介绍

我们认为不断询问自己为什么要做人和事是至关重要的：这样才好能理解为什么任何特定的解决方案以某种方式构建，以及首先为什么它被构建。因此，我们在文档中解释了为什么我们的产品是按照它现有的构造方式构建的，以及为什么我们最终使用区块链技术作为我们产品的支柱。

在本文中，我们希望更进一步，放大现代区块链解决方案的一个方面：代币经济。在此，我们再次问我们自己，为什么象征经济体是以现有的特定的方式设计的，为什么它有存在的必要。
每当引入新代币时，我们最终都会构建一个新的微型货币系统。在该系统中，所用技术的功能固有地与代币的价值及其使用相有关联，因为代币值与网络的安全性相关。在基于Proof of Stake（ “PoS” 权益证明）的系统中尤其如此。在与区块链项目合作很长一段时间后，我们发现 “代币经济” 是我们遇到的许多项目中最容易被忽视的设计步骤之一。代币往往简单地用于筹款，通常情况下，代币结构似乎与项目相关联，可有可无。

本文旨在说明我们创建的一个健康的区块链项目的方案，而该项目具有代币经济与解决方案运作之间的自然相互作用。我们将引导您完成从开发业务解决方案到构建全新代币经济的过程。在此过程中，我们将涵盖代币的功能和奖励机制。我们希望能向大家展示如何在LTO网络上创建和获取价值。

产品的设计及演化

早期的产品设计

LTO Network的故事始于2014年，由文档引擎的最小可行产品（MVP）逐渐演变为工作流程引擎。随着时间的推移，我们的客户群变得越来越大，流程也更加全面。 作为流程的服务商，我们成为了系统用户值得信赖的第三方。如果我们存储的数据被人为操纵了，相关组织可能会受到严重影响。 因此我们不能仅仅指望信任。 利用官僚主义或许会有所帮助，但这样会扼杀工作效率。接着出现了区块链技术，它具有在不影响生产力的情况下同时解决所有这些问题的巨大潜力。

意识到它的潜力之后，在我们开始将这项新技术应用于我们现有的业务解决方案之前，仍然需要做好准备工作。我们开始咨询不同行业的客户，例如供应链，保险和医疗保健，并询问他们对区块链技术的期望，以及哪些流程可以数字化并放在区块链上。还有法律和合规发展需要考虑进去，例如欧洲经济区内的数据保护法GDPR以及自2018年7月以来美国的新的隐私保护法。

我们最终设计了一个分布式业务流程管理引擎，而该引擎能遵循有限状态机逻辑的ad-hoc私有链。我们需要将系统锚定在公共分类帐本上，以提高数据完整性和安全性。但当我们继续尝试不同的公共分类账本时，问题开始出现了。

早期产品设计的一些问题
我们看到的大多数公链都有以下的技术缺陷：慢，昂贵且不适合在区块链上锚定事件。我们以代币化许可证的形式设置代币功能。它类似于Microsoft微软软件，区别在于我们的微型区块链工具包可以免费下载。然而只有你在证明自己拥有许可证的情况下才能安全访问区块链。在钱包中锁定的某些预定义数量代币将代表此类许可证。

虽然这种设置在技术方面上可行，但离完美还差得远。我们不得不依赖特定的公共分类账本来运行服务，而这又需要持续的支付交易费用。除此之外，代币并未真正体现解决方案的价值，因为网络功能的一部分依赖于我们无法控制的公有链。实际上，代币模型似乎仅仅出于它自身目的而存在，而不是为底层系统服务。社区对生态系统增长的激励措施非常有限。我们试图用折扣代币模型，但结果并如不人意。

我们遇到的大多数代币模型似乎都附属于项目，且主要目的用于筹款。通常也不提供经济激励措施。据了解，在设计代币经济时，经济激励应该是主要的优先事项。应根据解决方案的采用策略的需要来量身定制激励措施，并将其作为整个项目不可分割的一部分。因为公司在日常运营中引入新技术需要很大的勇气，特别是像区块链一样具有破坏性和很新的技术。因此，向他们展示采用此技术的经济利益和促进实验就显得至关重要了。而这只能通过提供经济激励来实现。我们设计的第一个产品在这方面缺乏发展，因此我们用了新的设计。在该设计中，激励机制不仅构成LTO代币经济的重要组成部分，且是整个LTO网络的重要组成部分。
在接受现有的公共分类账本不适合我们预期的目的之后，我们决定建立我们自己的去许可的公共分类账。这也将我们的生活变得更容易，原因有两个：

