



## Proof of Personhood

Encointer is a blockchain platform that aims to issue a universal basic income by means of community cryptocurrencies. To prevent Sybil attacks, the system relies on a proof-of-personhood algorithm, where participants have to attend meetups in person regularly at predefined times and locations to prove their human existence. Encointer is built as a Polkadot [1] parachain, using the subtraTEE framework [2].



This thesis aims to tackle scalability issues of Encointer. One urgent problem of the system is the computation of the meetup locations which have to meet certain properties, the most important being a mutual minimum distance to ensure the security of proof-of-personhood. As this computation is expensive, it should be implemented off-chain. The goal of this thesis is to find efficient means of verifying those locations on-chain in  $\mathcal{O}(n)$ . Other potential issues to be tackled include assigning participants to meetup locations or the actual issuance of the currency.

The thesis will be co-supervised by Alain Brenzikofer from the Encointer association.

**Interested? Please contact us for more details!**

**Contact:** Tejaswi Nadahalli: [tejaswin@ethz.ch](mailto:tejaswin@ethz.ch), ETZ G97

[1] Polkadot: Vision For a Heterogeneous Multi-Chain Framework (2016).

[2] SubtraTEE: <https://www.substratee.com>, visited May 21, 2021.