Crypto News?

Mining and Proof-of-Work

What is mining?

- Mining is the process of creating blocks and publishing them to the network
  - Mining is used in many cryptocurrencies to allow for coins to be created
- In exchange for mining, miners collect transaction fees and a **coinbase transaction**
- Miners build blocks using the same structure we discussed last week
- They specify an address and an amount to attach to the coinbase transaction (the coinbase transaction has a maximum), and then collect the coinbase transaction when the block is accepted by the network
  - Can they spend the coinbase transaction immediately?

What is mining?

- How often are valid blocks on Bitcoin’s blockchain found?
  - What makes a block valid?
- How is this time limit ensured?
  - Bitcoin Core
  - Difficulty
    - Recall the idea of the nonce and SHA-256
    - 0x0000023FB237A75C... vs 0x000000000000005C...
- Why would we have a time limit on how often blocks are found?
  - Prevent attacks
  - Keep a steady puzzle-to-network diffusion ratio

What is the coinbase transaction?

- Special transaction that the miner adds to his/her block that creates Bitcoins out of thin air as a reward for finding the block
- When BTC first started, the maximum value of any coinbase transaction was 50 BTC per block
- Every 210,000 blocks (or approx. 4 years), the maximum coinbase transaction halves
- In 2012, the coinbase transaction halved to 25 BTC
- In 2016, the coinbase transaction halved again to 12.5 BTC
- Eventually, the coinbase transaction will basically halve to 0
    - By 2060, the maximum coinbase transaction reward will be about 0.0061 BTC
- At that point, miners will mainly profit from collecting transaction fees

Why have a coinbase transaction?

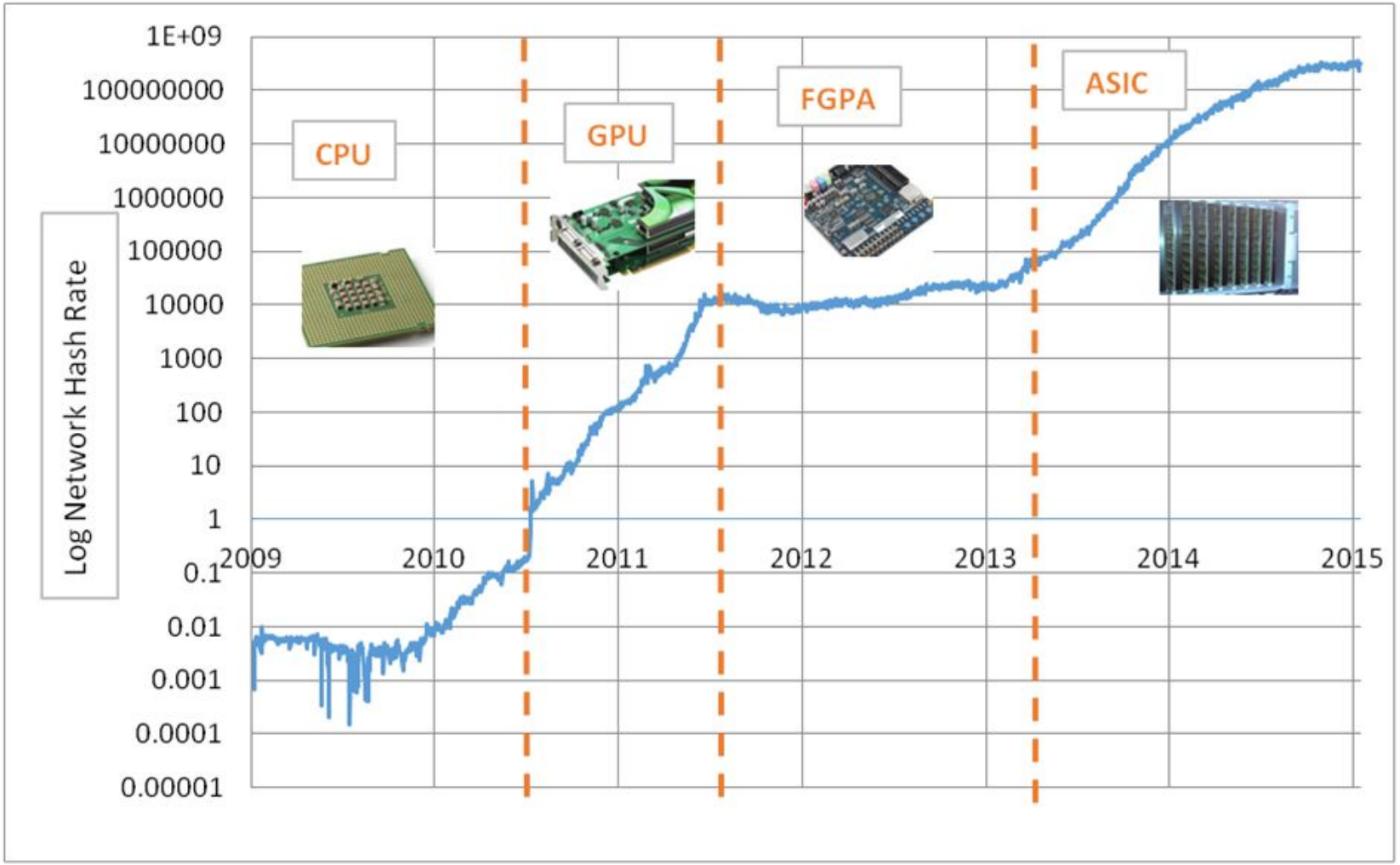
- Incentive!
  - The opportunity for miners to collect money helps keep them honest
  - **Keeps the network moving** (if miners aren't mining, no one can send money)
- Supply and Demand
  - Increase the total supply of bitcoin in circulation
  - Combat lost bitcoin (due to lost private keys, hacked exchanges, destroyed computers, etc.)
  - Coinbase transaction puts a limit on how many bitcoin there can ever be (approx. 21 million) while slowly distributing them over time
    - Why?

