ZKSwap 经济白皮书(草案)

L2 Lab

2021-2-24

项目背景

ZKSwap 是基于 ZK-Rollups 技术的 Layer2 自动做市商模型去中心化交易所，目前在以太坊 Layer2 上面完整实现了免信任并且免费的 Layer2 的支付和转账（ZKPay），以及 Layer2 上免费的、极速的、可以无限扩容的 Swap 交易体验（ZKSwap）。

在 ZKPay 中，我们提供一套完整的 Layer2 解决方案，可以支持所有的 ERC20 的免费、实时、最终 TPS 超过 2000 的转账体验，后续计划重点支持所有的稳定币，使用 ZKPay 的转账服务。

在 ZKSwap 中用户可以把已有 Layer1 上的资产（包括 ETH 和 ERC-20 Token）转移到 ZKSwap 合约中，并在 Layer2 中完成所有转账、交易等过程。ZKSwap Layer2 上的资金具有和以太坊 Layer1 一致的安全性，交易可以实时完成（不需要等待一个区块确认），不需要支付额外的 Gas 费用，并且具备几乎无限的可扩展性，摆脱了以太坊 TPS 和区块确认时间的限制，必将对现有所有的 DEX 和 CEX 带来极大的变革。

然而，要实现上述安全、实时、零 Gas 以及 可扩展的去中心化交易所，需要一套完整的 Token 经济激励机制使生态中所有参与者共同维护 ZKSwap 系统的运转：一方面，需要适当分配 Token 的比例和解锁周期，以充分发挥项目方，开发者，投资人以及社区参与者的能动性，使 ZKSwap 系统能够平稳启动并获得长远的发展；另一方面，需要针对流动性提供者、Gas 费用提供者和零知识证明服务提供者进行激励，以实现零 Gas 的实时交易，提升系统安全性和可扩展性。

ZKS 是一个 ERC20 代币，作为 ZKSwap 协议 Token，是激励 ZKSwap 系统正常运转的最重要因素，也是用户参与治理、上币、交易验证和回购的凭证。本文将详细描述 ZKS 的 Token 经济模型。

