# Low-Variance Mining with Bobtail

*– or –*

*Why Variance is the Root of All Evil*

**George Bissias**
and
**Brian Neil Levine**

College of Information & Computer Sciences

UMass Amherst

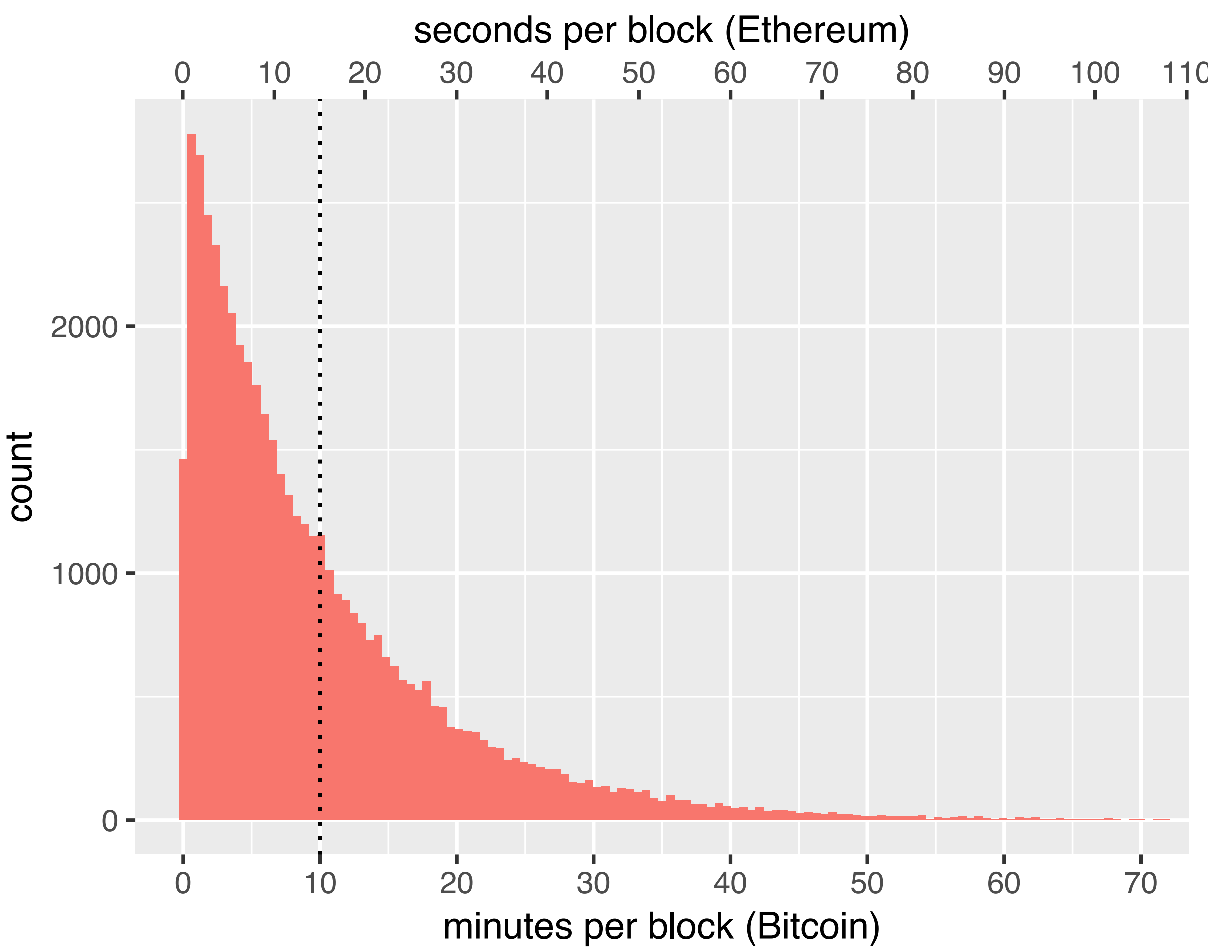
# Overview

- The variance of Bitcoin's inter-block delay is more than an annoyance.
- It's at the root of doublespend, selfish mining, and eclipse attacks.
- We propose a simple method of low-variance mining
- We evaluate its performance and show how it increases security
- We talk about consequences of deployment



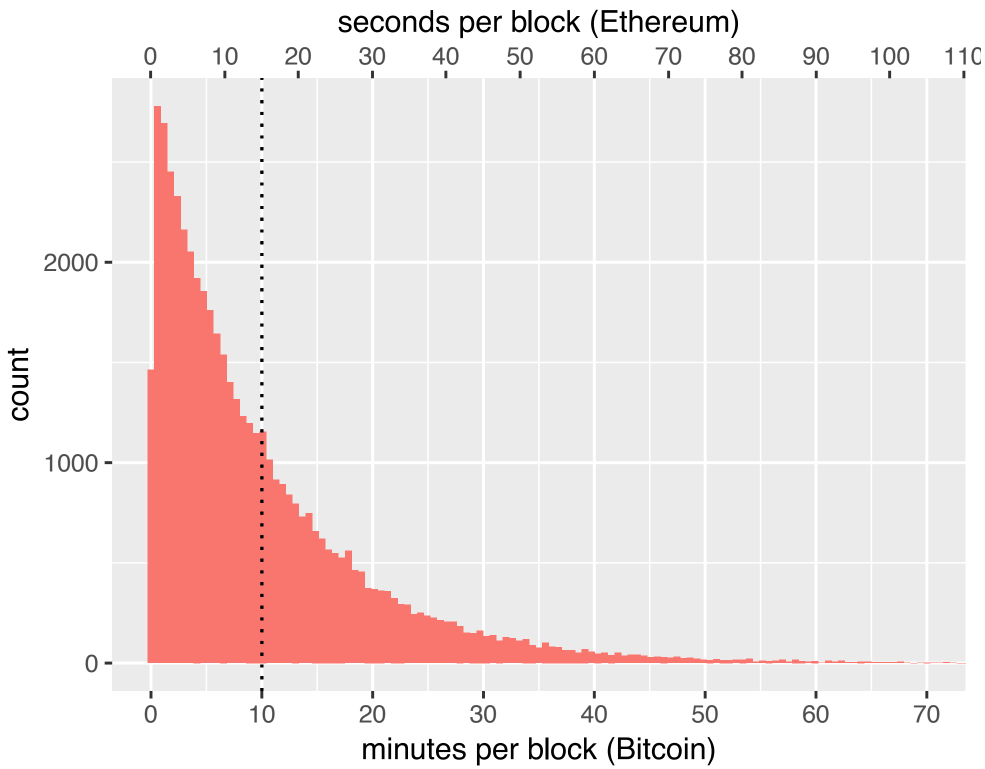
https://arxiv.org/abs/1709.08750

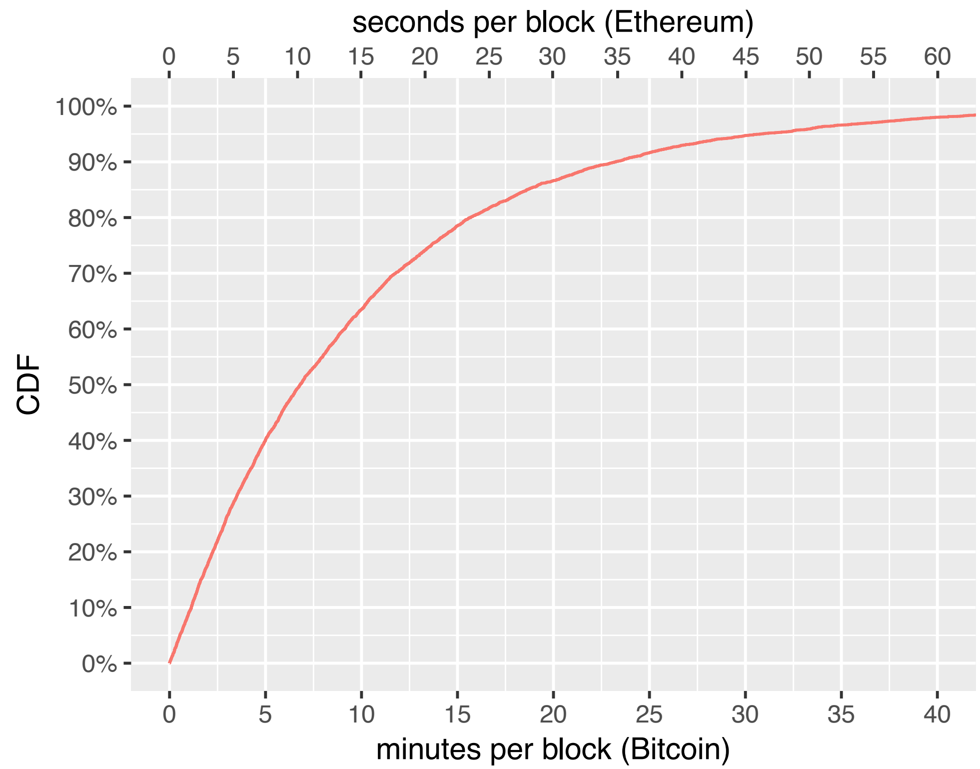
# Problem Definition




5% of blocks take at least 30 minutes
80% of blocks are between 1–21 minutes
https://arxiv.org/abs/1709.08750

# Problem Definition

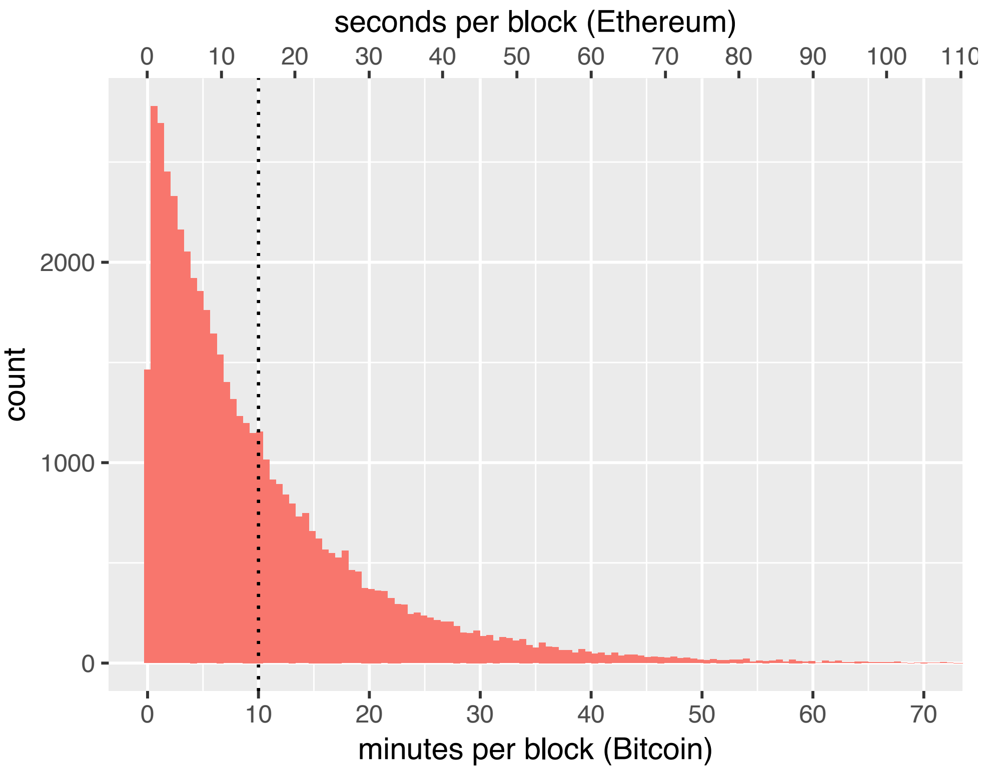


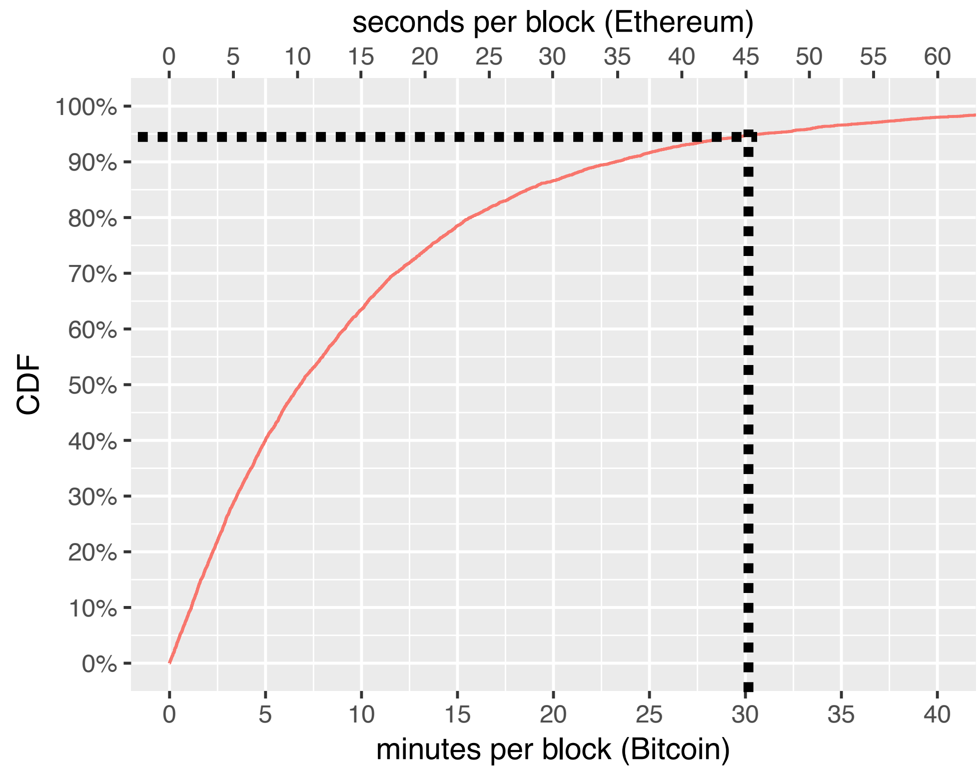




5% of blocks take at least 30 minutes
80% of blocks are between 1–24 minutes

https://arxiv.org/abs/1709.08750

# Problem Definition



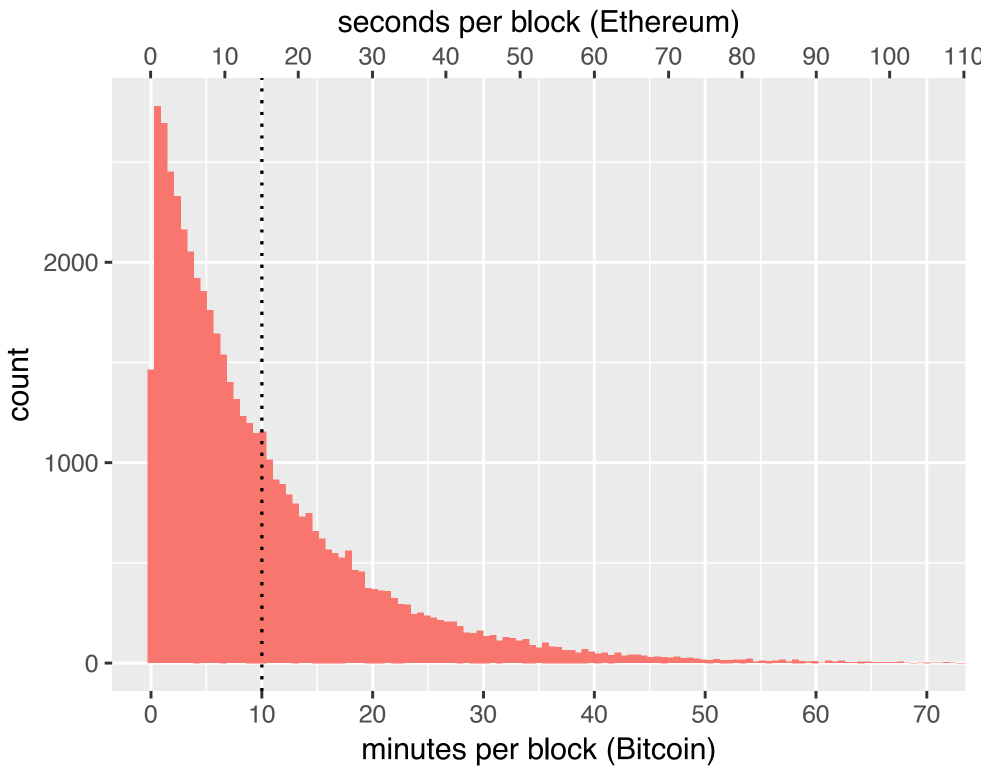



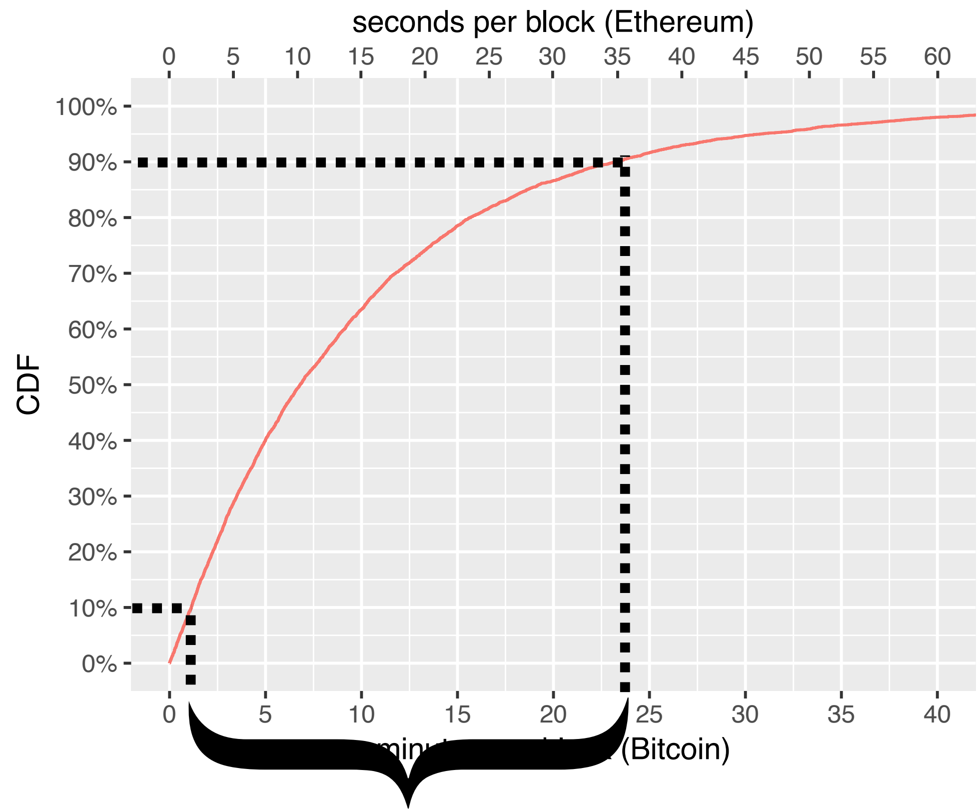

5% of blocks take at least 30 minutes

80% of blocks are between 1–24 minutes

https://arxiv.org/abs/1709.08750

# Problem Definition



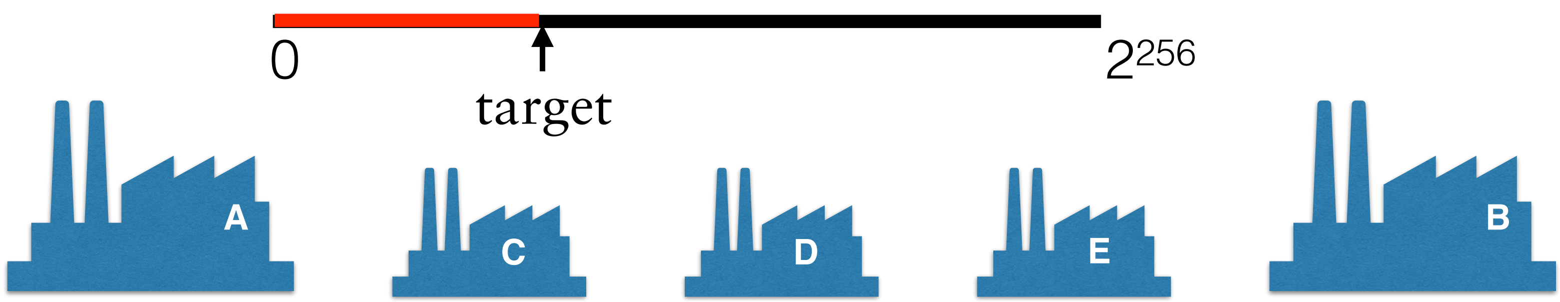




5% of blocks take at least 30 minutes
80% of blocks are between 1–24 minutes

https://arxiv.org/abs/1709.08750

# Variance in PoW Mining

- Inter-block time variance is due to Proof of Work mining.
  - Each miner samples from a uniform distribution
  - The first miner to find 1 sample below a target wins.
- Until they pick a number that meets the target.
  - When the network of miners get lucky, blocks come early.
  - When the network of miners get very unlucky, blocks come late.

