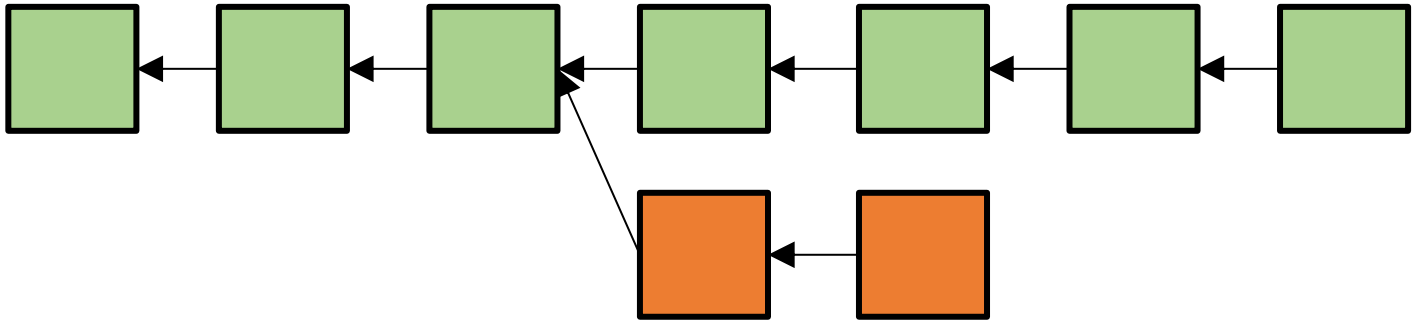
Proof-of-Work Consensus and Mining

Fan Long

University of Toronto

PoW Principle: The Longest Chain is the Valid Chain

- Honest nodes only work on the longest chain:



- Only transactions in the green nodes are validated by the network.
- **Assumption**: Honest nodes have more than 50% computation power!

How to Choose PoW Problem?

- Every node in the network needs to verify the solution of PoW!
- Proof of work criteria:
  - Easy to verify
  - Hard to compute

- SHA-256 Hash function satisfies these
  - One-way hash function; can hash any arbitrary date
  - Pretty much random (very useful property)
- Example
  - SHA256("Donald Trump") == "e4f2e1f0e2ae4d3ce7018cf3b4f3577c99714bdc9f5a4ac28e3e7cb2c505db6c”
  - SHA256("Donald trump") ==”6ad2fa6a5caaee9143578931456322c4433a92ae2af8f0d5c9b4f9bb080f49d6"

