

Countering Block Withholding Attack Efficiently

2nd Workshop on Cryptocurrencies and Blockchains for Distributed Systems
29th of April 2019, Paris, France

Suhyeon Lee¹² (Speaker) and Seunjoo Kim ¹

¹ Korea University

² Agency for Defense Development
{orion-alpha, skim71}@korea.ac.kr



KOREA
UNIVERSITY

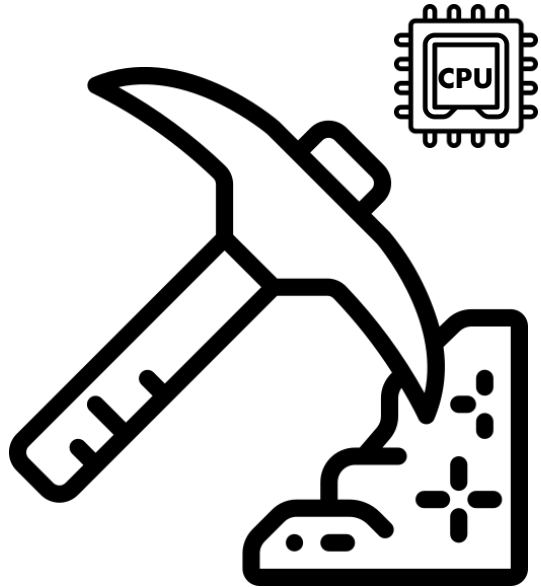


국 방 과 학 연 구 소
Agency for Defense Development

Index

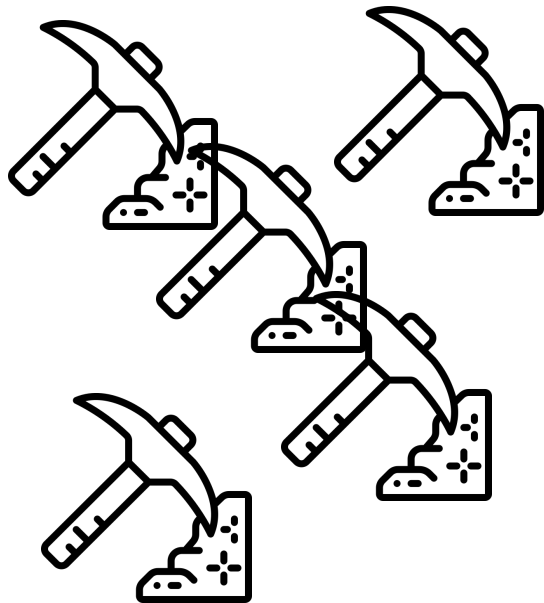
- Context in PoW
- Block Withholding Attack
- Our method
- Discussion
- Conclusion

Proof-of-Work (PoW)



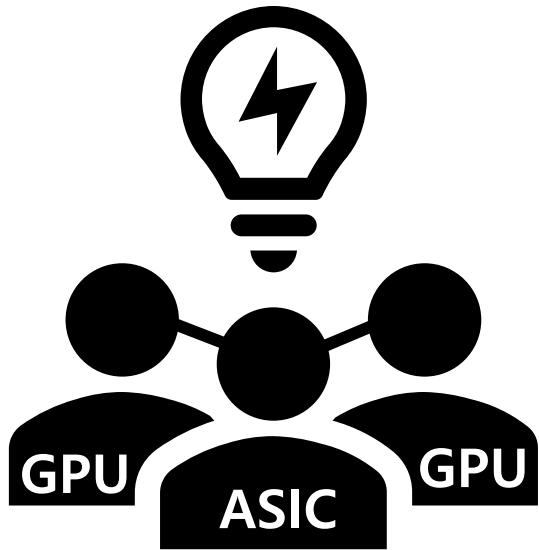
- PoW in *the white paper*¹
- Proof came from CPU power
- Majority attack – Double spending

Proof-of-Work (PoW)