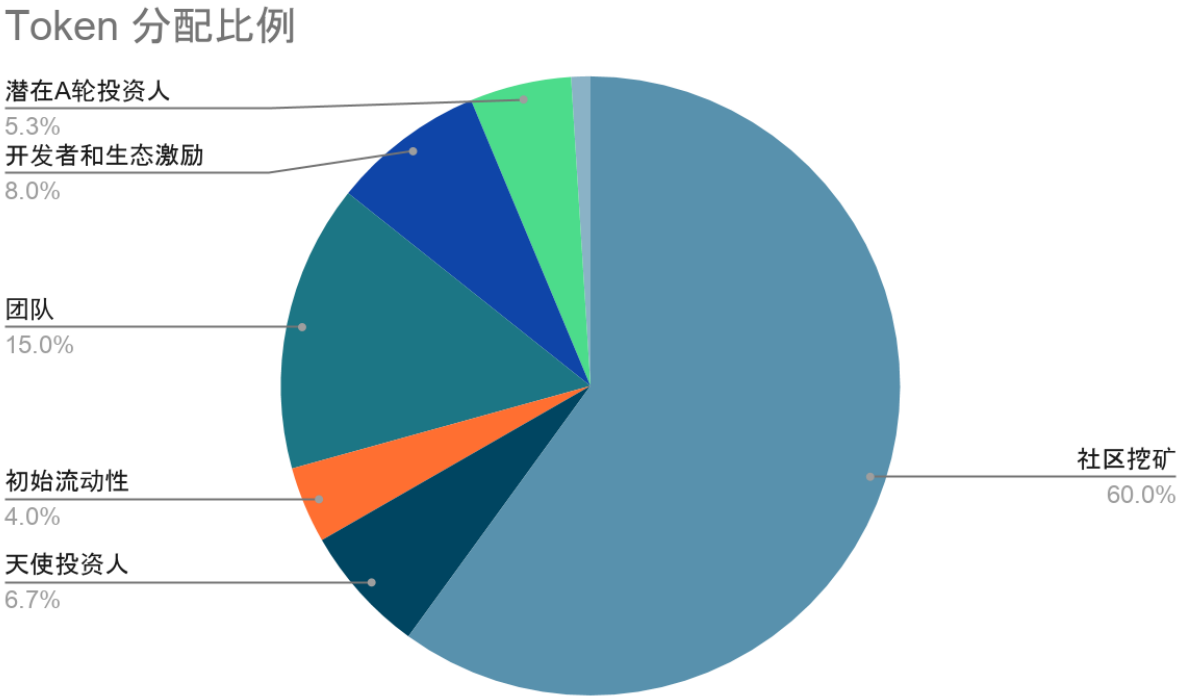
ZKS Token 分配和解锁

ZKS Token 分配

ZKS（合约地址 https://etherscan.io/token/0xe4815ae53b124e7263f08dcdbbb757d41ed658c6）是 ZKSwap 的协议 Token，总量为 10 亿枚 ZKS。Token 的分配比例如下：

- ZKSWap 代币符号： 英文：ZKS， 中文：零知兑，外号：灵芝

- 社区挖矿 60%，共计 6 亿 ZKS， 前 3 年分发 50%， 剩下 10% 长期激励，其中：
  - 第一年分发代币总量的 20%（其中 5% 用于空投奖励）， 第二年 15%， 第三年 15% 第四年及以后 合计 10%;
  - 分发方式：1、流动性挖矿 Proof-of-Liquidity-Mining（代币总量的 14%）； 2、代付 gas 费挖矿 Proof-of-Gas（代币总量的 9%）； 3、零知识证明挖矿 Proof-of-ZK-Snarks（代币总量的 14%）4、交易即挖矿（代币总量的 9%）Proof-of-TransFee 5、智能合约 Staking 锁仓挖矿（代币总量的 9%）6、上线以太坊主网前，将有与初始流动性等量的 ZKS（代币总量的 4%，即 4 千万 ZKS）被 1:1 空投到 ZKS 持有者的地址 7、主网上线后对主流 defi 项目用户地址进行空投（代币总量的 1%，即 1 千万 ZKS）
- ZKSwap 团队 15%，共计 1.5 亿 ZKS， 自上线起锁定一年，从第二年开始分发，每年发放代币总量的 5%，至第四年底发放完毕;
- 潜在 A 轮投资人 5.3%， 共计 5 千三百万 ZKS，项目上线 1 年后由社区治理决定是否开始募资：若开启 A 轮融资，则对应 Token 锁定 3 个月，然后分 12 个月解锁；若未开启融资，则由社区投票治理决定 Token 具体用途，或直接销毁。
- 初始流动性 4%，共计 4 千万 ZKS，将在北京时间 2021 年 1 月 6 日下午 3 点 全部用于在 uniswap 和 gate.io 上提供初始流动性（ZKS-USDT），初始流动性比例为 40,000,000 ZKS / 3,000,000 USDT。其中，uniswap 和 gate.io 各占初始流动性的 50%。
- 开发者和生态激励 8%，共计 8 千万 ZKS， 每年发放 2%， 4 年分发完毕
- 天使投资人 6.7%， 共计 6 千 7 百万 ZKS，上线主流中心化交易所后释放 30%，剩余部分上线后锁定 3 个月，然后分 6 个月分发完毕;
- 顾问 1%，共计 1 千万 ZKS，分 3 年发放，每年发放 0.33%。



ZKSwap 是一套社区化的去中心化交易协议，因此大部分的协议 Token 将由挖矿产生，分配给维护系统运行的社区参与者。社区挖矿占总供应量的 60%，其中流动性挖矿占比 14%，代付 Gas 费挖矿占比 9%，零知识证明服务挖矿占比 14%，交易即挖矿占比 9%，智能合约 Staking 挖矿占比 9%，上线主网前的空投激励占比 4%，主网上线后对其他主流 DEFI 项目用户进行空投激励占比 1%。