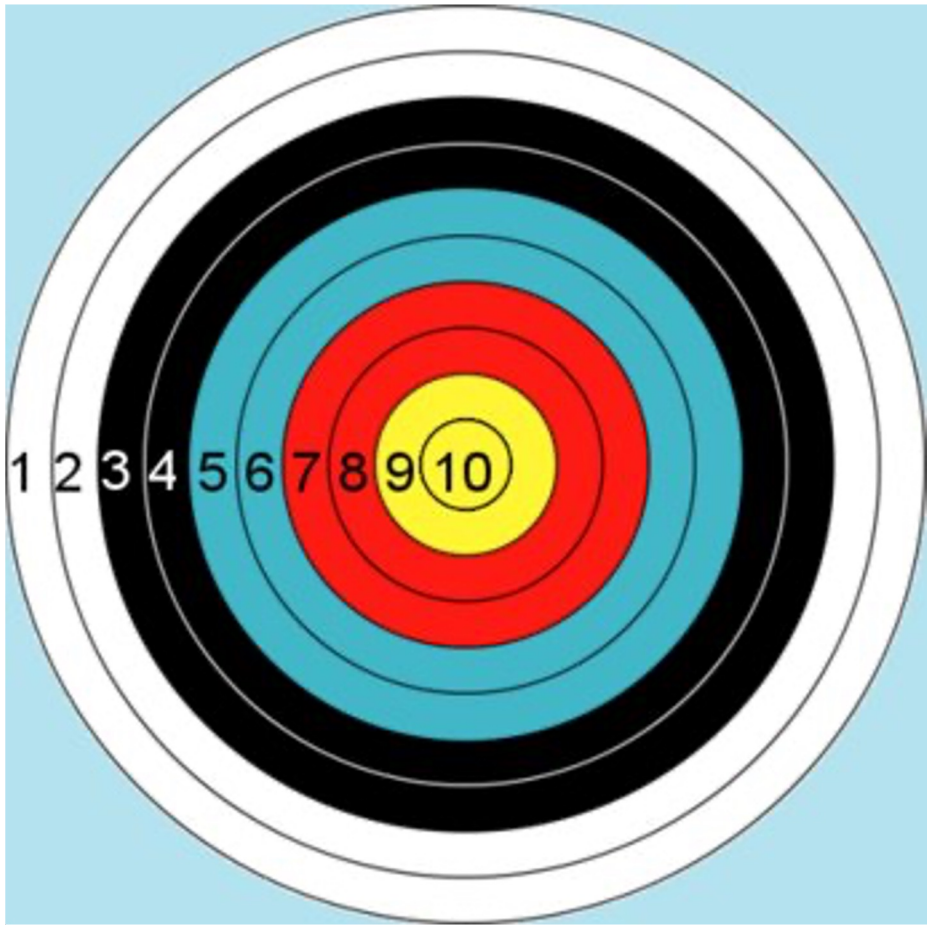
Sketch of Bitcoin Mining - PoW

- PoW: Find a value *nonce*, such that:
  - SHA256(*nonce* || PrevBlockHeader) has X leading zeros
  - X is determined by the *difficulty*
  - || means concatenation

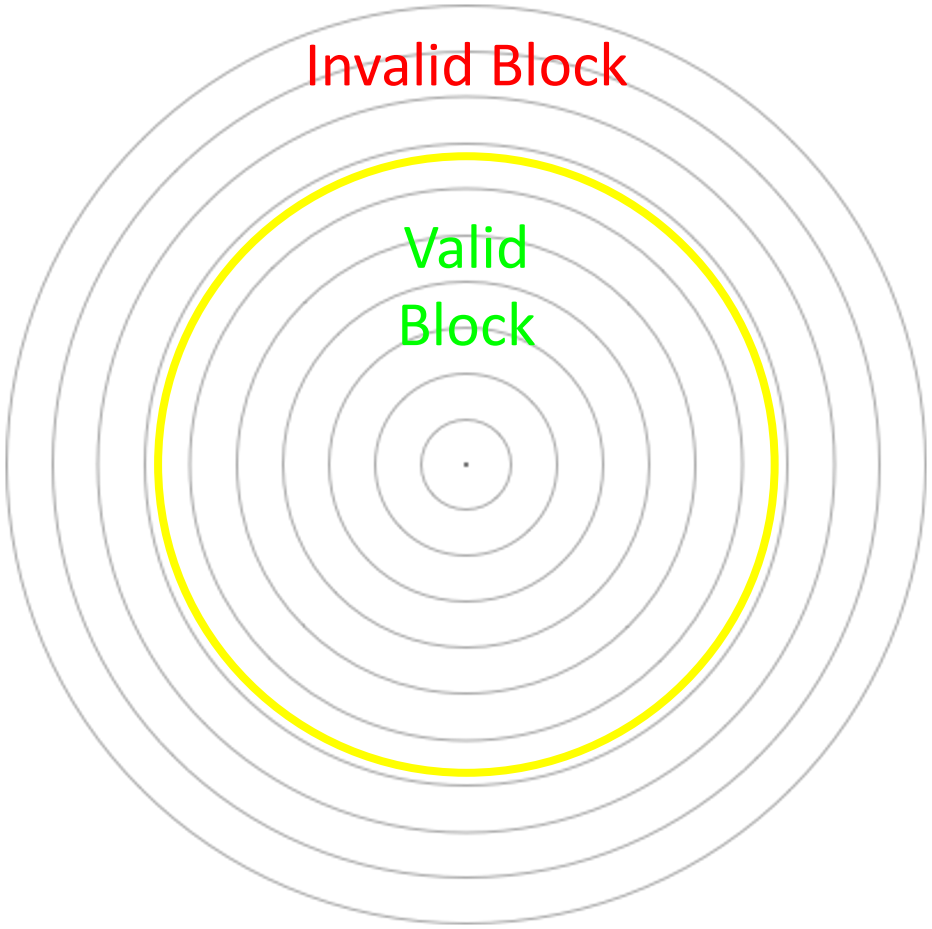
- No easy way to compute, have to search difference nonces
- Only need to compute SHA256 once to verify

