ZKSwap Economy Whitepaper(Draft)

L2 Lab

Feb 24, 2021

About ZKSwap

ZKSwap is an AMM modeled layer-2 dex using ZK-Rollups technology. ZKSwap has fully enabled trustless and gas-free payment and transfer (ZKPay) and gas-free, real-time, and infinitely scalable token swaps (ZKSwap) on Ethereum layer-2.

With ZKPay, we provide a full suite of layer-2 solutions and support all ERC20 token transfer with gas-free, real-time, and a final TPS over 2000. The follow-up plan focuses on supporting all stable coins and using ZKPay's payment services.

With ZKSwap, users can deposit layer-1 assets (ETH and ERC-20 tokens) to ZKSwap smart contracts and complete transfer, token exchange, etc., on layer-2. The funds on ZKSwap layer-2 have the same security as Ethereum layer-1. Transactions on layer-2 are executed in real-time, with no need to wait for one block confirmation, no gas fees, and almost unlimited scalability. ZKSwap is free from the bottlenecks of TPS and one block confirmation time from the underpinning native blockchain and hence will bring significant improvement to both DEXes and CEXes.

To achieve the secure, real-time, gas-free, and scalable decentralized exchange, there needs to be a well functioning token economy to incentivize all stakeholders in the ecosystem to maintain ZKSwap collectively. On one side, the allocation ratio to different participants needs to be balanced, and the lockup period needs to be both incentivizing and sustainable. This is mainly to incentivize the project team, developers, investors, and the community, striving for a smooth kick-off and stable long-term development. The other consideration is to incentive liquidity providers, gas providers, and zero-knowledge proof generators to build a sustainable system with zero-gas fees, real-time execution, scalability, and system security.

ZKS is an ERC20 token. As the ZKSwap protocol token, ZKS is a major component of the ZKSwap system. It is also a certificate for users to participate in governance, token listing, transaction verification, and buy-back. This whitepaper will elaborate on the economic model of ZKS.

ZKS Token Allocation and Vesting

ZKS Token Allocation

ZKS is the protocol token of ZKSwap, with a total of 1 billion ZKS. ZKSwap token ticker is ZKS.
The smart contract address of ZKS is
https://etherscan.io/token/0xe4815ae53b124e7263f08dcdbbb757d41ed658c6.
The distribution ratio of ZKS is as follows:

1. **60%** to **Community Mining**:
   Six hundred million ZKS is allocated for community mining. Five hundred million ZKS will be distributed in the first three years, and 100 million will be used for long-term incentives.
   a. The first year will distribute 20% of total token supply, among which 5% will be used for airdrops; the second year 15%, the third year 15%, the fourth year onwards totaling 10%;
   b. Community mining includes:
      i. Proof-of-Liquidity-Mining (14% of the total supply);
      ii. Proof-of-Gas (9% of total supply);
      iii. Proof-of-ZK-Snarks (14% of the total supply);
      iv. Proof-of-TransFee (9% of the total supply);
      v. Smart Contract Staking (9% of the total supply);
      vi. Pre-mainnet launch airdrop to early ZKS holders 1:1 to the initial liquidity (4% of the total supply);
      vii. Airdrop to users of other key DeFi projects after mainnet launch (1% of the total supply);
2. **15%** to the **ZKSwap Team:**
   One hundred fifty million ZKS will be allocated to the ZKSwap team, with a one-year lockup from the mainnet launch. Starting from the second year, 5% of the total token supply will be distributed to the ZKSwap team every year till the end of the fourth year;
3. **8%** to **Ecosystem Developers and Ecosystem Growth**:

8% of the total token supply, totaling 80 million ZKS, will be allocated to developers and ecosystem growth initiatives, distributed in 4 years, each year 2.0%;

4. **6.7%** to **Angel Investors**:

   6.7% of the total token supply, totaling 67 million ZKS, will be allocated to the angel investors. 30% of the allocated tokens will be distributed to the angel investors after ZKS being listed on the centralized exchanges, and the remaining allocation will be locked for three months and then distributed through 6-month linear vesting;