开发者是 ZKSwap 生态中最重要的参与者，负责搭建各项基础设施。ZKSwap 官方团队负责维护 ZKSwap 项目，将在四年内获得共计 15% 的 ZKS Token。社区开发者和其他成员为 ZKSwap 用户提供服务和周边产品，因此将在四年内获得共计 8% 的 ZKS Token，其中有一部分用于早期空投和激励参与早期测试的社区成员。

ZKS Token 总量的 4% 将在上线主网第一年内在 ZKSwap，Uniswap 等去中心化交易平台，以及 Gate.io 等中心化交易所上交易，提供 ZKS 的初始流动性。

此外，ZKSwap 项目还预留了总计 13% 的 ZKS Token 用于吸引天使投资人、潜在 A 轮投资人 以及 法务/交易所/媒体 顾问等参与生态建设，帮助项目实现进一步发展。

Token 解锁规则

ZKS Token 在上线后 4 年内解锁大部分代币，并在 4 年后对系统进行长期激励，具体时间节点如下：

第一年 流通 33.03%

挖矿和空投 20% + 天使投资人 6.7% + 初始流动性 4% + 生态开发者和生态激励 2% + 顾问 0.33%

第二年 流通 59.32%

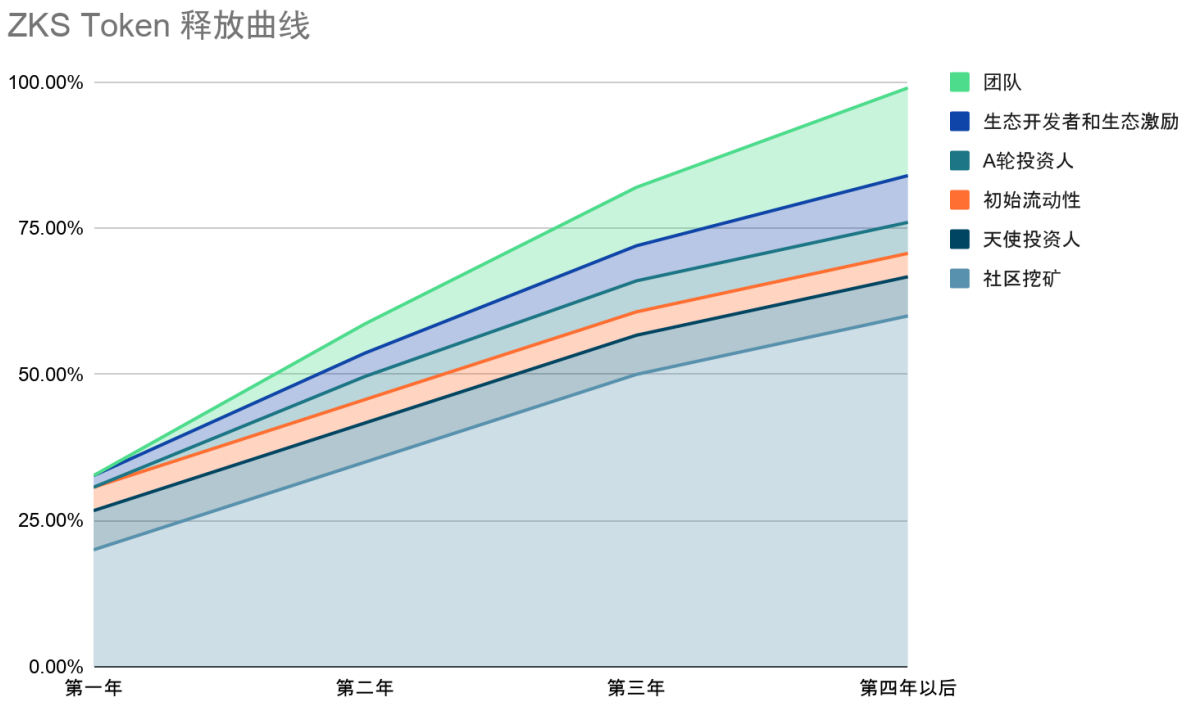
33.03% + 挖矿 15% + A 轮投资人 3.95% + 团队 5% + 生态开发者和生态激励 2% + 顾问 0.33%

