### 0.0.1 zk-rollup

Zk-rollup [**?**] is a layer-2 scaling approach first introduced to mass validate transfer of assets on the Ethereum blockchain in 2018. A user can deposit funds into a smart contract by providing a merkle path to its balance and adding funds to be deposited to the transaction. The smart-contract checks if its root can be recreated with the provided merkle path, updates the balance according to the funds in the transaction, rehashes the entire tree and updates its root to the resulting hash. An event is then emitted, containing the new balance, putting the data on-chain is a cheap way. The merkle tree, which is required for generating the merkle paths, containing the balances can be kept in sync by listing to these events.

To make a transfer, a user sends the receivers address, tranfer amount and its signature to the relayer as an http request. Once enough transfer requests have been received, the relayer checks if this transfer is covered by a users balance and if the signature is valid, and updates the balance of involved users accordingly. All of this is done in a zkSNARK program, which will return a proof object, the new balances and the new merkle root. These are then sent to the smart-contract. If the zkSNARK proof can be verified, we have proven that the new balances and the root are correct. We now emit the new balances as an event, thereby moving custody of transfered funds to the receiving users, who are now able to transfer or withdraw them. Withdrawing of funds follows the same logic as depositing, however instead of sending funds, a parameter is added containing the requested amount.