Power Adjusting and Bribery Racing: Novel Mining Attacks in the Bitcoin System

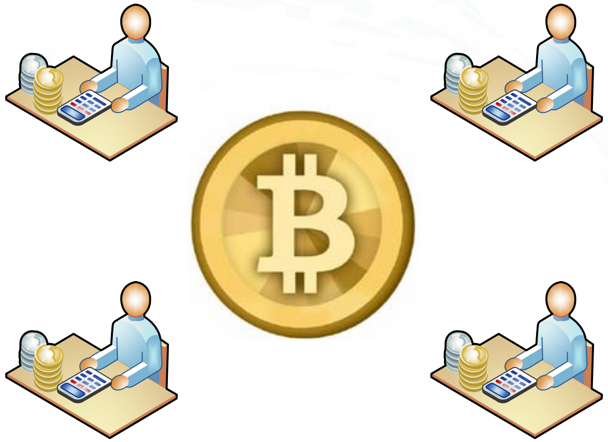
Shang Gao, Zecheng Li, Zhe Peng, and Bin Xiao
The Hong Kong Polytechnic University

Nov 12, 2019

Outline

- Bitcoin Overview
- Mining Attacks
- Power Adjusting Withholding
- Bribery Selfish Mining
- Discussion
- Conclusion

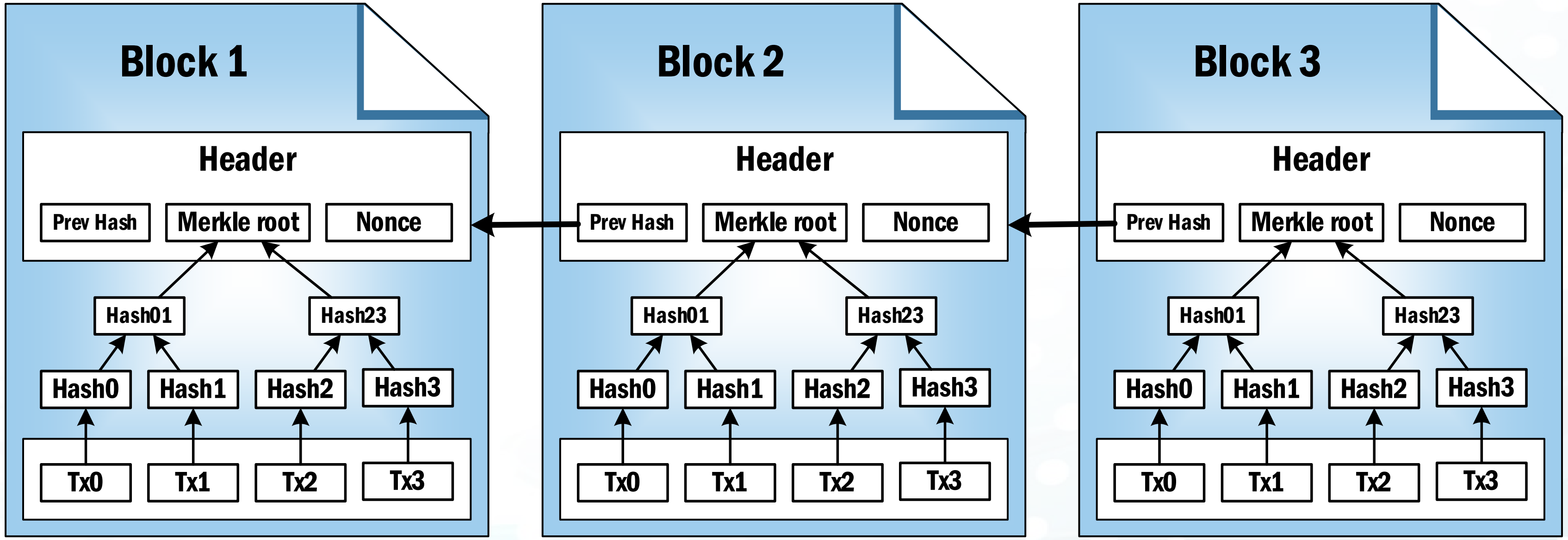
Bitcoin: Overview



- Blockchain based cryptocurrency
  - Decentralized ledger
- Price: more than 10000 USD in Aug, 2019.

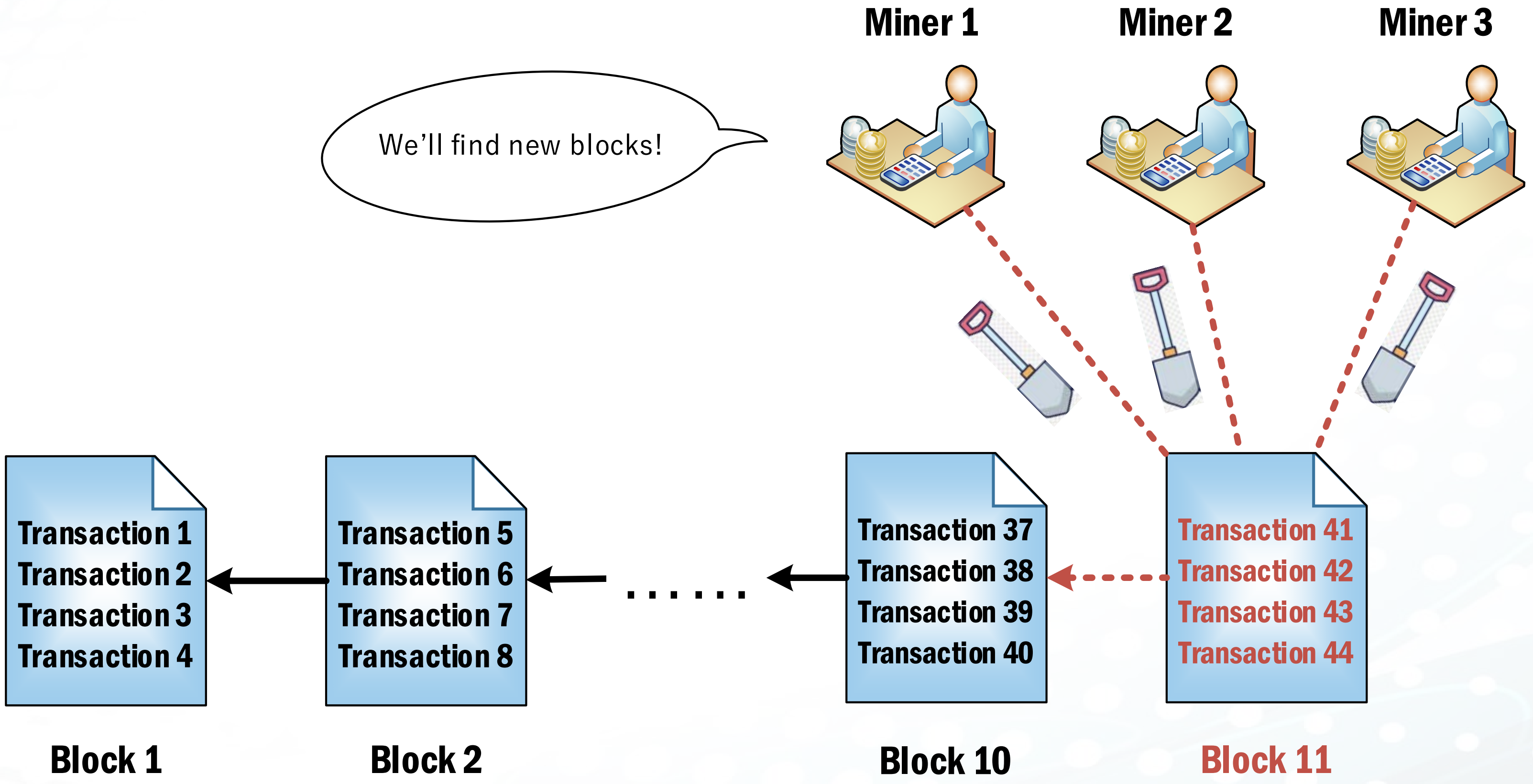
Bitcoin: Overview

- Participants: **miners.**
- New transaction records: recorded in **blocks.**
- Block: header and body
  - Header: previous block header hash, Merkle root, nonce, ...
  - Body: transaction records
- Ledger: **blockchain.**



Bitcoin: Mining Process

- **Mining process:** miners adding new blocks into the blockchain.

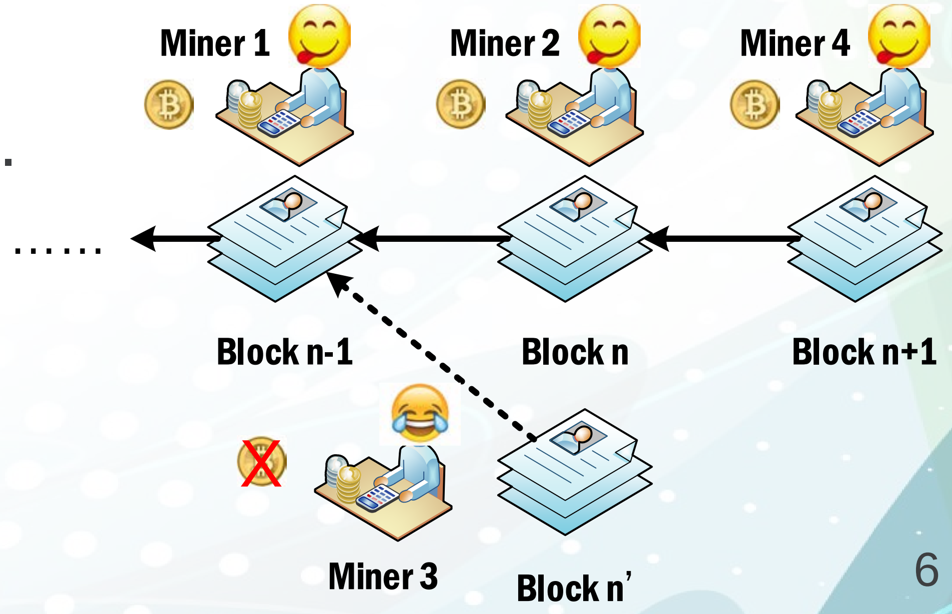


Bitcoin: Mining Process

- However, finding a new block is not easy.
  - Finding a proper **nonce** in the header that satisfies the difficulty constraint:

$$\boldsymbol{SHA256}\left(\boldsymbol{SHA256}(\boldsymbol{Block.Header})\right) < \boldsymbol{D}.$$

  - Need to enumerate all possible value.
- A proper nonce is called proof of work (**PoW**)
- The firstly discovered miner will be rewarded (12.5 BTC).

