SmartPool: Decentralized mining pools using smart contracts

Loi Luu
Cofounder, SmartPool.io
PhD candidate, National University of Singapore

loiluu@comp.nus.edu.sg
loi_luu
Outline

• What is mining & pooled mining
• Why centralized mining pool is not ideal
• SmartPool solution
What is mining

• Probabilistically elects leaders to propose blocks
  – By solving proof of work, or mining

• A way to issue more coins
  – 12.5 BTC per 1 Bitcoin block
  – 5 ETH per 1 Ethereum block
How to mine a block

• Need to find a nonce so that

\[
\text{Hash(BlockHeader, nonce)} \leq d
\]

or

\[
\text{Hash(BlockHeader, nonce, dataset)} \leq d
\]

• Finding a valid nonce is hard
  – Normal computers take years to find a valid nonce
Mining pool

- Group of miners join hand to mine blocks together
- Reward is split among miners based on their contributions
  - Reduce variance
  - Receive smaller rewards frequently
How mining pools work

- Pools track miner contributions by using shares
  - A share is similar to a block, but required less work to find

  Valid block  \[ \text{Hash(BlockHeader, nonce, dataset)} \leq d \]

  Valid share  \[ \text{Hash(BlockHeader, nonce, dataset)} \leq D \quad \text{with } D \gg d \]

- Each share has probability \( \frac{d}{D} \) being a valid block
How mining pools work (2)

- Pool operator records the shares, and distributes reward accordingly
Pooled mining is great

• For miners
  – Allow them to have stable income
  – Low variance means easier to make economic plan

• For the network
  – Help increase the security of the network by allowing more miners to join the mining process
Centralized pooled mining issues

- Mining in cryptocurrencies is highly centralized
  - 3-5 pools control majority of hash power

**Bitcoin’s mining power distribution**

**Ethereum’s mining power distribution**
Centralized pooled mining issues (2)

• Implicit trust
  – Miners trust pool to record shares and pay correctly

• Transaction censorship threat
  – Pools decide which transactions to include, not the miners

• Single point of failures
  – Easy to partition the network [IEEE SS&P ‘17]
SMARTPOOL: REPLACING POOL OPERATOR BY A SMART CONTRACT
Naïve solution

Miner’s Local environment

Miner’s mining software

getWork()

Work responded

submitWork()

Pool’s Gateway

Ethereum Blockchain

submitShares()

Mining pool Smart Contract

User’s address

Reward is sent when a block is mined

Miner uses the pool’s address as the coinbase address in their blocks
Naïve solution’s Problems

- Number of shares is large
  - May require billions of shares per block
  - Require as many messages to the contract
- Cost (gas) to verify a Ethash PoW is expensive
  - May be more than the reward per share
  - Render negative incomes to miners
- Verifying an Ethash PoW was not even technically feasible
  - Require access to 1GB data set
  - Smart contract storage is costly (around $80,000 USD per GB)

\[
\text{Hash(BlockHeader, nonce, dataset)} \leq d
\]
SMARTPOOL’S SOLUTION
SmartPool – Solution

• Allow batch submissions (up to millions of shares)
  – significantly reduce number of transactions to the contract
  – only submit the Merkle root of all the shares
SmartPool – Solution (2)

- Probabilistic verification to check a submission
  - Randomly verify only one share per submission
  - $\Pr[\text{of cheating detected}]$ is proportional to the amount of cheating
SmartPool: Disincentivize cheating

- Penalty scheme: pay 0 share in a submission if cheating detected
  - Expected reward is the same whether cheating or not
  - Miners have no incentive to cheat
- If we sample more than 1 share, can strongly disincentivize cheating miners
- Cryptoeconomic is powerful!

- Get 1.5 Reward with 2/3 probability
- Get 0 Reward with 1/3 probability
- Expected reward = 1
SmartPool: Cheaply Verify Ethash PoW

• Verifying Ethash PoW was thought to be impossible inside a contract
  – *dataset* includes 64 random elements from a 1GB dataset. We can’t store the entire 1GB dataset
  – Can we store just the 16MB dataset? Since the 1GB dataset is generated from the 16 MB one
    • Would cost hundreds of Ethers
    • The 16MB dataset changes every 30k blocks (4-5 days)
    • Getting the element in the 1Gb dataset from the 16MB seed is expensive
      – i.e. requires 8 SHA-512 computations per element, will run out of gas

\[ \text{Hash(BlockHeader, nonce, dataset)} \leq d \]
Our solution: only verify the result of Ethash

• Observation
  – We do not need the entire 1GB data set nor the 16Mb seed, we only care about the correctness of the 64 sampled elements (based on the nonce and the block header)

• Solution
  – Store the Merkle root of the 1GB dataset in the contract
    • Everyone can verify this Merkle root
  – Require the miners to send the merkle proof for each data element
    • Checking the proofs for 64 elements is much cheaper and simpler
SmartPool’s Ethash in Testnet

• We self-implement the SHA-512 in solidity
  – Cost is 200k of gas per computation

• Fully verify an Ethash PoW with 3.9M of gas
  – Current gasLimit > 4M
  – Can be optimized further

• Our solution can be used to build a lighter light-client
More in the white paper

• How to prevent miners from stealing others’ shares?
• How to prevent claiming a share multiple times
  – Within a submission
  – Across submissions
• How to run mining pools for other cryptocurrencies on Ethereum
SmartPool: Features and Plan

• Features
  – Totally decentralized
  – Secure
  – Efficient and scalable
  – Open source and non-profit

• Plan
  – Testnet deployment in March
  – Mainnet deployment in May
  – Supporting other cryptocurrencies depends on funding
SmartPool.io is calling for donation

WE ARE CALLING FOR DONATIONS

Current donated amount: 1633.77856 ETH

Our addresses

Ethereum: 0x98F62d8aD5a884C8bbcF262591DFF55DAb263B80
Bitcoin: 1Cs3D54RqjhNwHurj97qQpbiDSYw1EkjPC
ZCash: t1eZFvNbvfgGShyPX4RzScLd76apdVoD2qN
Closing thoughts

• Blockchains & smart contracts help remove middle man/centralized operators
  – Decentralized mining pools is one example.

• Blockchains & smart contracts are the tools, not the solutions
  – More thoughts on the design and implementations required
Acknowledgement

- Ethereum Foundation
- DinarDirham
- 24 pseudonymous donors
Thank you – Q&A

http://smartpool.io

SmartPool_Prj