Not So Predictable Mining Pools

Attacking Solo Mining Pools by Bagging Blocks and Conning Competitors

Jordan Holland, *R. Joseph Connor, Parker Diamond, Jared M. Smith, Max Schuchard*

University of Tennessee
VOLSEC
— COMPUTER SECURITY LAB —

Outline

- Predictable Solo Mining is a new payout scheme being used in real-world cryptocurrency mining pools
- Our work examines the security of the Predictable Solo Mining payout scheme
- We introduce three attacks on the payout scheme
  - One attack exploiting cheap rewards in the pool
  - Two attacks increasing the cost others pay for rewards

BACKGROUND

Mining Pools

- The number of miners means solo mining is realistically unprofitable due to variability in profits
- Variability in profits goes down with larger miner hashrates
- Mining pools aggregate computational power, receive more consistent rewards, and distribute rewards to the members of the pool

Payout Scheme

- Determines how to allocate the pools revenue between individual miners

- Ideally we want a mining pool scheme to exhibit:
  - Incentive Compatibility
  - Proportional Fairness

- Mining pool operators want competitive advantage, leading to different payout schemes being used that aren't vetted

Payout Schemes: Details

- Users submit partial proofs of work to receive “shares”
  - Higher difficulty proofs of work worth more shares
- Example: Pay Per Last N Shares (PPLNS)
  - Only the last N shares submitted are considered when calculating rewards after a block is found
- More in use today, prior work shows that some violate incentive compatibility and fairness properties

Predictable Solo Mining (PSM)

- Each submitted share will increase the credit of the miner who submitted the share by the share difficulty
  - Miners with higher hash rates move up the leaderboard faster

- PSM is unique in that it **does not** divide the block reward to the pool
  - Share leader receives entirety of the reward

- $Post\ Reward\ Shares = Pre\ Reward\ Shares\ - Runner\ Up\ Shares$

Simple PSM Example

Shares Pre Block

- 1. A - 10,000
- 2. B - 8,000
- 3. C - 4,000
- 4. D - 3,000
- 5. E - 1,000

Shares Post-Block

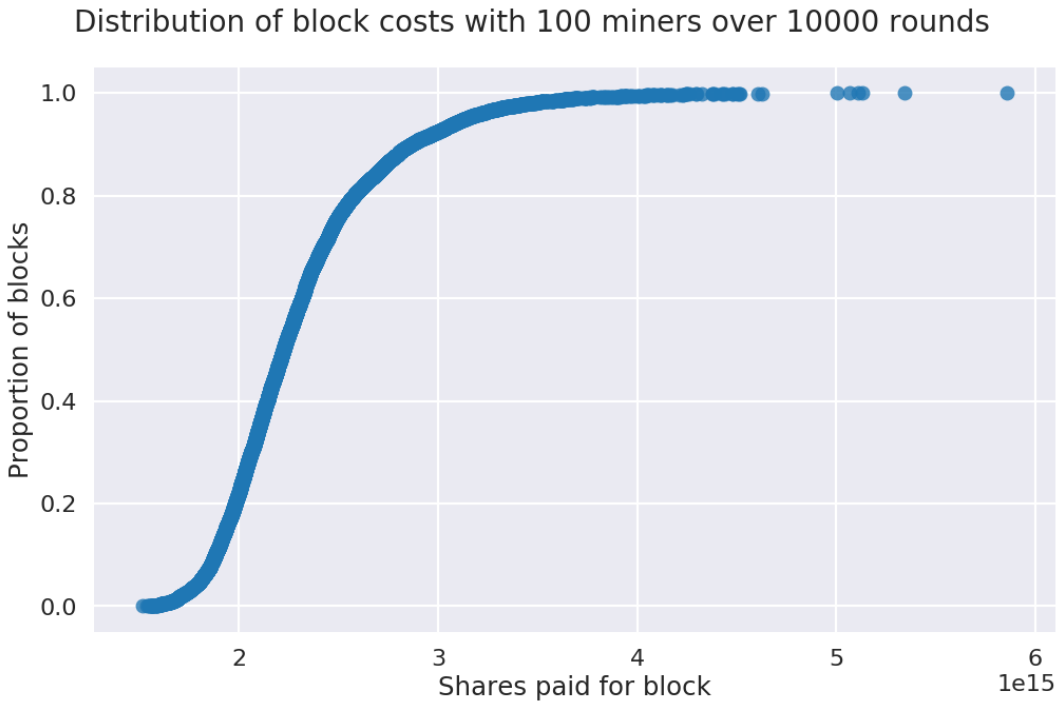
- 1. B - 8,000
- 2. C - 4,000
- 3. D - 3,000
- 4. A - 2,000 ← Previous Leader
- 5. E - 1,000

