ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

BA/MA:

Sleepy Bitcoin

Nakamoto's consensus protocol used in Bitcoin is considered to be very robust in practice. The reason behind this "robustness" is the protocol's ability to withstand sporadic participation in a permissionless setting in an asynchronous network. Bitcoin miners can be "sleepy" and go offline for a non-specific amount of time. In this "Sleepy Model" all previously known consensus protocols fail regarding security.

In this thesis, you will investigate the recently emerged "Sleepy Model of Consensus" and blockchain' s theoretical framework. Specifically, you will focus on blockchain's security proofs in the random oracle model. Your goal will be to comprehend the aforementioned work and combine them towards a proof of "robustness" for the Bitcoin protocol.

Requirements: Knowledge of discrete mathematics and cryptography. Basic knowledge on blockchain technology and/or mathematical maturity will be an advantage!

Interested? Please contact us for more details!

Contacts

- Zeta Avarikioti: zetavar@ethz.ch, ETZ G95
- Yuyi Wang: yuwang@ethz.ch, ETZ G94