Module 2: Cryptocurrency Intuition

What is Bitcoin?

- What is Bitcoin?
  - Technology: Blockchian
  - Protocol/Coin/: Bitcoin, Ethereum, Waves
  - Token: (ICO, rely on smart contract)
- Coin/Token Market: https://coinmarketcap.com/
- Satoshi Nakamoto(2008,2009): Bitcoin: A Peer-to-Peer Electronic Cash System
- The Bitcoin Ecosysytem:
  - Nodes
  - Miners
  - Large Mines
  - Mining Pools

BItcoin's Monetary Policy

- The Halving:
  1. The number of bitcoins released into the system is halved every single four years. 2020:6.25 2024:3.125 Bitcoin per block
  2. 21 Million Bitcoins by 2140 (last bit coin)
  3. Rewards: Block Reward + Transaction fees
- Block Frequency:
  1. Average block time
  2. Blockchain.com -> Explore

Understanding Mining Difficulty

- Q1: What is the Current Target and how does that feel?
  1. one less leading zero: 1/16
     XXX: 0-999
     0XX: 0-99
  2. Probability of Golden Blocks: 16^{64-# leading 0}/16^{64}
- Q2: How is "Mining Difficulty" Calculated
  1. Difficulty = current target / max target
     Difficulty is adjusted every 2016 blocks(2 weeks)
     Max target: 00000000FFFF00...000
     see: blockchain.com chart difficulty

Virtual Tour of Bitcoin Mine

- Photos: Inside one of the world's largest bitcoin mines

Mining Pools

- Miners combine together to solve problems, problem is distributed among mining pools
- Hashrate Distribution
  1. www.blockchain.com |chat|hashrate distribution
  2. get started with choosing mining pool
  3. 81% China Mining Pools, reason: electricity price super low

Nonce Range

1. One nonce range: 32-bit number: 0-4 Billion, 2^{32}, not enough
2. Nonce update per second w.r.t timestamp

How Miners Pick Transactions

1. each transaction has a fee, miners will pick top # fee transaction to write in block
2. what if nonce update slower than mining power? Ans: change block configuration

- MEMPOOL
  - Transaction Per Block/Average Block Size/ Total Transaction Fee -> www.blockchain.com
  - Accelerate your transaction -> BTC.com
- Data/Chart

CPUs vs GPUs vs ASICs

- General, < 10MH/s — CPU: Central Processing Unit
- Specialized, < 1 GH/s — GPU: Graphics Processing Unit
- Totally Specialized, > 1000 GH/s — ASIC: Application-Specific Integrated Circuit
- Cloud Mining

How do Mempools work?

1. pic
2. A Mempool is a storage area where transactions are stored before they are added to a block. Every participant of the P2P distributed network has their own mempool on their computer.
3. Blockchain.com chart
   mempools size
   unconfirmed transactions

Orphaned Blocks

The 51% Attack

The 51% attack is when a group of hidden participants with majority computational power conduct mining without announcing their version of the chain to the rest of the network.

The attackers can benefit by leveraging the double-spend problem.