Lecture 4 - Mining Incentives, Challenges and Future Directions

Rylan Schaeffer and Vincent Yang

April 26, 2016

Note: This lecture is based on Princeton University's BTC-Tech: Bitcoin and Cryptocurrency Technologies Spring 2015 course.

Review

- Need method to achieve distributed consensus
- One option is proof-of-work, in which we balance two opposing goals:

  challenging to validate transactions, to prevent interference

  rewarding to validate transactions, to encourage people to participate
- Accomplished through hash puzzles i.e. calculate nonce r such that $H(previoushash|tx_1|tx_2|...|tx_n|tx_s|r)$ has target number of leading zeroes
- Two incentives:

  Block reward i.e. tx_s is a new coin

  Transaction fees

To Be A Miner

1. Listen for transactions
2. Maintain block chain and listen for new blocks
3. Assemble new block
4. Mine that block i.e. find the nonce r
5. Hope your block is accepted
6. Profit

Note: Not all miners are working on the same problem! Miners (almost) always have unique set of transactions. Even if the transactions are identical, they're trying to send the transaction rewards and new block to themselves.

Protocol dictates that, on average, mining a new block should take about 10 minutes, adjusted about every two weeks.

1 Mining Hardware

- SHA-256 requires 32-bit words, 32-bit modular addition, some bitwise logic
- Central Processing Unit mining works, but is slow
- Graphics Processing Unit mining is faster, but wastes floating point unit and consumes more power.
- Field-Programmable Gate Arrays mining is comparable to GPUs, better with bitwise logic, can be easily packed together, can be controlled from one centralized unit. Difficult to optimize 32-bit step addition
- Application-Specific Integrated Circuits: best of all possible worlds

2 Mining Costs

- Technology quickly becomes antiquated
- Cheaper in cold locations with cheap electricity
- Shifted to professional companies
- Model as Poisson process
- Reduced variance when mining together

3 Mining as a Group

- Track each person's computational contribution, using "near misses" as a proxy measurement
- Model 1: Pay per share. Pool manager pays flat fee per near miss above a set difficulty. No incentive to send valid blocks. High risk for pool manager.
- Model 2: Pay proportionally. Low risk for pool manager.
- Model 3: Pay someone to run ASIC cluster. Receive share of reward when new block is mined

4 Pros and Cons of Proof-of-Work

- Pros: Allow individuals and groups to make money, where otherwise impossible
- Cons: Few possible attacks; leads to centralization; wasteful!

5 Attacks on Proof-Of-Work

- Forking attack: Double spending possible if thief controls >51% of the network. Spends money, seller accepts because chain is long enough, then thief extends alternative chain, effectively erasing the previous transaction. May not require 51%
- Block-withholding attack: Solve a block, wait til someone else solves a block, then release yours to prevent their from being accepted. Increases your effective share of rewards.
- Blacklisting: Can refuse to process transactions from certain public keys

6 Disincentivizing Pool Formation

- Note that pool formation requires two components:

  Easy for miner to prove amount of work they are doing

  Easy for miner to prove that they're following rules

- Possible Solution: Change puzzles from Hash(transactions) to Hash(signature of transactions), where the secret key used to sign is the secret key corresponding to the recipient of the newly mined block

  Pool operators either give out private key for pool members to use

  or compute signatures themselves (10x more computationally expensive than hashing)

- Does nothing to counter ASICs

7 Countering ASICs

- Alternative puzzle requirements:

  Easy to verify solutions

  Adjustable difficulty to control rate of mining

  "Program freeness": chances of winning should be proportional to computational power. Also known as memoryless process.

- Trust-based networks e.g. Ripple
- Memory-Hard Puzzles
- Moving Target i.e. change puzzle to prevent pooling
- Virtual Mining i.e. Proof-Of-Stake

8 Trust-Based Networks

9 Memory-Hard Puzzles

- Goal: Decentivize consolidation by making individual computers competitive with ASICs.
- Method: memory-hard puzzles i.e. puzzles that require large amount of memory to solve or memory-bound puzzles i.e. puzzles that are slowed down by memory access time.
- Also known as space-hard puzzles
- Example: Scrypt. Used in Lytecoin. Two steps.

  1) fill large buffer of RAM with pseudorandom data i.e. for i = 1 to N: V[i] = SHA-256(V[i-1])

  2) read and update the memory in pseudorandom order i.e. X = SHA-256(V[N-1]). for i = 1 to N, j = X % N; X = SHA-256(X ^ V[j])

  Memory-hard because if V isn't stored in memory, recomputing X = SHA-256(X ^ V[j]) takes $O(n^2)$ instead of $O(n)$ as j is generated pseudorandomly.

  Unfortunately, requires as much money to verify as does to compute

  Eventually Litecoin revealed that Scrypt ASICs were better than ordinary hashing ASICs

- Example: Balloon Hashing. New family of space hard password hashing functions recently invented at Stanford by Boneh and Corrigan-Gibbs
- Example: Cuckoo Cycle. Based on difficulty of finding cycles in a graph generated from a cuckoo hash table.

10 Moving Target Puzzles

- Strategy: change puzzles occasionally so that ASICs are less cost-competitive

11 Virtual Mining

- Want alternative basis for "voting power" in distributed consensus protocol
- Proof-of-Work also requires consuming real world goods (energy, equipment) to create virtual dollars.
- Idea: allocate mining power to currency holders in proportion to how much currency they hold

  : Advantages: removes centralization because ASICs have less of an advantage, currency holders have stake in future health of ecosystem

  : Disadvantages: Richest participants given easiest mining puzzle; vulnerable to burst attacks (i.e. store up stake)
- Example: Peercoin

  Uses combination of Proof-of-Work and Proof-Of-Stake

  To mine, solve SHA-256, but difficulty based on age of coin that is "consumed" by validating that block
- Nothing-at-Stake Problem (i.e. Stake-Grinding): attacker A, with less than 50% of stake, tries to create fork of k blocks

  If fork succeeds, success. If fork fails, no cost
- Someone who controls >51% of currency can exclude others and mine only their own blocks

12 Proof-of-Useful-Work

- Idea: Use computing energy for some benefit to society instead of wasting it. Examples include:
- Example: Distributed computing projects e.g. SETI at Home, Folding at Home (protein structure folding)

  Problem: solution space was not equiprobable
- Example: Great Internet Mersenne Prime Search

  Problem: solutions too rare
- Primecoin uses proof-of-useful work, by requiring miners to find Cunningham chains of prime numbers. Questionable how useful this is.

13 Proof-of-Storage

- Also called Proof-of-Retrievability
- Idea: use miners' storage power to help with some archival project/distributed computing problem
- Used in Permacoin as follows:

  Let F be a large file that we want stored e.g. Large Hadron Collider backup data of several hundred petabytes

  Construct Merkle Tree of F

  Each miner given random subset of F called $F_M \subset F$

  Go read the paper if you care.