ATTACKS

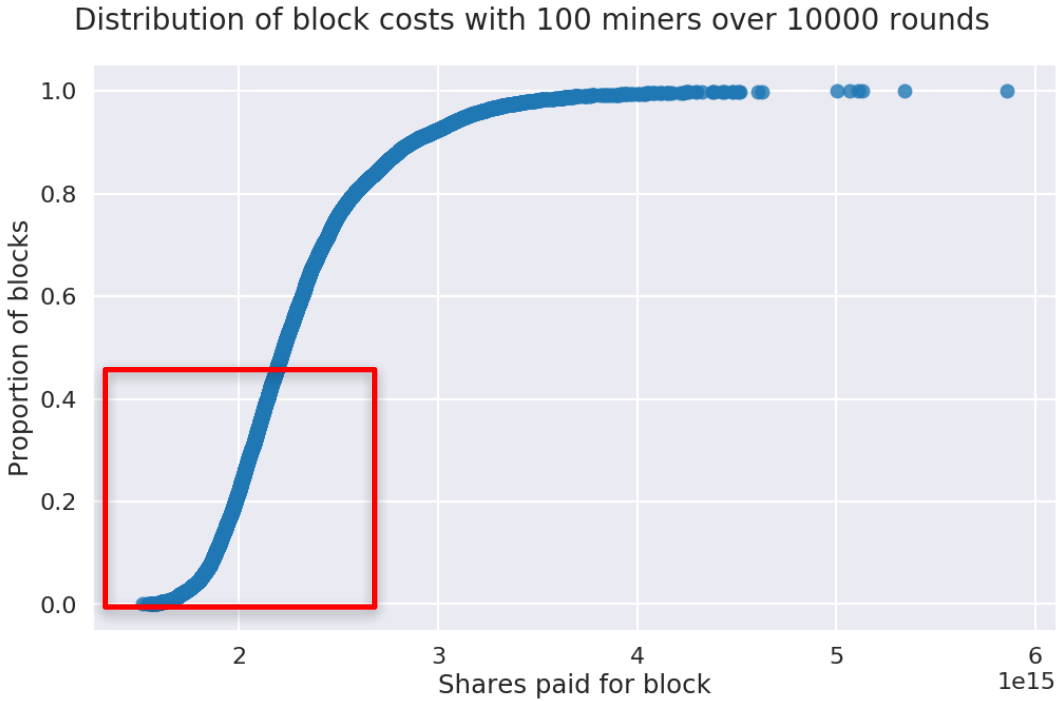
Key Insights

- “Cost” of a block reward can be characterized by the number of shares held by the second place miner
- PSM Claim: The average block cost is equal to the network difficulty
- The amount of shares expended winning two different blocks, which have the ***same monetary value***, varies by up to a factor of ***four***

Cost of Blocks in PSM



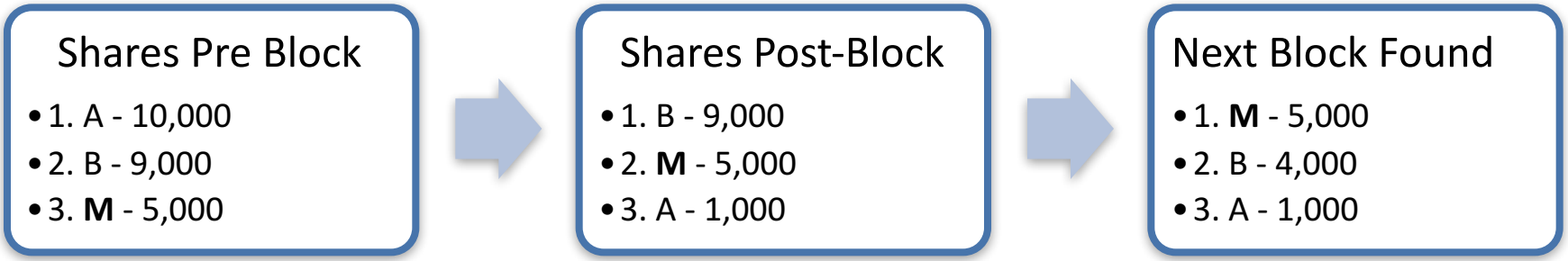
Exploiting Cheap Blocks



Share-Cost Minimization

- Honest miners submit all of their work to the pool, driving themselves up the leaderboard
- Attacker only wants to win “cheap” blocks
- A malicious miner can refuse to place any more than *n* shares into their account, and only win blocks at a cost of ***at most n*** shares
- Violates proportional fairness

Share-Cost Minimization: Example

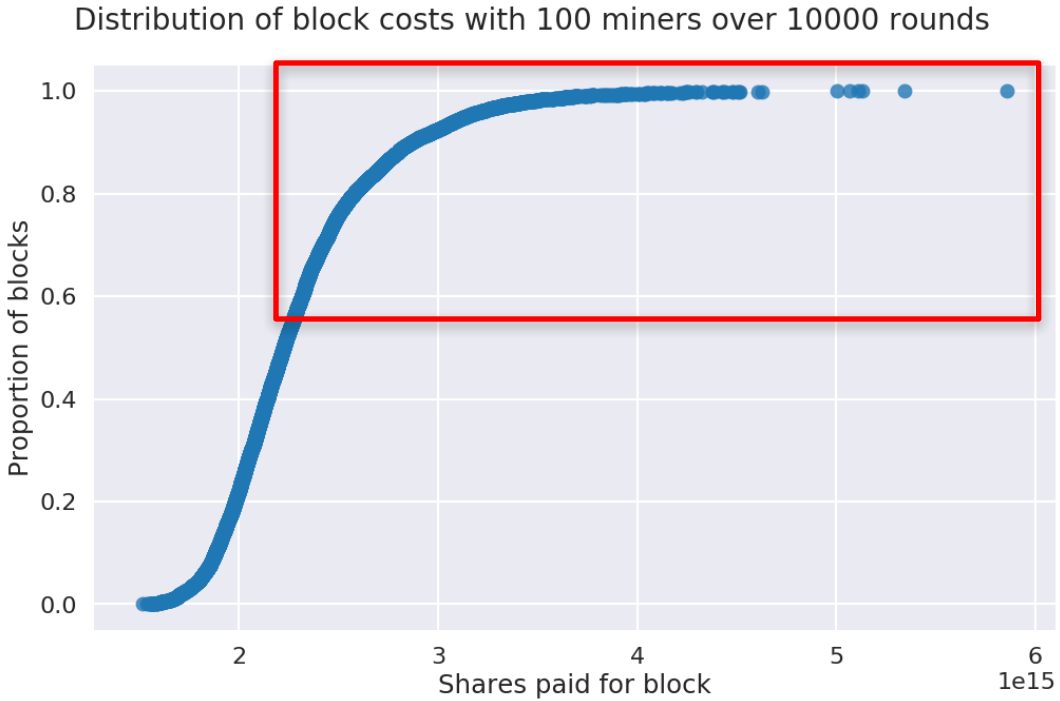


Leftover Computing Power

- Only submitting a set number of shares to the pool leads to leftover computing power
  - Spend this computational power in the same pool
  - Spend this computational power in other pools

- Violates incentive compatibility

Exploiting Expensive Blocks



Malicious Share Donation

- Many pools do not authenticate share submissions
- A malicious miner can submit shares to the 2nd place miner to minimize the gap between 1st and 2nd place
- Effectively maximizes the average cost the target miner pays for each block

Malicious Share Donation: Example

Shares Pre-Donation

- 1. **T** - 10,000
- 2. B - 9,000
- 3. C - 4,000

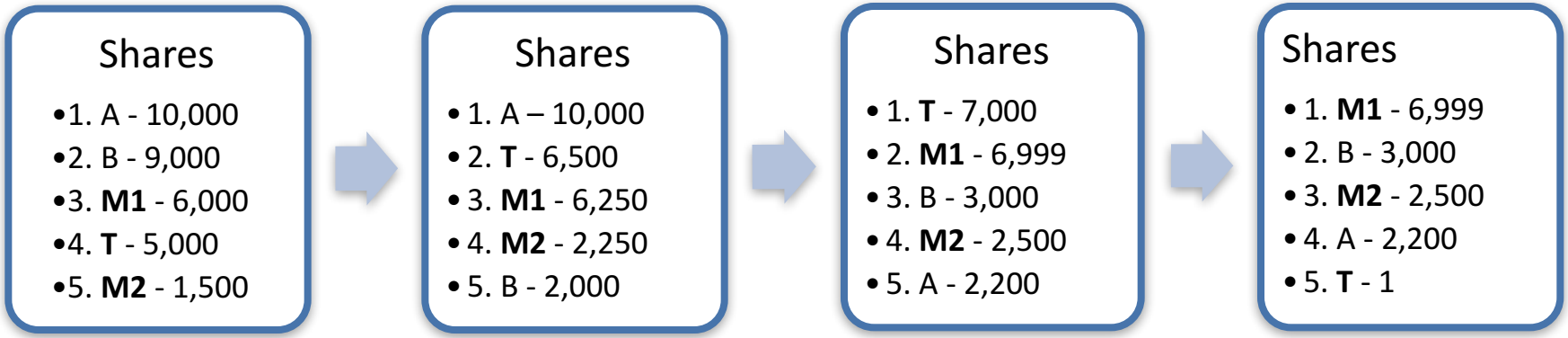
Shares Post-Donation

- 1. **T** - 10,000
- 2. B - 9,999
- 3. C - 4,000

Multiple Account Idling

- Share Donation Attack is intuitive and effective
  - Relies on lack of authentication in pools
- We can increase the average block cost for a target miner in pools with authentication
  - Do not need to donate to other miners
- Use multiple accounts, idle one account until target miner in range

Multiple Account Idling: Example

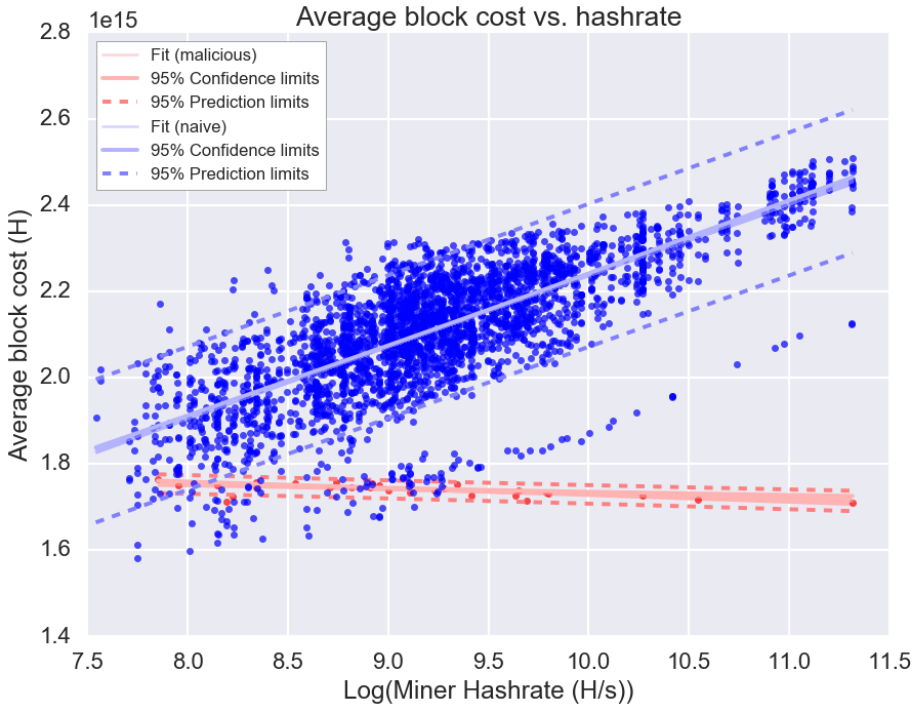


EVALUATION

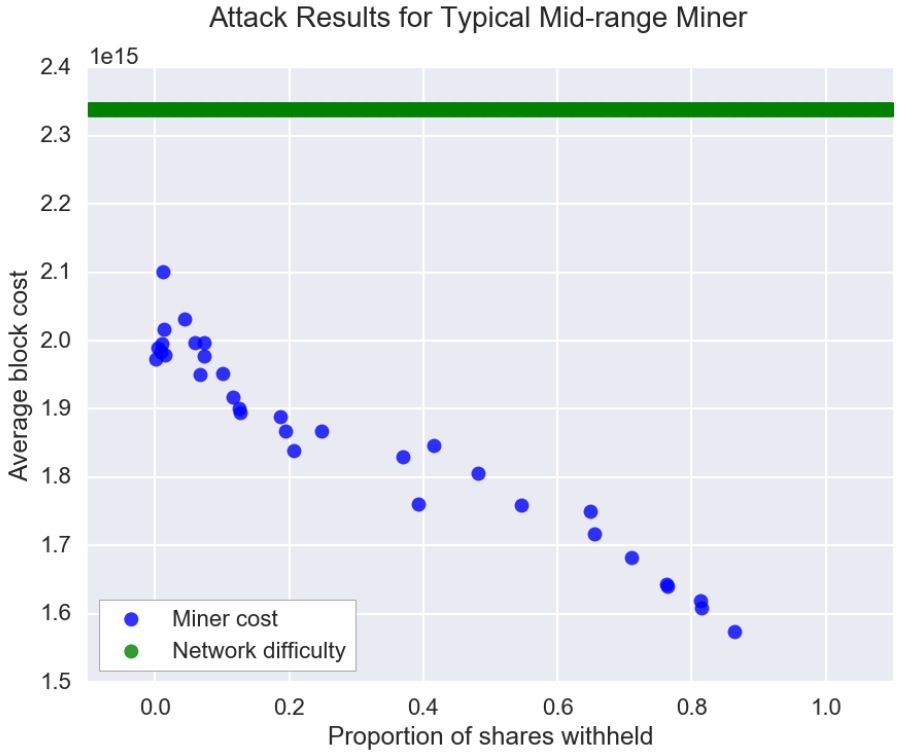
Simulation

- Important to test attacks with real-world pool hashrates
- Collected active miners via Ethpool and Ethermine API
- Built discrete mining pool simulator from collected hashrates
- Mining pool simulator runs with both honest and malicious miners using current network difficulty
- Code Available at: https://github.com/VolSec/aminingpoolsimulator

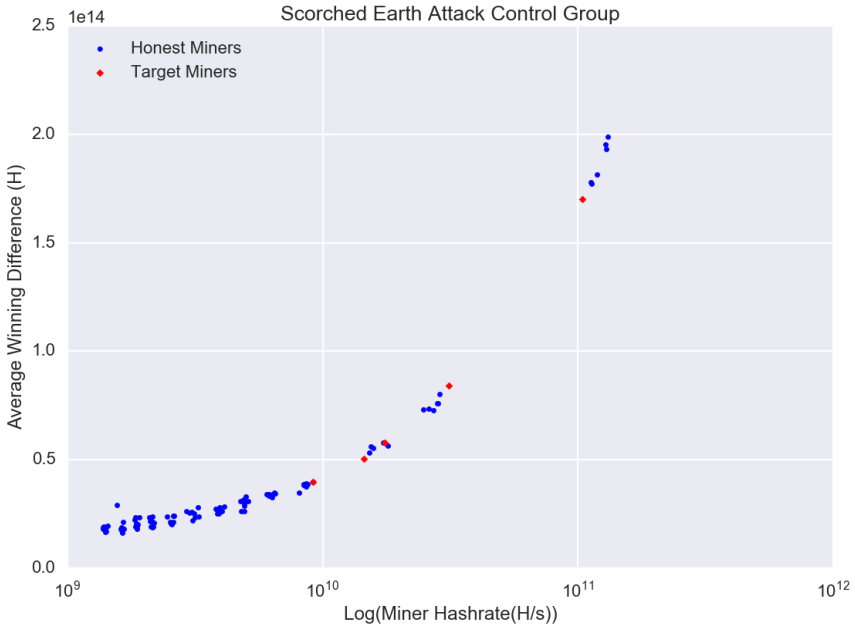
Share-Cost Minimization

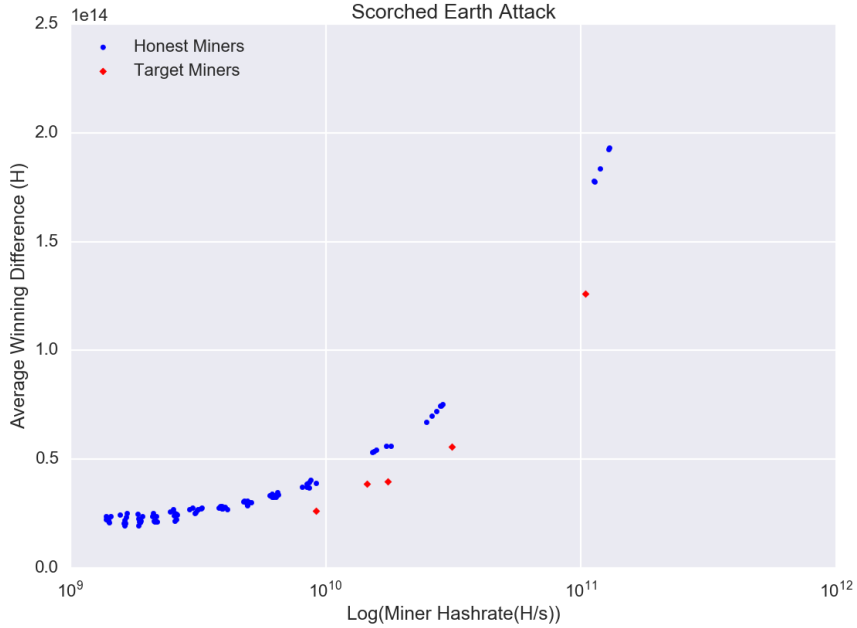


Share-Cost Minimization



Malicious Share Donation





Multiple Account Idling

Attacker / Target Ratio	% Decrease in Average Winning Difference
1.2	.03
4.2	5.02
7.5	6.31
9.0	5.6
14.2	8.36

Conclusions

- Payout schemes need to be vetted for incentive compatibility and fairness before being used in practice
- In any payout scheme, a single miner should not be able to influence the price of the reward of another miner
- Authentication in pools can help reduce future attacks

Questions?

Jordan Holland

jholla19@vols.utk.edu

University of Tennessee
VOLSEC
— COMPUTER SECURITY LAB —