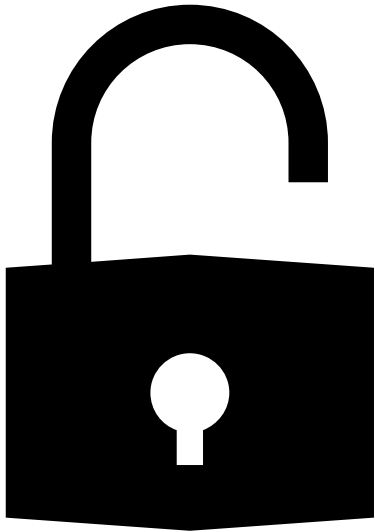
- PoW in *the white paper*¹
 - Proof came from CPU power
 - Majority attack – Double spending
 - "The war of all miners against all miners"

Proof-of-Work (PoW)



- PoW in *the real world*
 - Miners find efficient ways
 - GPU and ASIC mining
 - Pooled mining is a dominant approach

Attacks in PoW



- Selfish mining
- ***Block Withholding (BWH) Attack***
- Coin hopping

FPoW: 0000000486

PPoW: 0000821982

Submit



What is BWH attack?

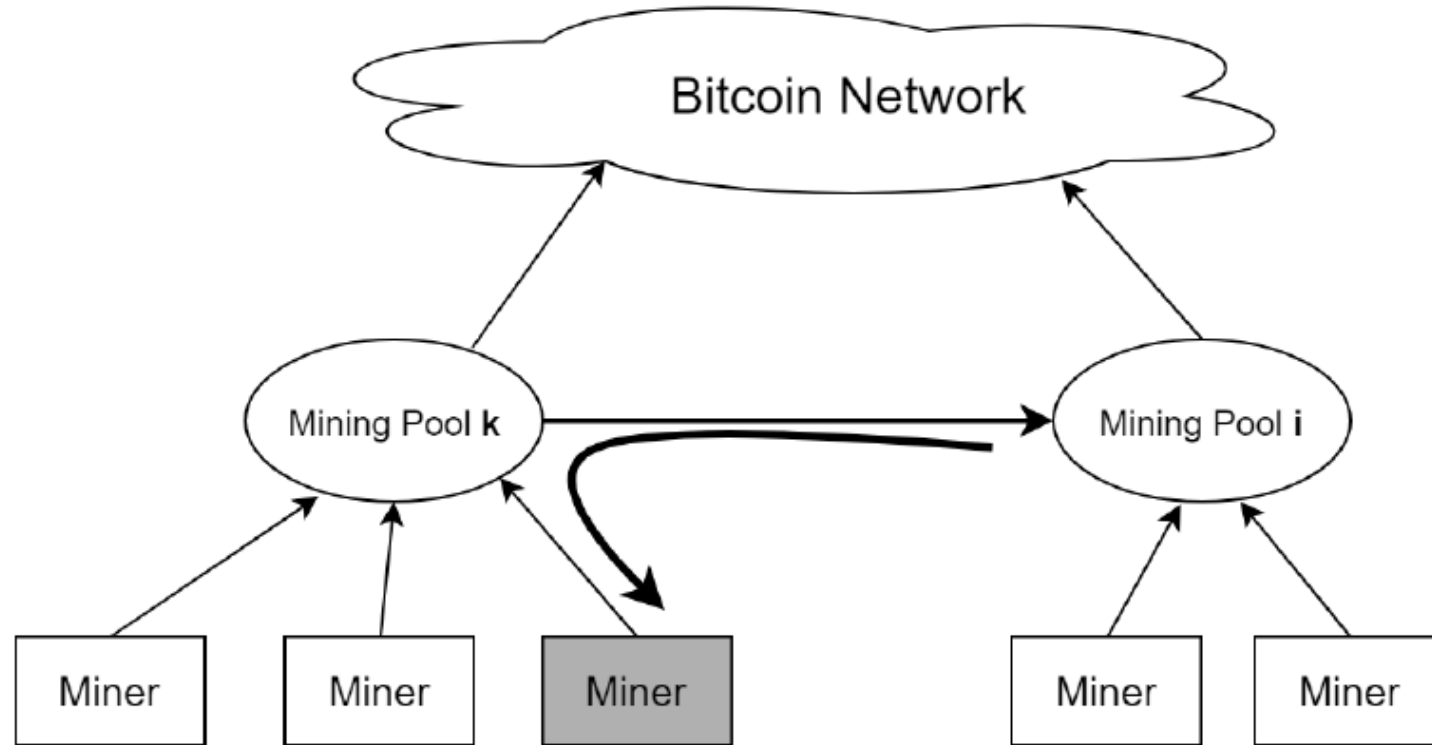
~~FPoW: 0000000486~~

PPoW: 0000821982

Submit






What is BWH attack?

