

Class 11: Pools and Profits

(See web version for additional links)

Schedule

- [Project 2](#), Part 1 is due **Sunday, 22 February**.
- Quiz 2 will be in class on **Wednesday, 25 February**. It will be similar in length, format, and content to Quiz 1 (except will cover material from the beginning of the class through
- Continue thinking about project ideas!

Mining Model

Mining Hardware on the market today: [Spondoolies SP20](#) (this is just an example, certainly not a commercial endorsement!)

Cost: US\$ 479

Hash rate: 1.7 TH/s

Power use: 1200 W

BTC Price: US\$ 240

Difficulty: 44455415962 # from <https://blockchain.info/stats>, 18 Feb 2015

[This spreadsheet](#) has lots of information about bitcoin difficulty over time.

Please don't make any investment decisions based on any of these models! Even the best one is still much simplified and with many guesses (e.g., assumption that BTC value will not change, slow increase in difficulty).

Super Simple Model

```
>>> expected_hashes / (1.7 * 10**12)
112314445.6981567 # expected seconds to find block
>>> _ / (60 * 60 * 24)
1299.935714099036 # days to find block
>>> block_value = 240 * 25
>>> earnings_per_year = block_value * (365.25 / 1300)
>>> earnings_per_year
1685.769230769231
```

Why is this estimate of expected earnings totally broken?

Better Model

```
def guess_difficulty(month):
    return difficulty * ((1 + rate_of_difficulty) ** month)

hash_rate = 1.7 * 10**12 # 1.7 Th/s
hashes_in_month = hash_rate * 60 * 60 * 24 * ave_days_in_month
block_value = 25 * 240 # assumes fixed BTC value
electricity_cost = (1.2 * kWh) * 24 * ave_days_in_month

def expected_revenue(month):
    success_probability = find_target(guess_difficulty(month)) / 2**256
    return block_value * hashes_in_month * success_probability

def cumulative_income(months):
    income = 0.0
    for month in range(months):
        income += expected_revenue(month) - electricity_cost
    return income
```

Given this model, when should the miner be turned off and turned to scrap?

What should happen to the bitcoin difficulty when subsidy is halved after block 420,000? (Current block is 344,044 so we should reach block 420,000 in $(420000 - 344000) / (6 * 24) = 527$ days.)

Mining Pools

How can an open mining pool fairly determine miners share of the reward? Why is it not sensible to use actual blocks mined to estimate pool share?

What are the risks of a mining pool controlling a large fraction over the hashing power? Does anything dramatic happen when that fraction exceeds 50%?