Tokenlon Protocol Litepaper V1.0

2020 年 12 月

ben@token.im | kai@tokenlon.im | lucas@tokenlon.im

Tokenlon

Protocol Litepaper V1.0
2020 年 12 月

Ben He ben@token.im
Kai Chen kai@tokenlon.im
Lucas Huang lucas@tokenlon.im

介绍

Tokenlon 是基于区块链网络实现的去中心化交易支付结算协议。

它秉持了区块链去中心化网络的特性

- 无许可：任何人在任何地方，可以无需许可地访问使用
- 零信任：基于智能合约摆脱第三方信任，透明安全
- 抗审查：无法被阻止的基于加密货币的价值转移
- 健壮性：7x24 无间断、无单点的作业

随着去中心化金融协议（DeFi）的创新发展，我们看到了货币市场、借贷市场、交易市场、支付网络、保险市场、衍生品市场等在区块链网络逐渐形成。不过各种协议还仍在持续演进，不同协议之间也存在产品体验差异、流动性割裂的问题。

得益于智能合约开放、可编程、可组合的特性，Tokenlon 将跨网络地整合各类成熟金融协议，在其之上构建全局化的结算协议层。Tokenlon 将作为应用端交易和支付的基础设施，与生态合作伙伴一起创造健壮且丰富的全球金融市场。

我们希望通过社区共建，为开发者提供全局统一的标准化访问接口，为用户提供简单易用的操作界面，让每个人都能自由平等地使用开放式金融服务。

起源

Tokenlon 作为项目代号，起源于 2017 年，旨在去中心化钱包内实现币币交易，同时团队也希望 Tokenlon 在未来能够成为去中心化支付的基础设施，在不同网络、不同币种之间实现实时支付结算。

如今，加密货币支付场景尚未到来，但去中心化交易（DEX）已经逐渐开始被市场认可且接受。流动性作为金融市场最重要的组成部分，DEX 的成功与否将直接关系到开放式金融能否革新传统金融，也将影响加密货币成为更普惠的价值存储和支付工具的节奏。

Tokenlon 4.0 是基于 0x DEX 协议改良的链下做市商报价（RFQ）、链上结算的交易模式，为用户提供了无需信任、无滑点、无抢跑的交易体验。自 2019 年 7 月上线以来，Tokenlon V4 已帮助 12 万用户完成累计 40 亿美元交易额，链上结算成功率 99.8%，遥遥领先其他 DEX 协议。

初心未改，我们仍将继续改进 Tokenlon，使之成为开放式金融的支付结算基础设施。

未来

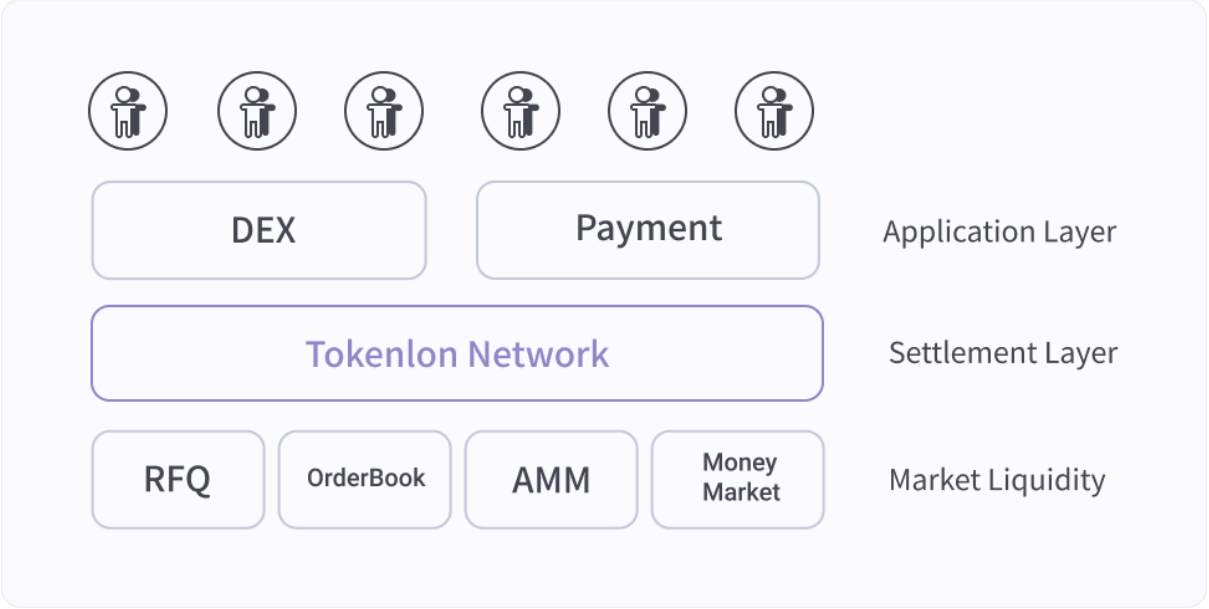
经过三年的探索实践，Tokenlon 已经完成了第一个里程碑，让钱包用户简单可靠地完成币币交易。这过程中少不了早期用户、核心团队、Kyber 团队、0x 团队、做市商等合作伙伴的支持。下一个里程碑，我们需要，也期待与更多的贡献者一起构建。