5. **5.3%** to **Potential A Round Investors:**

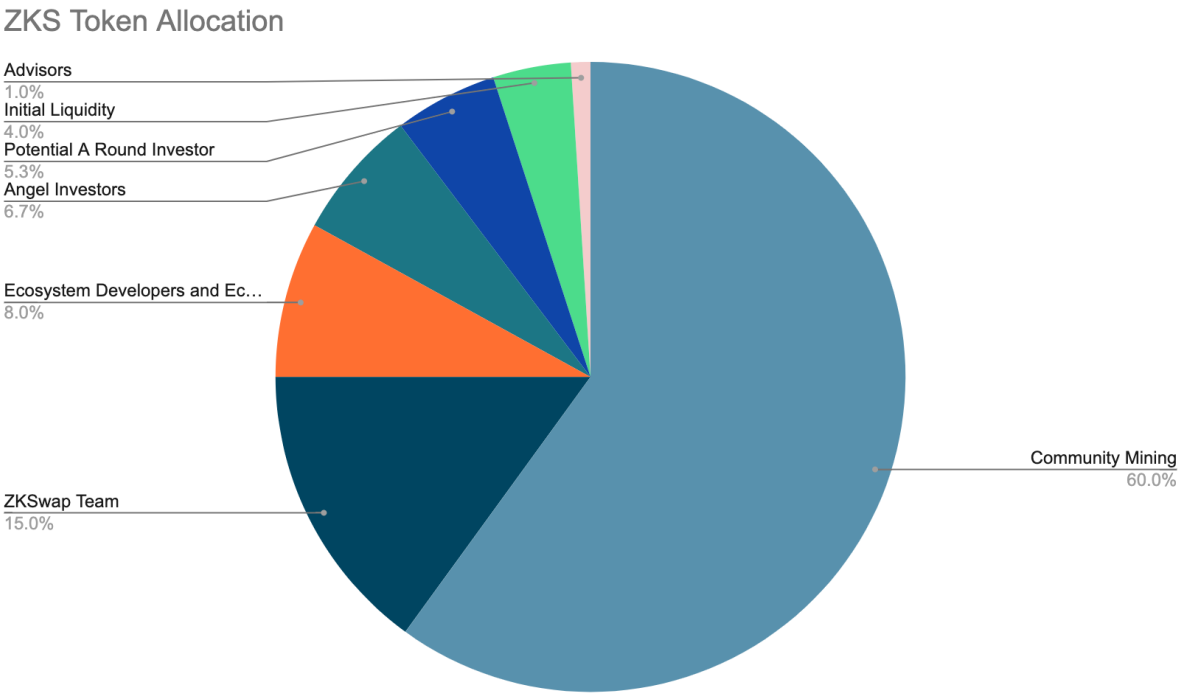
   A total of 53 million ZKS will be reserved for potential A round fundraising one year after the project is live. The community will jointly decide whether to launch the Round A investment. Should there be Round A investments, the allocated tokens will be subject to a 3-month lockup and 12-month linear vesting; should there be no Round A investment, the community will vote on the token usage or burning the tokens.

6. **4%** to **the Initial Liquidity**:

   A total of 40 million ZKS will be used to provide initial liquidity for (ZKS-USDT) on Uniswap and Gate.io at 3 pm on January 6, 2021, Beijing time. The initial liquidity ratio is 40,000,000 ZKS / 3,000,000 USDT. Among them, 50% of initial liquidity will each be allocated on Uniswap and Gate.io.

7. **1%** to **Advisors**:

   1% of the total token supply, 10 million ZKS, will be allocated to advisors. The tokens will be distributed in 3 years, 0.33% each year;



ZKSwap is a community-based decentralized token swap protocol. Most of the protocol tokens will be distributed through Community Mining and allocated to community members who participate in the system. Tokens allocated to Community Mining accounts for 60% of the total token supply. Proof-of-Liquidity-Mining accounts for 14% of the total token supply, Proof-of-Gas 9%, Proof-of-ZK-Snark 14% , Proof-of-TransFee 9%, and Smart Contract Staking 9%, pre-mainnet launch airdrop to early ZKS holders 4%, and airdrop to users of other key defi projects after mainnet launch 1%.

