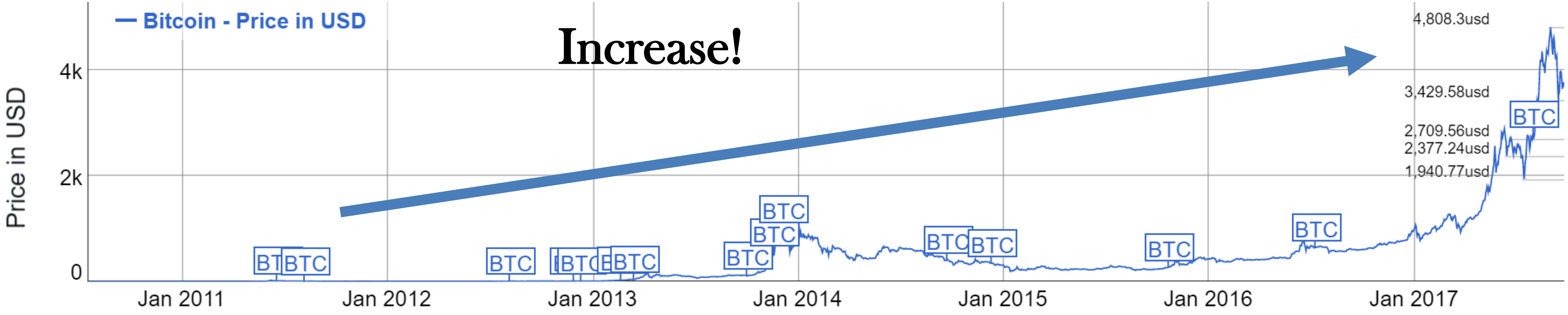
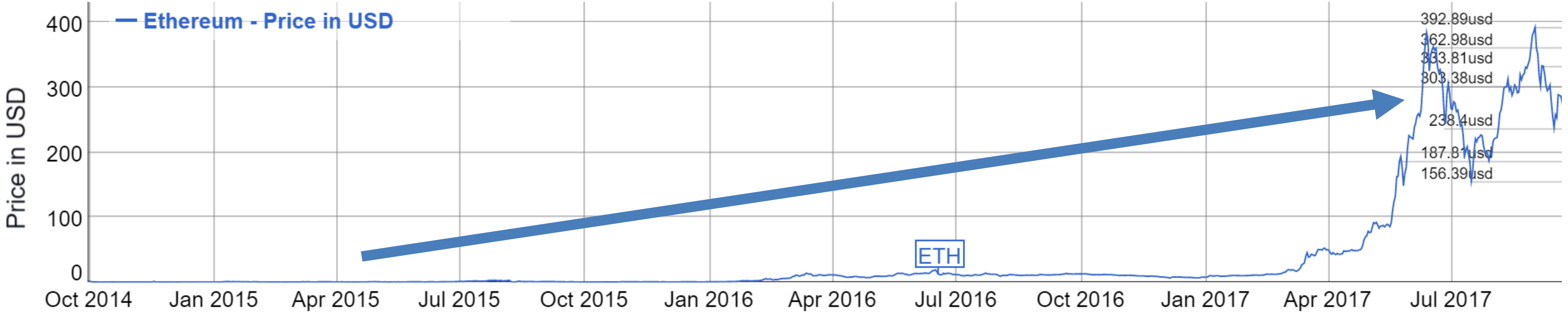
Attacks on Mining Protocol