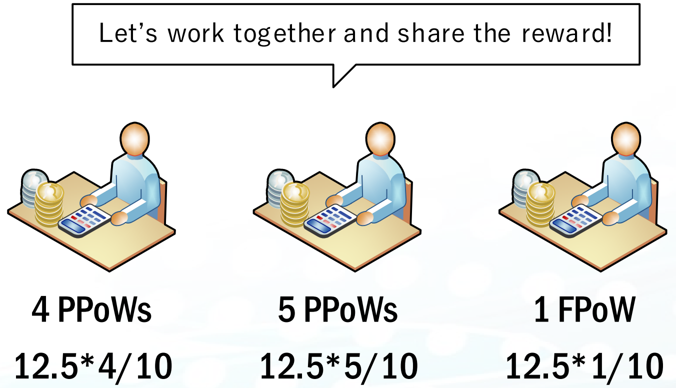


- Multiple miners find blocks simultaneously: **fork**.
  - A miner can choose which branch it works on.
  - The longest branch is selected as the main chain.
  - Only blocks on the main chain can be rewarded.

Bitcoin: Mining Pool

- To reduce the reward variance, miners can work together as **mining pools**.
  - Reward can be shared based on each miner's contribution.
  - Mining pool will set a less difficult constraint D' ($D' > D$).
  - A nonce that makes $D < Hash(header) < D'$ is called **PPoW** (partial proof of work).
  - A nonce that makes $Hash(header) < D < D'$ is called **FPoW** (full proof of work).
  - FPoWs and PPoWs are called shares. Number of shares is proportional to mining power.
  - A pool miner's reward is calculated by:

$$Miner's\ Reward = Pool's\ Reward * \frac{Number\ of\ miner's\ shares}{Number\ of\ total\ shares} = Pool's\ Reward * \frac{Miner's\ mining\ power}{Pool's\ mining\ power}$$



Outline

- Bitcoin Overview
- Mining Attacks
- Power Adjusting Withholding
- Bribery Selfish Mining
- Discussion
- Conclusion

Mining Attacks: Overview

- Attackers can increase their reward of mining when deviating from honest mining strategies.
  - Selfish mining [FC'14]
  - Block withholding [CSF'15, Oakland'15]
  - Fork after withholding [CCS'17]
  - Bribery attacks [FC'16]

[FC'14] Ittay Eyal and Emin Gun Sirer. 2014. Majority is not Enough: Bitcoin Mining is Vulnerable. In *Proc. of the International Conference on Financial Cryptography and Data Security (FC).*
[Oakland'15] Ittay Eyal. 2015. The Miner's Dilemma. In *Proc. of the IEEE Symposium onSecurity and Privacy (Oakland).*
[CSF'15] Loi Luu, Ratul Saha, Inian Parameshwaran, Prateek Saxena, and Aquinas Hobor. 2015. On Power Splitting Games in Distributed Computation: The Case of Bitcoin Pooled Mining. In *Proc. of the IEEE Computer Security Foundations Symposium (CSF).*
[CCS'17] Yujin Kwon, Dohyun Kim, Yunmok Son, Eugene Vasserman, and Yongdae Kim. 2017. Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin. In *Proc. of the ACM Conference on Computer & Communications Security (CCS).*
[FC'16] Joseph Bonneau. 2016. Why Buy When You Can Rent?. In *Proc. of the International Conference on Financial Cryptography and Data Security (FC).*

Mining Attacks: Overview

- Attackers can increase mining when deviating from honest mining strategies.
  - Selfish mining [FC’14]
  - Block withholding [CSF’15, O

These attacks also work for other PoW based cryptocurrencies!

Cryptography and Data Security (FC).

[Oakland’15] Ittay Eyal. 2015. The Miner’s Dilemma. In *Proc. of the IEEE Symposium onSecurity and Privacy (Oakland).*

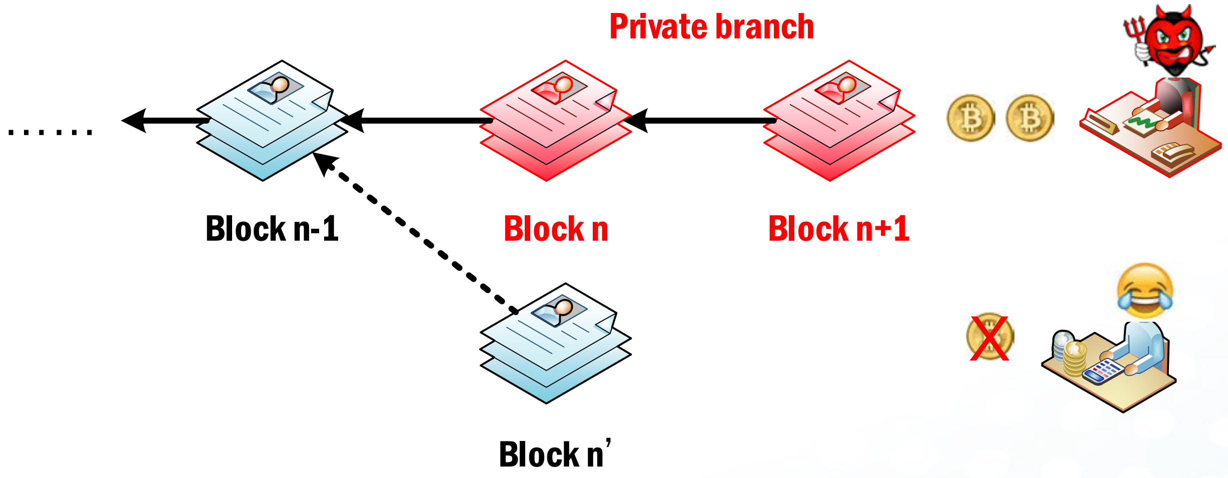
[CSF’15] Loi Luu, Ratul Saha, Inian Parameshwaran, Prateek Saxena, and Aquinas Hobor. 2015. On Power Splitting Games in Distributed Computation: The Case of Bitcoin Pooled Mining. In *Proc. of the IEEE Computer Security Foundations Symposium (CSF).*

[CCS’17] Yujin Kwon, Dohyun Kim, Yunmok Son, Eugene Vasserman, and Yongdae Kim. 2017. Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin. In *Proc. of the ACM Conference on Computer & Communications Security (CCS).*

[FC’16] Joseph Bonneau. 2016. Why Buy When You Can Rent?. In *Proc. of the International Conference on Financial Cryptography and Data Security (FC).*

Mining Attacks: Selfish Mining

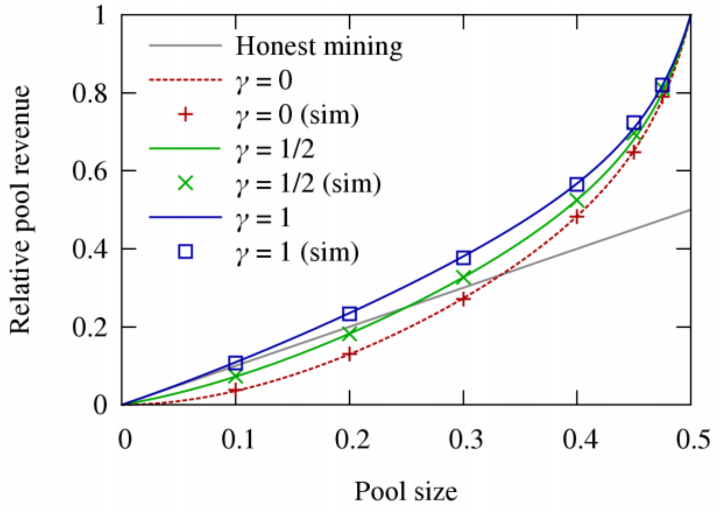
- An attacker will not publish the discovered block.
  - Continue mining on the discovered block as a **private branch**.
  - Publish the private chain when others discover a block (**cause a fork**).
  - Making others waste power when the private branch is selected as the main chain.



Mining Attacks: Selfish Mining

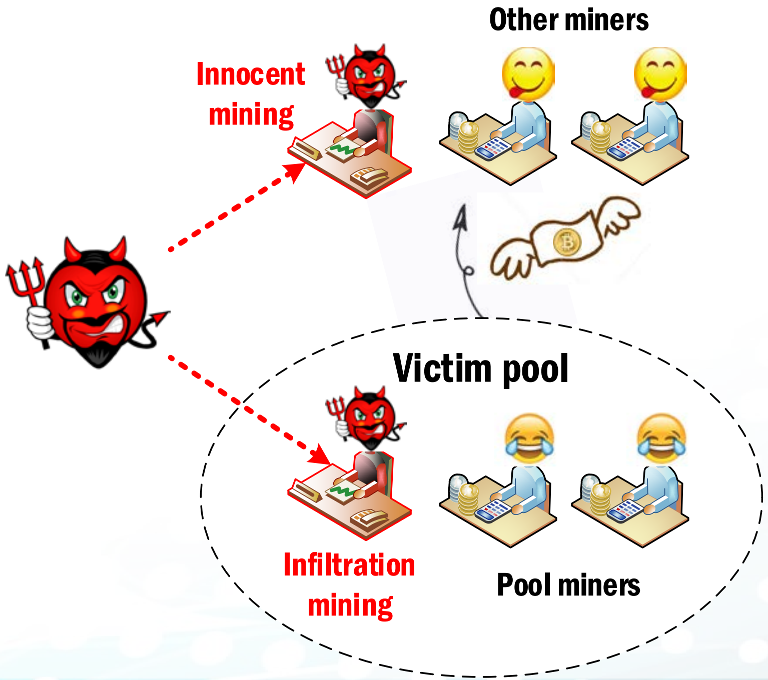
- An attacker will not publish the discovered block.
  - Continue mining on the discovered block as a **private branch**.
  - Publish the private chain when others discover a block (**cause a fork**).
  - Making others waste power when the private branch is selected as the main chain.

  - *Also may* ***lose*** *when the private branch is not selected as the main chain.*
  - *Need* ***1/3*** *mining power of the Bitcoin system to ensure a higher reward.*



Mining Attacks: Block Withholding (BWH)

- An attacker splits its power into innocent mining (mining solely) and infiltration mining (mining in pools).
  - Innocent mining: behaves exactly as honest mining.
  - Infiltration mining: only submits PPoWs (discards discovered FPoWs).
- Infiltration mining harms pools' reward, but makes other miners more profitable.