第三年 流通 83%

59.32% + 挖矿 15% + A 轮投资人 1.35% + 团队 5% + 生态开发者和生态激励 2% + 顾问 0.33%

第四年以后 流通 90%+

83% + 团队 5% + 生态开发者和生态激励 2% + 长期挖矿激励（比例待定）



ZKS 社区挖矿

从上述 ZKSwap 的 Token 体系中可以看出，除去主网上线前空投给早期持有 ZKS 用户的 4% 和主网上线后计划空投给其他 DEFI 用户的 1% 代币外， 55% 的 ZKS Token 将被分配给参与社区挖矿的“矿工”（前三年每年释放 15%，剩余 10% 作为长期激励），即 Gas 费用提供者，流动性提供者 以及 零知识证明服务提供者，以及交易即挖矿和 Staking 参与者。前三者是保证系统正确运行，实现零 Gas 费、可扩展以及实时交易的主要贡献者。三种参与者将分别通过 PoG、PoL 和 PoZK 三种证明获取挖矿收益。此外，所有在 ZKSwap 上进行交易的用户都可以通过 PoT 机制获取 ZKS 奖励。用户还可以质押 ZKS 参与 Staking 获得奖励。

Proof-of-Gas（PoG）

ZKSwap Layer2 中的所有交易都需要向以太坊 Layer1 提交证明，以保证安全性。在与以太坊 Layer1 交互的过程中，需要消耗一定量的 Gas 费用。在 zkSync 等其他基于 ZK-Rollups 的系统中，这部分 Gas 费用往往由用户承担。

ZKSwap 提出了 Proof-of-Gas (POG)，即 基于以太坊 Gas 消耗量的证明机制，使得代付 Gas 费用成为可能。Gas 费用给提供者可以在 ZKSwap 的代付合约中存入任意数量的 ETH，用户帮所有 ZKSwap 用户提供提交证明的 Gas 费用；作为回报，Gas 费用提供者将根据贡献手续费的多少获得相应数量的 ZKS Token。

PoG 机制以智能合约的方式实现，在 ZKSwap 主网上线时，会同时发布代付 Gas 费用的智能合约，任何用户都可以向该智能合约充值 ETH，并进行 pledge（Gas 划扣承诺），ZKSwap 系统会使用该智能合约中的 ETH 为普通用户支付向 Layer1 提交证明的 Gas 费用。总计将有占总量 9% 的 ZKS 代币用于 PoG 挖矿奖励（前三年每年最多 2.5%，剩余 1.5% 作为长期激励，总计 9 千万 ZKS）。假设某活动期间每天向 PoG 矿工发放 N 个 ZKS（N 的数量与 ZKSwap 每日消耗的 Gas 费用、平台交易量，用户数以及流动性相关，具体规则将在后续发布）。具体规则如下：假设当天所有 ZKSwap 用户消耗了 50 ETH 作为 Gas 费用，并且该 PoG 智能合约合计共锁定了 500 ETH。PoG 矿工如果充值了 1 ETH，那么当天智能合约会花费掉 PoG 矿工 1ETH / 500ETH * 50 ETH = 0.1 ETH，同时获得 0.1ETH / 系统总消耗 50ETH * N ZKS= 0.002N ZKS。注意，每天消耗的 Gas 费用由系统中实际产生的交易和以太坊网络拥堵程度决定，且 PoG 合约中锁定的 ETH 会随时改变，因此投入的 ETH 与获取 ZKS 的比例不固定。

PoG 合约中锁定的所有 ETH 只能用于支付 ZKSwap 系统所需的 Gas 费用，不会用于其他任何用途。PoG 合约地址将在主网上线时发布，并公布安全审计结果。

Proof-of-Liquidity-Mining（PoL）

流动性充足与否是影响 ZKSwap 交易体验的关键因素，因此，系统中 14% 的 ZKS Token 都将通过 Proof-of-Liquidity-Mining （POL 基于流动性的分发机制） 奖励给 ZKSwap 的流动性提供者（前三年每年最多释放 3.75%，剩余 2.75%作为长期激励，总计 1 亿 4 千万 ZKS）。