1. 它允许我们向公链添加新功能，并以固有的方式和根据路线图来进行配置。由于公共分类帐是为锚定而构建的，因此无需资产创建等额外功能，因为它们只会篡改了主要用例。
2. 这种设置使我们不仅可以试验代币模型，还可以建立一个适当的微型货币体系，当一个公司加入时， 用起来也更有效率。

这就是经济学，笨！

权益奖励机制模型的好处
现代软件即服务（“SaaS”）解决方案通常基于多年提供合同，无论使用何种情况都收取固定的费用。当然会有一些例外情况，但一般的想法是，顾客会被绑定一段固定的时间，然后无论他的实际使用情况如何都要付费。LTO网络采用的是不同的方法。用户自愿使用网络服务。我们允许用户在他们选择时停止使用，并在此期间免除他们的付款义务。因此，我们设法使用代币经济学和激励来为我们的网络创建高效灵活的用户模型。

为了实现这一目标，我们决定在我们的奖励机制模型中采用PoS的概念，以此来控制公司进入网络的新条目。这是我们的“内部突破” 。根据PoS奖励机制，选择验证者的可能性与其权益相对于权益代币总数的比例成正比。如果他的权益占权益代币总数的5%，他将有5%的可能性被选中来验证该区块。然而，这将意味着用户仅被授予持有代币，而不一定用于使用他们。这就是我们添加 “重要性证明”概念的原因，该概念奖励代币的实际使用。我们将在第四章对此进一步解释。

以上所述就导致了新代币模型的产生，该模型基本上允许网络基于可预测的定价模型向用户收费，因为每个用户的设置提供了他们在特定时间段内在网络上进行的交易的统计数据。

每个用户都知道他们自己拥有的客户和合作伙伴的数量，并且他们已经收集了他们所做交易量的情报和统计数据。这使得预先确定它们在固定时间段内将要运行的交易数量变得非常简单。此信息的使用能允许用户计算他们在这段时间内未来需要使用的网络百分比。通过获取网络中总权益代币的相同百分比并对其进行固定，用户可以使用LTO网络解决方案净零，而无需担心持续而经常性费用和付款。

我们的模型取决于网络用户的特征。此后我们将进一步阐述不同类别的用户。

LTO网络的用户类型

在LTO网络代币经济中，我们可以区分4种类型的代币持有者：

- **集成商与合作伙伴** -- 网络中的权益持币者，运行节点以验证交易。他们可以代表自己或代表客户行事;
- **客户** -- 使用网络和支付交易费用的参与者，偶然运行节点；
- **被动式权益人** -- 将投入代币（可能通过租赁）并运行节点以验证交易的参与者；
- **非活跃持有者** -- 网络中的非活跃参与者，只需持有代币。

“集成商和合作伙伴”和“客户”都被标记为网络中的“参与者”，并被视为LTO网络经济中的核心参与者。由于他们是网络的用户，他们有直接的动机去关心其稳定性和功能性。因此，我们的目标是在参与者持有的约80%的成熟阶段进行代币分配（见图1）。