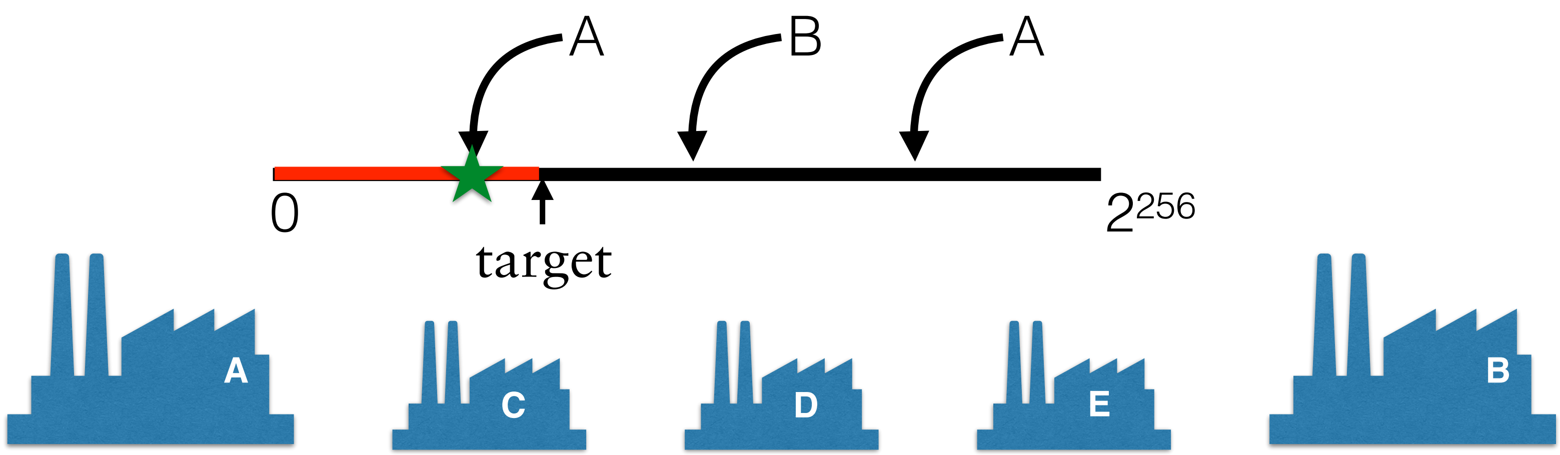





https://arxiv.org/abs/1709.08750

# Variance in PoW Mining

- Inter-block time variance is due to Proof of Work mining.
  - Each miner samples from a uniform distribution
  - The first miner to find 1 sample below a target wins.
- Until they pick a number that meets the target.
  - When the network of miners get lucky, blocks come early.
  - When the network of miners get very unlucky, blocks come late.






https://arxiv.org/abs/1709.08750

# Variance is the root of all evil

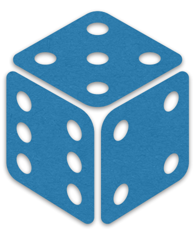
- With low variance between blocks, blockchains would perform more consistently.
  - Fast blocktimes are what some competitors have over Bitcoin.
  - Waiting 6 blocks to overcome fear of doublespend is a drag.
  - Wouldn't it be better if blocks almost always arrived within 7–12 minutes?
  - And if we were confident about waiting just 1 block?
  - But variance is not just an inconvenience:
- **High variance mining is the cause of low security in blockchains.**

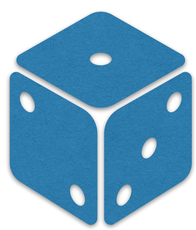


https://arxiv.org/abs/1709.08750

# Variance is the root of all evil

- When you enter a casino, the house has the advantage.
  - In expectation the house will win.
  - Your goal is to keep betting until you are ahead, and then exit.
  - This strategy is possible because you are taking advantage of variance
  - The house occasionally loses, possibly a few times in a row.



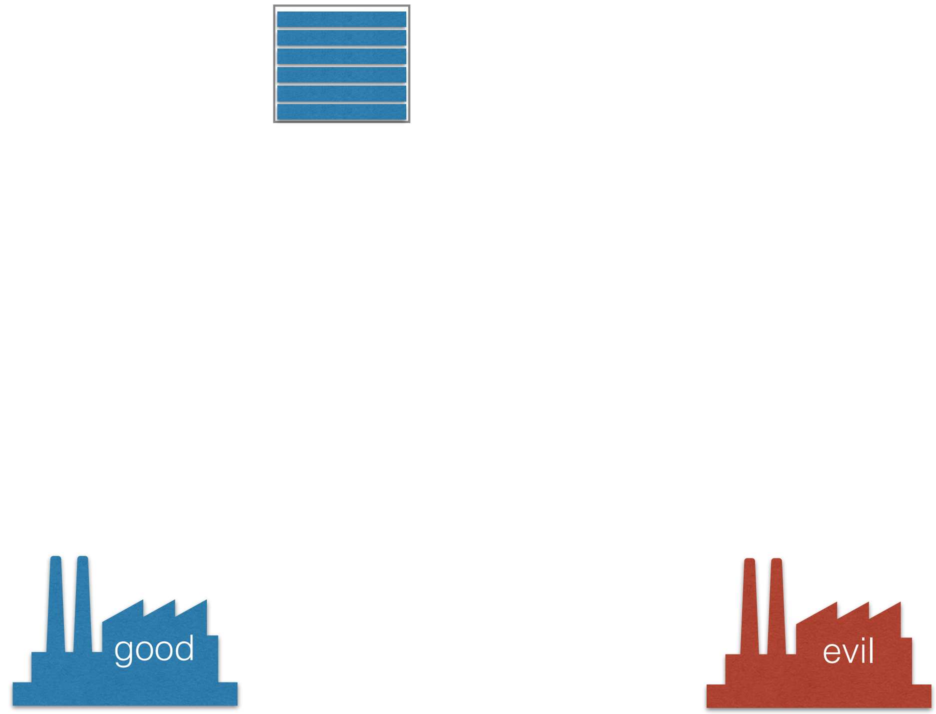




https://arxiv.org/abs/1709.08750

# Doublespend Attacks

- **Doublespend attacks** are a race between honest and attacking miners.
- Just like in the casino, there is a non-zero chance she'll win.
- She's waiting for either:
  - the honest miners to hit a sequence of unlucky block discovery times
  - for herself to hit a sequence of lucky block discovery times.



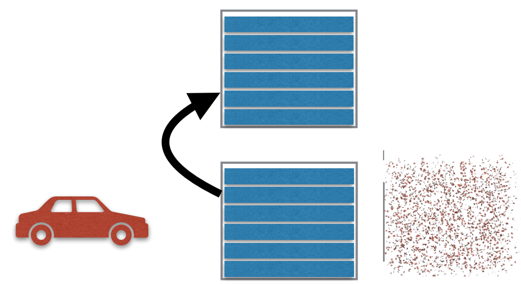

https://arxiv.org/abs/1709.08750

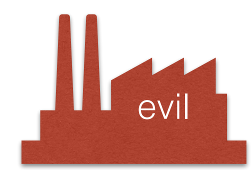
# Doublespend Attacks

- **Doublespend attacks** are a race between honest and attacking miners.

- Just like in the casino, there is a non-zero chance she'll win.

- She's waiting for either:
    - the honest miners to hit a sequence of unlucky block discovery times
    - for herself to hit a sequence of lucky block discovery times.



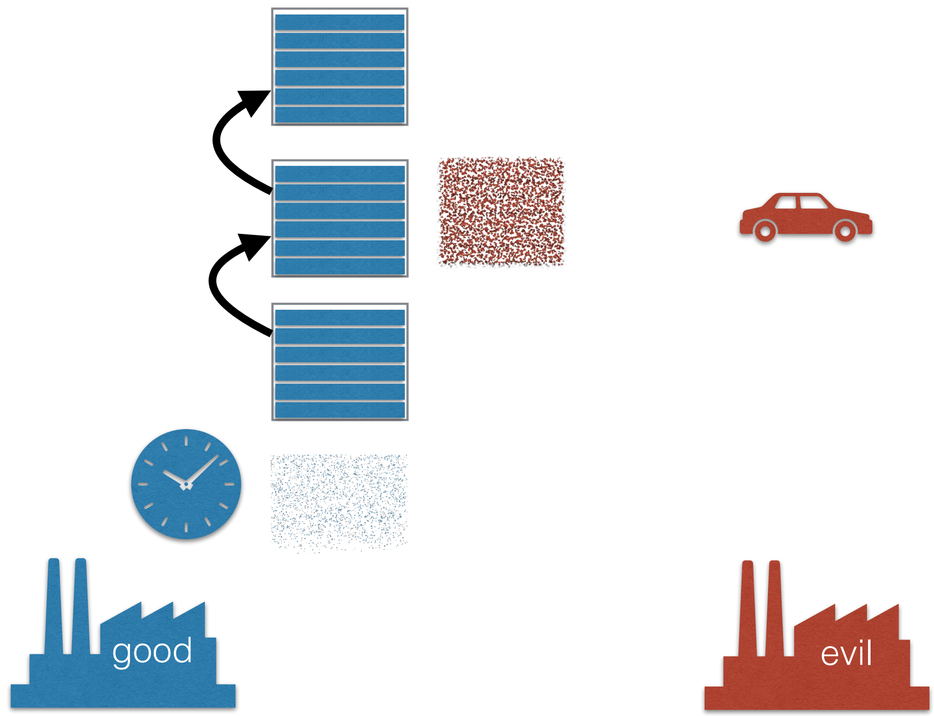






https://arxiv.org/abs/1709.08750

# Doublespend Attacks

- **Doublespend attacks** are a race between honest and attacking miners.
- Just like in the casino, there is a non-zero chance she'll win.
- She's waiting for either:
    - the honest miners to hit a sequence of unlucky block discovery times
    - for herself to hit a sequence of lucky block discovery times.

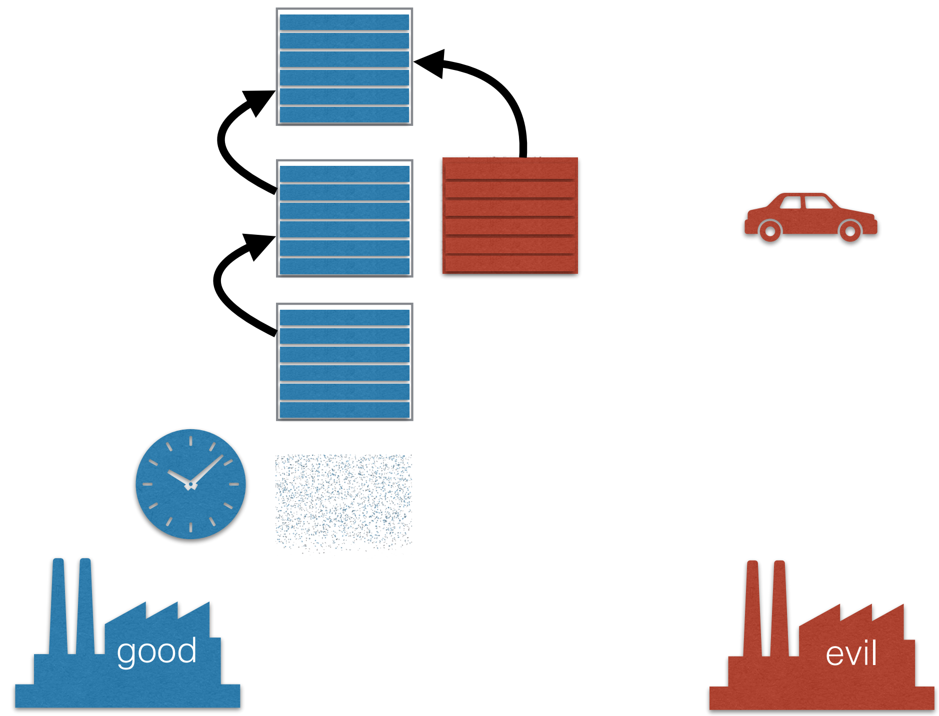





https://arxiv.org/abs/1709.08750

# Doublespend Attacks

- **Doublespend attacks** are a race between honest and attacking miners.
- Just like in the casino, there is a non-zero chance she'll win.
- She's waiting for either:
  - the honest miners to hit a sequence of unlucky block discovery times
  - for herself to hit a sequence of lucky block discovery times.

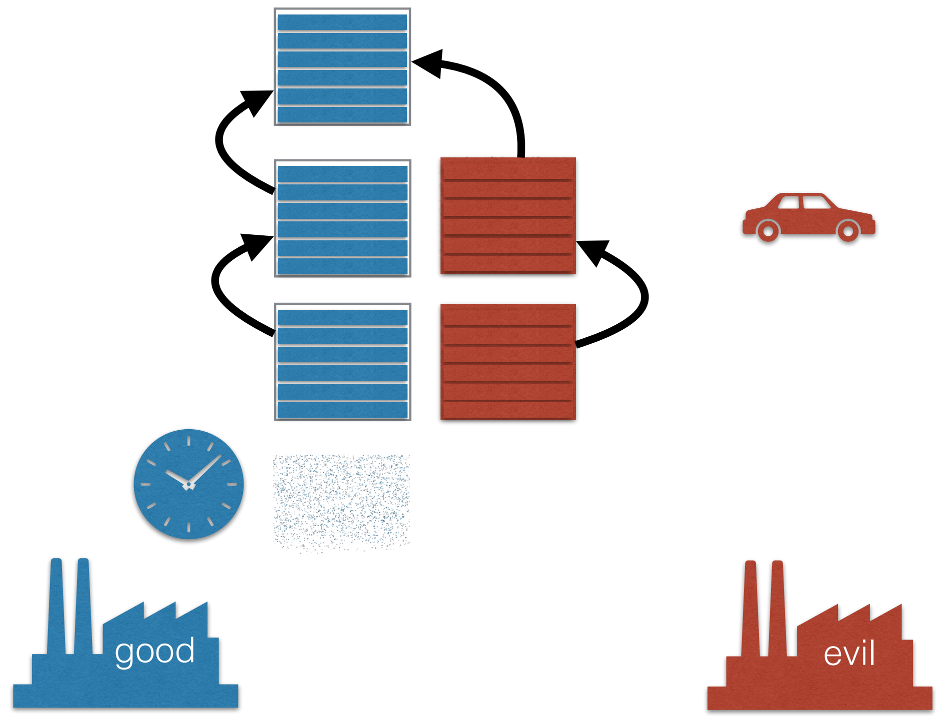





https://arxiv.org/abs/1709.08750

# Doublespend Attacks

- **Doublespend attacks** are a race between honest and attacking miners.
- Just like in the casino, there is a non-zero chance she'll win.
- She's waiting for either:
  - the honest miners to hit a sequence of unlucky block discovery times
  - for herself to hit a sequence of lucky block discovery times.

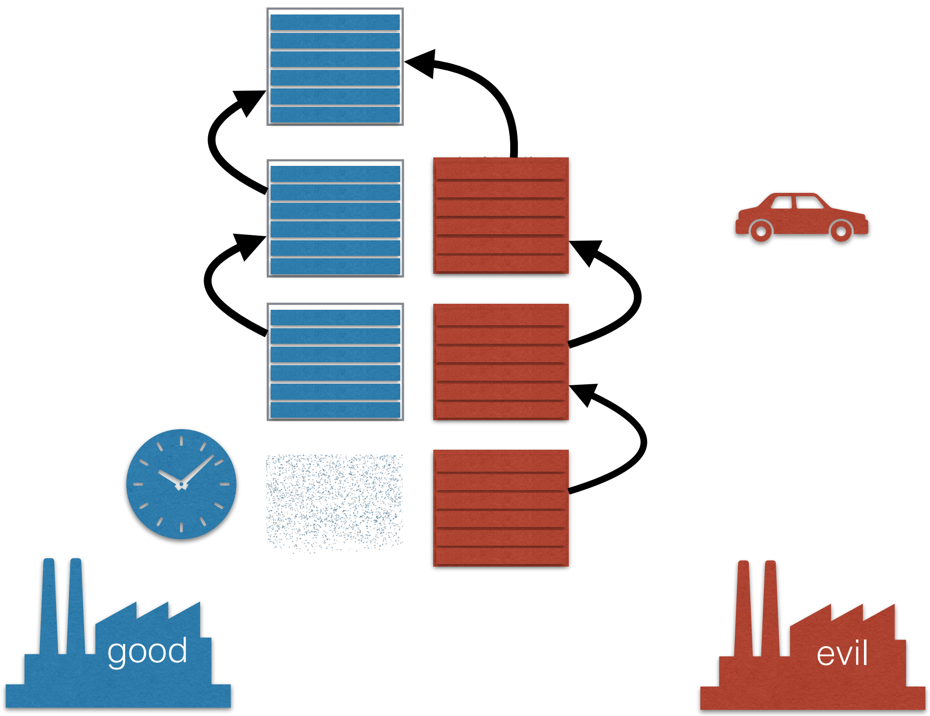





https://arxiv.org/abs/1709.08750

# Doublespend Attacks

- **Doublespend attacks** are a race between honest and attacking miners.
- Just like in the casino, there is a non-zero chance she'll win.
- She's waiting for either:
  - the honest miners to hit a sequence of unlucky block discovery times
  - for herself to hit a sequence of lucky block discovery times.

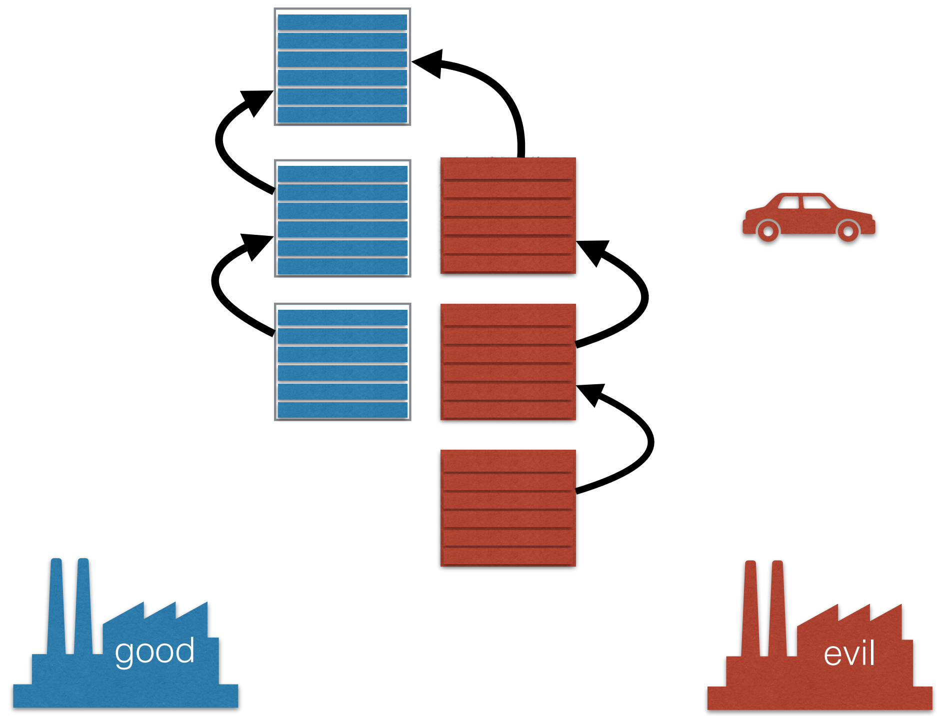





https://arxiv.org/abs/1709.08750

# Doublespend Attacks

- **Doublespend attacks** are a race between honest and attacking miners.
- Just like in the casino, there is a non-zero chance she'll win.
- She's waiting for either:
  - the honest miners to hit a sequence of unlucky block discovery times
  - for herself to hit a sequence of lucky block discovery times.

