Fee-Redistribution Contracts

1

Problem Definition

- ***Mining gap problem*** - miners not mining after new block was found until they have collect enough transactions to cover their expenses
- ***Undercutting attack*** - malicious miner remines top block to claim some fees from such block. Leaving fees to incentivize mining on his block. Please refer to Figure 3.
- ***Fluctuation in revenue*** - collected fees are created from dynamic market resulting in fluctuations.

2a

Proposed Solution

Contract defined as tuple *FRC*(v, λ, ρ),

- v - total value in collected coins in contract FRC
- λ - target length, at which we target to redistribute collected fees
- ρ - percentage of collected fees sent to this contract FRC,

where the miner receives reward nextClaim. This reward is calculated as sliding window average of total value in all contracts.

2b

$$nextClaim_{[H+1]} = \sum_{\mathcal{FRC}_{[H]} \in \mathcal{FRCs}_{[H]}} \frac{\mathcal{FRC}_{[H]}.\nu}{\mathcal{FRC}_{[H]}.\lambda}$$

2c

Single Contract

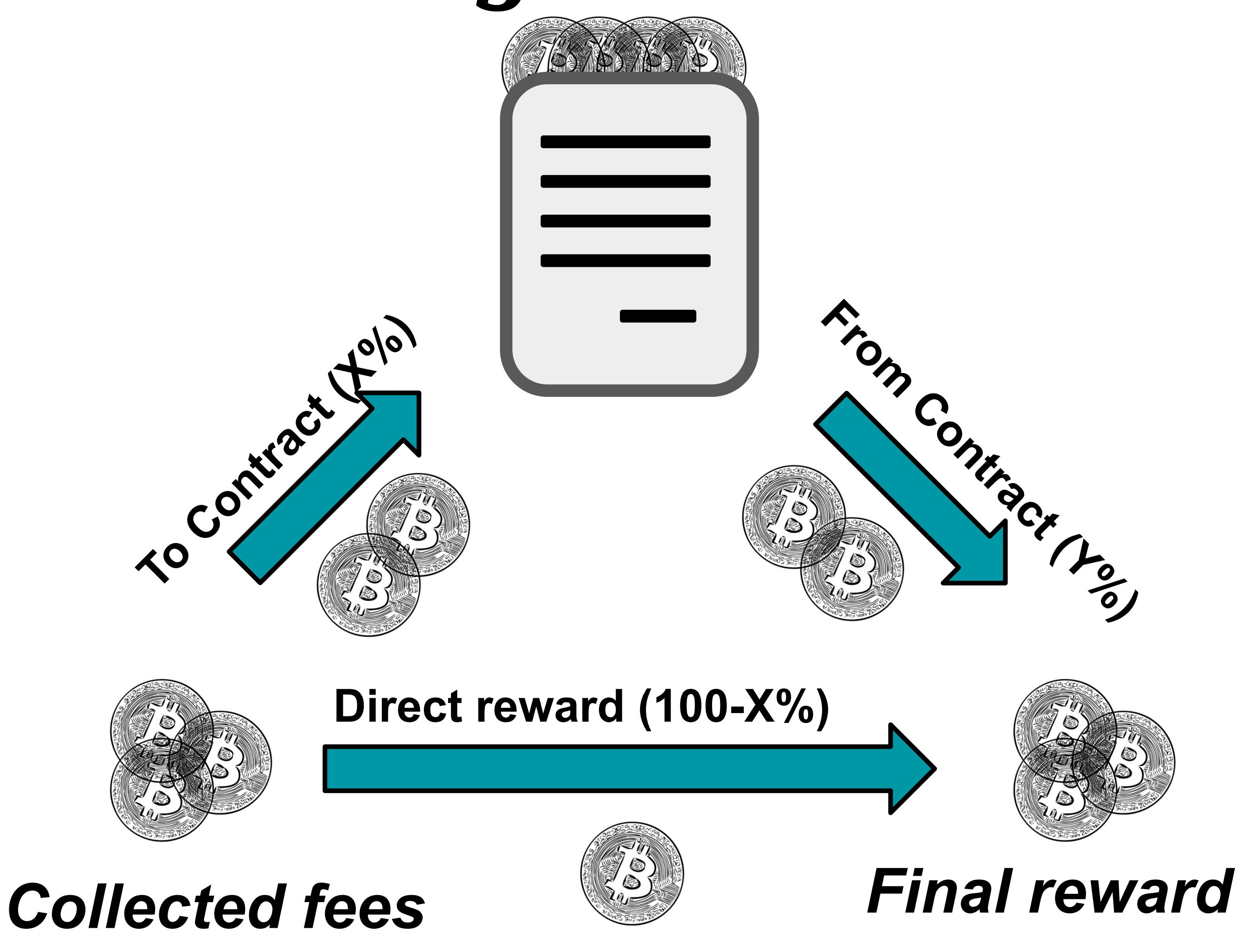


Figure 1.