Mining Attacks: Block Withholding (BWH)

- BWH can be better than honest mining when splitting properly.
  - Regardless of mining power

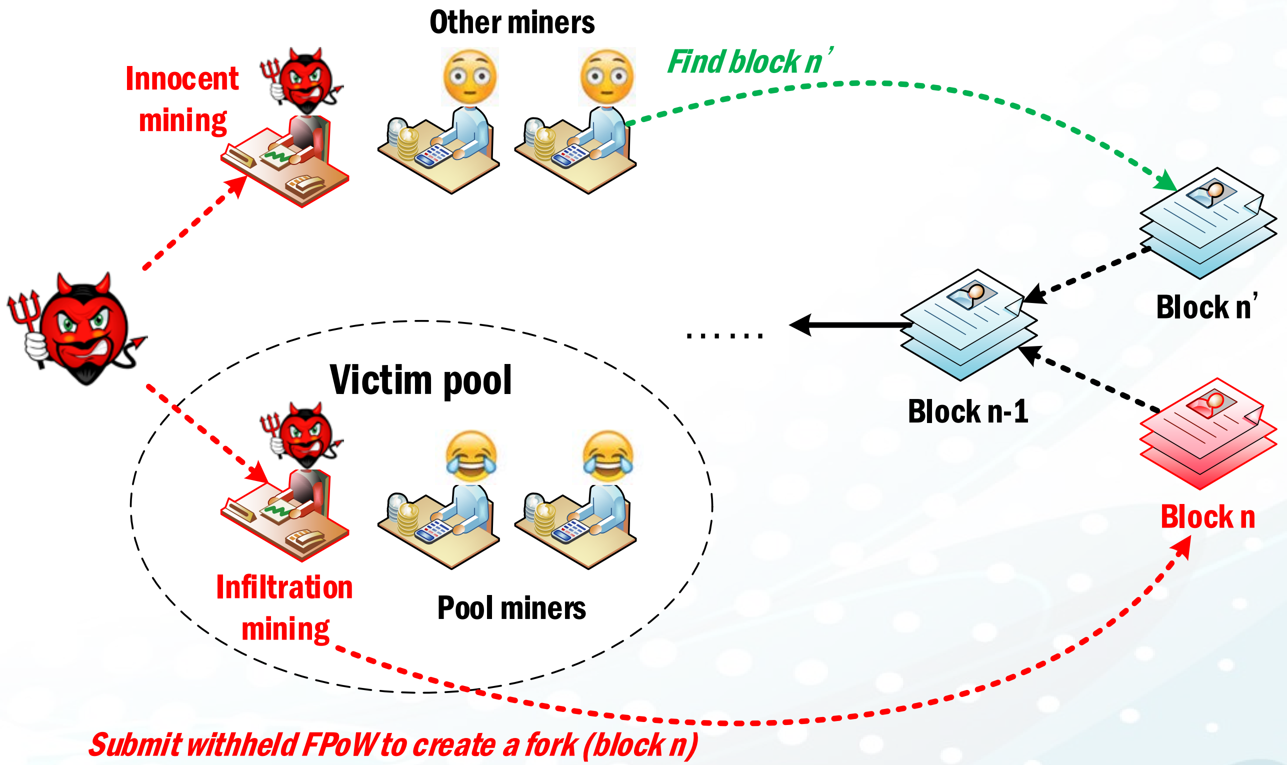
- Real-world BWH: Eligius pool lost 300 BTC in 2014.

- *It can be a "miner's dilemma" when two pools use BWH against each other.*
  - *Both pools will choose to attack under the Nash equilibrium.*
  - *Both pools always suffer from a loss due to BWH attacks (similar to the "prisoner's dilemma").*

Pool 2 \ Pool 1	no attack	attack
no attack	$(r_1 = 1, r_2 = 1)$	$(r_1 > 1, r_2 = \tilde{r}_2 < 1)$
attack	$(r_1 = \tilde{r}_1 < 1, r_2 > 1)$	$(\tilde{r}_1 < r_1 < 1, \tilde{r}_2 < r_2 < 1)$

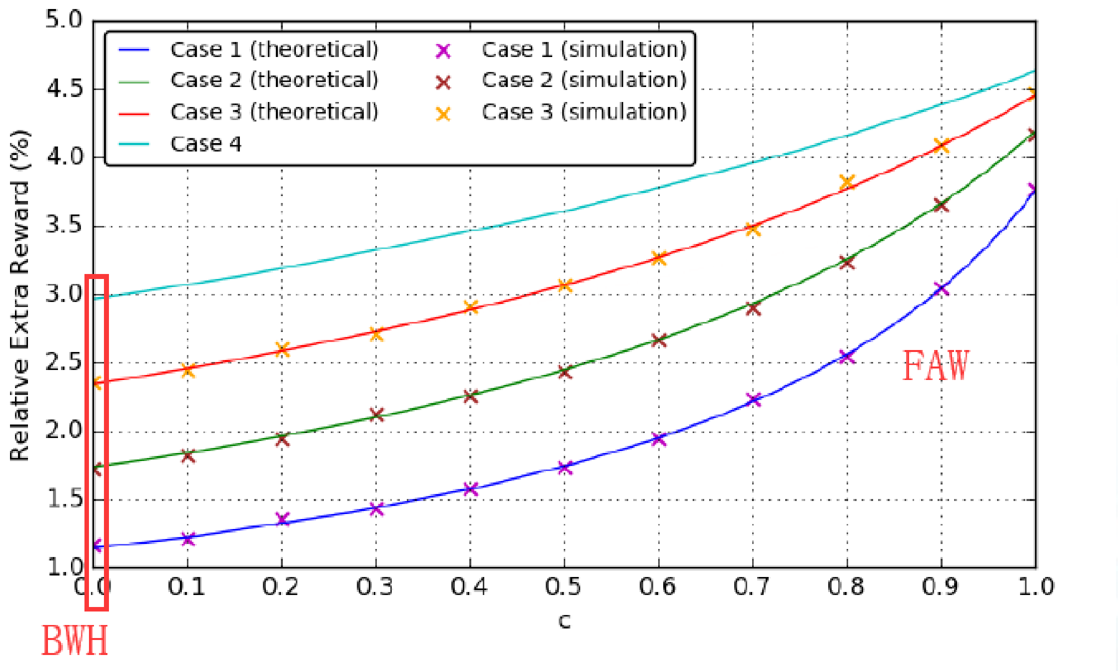
Mining Attacks: Fork After Withholding (FAW)

- FAW = BWH + Selfish Mining.
  - Splitting power into innocent mining and infiltration mining (as with BWH).
  - Infiltration mining withholds FPoWs, and *submits when others find blocks* (as with selfish mining).
    - Pool's reward: damaged by withholding FPoWs.
    - Other's reward: damaged by forks.



Mining Attacks: Fork After Withholding (FAW)

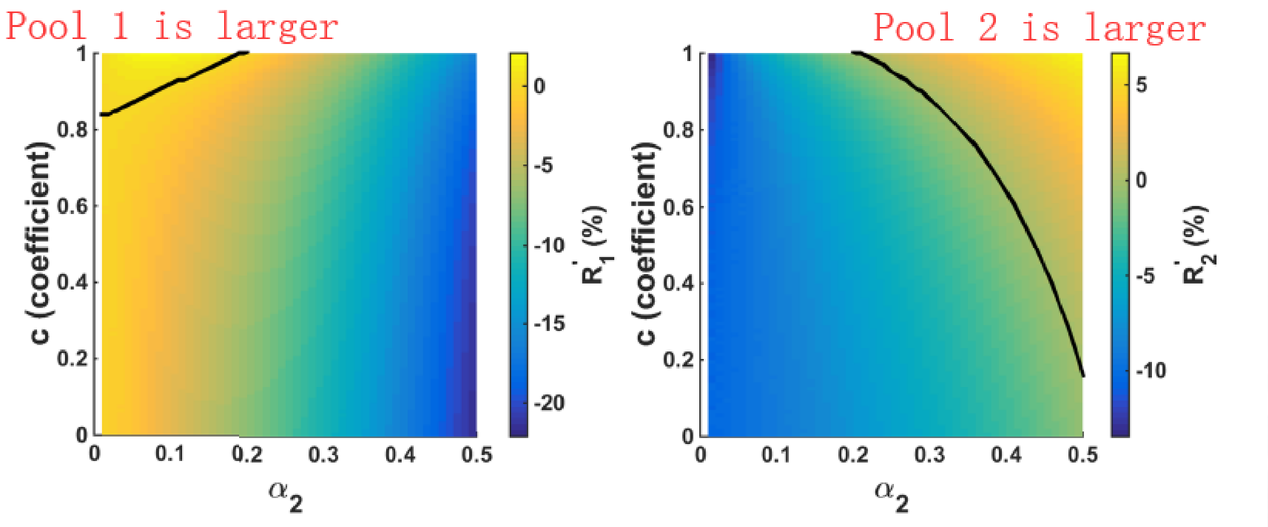
- Better than BWH.
  - The attacker can be rewarded from the fork (when attacker's branch becomes the main chain).
  - Lower bound is BWH (when attacker's branch is never selected).



Mining Attacks: Fork After Withholding (FAW)

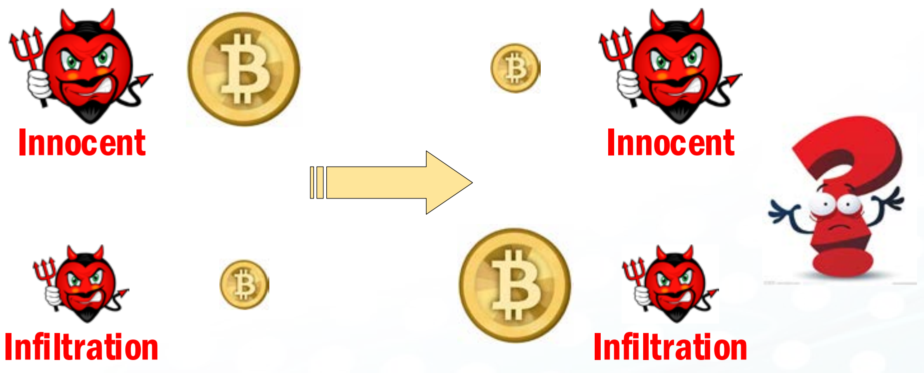
- Better than BWH.

- Break the dilemma: we may have a winner.
  - The smaller pool will always lose.
  - The larger pool may win.
  - Becoming a pool-size game.