Tokenlon 致力于成为全球金融市场的基础设施，开放包容地连接区块链生态。去中心化社区发展是其必经之路，一个设计良好并能动态演进的代币经济机制，能够促进各方参与者一起贡献打造开放式网络协议和社区生态。

LON，将扮演这个至关重要的角色，Tokenlon 也将开启去中心化社区治理之路。

系统架构

分层架构



Tokenlon 协议定义了为用户提供支付和交易结算的金融服务网络，本质上是通过连接用户与流动性市场达成安全、高效、低成本的交易。

流动性市场的供给方不仅是多样性的，也是割裂的，甚至充满不确定性风险。
用户需求的满足要求解决时间、信息、标的、支付媒介等的不对称性。

Tokenlon 通过三层结构来满足各方需求：

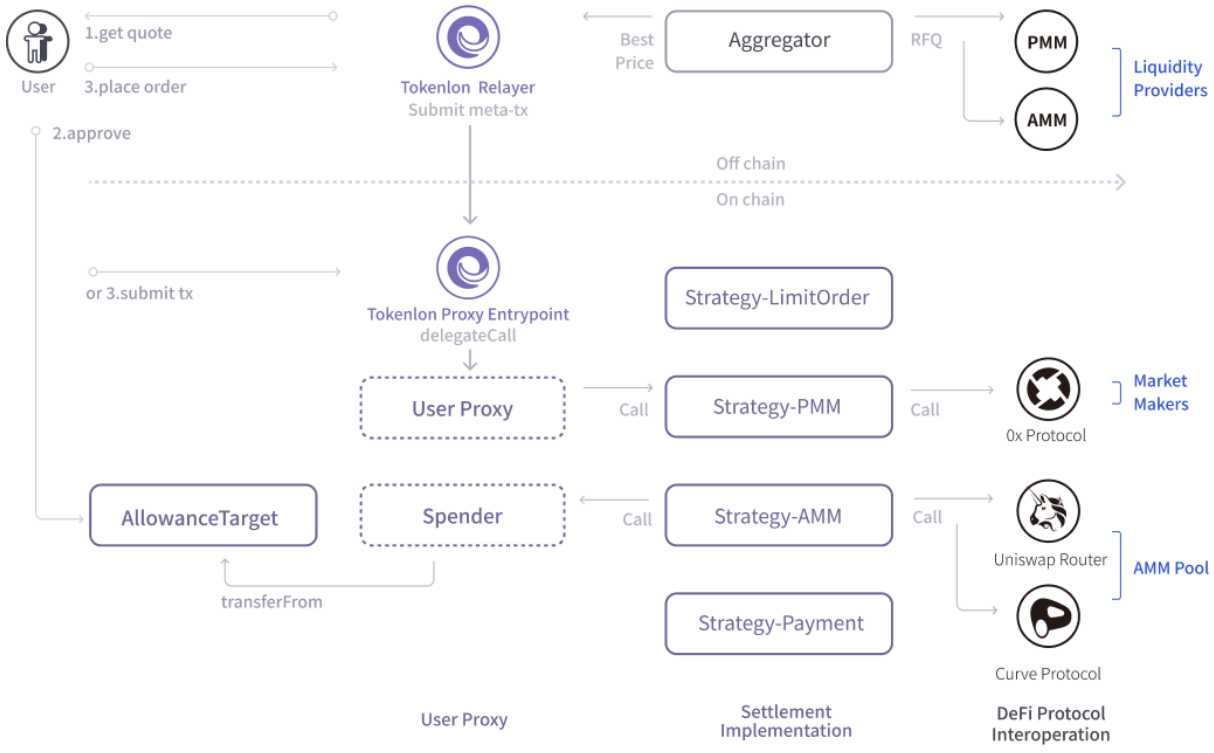
Market Liquidity（流动性市场）
通过智能合约定义不同流动性源的结算策略，不仅可以通过聚合不同流动性源来创造最佳交易价格，同时解决未知的对手方风险。合约的原子结算，确保了交易双方可在无需信任的条件下达成交易。