3

Miner's reward fluctuation

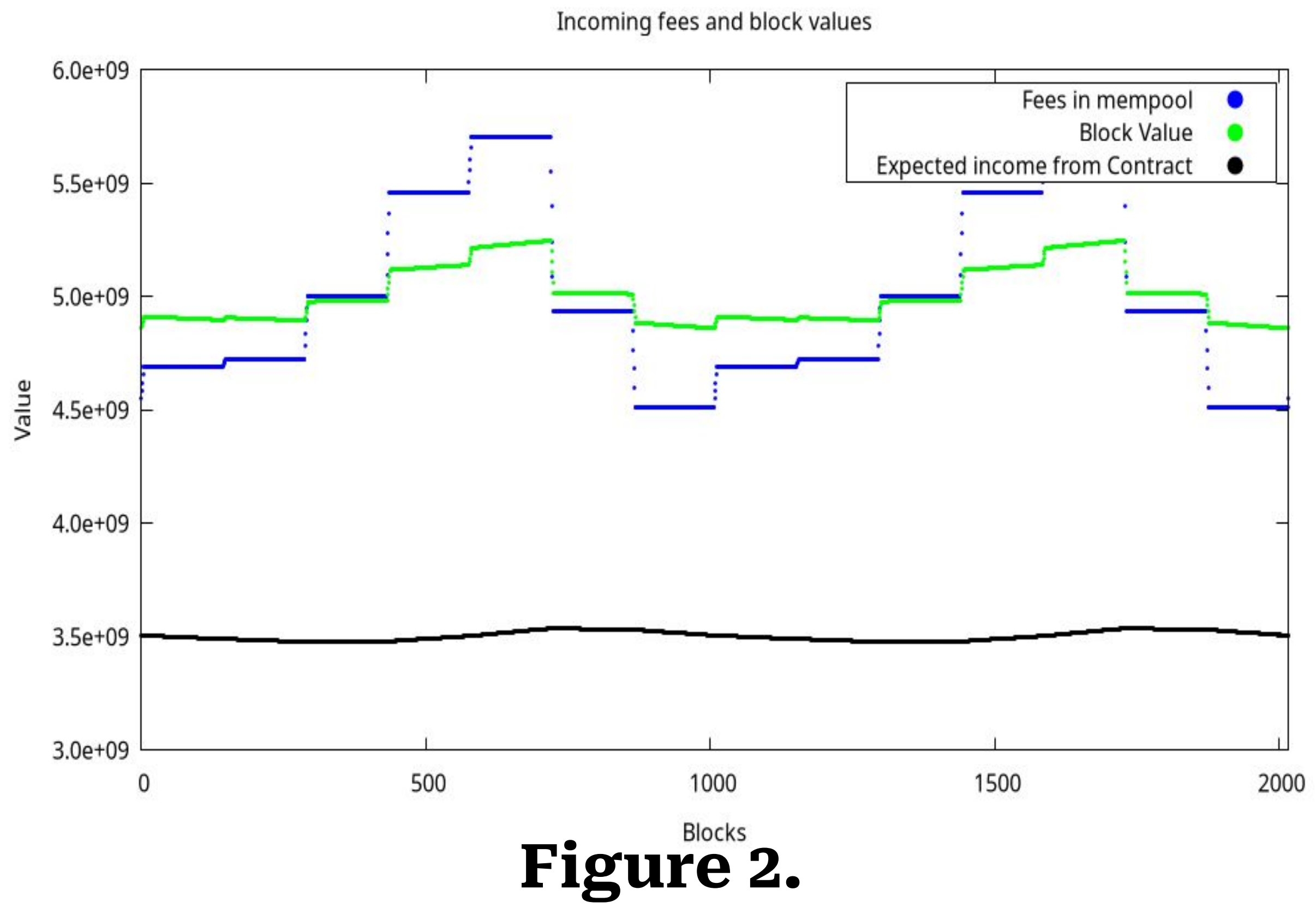