Mining Attacks: Fork After Withholding (FAW)

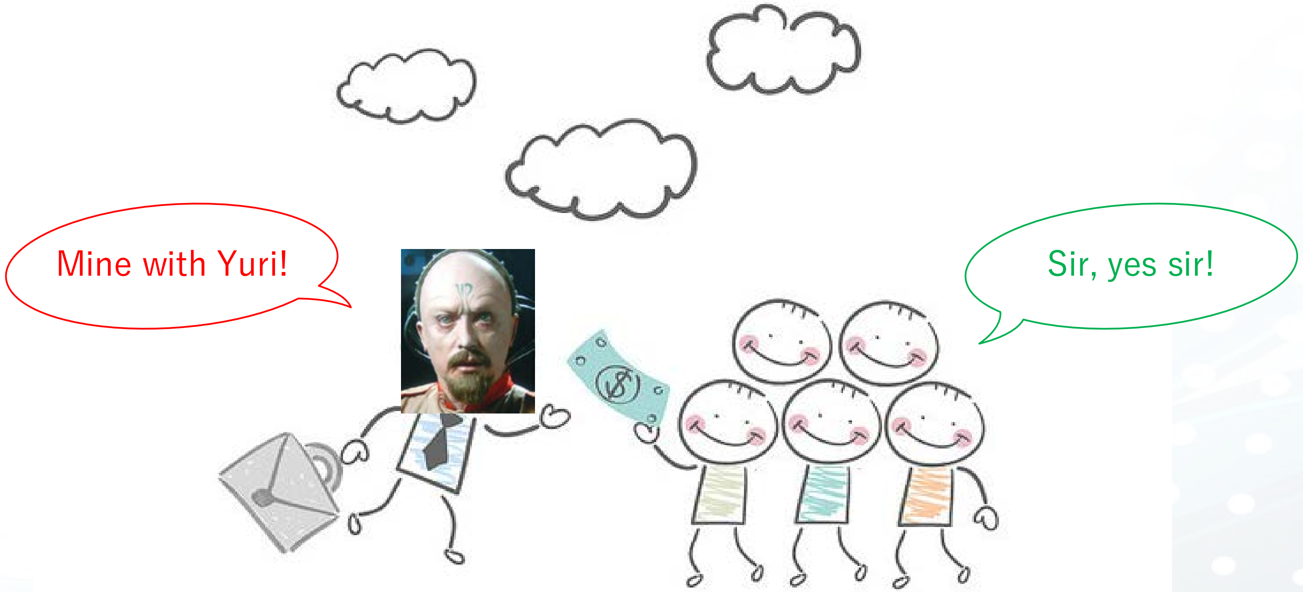
- Better than BWH.
- Break the dilemma: we may have a winner.
- *Fixed innocent-infiltration mining ratio*
  - *What if the value of one part of reward changes? E.g. shared reward becomes more “attractive”?*



Mining Attacks: Bribery Attacks

- When forks occur, attacker can bribe others to increase the chance of winning.
  - Sending "anyone can claim" transactions on attacker's branch
  - If bribes are considerable, others may be willing to work on attacker's branch.
    - Attacker may get more than 50% mining power in a short period (possible double-spending).

  - *Cost too much bribes to revert a long branch.*



Outline

- Bitcoin Overview
- Mining Attacks
- Power Adjusting Withholding
- Bribery Selfish Mining
- Discussion
- Conclusion

PAW: Observation

- In FAW, the value of the shared reward will change after infiltration mining finds an FPoW.

Case 1: *smaller* the pool, *higher* the chance to win in forks.

- When the pool size is small, I can share more profit if I allocate more power into it.
- Even when forks occur, I have a high chance to get a share.

The share is more attractive!

Case 2: *larger* the pool, *less* the chance to win in forks.

- Even when I allocate more power, I still get little shared reward.
- When forks occur, I only get very few shares

The share is less attractive!

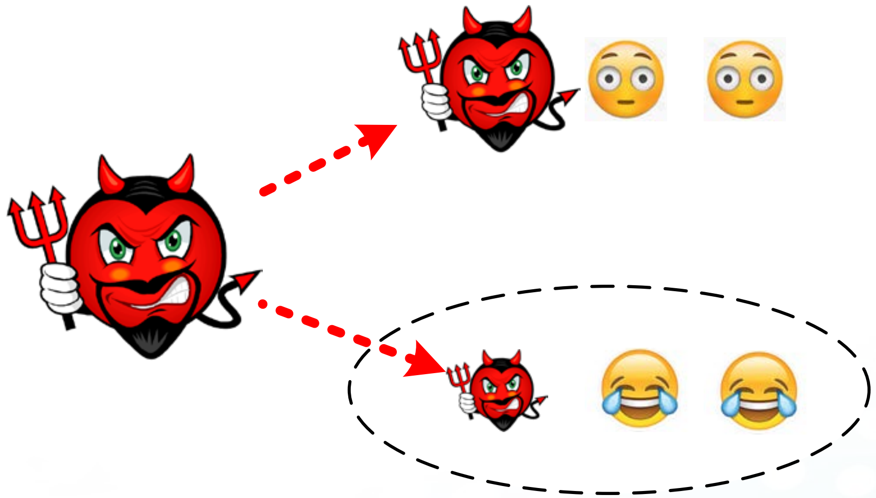
PAW: Observation

- In FAW, the shared reward's value will change after infiltration mining finding an FPoW.

Why not adjust my power splitting after finding an FPoW!

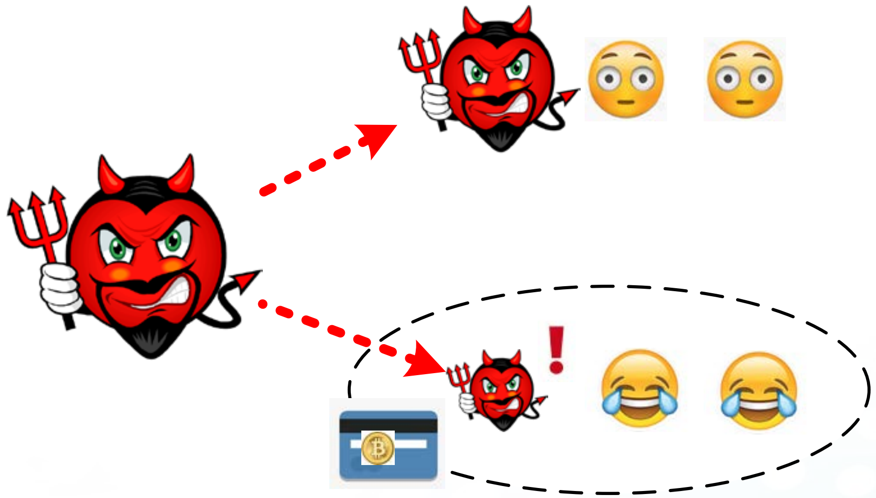
PAW: Power Adjusting Withholding

- PAW = <u>P</u>ower <u>A</u>djusting + FA<u>W</u>
  - Splitting power into innocent mining and infiltration mining (as with FAW).



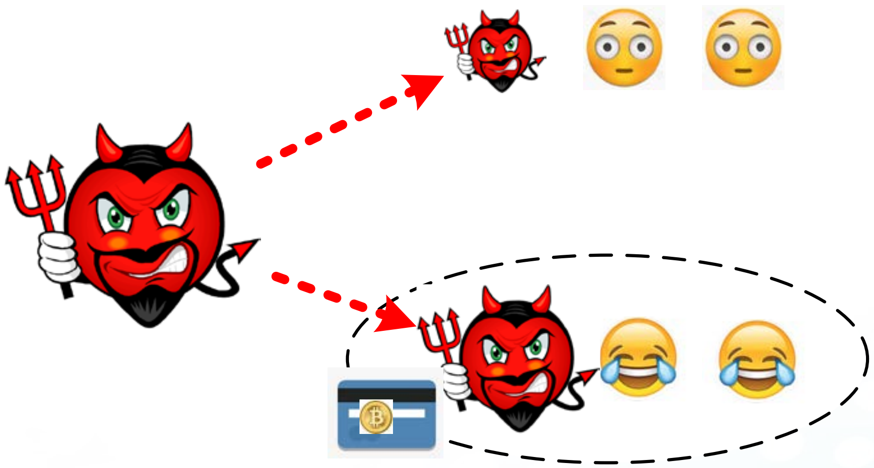
PAW: Power Adjusting Withholding

- PAW = **P**ower **A**djusting + FA**W**
  - Splitting power into innocent mining and infiltration mining (as with FAW).
  - When infiltration mining finds an FPoW, *adjust power splitting strategy*.



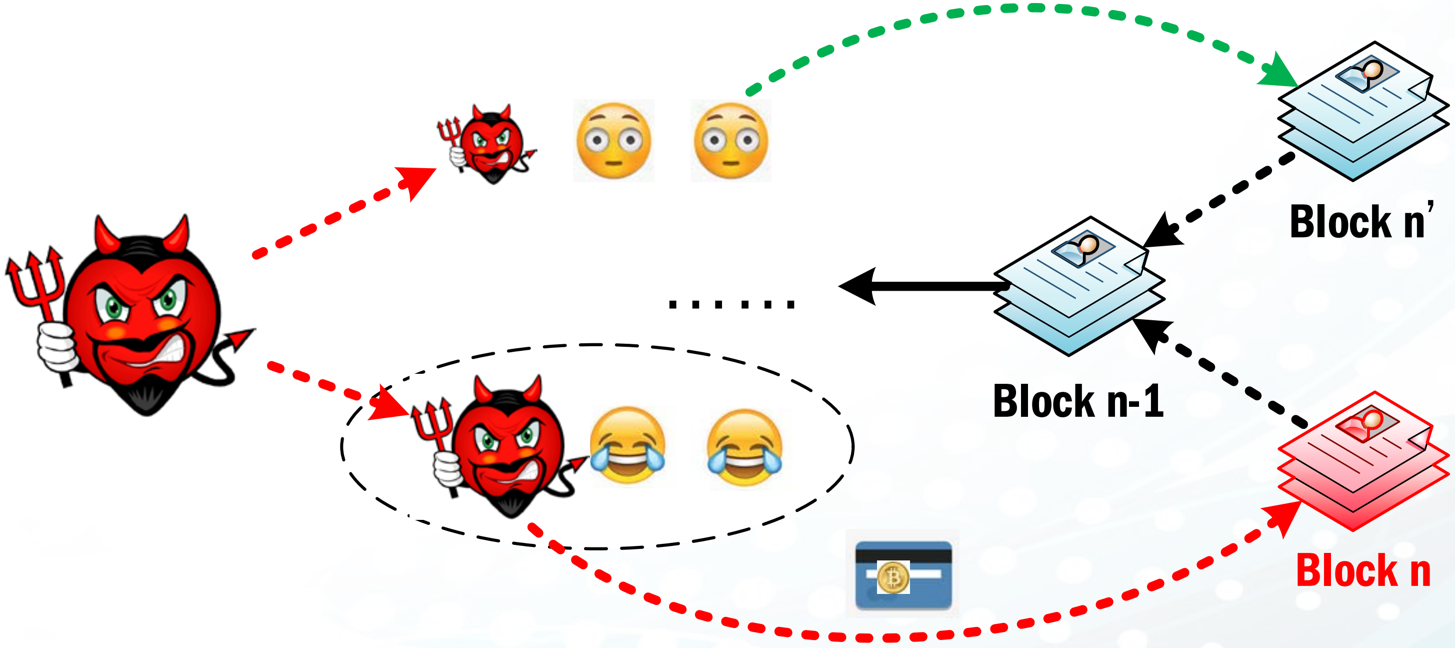
PAW: Power Adjusting Withholding

- PAW = **P**ower **A**djusting + FA**W**
  - Splitting power into innocent mining and infiltration mining (as with FAW).
  - When infiltration mining finds an FPoW, *adjust power splitting strategy*. NEW!



