The following is a summary of an article I published recently with my research team as part of my PhD. Don't hesitate to contact me if you have any comments, questions or contradictions! The aim is to exchange ideas and to give my team real feedback from outside the academic world.

TL;DR

- Zk-Rollups appear to be a promising way to improve the scalability of secure public blockchains while providing possible privacy and cost savings.
- We claim that zk-rollups present the advantages of both public and private blockchains providing privacy, customization, scalability, and a large user base along with security thanks to the underlying layer.
- This paper explores the benefits of zk-rollups as well as their potential to support transactions designed for specific applications.
- We study the possibility of having multiple zk-rollups co-exist on the same smart contracts, simplifying their creation and customization processes.
- Easier rollup creation could enable applications with sensitive data to avoid external validators and provers and thus retain data privacy when the rollup is used in validium mode.
- We evaluated the first implementation of our system highlighting a low overhead on existing transaction types and on proof generation while strongly decreasing the cost of new transaction types and drastically reducing zk-rollup creation costs.
- Our evaluation is based on zkSync Lite and is available on github here.

Core Research Question

Can several rollups (Zero-Knowledge or Optimistic) be built on top of a shared set of smart contracts? Does this bring improvements?

Citation

Lavaur, T., Detchart, J., Lacan, J., & Chanel, C. P. (2023). Modular zk-rollup on-demand. Journal of Network and Computer Applications, 103678.

Background

- Verifiable Computation:

A cryptographic protocol (e.g., STARK or SNARK) allowing a prover to convince a verifier of the correctness of a computation through an argument (often called a proof, even if it is probabilistic and not deterministic). They are also called proofs of computational integrity. When they are combined with zero-knowledge, they are called zero-knowledge verifiable computations where the most well-known are zk-STARKs or zk-SNARKs, depending on the cryptographic protocol.

- Optimistic rollups:

Layer 2 scalability solutions where all transactions are considered valid, a priori, allowing for a simple (easy to develop) and fast system. They rely on fraud proofs for their security.

- zk-rollups:

Prove all transactions using verifiable computation, allowing faster finality with fewer assumptions. They are harder to develop which makes it more difficult to make them EVM compatible.

Summary

- The use of blockchains is not a panacea and their use brings its own limitations and problems. The number of transactions per second (TPS) is limited and the cost of these transactions when the blockchain is highly decentralized is too high. This is mentioned in the trilemma of Surya Viswanathan and Aakash Shah between scalability, decentralization and security.
- Since 2019, the use of rollups has been growing and is becoming increasingly popular as an effective solution to the problems arising with the use of blockchains, i.e., Ethereum focused its roadmap on them.
- These solutions provide a significant reduction in transaction costs in exchange for a costly smart contract deployment. Currently, only a few major companies offer the use of permissionless rollups services. However, their solutions imply the centralization of zk-rollup ownership for now, which, while not decreasing security, increases the risk of censorship and decreases customization opportunities for users.

- Zk-rollups allow users to take advantage of pre-established communities, pre-established cryptocurrencies (and pre-audited security if they share the same smart contracts) while offering the flexibility of private blockchains designed for specific purposes.
- Setup requires significant expertise since one must:
- both develop and audit a zero-knowledge circuit that will correctly prove the validity of authorized rollup operations.
- establish safe implementation of the smart contracts.
- set up a central server that will play the role of validator.
- both develop and audit a zero-knowledge circuit that will correctly prove the validity of authorized rollup operations.
- establish safe implementation of the smart contracts.
- set up a central server that will play the role of validator.
- One solution put forward by different companies is to extend these services providing privacy and customization through layer 3s built on top of their own rollup.
- We propose allowing several zk-rollups to co-exist on the same smart contract, by including a group ID (or zk-rollup ID) system directly into the smart contracts. This drastically reduces the cost of subsequent “deployments” after an initial deployment. The functions of the smart contracts are shared by the different groups but it is possible to choose a specific smart contract for proof checking in order to use different circuits or systems.
- Using group-specific parameters, the rollups would either be permissionless or permissioned, post data on-chain or off and be optimistic or zk-rollup. All of this, using the same base of smart contracts.
- We advocate that this proposition solves privacy issues while democratizing easy access to zk-rollups for wider adoption. It can be very interesting even if they are all public and permissionless, bringing different prices, finalities, systems and applications.
- Secondly, we propose adding a new transaction type that can be interpreted by smart contracts and act as a bridge between two rollups. The main idea is to easily allow users to send/receive information or funds from one group to another without having to return them to the user’s address. This acts as a proof of burn to the underlying layer, automatically triggering a deposit request to the targeted rollup.
- Thus, with our proposition, it is possible to create a dedicated zk-rollup at low cost, easily and on-demand, managed by the user who creates the group. Such a zk-rollup can be customized to meet privacy and management needs. With our proposal, it is possible to:
- obtain the properties of the private blockchains we are interested in while also maintaining the security of a public blockchain.
- exchange information from one group to another efficiently and without difficulty as only one transaction, at a reduced cost, is required.
- obtain the properties of the private blockchains we are interested in while also maintaining the security of a public blockchain.
- exchange information from one group to another efficiently and without difficulty as only one transaction, at a reduced cost, is required.

