Master’s Thesis
zkSNARK-based Scalable Off-chain Value Transactions

Context
Currently, transactions in blockchain networks are processed redundantly at every node in the system. This happens in order to ensure validity of the blockchain’s state transition. However, this concept of data storage and processing at maximum redundancy imposes strong limitations on scalability. Off-chain computations can address this issue by off-loading the computation of state-transitions from the blockchain.

Problem
Recently, zkSNARK-based off-chain transaction processing systems to improve performance of value transactions have been proposed [1, 2]. However, actual performance of such a system in practice is not clear.

The general idea behind these approaches is the following [1]:
A merkle tree stores user balance in leaves of a merkle tree together with the public keys of the users. The root of this merkle tree is stored on the blockchain. Now, a value transaction essentially is an update of the merkle tree in a way that the leaves change, but the sum of the leaves remains constant and spends are signed by the user owning the balance.

A set of such updates can be batched together in one zkSNARK, which can then be efficiently verified on the blockchain and update the on-chain merkle root to the latest value.

Research Question
How can such a system be implemented and how does that implementation perform? Which throughput is achievable and what are limitations?

At ISE, we designed ZoKrates [3], a software tool which allows a more convenient programming abstraction for zkSNARKs, which can be used for the implementation in this thesis.

Skills: Good knowledge of blockchain systems, strong programming skills, basic knowledge of cryptography, curiosity

Resources:
2. https://ethresear.ch/t/roll-up-roll-back-snark-side-chain-17000-tps/3675

Contact: Jacob Eberhardt je@ise.tu-berlin.de

Our Mission:
Our lectures cover fundamental methods and techniques in the areas of service computing, cloud computing, and enterprise computing. We like to engage students in hands-on building of distributed information systems and to take an interdisciplinary approach to evaluating such systems. Through a close mentoring of students, especially in our seminars, we aim to introduce students to our ongoing research and to excite them to do future studies and research with us.