Technical University of Munich

Thesis B.Sc. Thesis M.Sc. IDP

Scalable Off-Chain Computing on Data Streams using Trusted Execution Environments

Motivation

As the adoption of blockchain applications grows, scalability becomes one of the key challenges faced by blockchain networks. Off-chain computing refers to computations that take place outside of a layer-1 blockchain. The basic idea of off-chain computing is to enhance blockchain scalability by offloading certain computation tasks from the layer-1 blockchain without sacrificing the security of the entire system. Off-chain computing is able to reduce the computational burden on the underlying layer-1 blockchain effectively, thereby resulting in improved transaction throughput and user experience. In the context of decentralized IoT applications, off-chain computing is a critical scaling component for handling a large number of IoT devices and data streams. Trusted execution environments (TEE) provides an effective hardware-based approach to proving validity of computations via a remote attestation. In this thesis, a student will investigate how to use TEE to build a scalable off-chain computing solution on IoT data streams.

Your Task

- Familiarize yourself with the topics (public blockchain, off-chain computing, trusted execution environments, data streaming in IoT)
- Research on the existing off-chain computing scaling solutions (rollups, zero knowledge proof, TEE)
- Design a TEE-based off-chain computing architecture on IoT data streams
- Build a proof-of-concept (PoC) implementation
- Evaluate the performance of the system

Requirements

- Knowledge in a common programming language
- Ability to write easy maintainable code
- Possible experience with TEEs

Sources

- [1] https://chain.link/education-hub/off-chain-data
- [2] https://entethalliance.github.io/trusted-computing/spec.html
- [3] https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9125420

Contact

Filip Rezabek frezabek@net.tum.de
Dr. Xinxin Fan xinxin@iotex.io