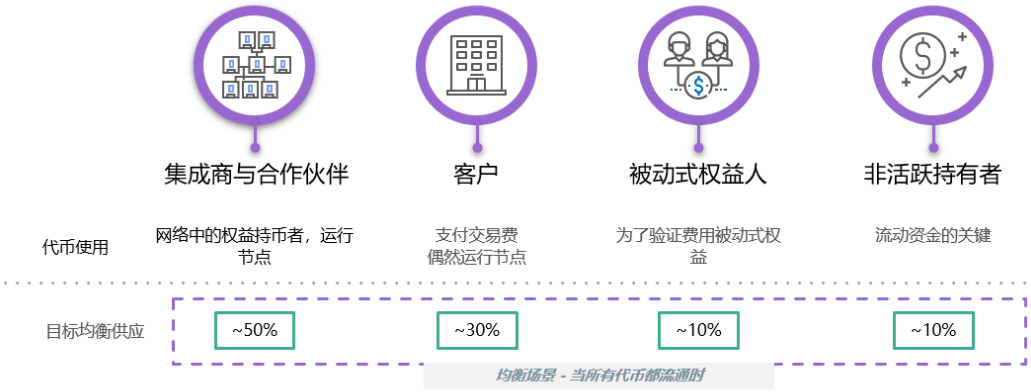


图: 成熟阶段的目标代币分配

Figure 1 成熟阶段的目标代币分配

在网络中的四类参与者中，非活跃持有者最不可能使用网络。它们不会生成交易，也不会使用其代币来验证事务。“集成商和合作伙伴”，“客户”和“被动权益者”可归类为“活跃用户”，并根据其在网络中的总体利益百分比绘制成矩阵（图2）。

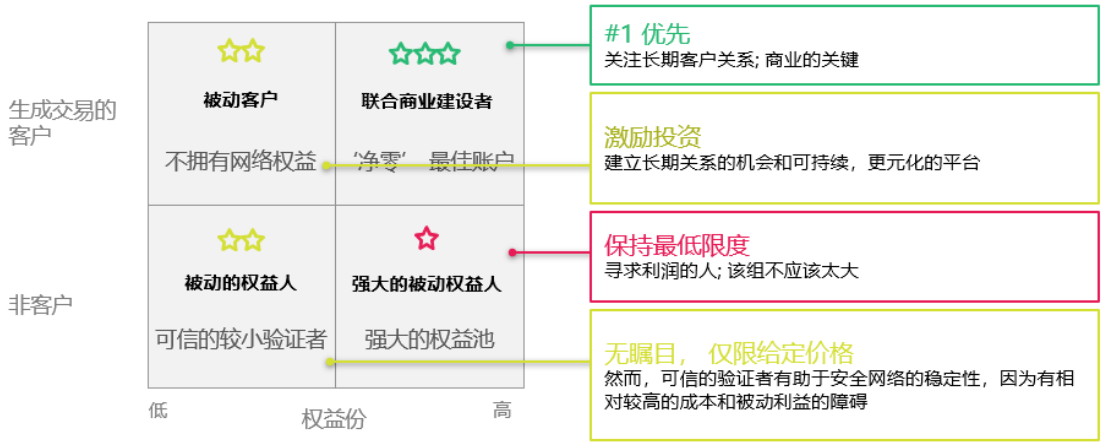


*Figure 2 LTO*景光的参与者与权益持币者

网络的四类用户可以描述如下：

- **强大的被动权益人**在平台中拥有很大比例的整体股份，但不会产生交易。他们运行一个节点来验证交易，然后接收交易奖励。
- **被动的权益人**是较小的（个体）参与者，持有代币，目的是在未来以更高的价格出售，以较小的百分比来支持网络。
- **被动客户**运行交易并使用该平台进行其服务，而不实际拥有网络权益。请注意，如果交易费用变得相对较大，这些客户将因使用该平台而产生大量运营成本。
- **联合商业建设者**是积极参与并与网络有利害关系的客户。

我们考虑通过刺激网络中的早期采用，参与和主动持币来达到均衡阶段。我们用

刺激这种行为的方式来设计我们的代币经济，以助快速达到均衡阶段。联合业务建设者将受益于我们的奖励机制，因为他们有助于平台的隐含价值，确保平台可持续但逐步使用网络并在中长期创造价值。