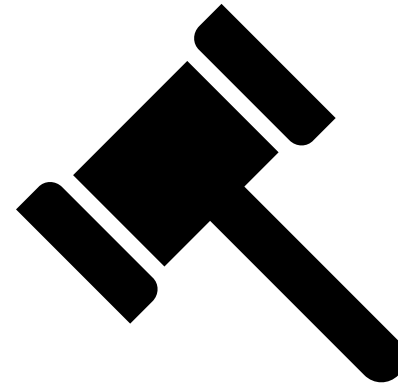


What is BWH attack?

Recent study in BWH countermeasure

Property	 Two-phase PoW	 Pool entrance fee	 FPoW centric reward policy
No loss	O	X	O
Compatibility	X	O	O
Fairness	O	O	X

So we still need a practical solution...



Our proposal : Detect & Punish

Given information for mining task



- Version
- PrevBlockHash
- **MerkleRootHash** ←
- Timestamp
- Bits
- (Nonce)
- Transactions
 - **Coinbase TX**



Our proposal



1. Detection phase

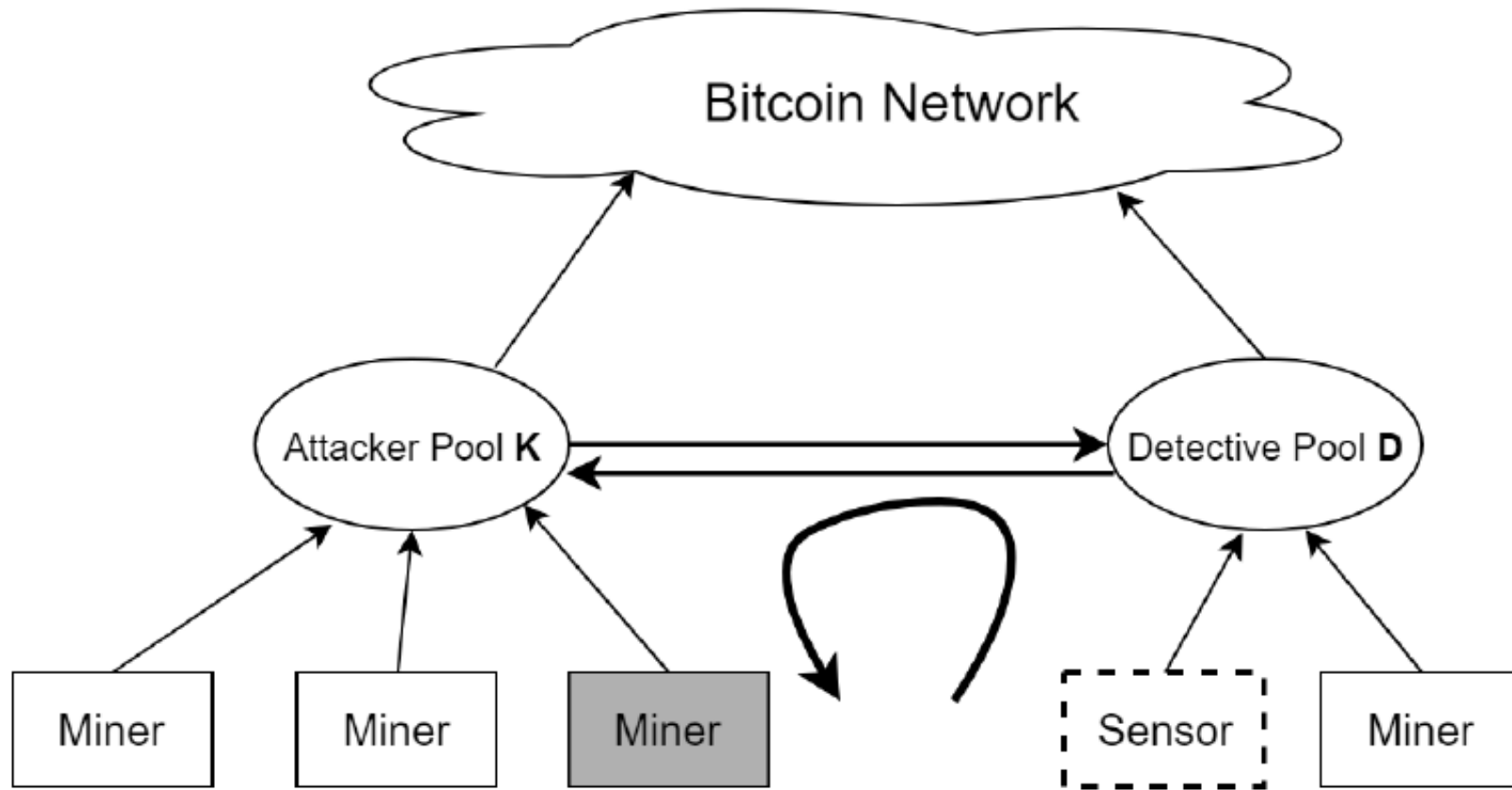
- Put sensor miners
- Check mining task includes specific *coinbase*

