ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

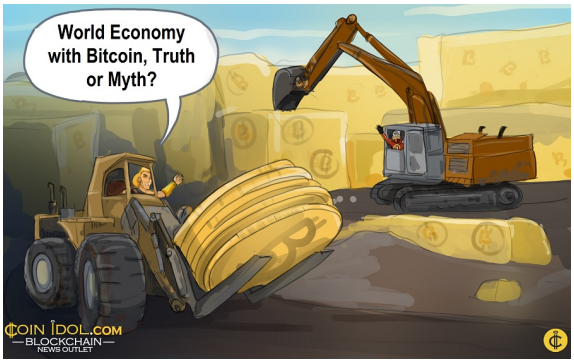
Prof. R. Wattenhofer

BA/MA/SA/Group:

Bitcoin as a Selfish Game

Cryptocurrencies are expected to be influential. Bitcoin is considered the "gold" of cryptocurrencies since it is the original, most famous cryptocurrency, with the largest market cap. However, many attacks have been proposed and not yet dealt with, e.g. selfish mining. From an economic point of view, honest mining might not be optimal when miners act as selfish agents. On the other hand, it seems that for small mining pools honest mining is optimal.

In this thesis, you will combine economics with cryptocurrencies and investigate some fundamental questions regarding this marriage. Ideally, you will focus on Nash Equilibria and optimal strategies of selfish miners on the Bitcoin network. A more realistic model where everyone acts as a selfish miner shapes a completely different network dynamic and your main task will be to explore it.



Requirements: Knowledge of blockchain technology and proof-of-work, cryptography, basic game theory.

Interested? Please contact us for more details!

Contacts

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

Papers to read:

1. Bitcoin: A peer to peer electronic cash system. Satoshi Nakamoto
2. Majority is not Enough: Bitcoin Mining is Vulnerable. Eyal et al
3. Blockchain Mining Games. Kiayias et al
4. FruitChains: A Fair Blockchain. Rafael Pass, Elaine Shi
5. When cryptocurrencies mine their own bussiness. Jason Teutsch, Sanjay Jain, and Prateek Saxena

Questions:

- Is there a Nash equilibrium where all miners play honestly?NO (FAW ATTACK)
- Under which circumstances could there exist an NE where selfish miners play honestly?

Other potential directions:

- Prove Bitcoin is secure on the sleepy model of consensus.
- Study proof of stake protocols (Snow white, Ouroboros, Algorand, iChing?, Fruitchain?). Comparison and attacks. Design a new proof of stake protocol (using a known consensus algorithm?). For bachelor thesis: implementation of one of the protocols.
- Is the dominance mechanism of Bitcoin optimal or not? (Panagiotakos, GHOST paper)
- Trust is risk (decentralized market places). Game theoretic modeling.