ETH Zurich, Department of Computer Science
SS 2020

Prof. Ueli Maurer
Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 13

13.1 Mining Pools

In order to win a reward in Bitcoin, miners generate blocks. Given that a miner's computing power is typically a small fraction of the total computing power this means that each miner rarely generates a block. Even though the revenue may be positive in expectation, a miner may have to wait for an extended period to obtain a reward.[1]

a) Design a mechanism that allows to reduce the *risk* of miners, while keeping the expected revenue. For this subtask, you may assume miners are honest.

HINT: Consider mining pools. How can one distribute the revenue?

b) In the above solution, consider a pool with total mining power $\alpha \in [0, 1]$, as a fraction of the total mining power, and a participant P in the pool with mining power $\beta < \alpha$. What is the expected revenue for P? Assume rewards are distributed proportionally.

c) In a withholding attack, a miner *pretends* to never find a complete solution. Consider the scenario with solo miners and two mining pools, M_1 and M_2, where M_1 uses some of its miners to perform a withholding attack on M_2. What is the revenue of each pool?

d) Compute the revenue when the two pools perform withholding attacks among each other.

[1] See the mining pool analysis by [Eyal14]: `https://arxiv.org/pdf/1411.7099.pdf`