Settlement Layer（结算层）
Tokenlon 网络在连接交易双方之后，基于数字签名授权，最终通过智能合约完成交易结算。结算逻辑即是由协议预定义交易条件、流动性源、约定费用组成的策略。

Application Layer（应用层）
应用层将网络提供的服务封装成业务 API，并且提供标准接入 SDK，方便开发者集成到不同的应用端，为用户提供易于理解、便于使用的交互界面。

以用户为中心展开设计，进而推及协议层和网络组件的构建，是我们的核心理念。

系统设计



系统架构图

各模块介绍

User
用户使用自我掌控私钥的数字钱包，访问 Tokenlon 或第三方集成商提供的 DApp 页面进行交易。

链上合约

AllowanceTarget + Spender[1]
用户在正式提交订单至链上结算前，需要先将 Token 代币授权至 **AllowanceTarget**。这是用户授权的最小单元，设计上兼顾了长期有效性（避免协议升级要求用户再次授权）和扣款权力安全性。当链上结算发生时，Tokenlon 将对订单和用户签名进行验证[2]。只有验签成功的情况下，才借助 **Spender** 进行代币扣款。

Tokenlon Proxy
遵循 EIP1967 Proxy[3] 标准，Tokenlon Proxy 作为协议入口将具体的业务逻辑代码代理到逻辑合约上，并分离了业务逻辑和持久化存储，让未来协议升级更方便和安全。

UserProxy
作为用户与链上合约交互的代理者，根据用户指令路由到不同的策略合约，比如

- Fill Order：提交一个链下签约的订单，进行链上原子结算；
- Swap：指定链上自动做市商进行代币兑换；
- Payment：指定向收款方支付既定数量的代币

同时，负责管理代理合约和策略合约的生命周期。

Liquidity Strategy
在区块链的智能合约上实现流动性结算策略，用以适配不同类型的流动性供给者。同时帮助流动性合作伙伴自定义其不同的交易策略。

链下系统

Relayer
Tokenlon 链下网络中继服务提供者，以点对点网络的方式运行中继节点，提供订单路由、交易撮合、上链结算等服务。

Aggregator
负责聚合多个流动性源，为用户找到最佳订单。

Liquidity Providers
统称为流动性提供者，Tokenlon 将集合不同的流动性源，包括：

- 链上算法自动做市商
- 链下专业做市商
- 用户挂单的订单薄
- 中心化交易所订单薄

我们的策略是包容整合来自各个市场的流动性供给者，系统自动为用户选择最佳路径。

安全

交易原子性
对于用户的链上交易行为，智能合约设计保障了交易结算的原子性，即要么交易条件达成完成结算，要么交易失败，用户资产始终保持在自己掌控下的钱包里。

合约权限控制
Tokenlon 协议涉及到升级和配置，需要动用管理员账户进行执行，管理员账户是一个 ⅗ 多签账户[4]，避免单点风险。同时，对于关系到用户资产相关的操作，合约设计了 timelock (时间锁）延迟生效的特性，避免意外即时生效，管理员可以在延迟周期内进行修正。