奖励机制： 从LPoS到LpoI

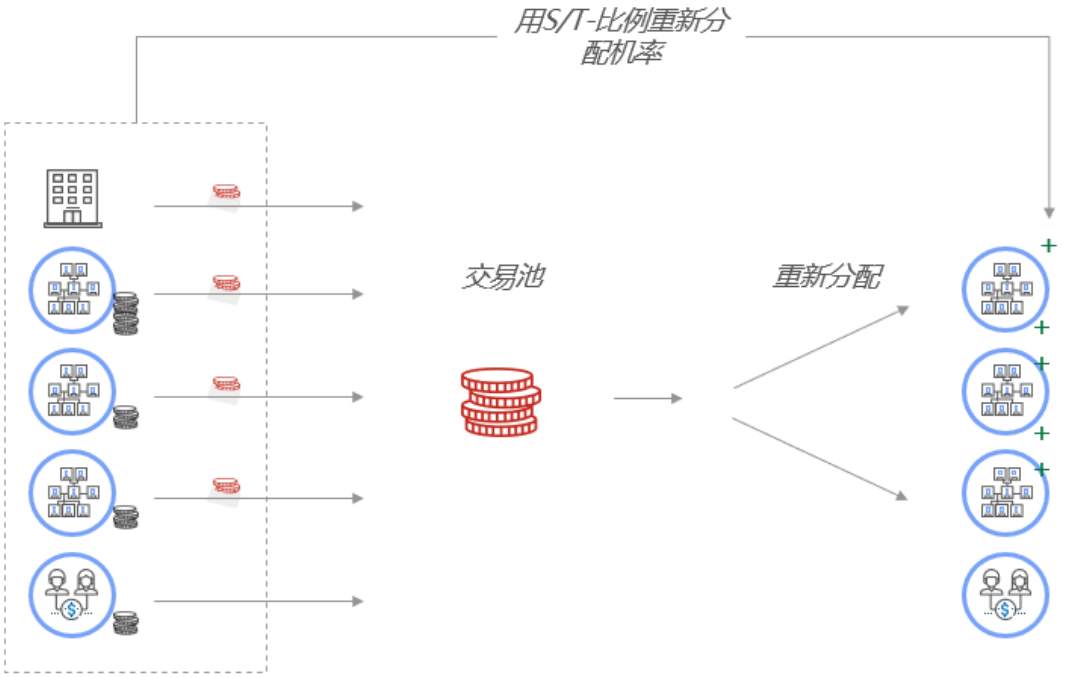
正如技术论文所概述的那样，现有的基于PoS的方法导致了中心化和大量强大的被动持币方式。给节点建设权益持币数量限制只会导致一种（sybil）女巫攻击：系统中会有更多的节点，但他们仍然只有一个操控者。因此，我们希望能避免这种情况，并为联合商业建设者提供更好的激励措施，在经济方面上阻止强大的被动的权益人，因为它们不会给网络带来任何价值。

我们将WAVES的租赁证明（“LPoS”）概念与NEM的重要性证明（“PoI”）概念相结合，并将我们称之为 租赁重要性证明（“LPoI”）的概念实施到我们的奖励机制中。“租用”部分允许小型代币持有者和持有代币的人 - 但不想运行节点 - 仍然可以获得支持网络的奖励。“重要性”因素可确保活跃网络成员获得的奖励多于被动奖励者。您可以在此处阅读有关DPoS / PoS / LPoS差异的更多信息。

从公司的角度来看，这可确保他们在无需购买或拥有代币的情况下运行本产品。他们可以简单地分离一个节点并吸引那些想要租用其代币的人，将模型从被动的持有者变为有用的网络参与者。

为了根据交易的百分比来激励权益，我们将验证的机会倾向于那些通过贡献交易实际使用网络的代币持有者（见图3）。在以下示例中，贡献对验证概率的影响变得清晰：

- 如果用户持有锁在网络上的代币总数的10%，并占总交易量的10%，则他的验证机会将高于10%。
- 如果用户持有总代币供应量的10%，但没有提供任何交易，则他的验证机会将低于5%。



图：LPoI 共识算法概念例子。 黑色硬币代表该受益量通过一方， 而红色的硬币代表交易量。

*Figure 3*图3： 概念例子 *LPoI* 共识算法。 黑色硬币代表该受益量通过一方， 而红色的硬币代表交易量。

为了确定持币与交易的平衡，它们的比率（“S / T比率”）公式如下：

$$ST\ ratio = \frac{Staked\ tokens\ as\ \%\ of\ total}{Contributed\ transactions\ as\ \%\ of\ total}$$

Raffle factor 抽签因子

S / T比率将与“抽奖因子”相关。 抽奖因子是一个数学公式，它影响节点被选择验证的机会。 抽奖因子将使用以下公式计算，最小值为1.0，最大值为1.5。由于重要性虚假增值，该最大值被选择为最小值和绝对最大值之间的中间值。