Method

- We added a group field of 16 bits to all transactions natively present on zkSync Lite, enabling the creation of a maximum of 2^{16}

groups on the smart contract.

- We modified the smart contract to include a group structure and added several fields such as a group identifier (or zk-rollup ID), a Boolean indicating whether the group is permissioned or not, and a mapping to manage a whitelist.
- We created two new types of transactions: ChangeGroup and FullChangeGroup, inspired by Withdraw and FullExit
- We have used the Hardhat local network to realize the gas measurements of transactions and the main functions of the smart contracts. We compared the performance of our new operations (i.e. their gas costs) to that of a user wanting to change zk-rollups in a case where two zkSync Lite rollups would be deployed at different addresses and on different smart contracts.
- To compute the proofs, we used a computer with an Intel Xeon Platinum 8164 CPU and 400GB of RAM.

Results

- The addition of the two new operation types, the inclusion of the group in the transactions and the modification of the public input create almost no overhead for the prover. The size of the first circuit only increases from 0.18% for the smallest blocks to 0.32% for the largest blocks, and the difference in proof time is not significant.
- When block size is the largest and the number of aggregated proofs is the highest, the cost of a deposit is only increased by 3% for ERC20 and 2% for ETH, while the rest of the transactions only see their costs increase by less than 1%. The ChangeGroup operation reduces gas consumption by more than 49% for ETH and more than 61% for ERC20.
- During the first deployment of the smart contracts, our proposal leads to an additional cost of about 4%, going from 22,106,772 gas to 22,904,219 gas. However, when we compare the cost of redeploying zkSync Lite with the cost of creating a group with our proposal, costs are reduced by more than 99% from 22,106,772 gas (zkSync Lite) to 184,258 gas.
- All of our graphics showing the results are available ongithub.

Discussion and Key Takeaways

- Our paper explores a different approach than deploying layer 3s for customization and application-specific rollups. In this cas, if the layer 2 validator becomes untrustworthy, it is not clear how this would affect the different layer 3s. Moreover, the layer 2 validator would still have visibility on all layer 3 transactions reducing privacy possibilities.

Implications and Follow-Ups

- Our proposition replaces the consecutive deployment of several rollups with a simple call to the smart contracts via a function enabling the creation of a group. This drastically reduces the cost of subsequent deployments following the initial one.
- We also propose a new set of transaction types that allow simple and low-cost transfers from one group to another like a bridge.
- However, as of yet, our implementation does not enable the creation of validium groups. This implementation may be necessary and is left for future work.
- We have developed our implementation over zkSync Lite, and we believe it would be interesting to apply it to a zkVM-compatible zk-rollup. Unfortunately, ZkSync Era was made public and open source just after the end of our implementation and so, we leave this avenue open for future exploration.

Applicability

- We are convinced that zk-rollups are the solution to many scalability problems and that they are part of the solution to enable the global adoption of blockchains across many sectors.
- Any application that cannot currently be deployed on blockchains due to their low capacities, can investigate the use of zk-rollups.
- Turnkey rollup creation without the need to audit or deploy smart contracts will make the adoption of rollups and blockchains simpler for applications outside of the fields of blockchain, cryptography or finance. This will bolster confidence in the security of smart contracts, enable strong privacy and greater flexibility in system customization.