Developers are also essential participants in the ZKSwap ecosystem. They are responsible for building and maintaining the technical infrastructures. The ZKSwap official team is responsible for the development and maintenance of ZKSwap and will obtain 15% of the total ZKS Tokens within four years. Community developers and other developers who provide services or products to ZKSwap users will receive from the allocation 8% of ZKS Token within four years, and some of the 8% will be used for airdrops and incentive programs for community members participating in early-stage testing.

4% of the total supply of ZKS Token will be used on decentralized trading platforms such as ZKSwap and Uniswap within the first year of the mainnet launch to provide initial liquidity of ZKS.

ZKSwap has reserved 13% of the total ZKS Tokens to attract angel investors and potential Series A investors, legal/exchanges/media advisors, etc.

Token Lockup Period and Vesting

Most of the ZKS Token will be unlocked within 4 years after its launch, and the rest provides long-term incentives to the system after 4 years. The vesting schedule is as follows:

The 1st Year 33.03% in circulation

Community Mining and airdrops 20% + Angel Investor 6.7% + Initial Liquidity 4% + Ecosystem Developers and Ecosystem Growth 2% + Advisors 0.33%

The 2nd Year 59.32% in Circulation

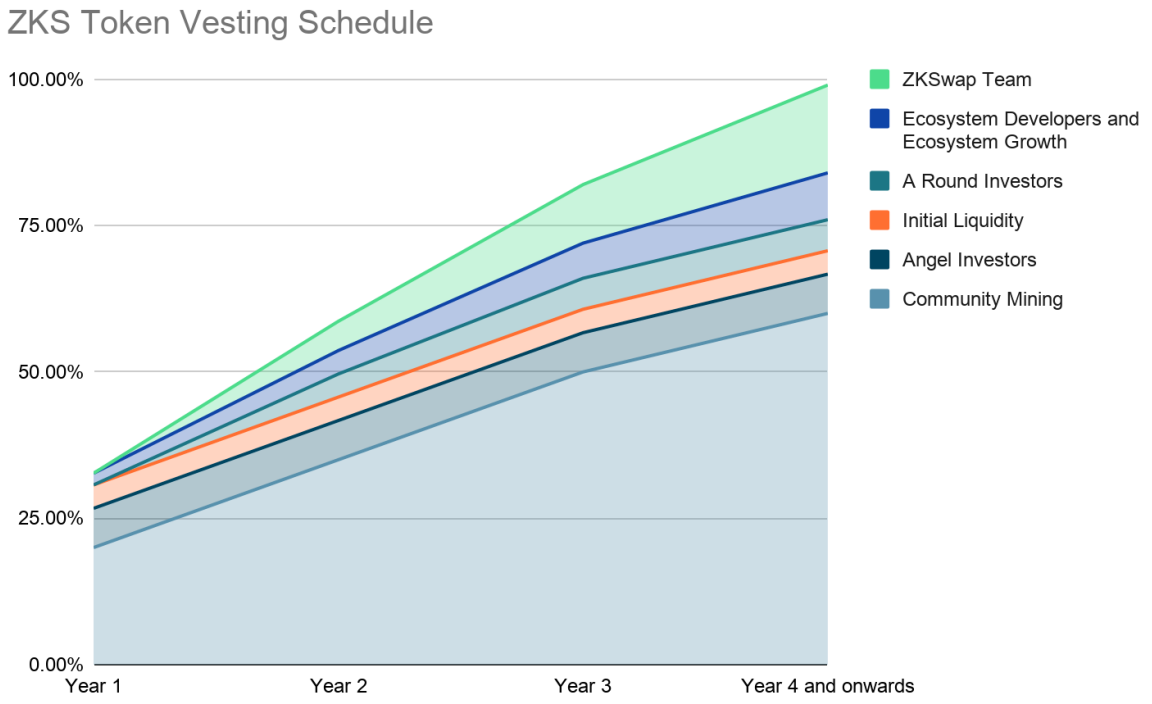
33.03% + Community Mining 15% + A Round Investors 3.95% + ZKSwap Team 5% + Ecosystem Developers and Ecosystem Growth 2% + Advisors 0.33%