S / T比越均衡（～接近1.0），抽奖因子就越高，最大值为1.5。如果S / T比率不平衡（节点不提供任何交易），则相关的抽奖因子将为1.0。由于钟形曲线具有较大的标准偏差，因此在达到净零效应时，可确保活动客户的稳健性和可预测性。交易基础的潜在变化对净零头寸的影响相对较小。如下图4，抽奖因子的图形表示。

$$Raffle\ factor = 1 + (0.5 * e^{-\frac{(STratio-1)^2}{2}})$$

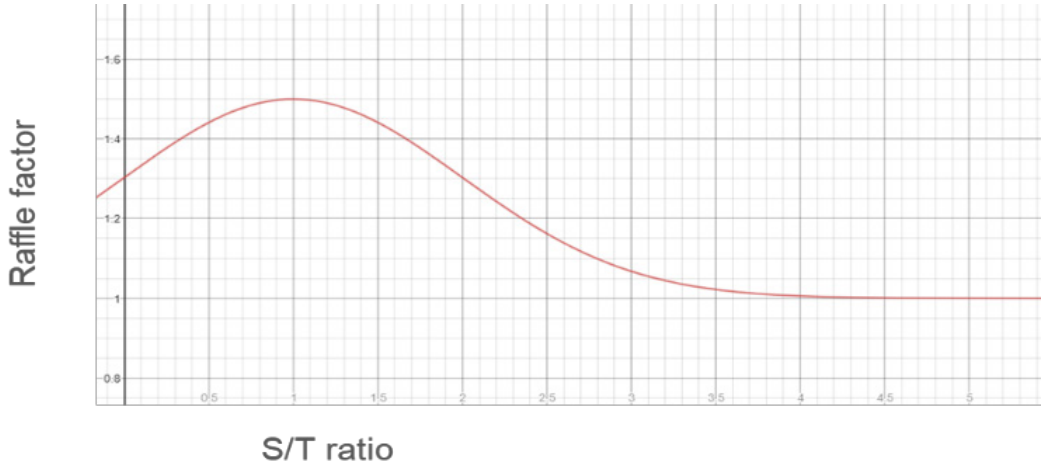


Figure 4. 图*4*：作为*S / T*比函数的抽签因子的表征图。

User	Balance	%	Transaction volume	%	S/T ratio	Raffle factor	Effective balance	P(forge)	Expected payout	Return on stake	Net profit
1 - Passive client	0	0%	350	35%	0	1.30	0	0%	0	n/a	-350
2 – Disproportionally large stake	8000	40%	200	20%	2	1.30	10426	39%	391	4,9%	191
3 - Client with balanced stake	4500	23%	250	25%	0.9	1.50	6739	25%	253	5,6%	3
4 - Client with balanced stake	4000	20%	200	20%	1.0	1.50	6000	23%	225	5,6%	25
5 - Passive staker	3500	18%	0	0%	n/a	1.00	3500	13%	131	3,8%	131
	20000		**1000**				**26665**	**100%**	**1000**		

如表1所示，用户2和3具有最平衡的利益和交易。他们的S / T比率接近1，产生一个高的抽奖因子（1.5）。因此，系统为它们分配了比用户1，2和5相对更高的有效平衡。有效平衡用于公平权益证明算法，它确定了伪造块的机会; P（锻造）。

由于抽奖因子较高，用户3和4成为验证者的机会增加了；分别从23%和20%到25%和23%。相反，作为被动锻造且不进行任何交易的用户5成为验证者的机会下降了；从18%到13%。

根据稿的数量，可以计算出预期的支出。这表明，尽管用户必须支付交易费用，用户2,3和4因其获得的奖励而产生利润。用户3和4的放样回报最高，因为它们具有良好平衡的S / T比。

重要性虚假增量

在构建这个系统的过程中，我们必须注意游戏的可能性。一种是通过垃圾交易。我们可以将垃圾交易的利润/损失计算为最大抽奖因子的公式;

- Raffle factor; r
- Percentage of staked tokens; S
- Cost of a transaction; c
- Total transactions on network; Γ
- Spam transactions: τ
- Rewards: p
- Profit/loss from spam: $\Delta p = p_{r=rmax} - p_{r=1}$

$p = (r \cdot S \cdot \Gamma \cdot c) - (\tau \cdot c)$
with $r = 1, \tau = 0 \Longrightarrow p = S \cdot \Gamma \cdot c$
with $r = r_{max}, \tau = S \cdot \Gamma \Longrightarrow p = (r_{max} \cdot S \cdot \Gamma \cdot c) - (S \cdot \Gamma \cdot c) = (r_{max} - 1) \cdot S \cdot \Gamma \cdot c$