PAW: Power Adjusting Withholding

- PAW = **P**ower **A**djusting + FA**W**
  - Splitting power into innocent mining and infiltration mining (as with FAW).
  - When infiltration mining finds an FPoW, *adjust power splitting strategy*. NEW!
  - Infiltration mining withholds FPoWs, and submits when others find blocks (as with FAW).



PAW: Power Adjusting Withholding

- PAW = **<u>P</u>**ower **<u>A</u>**djusting + FA**<u>W</u>**
  - Splitting power into innocent mining and infiltration mining (as with FAW).
  - When infiltration mining finds an FPoW, *adjust power splitting strategy*. NEW!
  - Infiltration mining withholds FPoWs, and submits when others find blocks (as with FAW).

- How to adjust power?
  - Based on the optimizing function.

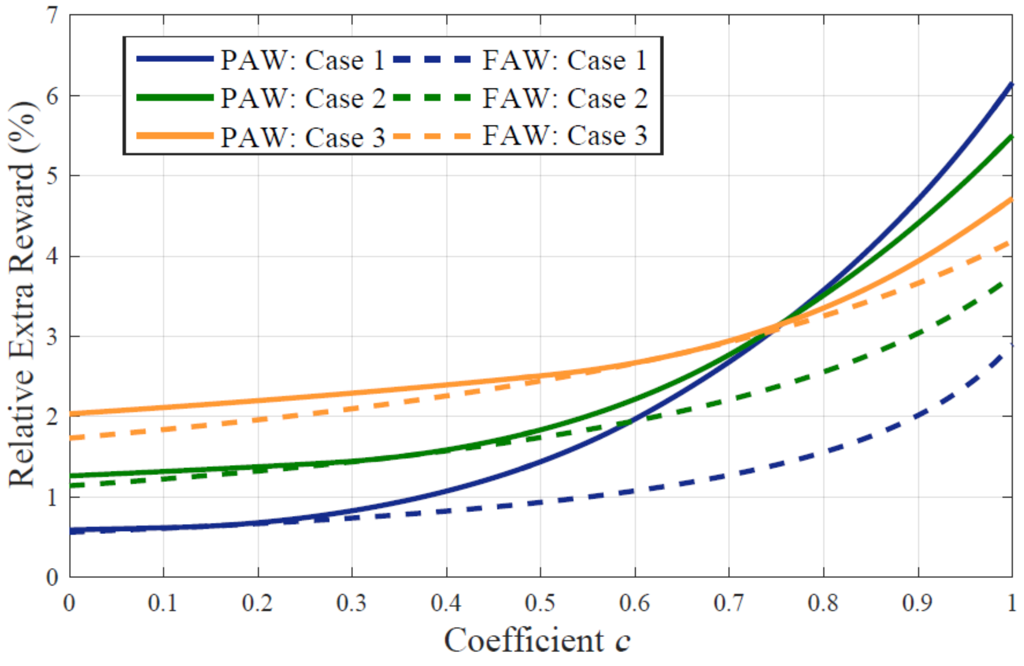
$$R_a^P(\tau_1, \tau_2) = (1-\tau_1)\alpha + \beta \cdot \frac{\tau_1\alpha}{\beta + \tau_1\alpha} + \tau_1\alpha \cdot \left(\frac{(1-\tau_2)\alpha}{1-\tau_2\alpha} + \left(c \cdot \frac{1-\alpha-\beta}{1-\tau_2\alpha} + \frac{\beta}{1-\tau_2\alpha}\right) \cdot \frac{\bar{\tau}\alpha}{\beta + \bar{\tau}\alpha}\right),$$

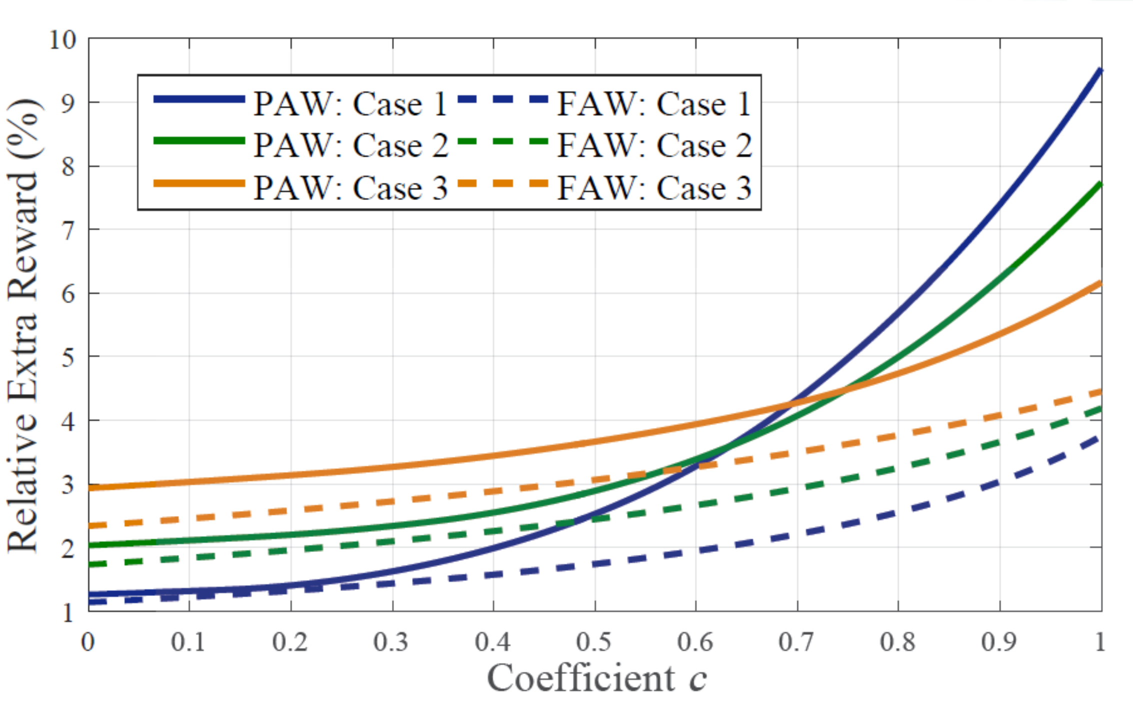
$$\arg\max_{\tau_1, \tau_2} R_a^P(\tau_1, \tau_2), \quad 0 \leqslant \tau_1 \leqslant 1, \quad 0 \leqslant \tau_2 \leqslant 1.$$

  - Allocating more power to infiltration mining when the share is more attractive; less power when less attractive.

PAW: Higher Reward

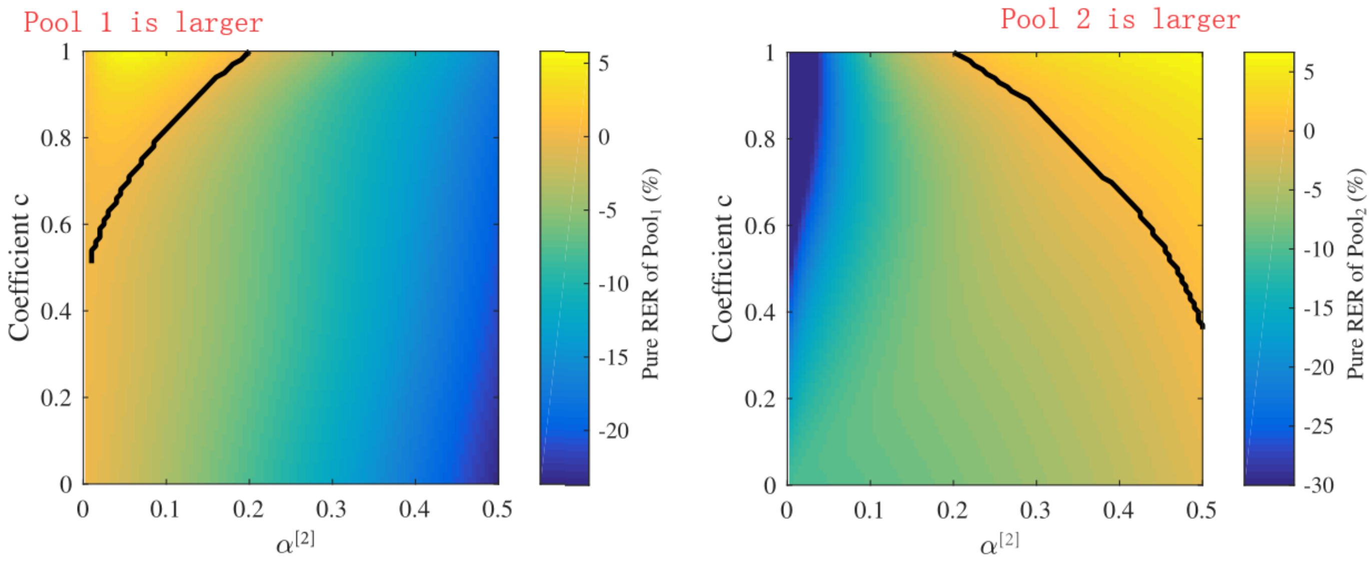
- Better than FAW.
  - We can ensure PAW = FAW with an additional constraint: $\tau_1 = \tau_2$ (not adjusting).
  - Without the additional constraint, PAW will get a better result (higher reward) than FAW.





PAW: Avoiding Dilemma

- Avoiding the “miner’s dilemma”.
  - Pool-size game: smaller pool will lose, larger pool may win.

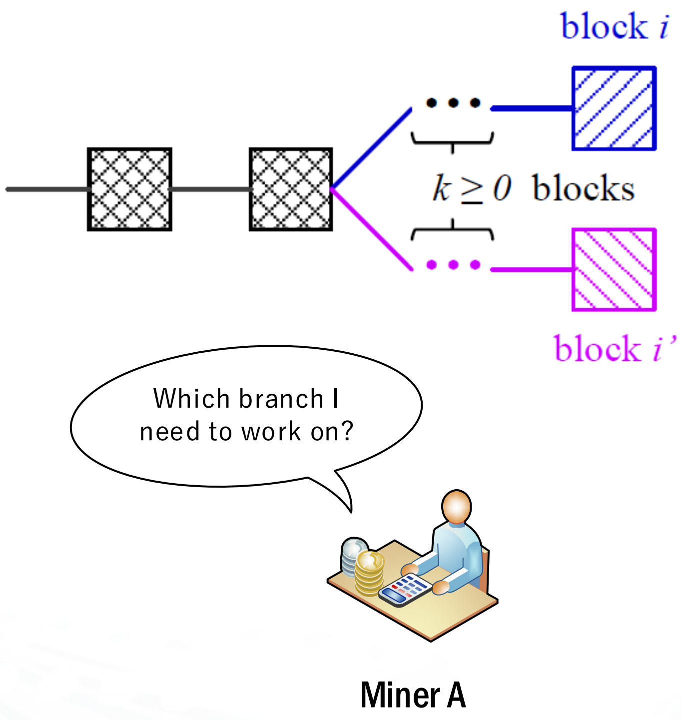


Outline

- Bitcoin Overview
- Mining Attacks
- Power Adjusting Withholding
- Bribery Selfish Mining
- Discussion
- Conclusion

BSM: 0-Lead Racing

- 0-lead racing: two branches of the same length racing in the system.
  - Other miners have no difference in working on which branch
  - Typical scenario: selfish mining



Case 1, ***A*** finds a block: he will get a reward and continue mining on the current branch.

