TinyCoin: Simulating mining strategies in a simplified Bitcoin Network

Final Project for the Peer to Peer course

Francesco Balzano
Master Degree in Computer Science and Networking
A.Y. 2016-2017

Contents

1 Overview

In this project I have implemented a simplified version of Bitcoin, called TinyCoin, whose specifications are reported in [1]. In brief, TinyCoin distinguishing features are:

- each user has a single address that records the unspent amount at that node
- each transaction has a single input, a single output and does not include neither a digital signature nor scripts
- network nodes may be either normal nodes or miners. In turn, miners may be either honest or fraudolent (*i.e. Selfish Miners*). Each miner has a type that reflects its mining hardware: CPU, GPU, FPGA or ASIC
- there is a centralized oracle that decides which miner has created a new block of hte blockchain at regular intervals of time. The decision is biased by the computational power of the miners. Each block is unique

The goal of this project is to evaluate the selfish mining strategy defined in [2] in TinyCoin. This strategy is evaluated by taking into account different metrics and parameters. The results and the discussion of this experiment are reported in the *Results* section.

2 Design choices

In the following subsections I explain the design choices that I made. This is a high level description, indeed the classes of the project are described in the *Implementation* section.

2.1 Network Nodes

Any node in the TinyCoin network is either a (normal) node, or a (honest) miner or a selfish miner.

- **node**: makes and receives transactions
- **miner**: makes and receives transactions and mines blocks of the blockchain. In particular, as soon as a new block is mined it is immediately advertized to all the nodes in the network.
- **selfish miner**: makes and receives transactions and mines blocks of the *private* blockchain. A selfish miner indeed holds both a copy of the public blockchain, which is the "official" blockchain, and a copy of the private blockchain, which is the blockchain created and maintained collectively by all the selfish miners. At any time the two blockchains may be equal or may differ for some block. If they differ, it is because the selfish miners have discovered new blocks which have been added to the private blockchain but have not been disclosed to the public. Indeed when a selfish miner mines a new block, it does not naively publish it and add to the public blockchain. Instead, it applies a strategy that allows it and the other selfish miners to get the maximum revenue from their computing power. One of the strategies that they can follow is explained in [2]. In this project, I chosed to implement it. The pseudocode is reported in algorithm 3

Algorithm 1 Selfish Miner initialization

```
1: public chain ← publicly known blocks
2: private chain ← publicly known blocks
3: privateBranchLength ← 0
4: Mine at the head of the private chain
```

alala

3 Implementation

alala

Algorithm 2 My pool found a block:

$\Delta_{\text{prev}} \leftarrow$ length(private chain) - length(public chain)
append new block to private chain
privateBranchLength $\leftarrow$ privateBranchLength + 1
if ($\Delta_{\text{prev}} = 0$ AND privateBranchLength = 2) **then**
    private chain $\leftarrow$ public chain
    privateBranchLength $\leftarrow$ 0
Mine at the new head of the private chain

Algorithm 3 Others found a block:

$\Delta_{\text{prev}} \leftarrow$ length(private chain) - length(public chain)
append new block to public chain
if ($\Delta_{\text{prev}} = 0$) **then**
    private chain $\leftarrow$ public chain
    privateBranchLength $\leftarrow$ 0
else if ($\Delta_{\text{prev}} = 1$) **then**
    publish last block of the private chain
else if ($\Delta_{\text{prev}} = 2$) **then**
    publish all of the private chain
    privateBranchLength $\leftarrow$ 0
else
    publish first unpublished block of the private blockchain
Mine at the new head of the private chain

4 Results

alala

5 Conclusion

6 Limitations

7 References

1. TinyCoin: Simulating mining strategies in a simplified Bitcoin Network
2. Majority is not Enough: Bitcoin Mining is Vulnerable