷款条款统一并且清晰明确，确保平台的透明性，有利于长期维护交易所之间的信任，消除不必要的低效率和隐藏条款的问题。

- 投资条款：借贷模式可以满足贷款方做出不同的安排来组织资金落地形式，以减少风险（比如贷款给多家交易所实现多样化）；根据借款方交易所的历史和当前财务表现，通过多轮融资来分配必要的资金。

- 网络效应：成功融资并执行得当的项目加强了 EXPREAD 的网络效应，也鼓励了交易所之间的进一步合作，在流动性紧张情况下互助，通过占据更大的市场份额，共建 EXPREAD 生态系统的安全网。

图 8.1.1 内部借贷市场

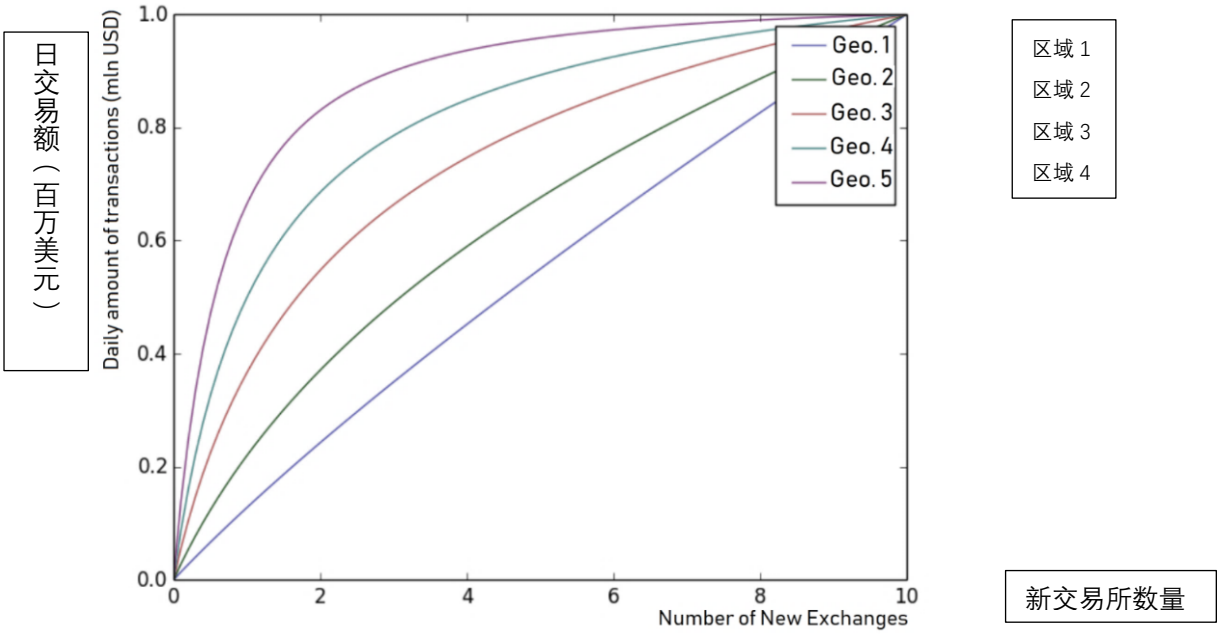


8.2 地理分布

为了保护 EXPREAD 系统中的交易所，同时确保整个生态系统地区人口均衡发展，系统将实施效益监测功能。在此功能范围内，整个交易所市场分成 25 个区（该列表会在网站上提供，交易所细节也会持续更新）。每个地理区域的总用户信息、订单数量和交易量都会被记录下来。

每个地理区域开设新的交易所后，新用户和老用户（换了交易所）的数量都会被记录下来，以便更好地评估市场状况。如果这个系统检测到两间交易所竞争过于激烈的话，Expread 可能会暂时（或永久）停止在特定地理区域新交易所的注册。总体而言，每个地理区域的需求可能会呈现以下边际递减趋势的函数形式：

图 8.2 不同地区交易所数量的需求弹性



不同地理区域的日常交易规模对该区域的交易所数量增加的弹性有所不同（见图 8.2.1 中的五个交易所区域）。为了监控交易所之间的潜在竞争，地理区域是根据同一国家领土当前的竞争强度而划分的，同时也需要考虑代理位置的竞争是否相对较低（比如在另一个国家没有交易所）。

