IT486 v3.0: Blockchains and Cryptocurrencies

Economics of mining, Punitive forking attack

Determining Mining Profitability

- Profit = Income - Expenses
- Income = $\sum_{\text{blocks mined}} \text{Convert}_{\text{BTC}\rightarrow\$}(\text{Block Reward} + \text{Txn fees})$
- $\text{Convert}_{\text{BTC}}$ is highly volatile!

Determining Mining Profitability

- Profit = Income - Expenses
- Income = $\sum_{\text{blocks mined}} \text{Convert}_{\text{BTC}\rightarrow\$}(\text{Block Reward} + \text{Txn fees})$
- $\text{Convert}_{\text{BTC}}$ is highly volatile!
- Expenses
  - Equipment
  - Real Estate
  - Staff
  - Electricity
  - Legal, Accounting support

Determining Mining Profitability

- One critical factor on the income side is
  - number of blocks mined

Determining Mining Profitability

- One critical factor on the income side is
  - number of blocks mined
- The number of blocks mined depends on the
  - hash rate = number hashes per second computed by the miner
  - relative hash power of the miner $= \dfrac{\text{hash rate of the miner}}{\sum_{\text{miners } m} \text{hash rate of miner } m}$

Nakamoto's vision

- Anyone can be a miner
- All users contributing to mining on their personal machines
- In practice, mining equipment has becoming increasingly specialised for increasing hash rate

Mining Equipment History

- CPU: 2009-mid 2011
  - sequential, one nonce at a time
- GPU: 2011-13
  - parallel and fast
- FPGA: 2013-14
  - parallel specially programmed circuits
- ASIC: 2013-today
  - highly parallel hardware chips, designed specifically to optimize hash function computations

Mining Market Dynamics

- Mining is a competitive market
  - Profit opportunities draw in new investors, increasing competition and decreasing profit
  - Unprofitable miners drop out, or buy better equipment

Mining Market Dynamics

- Mining is a competitive market
  - Profit opportunities draw in new investors, increasing competition and decreasing profit
  - Unprofitable miners drop out, or buy better equipment
- Lifetime of investment in equipment can be short
- The net effect is that profits tend to be only marginally above costs

How it has played out

- Large scale, professional mining installations with economies of scale, running specialised mining equipment
- Bitcoin mining in inner Mongolia

Additional factors

- The main manufacturers of mining ASICs (e.g. Bitmain) are also themselves major miners
- Are they likely to sell you their latest fastest equipment before they have had a chance to profit from it themselves?

Example

- Total number of blocks mined per year
  - 364 * 24 * 6 = 52,416
- Total Hash Rate of Bitcoin Network
  - 44,000,000 Terra Hash / second
- Antminer S9 Hash rate
  - 14 Terra Hash /second

Example

- Antminer S9 relative hash power
  - 14/44,000,000
- Expected number of blocks mined per year by Antminer S9
  - 14 * 52,416 / 44,000,000 = 0.016
- Expected number of years to mine one block with Antminer S9 = 60

Example

- Antminer S9 relative hash power
  - 14/44,000,000
- Expected number of blocks mined per year by Antminer S9
  - 14 * 52,416 / 44,000,000 = 0.016
- Expected number of years to mine one block with Antminer S9 = 60
- Running a mining rig involves continuous costs of energy, but earns revenue very infrequently

Mining pools

- In a mining pool, participants
  - combine their mining power to solve a common puzzle
  - share the reward from blocks mined by any pool member
- This produces a more continuous income stream for the participants

Mining pools

- In a mining pool, participants
  - combine their mining power to solve a common puzzle
  - share the reward from blocks mined by any pool member
- This produces a more continuous income stream for the participants
- First pools appeared in late 2010
  - By 2014: around 90% of mining pool-based

Example

- Consider a pool of miners with 60,000 Antminer S9 combined
- expects to mine 1,000 blocks per year $= 2.75$ blocks/day
- block reward (Jan 2019, excludes transaction fees) $= 12.5$ BTC
- exchange rate (Jan 2019) $= 1$ BTC $= \$3436$
- expected daily reward revenue from 1 Antminer S9

$$= (2.75 * 12.5 * \$3436)/60,000 = \$1.96$$

Pool operator

- Controls the pool private key / pool address
- Collects transactions into a block template, which includes a coinbase transaction paying to pool address, but lacks a nonce
- Distributes block template to the pool members
- Collects block solutions, and broadcasts on Bitcoin network
- Periodically distributes block rewards to pool members

Pool member

- Need not run a full node, can just operate hash power
- Returns hash puzzle solutions found to the pool operator
- Can pool members keep block rewards for themselves?

Pool member

- Need not run a full node, can just operate hash power
- Returns hash puzzle solutions found to the pool operator
- Can pool members keep block rewards for themselves?
  - No!

