ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

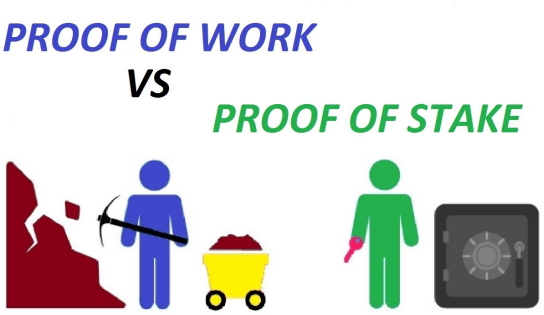
Prof. R. Wattenhofer

BA/MA/SA/Group:

Proof of Stake Blockchain Protocols

Proof of Stake (PoS) is a category of consensus algorithms for public blockchains that depend on a validator's economic stake in the network. In contrast to the typical mining process, known as Proof of Work, which is used in most cryptocurrencies nowadays to define the next block validator, PoS is considered more secure and energy efficient, while the threat of centralization is considerably reduced. Various provably-secure PoS protocols have been proposed so far such as Casper, Ouroboros, Algorand, Snow White etc.

In this thesis, your task will be to study the state of the art PoS protocols, explore their properties and weaknesses. Furthermore, you will implement one of those protocols or maybe a new and improved one. Your ultimate goal will be to design a future cryptocoin that exploits the advantages of PoS consensus protocols and maybe in the process identify specific attacks and propose solutions.



Requirements: Basic knowledge of discrete mathematics and advanced programming skills. Knowledge of blockchain technology and cryptography 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