Our proposal







2. Punishment phase

- Reducing the reward for the infiltration pool
- No blocking because of reentrance

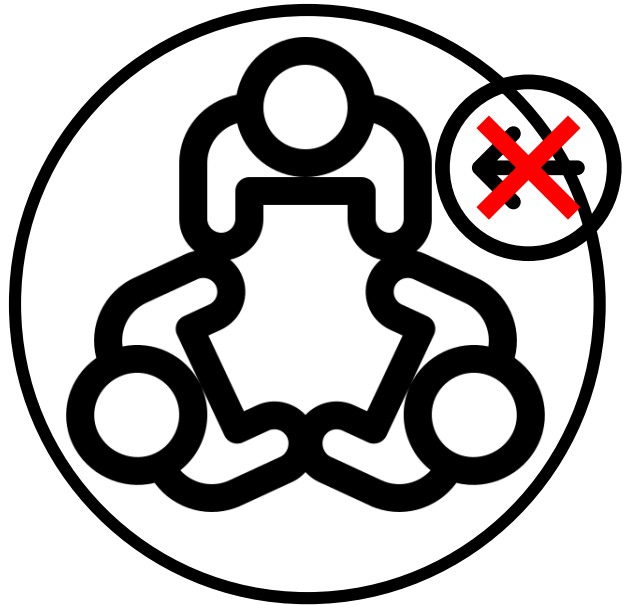


Our proposal : Detect & Punish

Discussion

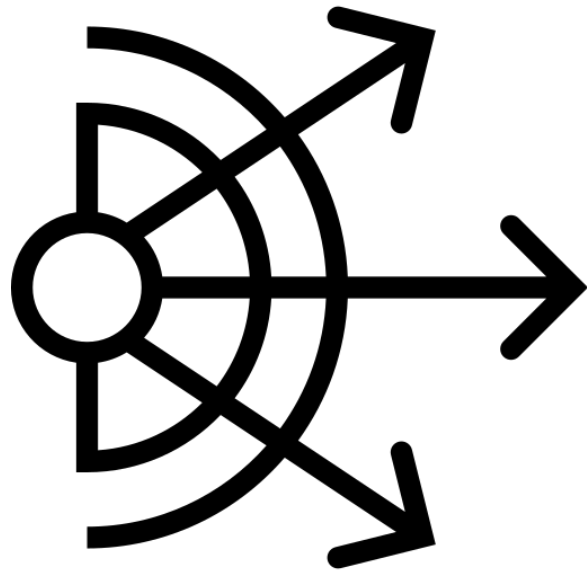
Property	 Our method	 Two-phase PoW	 Pool entrance fee	 FPoW centric reward policy
No loss	○	○	X	○
Compatibility	○	X	○	○
Fairness	○	○	○	X

