Joseph Bonneau

jbonneau@cs.stanford.edu
www.jbonneau.com

Bitcoin Overview & Mining

Monday, May 30 2016, 9:30-10:30 & Monday, May 30 2016, 16-17:30

The overview lecture provides a technical basis for understanding Bitcoin and other modern cryptocurrencies. We show how to use digital signatures to transfer digital tokens, how to build a blockchain and use it to detect double-spending, and how to use computational puzzles to maintain consensus on a blockchain in a decentralized manner.

In the next lecture we'll dive deep into the world of Bitcoin mining. We'll look at the technical challenges facing miners and how hardware has evolved to meet the task and consider the economics of the mining process as well as the rise of mining pools. Most importantly, we'll cover the strategic choices facing miners, with deviant strategies such as "selfish" mining, pool sabotage attacks, whaling and feather forking.

Reading:

- Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll and Edward W. Felten. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. IEEE Security & Privacy 2015. http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf
- Ayelet Sapirshtein, Yonatan Sompolinsky, Aviv Zohar. Optimal Selfish Mining Strategies in Bitcoin. https://arxiv.org/abs/1507.06183
- Ittay Eyal. The Miner's Dilemma. https://arxiv.org/abs/1411.7099