最小化信任原则
对于用户与协议之间的信任关系，我们遵循最小化原则。在 Tokenlon 5.0 设计的初版，用户需要信任策略合约的验签和结算逻辑。所有合约代码均开源，并且在链上完成合约透明验证，任何人都可以审计合约内容，由此基于透明建立信任。

第三方安全审计
主网上线前完成第一轮专业安全团队审计，基于审计报告结论安排上线时间表。
主网上线后，基于主网部署的合约进行第二轮安全审计。

每一次合约变更升级前，都将提交第三方安全审计。
另外，我们将持续提供 Bug Bounty，鼓励社区提交安全风险报告。

经济模型

去中心化 Tokenlon

为了实现中立、健壮的交易支付结算协议，Tokenlon 本身需要和区块链融为一体，成为整个去中心化网络的一部分。通过代币经济机制的设计以及社区自治的治理模型，协调各方网络参与者有动机、有回报、可持续地推动 Tokenlon 正向发展。

网络生态

网络生态的参与者包括：

- **用户**，包括：服务使用者、新用户的推荐者
- **流动性提供者**，包括：做市商、经纪商、资产供给者
- **开发者**，包括：核心开发团队、社区开发者、中继运营商、第三方服务集成商
- **治理参与者**，包括：治理提案人、参与讨论的审阅人、持有代币的投票人

正是由于开发者打造了有价值的协议、产品、服务，能够解决用户的实际问题，用户才能够被其吸引并愿意为之付费。

这个时候，如果将网络创造的价值继续投入到生态建设，就会激励更多的贡献者参与其中，推进网络各个层面的优化升级，进而创造更大的价值，整个网络进入正反馈的发展轨道。

而 LON 是推动整个生态经济循环最重要的媒介。

LON: Tokenlon Network Token

LON 是 Tokenlon 发行的应用型代币，用于激励生态中各方并确保其能够协力推动生态发展。

Token Utility 代币用途

LON 代币有以下两个主要用途：

1. 费率折扣：Tokenlon 目前对大部分交易收取 0.30% 的标准手续费。通过持有 LON，用户可以根据持有数量获得相应的手续费折扣。
2. 治理：LON 将赋予社区参与 Tokenlon 治理的权利，LON 持有者可以通过发起 Tokenlon Improvement Proposal（TIP）提案和投票来改进 Tokenlon，例如决定财库的用途、手续费参数、回购参数、支持资产、产品功能等。

LON 数量	费率
0	0.30%
20	0.29%
50	0.28%
150	0.26%
500	0.24%
1,500	0.22%
5,000	0.20%
10,000	0.18%
30,000	0.15%
100,000	0.10%

Tokenlon 费率表

经济机制

回购 Buyback

Tokenlon 协议所收取的手续费将会被用于在公开市场上回购 LON，回购的 LON 将被转移至财库以及用于质押奖励。

质押 Staking

LON 持有者将能够通过参与质押获得手续费折扣以及治理权利。作为回报，质押者将能够根据质押的 LON 数量按比例获得质押奖励。质押奖励来自于协议在公开市场上回购的 LON。每次回购中用于质押奖励的 LON 数量将由以下公式决定：

$$stakingRewardLON = buybackLON * stakingRewardFactor$$

*LON 质押奖励数量 = LON 回购数量 * 质押奖励因子*

初始质押奖励因子默认值为 0.6，即每回购 1 个 LON，就会有 0.6 个 LON 被用于质押奖励。

财库 Treasury

财库是由社区通过治理支配的 LON 储备池，用于建设和促进 Tokenlon 网络生态发展。财库中的 LON 来自于协议在公开市场上回购的 LON。每次回购中划分至财库的 LON 数量将由以下公式决定。

*treasuryLON = buybackLON * (1 - stakingRewardFactor)*
*LON 划分财库数量 = LON 回购数量 *（1 - 质押奖励因子）*

