ZKSwap on ZKSync Era

1 Introduction

1.1 DeFi and DEX

Since 2019, DeFi has rapidly grown, with blockchain developers creating various applications on Ethereum and other major Layer1 networks. The new use cases include exchanges, lending, stablecoins, insurance, oracles, games, etc., leading to an increasingly comprehensive DeFi ecosystem. After the explosive growth led by the DeFi Summer in 2020, the total value locked (TVL) in DeFi exceeded $180 billion in 2021. The biggest smart contract platform Ethereum is the leader in this landscape, with other chains such as BSC, Terra, Solana, Fantom, Avalanche, and Matic competing vigorously.

Following the global tightening of financial policy in 2022, we saw bubbles burst in the DeFi space after several rounds of industry reshuffling. Despite an economic downturn and unfavorable external factors, the TVL of DeFi remained stable at around $50 billion in 2023, with DEXs and lending protocols contributing the most TVL and possessing the most users. DeFi is playing an indispensable role in the global financial market, and as the Web3 industry develops and awareness of cryptocurrency grows, there is still broad room for growth in the future.

Among all DEXs, Uniswap is the pioneer and has gradually expanded to multiple chains. It is a decentralized trading protocol operating on the basis of a constant-product automated market maker (AMM) mechanism, consisting of a series of on-chain smart contracts. Users can create pools of funds by providing ETH and any ERC20 asset, with each pool holding a pair of assets and providing liquidity for trading between those two assets.

When we built ZKSwap in 2021, we incorporated several unique features into the constant-product AMM mechanism, such as allowing users to choose from four tokens to pay the network fee, a 100% buyback and burn program for ZKS tokens, and several rounds of unique liquidity mining. In 2021, ZKSwap achieved tens of billions of dollars in trading volume, with a peak TVL of $2.50 billion. Our team has gained extensive experience through continuous cultivation in the DEX field, and the growth of this field has become a driving force for us to make further breakthroughs.

1.2 Layer2 and ZK Rollups

Although DEXs on Ethereum, represented by Uniswap, have made significant progress in the past, there are still clear shortcomings in terms of user experience. Firstly, the high gas fees, that can be tens of dollars sometimes, deter new users from using them. Secondly, every transaction and operation requires at least one block confirmation, leading to a lack of real-time transaction

experience. Thirdly, due to the TPS limitation on Ethereum, there are obvious ceilings on the number of transactions per second and the transaction capacity. These are the pain points faced by all DEXs on the ETH mainnet.

As a scaling solution for Ethereum, Layer2 networks have become increasingly mature, and various projects in this space have emerged between 2021 and 2023. Among the different technologies they use, the most discussed are ZK Rollups, Optimistic Rollups, Validium, and Plasma.

ZK Rollups: Proposed by researchers of Ethereum, it is characterized by off-chain computing and on-chain storage, and the plaintext data involved in the calculation is sent to the on-chain contract in the form of calldata, reducing storage costs. At the same time, the correctness of off-chain computing is guaranteed by the zero-knowledge proof algorithm. This approach can not only greatly improve TPS, but also reduce the cost of a single transaction.

Optimistic Rollups: There are two types of Optimistic Rollups: Optimistic Rollup (ORU) and Arbitrum Rollup (ARU). Both ensure security through the challenge mechanism. The difference is that ORU challenges a transaction, requiring the EVM to fully execute the challenged transaction, while ARU breaks down the execution process of transactions into ordered instructions, and uses multiple rounds of interaction to identify problematic instructions to challenge, resulting in a lower verification cost. However, compared to ZK-Rollups, the security assumptions of Optimistic Rollups are weaker.

Validium: This solution was proposed by StarkWare and its name was endorsed by Vitalik Buterin. The computation is done off-chain and guaranteed by a zero-knowledge proof algorithm. The verification is done on-chain, and the final world state is stored on-chain. For better scalability, transaction data is also stored off-chain, and a credible Data Availability Committee (DAC) provides proof of data availability. Compared to the previous two solutions, Validium sacrifices some data availability but provides better data scalability. Therefore, this solution is likely to be favored in practical scenarios.

Plasma: Proposed by Vitalik Buterin, Plasma was earlier than the other three solutions, with computation off-chain, storage on-chain, and transaction data stored off-chain. Users can initiate fraud proofs to prove the operator's fraudulent behavior, thereby obtaining rewards and punishing the fraudulent operator.

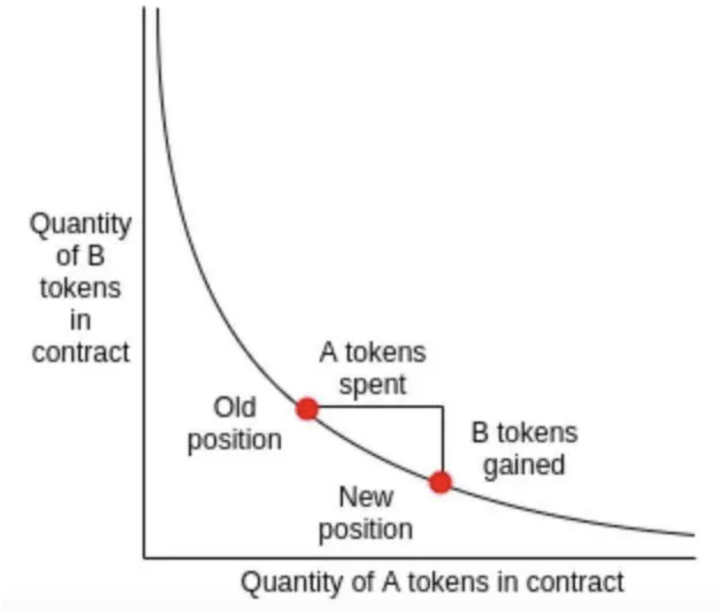
After years of technology development, Validium and Plasma have gradually been phased out, leaving Layer2 development focused on Optimistic Rollups and ZK Rollups solutions. Optimism and Arbitrum represent the Optimistic Rollup solution, and because they are EVM-compatible, Defi protocols on the Ethereum mainnet can easily migrate to Optimism and Arbitrum. Currently, dozens of Dapps covering various fields such as DEX, lending, insurance, and aggregation transactions have been deployed on these two Layer2 networks, bringing billions of dollars in TVL.