Pool member

- Need not run a full node, can just operate hash power
- Returns hash puzzle solutions found to the pool operator
- Can pool members keep block rewards for themselves?
  - No!
- To do that they need to change the coinbase transaction
- Then they effectively are mining for themselves, with low expected payout rate

Dishonest pool members

- Can pool members pretend to be mining for the pool, to collect a share of rewards, but actually mine for themselves/others?

Dishonest pool members

- Can pool members pretend to be mining for the pool, to collect a share of rewards, but actually mine for themselves/others?
  - Yes!

Dishonest pool members

- Can pool members pretend to be mining for the pool, to collect a share of rewards, but actually mine for themselves/others?
  - Yes!
- Countermeasure:
  - pool members have to prove that they are doing work!

Keeping pool members honest

- Have pool members prove that they are doing work, by providing near miss solutions
- If the puzzle is Hash(PoolBlock(nonce)) $<$ D, they provide solutions to Hash(PoolBlock(nonce)) $<$ E, where $D < E$, so expected time to solutions is smaller (e.g., 1,000 times easier)
- Reward to the miner depends on the number of near miss solutions they provide

Pool member payout schemes

- Flat fee / Pay-per-share:
  - miner gets a flat fee per near miss solution provided

Pool member payout schemes

- Flat fee / Pay-per-share:
  - miner gets a flat fee per near miss solution provided
- Issue: a malicious pool member can impose a cost on the pool by sending near miss but discarding complete solutions

Pool member payout schemes

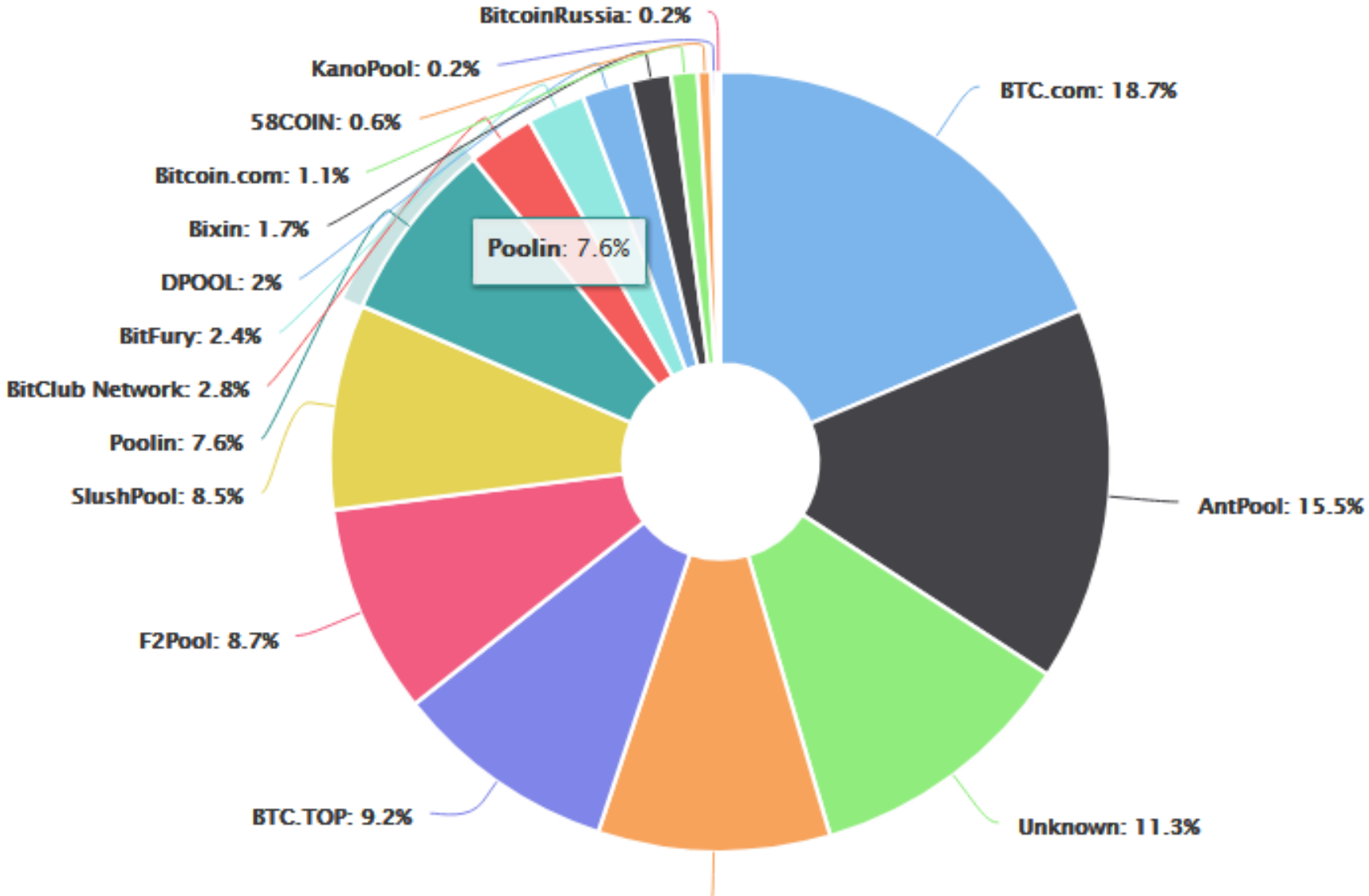
- Proportional: miner reward is
  - Pool Rewards - operator fee * $\frac{\text{number of near miss solutions found by miner}}{\text{total near miss solutions found by all miners in pool}}$