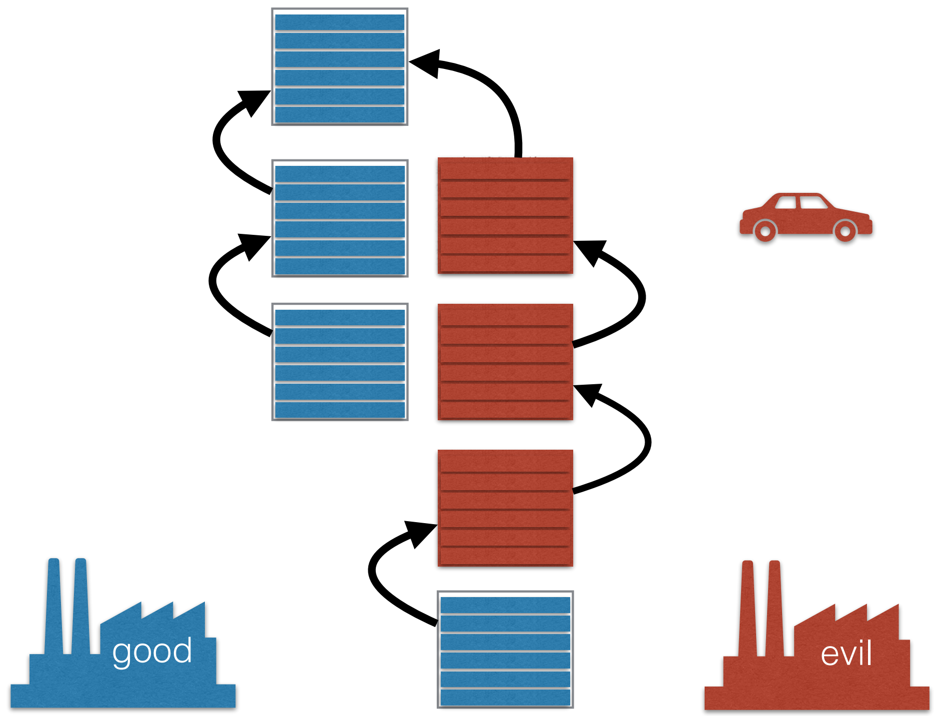





https://arxiv.org/abs/1709.08750

# Doublespend Attacks

- **Doublespend attacks** are a race between honest and attacking miners.
- Just like in the casino, there is a non-zero chance she'll win.
- She's waiting for either:
  - the honest miners to hit a sequence of unlucky block discovery times
  - for herself to hit a sequence of lucky block discovery times.

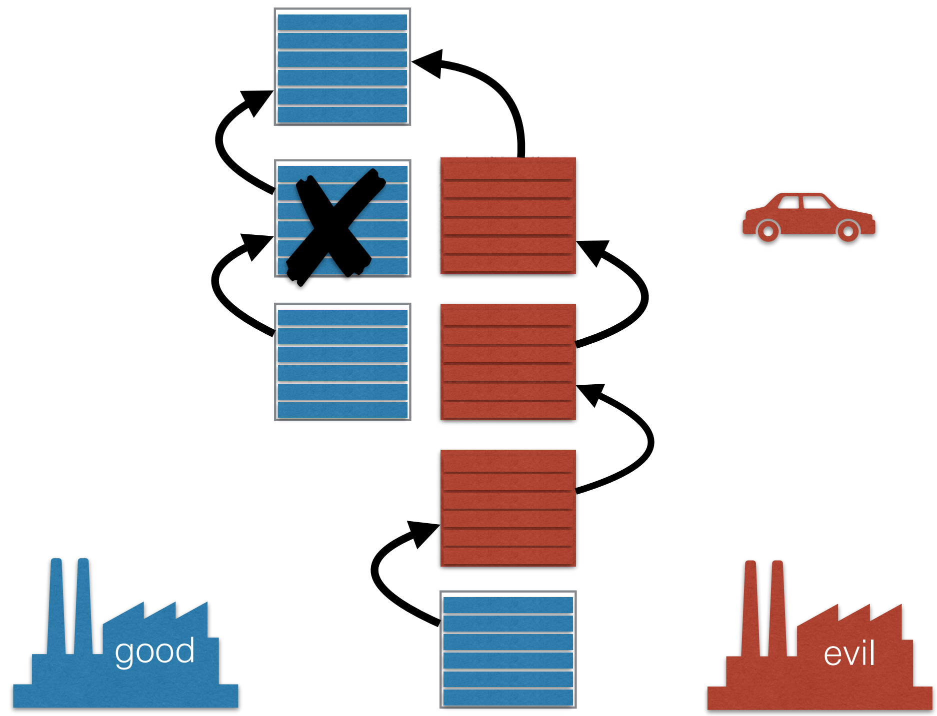





https://arxiv.org/abs/1709.08750

# Doublespend Attacks

- **Doublespend attacks** are a race between honest and attacking miners.
- Just like in the casino, there is a non-zero chance she'll win.
- She's waiting for either:
  - the honest miners to hit a sequence of unlucky block discovery times
  - for herself to hit a sequence of lucky block discovery times.

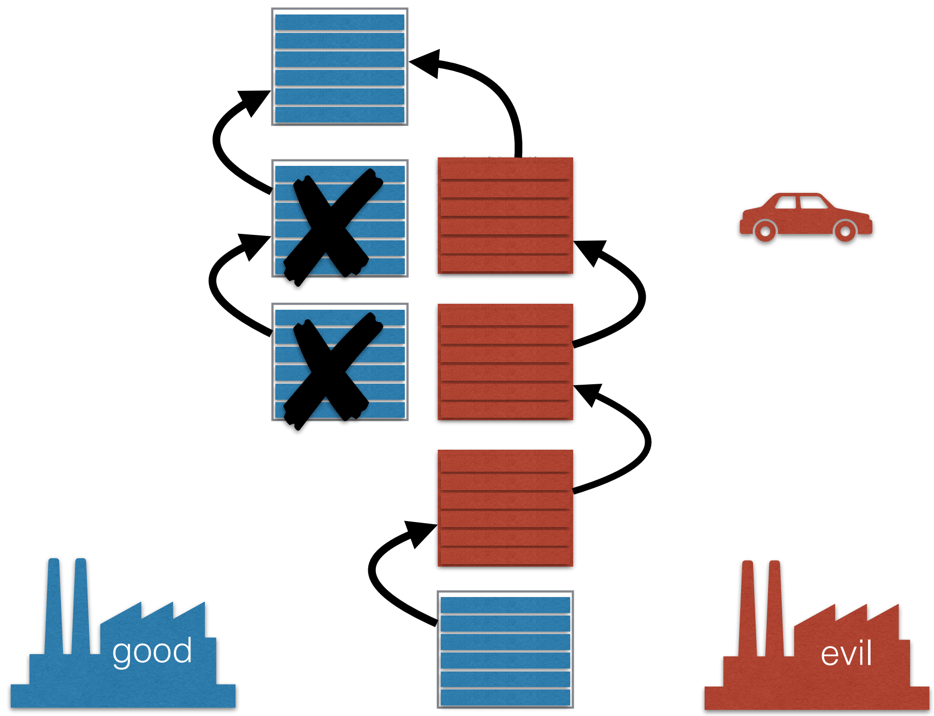





https://arxiv.org/abs/1709.08750

# Doublespend Attacks

- **Doublespend attacks** are a race between honest and attacking miners.
- Just like in the casino, there is a non-zero chance she'll win.
- She's waiting for either:
  - the honest miners to hit a sequence of unlucky block discovery times
  - for herself to hit a sequence of lucky block discovery times.





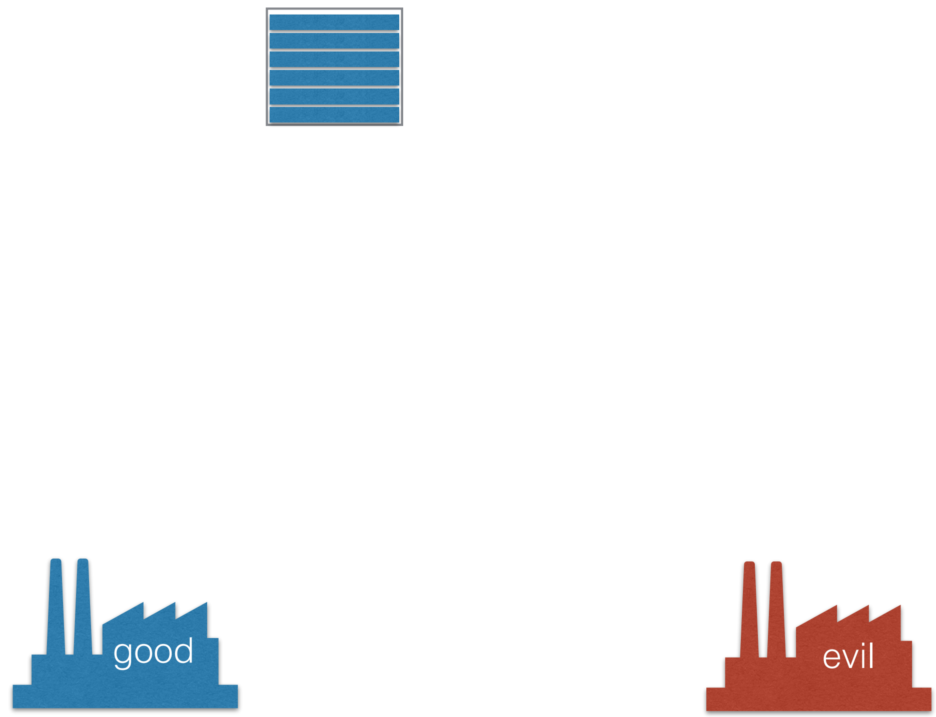

https://arxiv.org/abs/1709.08750

# Selfish Mining Attacks

- **Selfish mining attacks** have the same story.

- Several countries are considering launching blockchains
  - Some countries are starting to not like them.

- What is the current defense against Nation/state-based SM attacks on a currency?

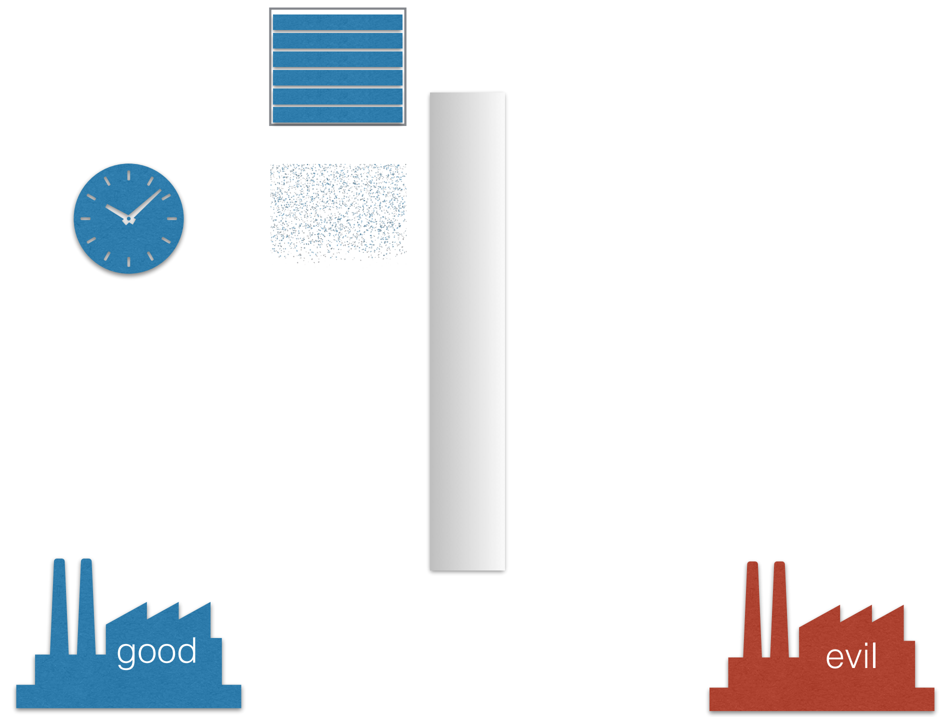





https://arxiv.org/abs/1709.08750

# Selfish Mining Attacks

- **Selfish mining attacks** have the same story.
- Several countries are considering launching blockchains
  - Some countries are starting to not like them.
- What is the current defense against Nation/state-based SM attacks on a currency?

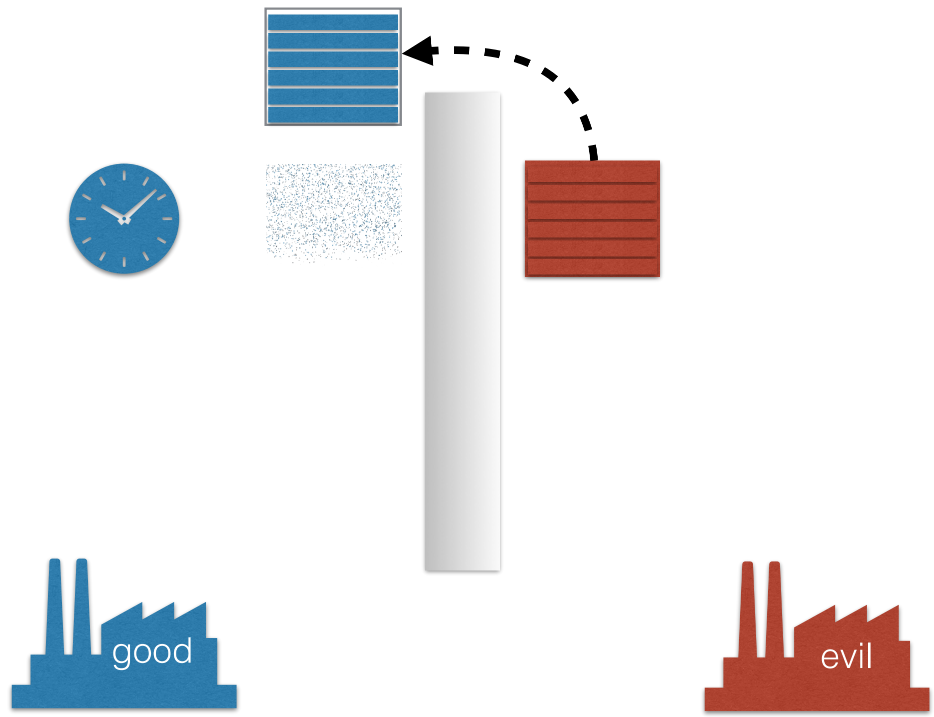





https://arxiv.org/abs/1709.08750

# Selfish Mining Attacks

- **Selfish mining attacks** have the same story.
- Several countries are considering launching blockchains
  - Some countries are starting to not like them.
- What is the current defense against Nation/state-based SM attacks on a currency?

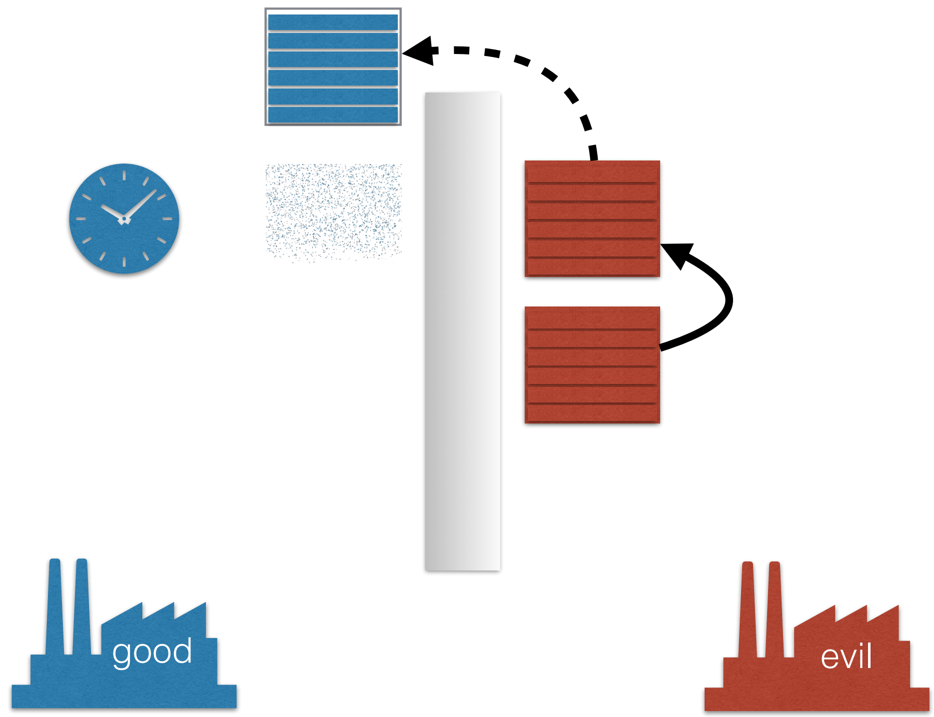





https://arxiv.org/abs/1709.08750

# Selfish Mining Attacks

- **Selfish mining attacks** have the same story.
- Several countries are considering launching blockchains
    - Some countries are starting to not like them.
- What is the current defense against Nation/state-based SM attacks on a currency?

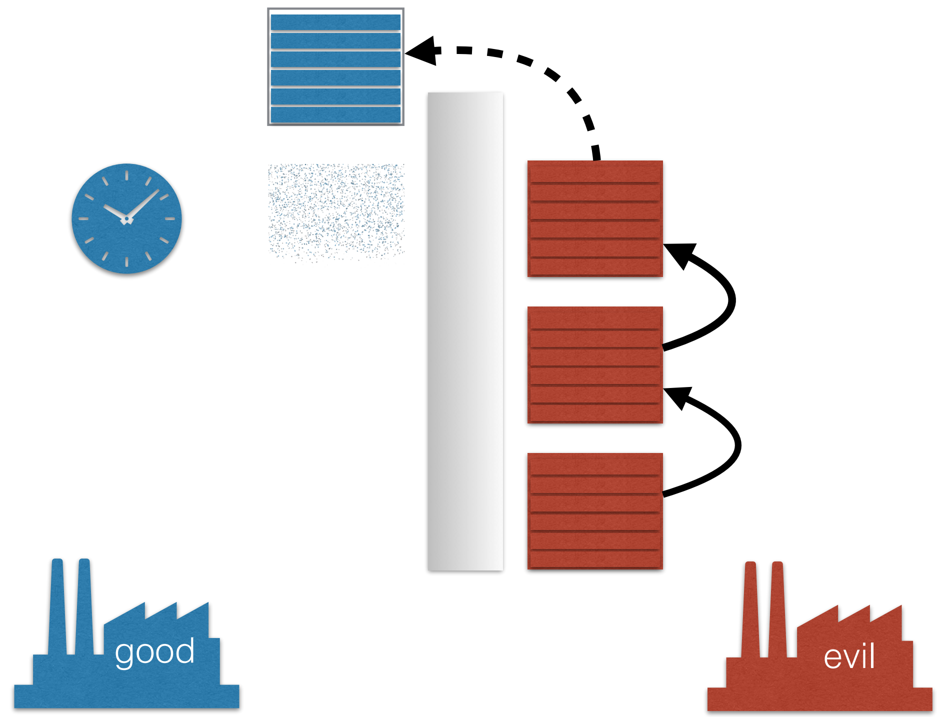





https://arxiv.org/abs/1709.08750

# Selfish Mining Attacks

- **Selfish mining attacks** have the same story.
- Several countries are considering launching blockchains
    - Some countries are starting to not like them.
- What is the current defense against Nation/state-based SM attacks on a currency?