This gives

$$\Delta p = ((r_{max} - 1) \cdot S \cdot \Gamma \cdot c) - (S \cdot \Gamma \cdot c)$$
$$= ((r_{max} - 2) \cdot S \cdot \Gamma \cdot c)$$

Given $s > 0, \Gamma > 0, c > 0$

$\Delta p < 0 \Longrightarrow (r_{max} - 2) < 0 \Longrightarrow r_{max} < 2$

这证明在最大抽奖系数小于2的情况下， 直接从垃圾交易中获取利润是不可能的。接近2的抽奖因素将使垃圾交易几乎免费。免费或低费增加在网络的重要性是不太理想的，因为它可以帮助攻击者试图以51%的攻击力破坏网络。 1.5的最大抽奖因子确保了虚假增量重要性的高成本。

摘要块
为了解决区块链在数据存储容量方面的增长问题，我们引入了一种额外的区块类型；摘要块。这些块大约每天生成一次。技术论文里会详细解释其推理和细节。

为了激励节点参与创建摘要块，只有97%的交易费可被用于锻造密钥区块。其余3%的交易费用保留用于锻造摘要块。

产生的用户动态

由于对联合商业建筑商（拥有均衡股权和交易比率的客户）的相对较大的回报，我们预计客户将在平台上购买相当大的股份，以获得“净正”利润。这样，进行交易就没有边缘成本，从而激励了平台的采用。

预期的动态如图5所示。

- 被动客户转向联合业务建设者，因为他们被激励并将相似比例的代币作为其交易比例：由此降低了他们使用平台的边缘成本；
- 被动客户从（强的）被动式锻造者那里购买代币，因为被动式锻造者的回报相对较低；
- 当平台上的活动客户端数量增加时，被动受益池将耗尽。
-

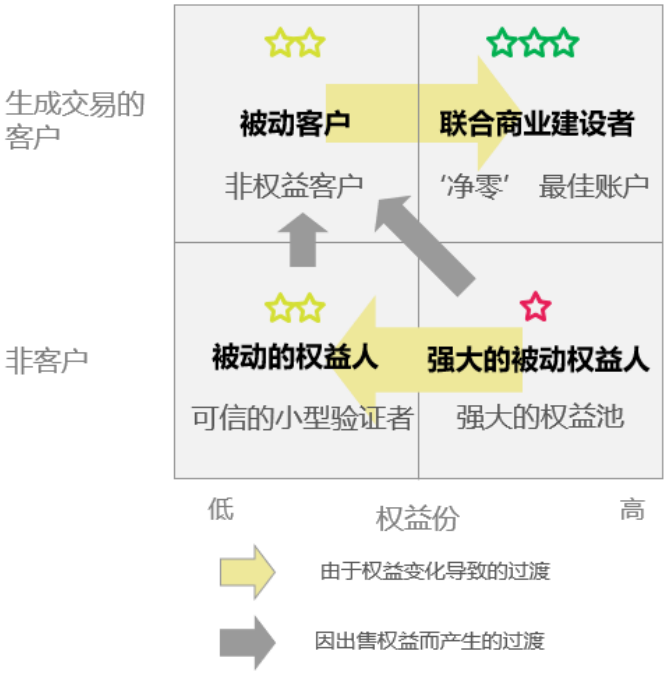


*Figure 5*图*5*：市场发展过程中的利益相关者动态。

平台采用和动态随着时间的推移

LTO网络经济中的这些动态将随着时间的推移而发生在四个不同的阶段 发展，成长，动摇和成熟。市场发展的速度在很大程度上取决于代币价格变动，交易价格和早期采用率。我们估计在3 - 5年内达到市场成熟期。四个阶段的描述如图6中。

