Technical University of Munich

Thesis B.Sc. Thesis M.Sc. IDP

Offering Privacy to Blockchain Clients

Motivation

Since the origin of blockchain protocols privacy of its users has become a significant topic. Blockchain protocols like ZCash and Monero aim to offer privacy to transactions. Even such solutions allow for privacy leaks on the networking layer.
Therefore, we want to identify current solutions offering privacy at the network and application layers, e.g., Nym [1]. Once such solutions are in place, it is crucial to assess the impact on the overall system's performance and its impact on its performance. It is essential to identify processing or other bottlenecks and consider ways to deal with them, e.g., using HW acceleration of cryptographic primitives [2] or network functionality [3]. Finally, with a proper analysis we can identify suitable steps on how to integrate underlying privacy preserving network to the blockchain protocol without impacting its performance.

Your Tasks

- Get familiar with the infrastructure of the Chair for reproducible blockchain experiments
- Get familiar with the blockchain technologies
- Identify suitable approaches for privacy and security aspects for users' privacy
- Implement the techniques into the evaluation framework
- Evaluate the impact of the techniques on overall performance of the system

References

[1] - https://nymtech.net/nym-whitepaper.pdf
[2] - https://ieeexplore.ieee.org/document/5703261
[3] - https://arxiv.org/abs/2104.06968

Contact

Filip Rezabek rezabek@net.in.tum.de
Richard von Seck seck@net.in.tum.de