- The people who solves PoW first and writes the next block receive rewards
  - Encouraging people to perform PoW to secure the network
  - Compute PoW is also called mining

Block Reward and Difficulty



Block Reward and Difficulty



- Equally likely to hit ring 1, 2, 3, …
- Faster miners = more hits / second
- Target: inside the yellow ring
- Keep decreasing the size of the yellow ring…
- Mining difficulty adjustment every 2016 blocks
- Difficulty adjusted to:

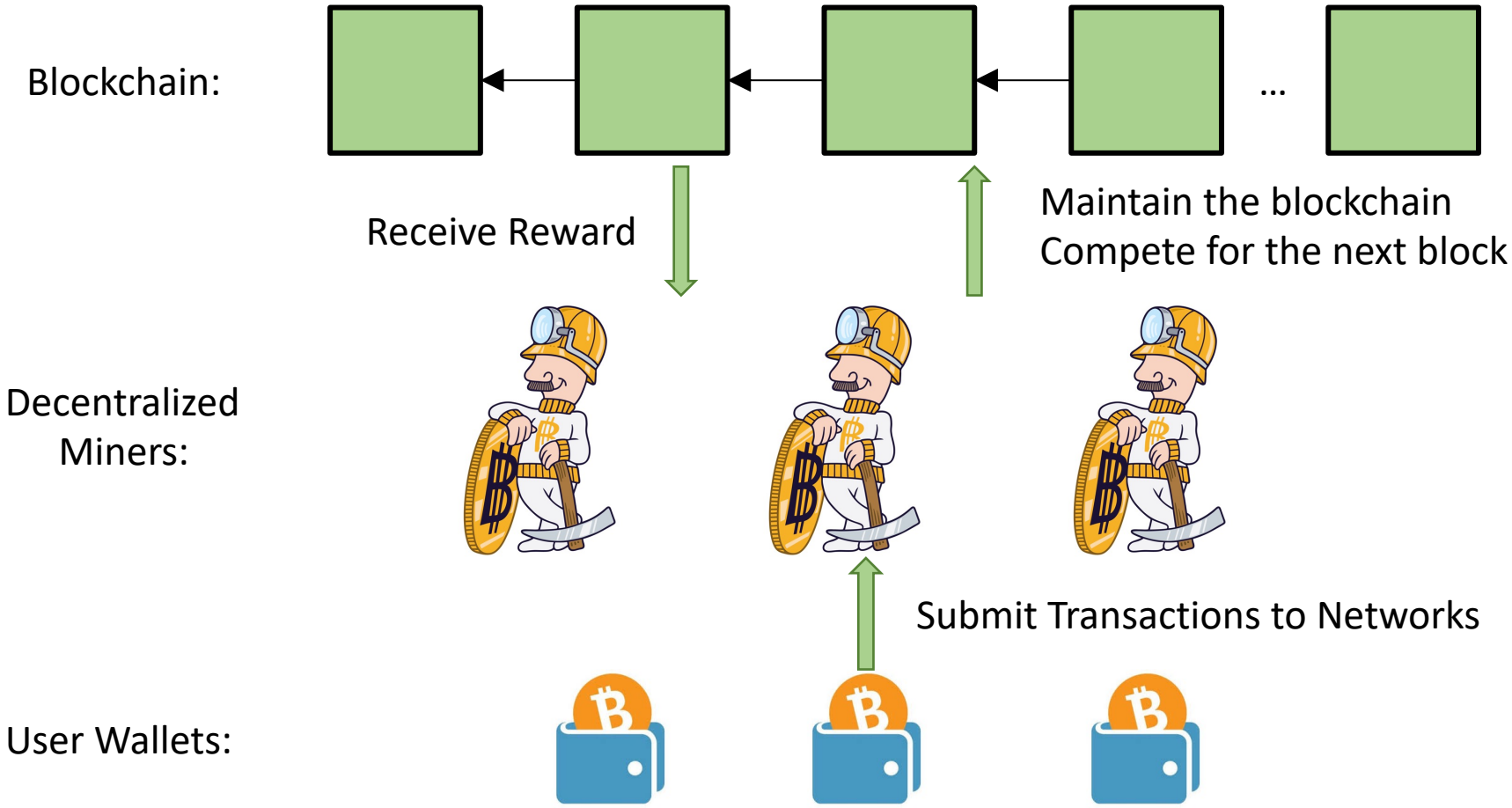
next_difficulty = previous_difficulty * (2 weeks) / (time to mine last 2016 blocks)