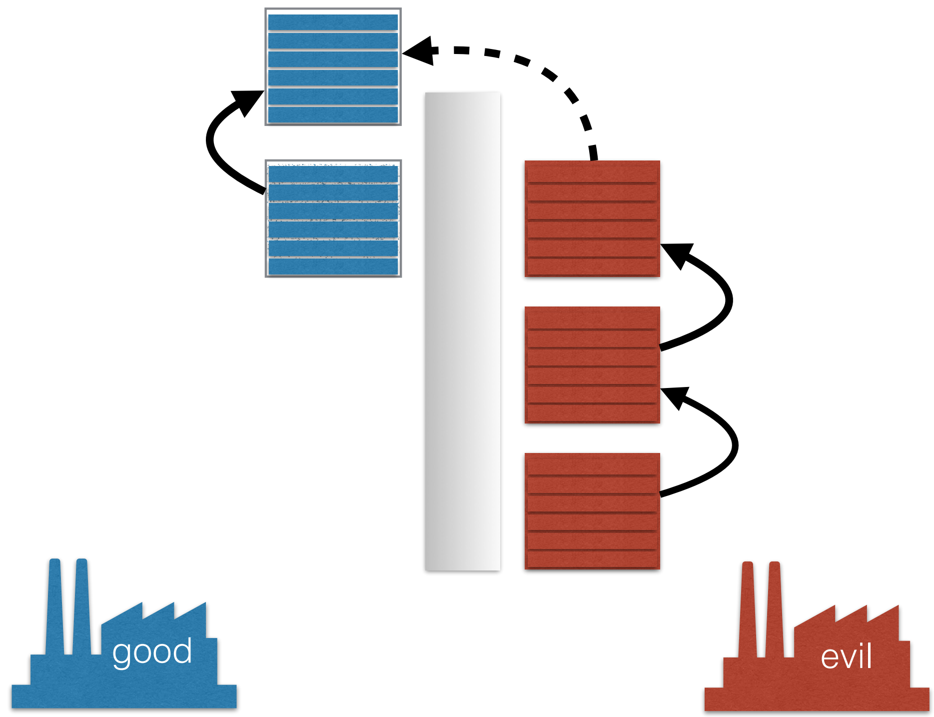





https://arxiv.org/abs/1709.08750

# Selfish Mining Attacks

- **Selfish mining attacks** have the same story.
- Several countries are considering launching blockchains
    - Some countries are starting to not like them.
- What is the current defense against Nation/state-based SM attacks on a currency?

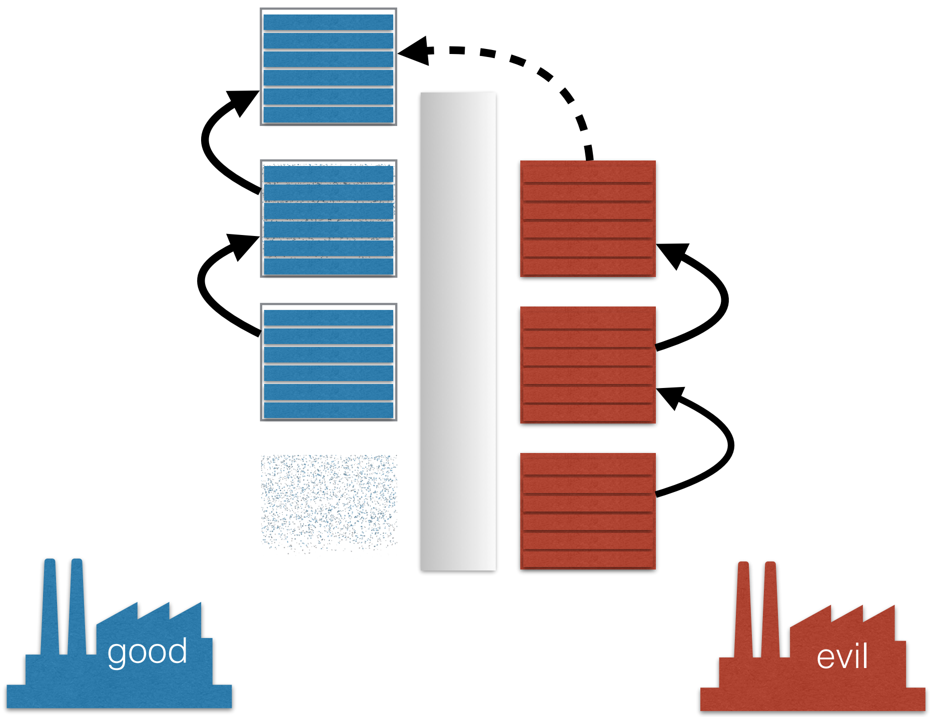





https://arxiv.org/abs/1709.08750

# Selfish Mining Attacks

- **Selfish mining attacks** have the same story.
- Several countries are considering launching blockchains
    - Some countries are starting to not like them.
- What is the current defense against Nation/state-based SM attacks on a currency?

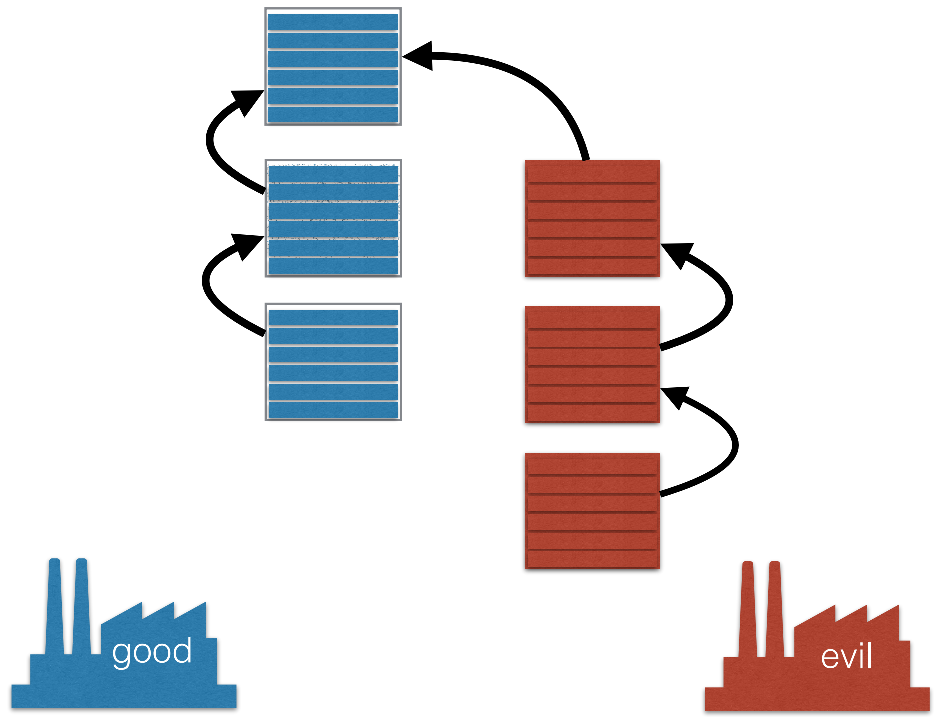





https://arxiv.org/abs/1709.08750

# Selfish Mining Attacks

- **Selfish mining attacks** have the same story.
- Several countries are considering launching blockchains
  - Some countries are starting to not like them.
- What is the current defense against Nation/state-based SM attacks on a currency?

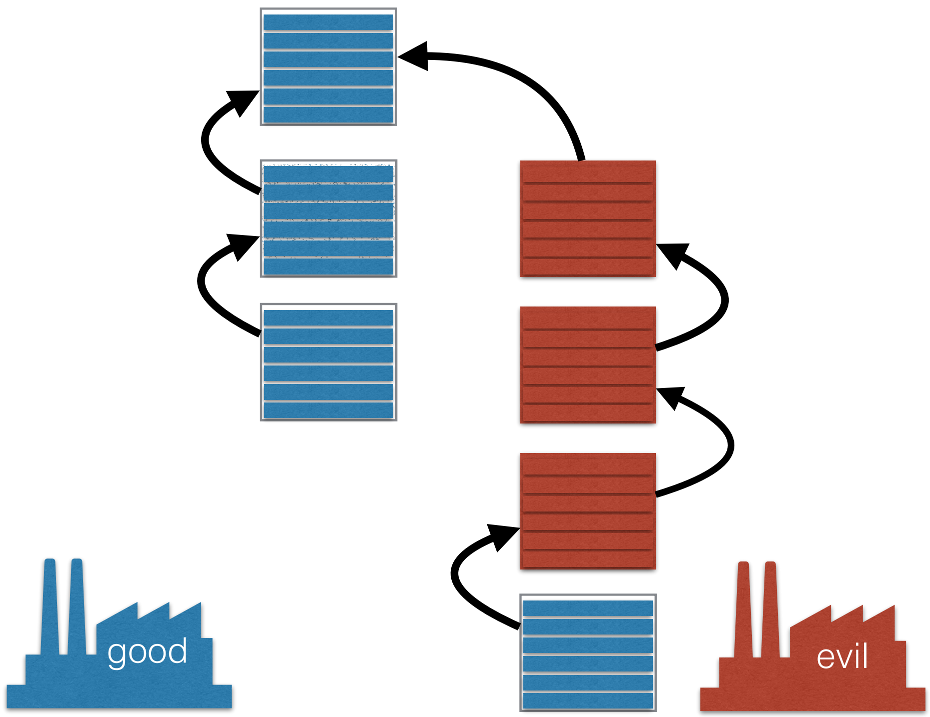





https://arxiv.org/abs/1709.08750

# Selfish Mining Attacks

- **Selfish mining attacks** have the same story.
- Several countries are considering launching blockchains
  - Some countries are starting to not like them.
- What is the current defense against Nation/state-based SM attacks on a currency?

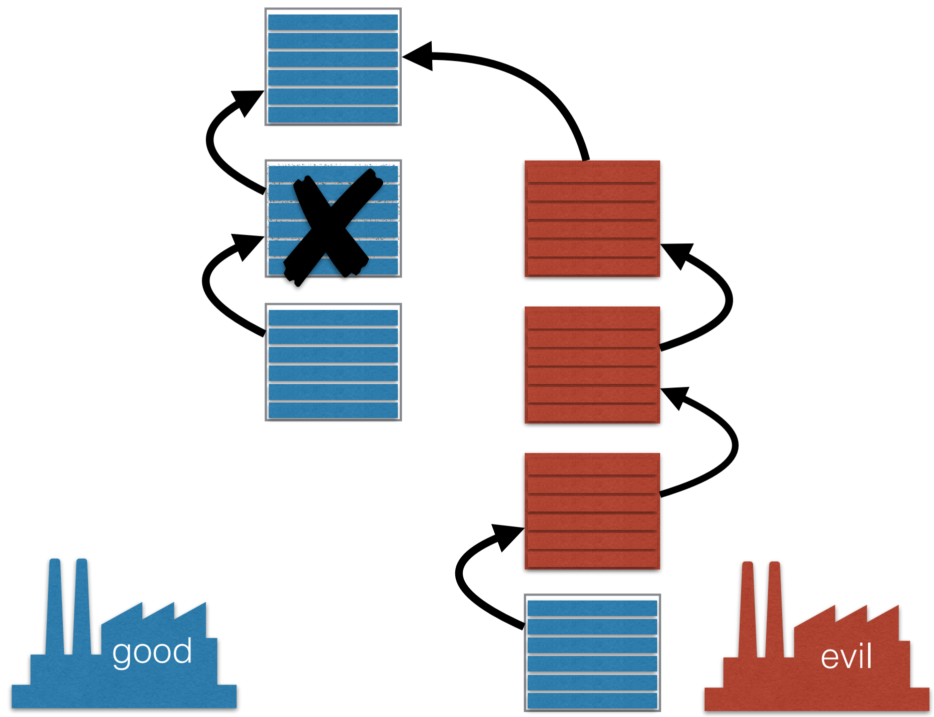





https://arxiv.org/abs/1709.08750

# Selfish Mining Attacks

- **Selfish mining attacks** have the same story.
- Several countries are considering launching blockchains
    - Some countries are starting to not like them.
- What is the current defense against Nation/state-based SM attacks on a currency?

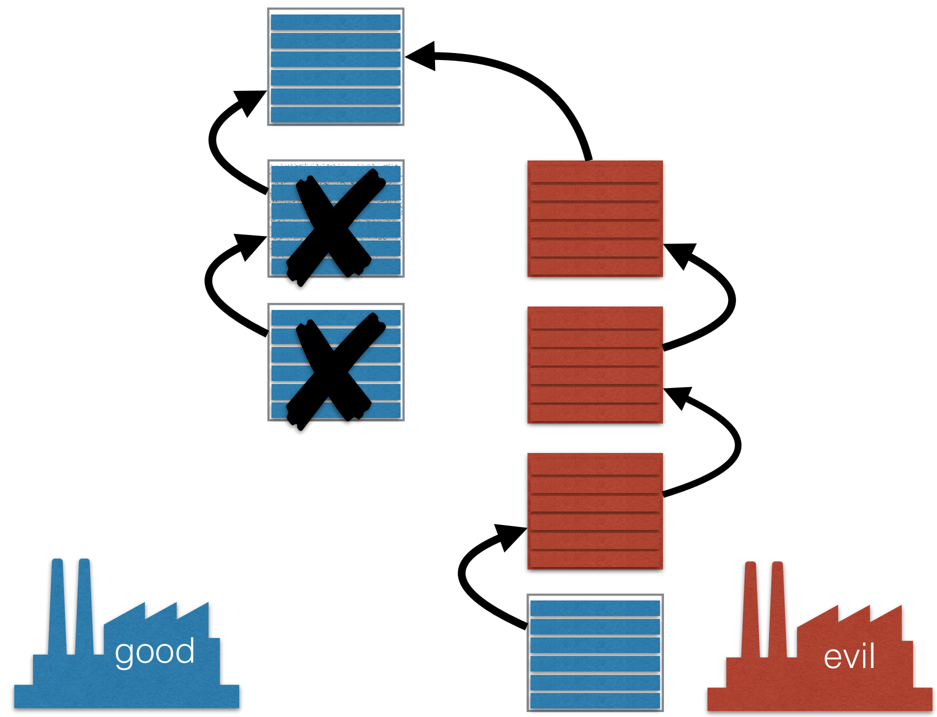





https://arxiv.org/abs/1709.08750

# Selfish Mining Attacks

- **Selfish mining attacks** have the same story.
- Several countries are considering launching blockchains
    - Some countries are starting to not like them.
- What is the current defense against Nation/state-based SM attacks on a currency?






https://arxiv.org/abs/1709.08750

# Reducing Variance in PoW Mining

- Bobtail: the mean of the ***k*-lowest samples** must be below the target.
  - The samples come from all miners.

$k = 4$

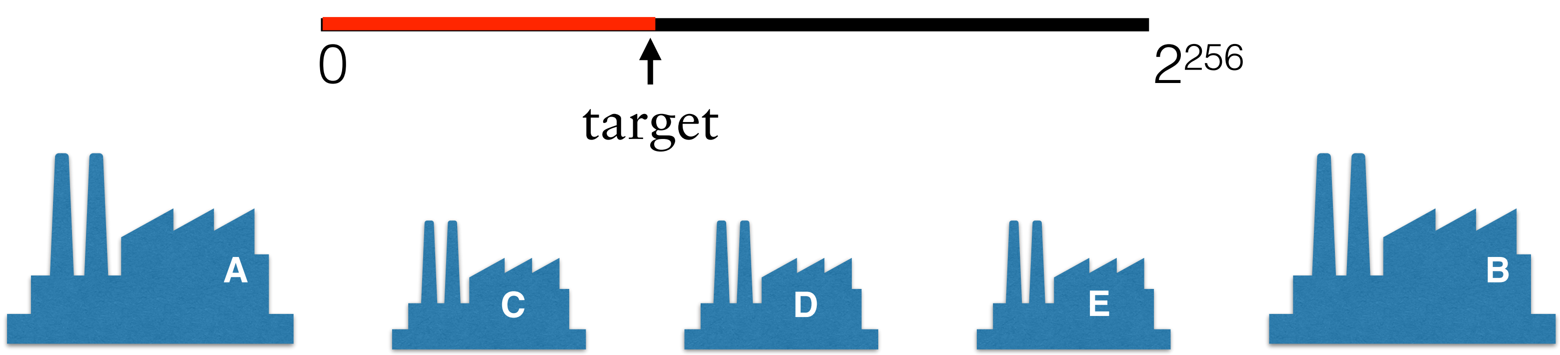



https://arxiv.org/abs/1709.08750

# Reducing Variance in PoW Mining

- Bobtail: the mean of the ***k*-lowest samples** must be below the target.
  - The samples come from all miners.

$k = 4$



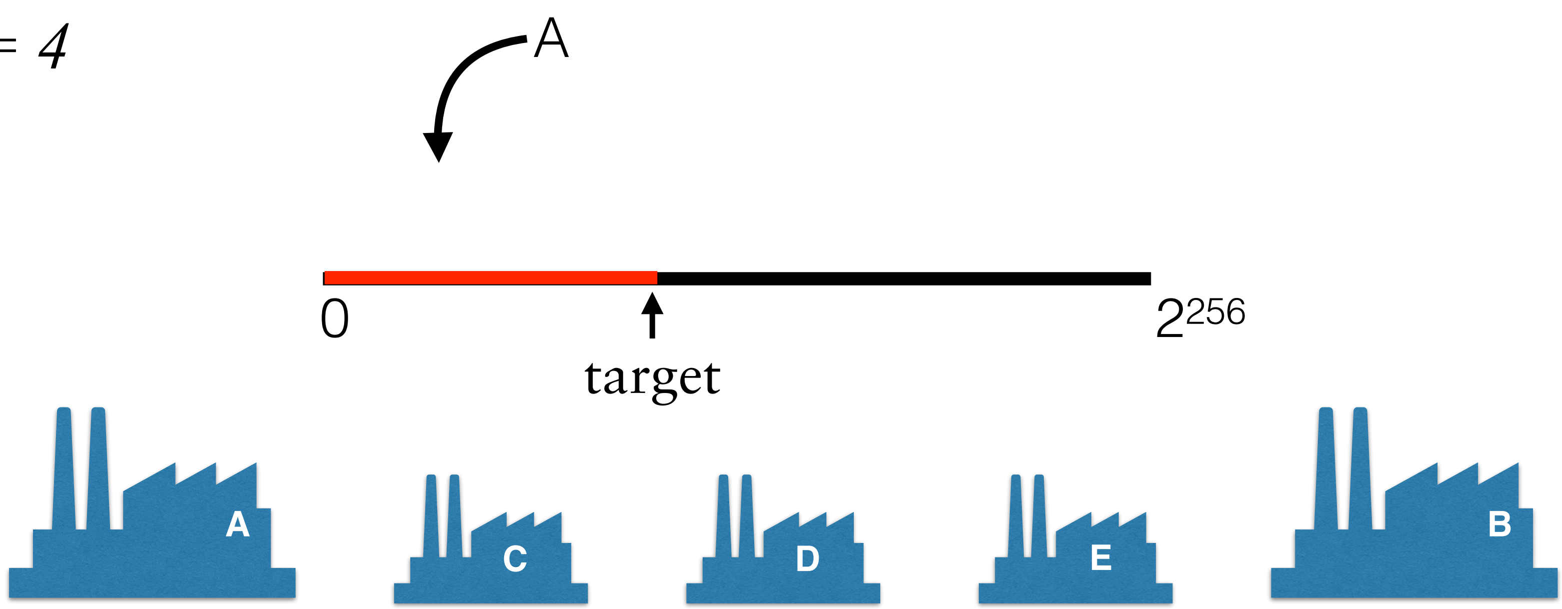



https://arxiv.org/abs/1709.08750

# Reducing Variance in PoW Mining

- Bobtail: the mean of the ***k*-lowest samples** must be below the target.
  - The samples come from all miners.