Yujin Kwon
KAIST
2018.03.22

Cryptocurrencies

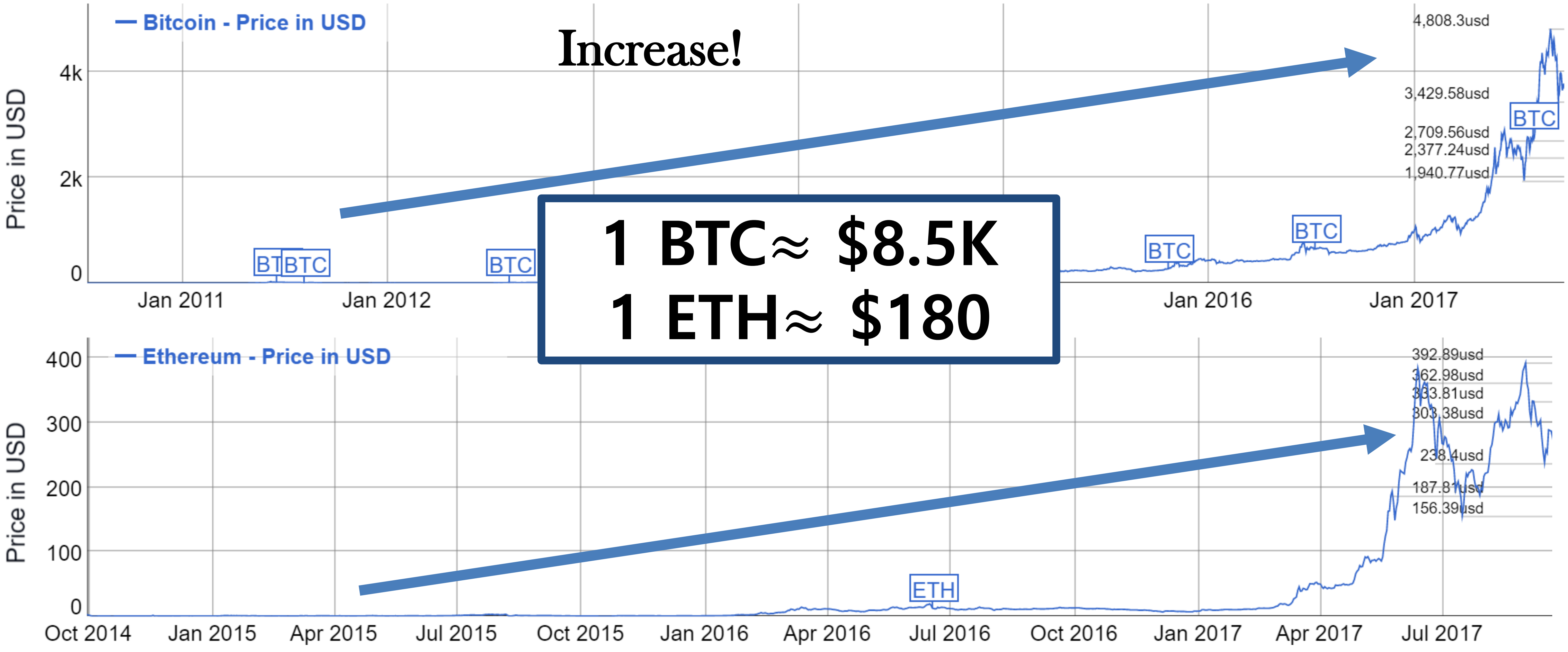
Cryptocurrencies





SysSec
System Security Lab

Cryptocurrencies

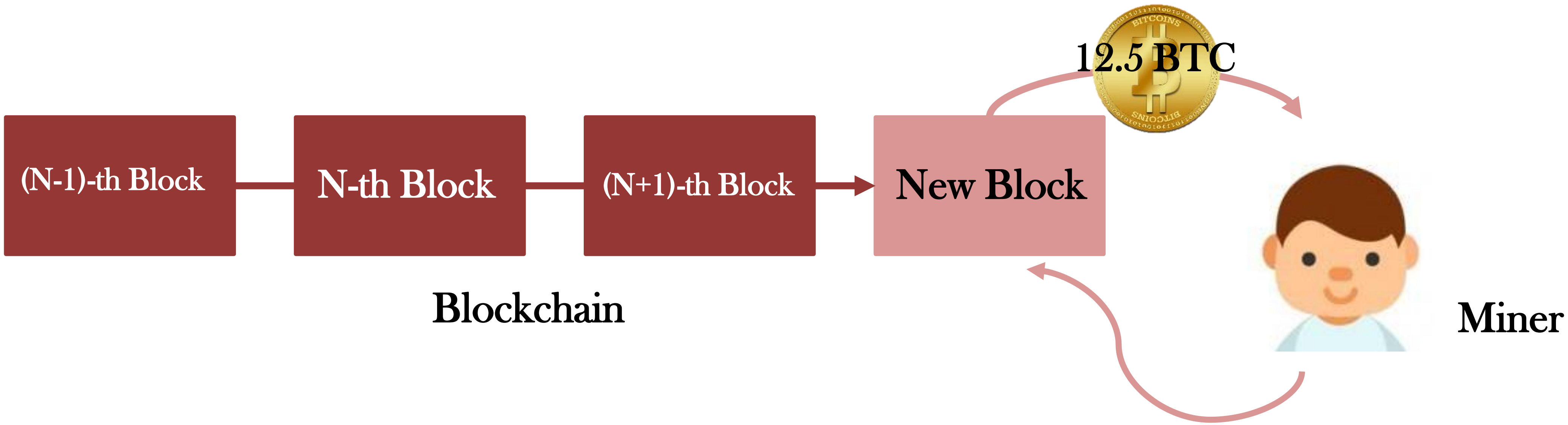


1 BTC≈ $8.5K

1 ETH≈ $180

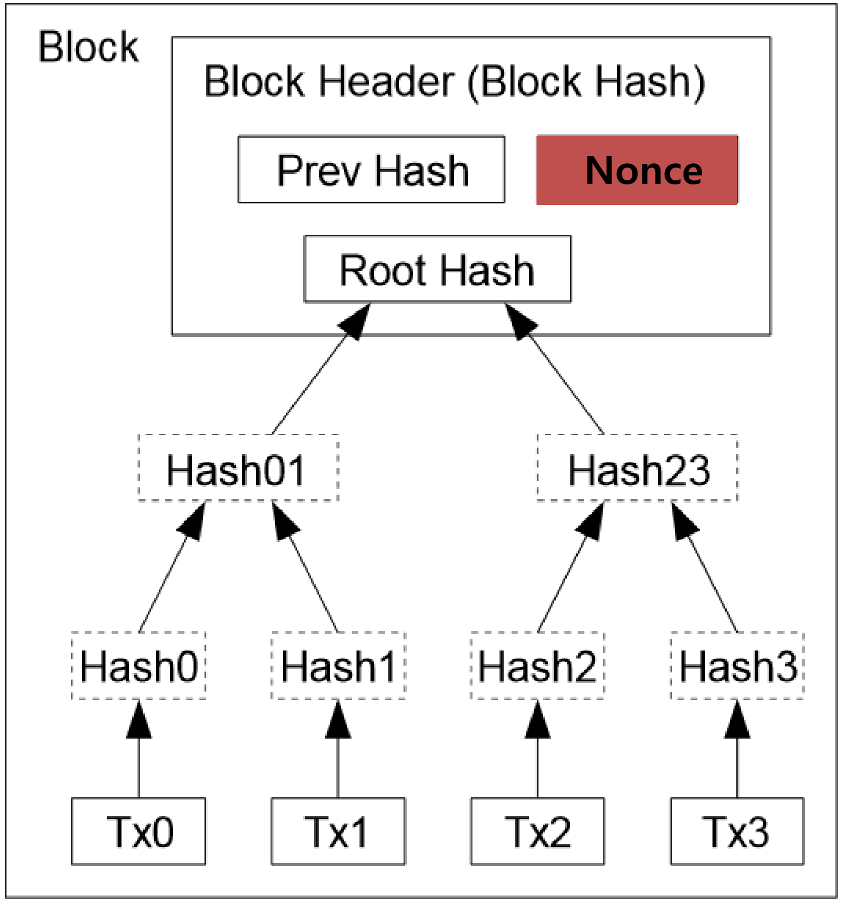
Proof-of-Work Mining

- They use **blockchain** to run without a trusted third party.
- Miners generate blocks by spending their **computational power**.
- If a miner generates a valid block, he earns **reward for the block.**
- This process is **competitive.**



Proof-of-Work Mining

- Problem
  - Miners must solve cryptographic problems to generate a valid block.
  - What is the valid nonce such that $H(contents||nonce) < \mathrm{TARGET}_F$?
  - $H(\cdot)$ is a hash function based on SHA-256 in Bitcoin.