Although ZK Rollups are slightly slower in application development than Optimistic Rollups due to their poorer EVM compatibility, their technical solution is superior in terms of security and scalability. Vitalik has repeatedly publicly stated that ZK Rollups are a better solution and an inevitable choice from a long-term perspective. Recently, the ZKSync team launched a compiler-based ZKEVM solution and the ZKSync Era mainnet, which can optimize circuit efficiency and achieve higher performance.

Based on this, we've decided to deploy ZKSwap on ZKSync Era to jointly build a ZK Layer2 ecosystem together with early ZKSync developers.

2 The AMM DEX ZKSwap

With the successful experience of ZKSpace, we will first deploy ZKSwap—a DEX based on the constant-product AMM model—to ZKSync Era.



The above figure is the A * B = K function diagram. As users conduct swaps, the product of the number of two tokens A and B in the liquidity pool stays at a fixed value. Here are some important concepts:

Liquidity pool

Each trading pair on ZKSwap has a single liquidity pool, which can be created by either the official team or the first liquidity provider. Users can create liquidity pools for any two tokens on ZKSync Era, and the first liquidity provider is allowed to freely determine the ratio of those two tokens within the pool.

Liquidity token

Liquidity Providers (LPs) receive Liquidity Provider Tokens (LP Tokens) corresponding to the pool they provide liquidity for, which represent their share of the pool. LP Tokens are ERC-20 tokens that can be transferred without removing the liquidity of the pool. Each pool has its own corresponding LP Token.

Add liquidity

Users can add liquidity in the same ratio as the ratio of tokens in the current pool and receive a certain amount of LP Tokens.

Remove liquidity

LPs can remove liquidity by burning a certain amount of their LP Tokens in the liquidity pool contract and receive the corresponding share of the two tokens used to make up the liquidity pool. The amount and ratio of tokens deposited and withdrawn by the LP may change due to changes in the swap price of the two tokens and the liquidity fee earned during the market-making process.

Swap

After creating a liquidity pool with A and B tokens, users holding either token can start swapping in the pool, exchanging one token for the other. The product of the number of A and B tokens in the pool will remain constant after each swap, as will the total amount of LP Tokens.

For the detailed mathematical model of ZKSwap, please refer to the original ZKSwap White Paper:

https://github.com/l2labs/zkswap-whitepaper/blob/master/zkswap_en.pdf

At the same time, we also support some features of Uniswap V2, as detailed below:

1. **Flash Swap**: Users can obtain the target token first and complete the swap later; or they can return the token within the specified time without triggering the swap process, which is equivalent to borrowing tokens from the pool.
2. **Dynamic allocation of transaction fees**: A 0.3% protocol fee from the input token is charged for each swap, of which 0.25% is distributed as liquidity fees to LP Token holders and the remaining 0.05% is charged by the protocol and sent to a predetermined address. The community can vote to adjust the proportion of the fees and decide on the utility of the protocol fee.
3. **Transaction routing**: In cases where there is no liquidity between the user's input token and the output token, or when the transaction slippage is high due to insufficient liquidity, the protocol will automatically search for the best transaction route. This may involve using intermediate tokens to provide users with a more optimal transaction path. For example:

If a user wants to trade A token for B token, but there is no liquidity for the A/B pair or the slippage for a direct swap is too high due to low liquidity, the protocol will automatically search for a multi-layer optimal route. This may involve swapping A token for a certain amount of ETH, and then swapping that ETH for B token, in order to obtain the highest possible quantity of B tokens for the user's trade.

3 Outlook

As a team, we recognize the significance of DEXs in the DeFi space and we will continue our dedicated efforts in this field. With the deployment of ZKSwap onto ZKSync Era, we will join the teams that are building the ZKSync Era ecosystem and leverage its excellent ZKEVM infrastructure to construct an innovative, user-friendly, and distinctive Layer2 DEX. **Our future plan is not confined to the following:**

1. Launch ZKSwap and initiate a series of activities to enhance the liquidity and trading volume of the platform.
2. Bridge ZKS to ZKSync Era and launch a liquidity bridge to improve ZKSpace/ZKSync Era asset liquidity.
3. Work on ZKSwap V2, adopt a concentrated liquidity solution to further improve capital efficiency and reduce trading slippage.
4. Continue to develop a cross-chain DEX and support liquidity sharing between ZKSpace and ZKSync Era, enabling users to benefit from the liquidity of both chains when trading on either one.

4 Summary

With a long-term focus on ZK Rollups, we've launched DEX, NFT Marketplace, and other products in the ZKSpace ecosystem with impressive results. However, the mass adoption of DeFi still has a long way to go. By expanding ZKSwap to ZKSync Era in 2023, we aim to provide the largest and most user-friendly DEX on ZKSync Era and join ZKSync's mission to accelerate the mass adoption of crypto for personal sovereignty.

Moving forward, we will continue to focus on ZK Rollups, grant more utility to ZKS token, and collaborate with the ZKSync team to further develop a robust Layer2 ecosystem.

ZKSpace team

June 2023