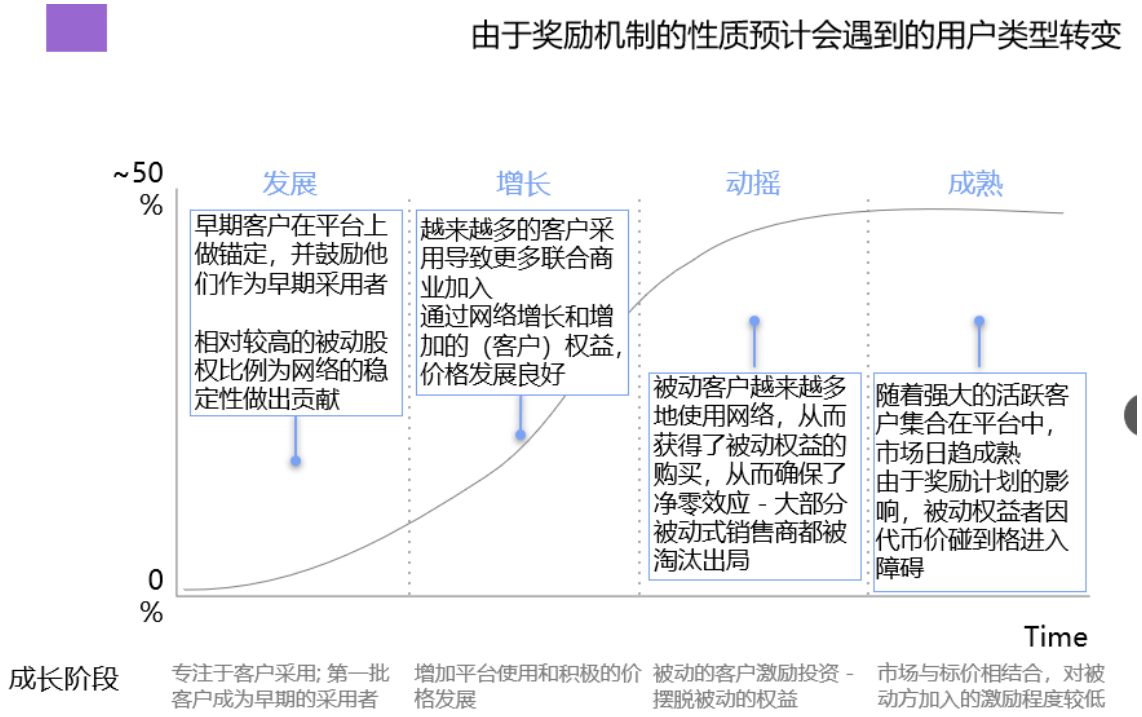


*Figure 6*图6：平台开发到市场成熟。

经过四个阶段，由于奖励机制的性质，我们预计会遇到用户类型的转变（见图7）。在开发阶段，直接在代币销售之后，将会有相对较高的被动股权比例。早期采用客户的目的是迅速进入净零点，因为相对较低的代币投资将为他们的交易量带来净正回报。在增长阶段，平台采用率的提高会导致（被动）客户端的增加。

由于解决方案的性质，客户不太可能每月都购买代币。相反，我们希望他们选择在LTO网络中占有一席之地，将运营的成本降低到零，或者通过拥有网络一部分的集成商来使用不同服务。被动客户将逐渐从大型被动式移动端购买代币。随着淘汰和成熟阶段的进行，由于客户和集成商越来越需要运行其节点的权益，权益池因此而耗尽。

防止投机破坏经济假设

波动性仍然是一个需要在本系统中解决的问题，因为我们不能允许投机篡改可预测的定价模型。如果很多人在不使用网络的情况下随意投入和重新投入代币，则会影响预测网络部分的经济设置，从而影响公司需要运行净零的代币数量。因此，在系统至少达到早期成熟阶段之前，我们将在主网和ERC-20代币池之间引入一个名为“Bridge（桥）”的概念。

两个池都有不同的用途：

- 主网池旨在用于网络的实际使用：为平台投入或支付交易并用作功能作为平台的实用程序代币
- ERC-20池主要用于流动性，也是公司加入网络的网关。

Bridge将管理两个池之间的流量。随着市场的成熟，此桥的目标是确保稳定和逐步采用和流入主网。为此，在从一个池向另一个池转移代币时，将指定一名Bridge Troll （桥梁巨魔）收取费用。桥梁巨魔费用会被烧毁，以确保在网络发展阶段大型锻造者的交易不会对价格产生巨大影响。