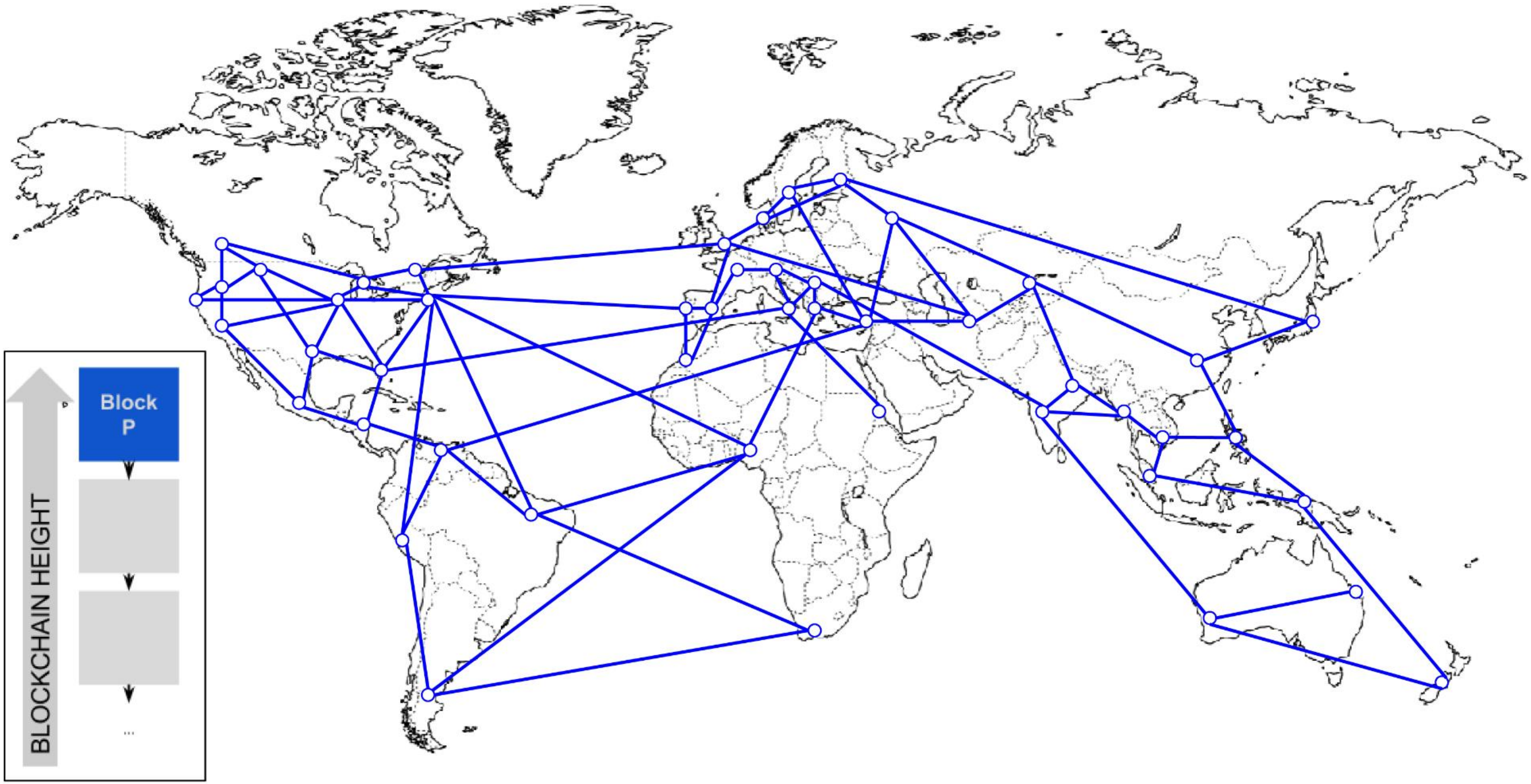


Transactions Hashed in a Merkle Tree

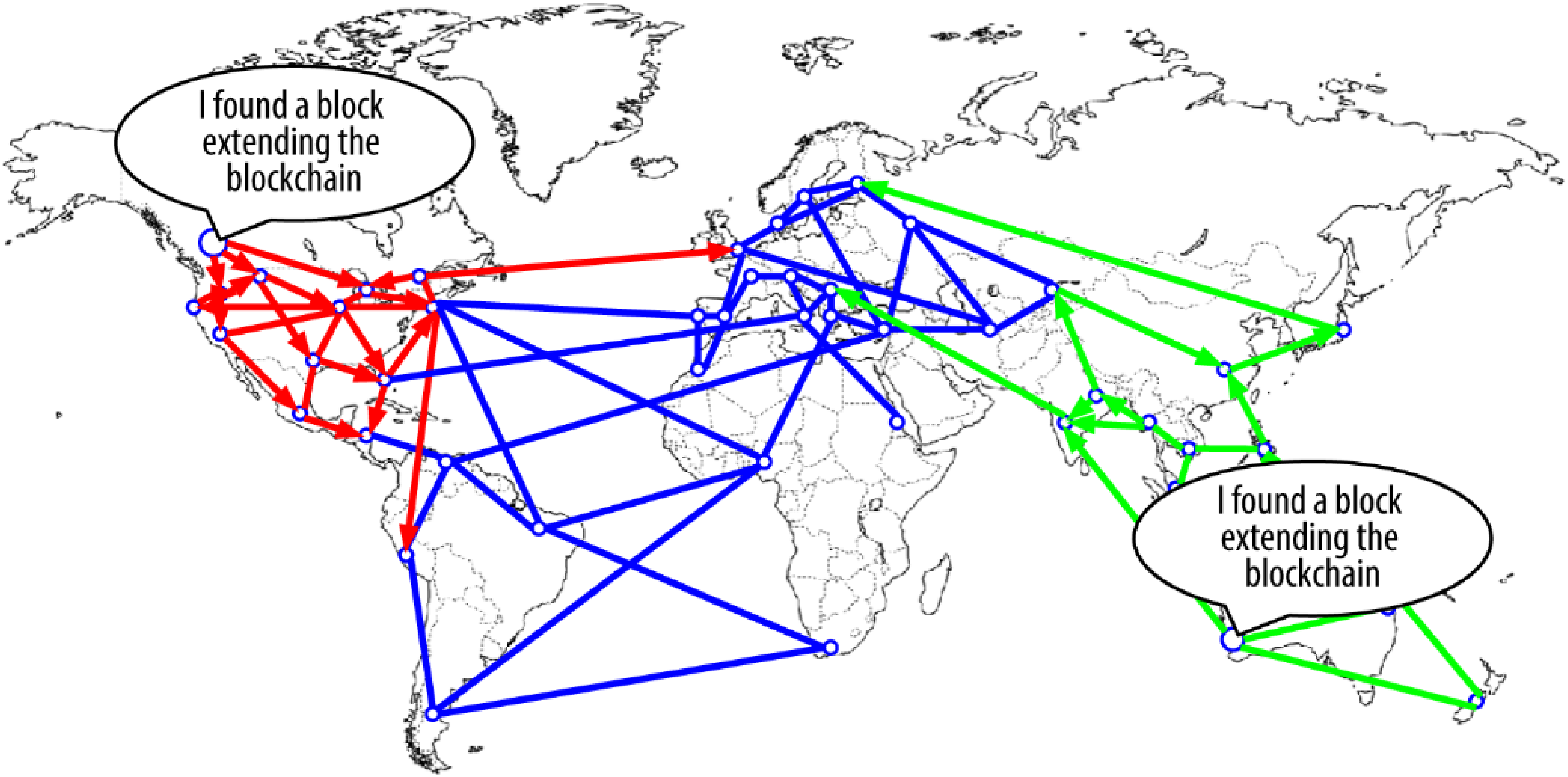
Step (Miner)

- New transactions are broadcast to all nodes.
- Each node collects new transactions into a block.
- Each node works on finding a difficult proof-of-work for its block.
- When a node finds a proof-of-work, it broadcasts the block to all nodes.
- Nodes express their acceptance of the block by working on creating the next chain, using the hash of the accepted block as the previous hash.