$k = 4$



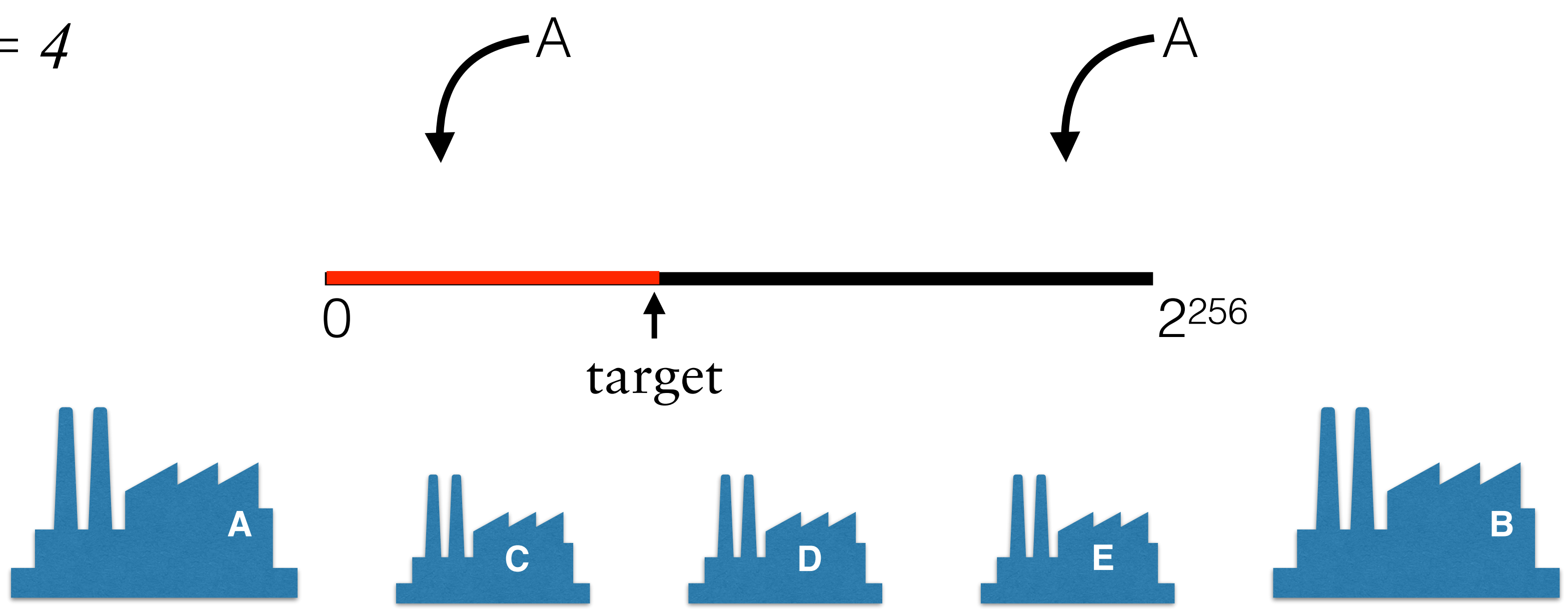



https://arxiv.org/abs/1709.08750

# Reducing Variance in PoW Mining

- Bobtail: the mean of the ***k*-lowest samples** must be below the target.
  - The samples come from all miners.

$k = 4$

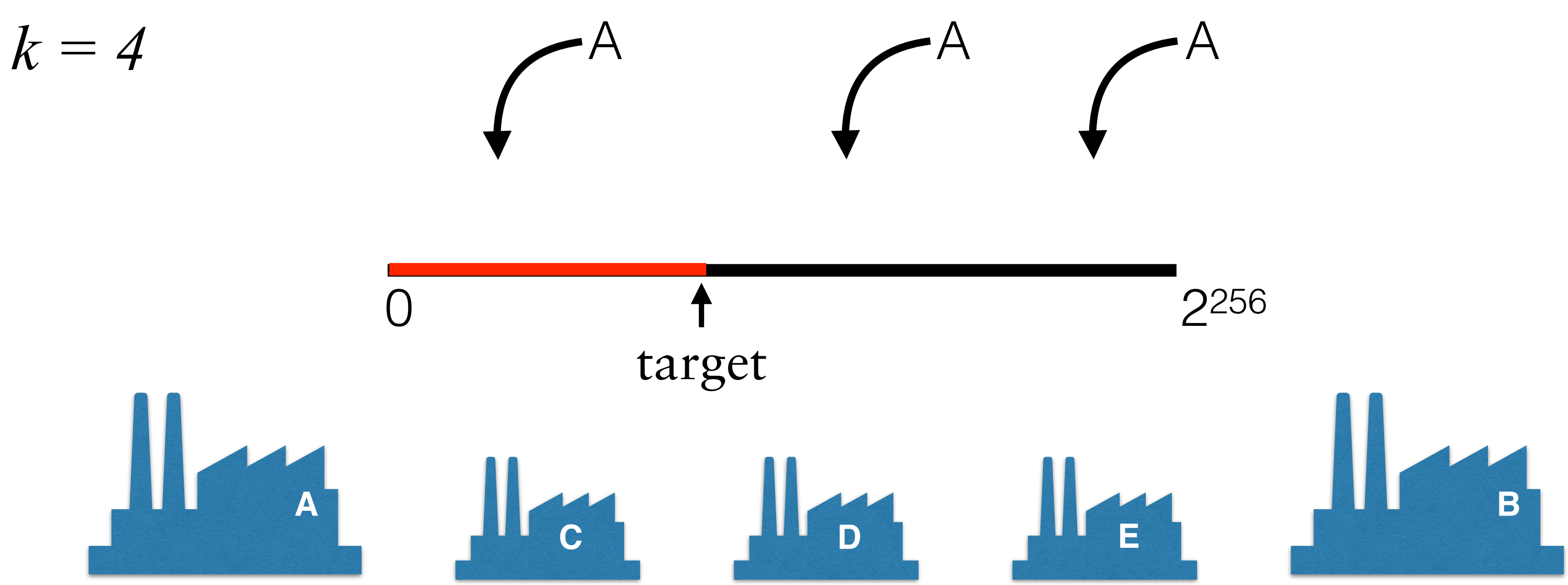





https://arxiv.org/abs/1709.08750

# Reducing Variance in PoW Mining

- Bobtail: the mean of the ***k*-lowest samples** must be below the target.
  - The samples come from all miners.

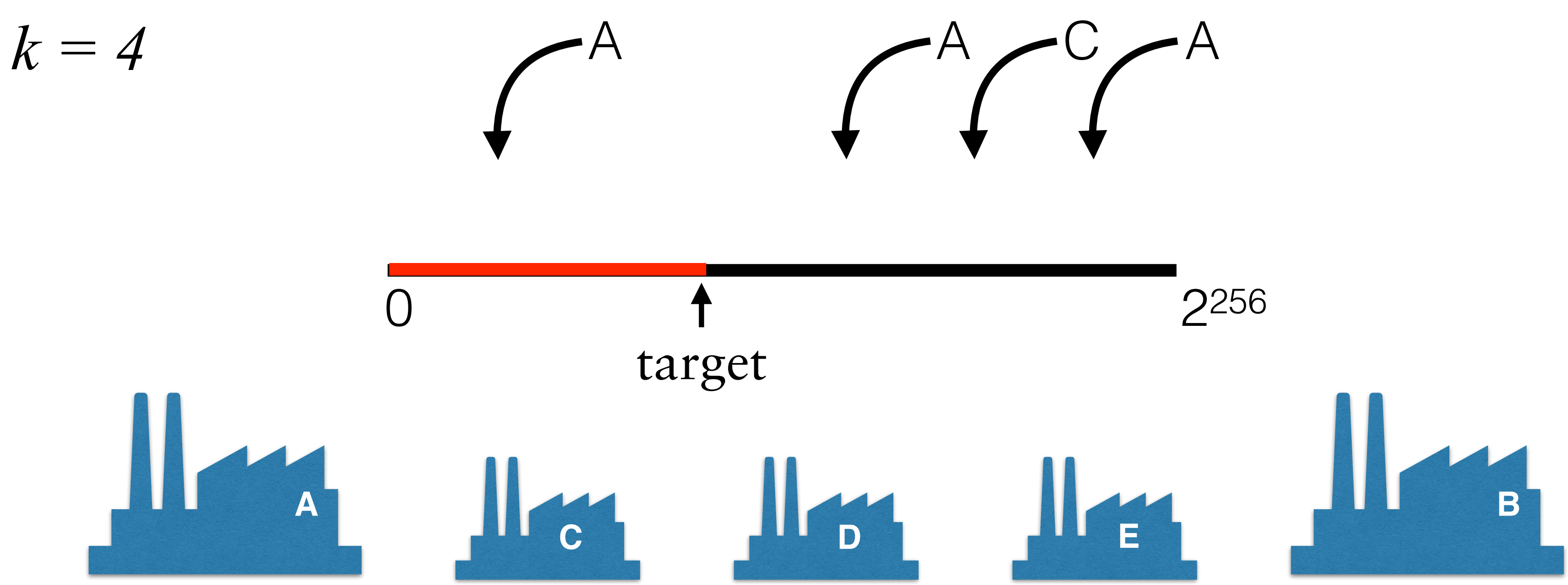





https://arxiv.org/abs/1709.08750

# Reducing Variance in PoW Mining

- Bobtail: the mean of the ***k*-lowest samples** must be below the target.
  - The samples come from all miners.



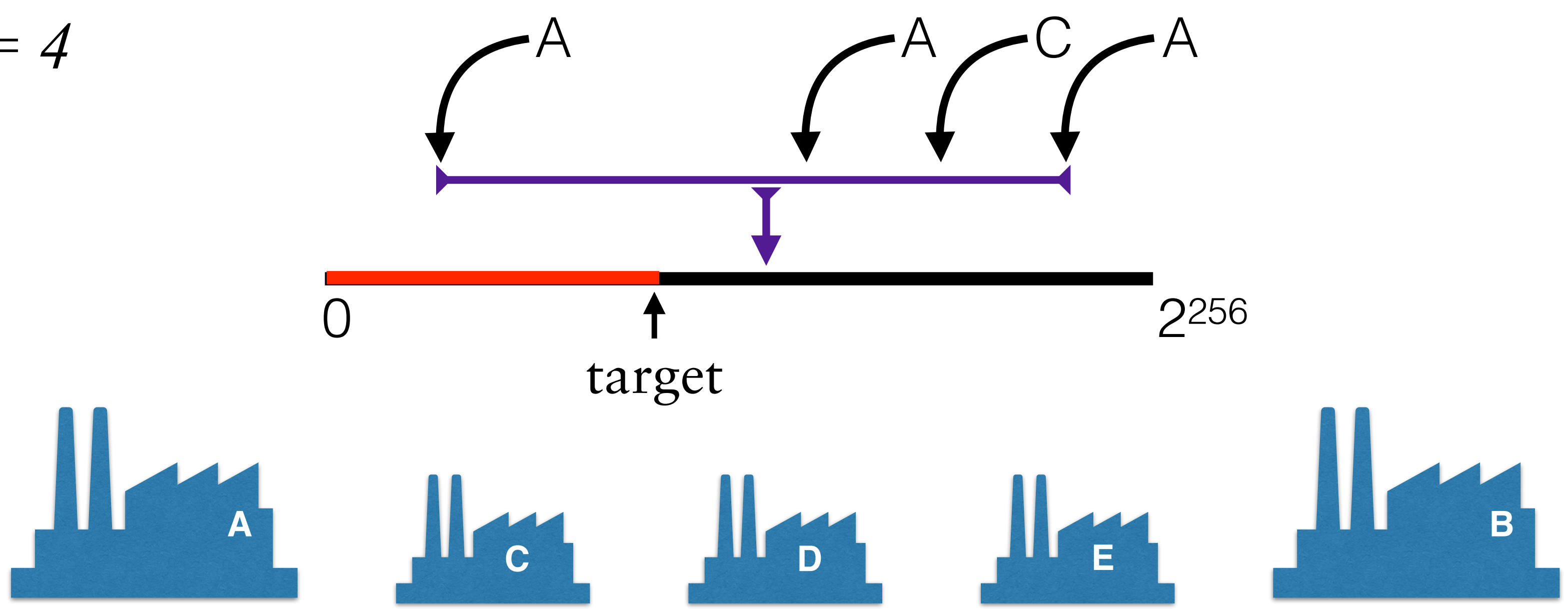



https://arxiv.org/abs/1709.08750

# Reducing Variance in PoW Mining

- Bobtail: the mean of the ***k*-lowest samples** must be below the target.
  - The samples come from all miners.

$k = 4$



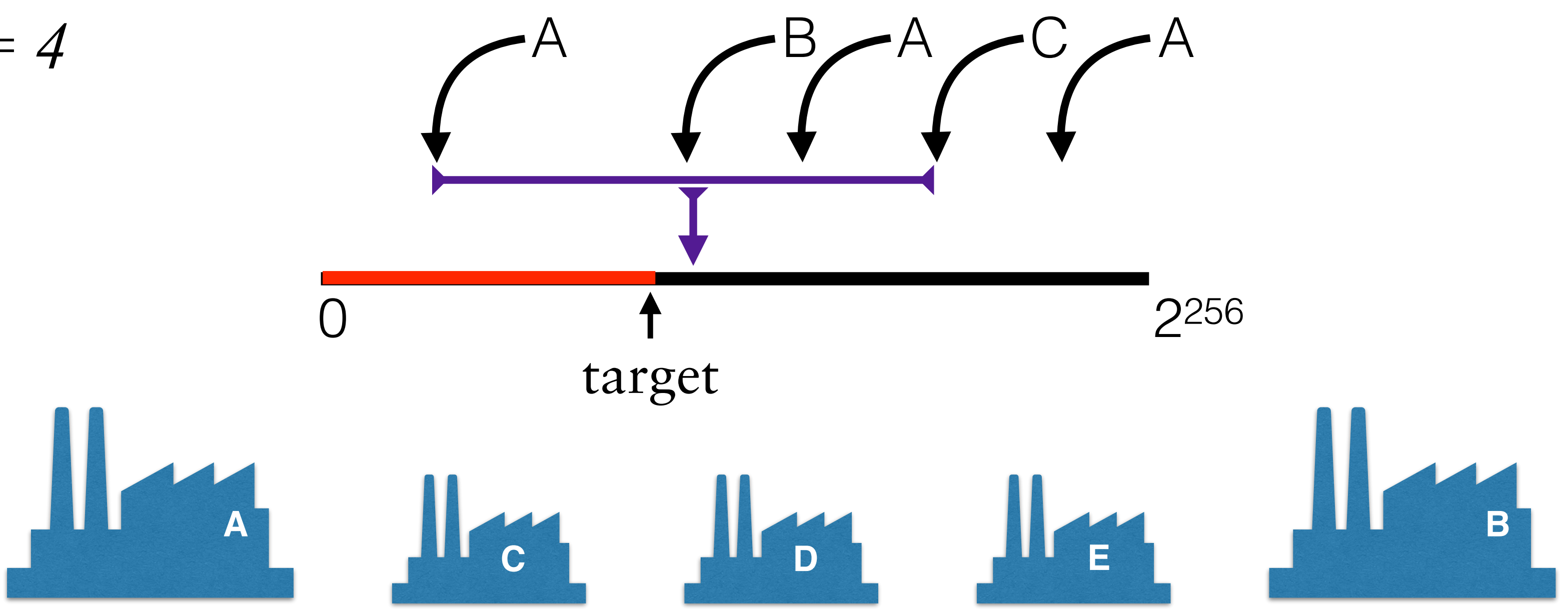



https://arxiv.org/abs/1709.08750

# Reducing Variance in PoW Mining

- Bobtail: the mean of the ***k*-lowest samples** must be below the target.
  - The samples come from all miners.

$k = 4$



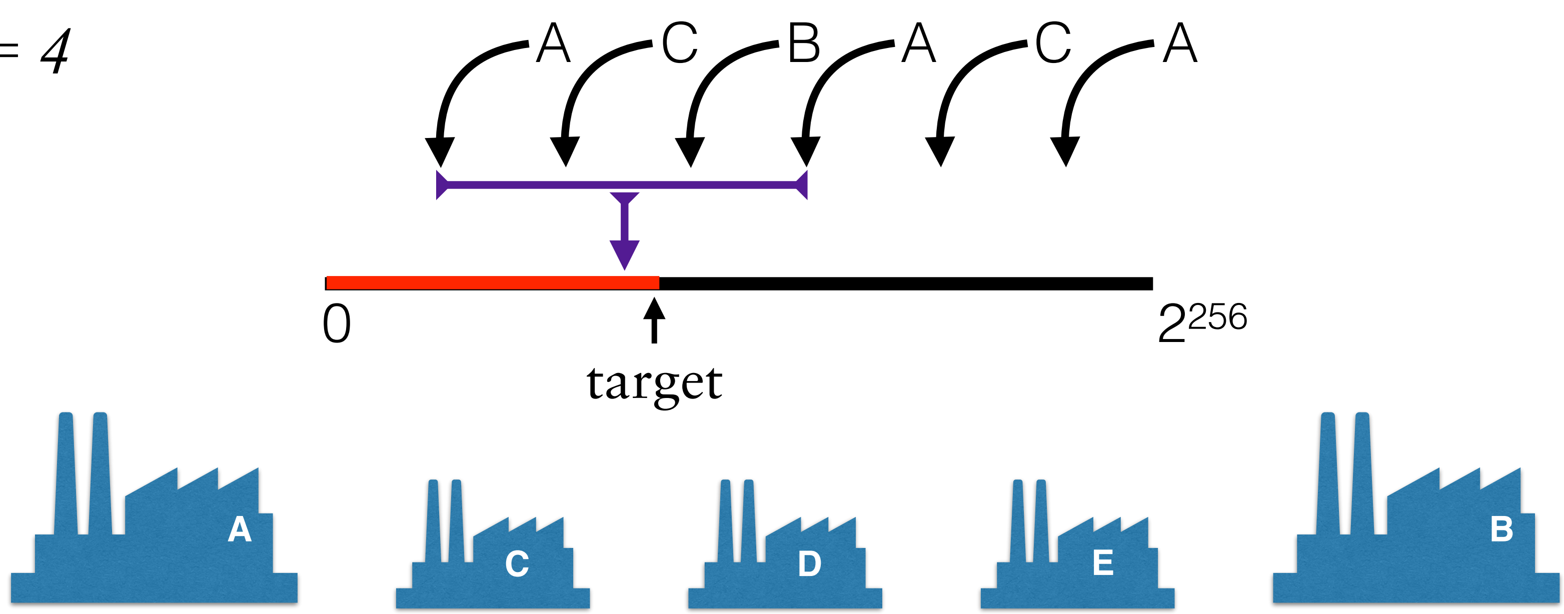



https://arxiv.org/abs/1709.08750

# Reducing Variance in PoW Mining

- Bobtail: the mean of the ***k*-lowest samples** must be below the target.
  - The samples come from all miners.

$k = 4$



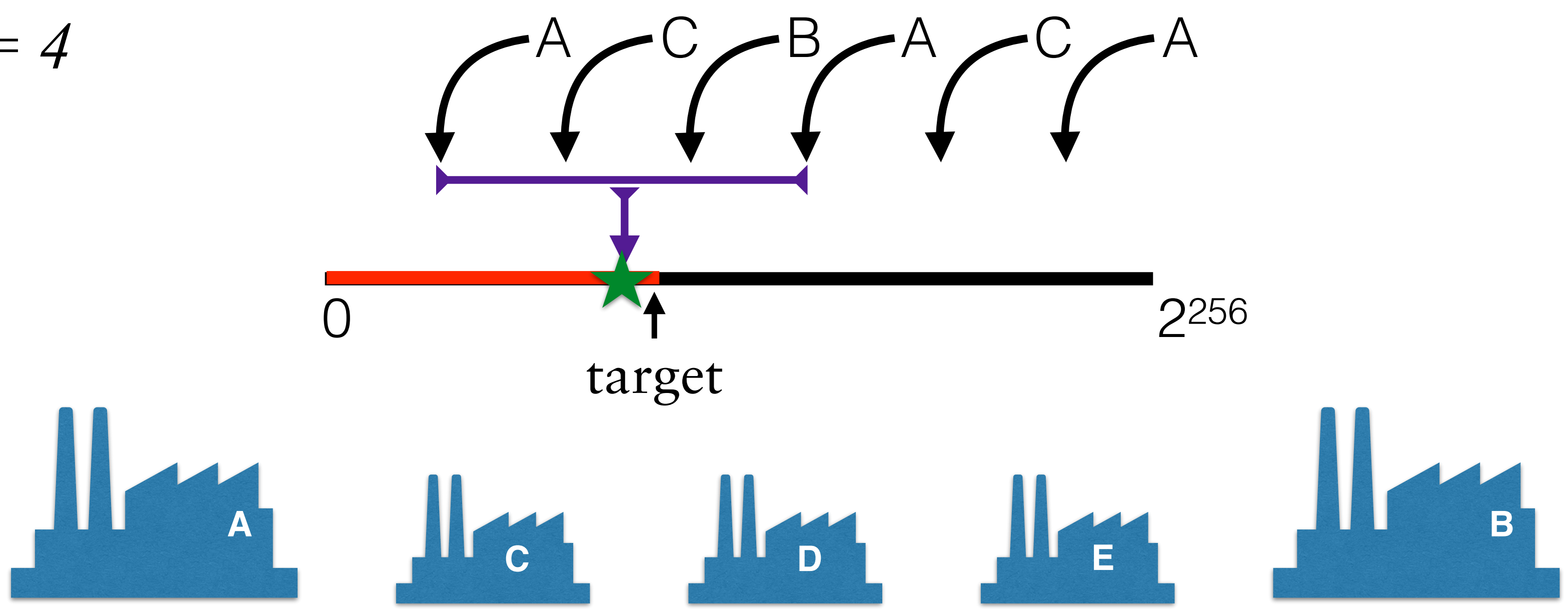



https://arxiv.org/abs/1709.08750

# Reducing Variance in PoW Mining

- Bobtail: the mean of the ***k*-lowest samples** must be below the target.
  - The samples come from all miners.