Pool member payout schemes

- Proportional: miner reward is
  - Pool Rewards - operator fee * $\frac{\text{number of near miss solutions found by miner}}{\text{total near miss solutions found by all miners in pool}}$
- Issue: pool hopping
  - expected miner payout can be higher early in the search (larger share of near misses) than later
  - this may incentivise the miner to switch effort to a flat fee pool

Pool distribution (Oct 2018)

- Percentage of network hash power from `blockchain.com`



Concerns about mining pools

- Mining pools and large miners decrease the decentralisation of the network
  - increased potential for 51% attacks
- In 2014, Ghash.io briefly had $> 50\%$ of the total hash rate
- Miner response was to switch to other pools, Ghash voluntarily closed membership

Environmental impact of mining

- Energy costs of bitcoin mining include:
  - electricity consumption of mining equipment
  - cooling of the mining equipment
- The total energy costs of running the Bitcoin network are large enough to raise concerns (as early as 2013) about the environmental impact and economic efficiency

Cooling of mining equipment

- Mining rigs generate a lot of heat and need to be cooled
- Beneficial to run mining rig in places with cold climates (e.g. Canada, Northern Europe, Himalayas)
- Can we utilize the generated heat instead of venting it?

Is Bitcoin Mining Wasteful?

- Any payment system requires energy (digging gold out of the ground, printing dollar bills, running a bank, etc.)
- Bitcoin is not necessarily the best we can do
- There are much more energy efficient alternatives to hash-puzzle proof of work (e.g., proof of stake)

Blacklisting

- Say Gloria is a government, or has control over a government, that has jurisdiction over mining pools (The Glorian nation)
- In addition, Gloria's mining pools have over 51% of the network's hashpower

Blacklisting

- Say Gloria is a government, or has control over a government, that has jurisdiction over mining pools (The Glorian nation)
- In addition, Gloria's mining pools have over 51% of the network's hashpower
- Objective:
  - Censor the Bitcoin addresses owned by certain people, say Rustie, and prevent them from spending any of their Bitcoin

Blacklisting

First strategy: Gloria tells her mining pools not to include Rustie's transactions

Blacklisting

First strategy: Gloria tells her mining pools not to include Rustie's transactions

- Doesn't work unless you are 100% of the network

Blacklisting

First strategy: Gloria tells her mining pools not to include Rustie's transactions

- Doesn't work unless you are 100% of the network
- Other miners will eventually include Rustie's transactions in a block

Blacklisting

First strategy: Gloria tells her mining pools not to include Rustie's transactions

- Doesn't work unless you are 100% of the network
- Other miners will eventually include Rustie's transactions in a block
- Can only cause delays and inconveniences

Blacklisting

Second strategy:

- Remember you are Gloria: you have $>51\%$ of the network hashrate

Blacklisting

Second strategy:

- Remember you are Gloria: you have >51% of the network hashrate
- Mandate that Glorian pools will refuse to work on a chain containing transactions spending from Rustie's address

Blacklisting

Second strategy:

- Remember you are Gloria: you have >51% of the network hashrate
- Mandate that Glorian pools will refuse to work on a chain containing transactions spending from Rustie's address
- Announce this to the world

Blacklisting

- If miners include a transaction from Rustie in a block, Gloria will fork and create a longer proof-of-work chain
- Block containing Rustie's transaction now invalidated, can never be published

Blacklisting

- Non-Glorian miners eventually stop trying to include Rustie's transactions when mining blocks, since they know that their block will be invalidated by Glorian miners when they do
- We have now shown how a 51% majority can prevent anyone from accessing their funds

Blacklisting

- Non-Glorian miners eventually stop trying to include Rustie's transactions when mining blocks, since they know that their block will be invalidated by Glorian miners when they do
- We have now shown how a 51% majority can prevent anyone from accessing their funds
- This is called **punitive forking**