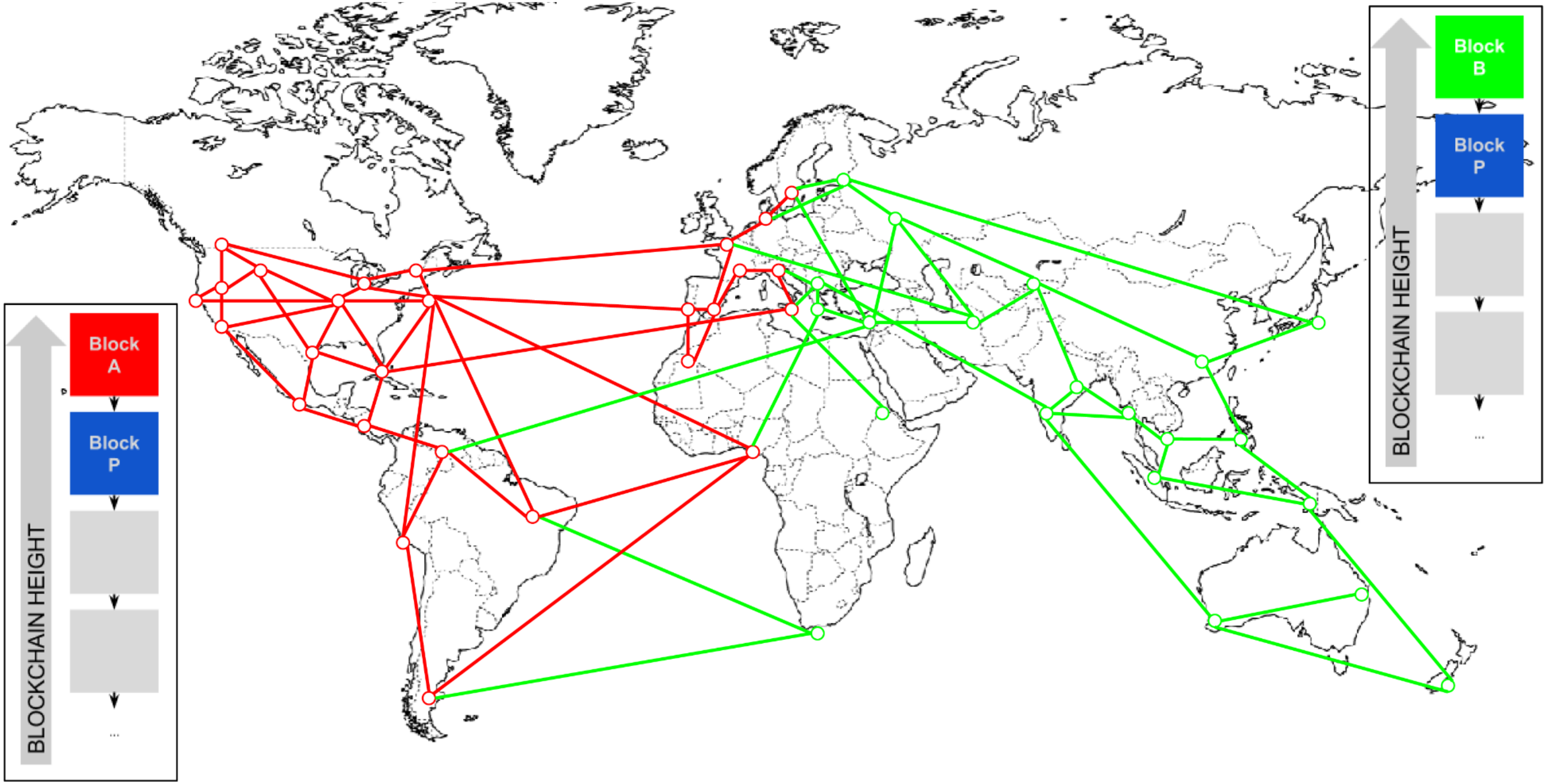
Forks



Forks

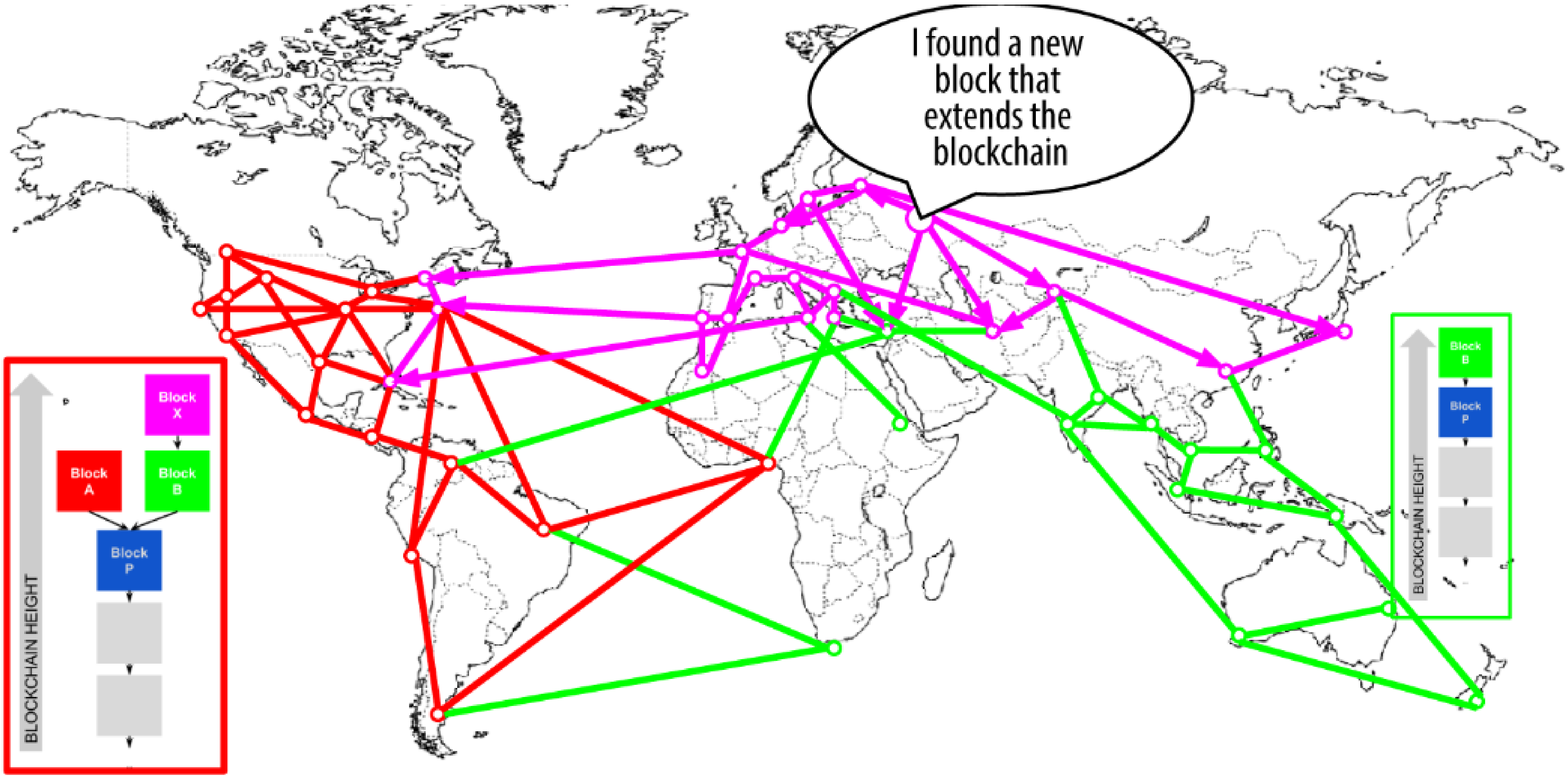

I found a block extending the blockchain
I found a block extending the blockchain

