



BA/MA/SA:

A Hybrid Blockchain System

In January 2018, *The Guardian* wrote about the Bitcoin cryptocurrency:

Bitcoin's electricity usage is enormous. In November, the power consumed by the entire bitcoin network was estimated to be higher than that of the Republic of Ireland. Since then, its demands have only grown.

Scientists have tried to resolve these climate-related issues with the current blockchain implementations by replacing so-called *proof of work* systems with *proof of stake* systems.

In brief, in a proof of work system, distributed consensus is achieved through miners proving to have done a significant amount of work – hence, making it costly to cheat. In such a system, miners do not necessarily own any of the currency they are mining.

In a proof of stake system, however, the consensus protocol is not dependent on computing power but on possession of the cryptocurrency. In other words, those protecting a currency's value will always be the largest stakeholders.

In this thesis, you will explore both proof of work and proof of stake systems with a focus on the Ethereum proposal called Casper.



Requirements: Basic knowledge of probability theory is necessary. A general interest in formal proofs and blockchain technology is an advantage.

Interested? Please contact us for more details!

Contacts

- Georgia Avarikioti: zetavar@ethz.ch, ETZ G95
- Roland Schmid: roschmi@ethz.ch, ETZ G94