Case 2, ***A*** does not find: he will switch to the main branch (if necessary) and continue mining.

No difference between blue and pink branches!

BSM: Observation

- When 0-lead racing occur, attacker can “lure” others to work on his branch.
  - Increase the chance of winning in forks with little cost.

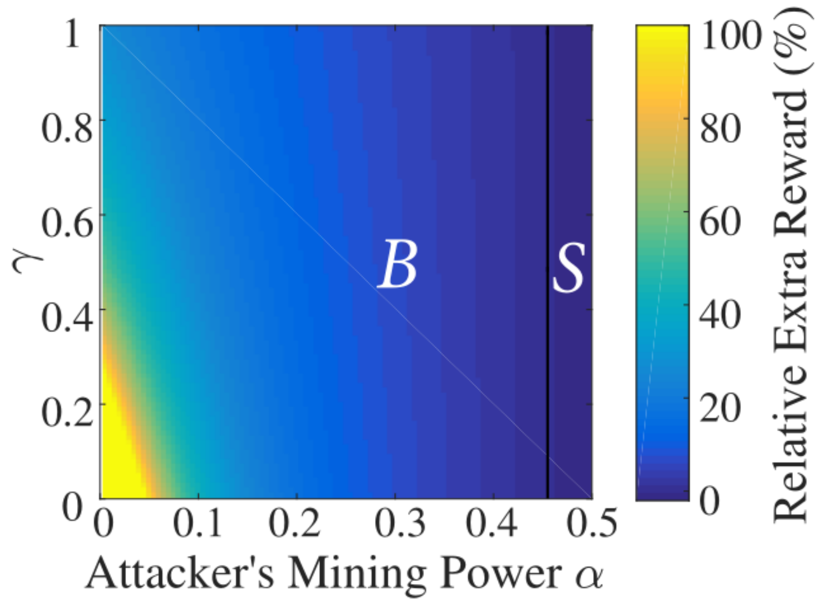
Why not bribe others (with little cost) to work on my branch!

BSM: Bribery Selfish Mining

- BSM = **B**ribery attacks + **S**elfish **M**ining
  - Publish the private branch when public branch catches up to cause 0-lead racing in selfish mining.
  - Including bribery transactions when mining the new private block.
  - When mining the second private block, transferring the money back and including new bribery transactions.

BSM: Higher Reward

- More venal miners = better chance of wining in forks
  - A critical parameter in selfish mining: the ratio of venal miners
  - Can be more profitable than selfish mining with a proper amount of bribes.

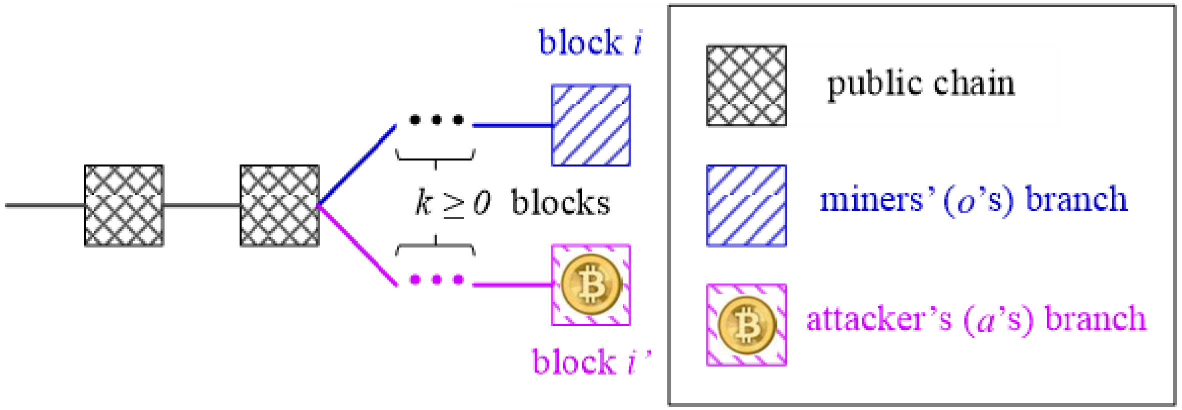


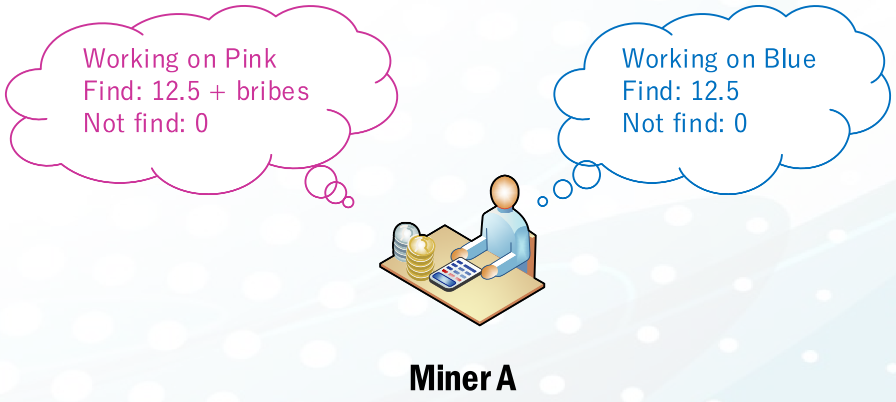
Attacker’s dominant strategy (BSM VS selfish mining).

bribes = 0.02; B = BSM; S = Selfish mining

BSM: Higher Reward

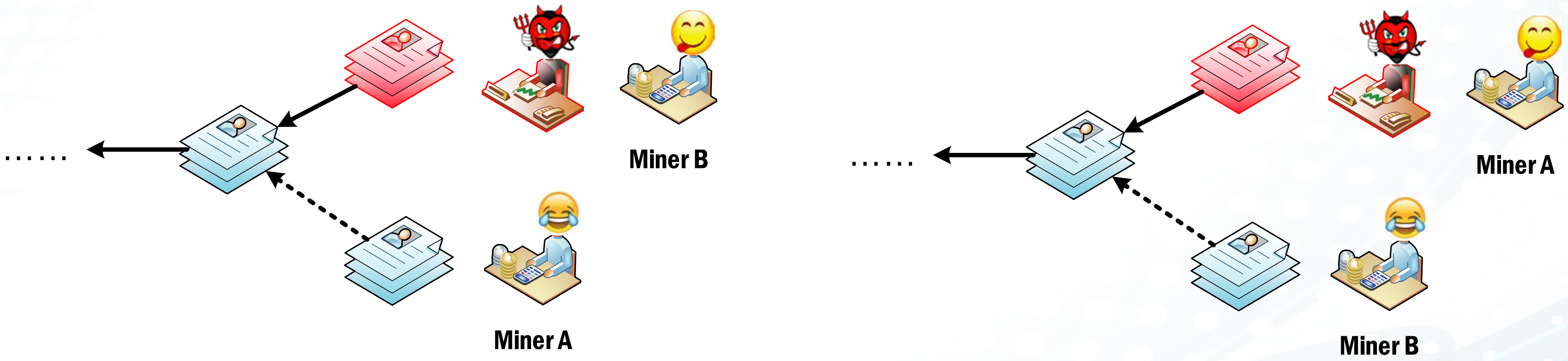
- More venal miners = better chance of wining in forks
  - A critical parameter in selfish mining: the ratio of venal miners
  - Can be more profitable than selfish mining with a proper amount of bribes.
- How much to pay for bribes?
  - **Almost nothing!** As long as bribes > 0.
  - Profit-driven miners: something is better than nothing





BSM: The Venal Miner's Dilemma

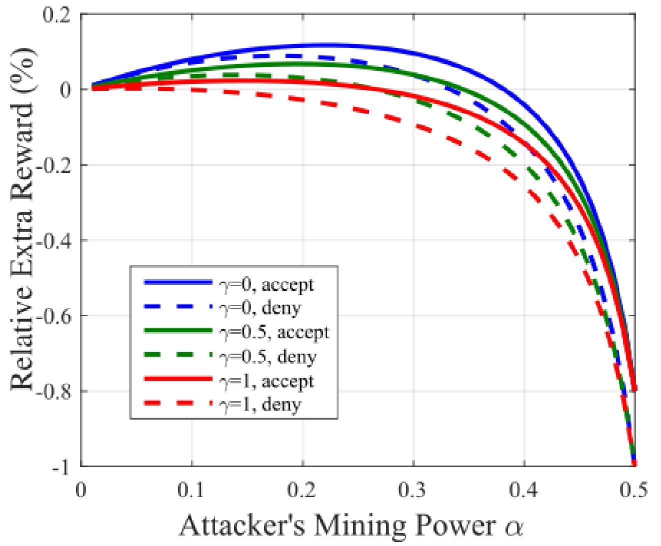
- What if the attacker races with venal miner?
  - For miner A and B, their dominant strategy is mining on attacker's branch.
  - A and B are harming each other's profit, while making the attacker more profitable!



BSM: The Venal Miner's Dilemma

- What if the attacker races with venal miner?
  - For miner A and B, their dominant strategy is mining on the attacker's branch.
  - A and B are harming each other's profit, while making the attacker more profitable!

  - When more venal miners are involved, there will be a "venal miner's dilemma".
    - All venal miners choose to accept the bribes (mine on the attacker's branch), but will suffer from a lost comparing with none acceptance.