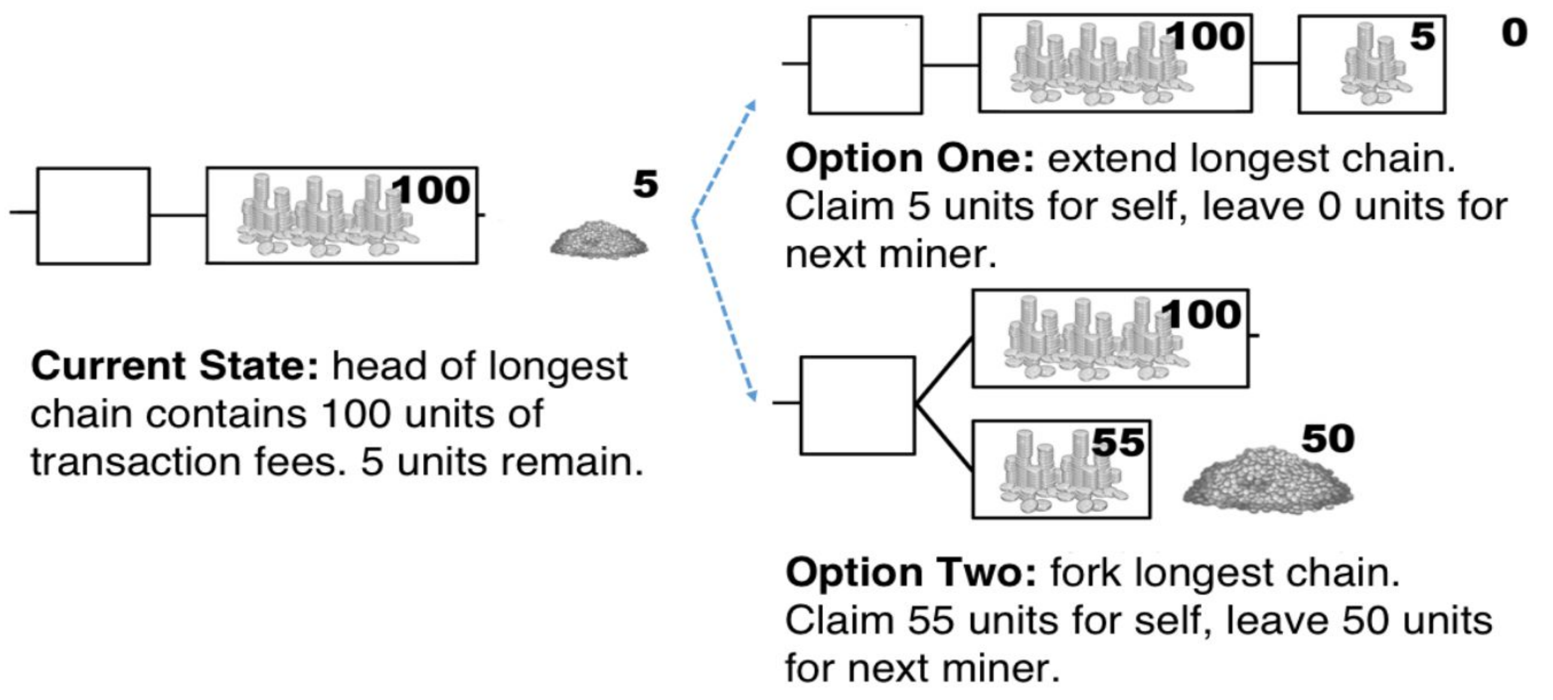


Figure 2.