Forks

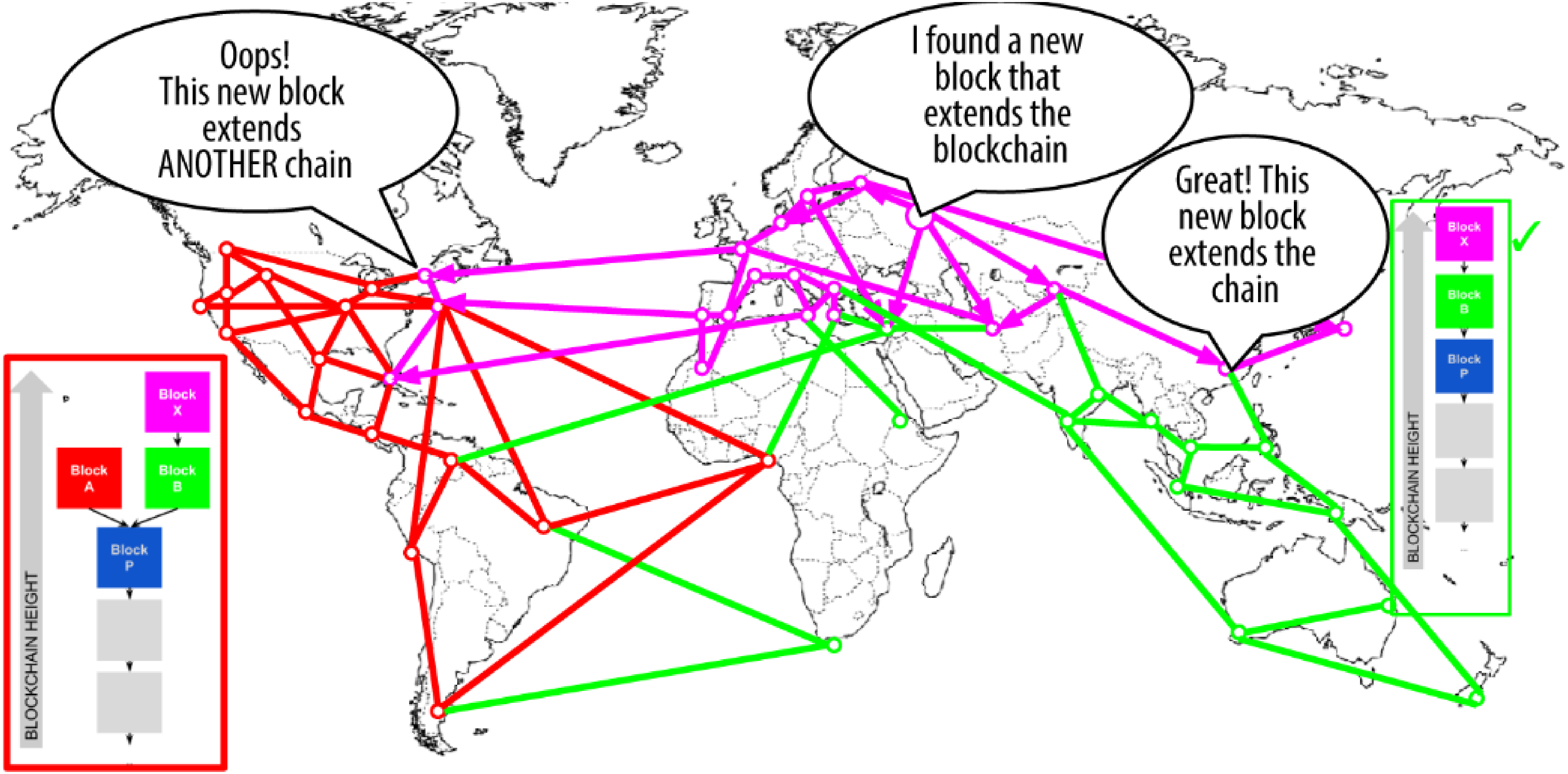


Block
A
Block
P
BLOCKCHAIN HEIGHT
...
Block
B
Block
P
BLOCKCHAIN HEIGHT
...

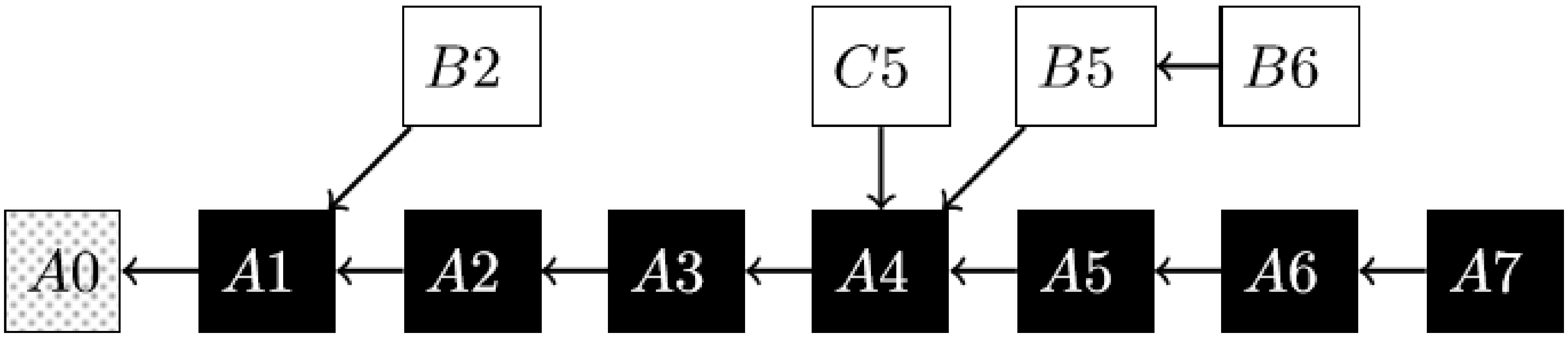
Forks


I found a new block that extends the blockchain
BLOCKCHAIN HEIGHT
Block X
Block A
Block B
Block P
BLOCKCHAIN HEIGHT
Block B
Block P

Forks


Oops! This new block extends ANOTHER chain
I found a new block that extends the blockchain
Great! This new block extends the chain
BLOCKCHAIN HEIGHT
Block X
Block A
Block B
Block P
BLOCKCHAIN HEIGHT
Block X
Block B
Block P

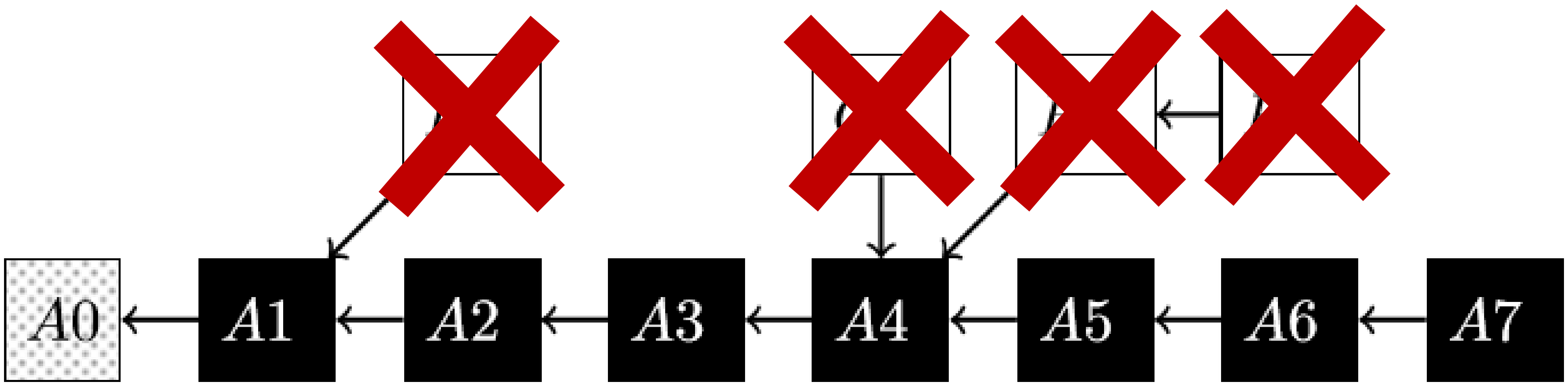
Forks



❖ Only one head is accepted as a valid one among heads.