Scenarios against our method



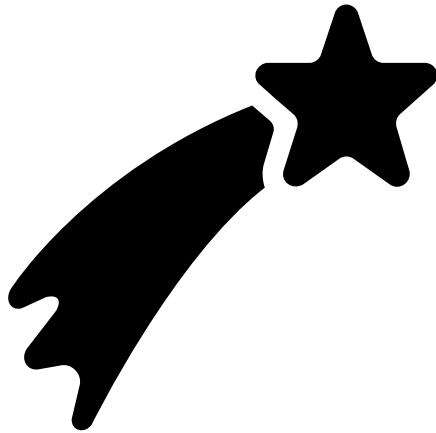
- **Closed pools**
Only approved miners can join
- **Multiple infiltration**

Scenarios against our method



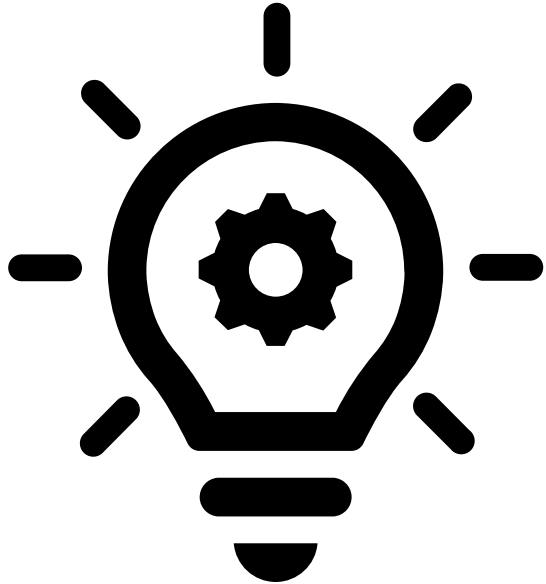
- **Closed pools**
Only approved miners can join
- **Multiple infiltration**
Sensor coverage can be poor

Future Work



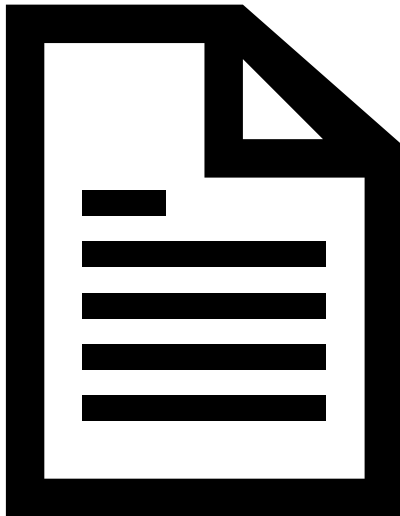
- Information share in mining pools should be studied more
- ~~BWH attack~~
- Selfish mining ?
- Coin hopping ?

Conclusion



- BWH attack can be detected and punished efficiently
- Our method meets three conditions to be a good countermeasure

Reference



1. Nakamoto. Bitcoin: A peer-to-peer electronic cash system.
2. Ittay Eyal. The miner's dilemma. In Security and Privacy (SP), 2015 IEEE Symposium on, pages 89–103. IEEE, 2015.
3. Meni Rosenfeld. Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980, 2011.
4. Ittay Eyal and Emin Gun Sirer. How to "disincentivize large bitcoin mining pools. Blog post: <http://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools>, 2014.
5. Samiran Bag, Sushmita Ruj, and Kouichi Sakurai. Bitcoin block withholding attack: Analysis and mitigation. IEEE Transactions on Information Forensics and Security, 12(8):1967–1978, 2017.
6. Loi Luu, Ratul Saha, Inian Parameshwaran, Prateek Saxena, and Aquinas Hobor. On power splitting games in distributed computation: The case of bitcoin pooled mining. In Computer Security Foundations Symposium (CSF), 2015 IEEE 28th, pages 397–411. IEEE, 2015.

Thank you :)

Suhyeon Lee

Ph.D student in Korea Univerisy

Researcher in Agency for Defense Development

orion-alpha@korea.ac.kr



BACK UP SLIDES

What is BWH attack?

Total Computational Power = 1

Computational Power of Attacker = a

Computational Power of Victim = b

Relative Infiltration Power = t

Infiltration Computational Power = ta

$$\text{Reward} = \frac{(1-t)a}{1-ta} + \frac{b}{1-ta} \frac{ta}{b+ta}$$