初始质押奖励因子默认值为 0.6，即每回购 1 个 LON，就会有 0.4 个 LON 被划分至财库。

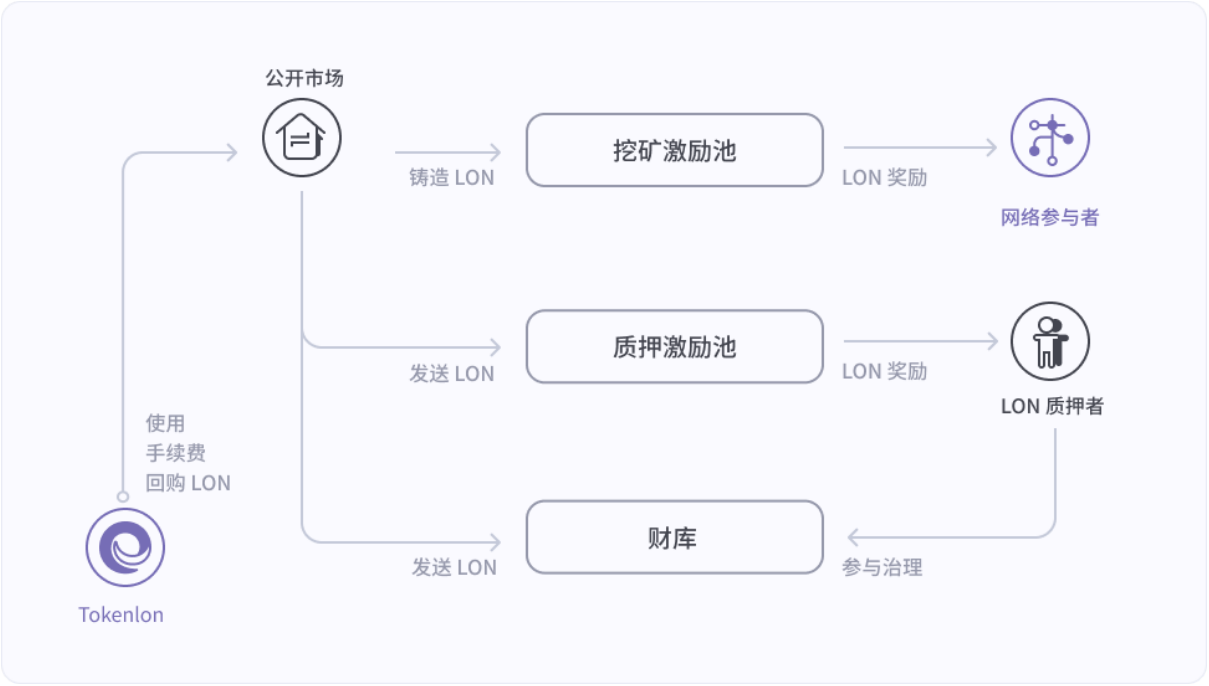
挖矿 Mining

在 LON 发行数量未达到上限时，每次回购都将触发铸币。铸币数量将由以下公式决定，铸出的 LON 将通过 LON Incentive Plan 激励网络参与者。

*issueLON = buybackLON * mineFactor*
*LON 铸币数量 = LON 回购数量 * 挖矿因子*

初始挖矿因子默认值为 1，即每回购 1 个 LON，就会有 1 个 LON 被铸出。铸出的 LON 将根据网络参与者的奖励比例来进行分配。

网络参与者	奖励比例
用户	35%
流动性提供方	25%
中继方	25%
推荐者	15%



核心经济机制

社区治理

Tokenlon 治理将通过以下三个阶段渐进式开放，逐步将决策权交予社区。

时间	阶段	规则
2020	Phase 0 - 预治理	TFT 持有者通过 Snapshot 链下治理，由核心团队主导收集并发起提案
2021	Phase 1 - 早期治理	LON 持有者通过 Snapshot 链下治理，由核心团队主导收集并发起提案，治理内容将覆盖核心经济机制参数
2022	Phase 2 - 开放治理	LON 持有者通过质押以及治理合约参与链上治理，由社区与核心团队共同收集并发起提案，治理内容将完全开放，并支持代理投票