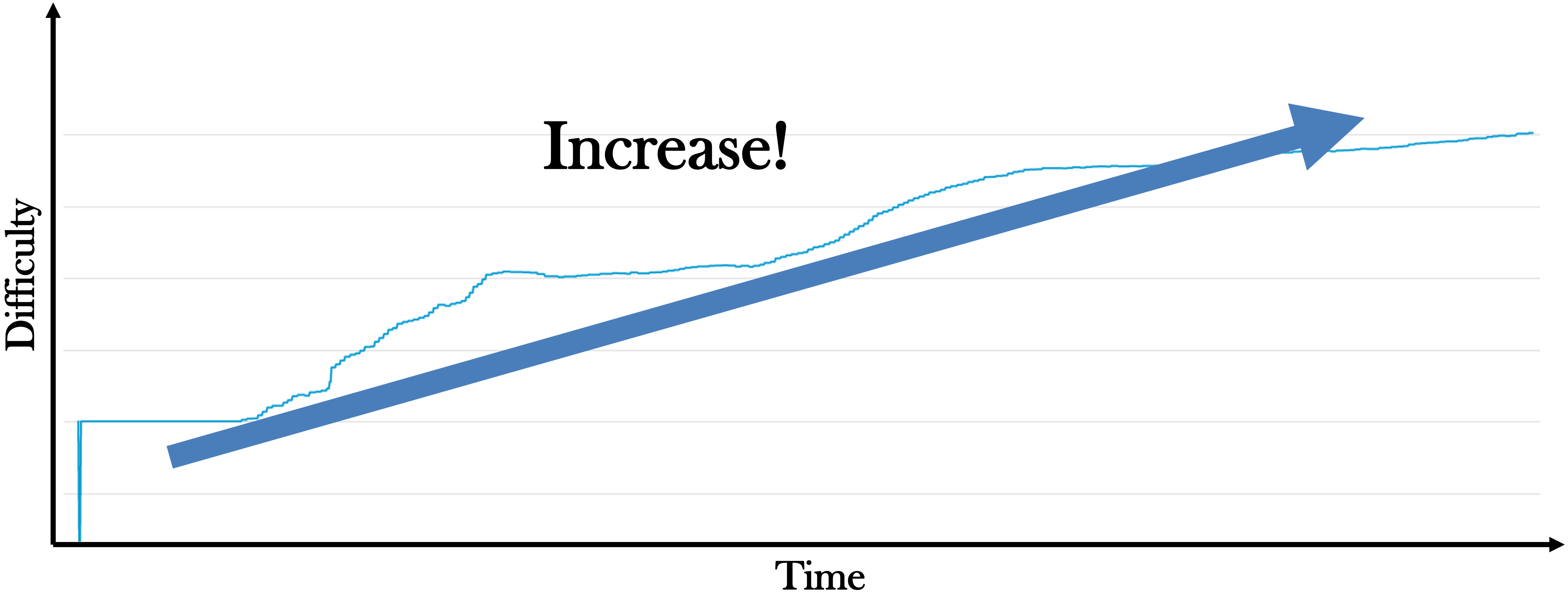
❖ An attacker can generate forks intentionally by holding his found block for a while.

Forks



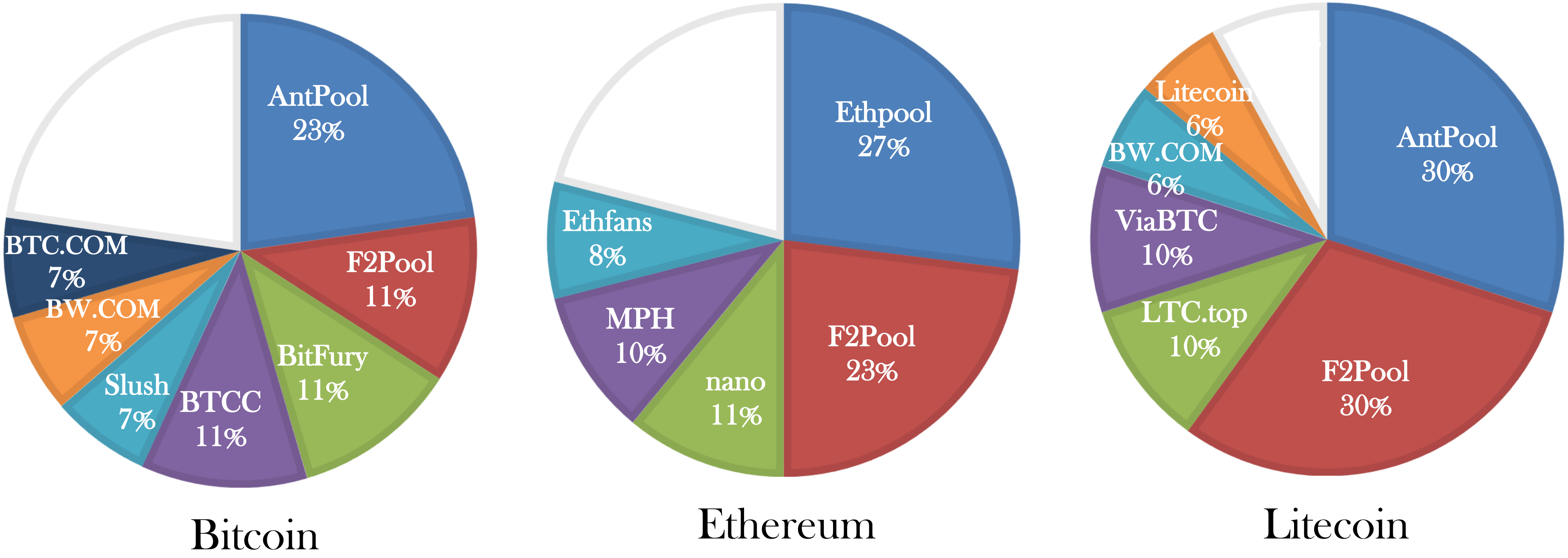
- Only one head is accepted as a valid one among heads.
- An attacker can generate forks intentionally by holding his found block for a while.

Mining Difficulty



From “https://blockchain.info”

