Lecture #5: Bitcoin Mining

Recap: Bitcoin miners
Bitcoin depends on miners to:

- Store and broadcast the blockchain
- Validate new transactions
- Vote(by hash power) on consensus

Lecture 5.1 The task of Bitcoin miners

Setting the mining difficulty

Every two weeks, compute:
Next_difficulty = previous_difficulty * (2 weeks)/(time to mine last 2016 blocks)

Lecture 5.2 Mining hardware

SHA-256

- General purpose hash function
- Published in 2001
- Designed by NSA
- Reamins unbroken cryptographically
- SHA-3 (replacement) under standardization

***CPU** mining*

Throughput on a high-end PC = 10-20 MHz ~ 2^24

***GPU** mining*

- GPUs designed for high-performance graphics
    - High parallelism
    - High throughput

Advantages:

- Easily available, easy to set up
- Parallel ALUs
- Bit-specific instructions
- Can drive many from 1 CPU
- Can overlock!

Disadvantages:

- Poor utilization of hardware
- Poor cooling

- Large power draw
- Few boards to hold multiple GPUs

Throughput on a good card = 20 - 200 Mhz ~ 2^27

***FPGA** mining*

- Field Programmable Gate Area

Advantages:

- Higher performance than GPUs
    - Excellent performance than GPUs
- Better cooling
- Extensive customization, optimization

Disadvantages:

- Higher power draw than GPUs designed for
    - Frequent malfunctions, errors
- Poor optimization of 32-bit adds
- Fewer hobbyists with sufficient expertise
- More expensive than GPUs
- Marginal performance/cost advantage over GPUs

Throughput on a good card = 100 - 1000MHz ~ 2^30

Bitcoin ASICs mining

Lecture 5.3 Energy consumption & ecology
Estimating energy usage: top-down

- Each block worth approximately US$15,000
- Approximately $25/s generated
- Industrial electricity(US): $0.03/MJ
    - $0.10/kWh

Upperbound on electricity consumed:
900 MJ/s = 900 MW

Estimating energy usage: bottom-up

- Best claimed efficiency: 1GHz/W
- Network hash rate: 150,000,000 GHz

- (Excludes cooling, embodied energy)

Lower bound on electricity consumed:
150 MW

Lecture 5.4 Mining pools
Goal: pool participants all attempt to mine a block with the same coinbase recipient

- Send money to key owned by pool manager

Distribute revenues to members based on how much work they have performed

- Minus a cut for pool manager

Mining shares
Idea: prove work with "near-valid blocks" (shares)

Are mining pools a good thing?

- Pros
  - Make mining more predictable
  - Allow small miners to participate
  - More miners using updated validation software
- Cons
  - Lead to centralization
  - Discourage miners from running nodes

Lecture 5.5 Mining incentives and strategies
Game-theoretic analysis of mining
Forking attacks

- Certainly possible if alpha > 0.5
  - May be possible with less
  - Avoid block collisions
- Attack is detectable
- Might be reversed
- Might crash exchange rate

Block-withholding attack(selfish mining)
Punitive forking
Feather-Forking

Summary
Miners are free to implement any strategy

Very little non-default behavior in the wild
No complete game-heretic model exists