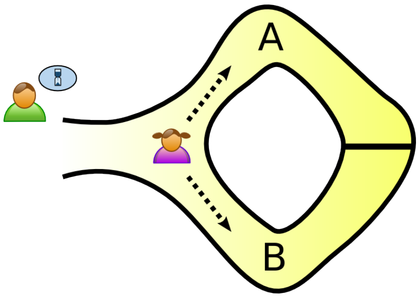
Prof. R. Wattenhofer

# Zero Knowledge Rollups in Python3

Blockchain systems like Ethereum do not support 1000's of transactions per second without resorting to so-called L2 systems - where orders of more transactions are executed off-chain, but succinct commitments to their results are written on-chain. Zk-SNARK is an acronym that stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge", and in some cases, the L2 layer provides a ZK-SNARK based proof that all of its transactions are valid, and a smart contract on the base blockchain verifies this proof.



In this project, we investigate possible ZK-SNARK schemes where the prover is implemented in an off-chain general purpose language (say, Python3), and the verifier smart contract is written in Ethereum supported languages like Solidity or Vyper. The focus will be more on clarity of the ZK-SNARK and transaction data structures than gas efficiency/smart-contract design.
**Requirements:** This project involves understanding Ethereum, ZK-SNARKS, smart contract design, being able to program in Python3 and Solidity/Vyper.

**Interested? Please contact us for more details!**
**Contact:** Tejaswi Nadahalli: tejaswin@ethz.ch, ETZ G97