计算矩阵的校量方式将帮助当地的 EXPREAD 生态系统优化同行竞争成本和扩容效益。同行竞争的成本定义如下：老用户的 KYC 被新开的交易所（同个地理区域）获得，考虑其交易量的多少；或者是（由于新交易所的进入）特定交易所的交易量损失多少。效益的多少取决于新交易所加入后的区域整体交易量增长。为了优化这个过程，计算公式假设如果分段中最后一个交易所同行竞争的边际成本（MCC）大于或等于边际扩容效益（MEB），那么这个地区的将暂时或永久禁止新交易所加入。

$$MCC = \frac{dCC}{dN} \geq \frac{dEB}{dN} = MEB$$

其中，N 为该地理区域交易所的数量。

我们需要中心监控来保证当新交易所加入网络的时候，他们锁定的目标群体和用户群不会和其他交易所发生同行竞争，而是注重原始用户的参与。

9. 代币和治理的经济模型

本系统旨在利用代币经济模型促进 EXPREAD 的发展，为交易所创造拉动机制，协助去中心化、以用户为中心的生态系统管理。通常，代币的功能分为三大元素：特定用户效用、生态系统的内部货币和管理工具。

对终端用户来说，用 EXC 代币交易可享有明显折扣。特别是在交易量大和交易频率高的情况下，代币对用户的效用更高。折扣模型应用简单的机器学习处理来优化白标交易所的快速回报／高利润和代币持有者所享有的折扣之间的权衡。折扣力度取决于所持代币量，如果持有的数额达到一定数量，折扣可能会达到 100%。因为代币发行量非常有限（仅 2100 万），所以代币的需求和效用将随着生态系统流动性和共享订单簿的深度而不断增加。按折扣所节约的成本来看，行动的越早，获得的价值更大。

外部代币持有者的第二个好处是，他们可以通过代币为交 易所或整个 EXPREAD 生态系统提供服务。 服务内容包括为交易所提供专门的新闻推送或者是撰写关于加密货币的报告和投资咨询文件，也可能关乎与交易所本身直接相关的需求，比如设计修改、广告营销和推广计划等。在 EXPREAD 基金会官网上，我们将有专门的版块来发布不同交易所的外包工作信息，协助代币持有者参与到社区里 。

除了代表折扣优惠外，代币同时也是 EXPREAD 生态系统的内部货币。平台上的维护费、在终端订阅功能的费用和交易所之间的内部资源流动（交易所之间的借贷）都会用平台代币来执行。外部用户所提供服务的报酬也是使用 EXC 代币。

如上所述，EXPREAD 生态系统旨在实现以用户为中心的治理。EXPREAD 基金会有战略性治理功能，如协调各交易所的运作和把握生态系统的总体发展。交易所所有者和代币持有者对功能和具体协议方面的决策都有很大影响力。他们提出升级方案并投票决定，系统据此运行流程治理。只有交易所所有者、EXPREAD 基金会和部分代币持有者（代币持有量大且有既定利益）才有权力提出方案进行公开讨论和投票。所有代币持有者都可以参与到投票过程当中，以选出对生态系统最好的方案。

EXC 代币另一个特点就是在后 ICO 阶段的发行机制(为了推广, 部分代币会用于发行)。我们称这个代币发行机制为“交易证明”。代币的发行和比特币协议类似（每十分钟发行 12.5 EXC 代币），发行数量递减（与比特币发行计划挂钩）。

对个人用户而言，代币的发行取决于（单个用户的）交易量、生态系统的总交易量和交易所用于发布订单的交易所指数。

$$Distribution\ to\ an\ end\ user = \frac{ex.Index\ *\ user\ trading\ volume}{sum(\ trading\ volume\ of\ the\ exchange * ex\ Index)}$$

$$终端用户代币分配 = \frac{ex.指数 * 用户交易量}{sum(\ 交易所交易量 * ex\ 指数)}$$

在公式中：

- 用户交易量和交易所交易量由所有完成的加密交易（由 EXC 代币体现）决定。
- Ex 指数表示所用的特定网关的特征。

为了对交易所进行区分，系统会根据交易所加入 EXPREAD 生态系统的时长定期把它们指数化。新建的交易所会享受代币发行的优惠待遇，为它们的用户提供更大的发行量。采用这种方式是为了推动新交易所的发展。

参考文献

[1] Sprites and state channels: Payment networks that go faster than lightning, Andrew Miller, IddoBentov, RanjitKumarsen, etc., 2015.

[2] The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, Joseph Poon, Thaddeus Dryja, 2016.

[3] How to use bitcoin to design fair protocols, IddoBentov, RanjitKumaresa, 2014.

[4] An open protocol for decentralized exchange on the Ethereum blockchain, Will Warren, Amir Bandeali, 2017.

[5] A fast and scalable payment network with bitcoin duplex micropayment channels, Christian Decker, Roger Wattenhofer, 2015.

[6] Electronic Communication Networks and Liquidity on the Nasdaq, James Wetson 2002.

[7] Trade classification algorithms for electronic communications network trade,BidishaChakrabatry, Bingguang Li, VanthuanBguye, Robert Ven Ness, 2007.

[8] A fast and scalable payment network with bitcoin duplex micropayment channels, Christian Decker, Roger Wattenhofer, 2015.