$k = 4$






https://arxiv.org/abs/1709.08750

# Reducing Variance in PoW Mining

- Target is adjusted so there is no change in the expected number of samples.

$$t_k = \frac{t_1(k+1)}{2}$$

  - k can be raised or lowered from one block to the next without issues.

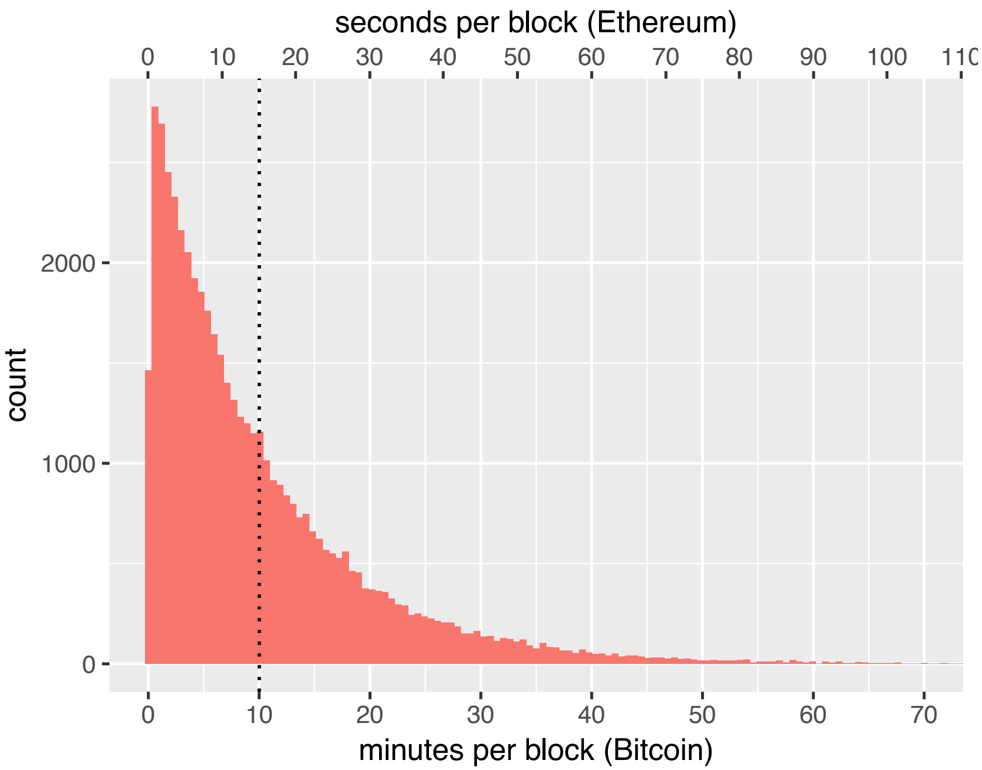
- This is basic applied statistics:
  - if you want a better estimate, take more samples.
  - Compared to Bitcoin, variance of inter-block time is reduced:

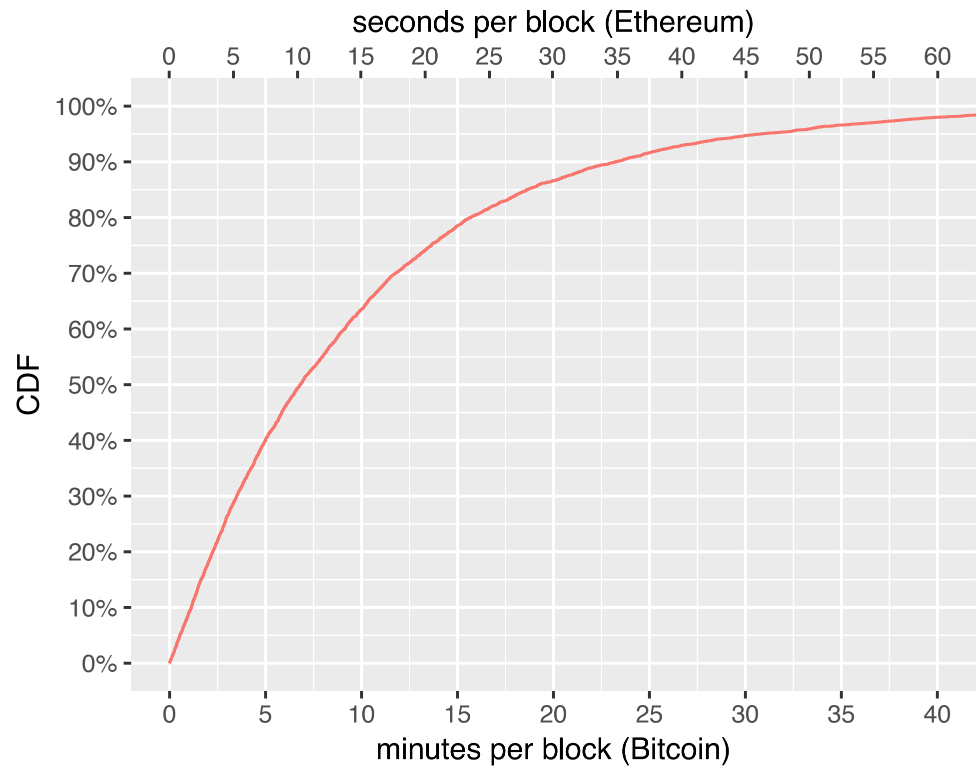
Reduction in variance: $$\frac{8k+4}{6(k^2+k)} = O\left(\frac{1}{k}\right)$$



https://arxiv.org/abs/1709.08750

# Problem Definition



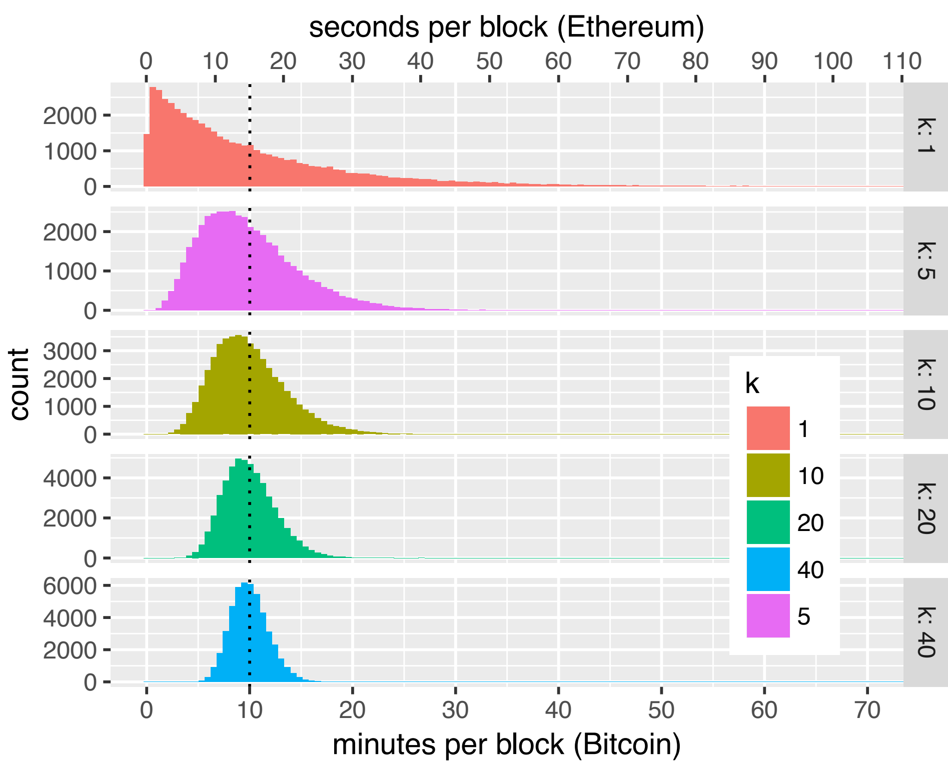



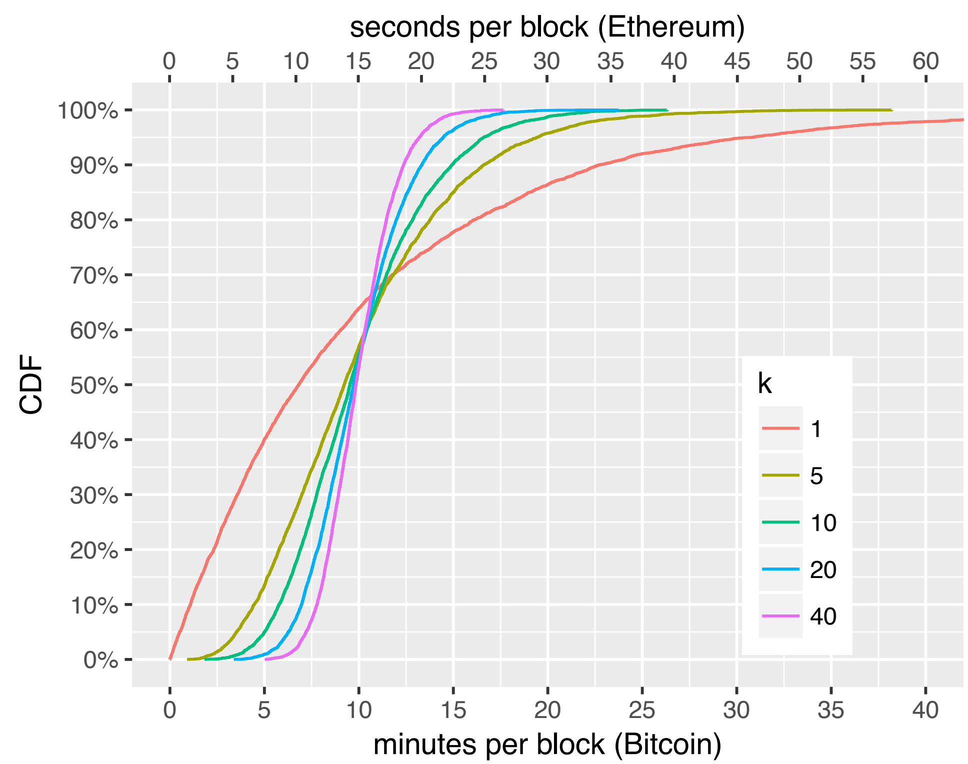

5% of blocks take at least 30 minutes
80% of blocks are between 1–24 minutes



https://arxiv.org/abs/1709.08750

# Problem Definition



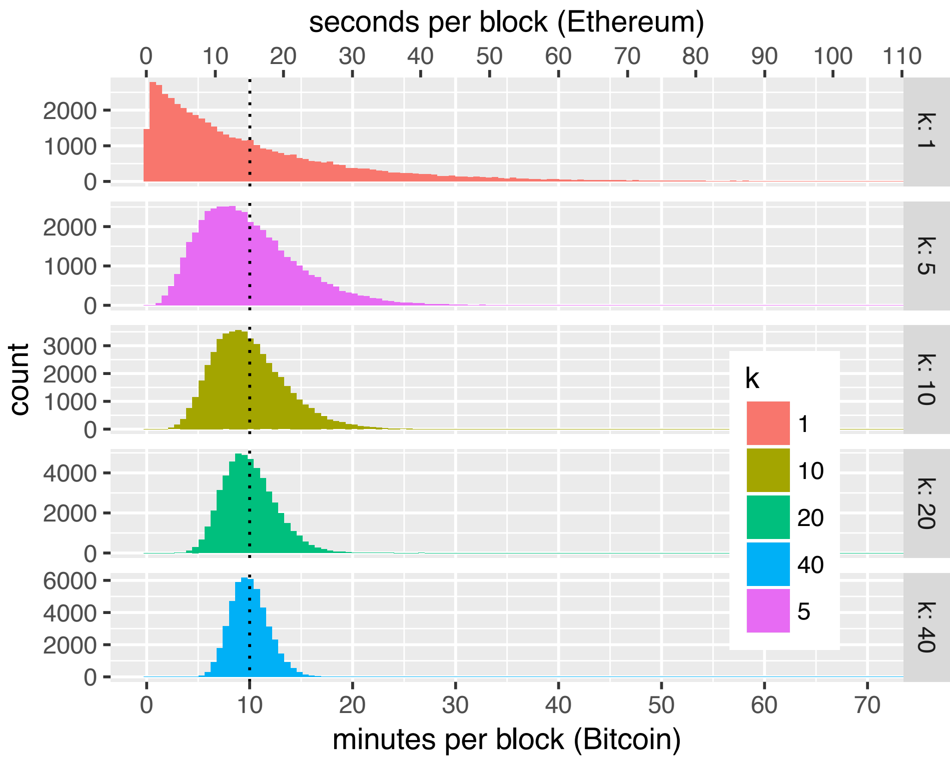



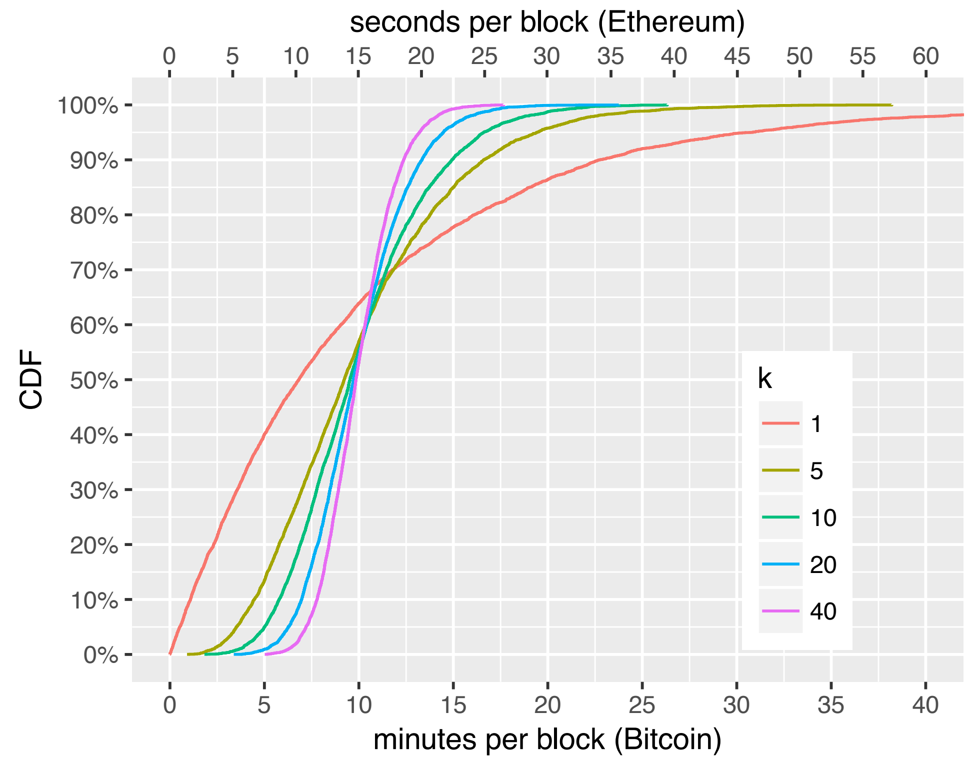

5% of blocks take at least 30 minutes
80% of blocks are between 1–24 minutes



https://arxiv.org/abs/1709.08750

# Problem Definition




5% of blocks take at least 30 minutes
80% of blocks are between 1–24 minutes

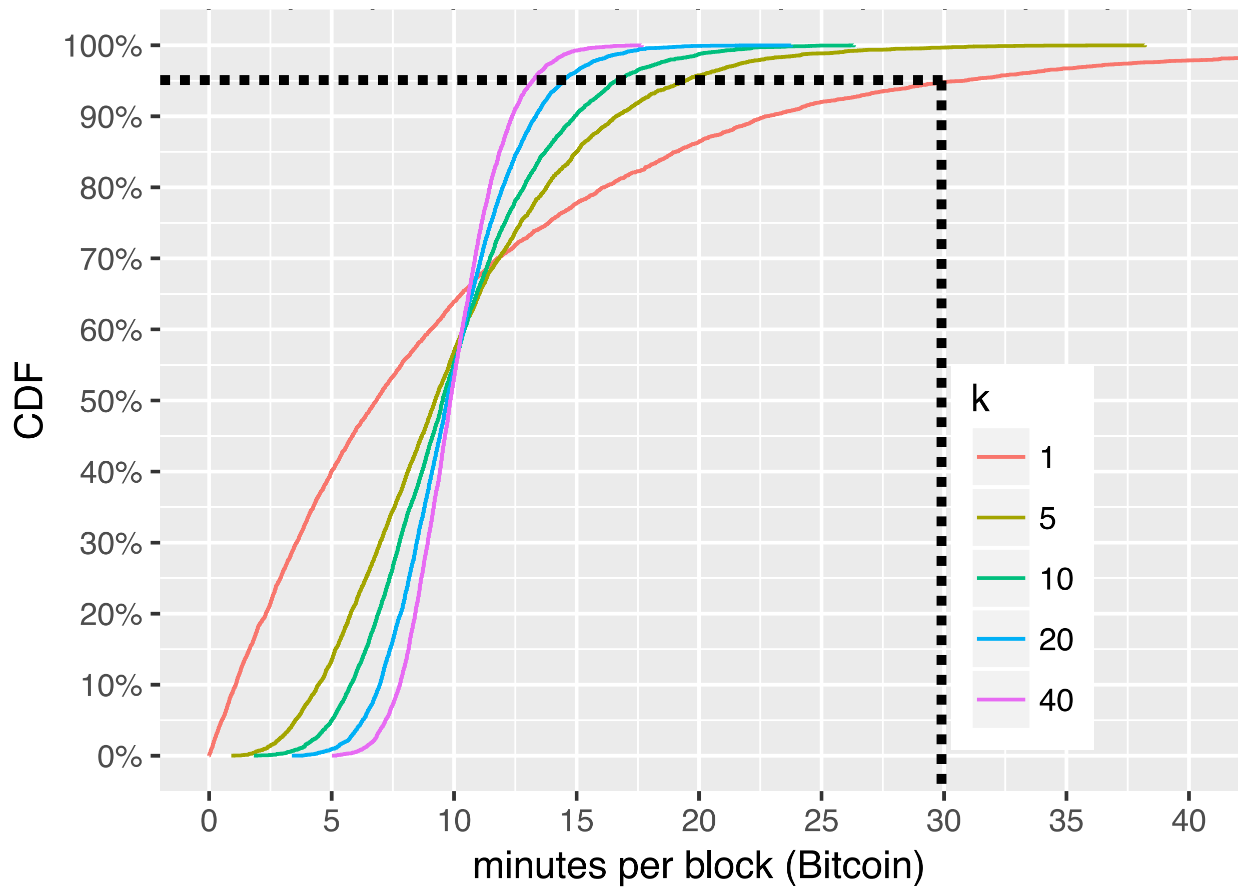


https://arxiv.org/abs/1709.08750

# Problem Definition

For Bitcoin now (k=1):

- Worst 5% of blocks take 30–70 minutes.