The 3rd Year 83% in Circulation

59.32% + Community Mining 15% + A Round Investors 1.35% + ZKSwap Team 5% + Ecosystem Developers and Ecosystem Growth 2% + Advisors 0.33%

The 4th Year and onwards 90%+ in Circulation

83% + ZKSwap Team 5% + Ecosystem Developers and Ecosystem Growth 2% + Long-term Mining Incentives (proportion to be determined)



ZKS Community Mining

As listed above 60% of the ZKS Token will be allocated to Community Mining and airdrops, including liquidity providers, gas fee providers, zero-knowledge proof providers, and users who participate in trading as mining. Those participants ensure the correct operation of the system. They are the key contributors to the realization of zero gas fees, scalability, and real-time trading. 55% to community mining(with 15% each year for the first three years, and 10% as long-term incentives), 4% to pre-mainnet launch airdrop to early ZKS holders, and 1% to post launch mainnet airdrop to users of other key DeFi projects.

We name the three types of mining as Proof of Liquidity Mining, Proof of Gas, Proof of ZK-Snarks, and Proof of Trading.

Proof-of-Liquidity-Mining (PoL)

Liquidity is the most critical factor for the ZKSwap trading experience. Therefore, 14% of the total supply in the system will be distributed via Proof of Liquidity Mining to reward ZKSwap liquidity providers.

A total of 140million ZKS will be distributed through PoL. For the first three years, each year 3.75% max will be distributed, and the rest 2.75% as long-term incentive.

ZKSwap liquidity mining is expected to start about 2-3 weeks after the official launch. It is analogous to Uniswap's liquidity mining mechanism. For some specific trading pairs, users who provide liquidity will be rewarded with ZKS. The liquidity provider of specific ZKSwap Layer2 liquidity pool(s) can obtain a corresponding proportion of ZKS Token by the LP Token of the corresponding liquidity pool. The liquidity pool and reward ratio will be announced at the same time when the mainnet is launched. Subsequently enabled pools and respected rewards will be jointly decided by the community.

Proof-of-Gas (PoG)

For each transaction on the ZKSwap layer-2, ZKSwap needs to submit zero-knowledge proofs to Ethereum layer-1 to ensure security. For each interaction with the Ethereum layer-1, a certain amount of Gas fee will be consumed. In zkSync and other ZK-Rollups-based systems, this part of the Gas cost is covered by the user.

ZKSwap proposes Proof-of-Gas (POG), a proof mechanism based on Ethereum Gas consumption, making it possible to allow a third party to pay the user's gas fees.

The gas fee provider can deposit any amount of ETH in ZKSwap's payment contract and pay all ZKSwap users' gas fee. In return, the Gas fee payer gets reimbursed with corresponding ZKS tokens.

The PoG mechanism is implemented by smart contracts. When the ZKSwap goes live on the Ethereum mainnet, a smart contract will be deployed for paying gas fees. Any user can deposit ETH to the smart contract and make a pledge (Gas deduction commitment), the ZKSwap system will use the ETH in the smart contract to pay gas fees for the users.

Nine percent of the total supply will be allocated for POG mining rewards. In the first three years, each year 2.5% of total supply will be distributed max, and the rest 1.5% will be long-term rewards.

Suppose during one mining event, the system distributes N ZKS tokens to the POG miners per day, (The number N is proportionate to the daily gas fee consumption of the ZKSwap system, the trading volume on ZKSwap, number of users and locked liquidity, detailed rules will be published later.), the specific rules are as follows:

Suppose the total gas fee consumed by all ZKSwap users in one day is 50 ETH, and the PoG smart contract has already locked a total of 500 ETH. If the PoG miner deposits 1 ETH to this smart contract, then the smart contract will use this much of ETH each day for the amount this miner has deposited:

1ETH / 500ETH * 50 ETH = 0.1 ETH,

And this miner will, in turn, get this much of ZKS on this day:

0.1ETH / total system consumption 50ETH * N ZKS = 0.002N ZKS.

