A Decentralized Shared Calendar in Blockchain

Whether any individual wants to make an appointment with the doctor's, the Citizens Registration Office, or the barber's, one has to rely on that authority to provide accurate information on the availability of the appointment one is endeavouring to make. The following solution aims to solve this issue by creating a decentralized unalterable calendar for such institutions that give all seekers of an appointment democratic and equal access to available timeslots.

The necessary components to be designed are means to identify on the one hand the individual - a uniquely identifiable and authenticable individual - and on the other hand the desired institution. Beyond that the process for identifying, selecting, and fixing an appointment in a free timeslot and then storing that information needs to be fashioned.

Identification and Authentication of Individuals and Institutions

Any natural person is uniquely identifiable by a set attributes such as a first and last name, a place and a date of birth. Constant length digests respectively created from such a paradigmatic data set with a given hash function are usable pseudonyms for persons. In the following such hash values will denote wallet IDs. For someone to now participate in this scheme of decentralized appointment fixing at any institution a verification of this person is necessary. To that end existing methods such a POSTIDENT is used to verify the affiliation of a certain wallet ID to an individual. After such a verification by an independent entity the wallet ID becomes usable. When then at some point a person actually observes an appointment, they can be authenticated in situ by comparison of the aforementioned personal data and one's wallet ID.

Similar to the hash function described above, a unique identifier of a participating institution (e.g. location in coordinates) can also be hashed to a constant length digest.

Identification, Selection, and Fixing of an Appointment and Storage in a Blockchain

A key property of a blockchain is that the data stored within is stored in a decentralized and unalterable fashion. For this solution the blockchain contains transaction data in blocks, where these blocks store the information of a fixed appointment of an individual (identified with their respective wallet ID) at a specific institution (identified with their respective constant length digest). The privacy of any participant is ensured by the inherent pseudonymity of the architecture.

The storage of made appointments is facilitated by an object for each participating institution which is modified with each fixing of an appointment to represent the current availability schedule of that institution. This object can be read in order to identify free and taken appointments. Thereafter only transactions onto free timeslots can be taken.

Technical Challenges and Outline

The first step to the realisation of a prototype will be the implementation of a Smart Contract on top of the Ethereum Blockchain, that allows for reliable fixing, storing and potential rejection of appointments from participants' wallets with institutions' wallets.

The second step is a realisation of the identification measures in form of unique identifiers for individuals and institutions that are translated into wallet IDs by constant length hash functions.

The third step will be a realisation of a visualisation of the availability schedule object of institutions and therein a comfortable solution for selection and fixing of an appointment. Herein a token-like mechanism will need to be devised, so as not to enable malicious participants to block all calendar entries with fraudulent dates.

Finally, a scheme for the cancellation of appointments will need to be considered, designed and implemented.

project group stellar: Marcin Bosk | Fabian Hofmann | Dominik Nafz | Jörn Strömsdörfer