LON 治理阶段

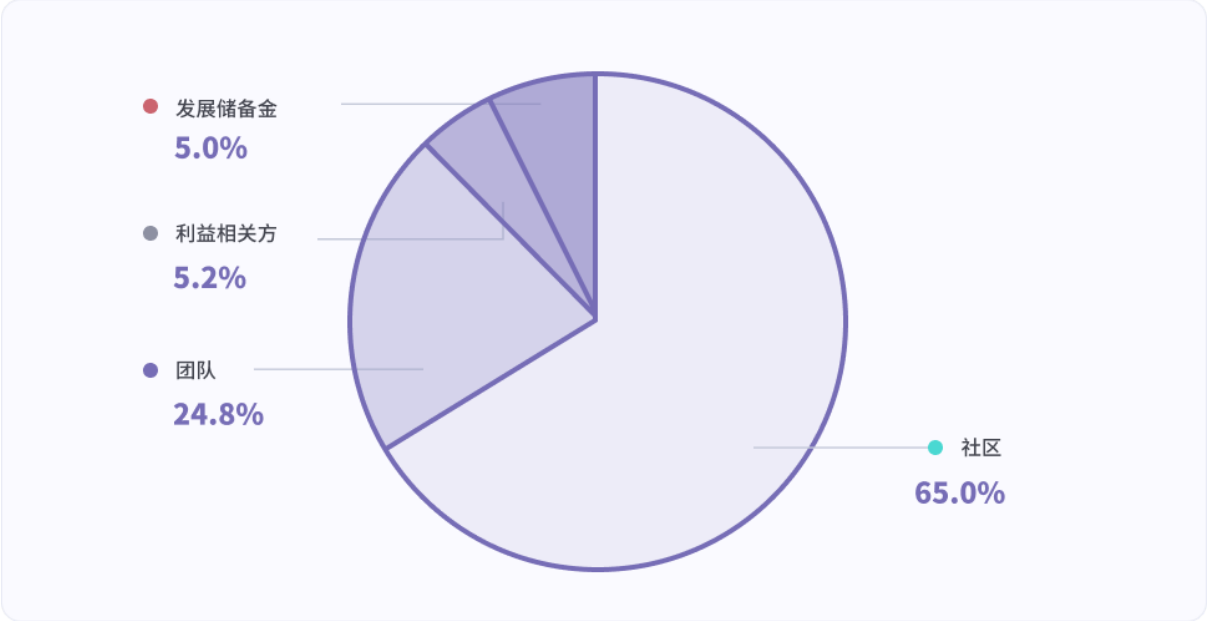
核心团队预计于 2021 年第三季度启动治理合约开发，具体的上线日期和执行方案将在后续公布。在治理合约上线前，社区将可以通过 Snapshot[5] 参加早期治理，进行链下投票，参与由核心团队主导的提案决策。早期治理将覆盖各核心经济机制参数，包括手续费规则设计。

代币分配

LON 总量上限为 200,000,000，其中 130,000,000 LON 通过 LON Incentive Plan (LIP) 分配至社区，49,680,000 LON 分配至核心团队，10,320,000 LON 分配至利益相关方，剩余 10,000,000 则分配至发展储备金。