Please note that the gas cost per day is determined by the system's actual transaction numbers and the congestion level of the Ethereum network. And the total amount of ETH locked in the PoG contract is changing over time, so the minging ratio of ETH/ZKS is not fixed.

All ETH locked in the PoG contract can only be used to pay for the Gas fee required by the ZKSwap system, and will not be used for any other purposes. The PoG smart contract address will be released when the mainnet goes live, and the corresponding security audit results will be announced.

Proof-of-ZK-Snarks (PoZK)

All transactions in layer-2 of the ZKSwap system need to generate zero-knowledge proofs and submit them to Ethereum layer-1, so there will be a lot of computation. In the initial stage of the project's launch, the ZKSwap team has deployed many high-frequency AMD CPU servers to generate zero-knowledge proofs(ZK-Snarks). In fact, it doesn't matter who generates and provides the ZK-Snarks, as long as the ZK-Snarks are submitted to the layer-1 in time. In theory, the more people participate in the generation of proofs, the higher the system's TPS will be, hence to realize safe and real-time transactions.

ZKSwap will open Proof-of-ZK-Snarks mining one month after its mainnet launch to encourage users to contribute their computing power to generate ZK-Snarks. Fourteen percent of the total supply, 140 million ZKS, will be used for PoZK mining rewards. In the first three years, each year 3.75% will be distribute max, with the rest 2.75% as long-term rewards.

Suppose during one event, N ZKS tokens are distributed daily, (The amount N will be proportionate to the trading volume, number of users and liquidity volume on ZKSwap. Detailed rules about it will be published later.), the specific distribution rules are as follows:

Assuming that a total of 10,000 ZK-Snarks are submitted in the ZKSwap system that day, and if a PoZK miner submits 10 of these ZK-Snarks, the PoZK miner will get:

N ZKS* (10 ZK-Snarks/Total 10,000 ZK-Snarks) = 0.001 N ZKS

as that day's PoZK mining reward.

Please note that the number of ZK-Snarks assigned to PoZK miners is proportional to the number of ZKS pledged by the node itself.

The ZKSwap team is also working hard to develop the GPU compatible Plonk. So when we officially announce it, it is expected to support CPU and GPU to generate ZK-Snarks. Of course, if community members are interested, they can also research the Plonk proof FPGA version and even ASIC chips to speed up ZKSwap's layer-2 proof calculation process and improve ZKSwap's TPS.

If so, ZKSwap's trust-free TPS can break through 100 or even 1,000 as soon as possible. By then, the efficiency advantage of layer-2 is comparable to be dozens or even hundreds of times improvement of Ethereum yet with the same security as the layer-1. It will inevitably bring about the explosion of

blockchain applications on the layer-2. ZKSwap will also become a portal to layer-2, driving all DeFi based on ZKSwap to achieve a smooth experience on layer-2.

Proof-of-TransFee (PoT)

ZKSwap is a new generation of a layer-2 decentralized exchange, and the token swap is the core of the entire system. To incentivize users, ZKSwap introduces Proof-of-TransFee(PoT, proof of transaction fee). All users who trade on ZKSwap layer-2 will get ZKS according to the number of daily transaction fees paid.

Nine percent of the total supply, 90 million ZKS, will be allocated to PoT mining rewards. In the first three years, each year 2.5% will be distributed max, with the rest 1.5% as long-term rewards.
Suppose in the first year, N ZKS will be distributed as PoT mining rewards every day. Specific reward rules are as follows:

Assuming that the transaction fee of all liquidity pools of ZKSwap on one particular day is equivalent to $50,000, and a user pays a total of $50 for the transaction fee, then
The user can get

($50/$50,000) * N ZKS = 0.001 N ZKS

as a PoT mining reward on that day.

Smart Contract Staking (PoS)

To incentivize long-term ZKS holders, ZKSwap will also support Smart Contract Staking after the mainnet is launched. Staking participation and reward distribution are completed through smart contracts to avoid centralization risks. It is expected that 9%of the total ZKS tokens will be distributed through Smart Contract Staking (for the first three years 2.5% max each year, and the rest 1.5% as long term rewards, totalling 90 million ZKS).