Block Reward and Difficulty

- Average Block Time ~10m
  - How to control the time?
  - If more people compute PoW, blocks will be generated faster?
- Difficulty are automatically adjusted every 2 weeks
  - If blocks generated too fast, difficulty will increase
  - If blocks generated too slow, difficulty will reduce

- Block Rewards are also halved every 4 years.
  - Starting at ~50BTC per block at 2009
  - Right now only ~12BTC per block
- Miner can pick transactions to include in the next block
  - Miner will pick transactions with higher fees (additional to block reward)

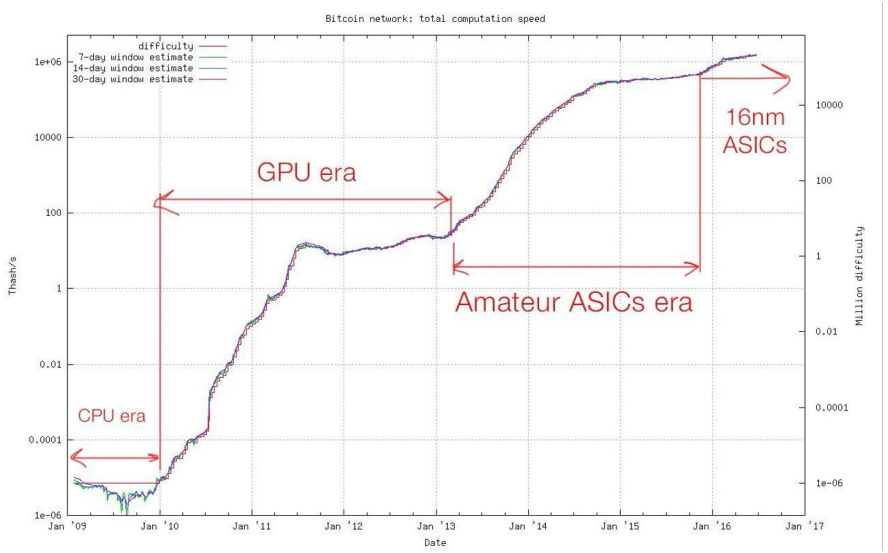
Bitcoin Ecosystem in Early Days



Is Bitcoin Mining Still Decentralized?

Mining Hardware Evolution

	hashes / second	time to block
CPU	20 million	300,000 years
GPU	200 million	30,000 years
FPGA	1 billion	600 years
ASIC	10 trillion	22 days



As the mining evolves, it becomes more and more **centralized**!

Mining Hardware Evolution

	hashes / second	time to block
CPU	20 million	300,000 years
GPU	200 million	30,000 years
FPGA	1 billion	600 years
ASIC	10 trillion	22 days

- For each nonce
  - Run SHA256
  - Check if result was a valid block
- Slowest
- What Satoshi used
- Your comupter!

No longer profitable since 2011!

Mining Hardware Evolution

	hashes / second	time to block
CPU	20 million	300,000 years
GPU	200 million	30,000 years
FPGA	1 billion	600 years
ASIC	10 trillion	22 days

No longer profitable since 2013!