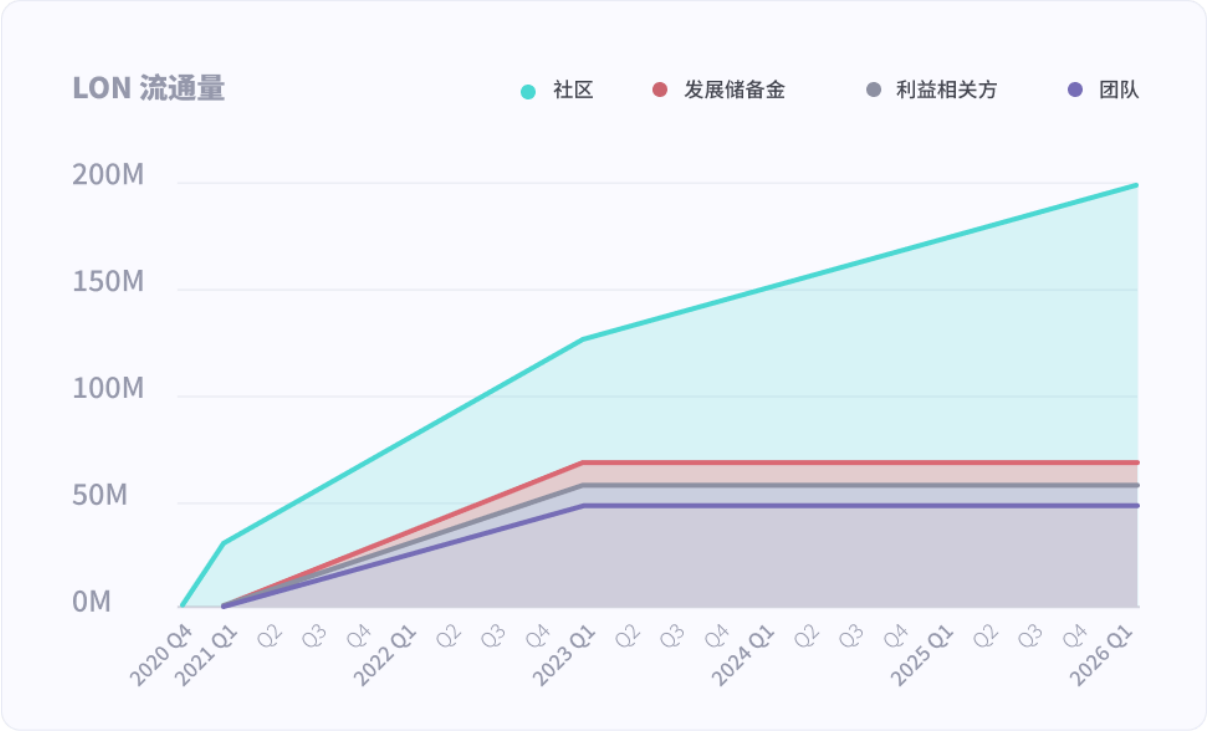
LON	总分配	初始流通	流通规则
社区 - 创世挖矿	15,000,000	12,000,000	交易者以及推荐者部分立即流通，做市商部分 180 天线性释放
社区 - 早期支持者回馈	15,000,000	15,000,000	立即流通
社区 - 流动性池激励	10,000,000	0	一年内根据激励计划释放
社区 - 持续挖矿激励	90,000,000	0	根据经济参数以及交易情况决定，预计需五年*
团队	49,680,000	0	两年线性释放
利益相关方	10,320,000	0	两年线性释放
发展储备金	10,000,000	0	两年线性释放

LON 分配以及流通规则



LON 分配饼状图

为了鼓励社区参与，LIP 将通过两个阶段逐步实施并完成 130,000,000 LON 的分发。归属团队、利益相关方以及发展储备金的 70,000,000 LON 将在代币流通后开启两年线性解锁释放。



LON 流通量预估

LON 激励计划 (LIP)

阶段零：三个月（2020.9.26 至 2020.12.22）

30,000,000 LON 会在 LON 开启流通时分配至社区。其中 15,000,000 LON 分发至参与创世激励计划的交易者、推荐者以及做市商。另外 15,000,000 LON 分发至早期支持者。

激励/回馈	时间	激励数量	激励对象
交易，推荐激励	5 周	5,000,000 LON	期间在 Tokenlon 交易的用户以及推荐人
交易，推荐，做市激励	50 天	10,000,000 LON	期间在 Tokenlon 做市的做市商，交易用户，以及推荐人
早期支持者回馈	2020.12.23	15,000,000 LON	早期对 Tokenlon 做出过贡献的用户以及团队

阶段零 LON 激励计划

阶段一：预计五年（2020.12.23 开始）

10,000,000 LON 将被用于流动性池激励，用于激励期间为指定 LON 池提供流动性的用户。

根据经济机制，至多 90,000,000 LON 将在阶段一被挖矿铸出，用于奖励网络参与者；同时 Tokenlon 协议所收取的手续费用将被用于在公开市场上回购 LON，回购所得的 LON 将根据经济参数用于质押奖励以及财库储备。

里程碑

为了能够实现 Tokenlon 的愿景，以下是我们计划在未来几年内专注的工作内容以及相关的里程碑。

2020 - 创世挖矿

建立奖励机制，通过创世挖矿，激励网络参与者中的交易者、推荐者以及做市商；同时向 Tokenlon 相关的早期贡献者回馈 LON，完成向社区分发 3000 万 LON 代币。

