Technical University of Munich

TUM

Federated Identity and Transaction Management over Blockchain

Motivation

Various large technical infrastructures are federations of smaller ones operated by individual organizations. An example is eduroam, which consists of various WLANs of different universities. The management of eduroam users is decentralized: each university is responsible for identity management of those users belonging to the university. Trust relationships between participating universities enable identity federation and users can use the same login as at home.

One particular problem is that the administrator of a local organization might perform faulty or even hazardous configurations. For this reason the idea is to distribute the power over keys, identities, and related objects to multiple entities who have to agree on changes instead of giving each administrator the power to do this.

Approach

In this thesis we want to investigate how identity management and related federations can be decentralized with the help of Blockchain technology. In particular, we want to examine how federated identity management can be performed over Blockchains in an eduroam-like scenario. Besides ordinary use cases, like issuing credentials (e.g. a certificate) to a new user, the system also needs to cover failures and changes. For instance, organizations need to be able to change the set of admins with key signing power, etc. Furthermore, users need to be able to update their key and invalidate the old one. We might also want to bootstrap new organizations which requires multi-party approval.

Our idea is to use the Blockchain as basis and design a solution on top of its transactions or smart contracts. There are many open issues that we have to resolve!

Your Tasks

1) Study related work (e.g. Blockstack) and other Blockchain-based ID management solutions. **2)** Study the scenario and further define it: write user stories, define requirements. **3)** Compare requirements from our scenario with related work. **4)** Design a concept based upon existing Blockchain software such as Multichain or Hyperledger. **5)** Elaborate how multi-party approval can be achieved in the scenario. **6)** Implement a demo showcasing selected functionality of the overall system.

Contact

Dr. Heiko Niedermayer   niedermayer@net.in.tum.de
Dr. Holger Kinkelin   kinkelin@net.in.tum.de