- Designed for parallel computation
- Order of magnitude faster than CPUs
- Consumes a lot of energy, produces a lot of heat
- $446.66 for the R9 290 back in the day

Mining Hardware Evolution

	hashes / second	time to block
CPU	20 million	300,000 years
GPU	200 million	30,000 years
FPGA	1 billion	600 years
ASIC	10 trillion	22 days

No longer profitable

- **F**ield **P**rogrammable **G**ate **A**rrays
  - Getting more application specific
- A trade-off between ASIC and general purpose

Mining Hardware Evolution

	hashes / second	time to block
CPU	20 million	300,000 years
GPU	200 million	30,000 years
FPGA	1 billion	600 years
ASIC	10 trillion	22 days

- **A**pplication-**S**pecific **I**ntegrated **C**ircuits.
  - Circuits specifically designed to do Bitcoin mining (SHA256)
  - Extremely expensive
- Fastest miners around
- ~$1600

70% of ASICs are sold by one company!

Lesson Learned

- Proof of work criteria of future cryptocurrencies:
  - Easy to verify
  - Hard to compute
  - ***Hard to design ASIC (ASIC-Resilience)***
- Because ASIC means centralization!
- Use memory-hard problems:
  - Designing ASIC can reduce the cost of computations but not the memory read/write
- Examples:
  - Ethereum PoW: Ethash
  - Zcash PoW: Equihash

Equihash Sketch

- Given 2^20 large numbers, each of which has 200 bits, find 512 numbers whose XOR result is 0
  - The SHA256 of the 512 numbers also needs to be less than a predefined difficulty
- Solving the problem requires reading and writing a large hash tables 10 times.
- Sequential read + Random write
- Memory bandwidth bound
- Mining hardware: GPU

Ethash Sketch

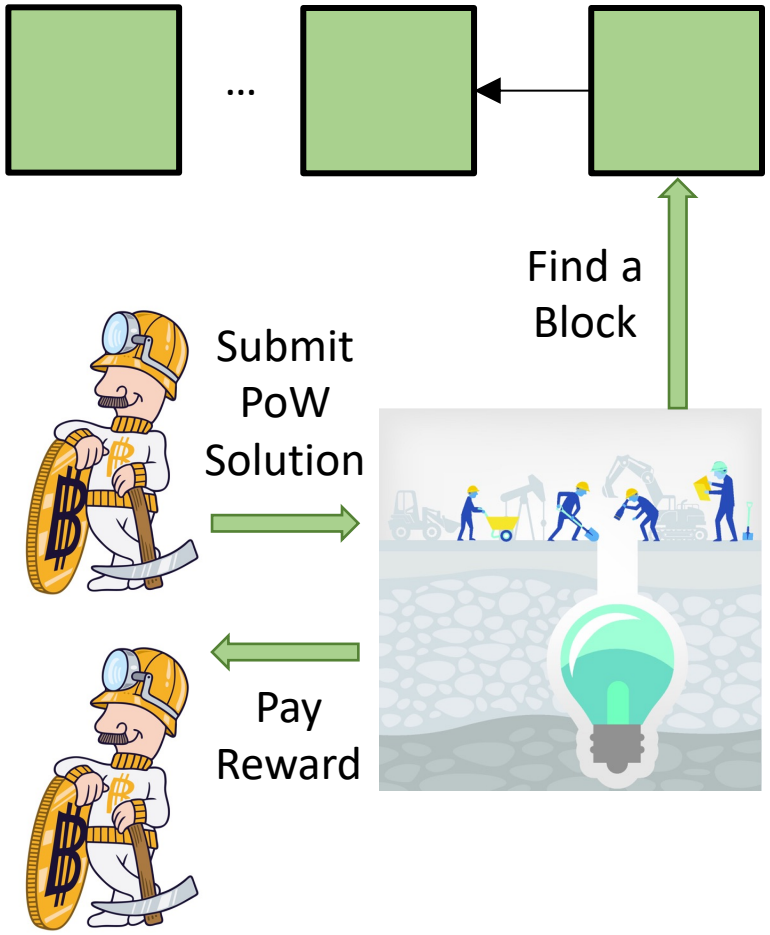
- A large growing directed acyclic graph (~4G DAG before PoS)
  - Graph is generated by one way hash functions
- Find a *nonce* as a start point of the graph such that:
  - After following 64 edges, it reaches a node with id less than a predefined difficulty
- Solving one nonce requires many random read requests on the 3G data
- Memory latency/bandwidth bound
- Mining hardware: GPU

