Task description - Master Thesis

Name, Vorname:	Idrees, Mujtaba
Studiengang:	Distributed Systems Engineering
Matrikelnummer:	4807174
Thema:	***Trusted computation based ecosystem for blockchain and beyond***

Blockchain provides computational trust by replicating the ledger state across the nodes. Most blockchain technologies of today support smart contracts which are executed by miners in the network. In doing so the contract between two parties becomes available for every node in the network. Essentially, we trade privacy for trust. For a better blockchain adaptability and integration in real-world systems the blockchain technology of future must be privacy preserving without trading off the trust factor.

Meanwhile a lot of work is being done in the field of trusted computing. By means of trusted computing we can ensure that correct program is being executed and execution of a particular workload is not visible to other processes and even the root admin, thus mitigating the possibility of meltdown or side channel attack. Pertaining to the privacy benefits of trusted computing it makes sense to leverage its properties to make the future blockchains more secure and privacy preserving. Moreover, if we somehow off-load the heavy computational work from blockchain to separate worker nodes it would make the blockchains lightweight and more scalable.

Hyperledger foundation has an ongoing project named "Hyperledger Avalon" that is trying to solve the same problem. It aims to enable creation of a network of dedicated trusted compute workers which could serve both blockchains and non-blockchain based clients. The Avalon project is still in its incubation phase and they have published an opensource architecture of the product and a demo application as a proof of concept with minimum functionality i.e. only a singleton worker node of Intel SGX based trusted execution environment. The key management of trusted compute workers and their implementation in scalable and fault tolerant clusters is still an issue for Avalon developers.

There are multiple platforms that support application deployment upon Intel SGX based trusted compute workers and one of them is "SCONE". It enables trusted execution of complex applications in docker based containers on Intel SGX hardware. It has inherent support for Kubernetes based clusters and has an efficient mechanism of key management and attestation. Hence SCONE platform can be reused and plugged inside Hyperledger Avalon's current design to make it more scalable and fault tolerant.

This thesis proposes a ***Trusted Computation based Ecosystem for Blockchain and Beyond (TCEBB)*** – An ecosystem that would enable thin and secure future blockchains by off-loading the heavy computations to outside trusted workers. At the same time, it can also be used as privacy preserving function as a service for end users. The main idea of the thesis would be to fork the opensource code of Avalon at current point or some stable release that supports blockchain integration and basic registry service for trusted compute workers and then merge it with SCONE based clusters that it supports out-of-box.

The thesis would have the following high-level tasks:

- Fork Avalon to have SCONE workers
- Evaluating how to fit SCONE out-of-box into Avalon ecosystem
- Use SCONE with Kubernetes to support worker pools in Avalon
- Evaluating key management techniques of SCONE & Avalon and figure out how to use SCONE's key management out-of-box
- Support fault tolerance in scone based trusted workers
- Compare Avalon's native workers with SCONE based worker pools (If available)

This thesis would be done in collaboration with T-Systems MMS and is a possible service for German Blockchain Ecosystem (GBE). It will be written in English.

Betreuer:	Dr. Do Le Quoc
Zweitgutachter:	
Verantwortlicher Hochschullehrer:	Prof. Christof Fetzer
Institut und Lehrstuhl:	Systemarchitektur, Systems Engineering
Beginn am:	
Einzureichen am:	

Student	Betreuer	Verantwortlicher HSL