This work suggests that Uniswap trades can be aggregated with zk-rollup, reducing the gas amount per trade. The proposed design is non-custodial, trustless and the data availability problem has been solved by storing state in the event log. Increasing the batch size will further reduce the gas cost per trade while reducing strain on the Ethereum network. The overall efficiency of the proving steps has to be improved to allow bigger batch sizes. The batch size can be increased by several improvements, like utilizing more efficient hashing functions and parallelizing the proving steps.

This work was also aimed at exploring the viability of integrating a zk-rollup based application with third-party smart-contracts. As described in S. **??**, one core problem that has been identified is ensuring the correct return values of the third-party smart-contract interaction are used in the aggregation. In our case, that results in custodial issues of assets. Other problems in other scenarios can be expected as well. Solving this problem would make integrating third-party smart-contracts into a zk-roll application a viable solution.

Projects like zkSync have shown the technological potential of zk-rollup. However, one core difference to our system is that aggregation batches are not dependant on external smart-contract interactions to be executed. As described above, being dependant on other smart-contracts adds complexities to the system that are difficult to overcome. While zkSync is an isolated application that interacts with no third-party smart-contract, rollup to rollup transactions preserve composability between rollup enabled applications. Another development worth mentioning is the prospect of recursive PLONK proofs. Recursive PLONK proofs could enable different smart-contract-like applications to be deployed into a zk-rollup based applications layer-2, secured by its on-chain verification. The idea, proposed by Matterlabs, envisions a zkSNARK based sidechain essentially, securing correct execution with a recursive proof construction, verified on Ethereums mainnet.

Zk-Rollup shows great promise to reduce strain on the Ethereum blockchain. Trustless and permissionless applications can be built with zk-rollup that do not rely on external data availability. Transaction costs can also be reduced significantly, saving users money and reducing strain on the Ethereum blockchain. Some issues remain and need to be resolved, but in general, zk-rollup is a promising scaling solution. Failing to resolve these problems would lead to applications being rebuilt as a zk-rollup native application. Projects like zkSync have shown this to be viable. The ongoing development of zero-knowledge protocols is expected to make the technology a foundation for scaling the Ethereuem blockchain in the near future.