Staking participants need to lock ZKS to the designated staking smart contract. The contract will automatically calculate the staking reward based on the locked ratio. Users can not withdraw during each staking period. Suppose during one event, the system sends N ZKS to PoS participants daily. The amount of N is proportionate to the trading volume, number of users and liquidity of ZKSwap. Detailed rules will be published later.

For example, if a user's effective lock-up amount is 50,000 ZKS on that day, and the total lock-up amount in the staking contract is 50,000,000 ZKS, the user is expected to receive

(50,000 ZKS / 50,000,000 ZKS) * NZKS = 0.001N ZKS

on the day. The specific rules and smart contracts for lock-up will be released after the mainnet goes live and will be fully open source.

Please note that:
After ZKSwap launches on the Ethereum mainnet, the first phase of the above community mining activities will be officially planned and announced by the ZKSwap team. There will be a detailed announcement before each event. The number of ZKS for subsequent mining rewards is positively correlated with ZKSwap's trading volume, number of users, and liquidity. The larger the transaction volume, the greater the number of users and locked liquidity, the higher the amount of ZKS prize pool will be unlocked. The specific rules will be released after the end of the first mining activity.

ZKS Usage Scenarios

As the protocol Token of ZKSwap, ZKS represents the holder's rights and has practical utility value. ZKS can be used in the following scenarios.

Governance

ZKSwap is a decentralized project led by the community. ZKS is the certificate of community participation in governance:

- Users who hold a certain number of ZKS can initiate upgrade proposals, such as modifying the transaction fees, editing liquidity mining enabled pools and the ZKS long-term incentive plan, etc.;
- All ZKS token holders can vote on the proposal, and only the proposal with the majority vote will be passed, and the development team is responsible for implementation.

Vote/Pledge for Listing

ZKSwap supports limited trading pairs. Except for the initial trading pairs set by the ZKSwap team, users who hold ZKS can vote or pledge ZKS to list certain tokens:

- ZKS holders can initiate a coin listing proposal through the above governance process, and they can list the coin if they get a majority of votes;
- For users who hold a large amount of ZKS, they can pledge ZKS for listing;

The ZKSwap team will execute token listing based on the results of voting or pledge. All users can create trading pairs or adding liquidity after one token is listed.

ZKS Protocol Fee

The ZKSwap agreement will charge 0.3% of all Layer2 Swap transactions as the transaction fee. Among them, 0.25% will be automatically allocated to the liquidity provider, and the other 0.05% will be used as the protocol fee. All protocol fees (100%) will be used as long-term incentive for the project, and ZKSwap officials will not receive any transaction fees.

Layer-2 Node Plan

As mentioned in the previous section, ZKSwap's layer-2 nodes are responsible for submitting the transaction's zero-knowledge proofs to layer-1. The prover nodes will get ZKS rewards by participating in PoZK mining. These Prover nodes responsible for submitting proofs need to pledge ZKS tokens to obtain the right to generate ZK-Snarks. The amount of the pledge is proportional to the ZK-Snarks task assigned. After ZKSwap goes live on the mainnet, the layer-2 node plan will be released. The prover nodes will participate in PoZK mining to jointly maintain system security and scalability while obtaining ZKS as mining rewards.

To Sum Up

ZKS is the ZKSwap protocol token, which is a crucial link to incentivize participants to build the ZKSwap ecosystem jointly. 90% of the total token distribution will be completed within the first four years. Among them, more than 60% of ZKS Token will be distributed to ZKSwap infrastructure providers via community mining and airdrops, including liquidity providers, Gas fee providers, zero-knowledge proof service providers, early ZKS holders and everyday users.

Users who hold ZKS can participate in ZKSwap governance, to vote or pledge to list tokens, and pledge ZKS to be a layer-2 PoZK node.

Thanks again to the global ZKSwap community for your support of ZKSwap. The ZKSwap team also hopes to work with users to create a real-time, gas-free, and secure layer-2 swap protocol, which will become an important part of the future layer-2 infrastructure.