Target_2 \ Target_1	Accept at $0'_o$	Deny at $0'_o$
Accept at $0'_o$	(**-2.58%**, **-0.62%**)	(-6.44%, **1.63%**)
Deny at $0'_o$	(**3.85%**, -1.85%)	(0.45%, 0.45%)

BSM: Venal Miner’s Dilemma VS Miner’s Dilemma

- Differences between the “miner’s dilemma”:

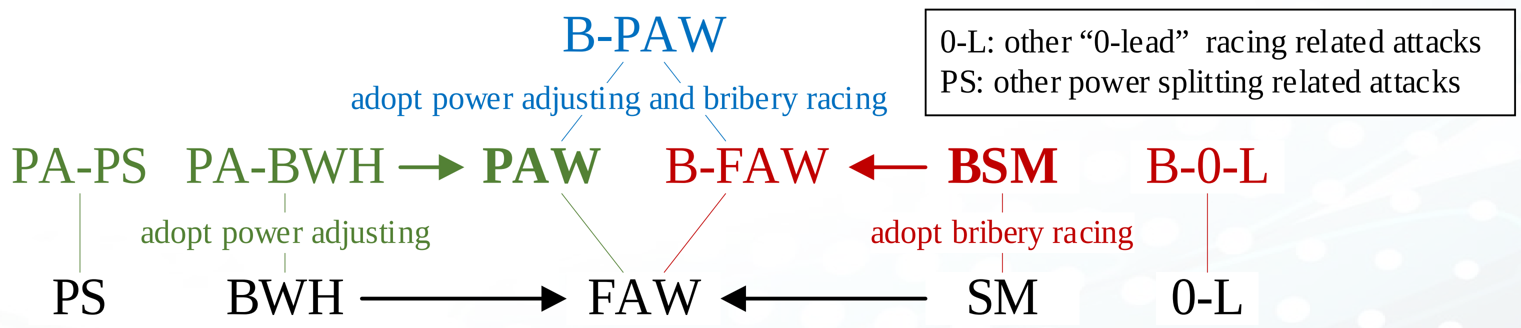
	Venal Miner’s Dilemma	Miner’s Dilemma
Participants	1 attacker, 2 venal miners	2 attackers, and other miners
Beneficiary	Attacker	Other miners
Victim	Venal miners	Attackers
Good property for the attack?	Yes	No

Outline

- Bitcoin Overview
- Mining Attacks
- Power Adjusting Withholding
- Bribery Selfish Mining
- Discussion
- Conclusion

Discussion: Attack Strategy Space

- PAW: power splitting related.
  - The idea of power adjusting can be used to other power splitting related attacks, after some part of reward value changes.
    - E.g., power adjusting + BWH = PA-BWH.
- BSM: 0-lead racing related.
  - The idea of bribery can be applied to other 0-lead racing related attacks.
    - E.g., Bribery + FAW = B-FAW; Bribery + PAW = B-PAW.



Discussion: Countermeasure

- PAW detection.
  - Power adjusting is hard to be detected.
    - Not always happen: only after infiltration mining finds an FPoW.
    - Non-frequent power adjusting is legal and acceptable for honest miners.
  - PAW can be detected via BWH/FAW detection.
    - BWH detection: statistic (PPoW/FPoW ratio).
    - FAW detection: stale FPoWs.
      - Timestamp based detection: synchronize miner's time; verify timestamp field.

- PAW attacker can use Sybil nodes when detected to get more profit.

Open problem to prevent PAW

Discussion: Countermeasure

- Bribery countermeasures.
  - Restrict the use of “anyone can claim” transactions.
    - *Sacrifice the flexibility and programmability.*
  - Miners should preferentially choose the branch containing the transactions which they previously received.
    - *Unrealistic to assume all miners adopt this approach.*
  - Pool managers should expel pool miners who submit FPoWs containing bribes.
    - Avoiding bribery racing in FAW/PAW.
    - Pool miners should leave pools when pools accept FPoWs containing bribes.

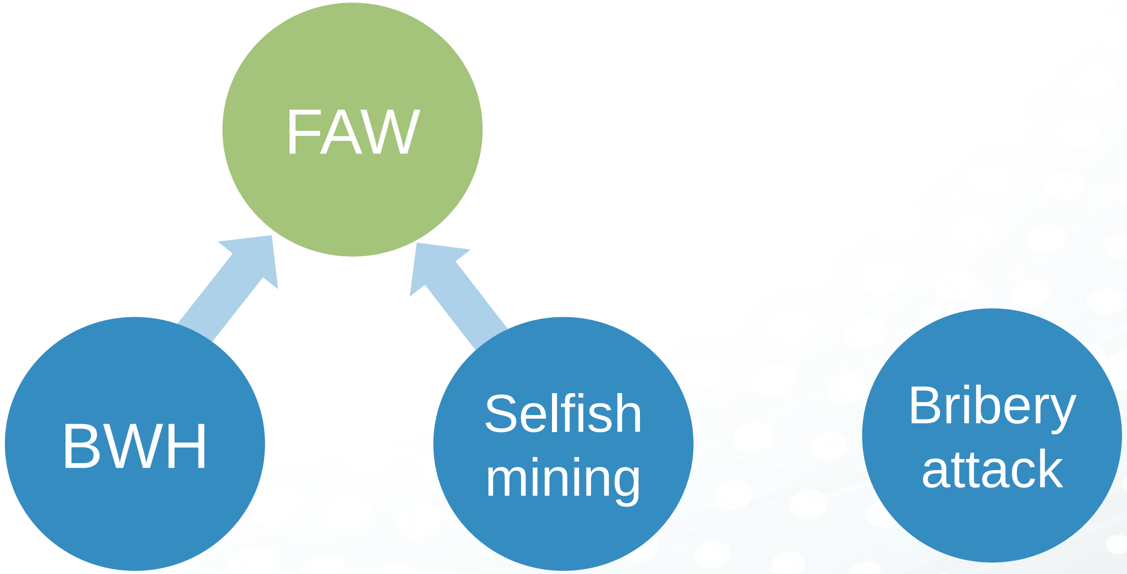
- Bribery related attacks are hard to be avoided.
  - Greedy.
  - Out-of-band transactions.

No silver bullet

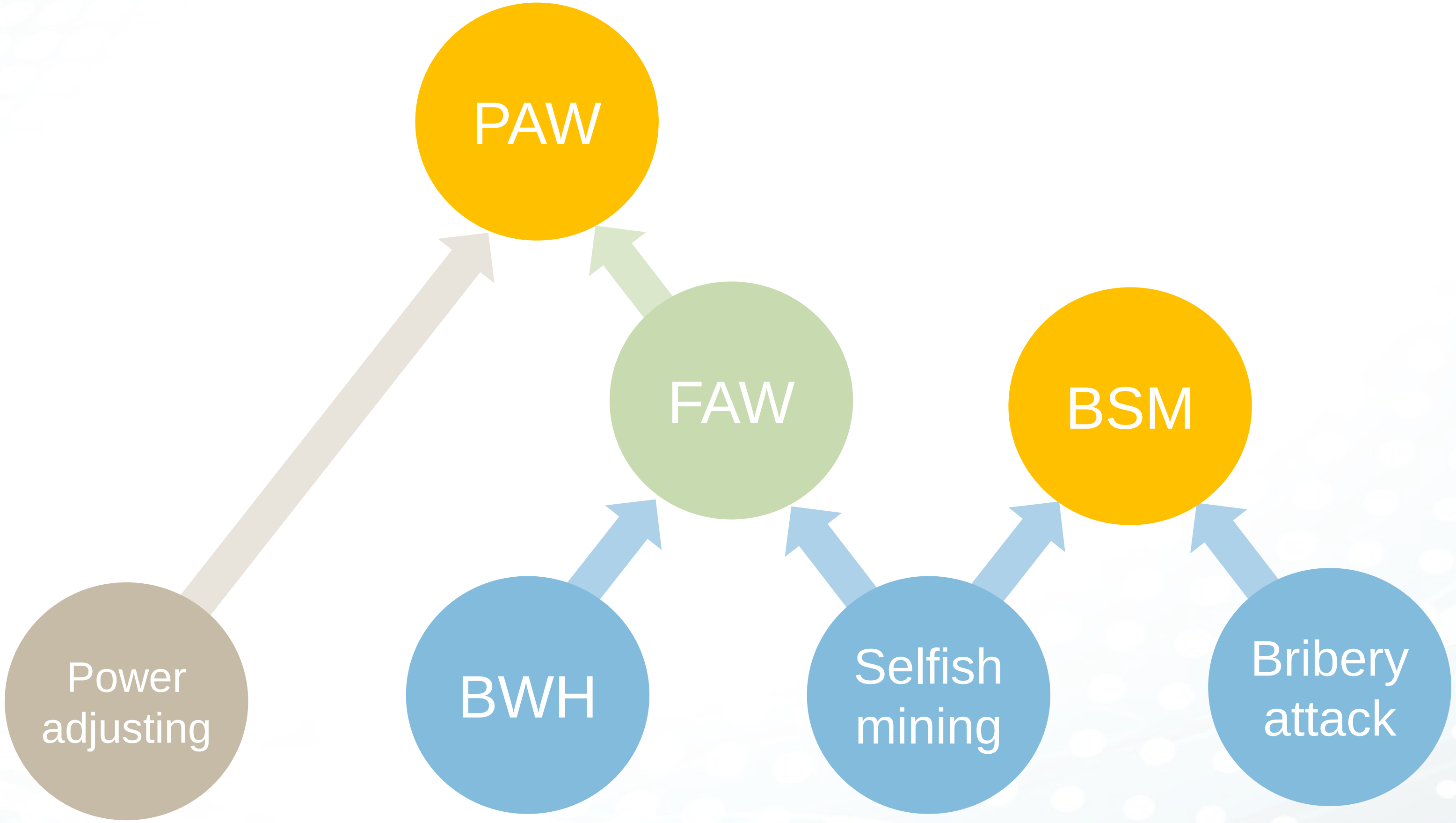
Outline

- Bitcoin Overview
- Mining Attacks
- Power Adjusting Withholding
- Bribery Selfish Mining
- Discussion
- Conclusion