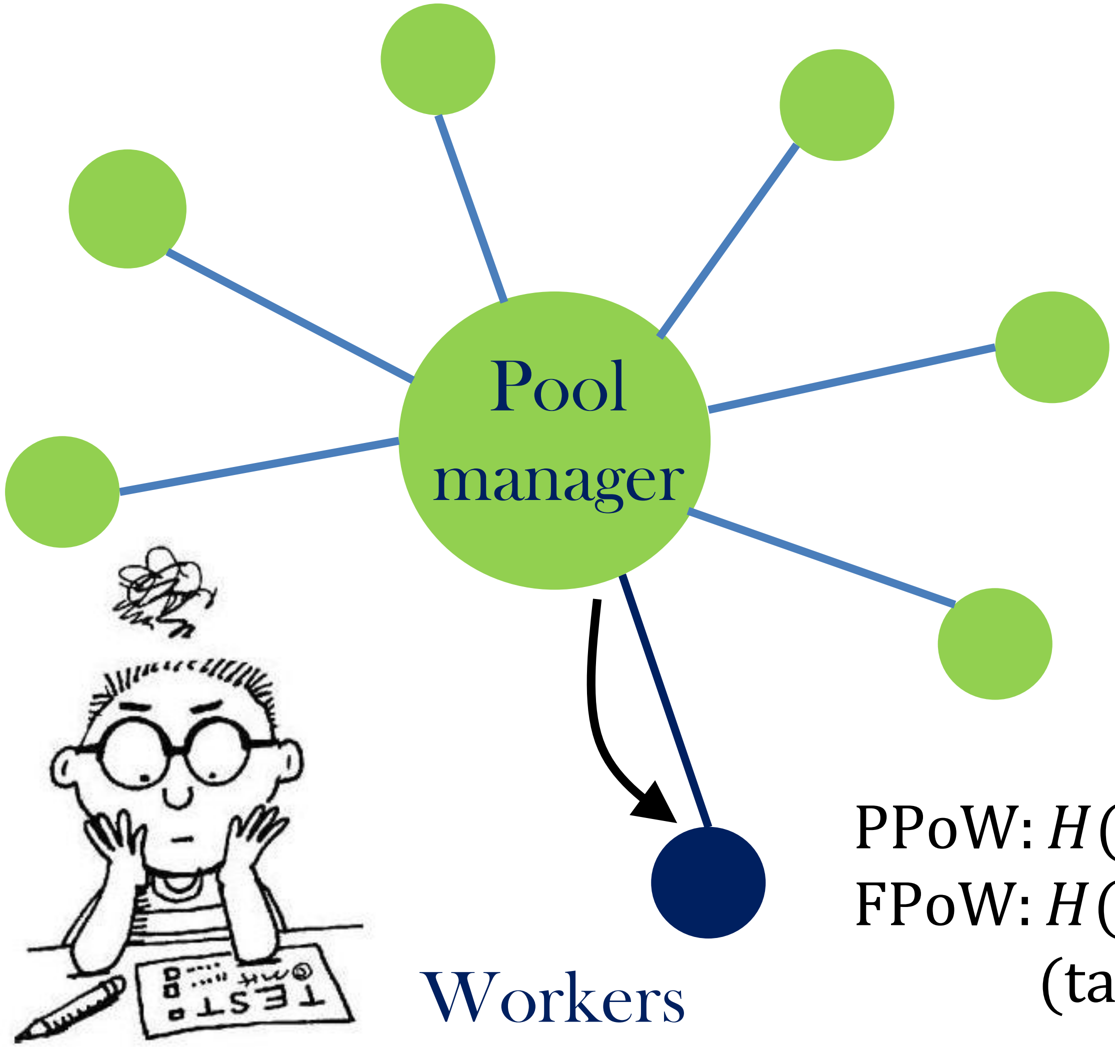
Mining Pool

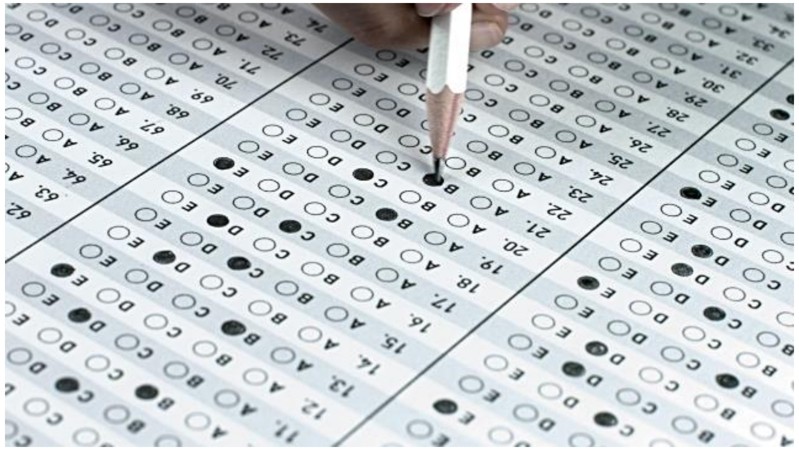


❖ Miners organize pools and prefer to mine together to reduce the variance of reward.

❖ Currently, major players are pools.

Mining Pool





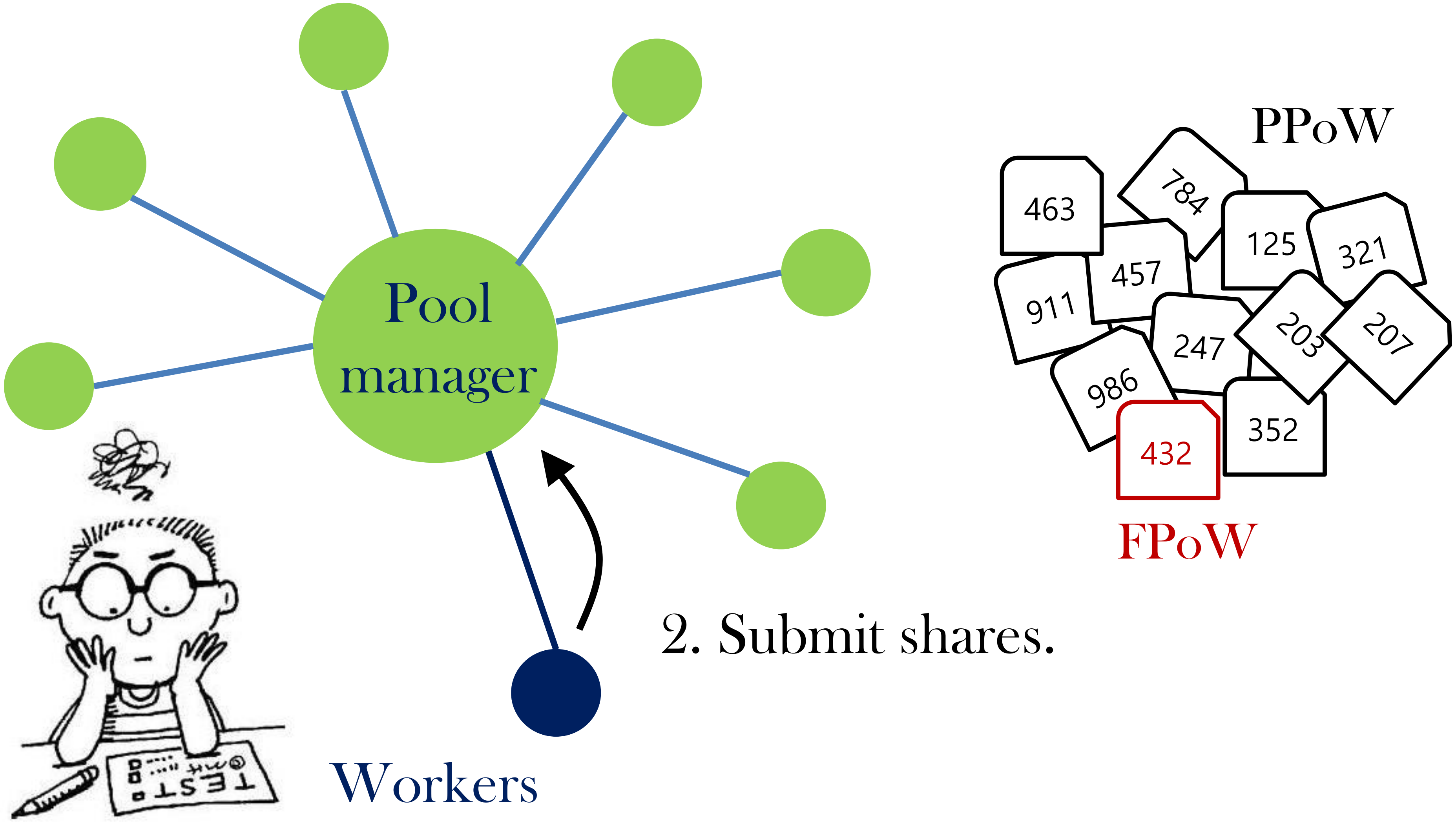
1. Give the problem.

PPoW: $H(contents||\textcolor{red}{nonce}) < \text{target}_P$?

