Master’s Thesis
Exploring TEE-based Preprocessing in Blockchain-based Applications

Context
Blockchain technology is increasingly applied in contexts where critical measurements generated by sensor devices are to be processed and stored in a secure and trustless manner. One use case is decentralized energy trading [1]. However, while blockchains suffer from privacy and scalability limitations, the data generated by sensors is typically large scale and potentially sensitive. Consequently, not all data can be stored on the blockchain. One way to hide sensitive data and reduce the on-chain data footprint is off-chain preprocessing.

Problem
Since blockchains are typically applied to solve trust issues among collaborating but distrusting parties, blockchain application users are typically non-trusted and so are any preprocessing activities executed off-chain. To solve this problem and allow on-chain verification of the computational correctness of off-chain preprocessing activities, Trusted Execution Environments (TEE) [2,3,4] provide a promising solution. However, to date, verifiable off-chain computation using TEEs has not sufficiently been investigated and, hence, insights about performance, applicability, and other qualities are missing.

Tasks
To address this problem and gain meaningful insights, three tasks are to be solved as part of this thesis:
1. Analyze how TEEs can be applied for preprocessing in blockchain-based applications by reviewing relevant literature. How can the computational correctness of TEE-based processing be verified on-chain?
2. Design and implement a TEE-based preprocessing workflow for sensor-generated data similarly to the example depicted in Figure 1. Explore the applicability of existing TEE programming abstractions, e.g., Microsoft’s Open Enclave [3] or Google Asylo [4].
3. Benchmark the workflow’s performance based on meaningful metrics, e.g., throughput and cost. Discuss and evaluate experimental results. How does the performance compare to a non-TEE deployment?

Skills
• Good programming skills.
• Basic knowledge of blockchain technology (Ethereum) and smart contract development (Solidity).
• Expertise in TEEs and benchmarking beneficial.

References

Contact: Jonathan Heiß, Email: j.heiss@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.