4

Undercutting attack



Current State: head of longest chain contains 100 units of transaction fees. 5 units remain.

Option One: extend longest chain. Claim 5 units for self, leave 0 units for next miner.

Option Two: fork longest chain. Claim 55 units for self, leave 50 units for next miner.

Figure 3.

Mitigation of undercutting attack

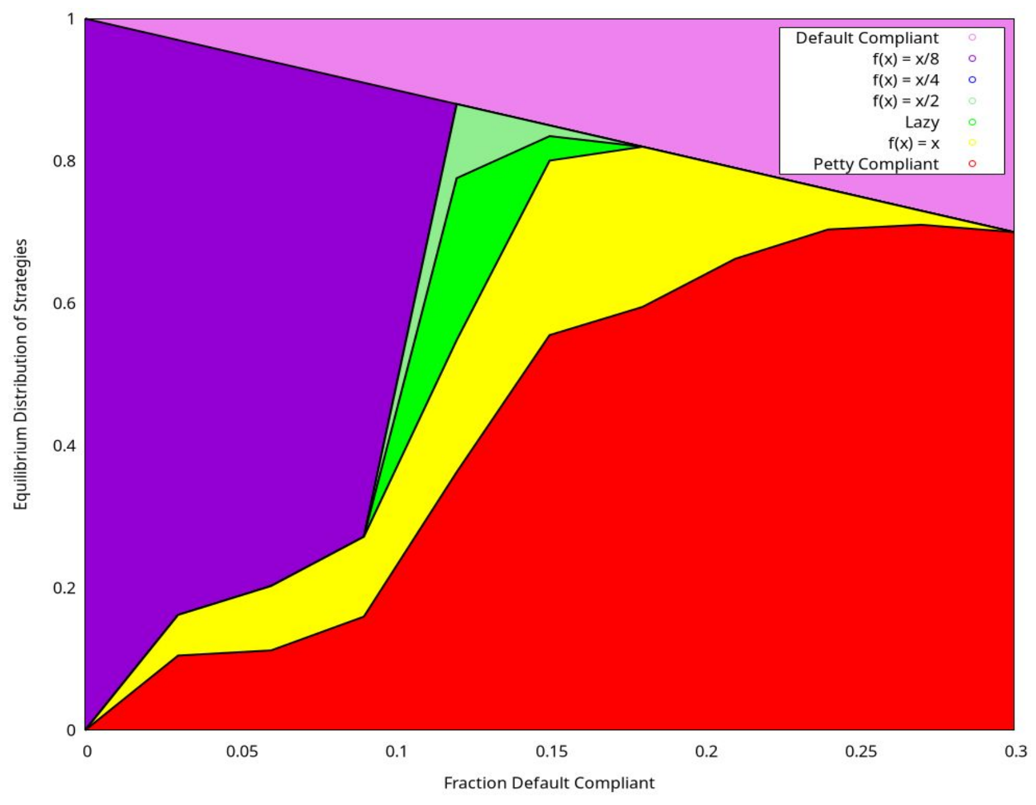


Figure 4.

5

Features & Benefits

- Multiple contract setup allows for better redistribution targeting different lengths
- Sliding window averaging of fees
- Mitigating Miner gap problem
- Delivers more stable rewards
- Fee-Redistribution Contracts significantly reduced Under Cutting Attack.
- Protocol is resilient against ~70% of adveseries compared to previous ~33%.

Real world applications

- Improvement proposal is being discussed on first blockchain.
- Implemented utilizing single Smart Contract

Rastislav Budinský, supervised by Ing. Ivan Homoliak Ph.D.

Excel@FIT 2023

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY