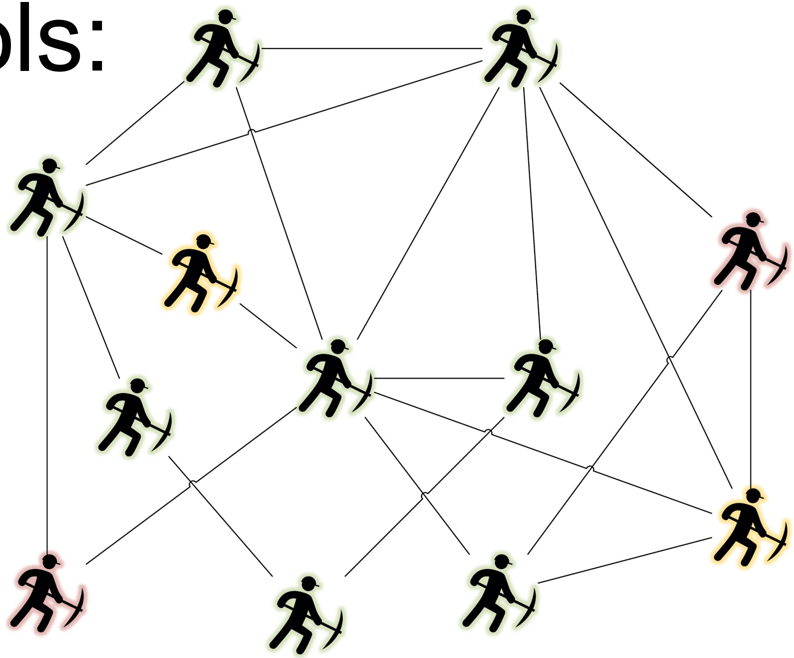
Imperial College London
SBA Research

Decentralized Mining Pools: *Security and Attacks*



Alexei Zamyatin

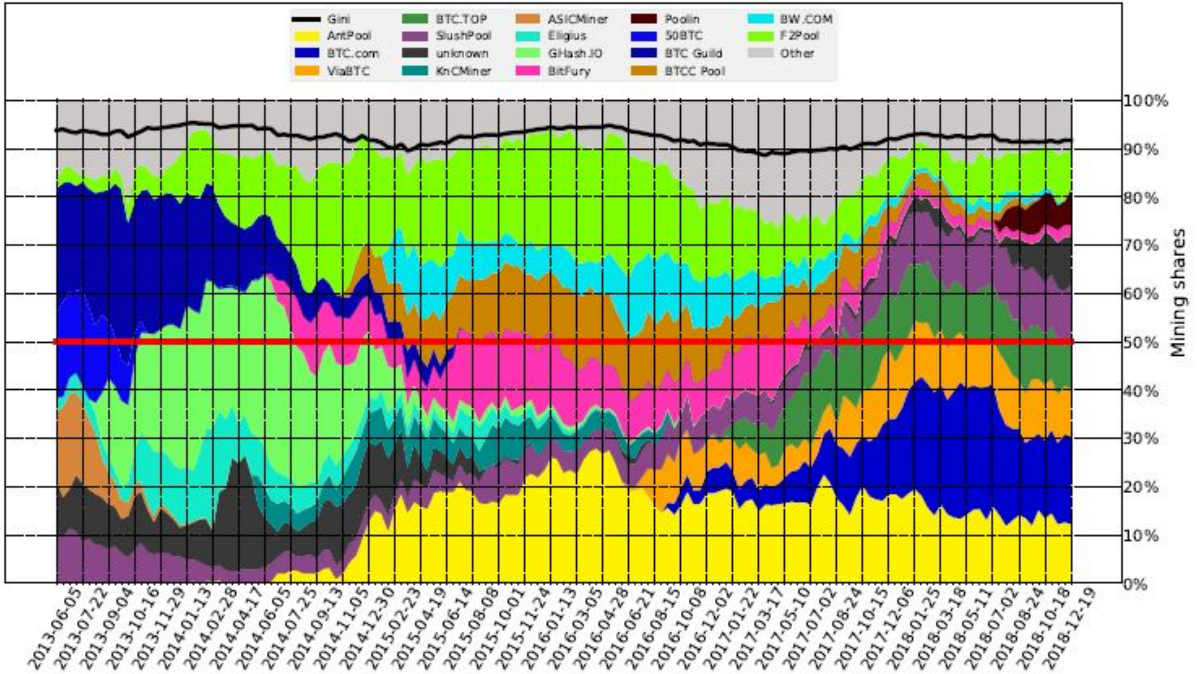
Breaking Bitcoin 2019, Amsterdam

2F5F E92D CDAC 15B0 84A6 9FE9 9018 A958 5485 B999

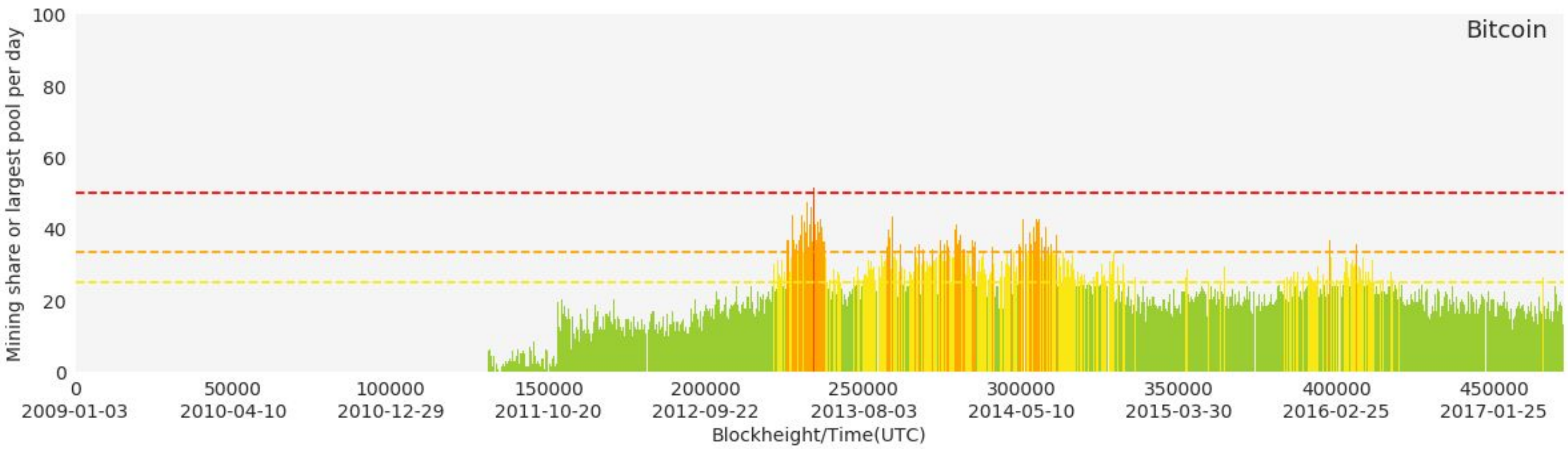
Motivation

Centralization around large mining pools in PoW cryptocurrencies

Censorship resistance & fair payouts **not guaranteed**



Source: A Deep Dive into Bitcoin Mining Pools: An Empirical Analysis of Mining Shares. Romiti M, Judmayer A, Zamyatin A, Haselhofer B. *Workshop on the Economics of Information Security (WEIS)*, 2019



College

earch

While Bitcoin appears balanced, small cryptocurrencies often suffer from centralization

Source: Merged Mining: Curse or Cure?. Judmayer A, Zamyatin A, Stifter N, Voyiatzis AG, Weippl E. *International Workshop on Cryptocurrencies and Blockchain Technology (CBT),* 2017


Bitcoin
Mining share or largest pool per day
Blockheight/Time(UTC)
0 2009-01-03
50000 2010-04-10
100000 2010-12-29
150000 2011-10-20
200000 2012-09-22
250000 2013-08-03
300000 2014-05-10
350000 2015-03-30
400000 2016-02-25
450000 2017-01-25
Namecoin
Mining share or largest pool per day
Blockheight/Time(UTC)
0 2011-04-17
50000 2012-04-03
100000 2013-03-13
150000 2013-12-08
200000 2014-10-07
250000 2015-09-23
300000 2016-08-13
Introduction of merged mining (block 19200)
50% Theshold
33.33% Theshold
25% Pessimistic Theshold
Insignificant
Greater 25%
Greater 33.33%
Greater 50%

Goals of Decentralized Mining (Pools)

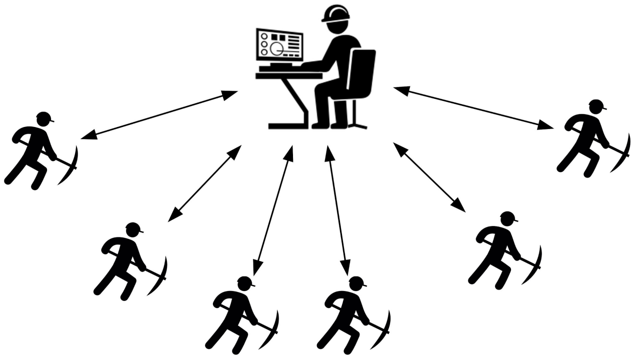
1. **Censorship resistance**: allow miners to select transactions

2. **Incentive compatibility:** transparent & fair payout scheme

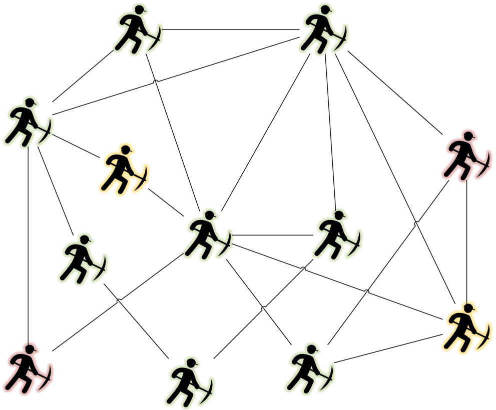
Goals of Decentralized Mining (Pools)

Challenge: agreement on reward distribution

- **Centralized pool:** single leader (trusted operator)
- **Decentralized pool**: agreement among all miners
  - Must verify other miner's shares



VS



Goals of Decentralized Mining (Pools)

1. **Censorship resistance**: allow miners to select transactions

2. **Incentive compatibility:** transparent & fair payout scheme

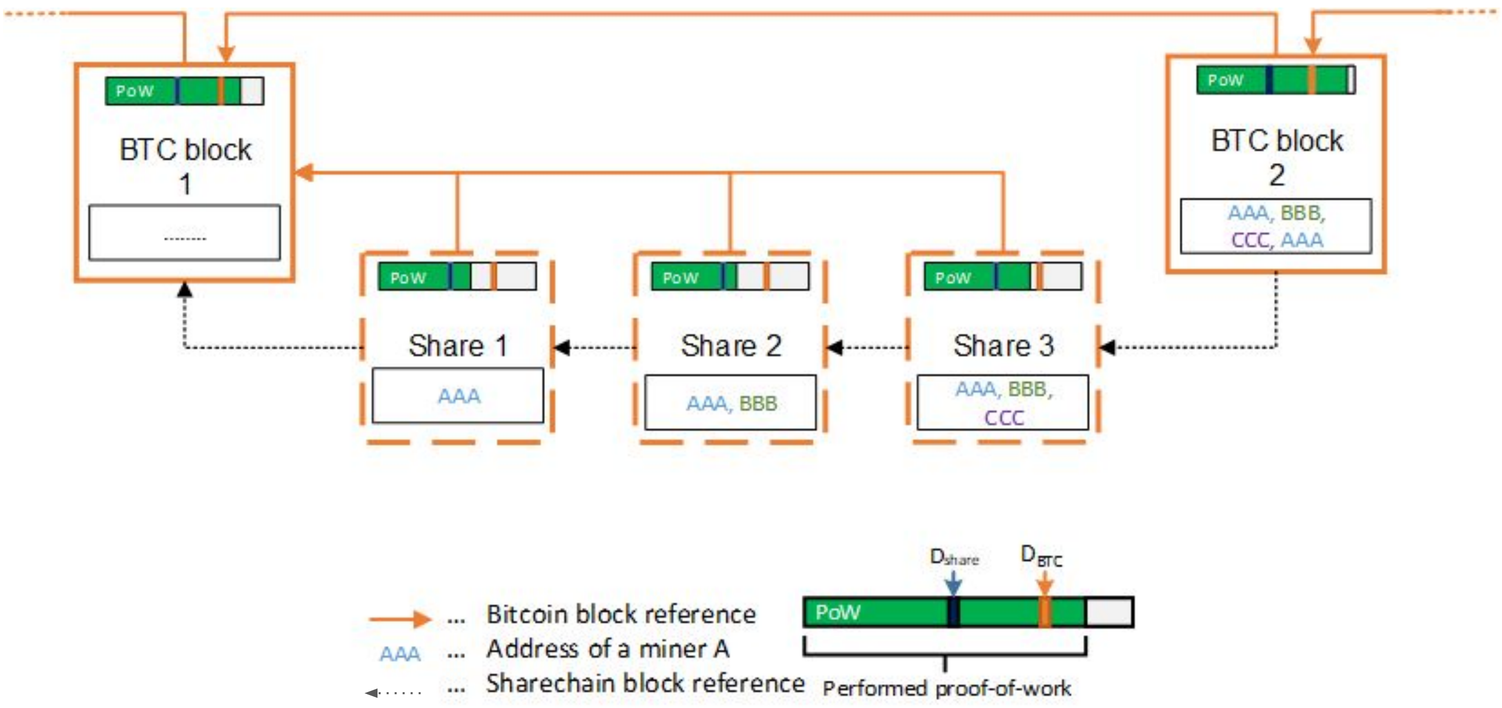
3. **Efficiency:** Minimal performance overhead

P2Pool (Voight et al., 2011)

Uses a separate “Sharechain” (FIFO queue) consisting Bitcoin weak blocks to agree on reward distribution

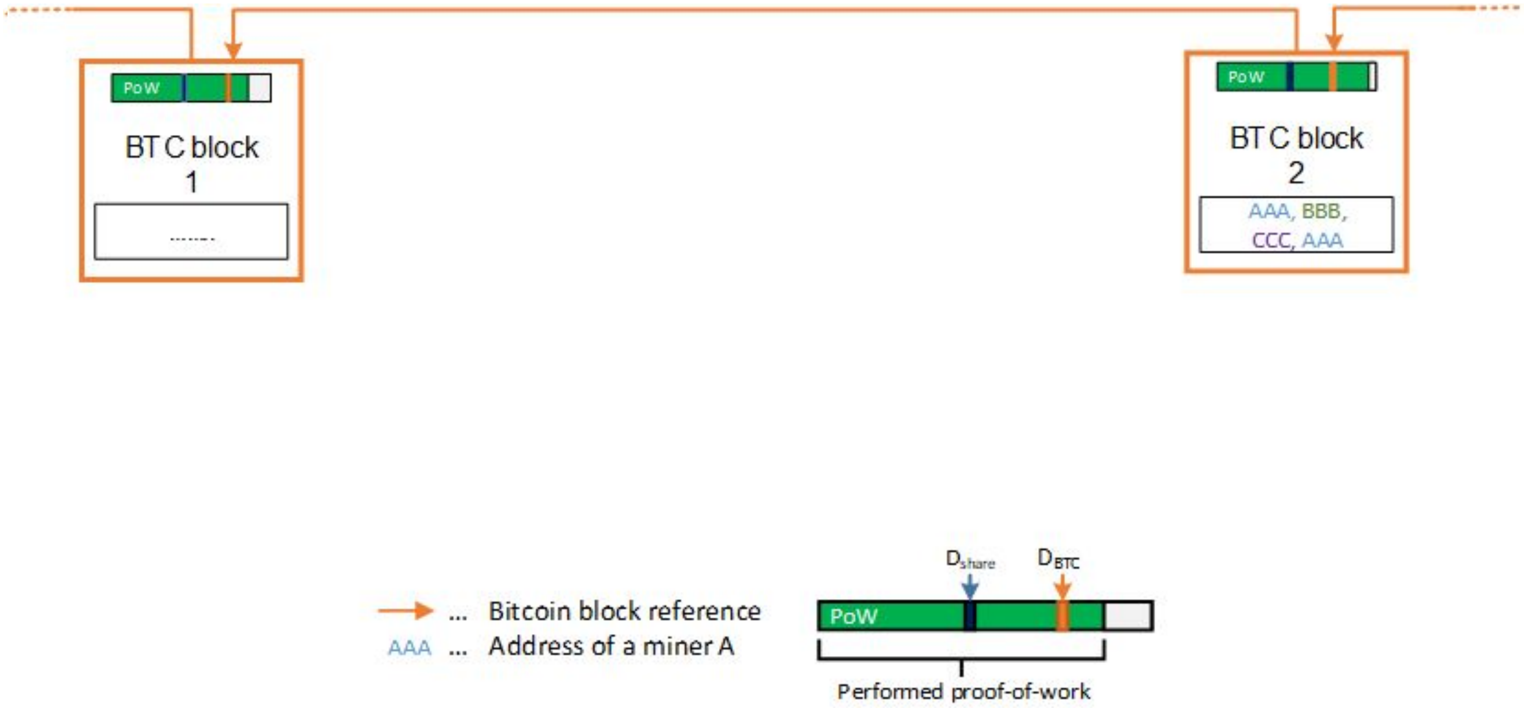
P2Pool contd.

As seen by P2Pool miners:



P2Pool contd.

As seen by the rest of the network:



P2Pool contd.

Agreement:

- Separate, bounded “Sharechain” → Bitcoin weak/near blocks
- Miners compete for shares in Sharechain

Scheme: PPLNS (~3 days)

Share Difficulty:

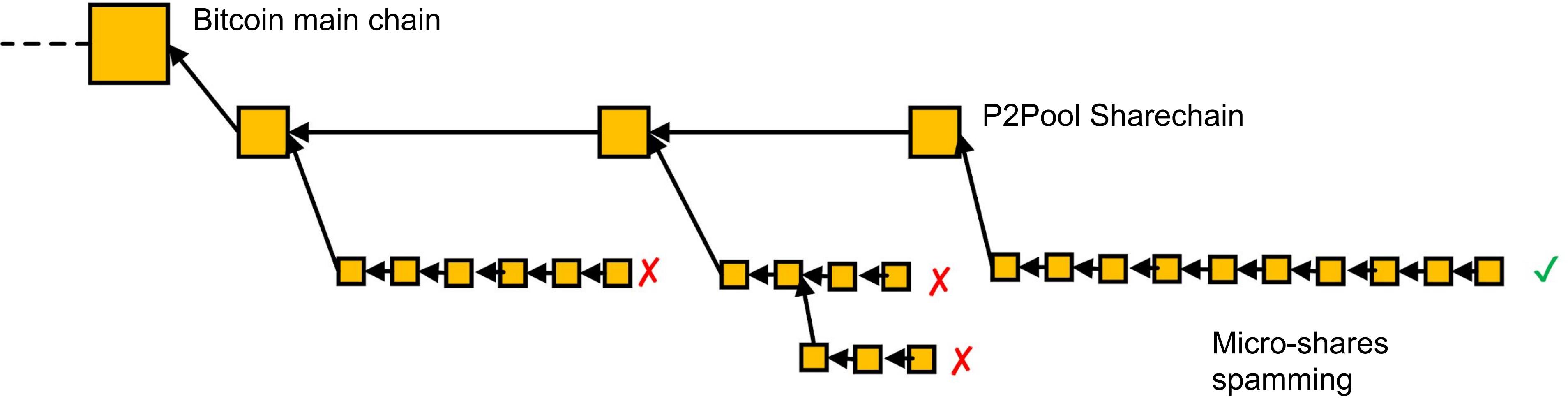
- Defined by overall P2Pool hash rate (~30 sec block interval)
- varDiff not possible

Requirements: none (block intervals can’t be too low, e.g. >1min)

P2Pool Challenges

Share Difficulty Handling

- Sharechain **must** define minimum difficulty
- **Reason: micro-share spamming!**
  - Even with “heaviest” chain rule: high level of forking = destabilization



Share Difficulty Handling

- Sharechain **must** define minimum difficulty
- **Reason: micro-share spamming!**
  - Even with “heaviest” chain rule: high level of forking = destabilization

- **Approaches**:
  - Static - fixed percentage of Bitcoin’s difficulty.

    Problem: May be too high for small miners / too low for large miners

Share Difficulty Handling

- Sharechain **must** define minimum difficulty
- **Reason: micro-share spamming!**
    - Even with "heaviest" chain rule: high level of forking = destabilization

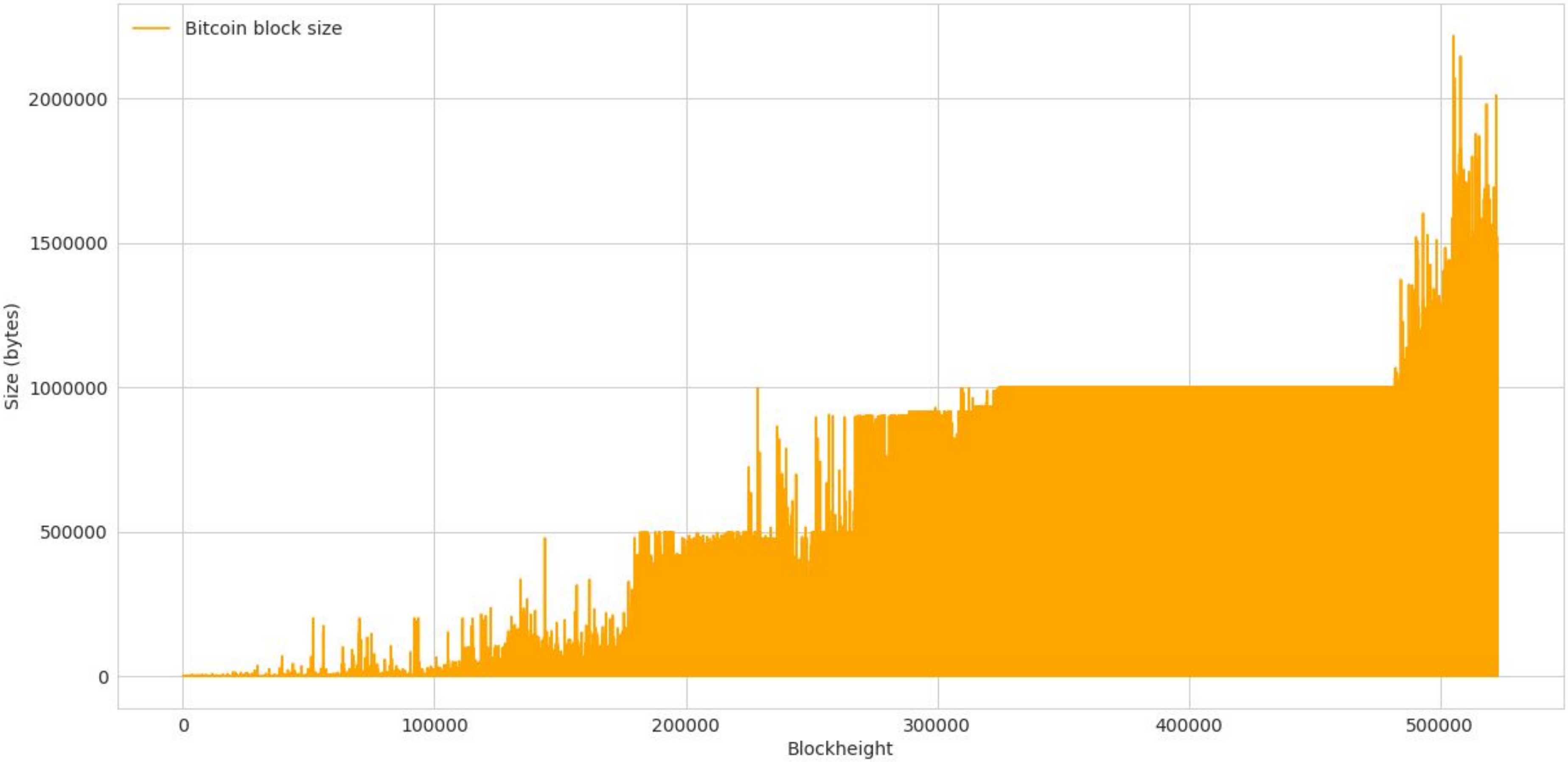
- **Approaches**:
    - ~~Static - may be too high for small miners / too low for large miners~~
    - Dynamic - like in Nakamoto consensus (currently implemented)

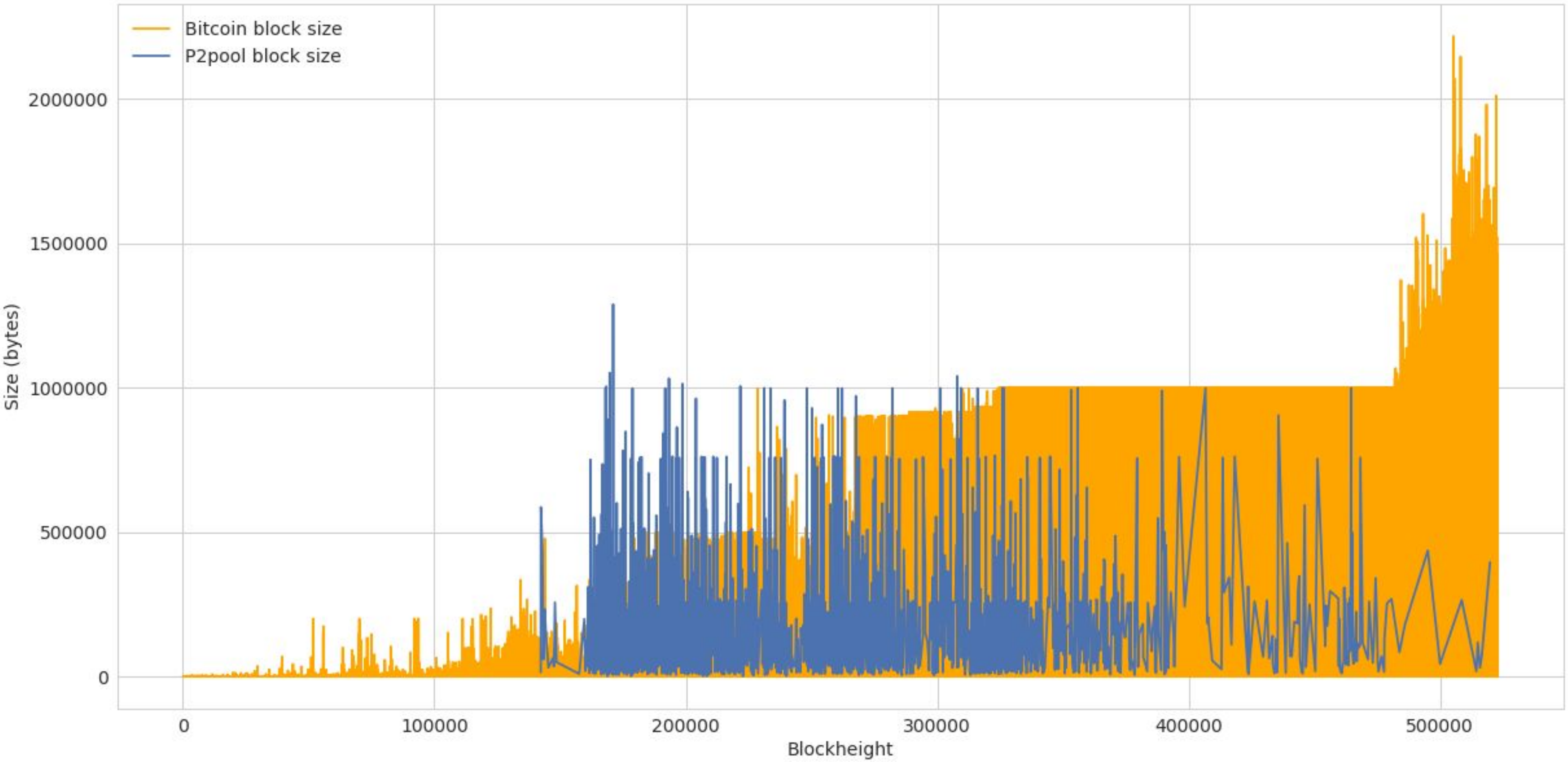
      Problem: large miner(s) can push difficulty upward, **yielding P2Pool useless for small miners**

      → Leads to multiple pools in the long run

Block Size and Latency Issues

- Each share is broadcasted to P2Pool network
  → **Significant overhead**
- Miners with low bandwidth have troubles handling network load
- Original P2Pool code imposed Tx size limit


Bitcoin block size
Size (bytes)
2000000
1500000
1000000
500000
0
0
100000
200000
300000
400000
500000
Blockheight


Bitcoin block size
P2pool block size
Size (bytes)
2000000
1500000
1000000
500000
0
0
100000
200000
300000
400000
500000
Blockheight

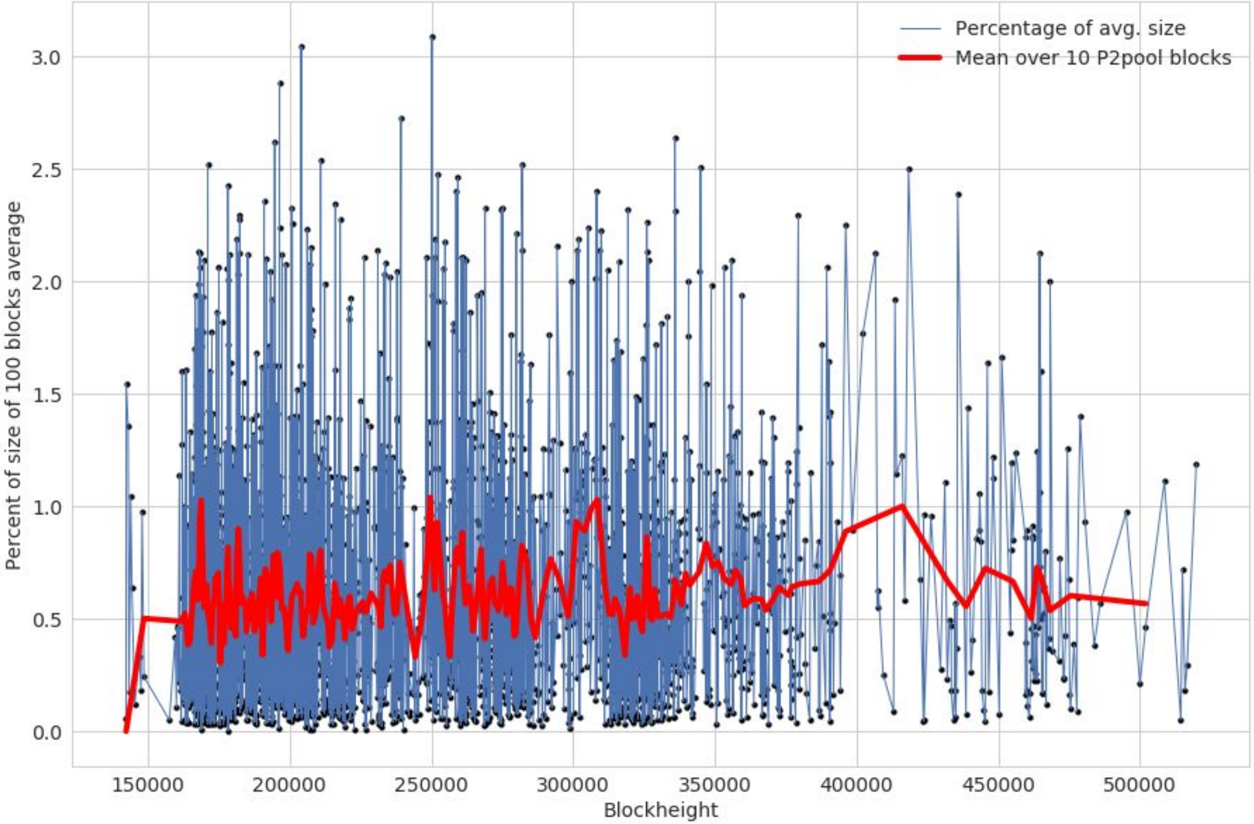
Block Size and Latency Issues - Observations

High fluctuation of block size

P2Pool blocks **only had ~ 60.8% of the size of Bitcoin blocks on average***

Resulted in two P2Pool networks being created

* 100 block moving average



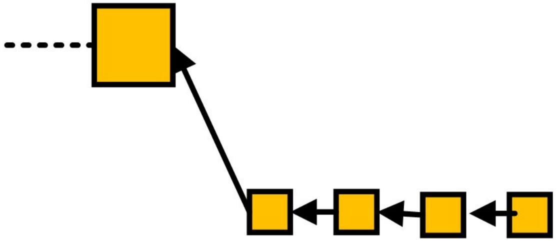
Attacking P2Pool

Selfish Mining & 51% Attacks

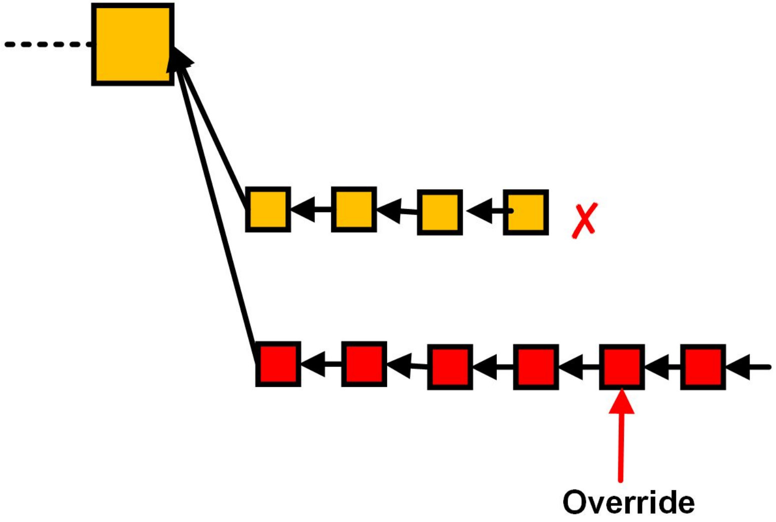
- P2Pool participation is optional (velvet fork!)
  - Separate consensus protocol (Nakamoto)!

- Even small attackers can be successful
  - Example:
    - P2Pool: 10% hash rate
    - Attacker: 6% or even 4% hash rate

Selfish Mining & 51% Attacks

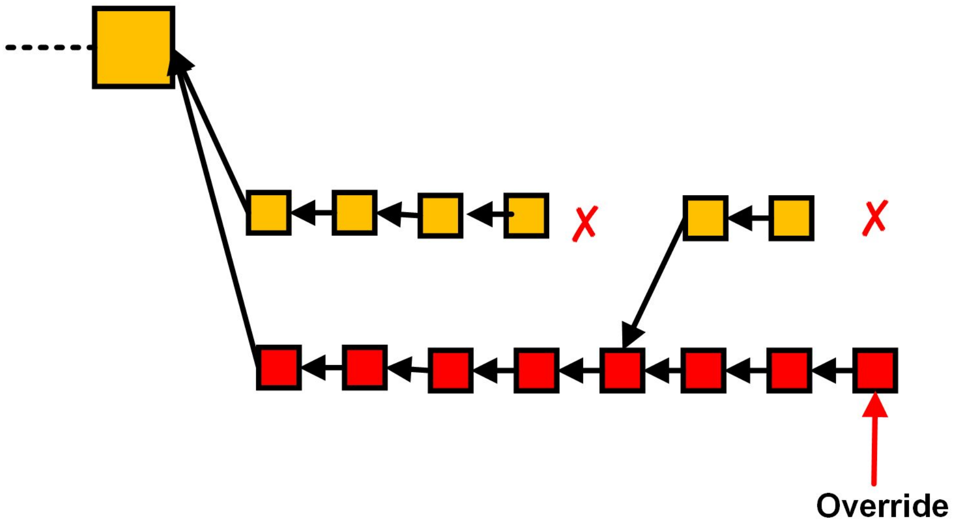


Selfish Mining & 51% Attacks

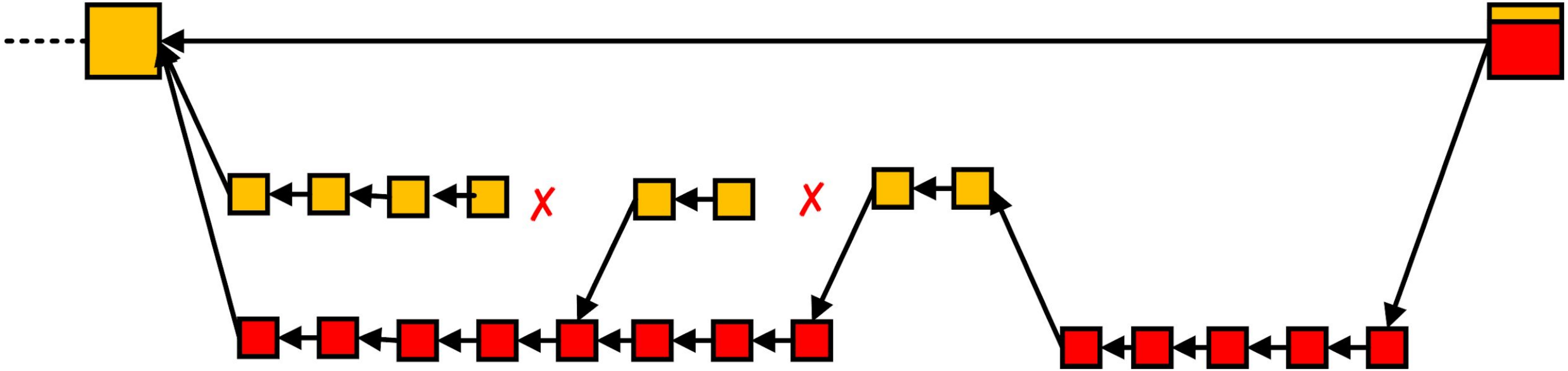


Attacker dominance / majority on Sharechain

Selfish Mining & 51% Attacks



Selfish Mining & 51% Attacks



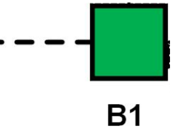
Can increase of rewards at the cost of P2Pool miners

Impacts on Bitcoin security?

Temporary Dishonest Majority

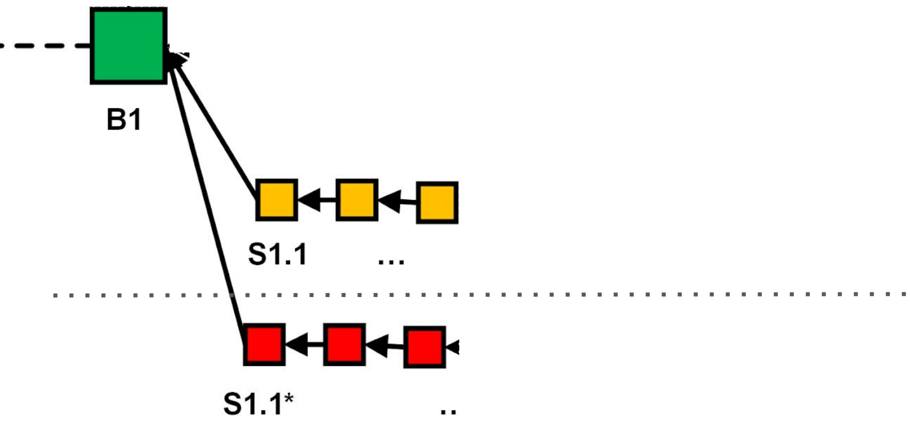
- Attacker may attempt to use P2Pool for a temporary main chain majority
- Example: **P2Pool: 30% , Attacker: 21% of overall hash rate**
- Attacker wants to launch forking attack on main chain
  - e.g. double spend, selfish mining, ...

Temporary Dishonest Majority



Attacker executes selfish mining attack, both on Bitcoin and Sharechain

Temporary Dishonest Majority

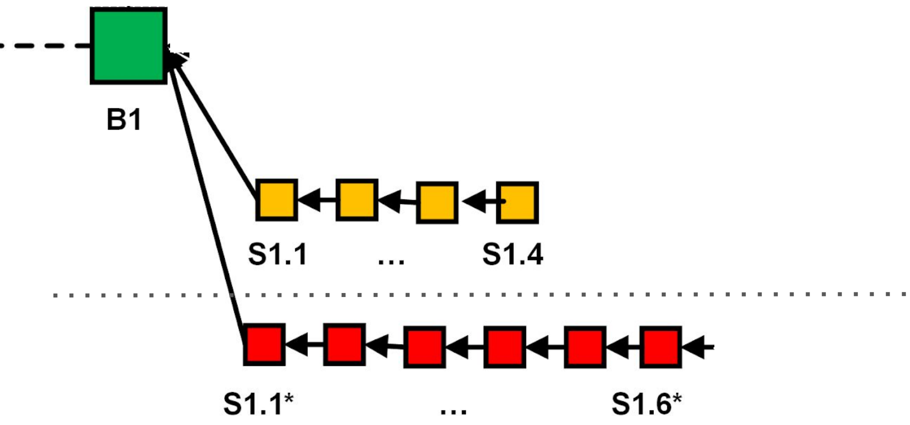


Red = attacker's "secret" chain

Orange = P2Pool Sharechain

Green = Honest main chain

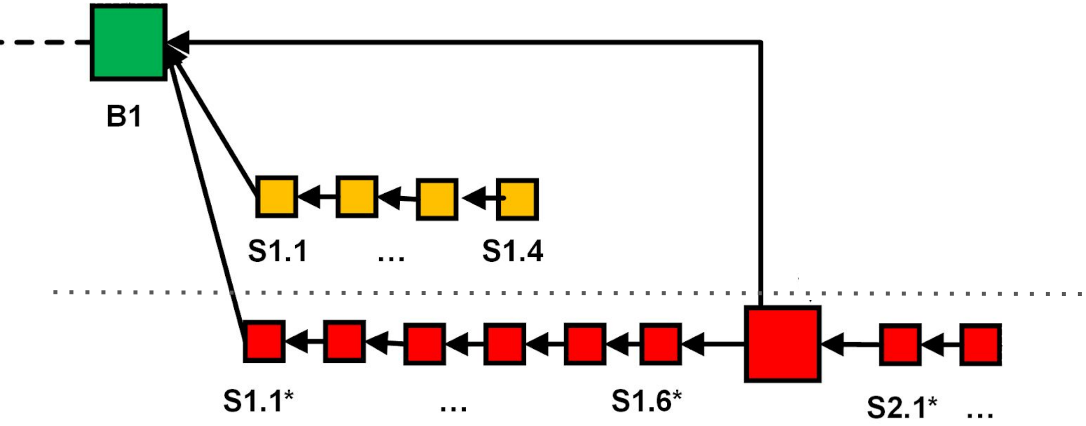
Temporary Dishonest Majority



Attacker has >51% of P2Pool hash rate

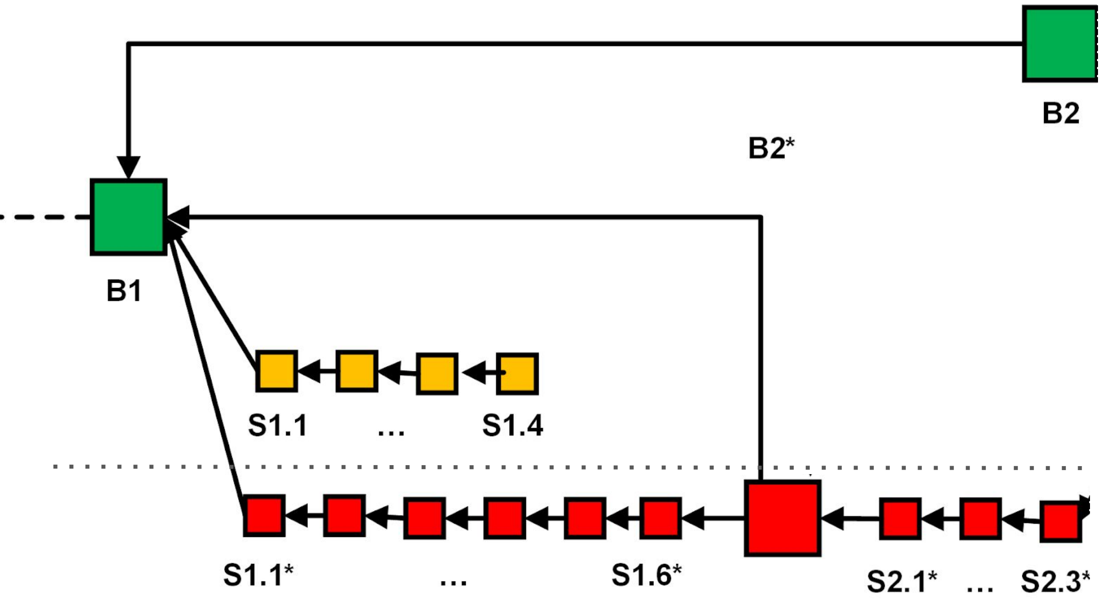
→ Can easily mine longer & heavier Sharechain (in secret!)

Temporary Dishonest Majority



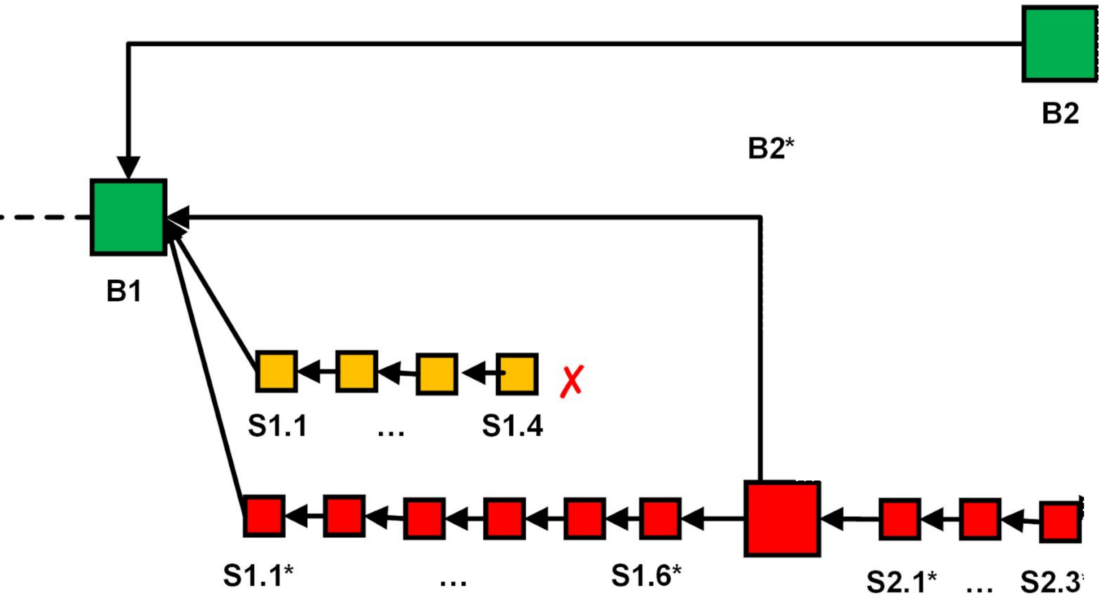
Attacker overtakes honest chain

Temporary Dishonest Majority



Alas, honest chain finds block matching attacker chain's height

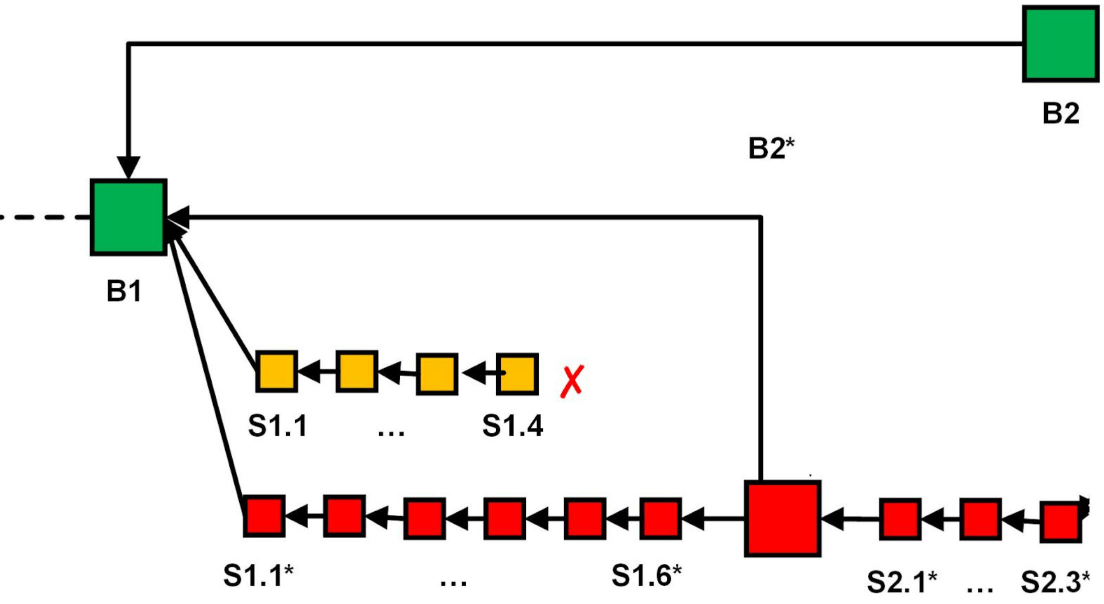
Temporary Dishonest Majority



“Match“: attacker broadcasts

- ***B2**** to main chain
- ***(S1.1*,…,S1.6*), B2*, (S2.1*,…,S2.3*)*** to P2Pool

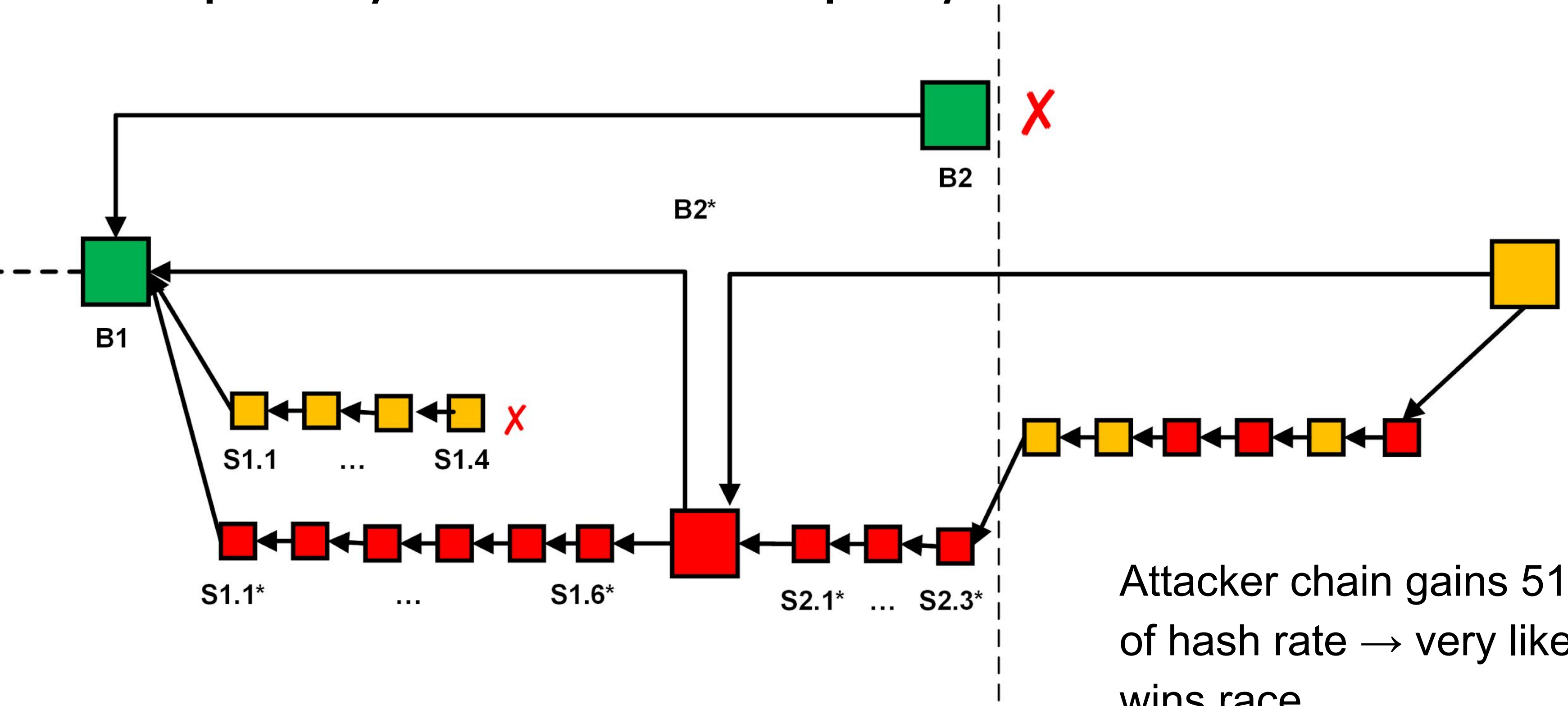
Temporary Dishonest Majority



<u>Normal SM</u>: better network connectivity wins

<u>However</u>: P2Pool miners extend longest share chain → attacker's chain

Temporary Dishonest Majority

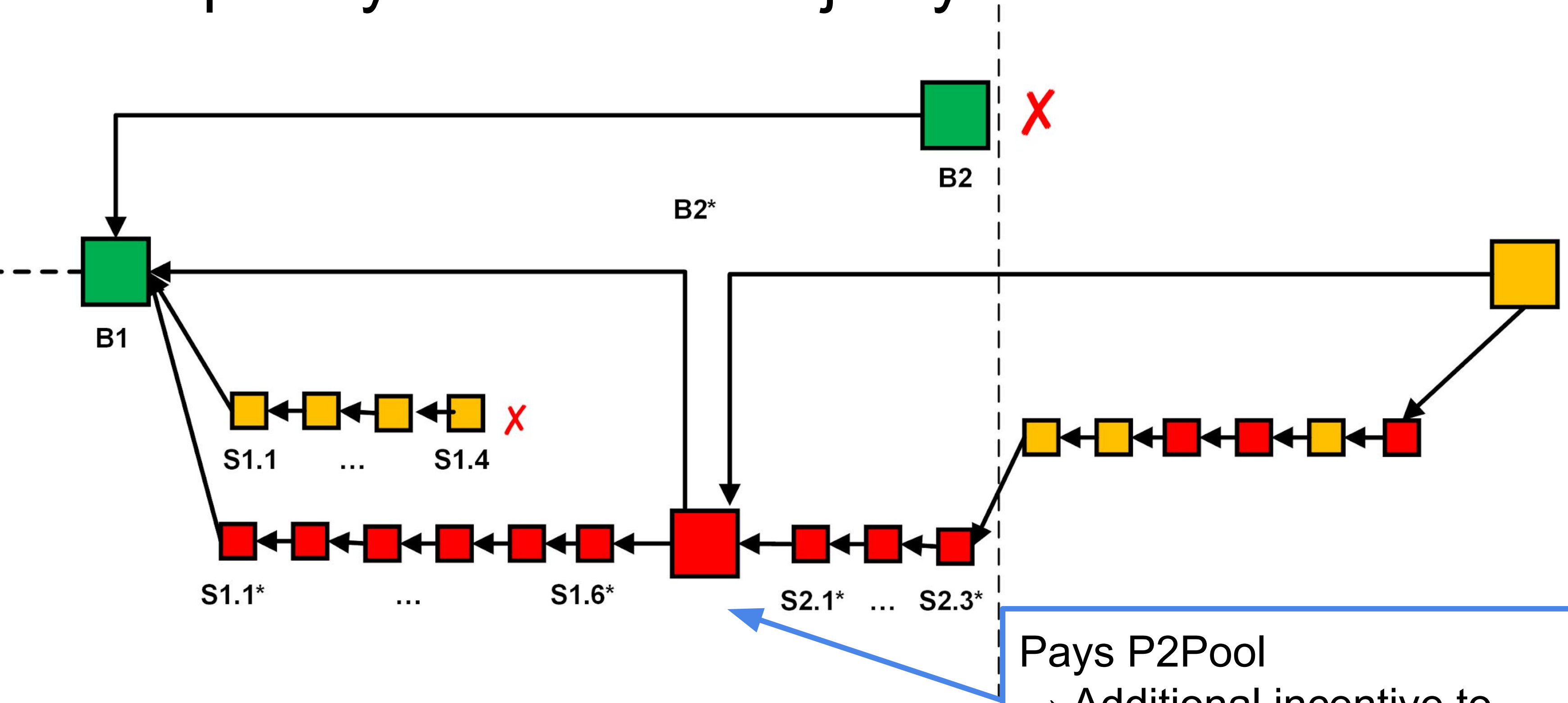


Attacker chain gains 51% of hash rate → very likely wins race

Temporary Dishonest Majority - Extended

- Until now we **assumed P2Pool miners broadcast blocks received over Sharechain to Bitcoin**
  - Hence the attacker keeps Sharechain blocks secret
- **If this is not the case:**
  Attack becomes **more effective** → P2Pool may join attacker chain from start

Temporary Dishonest Majority - Extended

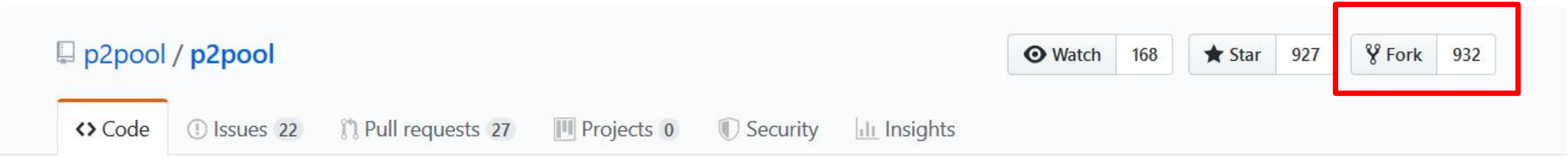


Pays P2Pool
→ Additional incentive to comply?

P2Pool Today

- Codebase not actively maintained?
  - Main net: Latest commit 53c438b on Sep 19, 2018
  - jtoomimnet : Latest commit ad3cbde on Dec 18, 2018

- Lots of forks
  - Some implement broken concepts discussed today (e.g. miner-chosen share difficulty) :(



P2Pool - Did it work?

Interesting observation:

- P2Pool setup and node hosting complex/costly

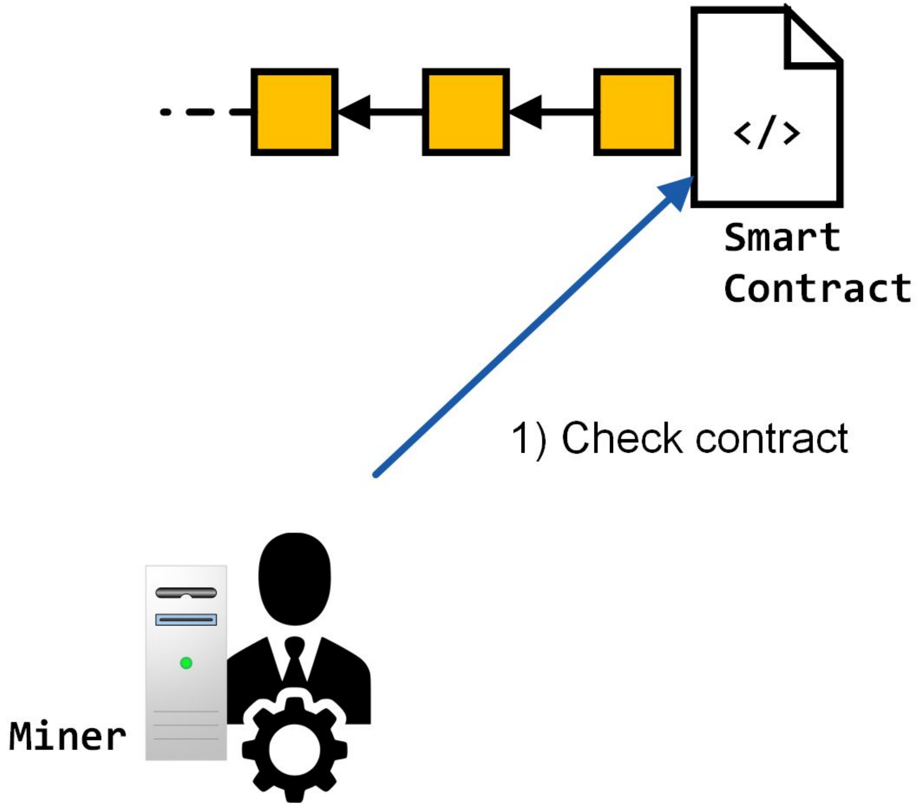
- Some miners preferred to connect to “public” and **“trusted”** P2Pool nodes as workers.

- Contradiction to P2Pool idea?
  - Does not contribute to censorship resistance

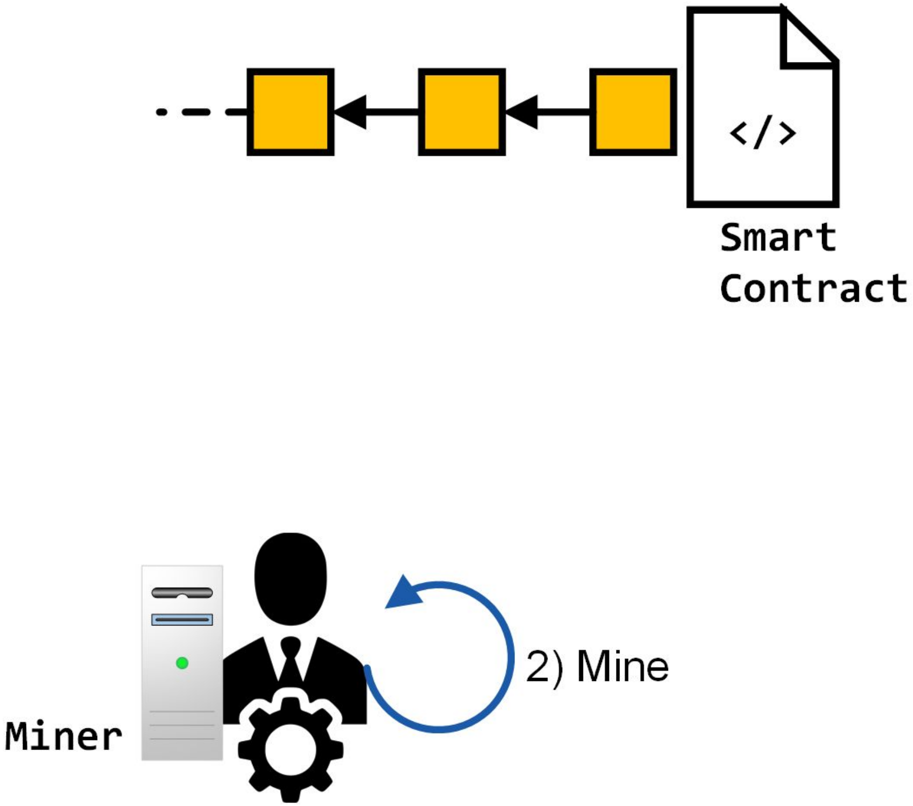
SmartPool (Luu et al., 2017)

Uses a smart contract to verify shares (probabilistically) and calculate reward distribution

SmartPool contd.



SmartPool contd.



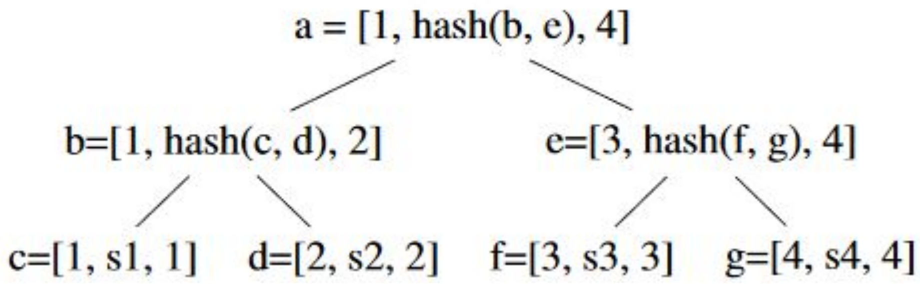
Augmented Merkle Tree

Leaf format:
(min, hash, max)

- min - minimum counter value in this branch
- max - maximum counter value in right branch

Counter value - e.g. timestamp

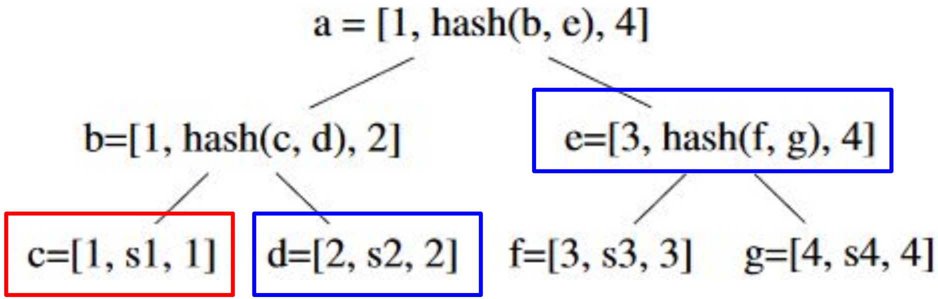
<u>Prevents duplicate share submission!</u>



For more details & proofs, see:
Luu, Loi, et al. "Smartpool: Practical decentralized pooled mining." *26th USENIX Security Symposium*, 2017.

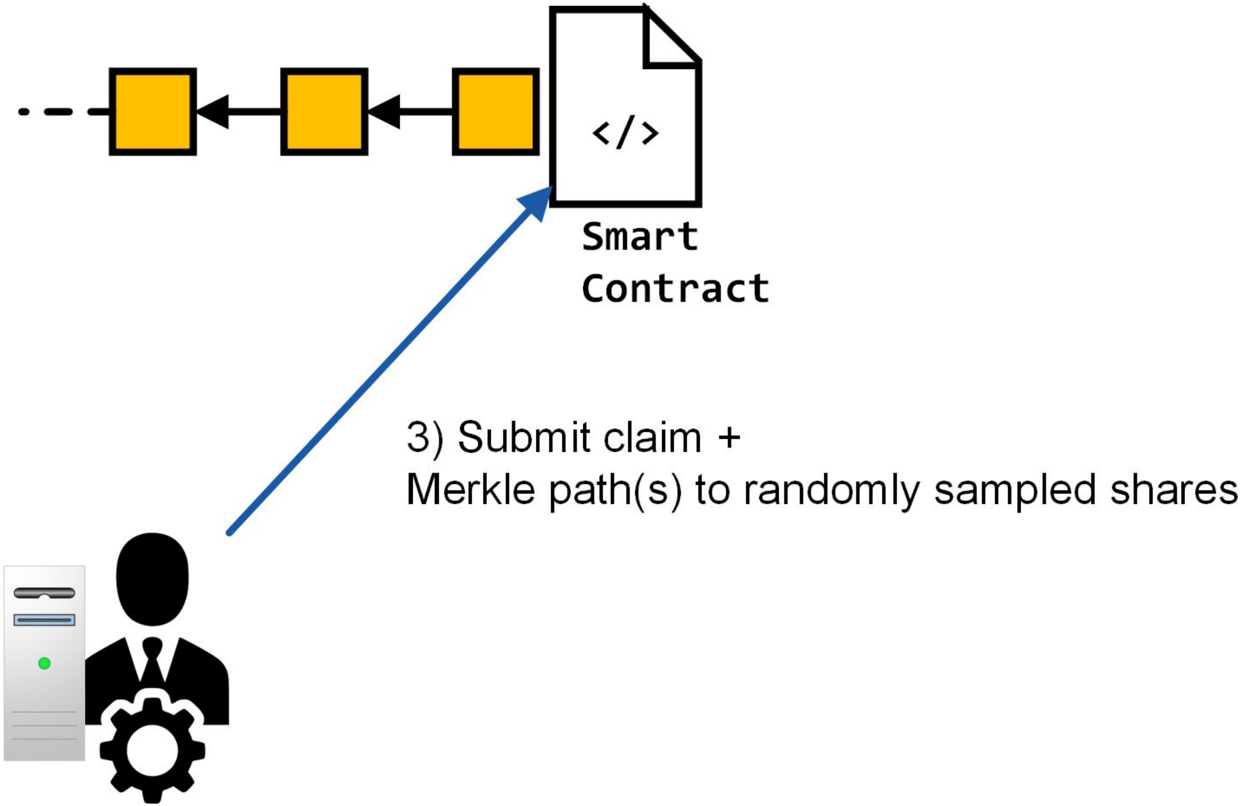
Probabilistic Verification

- Prove only small number (n) of shares.
- Randomly sampled
- If 1 share wrong → entire claim invalid
- E.g. 1 proof enough to disincentivize misbehavior (risk > gain!)

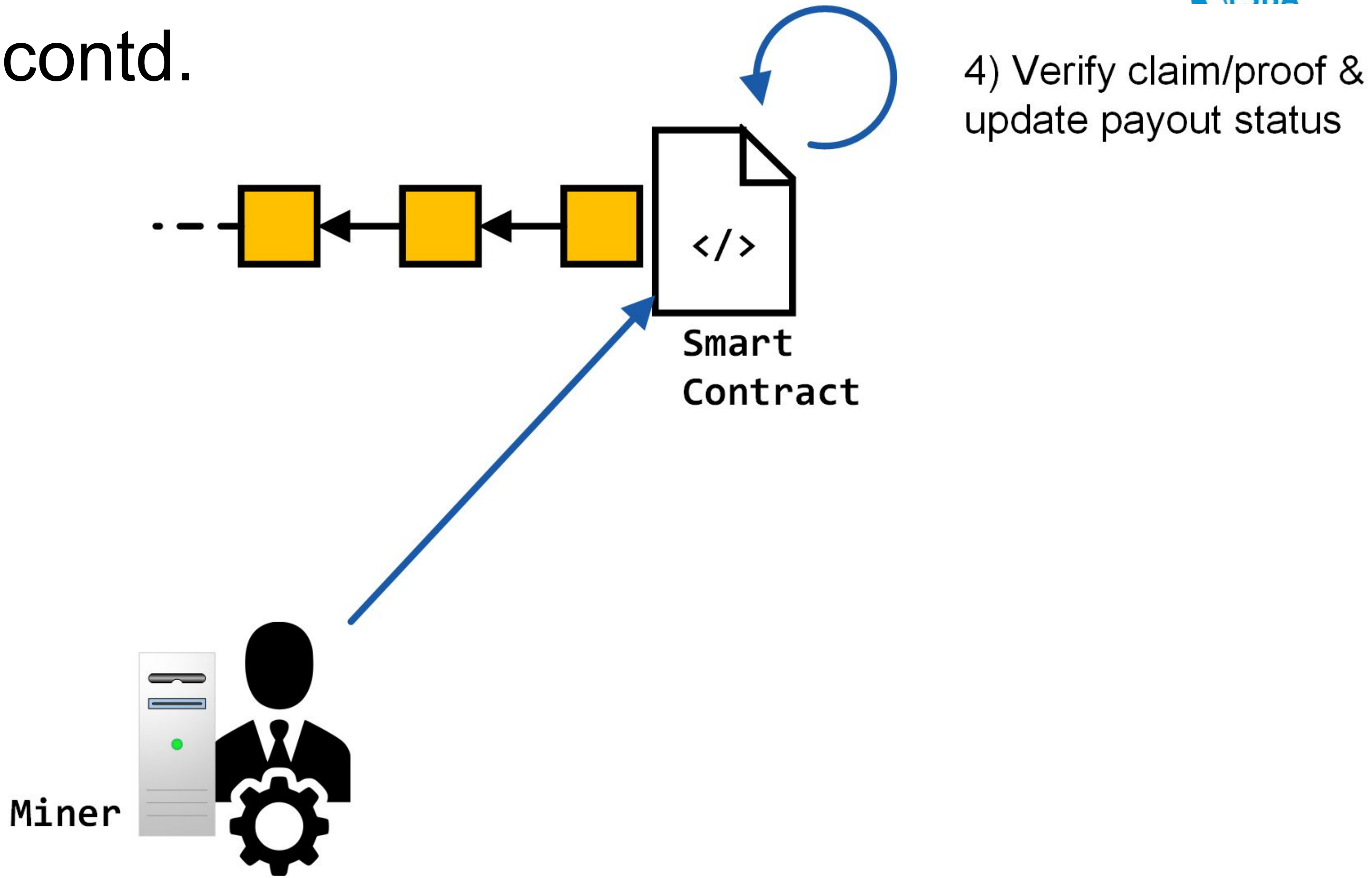


For more details & proofs, see:
Luu, Loi, et al. "Smartpool: Practical decentralized pooled mining." *26th USENIX Security Symposium*, 2017.

SmartPool contd.



SmartPool contd.



SmartPool (Luu et al., 2017)

Agreement:

- via on-chain smart contract
- miner claim payment via on-chain TX

Difficulty: selected by each miner

Requirements:

- **smart contract** (verification of PoW and Merkle inclusion proofs)
- Bias resistant random seed

Practical Challenges

- **PPLNS difficult to implement** (if possible at all)
    - Needs timely information vs. irregular claim/proof submissions
- **Payout delays possible** if network is congested
    - e.g. many small miners in pool
- **Applicability to Bitcoin???**
    - Smart contract must run on another chain
    - Payouts handled cross-chain?

Security Issues

- **Smart contract cannot verify transaction validity**
  - Submitting entire block to SC → too expensive
  - SC will accept an invalid TX as "valid"
  - Malicious miner can execute block withholding attacks **undetected**!

- **Fork handling not discussed**
  - Claims submitted irregular → Expensive to check if references main-chain

- **Bribing attacks** via mining contract!
  - Even works cross-chain → undetectable in Bitcoin!

Outlook

Combine P2Pool with SmartPool verification (Future work)?

- P2Pool miners broadcast share claims + proofs
- Other miners validate & update payout structure locally
- Benefits:
  - Allows vardiff
  - Less overhead?
  - ….
- Challenge: compatibility with PPLNS

Centralized mining pools allow miners to select transactions

→ BetterHash (Corallo et al, 2019)

Questions?

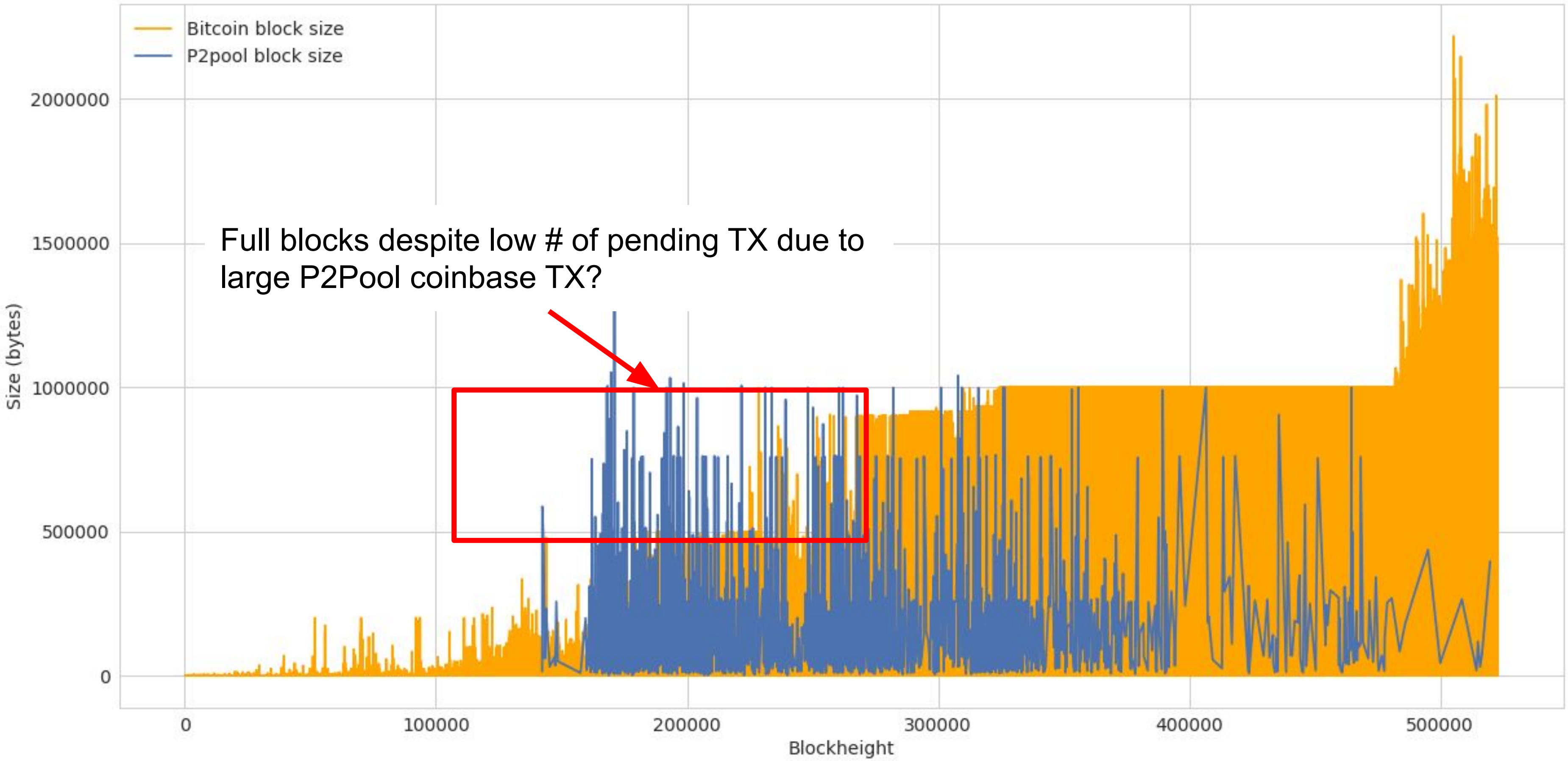
Alexei Zamyatin

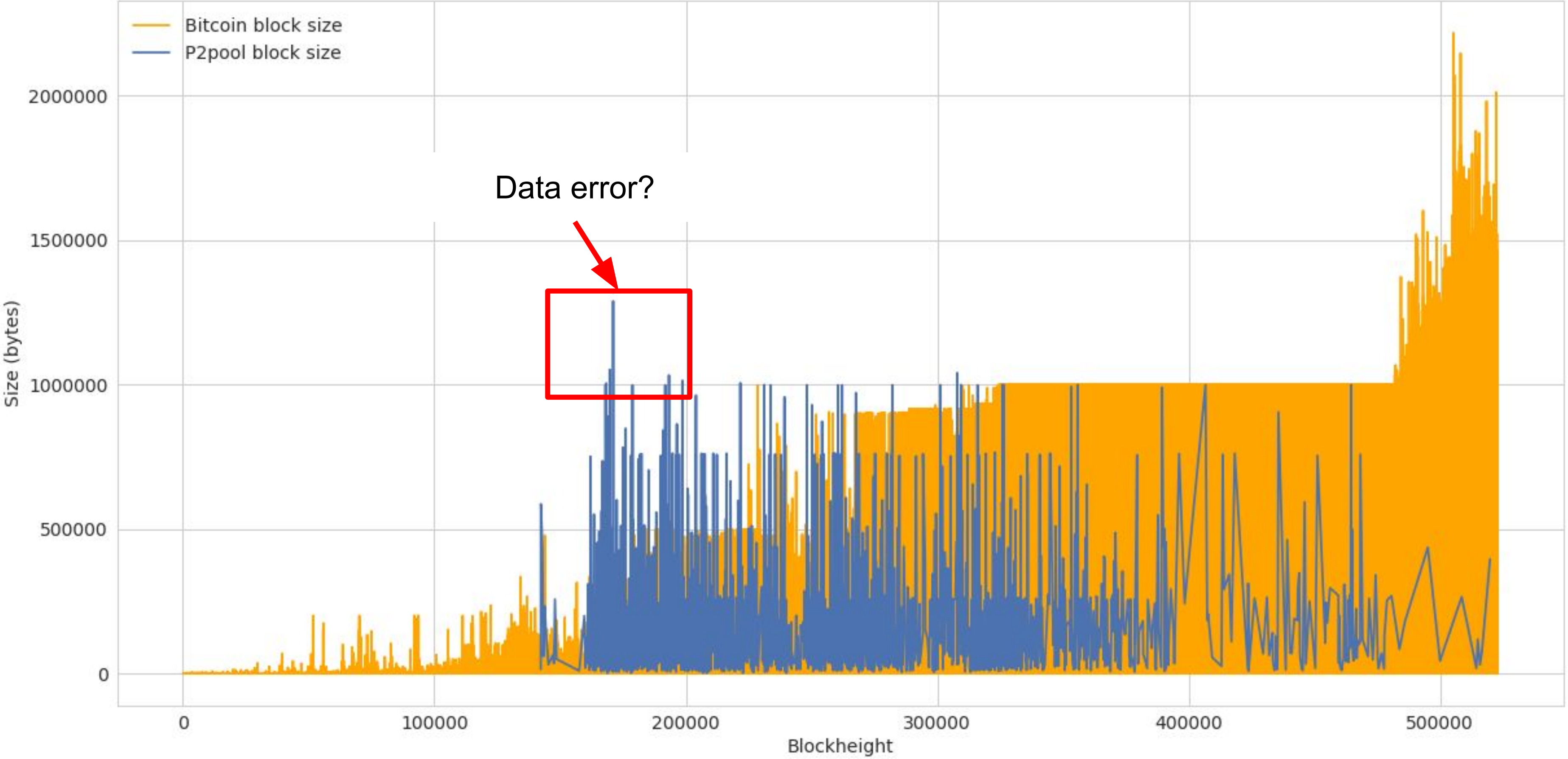
a.zamyatin@imperial.ac.uk

2F5F E92D CDAC 15B0 84A6 9FE9 9018 A958 5485 B999

@alexeiZamyatin

Appendix


Bitcoin block size
P2pool block size
Full blocks despite low # of pending TX due to large P2Pool coinbase TX?
Size (bytes)
2000000
1500000
1000000
500000
0
0
100000
200000
300000
400000
500000
Blockheight


Bitcoin block size
P2pool block size
Data error?
Size (bytes)
0
500000
1000000
1500000
2000000
Blockheight
0
100000
200000
300000
400000
500000

Temporary Dishonest Majority - Model (MDP)

Imperial College London

SBA Research

State $\times$ Action	Resulting State	Probability	Reward (in block reward)[‡] (attacker, honest, P2Pool)
$(l_a, l_h, \cdot)$, *adopt*	$(1, 0, \textit{irrelevant})$ $(0, 1, \textit{irrelevant})$	α β	$(0, l_h \cdot \beta, l_h \cdot \phi)$
$(l_a, l_h, \cdot)$, *override*	$(l_a - l_h, 0, \textit{irrelevant})$ $(l_a - l_h - 1, 1, \textit{relevant})$	α $\beta + \phi$	$(l_h + 1), 0, 0$
$(l_a, l_h, \textit{irrelevant})$, *wait* $(l_a, l_h, \textit{relevant})$, *wait*	$(l_a + 1, l_h, \textit{irrelevant})$ $(l_a, l_h + 1, \textit{relevant})$	α $\beta + \phi$	$(0, 0, 0)$ $(0, 0, 0)$
$(l_a, l_h, \textit{irrelevant})$, *wait* $(l_a, l_h, \textit{relevant})$, *match*	$(l_a + 1, l_h, \textit{active})$ $(l_a - l_h, 1, \textit{relevant})$ $(l_a, l_h + 1, \textit{relevant})$	α $\gamma \cdot \beta + \phi$ $(1 - \gamma) \cdot (\beta + \phi)$	$(0, 0, 0)$ $\left(l_h \frac{\alpha}{\alpha+\phi}, 0, l_h \frac{\phi}{\alpha+\phi})\right)$ $(0, 0, 0)$
$(l_a, l_h, \cdot)$, exit[†]	`exit`	1	$\left(l_a \frac{\alpha}{\alpha+\phi}, 0, l_a \frac{\phi}{\alpha+\phi})\right)$

[†]Only feasible if $l_a > l_h$ (and $l_h \geq k$ for double spending)

l_a - attacker chain length
l_h - honest chain length
α - attacker hash rate
ϕ - P2Pool hash rate
β - honest non-P2Pool hash rate
$(\alpha + \phi + \beta = 1)$
γ - network connectivity of attacker (probability that honest miners accept attacker's block)

What does this mean?

- Attacker can increase chance of winning a race in case of a “Match”
  - Normal SM: success of “Match” depends on network connectivity only

    $$(1-\gamma)\cdot(\beta+\phi)$$

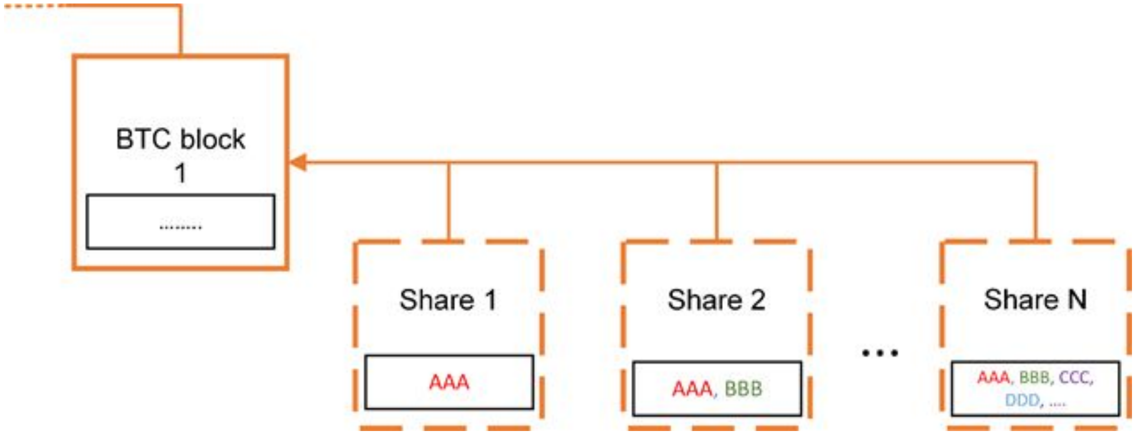
  - P2Pool SM: additional success chances, depending on P2Pool hash rate

    $$\gamma\cdot\beta+\phi$$

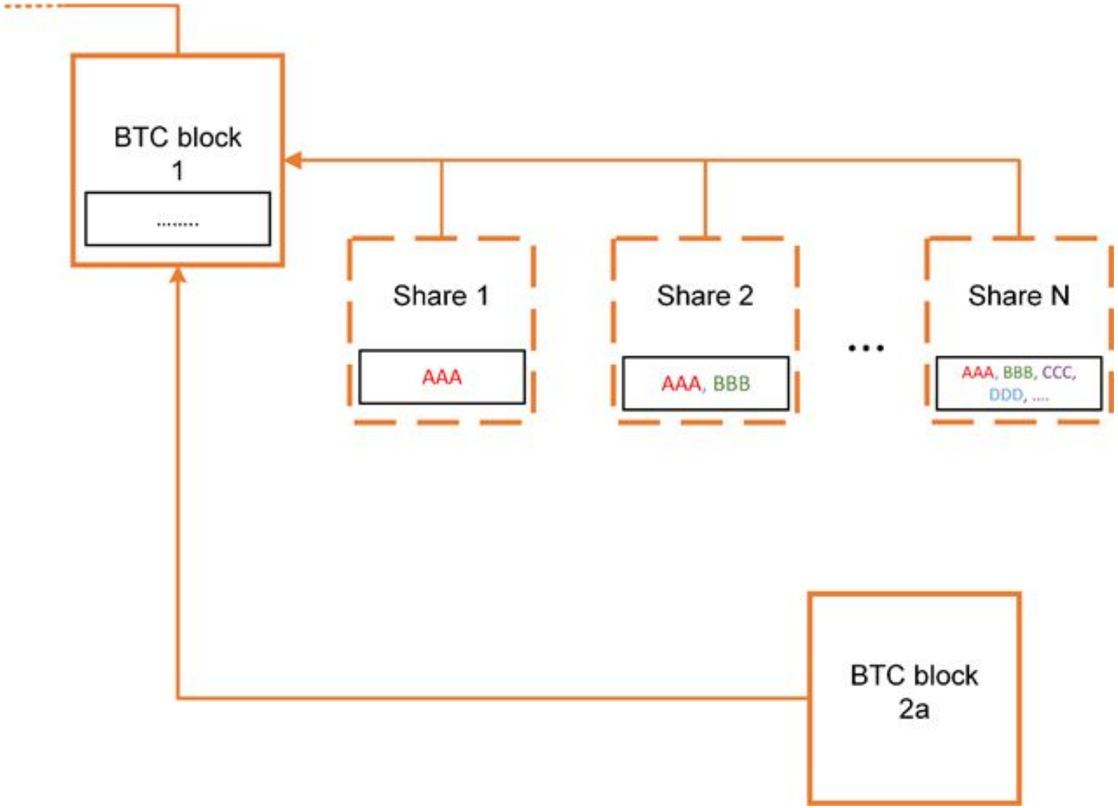
P2Pool Incentives

- P2Pool blocks: **higher value** for P2Pool miners!
- Bitcoin's security model: based on "same value" assumption
- Large P2Pool (e.g. > 50% of hash rate) may be incentivized to fork other blocks

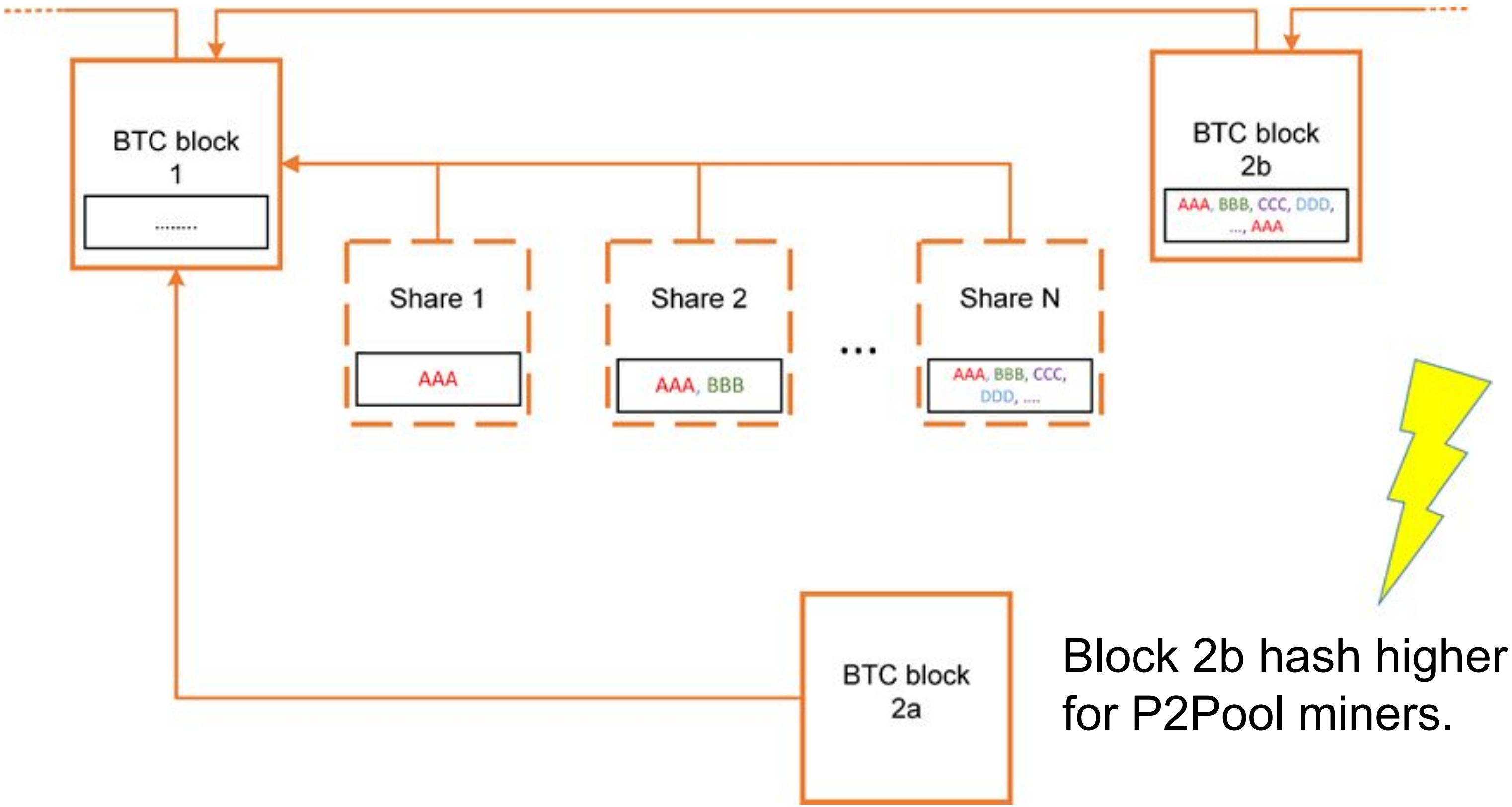
P2Pool Incentives



P2Pool Incentives



P2Pool Incentive Attacks



Block 2b hash higher value than 2a for P2Pool miners.