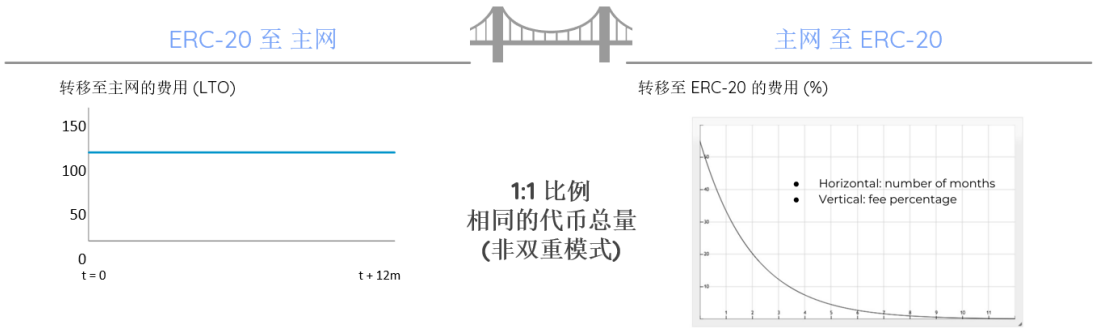


*Figure 7Bridge Troll*费用随着时间的推移。

从ERC-20池迁移到主网池，Bridge Troll将收取每笔交易100个LTO网络代币的固定费用。这个小障碍不会阻止网络（客户，集成商）的实际用户将流动性转移到主网，但会阻止投机者和小型被动主体转向主网。

从主网到ERC-20，Bridge Troll将根据与开发路线图相对应的曲线收取费用。随着平台成熟并且市场受到更多教育，价格波动不再会带来负面影响的威胁。在此之前，费用曲线将减少随机存储并且不使用网络。这保证了可预测的定价模型的假设仍然存在。

代币价格波动会阻止公司加入吗?

我们将锚定交易价格设定在能够为代币价格增长留出空间的水平。这意味着如果代币价格上涨，系统设置仍将确保激励公司加入网络，因为它将降低运营成本并具有竞争优势，而不是其他现场解决方案。

然而这里还存在一个潜在的问题，即代价越来越高，由此成为公司进入市场的障碍。与任何区块链一样，用户可以将费用设置为其想要支付的金额。挖掘块的节点可以选择是否接受它。市场将因此达到均衡。在这种情况下，节点协调人倾向于降低费用，否则会阻止更多人加入网络，从而对网络的当前参与者和那些确切的节点协调者产生负面的经济影响。

价值创造和获取

大多数区块链项目都在创建非许可的公共分类账。由于后勤和法律问题，商业，企业和政府不愿意甚至无法利用这些。这些限制是公共部门采用该技术的障碍，而公共部门又是一个巨大的市场。根据像麦肯锡这样的报告，公共部门是迄今为止区块链采用的最大用例。

到目前为止，区块链技术所发生的情况是私人公司使用私有链。而公链迄今所看到的唯一用例是dApps（dAPP的现状：每日活跃用户数量非常低），或者他们仅作为ICO的收款平台。

尽管去许可的公有链的未来仍然存在，但公共部门却无法为其业务目的充分优化它们。

代币及无代币

私有链不使用代币。相反，网络值在所选公司集团的权限中表示。换句话说，对网络的访问是排他性的，并且基于管理方的某些标准。

随着管理结构的建立和行业的采用，授权方几乎没有经济动机来通过增加新成员以重新分配权力。由于能够接受或拒绝新加入的人员，这种设置可能会导致卡特尔。

在许可公有链上，特别是在PoS的情况下，网络具有在底层代币所表示的经济价值。如果代币是公开的，任何人都可以加入网络并成为验证者。

分层解决方案

那么LTO网络与其他项目有什么不同？关键在于产品是私有层和公共层的组合。私有层授予组织将区块链应用于其业务所需的所有工具。公共权限层提供了保护私有层的数据完整性的去中心化方法。

经济价值实际上存在于基础公链中，其中网络的访问和“共享”在全球范围内分布并以代币表示。这种设置的结果就是网络平台的采用，通过私有特设链中的解决方案引入网络，基于本文前面的经济假设对代币值产生直接影响。

公司集成商在经济方面受到激励，成为联合业务建设者，并获得了股权网络的一部分。该产品由私有层和公共层组成，创建并获取价值：私有层从业务角度创造价值，而公共层从经济角度来获取利益。