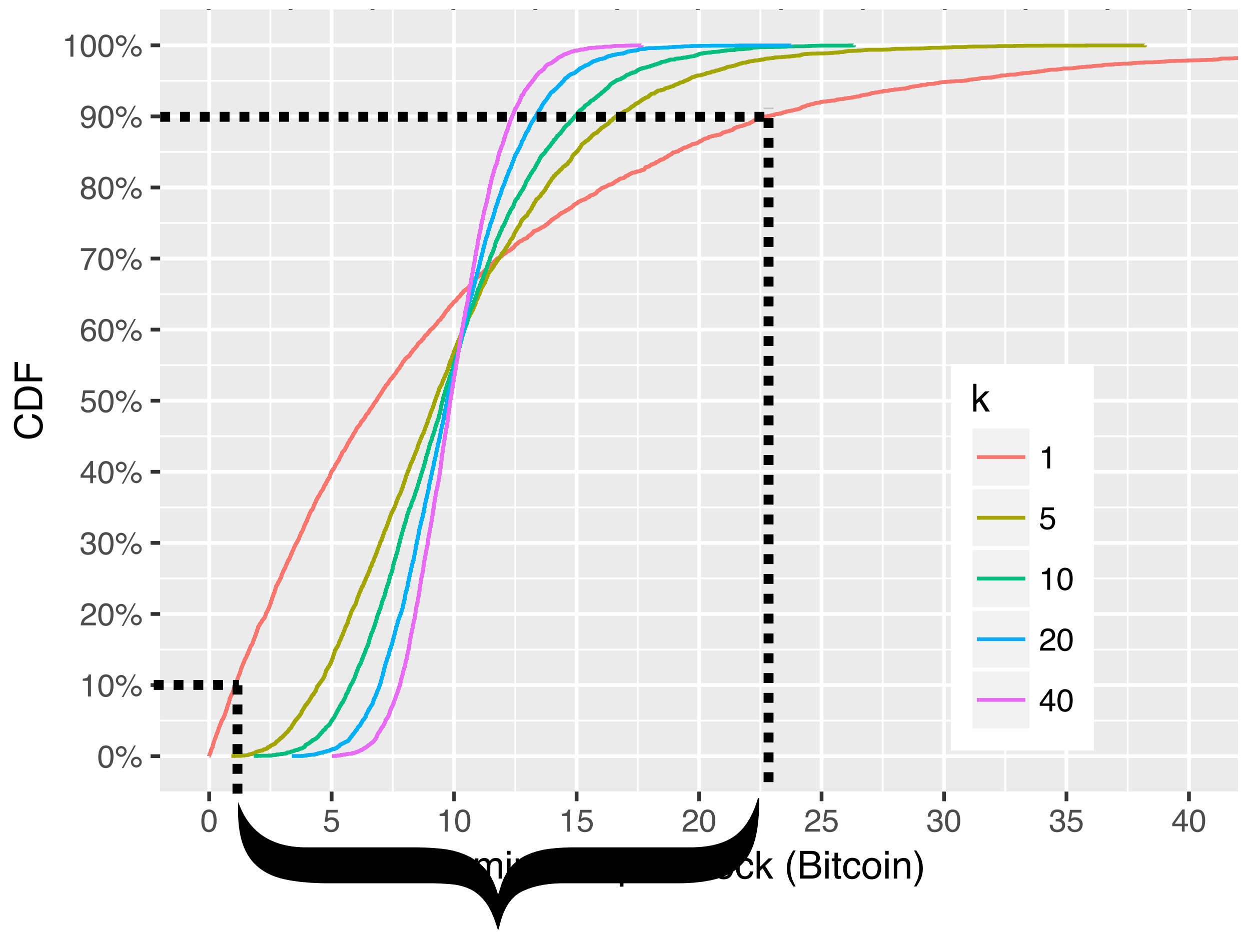

https://arxiv.org/abs/1709.08750

# Problem Definition

For Bitcoin now (k=1):

- Worst 5% of blocks take 30–70 minutes.

- Middle 80% of blocks take 1–24 minutes.

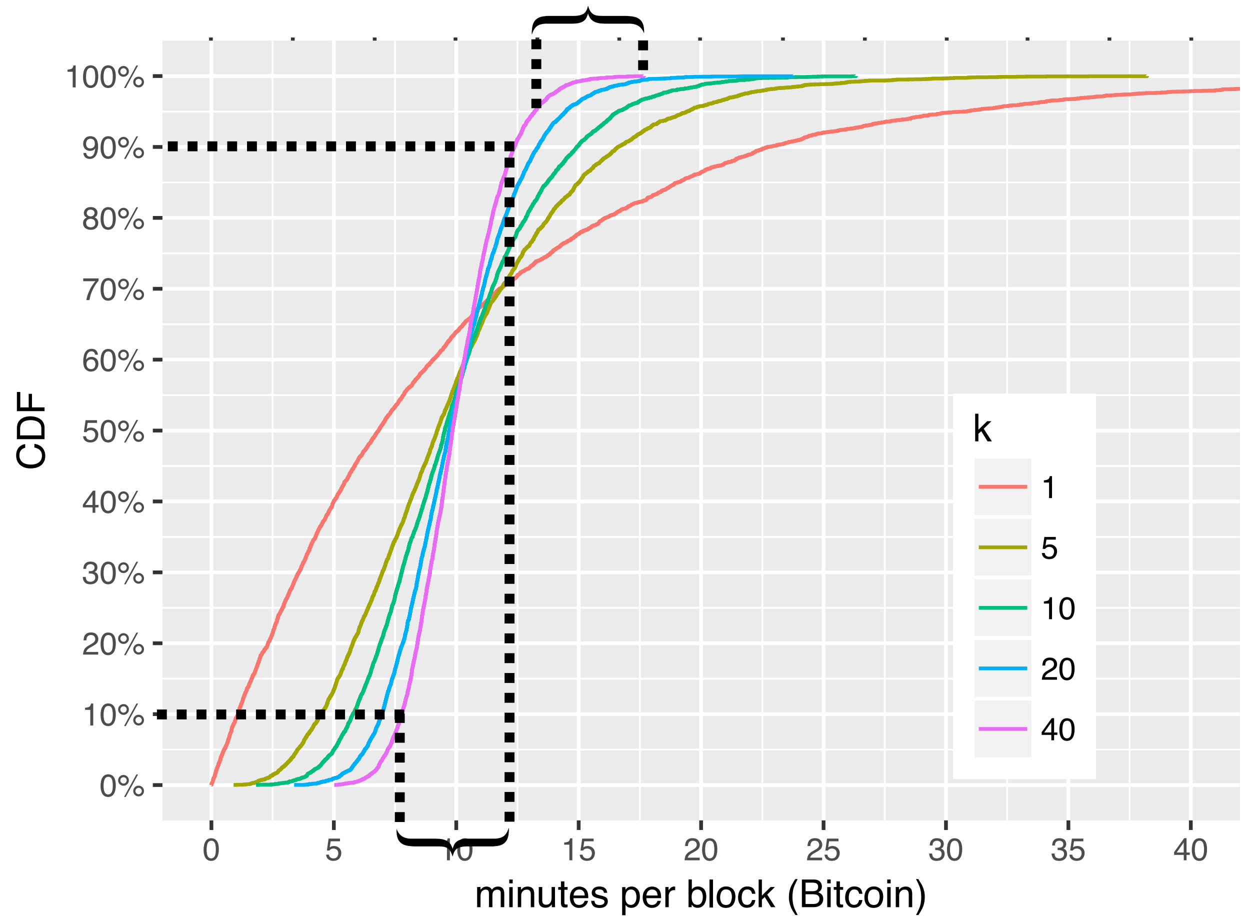



https://arxiv.org/abs/1709.08750

# Problem Definition

For *k=40*:

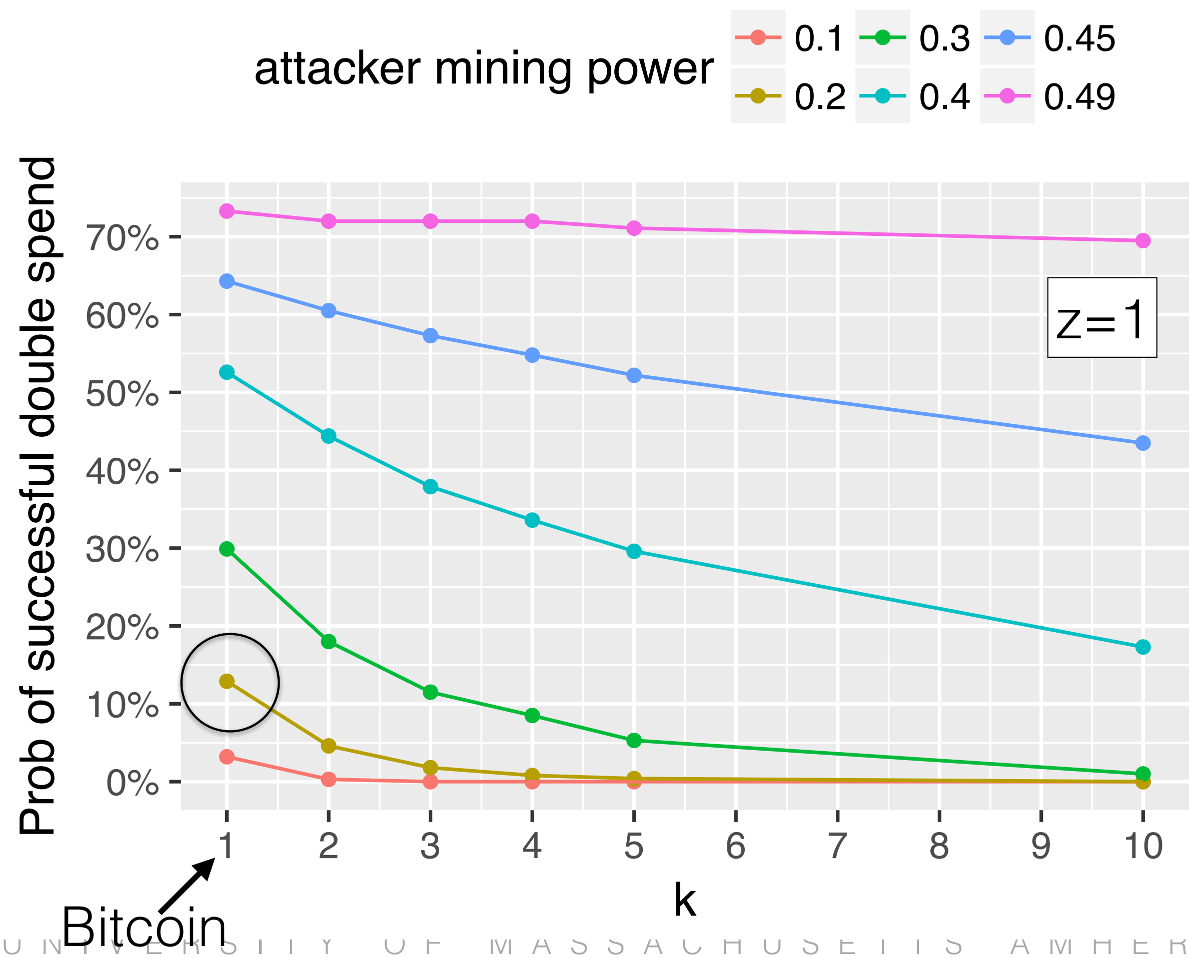
- Worst 5% of blocks take 13–18 minutes.
    - eclipse attacks are trivial to detect.
- Middle 80% of blocks take 7–12 minutes.






https://arxiv.org/abs/1709.08750

# Increased Security: Doublespend



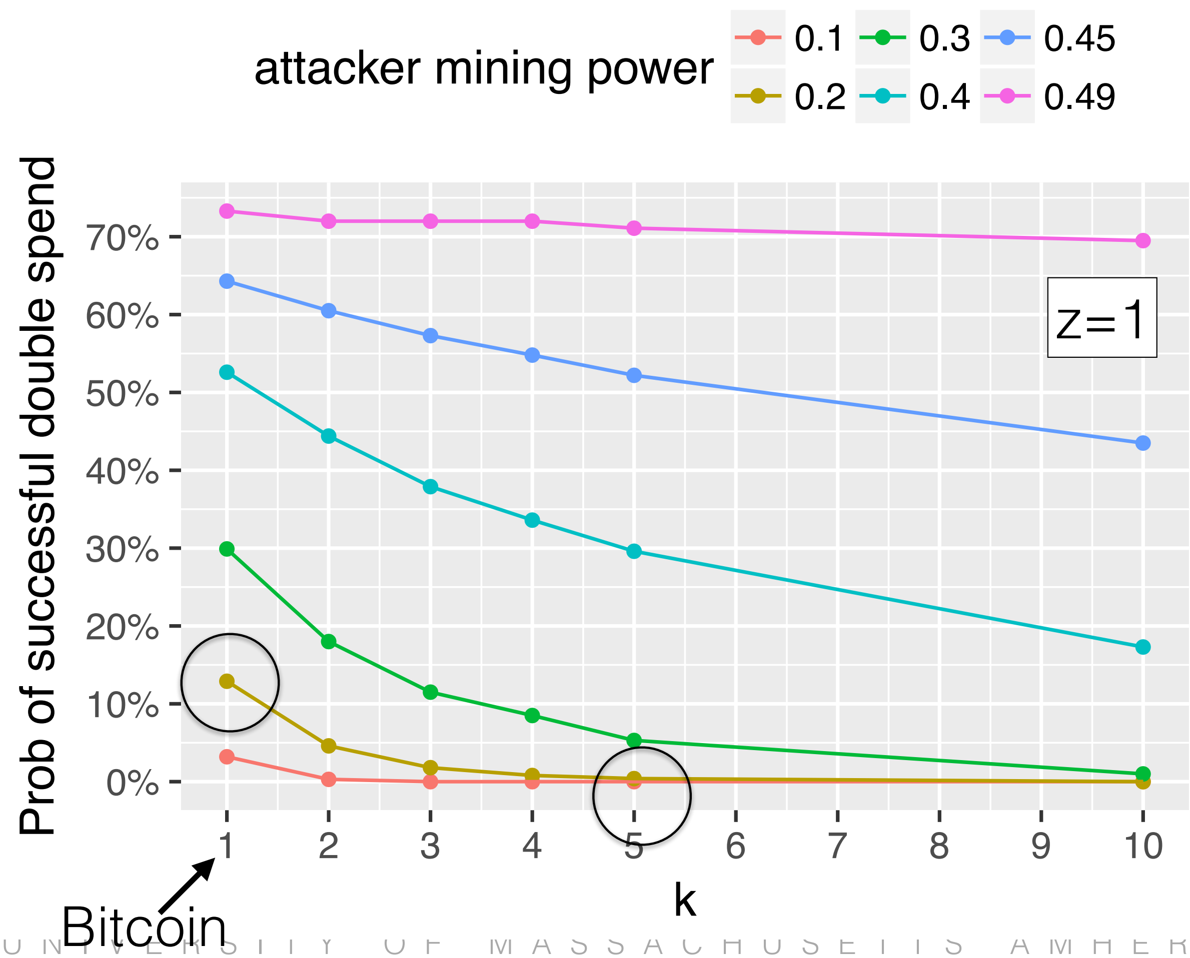

For Bitcoin now (k=1):

- A 20% miner has a 13% chance of doublespend at z=1 blocks.
- And 1% chance at z=6 blocks.

When k=5, the 20% miner at z=1 block is 1%.

https://arxiv.org/abs/1709.08750

# Increased Security: Doublespend




For Bitcoin now (k=1):

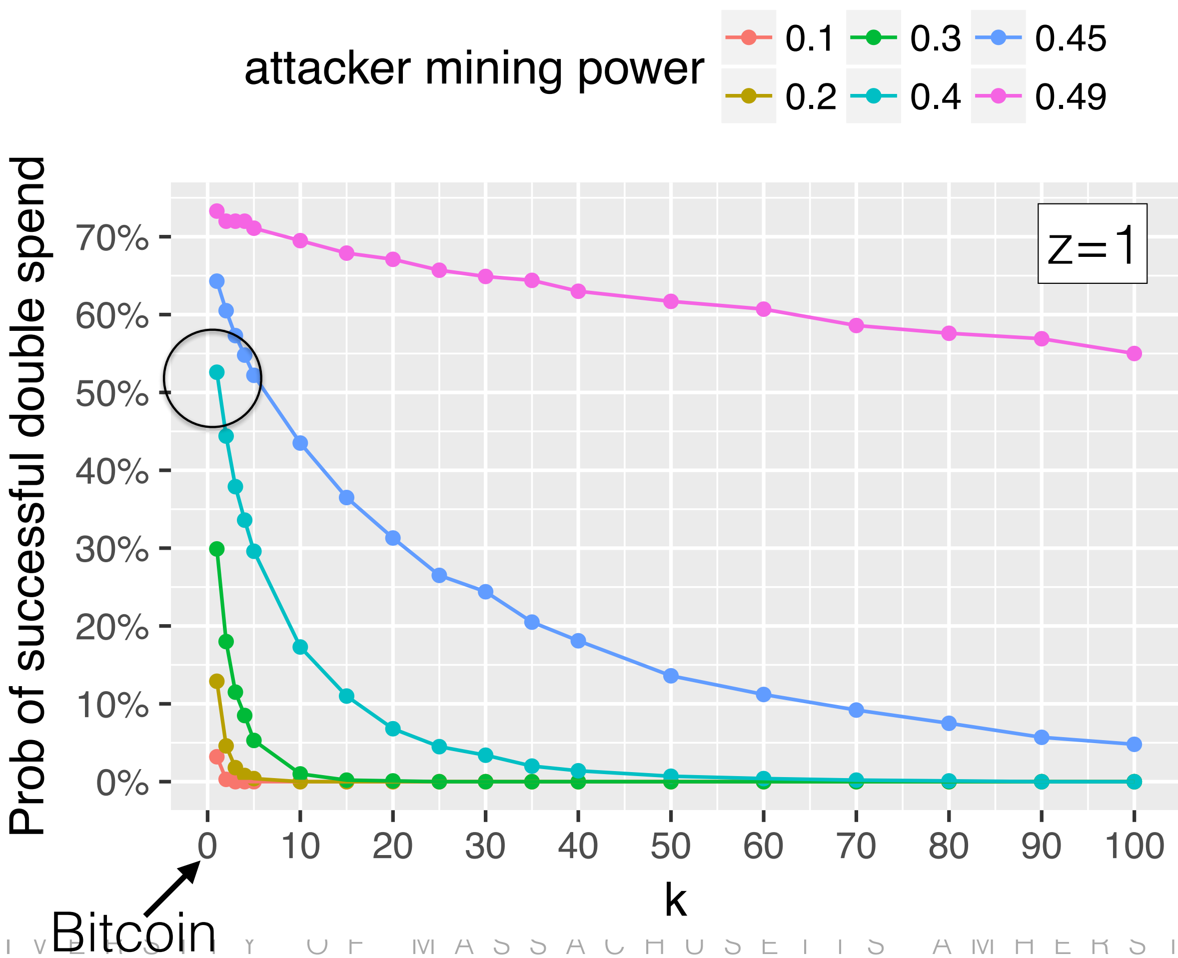
- A 20% miner has a 13% chance of doublespend at z=1 blocks.
- And 1% chance at z=6 blocks.