ZKSwap 流动性挖矿预计在正式上线后 2-3 周左右开启，类比 Uniswap 的流动性挖矿机制，对一些特定的交易对，会给提供流动性的客户进行奖励，并进行 ZKS 的分发。 ZKSwap Layer2 资金池的流动性提供者，凭借对应资金池的 LP Token，可以获得相应比例的 ZKS Token。首期支持的资金池和奖励比例将在上线主网时同时公布。后续参与流动性挖矿的资金池及奖励分配将由社区共同决定。

Proof-of-ZK-Snarks（PoZK)

ZKSwap 系统 Layer2 中的所有交易都需要生成零知识证明，并提交到以太坊 Layer1，因此需要大量的计算。零知识证明服务是 ZKSwap 安全性和可扩展性最重要的保障。在项目上线初期，ZKSwap 官方部署了大量高主频 AMD 的 CPU 服务器来生成 零知识证明。然而实际上，不论是官方部署还是用户自己部署证明生成节点，只要按时提交证明到 Layer1 都不会影响系统的安全性。理论上，越多人参与证明生成，系统的 TPS 就越高，从而实现安全、实时的交易。

ZKSwap 将会在上线主网 1 个月以后开放 Proof-of-ZK-Snark （PoZK 基于零知识证明的工作量证明），以鼓励用户贡献自己的计算能力生成证明。总计将有占总量 14% 的 ZKS 代币用于 PoZK 挖矿奖励（前三年每年最多释放 3.75%，剩余 2.75% 作为长期激励，总计 1 亿 4 千万 ZKS），假设某活动期间每天分发 N 个 ZKS （N 的数量与 ZKSwap 的交易量，用户数以及流动性相关，具体规则将在后续发布）作为 PoZK 奖励。具体发放规则如下：假设当天 ZKSwap 系统中共提交 10000 笔交易证明，某 PoZK 矿工提交了其中的 10 个证明，则该 PoZK 矿工将获得 N ZKS*（10 笔证明/总共 10000 笔证明）= 0.001N ZKS 作为奖励。注意，PoZK 矿工被分配到的证明任务数量和节点本身质押的 ZKS 成正比。

ZKSwap 团队也在全力开发 Plonk 证明的 GPU 版本，这样在正式公布的时候，预期将会支持 CPU 和 GPU 分别参与零知识证明的计算，当然如果社区成员有兴趣，也可以研究 Plonk 证明的 FPGA 版本，甚至 ASIC 芯片，来加速 ZKSwap 的 Layer2 证明计算过程，并提升 ZKSwap 的 TPS，使 ZKSwap 的免信任 TPS 可以尽快突破 100 或者 1000 以上，这样 Layer2 的效率优势相对以太坊将有数十倍甚至上百倍的提升，并且具备和 Layer1 等同的安全性，那么必然会带来 Layer2 上大量区块链的应用爆发，ZKSwap 也将成为 Layer2 的入口，带动所有 DeFi 基于 ZKSwap 的基础设施，在 Layer2 上实现丝滑的体验。

Proof-of-TransFee (PoT)

ZKSwap 作为新一代 Layer2 去中心化交易所，交易本身是整个系统的核心。为了激励所有参与交易的用户，ZKSwap 引入了 Proof-of-TransFee-Mining（PoT，交易手续费证明机制），交易即挖矿。所有在 ZKSwap Layer2 进行交易的用户，将根据每天付出手续费的金额获取 ZKS Token 补贴。总计将有占总量 9% 的 ZKS 代币用于 PoT 挖矿奖励（前三年每年最多 2.5% ，剩余 1.5% 作为长期激励，总计 9 千万 ZKS）。假设第一年每天向 PoT 矿工发放 N 个 ZKS（N 的数量与 ZKSwap 的交易量，用户数以及流动性相关，具体规则将在后续发布） 。具体奖励规则如下：假设当天 ZKSwap 所有资金池收入手续费等值 $50,000，其中某用户共支付 $50 手续费，则该用户可以获得 ($50/$50,000) * N ZKS = 0.001N ZKS 作为 PoT 挖矿奖励。