2021 - 经济模型搭建

完成 Tokenlon 5.0 版本升级发布。启动交易、推荐、做市等社区持续激励计划，并推出流动性池激励，引入回购、质押等机制，完善 LON 经济模型，让 LON 成为推进 Tokenlon 网络发展的主要推动力。

2021, 2022 - 社区治理

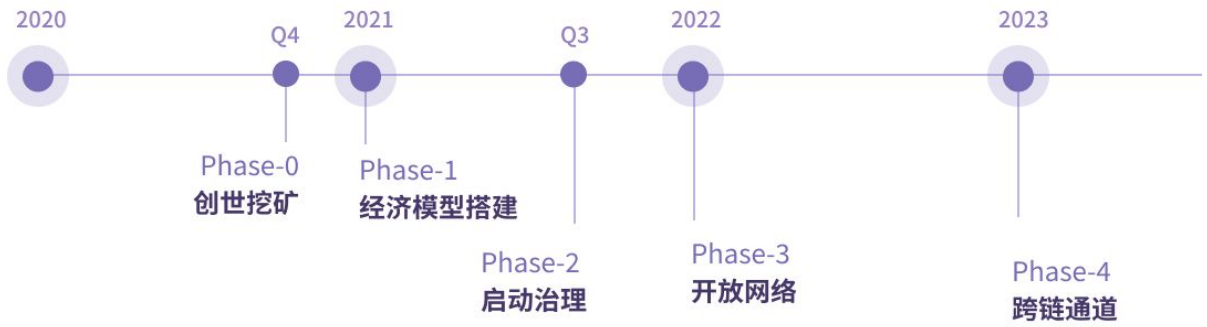
在目前链下预治理的基础上，引入基于 LON 的治理模块，开启最小化治理，并逐渐开放各经济参数以及机制的治理，将决策过程去中心化，最终完全由社区提案主导和推动 Tokenlon 发展，形成去中心化自治组织（DAO）。

2022 - 开放网络

通过组建 P2P 中继网络，让核心团队以外的开发者也能够成为 Tokenlon 中继方，使 Tokenlon 成为由多个中继方共同支持的流动性网络。同时建立无需准入的开放策略平台，流动性提供方将可以基于协议标准，自由设计和部署流动性策略，接入 Tokenlon 网络。

2023 - 跨链通道

基于行业中成熟的跨链方案，启动建立跨链通道，支持跨链交易原子结算。同时利用 Tokenlon 搭建的跨链流动性网络，推出开放性支付结算服务，将去中心化流动性注入支付等更多生活场景当中。



风险

投资风险
LON 是 Tokenlon 发行的应用型代币，非投资产品。在作出购买决定前，购买者应仔细考虑其是否适合其财务状况、购买目标和经验、风险承受能力、以及其他有关情况，亦应了解购买 LON 所涉及的相关风险。

系统风险
安全是 Tokenlon 协议的最高优先级，核心团队以及外部安全审计团队一起投入了大量精力确保协议安全可靠。Tokenlon 相关智能合约代码均公开可验证，我们也邀请外部安全人员寻找协议中的漏洞，获取赏金。

术语表

DeFi
Decentralized Finance 缩写，特指在区块链的去中心化网络里，借助智能合约实现的，具备开放，透明，低门槛的金融协议或产品。

DEX
Decentralized Exchange，去中心化交易所。

RFQ
Request for quotation，是指买家寻求柜台报价的一种交易模式。

LON
Tokenlon 生态的应用型代币，用于鼓励网络参与者一致为生态做出贡献。

LIP
LON Incentive Plan，基于分配 LON 的激励计划，用于激励生态中的所有参与者。

TIP

Tokenlon Improvement Proposal，特指 Tokenlon 改进提案，LON 持有者可以通过对提案投票进而参与治理。

参考资料

[1] 0x Protocol Specification

[2] EIP-1271: Standard Signature Validation Method for Contracts

[3] EIP-1967: Standard Proxy Storage Slots

[4] dYdX PartiallyDelayedMultiSig

[5] Snapshot is an off-chain gasless multi-governance client