When k=5, the 20% miner at z=1 block is 1%.



https://arxiv.org/abs/1709.08750

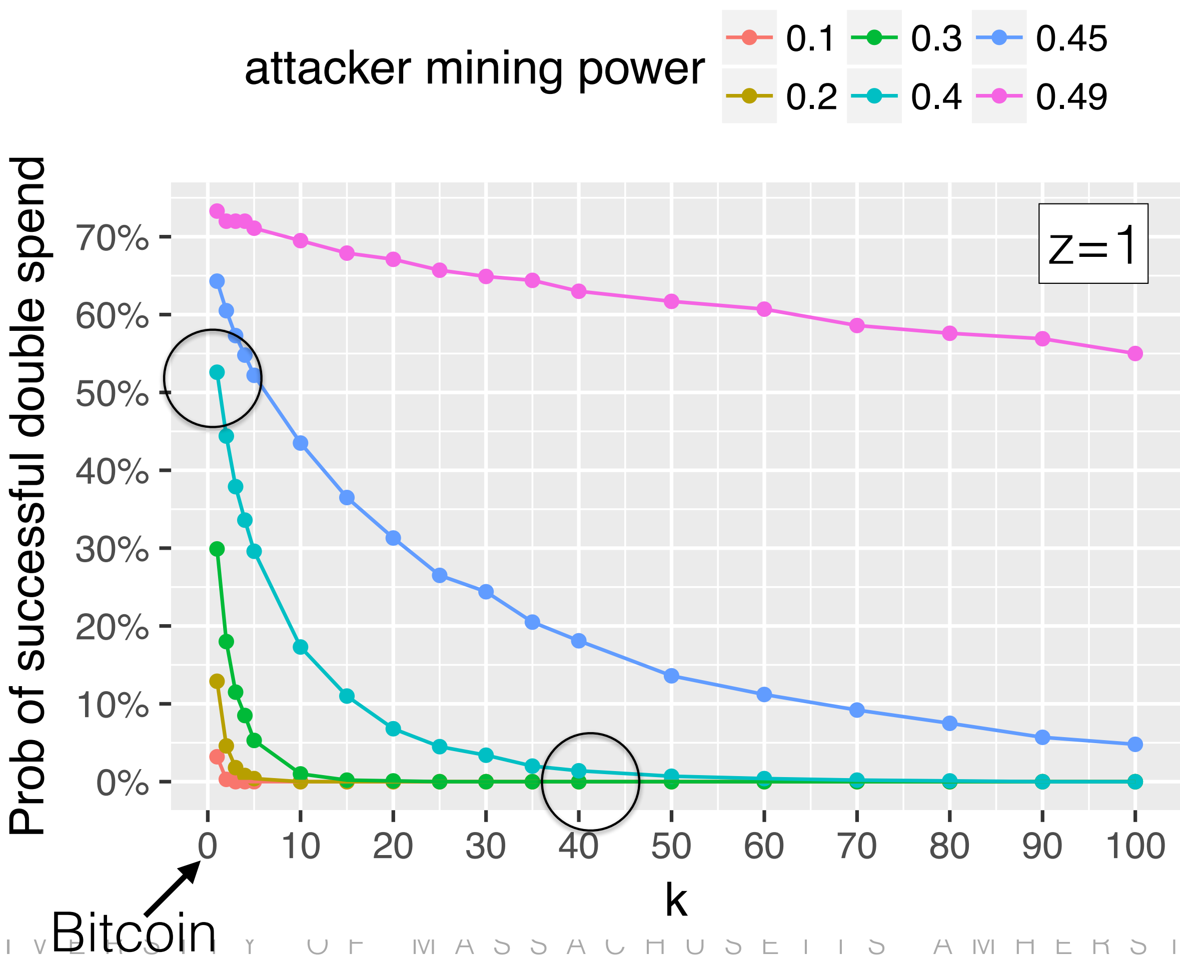
# Doublespend for z=1 block




- When k=40, Bitcoin double spending after z=1 blocks requires ~40% of the mining power to get above 1% chance of success.
- 50x improvement.

https://arxiv.org/abs/1709.08750

# Doublespend for z=1 block



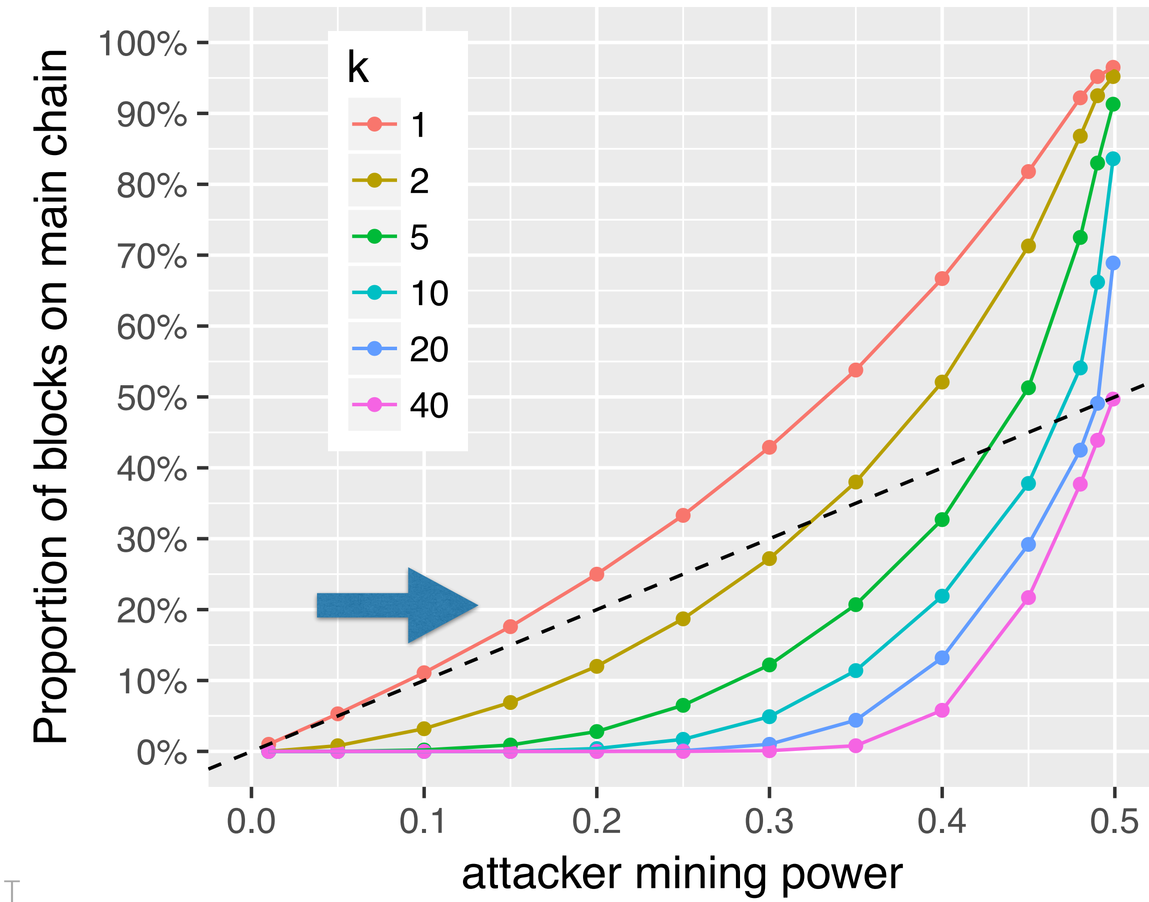

- When k=40, Bitcoin double spending after z=1 blocks requires ~40% of the mining power to get above 1% chance of success.
- 50x improvement.



https://arxiv.org/abs/1709.08750

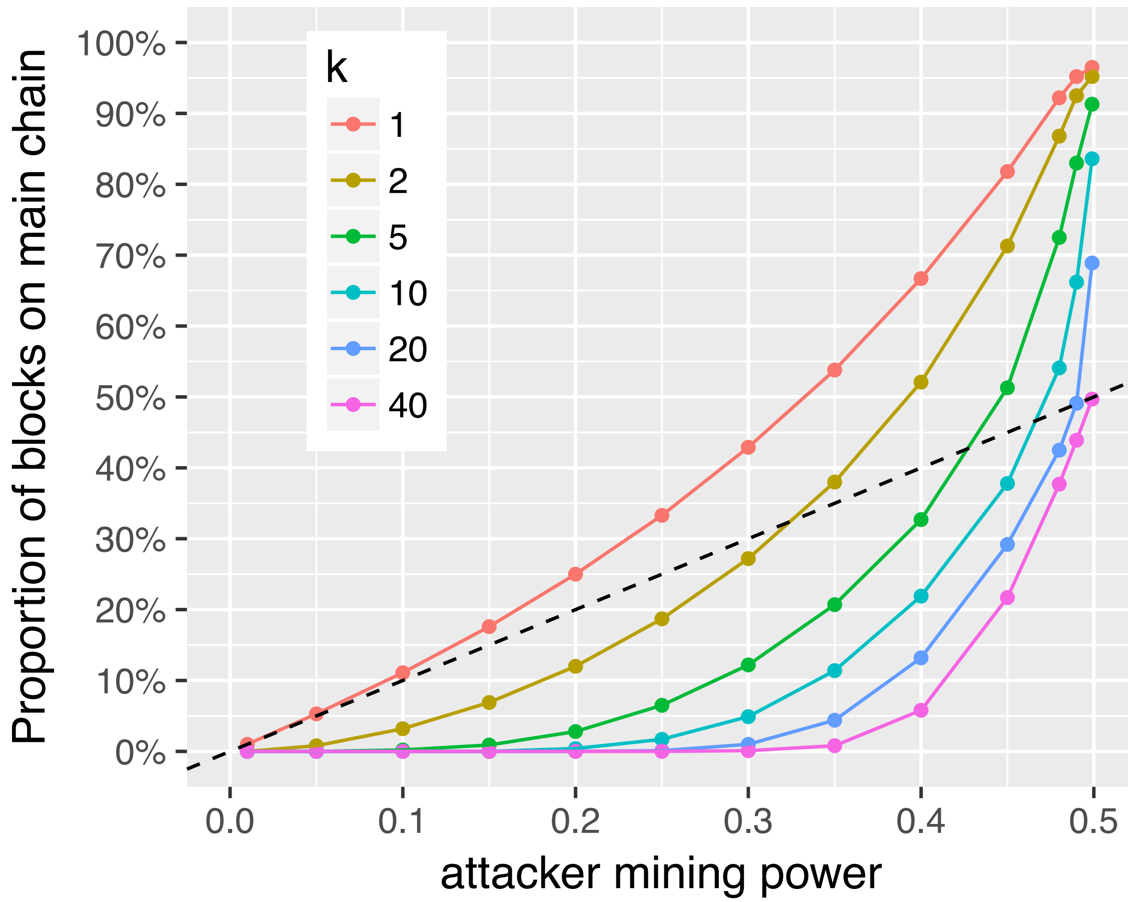
# Selfish Mining can be eliminated

- With Bitcoin, any amount of mining power enables the attack.



# Selfish Mining can be eliminated

- With Bitcoin, any amount of mining power enables the attack.
- When *k≥5,* attackers need 43% of the mining power to selfish mine.
- When *k≥20,* attackers need 49% of the mining power to selfish mine.
- No other defense against DoS attacks are available.
    - *k* can be adjusted on the fly.



# Version 1 Deployment (Naive)

- Naive version: miners simply announce block headers as they find them.
- Each new block on the chain is a collection of *k* full headers.
  - Instead of an 80-byte header, headers would be *k*80* bytes.
    - That's 800B for k=10, and 3KB for k=40
- A lot of traffic as values are found.
  - But values greater than ***k*target*** will never be part of the block.
- Since headers can be stolen, no incentive for miners to share.



https://arxiv.org/abs/1709.08750

# Version 2 Deployment (no stealing)

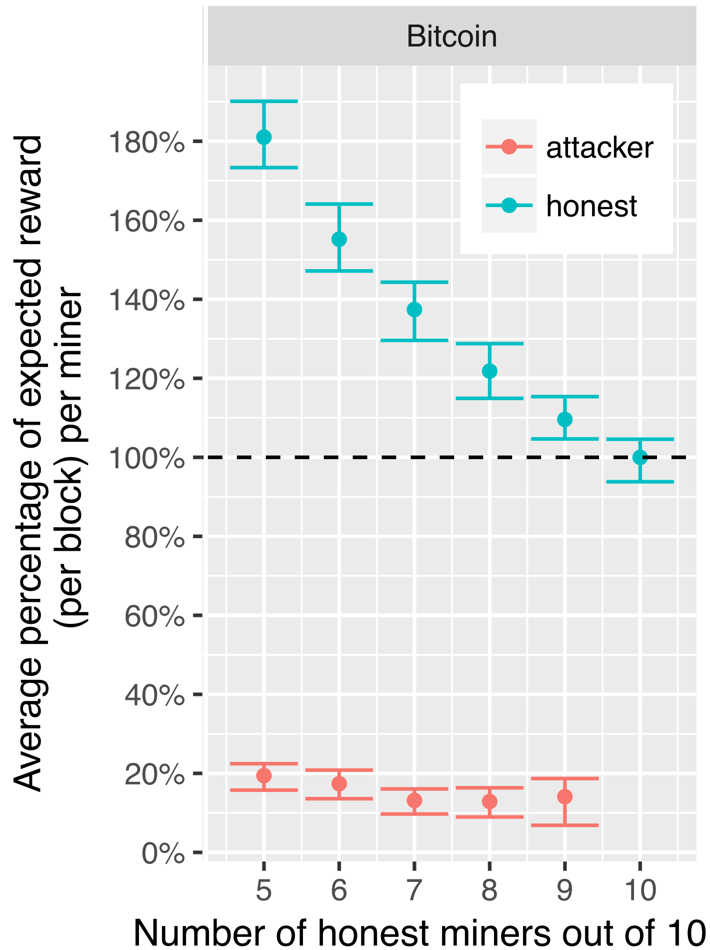
- Reward all miners who helped find the k values
- Miners collect transactions and create standard header, h.
- let ***v*= Hash( Hash(h), prior, Address)** (8Bytes of Hash(h), 8Bytes of prior)
  - If v<kt, then miners announce the pre-image of 36 bytes
  - Recipients check if hash of pre-image is less than ***kt*.**
- Values cannot be stolen as **Address** is a part of the hash pre-image.
- Values cannot be reused since **prior** is part of the hash pre-image.
- Still: When a block is found, there are k-1 values that can be reused!



https://arxiv.org/abs/1709.08750

# Version 3 (no reuse of values)

- To prevent this problem, we add another field to the hash.
  - Miners keep track of the Least Order Stat they've seen to date
  - **v= Hash( Hash(h), Address, Prior, LOS)**
  - **8+20+8+8= 44 bytes per k**
  - No values can be included in the LOS is lower than the lowest OS.
  - Coinbase reward is via a ranking by LOS; ties are broken by *v.*
- Reduces the rewards for miners that attempt it.
  - This drastically reduces the opportunities for reuse.
  - This also thwarts hoarding among a collusion of miners.




https://arxiv.org/abs/1709.08750

# Rewards

| k | L.O.S. | Proof | Reward (BTC) |
|---|---|---|---|
| 1 | - | 358325 | 11.9882020 |
| 2 | 358325 | 1217458 | 0.2827381 |
| 3 | 358325 | 1721868 | 0.1339286 |
| 4 | 358325 | 1777139 | 0.0632440 |
| 6 | 358325 | 1995396 | 0.0139509 |
| 8 | 358325 | 3621245 | 0.0030227 |
| 12 | 358325 | 4582015 | 0.0001308 |
| 14 | 358325 | 4781376 | 0.0000254 |
| 17 | 358325 | 7277279 | 0.0000018 |

| k | L.O.S. | Proof | Reward (BTC) |
|---|---|---|---|
| 9 | 1826037 | 3761724 | 0.0012788 |
| 11 | 1826037 | 4420661 | 0.0002906 |
| 15 | 1826037 | 6302668 | 0.0000109 |
| 18 | 1826037 | 7514262 | 0.0000007 |
| 19 | 1826037 | 7601030 | 0.0000002 |
| 5 | 3521660 | 1826037 | 0.0111607 |
| 13 | 3521660 | 4707122 | 0.0000363 |
| 7 | 3927808 | 3521660 | 0.0018601 |
| 20 | 3927808 | 7881560 | 0.0000001 |
| 10 | 6374495 | 3927808 | 0.0001163 |
| 16 | 9175814 | 6374495 | 0.0000009 |

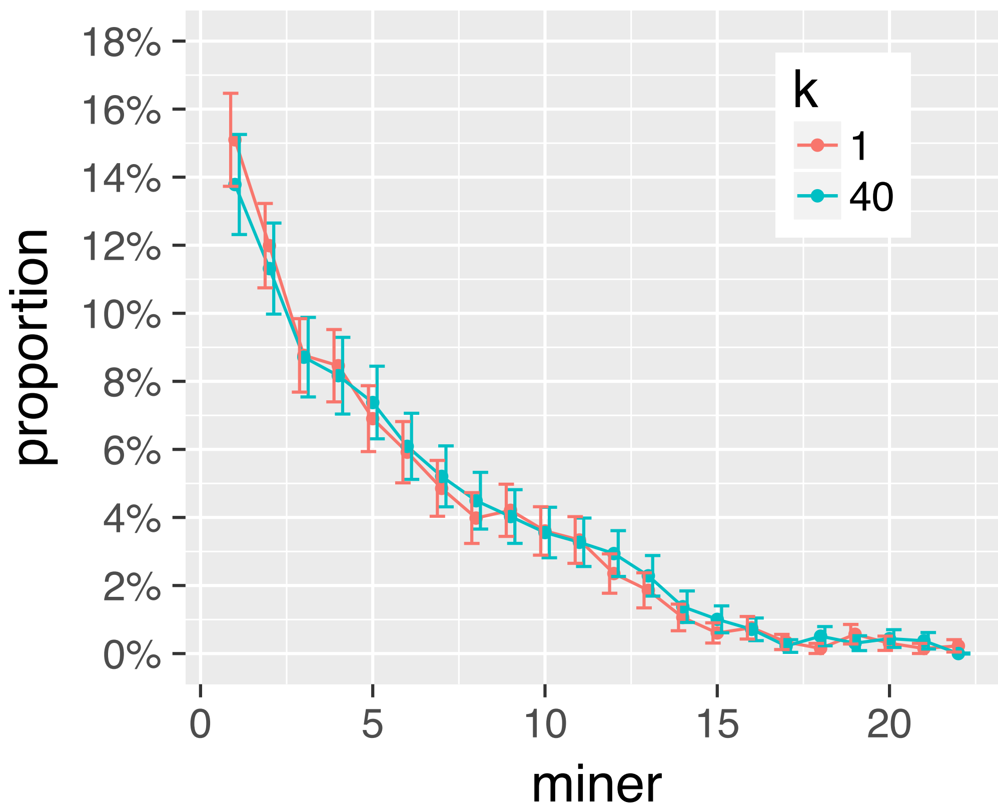


https://arxiv.org/abs/1709.08750

# Proportional Rewards

- Simulations show that rewards are proportion to mining power

- Results are same as Bitcoin today.




https://arxiv.org/abs/1709.08750

# Frequently Asked Questions

- Doesn't this slow down the block announcements?
  - Seen my Graphene presentation?
  - Each k value has an INV.
  - And can be stuffed into Bloom Filter and IBLT.
- Don't the rich get richer?
  - No, that would be the case if we took the k-lowest values from **each** miner.
- What about existing ASICS?
  - Yes, I think maybe they can be used for this (possibly).

# Using existing ASICs

- version (4) → version (4)
- prior (32) → address (20), and LOS (12)
- merkle (32) → Hash(h)>> 24 (8), Prior>>24 (8), pad with 16 bytes of zeros
- time (4) → nonce (4)
- nBits (4) → kt bound
- nonce (4) → nonce (4)

64 bits of nonce to play with

**Header would be 56(k-1)+80 bytes**



https://arxiv.org/abs/1709.08750

# Summary

| k | header (bytes) | coinbase (bytes) | equivalent to #TXNs | 90% delay (minutes) | mining power needed for selfish mining | mining power needed to doublespend (2 blocks) |
|---|---|---|---|---|---|---|
| 1 | 80 | 205 | 0 | ½ – 40 | 0% | 10% |
| 5 | 256 | 345 | 1 | 3½ – 19 | 42% | 20% |
| 10 | 476 | 520 | 3 | 5 – 16½ | 46% | 25% |
| 20 | 916 | 870 | 7 | 6½ – 14½ | 49% | 35% |
| 40 | 1796 | 1570 | 14 | 7½ – 13 | 49.5% | 40% |



https://arxiv.org/abs/1709.08750

# Conclusion

- Bobtail reduces inter-block time variance in PoW blockchains
  - by generalizing target criterion to k values.
- Significantly increases difficulty of doublespend
- Effectively eliminates selfish mining
- Reward rate and orphan rate do not change.
- Secure against attacks
- Cost is very small in terms of bytes.
- Adjustable and incrementally deployable

bnl@umass.edu

https://arxiv.org/abs/1709.08750

# Conclusion

- Bobtail reduces inter-block time variance in PoW blockchains
  - by generalizing target criterion to k values.
- Significantly increases difficulty of doublespend
- Effectively eliminates selfish mining
- Reward rate and orphan rate do not change.
- Secure against attacks
- Cost is very small in terms of bytes.
- Adjustable and incrementally deployable


bnl@umass.edu

https://arxiv.org/abs/1709.08750