智能合约 Staking 锁仓挖矿（PoS）

为了激励 ZKS 的长期持有者，ZKSwap 在上线主网后还将支持 Staking 锁仓挖矿，Staking 的参与和奖励发放都通过智能合约完成，避免中心化风险。预计将有 ZKS 总量 9% 的 Token 将通过 Staking 锁仓挖矿的形式发放（前三年每年最多 2.5% ，剩余 1.5% 作为长期激励，总计 9 千万 ZKS）。

参与 Staking 挖矿的用户需要把 ZKS 锁定到指定的 Staking 智能合约，合约会根据锁定的比例自动计算 Staking 奖励，在每期锁仓活动期间不支持提前取回。假如某期活动每天向 Staking 锁仓用户发放 N 个 ZKS（N 的数量与 ZKSwap 的交易量，用户数以及流动性相关，具体规则将在后续发布），当天某用户有效锁仓额为 50,000 ZKS，Staking 合约中总锁仓量为 50,000,000 ZKS，则该用户预期当日将获得 （50,000 ZKS / 50,000,000 ZKS) * N ZKS = 0.001N ZKS 的奖励。锁仓的具体规则和智能合约将在主网上线后发布，并完全开源。

备注

主网上线后各类挖矿的首期活动将由官方制定 ZKS 奖励方案，活动开始前会有详细公告。后续每日挖矿奖励的 ZKS 数量与 ZKSwap 的交易量，用户数以及流动性正相关，越大的交易量、越多的用户数和流动性会解锁越高额度的 ZKS 奖池。具体规则将在首期挖矿活动结束后发布）

ZKS 使用场景

ZKS 作为 ZKSwap 的原生协议 Token，既代表了持有者的权利，也具有实际使用价值。ZKS 可以在以下场景中使用。

治理代币

ZKSwap 是一个由社区主导的去中心化项目，ZKS 是社区参与治理的凭证：

- 持有一定数量 ZKS 的用户可以发起升级提案，如修改手续费，流动性挖矿资金池分布 以及 ZKS 长期激励计划等；
- 所有 ZKS 持币者都可以对提案进行投票表决，获得大多数同意投票的提案才会通过，并由开发团队负责实施。

投票/抵押上币

ZKSwap 支持的交易对有限，除了官方团队初始添加的交易对外，持有 ZKS 的用户可以通过投票或质押实现上币：

- 持币用户可以通过上面的治理流程发起上币提案，如果获得大多数投票通过即可上币；
- 对于持币较多的用户，可以通过抵押 ZKS 的方式竞争上币。

ZKSwap 官方团队将根据投票和质押的结果实施上币操作。上币完成后所有用户都可以创建交易对或提供流动性。

ZKS 协议手续费

ZKSwap 协议将收取所有 Layer2 Swap 交易额的 0.3% 作为交易手续费。其中，0.25% 将自动分配给流动性提供者，另外 0.05% 将作为协议手续费。所有协议手续费（100%）都将用于项目的长期激励，ZKSwap 官方不会获取任何交易手续费。

Layer2 节点计划

前面章节提到，ZKSwap Layer2 的节点负责提交交易的零知识证明上链，通过提供 PoZK 服务以获得 ZKS 奖励。这些负责提交证明的 Prover 节点需要质押 ZKS 代币以获得生成证明的权利，质押金额与被分配到的证明任务成正比。ZKSwap 上线主网后将发布 Layer2 节点计划，通过质押 ZKS 参与 PoZK 挖矿，共同维护系统安全性和可扩展性，同时获取 ZKS 收益。

总结

ZKS 是 ZKSwap 协议 Token，是激励参与者共同构建 ZKSwap 生态的关键环节。ZKS 将在四年内完成总量 90% 的 Token 分配。其中，超过 60% 的 ZKS Token 将通过社区挖矿和空投的形式分配给 ZKSwap 基础设施提供者，包括 Gas 费用提供者，流动性提供者， 零知识证明服务提供者、参与交易的用户及早期的 ZKS 持有者。持有 ZKS 的用户可以参与 ZKSwap 生态治理，投票或抵押上币，质押成为 Layer2 PoZK 节点。