Mining is a Lottery

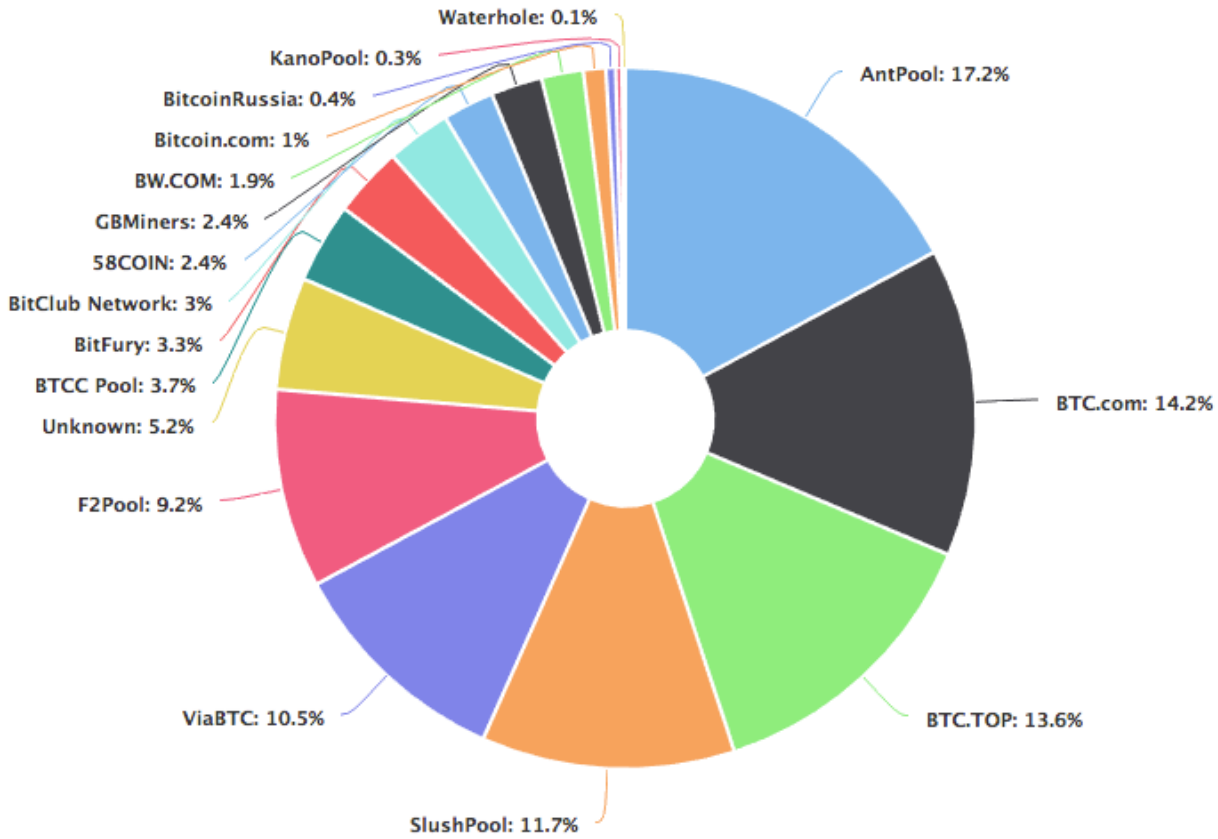
- Mining is a lottery:
  - You compute hashes -> buy lottery tickets
  - More computation power -> more lottery tickets
  - If the result is less than difficulty -> you win the lottery
  - Get block reward -> you get the lottery prize
- If you buy an ASIC miner and do solo-mining:
  - Most likely for days and weeks, you get nothing
  - Or one day you are extremely lucky, you get 12BTC, which is now ~$100000
- But miners want constant income

Mining Pools

- Miner submits PoW solutions to the pool
- By large number theorem, the pool will find results constantly
- The pool pays miners based on contributions
- **Pro**: Constant revenue for miners
- **Con**: Centralization!



