zkSwap - Scaling Decentralized Exchanges through Transaction Aggregation

Paul Etscheit

March 2021

0.1 Introduction

When being launched in 2015, Ethereum set out to change the way we compute. A trustless, permissionless, and decentralized world computer was envisioned, set to open a new class of applications. The importance of running verifiable code in a permissionless and trustless manner cannot be overstated and enables products and services not thought to be possible. However, the technical limitations have also become apparent quickly. Computations are expensive, theoretical transactions per second are low, and the overall throughput has been stagnant. While Eth2 gives a path towards scaling the network, it is expected to take years to complete.

The first major use case for Ethereum was tokenization. With the development of the ERC-20 standard, launching a token on the Ethereum blockchain was trivial. As tokens run as smart-contracts on the Ethereum blockchain, they are secured by its proof of work consensus, which, given Ethereums PoW hash rate, makes consensus attacks infeasible. Running on Ethereum blockchain is a significant benefit when looking to tokenize things, as network security can be assumed. While tokenizations are a step in the right direction, they do not come close to the initial vision. While the standardization enables simple integrations into exchanges and wallets, most tokens are isolated in their functionality and ecosystem and lack productive usage.

token all isolated, not working together... Not a lot of gas needed blabla

With all of these developments over the past couple of years, it seems we have now entered a new phase of smart-contract use-cases, namely Decentralized Finance (DeFi). While DeFi has many different products and functionalities, at its core aims to utilize tokenized assets in some productive form. Collateralized lending is possible with Aave, yields can be generated by providing assets as liquidity or tokens traded in a non-custodial fashion with Uniswap. It can be questioned how useful or necessary these protocols really are, but the core idea behind them is impressive. Rebuilding traditional financial products, running as non-custodial and permissionless smart-contracts, all based on the same standardizations, has the potential to reshape the way finance works. With these developments not looking to slow down, they are quickly overwhelming the Ethereum blockchain, pushing transaction costs higher and higher. With the DeFi space moving quickly, this is becoming a real hindrance to innovation and is the biggest challenge Ethereum is currently facing.

With longer-term scaling solutions in development, several shorter-term approaches have been proposed. While these do differ, they all aim to move transactional data to a layer-2[1] system, ensuring correctness of that data in some way. One of the approaches is called zk-rollup, the focus of this work. Moving data to a layer-2 system can increase the number of transactions that fit into a block, while also reducing transaction costs for the user. Currently, the most used smart-contract is the Uniswap router, which handles

[1] A layer-2 system is a data storage that is not on the blockchain but has its state committed to it some way

all Uniswap trades. To date, it has accrued $290m in transaction fees and makes up around 15% of a block's gas limit, putting strain on the Ethereum network. With rising gas prices, performing Uniswap trades has also become prohibitively expensive. This work will explore how zk-rollups can be used to aggregate Uniswap trades to reduce on-chain transactions while ensuring correctness with a zkSNARK proof. This could be a useful scaling technique, as it reduces strain on the network while at the same time reducing transaction fees for users.

Bibliography