Conclusion

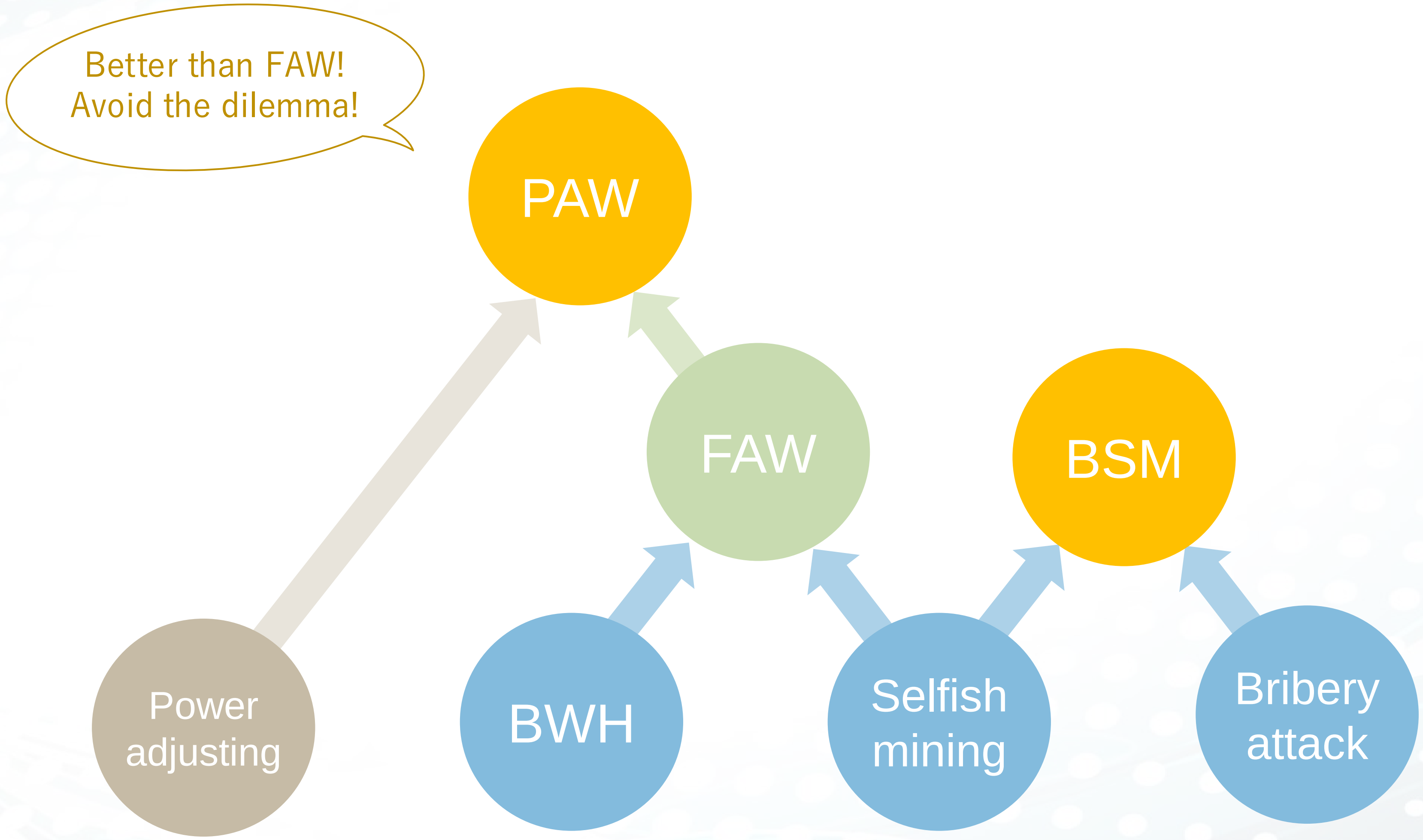


Conclusion



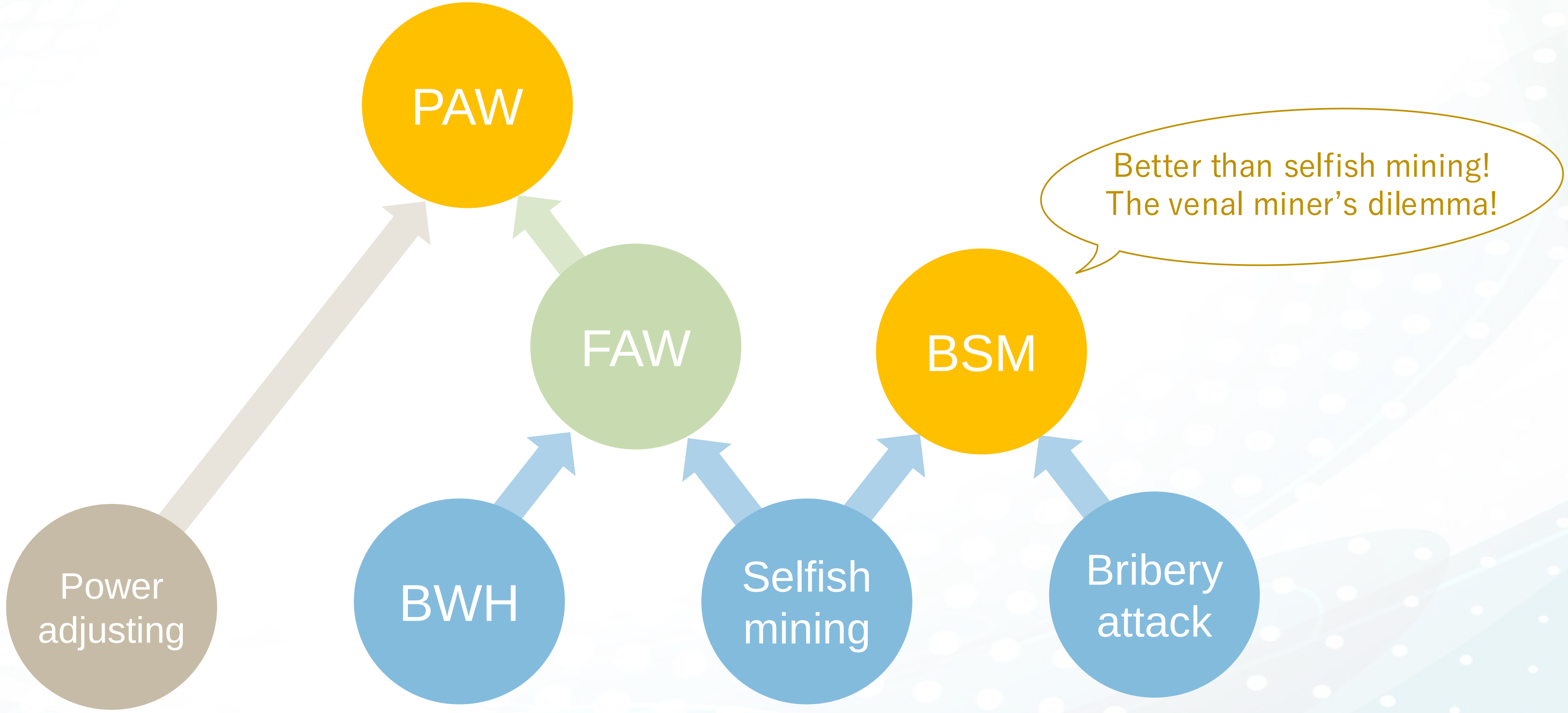
PAW
FAW
BSM
Power adjusting
BWH
Selfish mining
Bribery attack

Conclusion

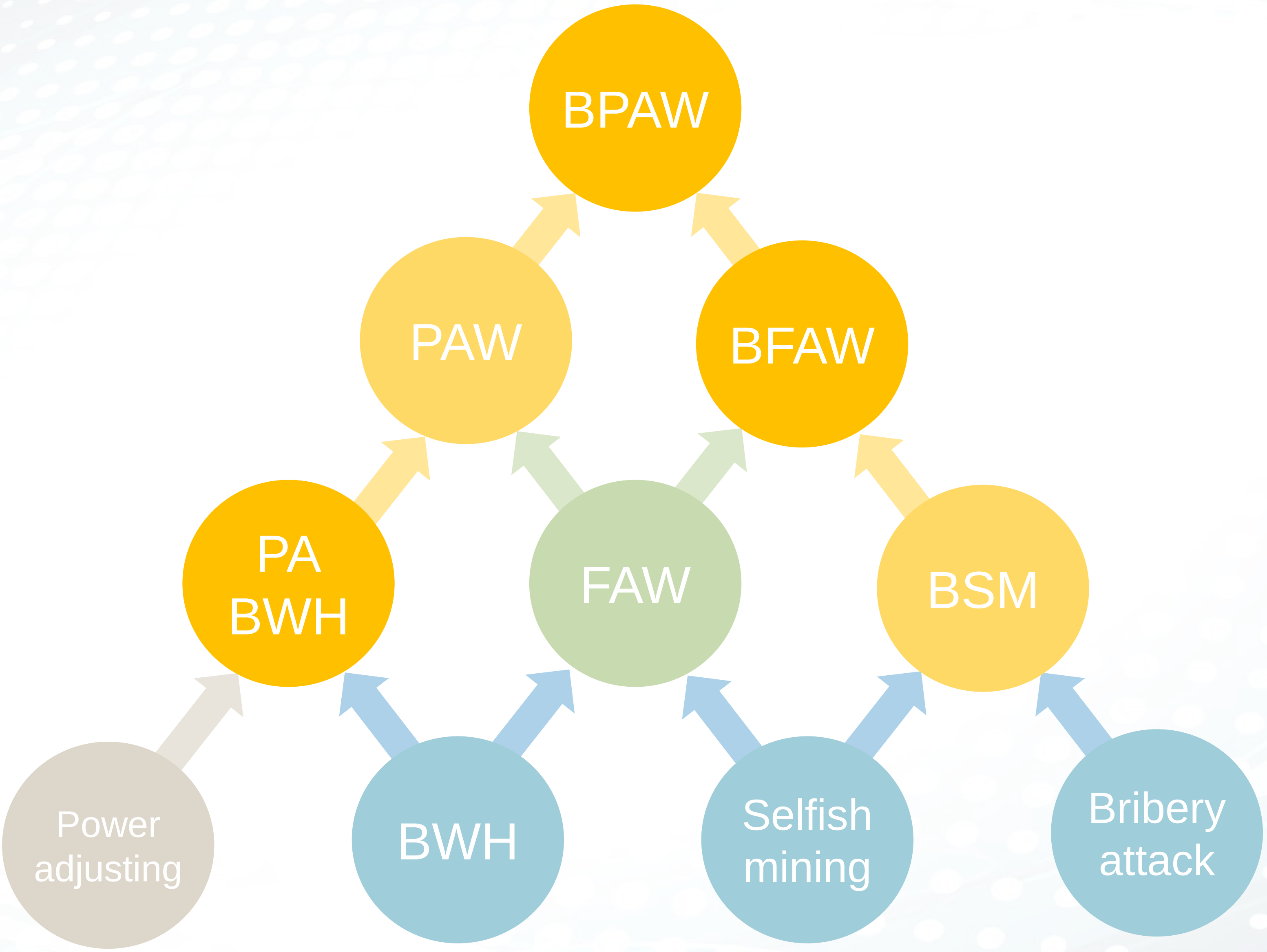


Better than FAW!
Avoid the dilemma!
PAW
FAW
BSM
Power adjusting
BWH
Selfish mining
Bribery attack

Conclusion


PAW
FAW
BSM
Better than selfish mining!
The venal miner's dilemma!
Power adjusting
BWH
Selfish mining
Bribery attack

Conclusion


BPAW
PAW
BFAW
PA BWH
FAW
BSM
Power adjusting
BWH
Selfish mining
Bribery attack

Q&A

THANK YOU