Bitcoin Mining Pool Distribution



The largest four pools control more than 50% of computation power!

How Mining Pool Make Money

- Mining pools keep some of the block rewards as charged fees (typically 1%-5%) for miners
- Some mining pools keep 100% of the transaction fees collected in a block.
- **Share stealing**: A dishonest mining pool keep more than its advertised fees
  - Eventually detectable by miners
  - Miners will switch to other pools

Are Those Pools 100% Honest Nodes?

Most of them in most of time? Maybe

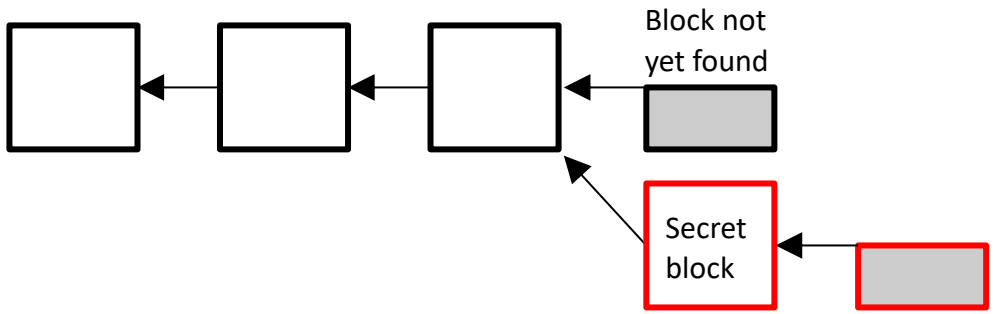
All of them always? No!

Selfish Mining

You are a miner; suppose you have just found a block.

- Instead of announcing block to the network and receiving reward, keep it secret
- Try to find two blocks in a row before the network finds the next one

This is called **selfish mining** or **block-withholding**

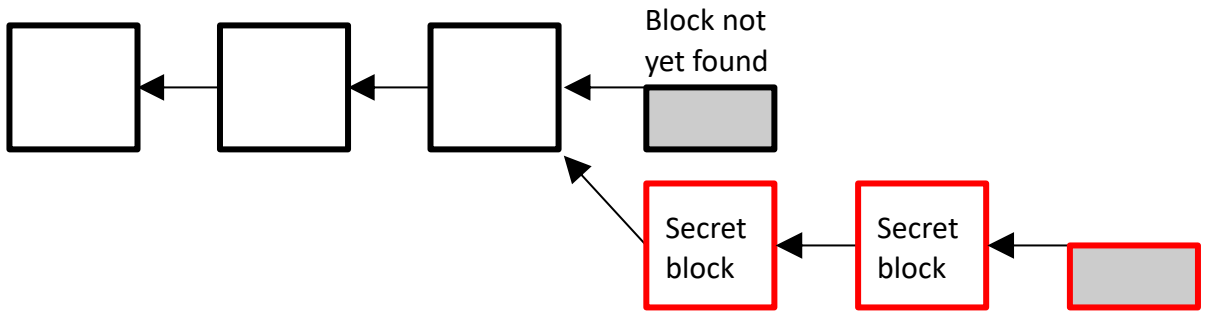


Note: "block-withholding" is also sometimes used in the context of mining pools - submitting shares but withholding valid blocks