Mining Pools

- A pool is an entity that allows miners to use their hash power together, with the goal of discovering a block
- Block reward is usually distributed among miners based on the amount of hashing power they provide to the collective pool
    - Other reward systems exist, including those that reward based on who found the block, and those that work like a lottery.
    - Cryptojacking - The technique of hijacking computer systems for mining cryptocurrency (without user consent) using some or all of the system's CPU/GPU power.
- In addition to creating new coins, pools simultaneously work to keep bitcoin's network functioning

Why join a mining pool?

- When Bitcoin first started, anyone could mine using their at-home CPU
  - Difficulty was relatively low compared to the amount of computing power at the time
- As time moves on, people get better and faster hardware — this requires more electricity
- Mining is only profitable if you make more in bitcoin than you spend on electricity per month
- Pools guarantee your expected reward for your hashing power over time
  - Reduces your variance while fixing expected payoff


Log Network Hash Rate
1E+09
100000000
10000000
1000000
100000
10000
1000
100
10
1
0.1
0.01
0.001
0.0001
0.00001
2009
2010
2011
2012
2013
2014
2015
CPU
GPU
FGPA
ASIC

What is Proof-of-Work?

- A proof-of-work (POW) system is a measure to deter attacks and other abuses (such as spam) by requiring some work from the service requester, usually meaning processing time by a computer
- In terms of Bitcoin, proof-of-work makes it extremely difficult as an individual to double-spend coins or control which transactions go on the blockchain
    - What would it take for someone to control the transactions on bitcoin’s blockchain?
    - 51% attack

How does POW work?

- Let’s take a deeper look at the concept of the nonce
- Recall the main information we need to build a block
  - Prev. block hash, merkle root, nonce
- The nonce is one thing that is easily changeable, so we try to guess the proper nonce that hashes the entire block with the correct number of 0 bits
  - Remember, the hash must look like 0x00000000 23FB23..., **not** 0x12FD23A123...
- Since the nonce is a 32-bit integer, a miner has to try ~4 billion values
  - However, this may not be enough!

What to do if we can’t find a proper nonce?

- Recall that the nonce is the most easily changeable thing about our block, but there’s something else we can change: the merkle tree
- Two main ways to change your merkle tree:
  - The coinbase transaction we mentioned earlier also has arbitrary data that can act as a second “nonce”
  - We can update the coinbase “nonce” by simply changing some small data, and then trying all 2^{32} possible nonces again
  - We can also reorder the transactions we gathered to create a different merkle tree
  - Since there can be several thousand transactions in a block, this creates an almost inconceivable number of nonces that can be tried
  - However, many nonces may lead to the correct number of 0 bits, so the search isn’t usually exhaustive

So we've found the proper nonce, now what?

- Once you've determined a proper nonce and merkle tree to create a valid block, publish!
- Problems
  - Just because you've found a block doesn't mean it will be accepted by the network
  - Recall that the one valid blockchain is the longest one
  - If people choose not to build on your block, or they start building but switch to another chain, then your work goes to waste!
  - What happens to the transactions in your block if it's not accepted by the network?

Summary

- In order for new blocks to be created, miners have to mine them
- Mining involves a proof-of-work puzzle to keep miners honest
- Miners are incentivized by collecting coinbase transactions and transaction fees
- Mining is extremely difficult mathematically to the point of blocks only being found every 10 minutes
    - Difficulty is adjusted as computing power increases

Questions?