Selfish Mining

If you succeed in finding a second block, you have fooled the network

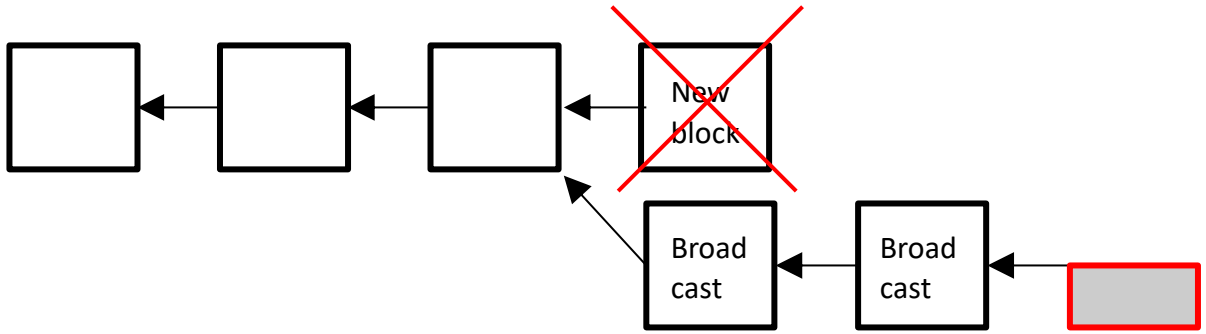
- Network still believes it is mining on the longest proof of work chain
- You continue to mine on your own chain



Selfish Mining

If the network finds a block, you broadcast your two secret blocks and make the network block invalid

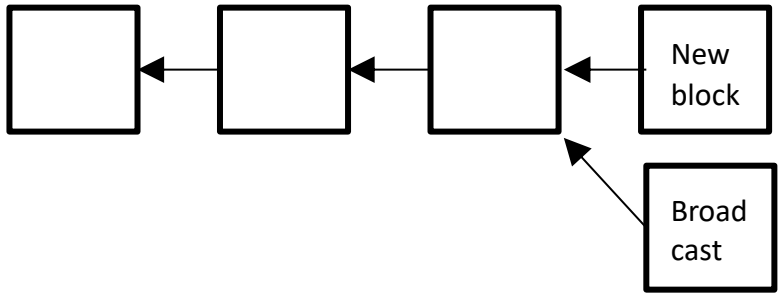
- While network was working on the invalid block, you got a bunch of time to mine by yourself... for free!
- Free time mining on network
  => higher effective proportion of hashrate **=> higher expected profits!**



Selfish Mining

But what if the network found their new block before you could find a second one? **Race to propagate!**

- If you have 50% chance of winning the race and having your block accepted:
  - Malicious strategy is more profitable if you have >25% mining power
- If you have >33% mining power, **you can lose the race every time and malicious strategy is still more profitable! Why?**



Pool Wars (Block Withholding)

You have 30% of the hashrate. Assume 1 BTC block reward. All of the following numbers are expected value.

- 30% HR (hashrate)
  = 30% MR (Mining Reward) = 0.3 BTC

You buy more mining equipment, worth 1% of current network hashrate

Standard mining strategy

- Add 1% HR => 31/101 = 30.69% HR = .3069 BTC
  - Revenue gain = **0.0069 BTC for 1% hashrate added**

Pool Wars (Block Withholding)

Cannibalizing Pools - Distribute your 1% equally among all other pools, withhold valid blocks.

- Rewards will still be received
- Undetectable unless statistically significant

Other pool hashrate breakdown:

- (70/71 honest, 1/71 dishonest)
  = 70% honest hashrate = .7 BTC
- You own (1/71) of other pools, so expected value of mining there is
  (1/71) * .7 = **0.0098 BTC**
- **0.0098 (cheat) > 0.0069 (honest)**

More profitable to cannibalize pools than mine honestly

Summary

- Large players have incentives to not mine honestly
- Centralization -> Larger pool players cheat -> Smaller players kicked out -> More centralization
- Measures against mining attacks:
  - Miners switch pools to prevent monopoly
  - Punish cheaters in protocol (very hard)

- Comparing to mining attacks, double-spend attacks never occurred in the cryptocurrency history. **Why?**

Discussion

- Bitcoin is increasingly centralized
  - The network safety is dependent on very few large players
- Technical design reasons
  - PoW algorithm and ASIC
  - Mining reward scheme → Mining pools
- Economical reasons?