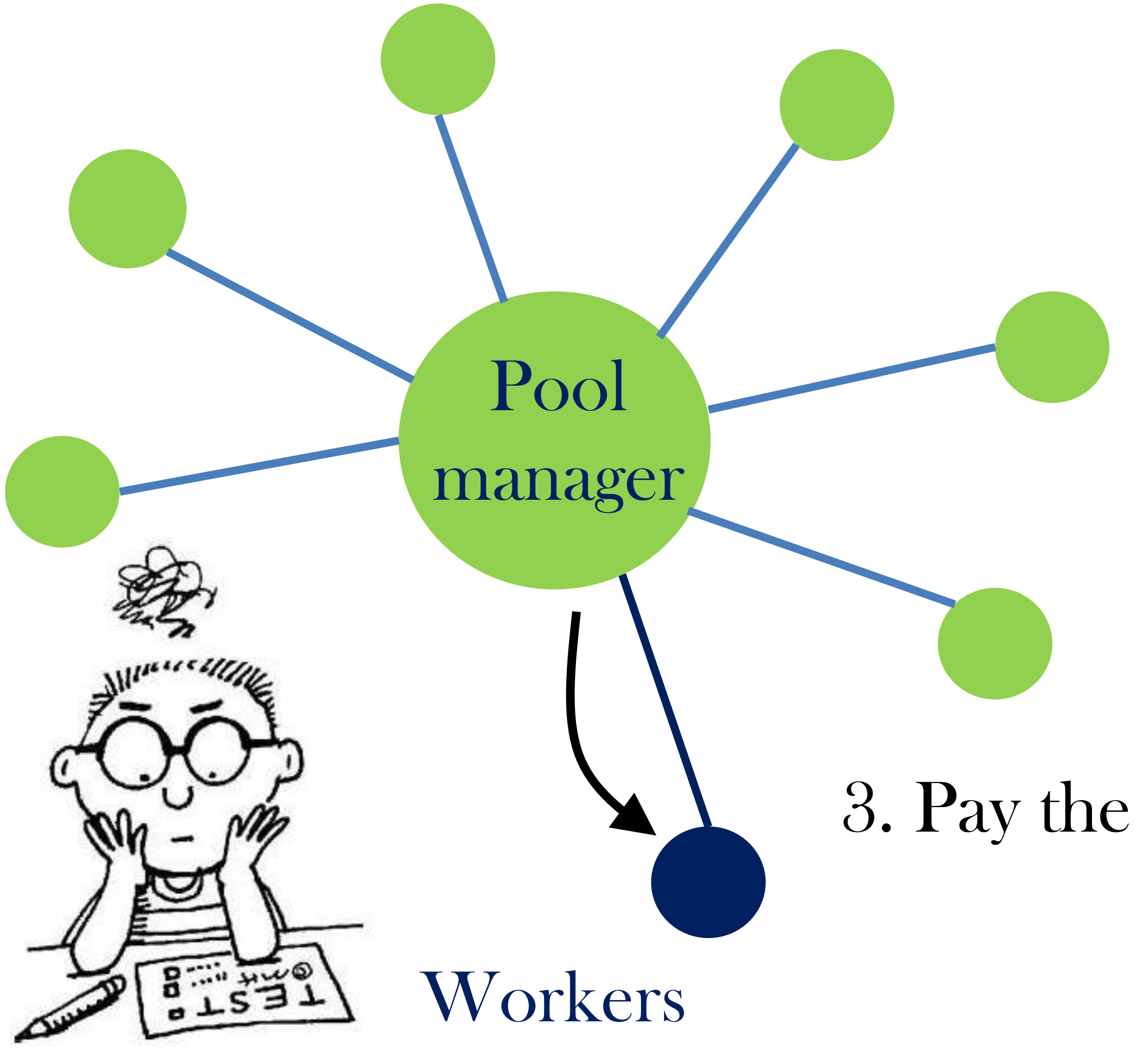
FPoW: $H(contents||\textcolor{red}{nonce}) < \text{TARGET}_F$?

$(\text{target}_P \gg \text{TARGET}_F)$

Mining Pool


Pool manager
Workers
2. Submit shares.
PPoW
463
784
125
321
457
911
247
203
207
986
432
352
FPoW

Mining Pool



3. Pay the reward.

Several Mining Attacks

- The 51 % Attack
    - “The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries”, WEIS 2013
- Selfish mining
    - Generate forks intentionally
        - “Majority Is Not Enough: Bitcoin Mining Is Vulnerable”, FC 2014
- Block withholding (BWH) attack
    - Exploit the pools’ protocol
        - “The Miner’s Dilemma”, IEEE S&P 2015
        - “On Power Splitting Games in Distributed Computation: The Case of Bitcoin Pooled Mining”, CSF 2016
- Fork after withholding (FAW) attack
    - Generate forks intentionally through pools
        - “Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin”, ACM CCS 2017

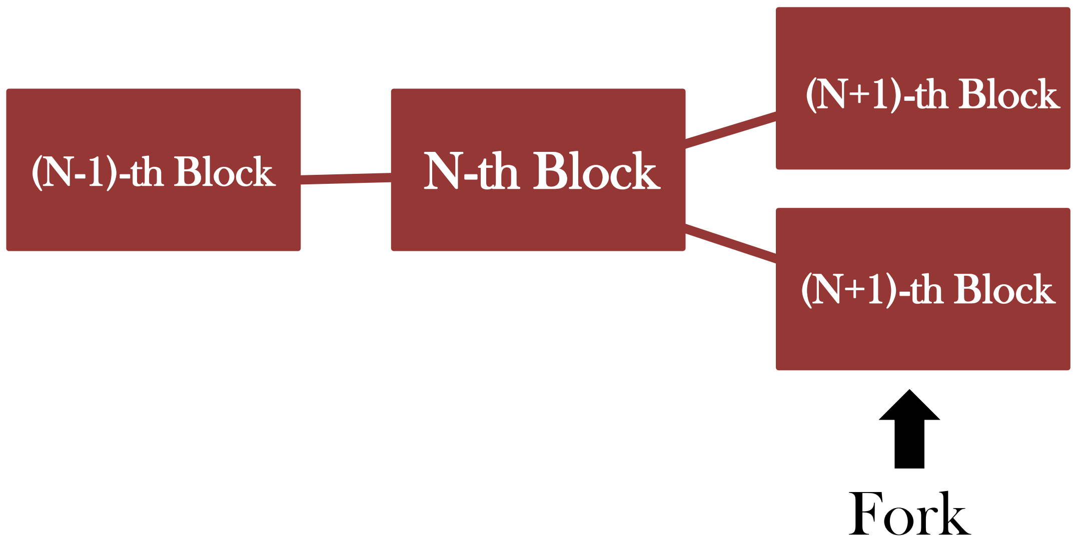
Selfish Mining

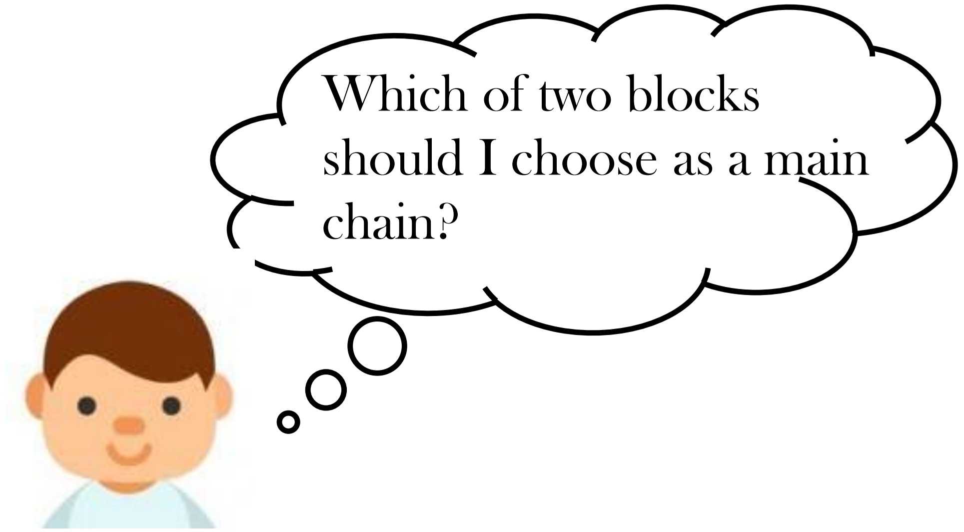
Selfish Mining

❖ Forks

– Due to the nonzero block propagation delay, nodes can have different views.

– When a fork occurs, only one block becomes valid.



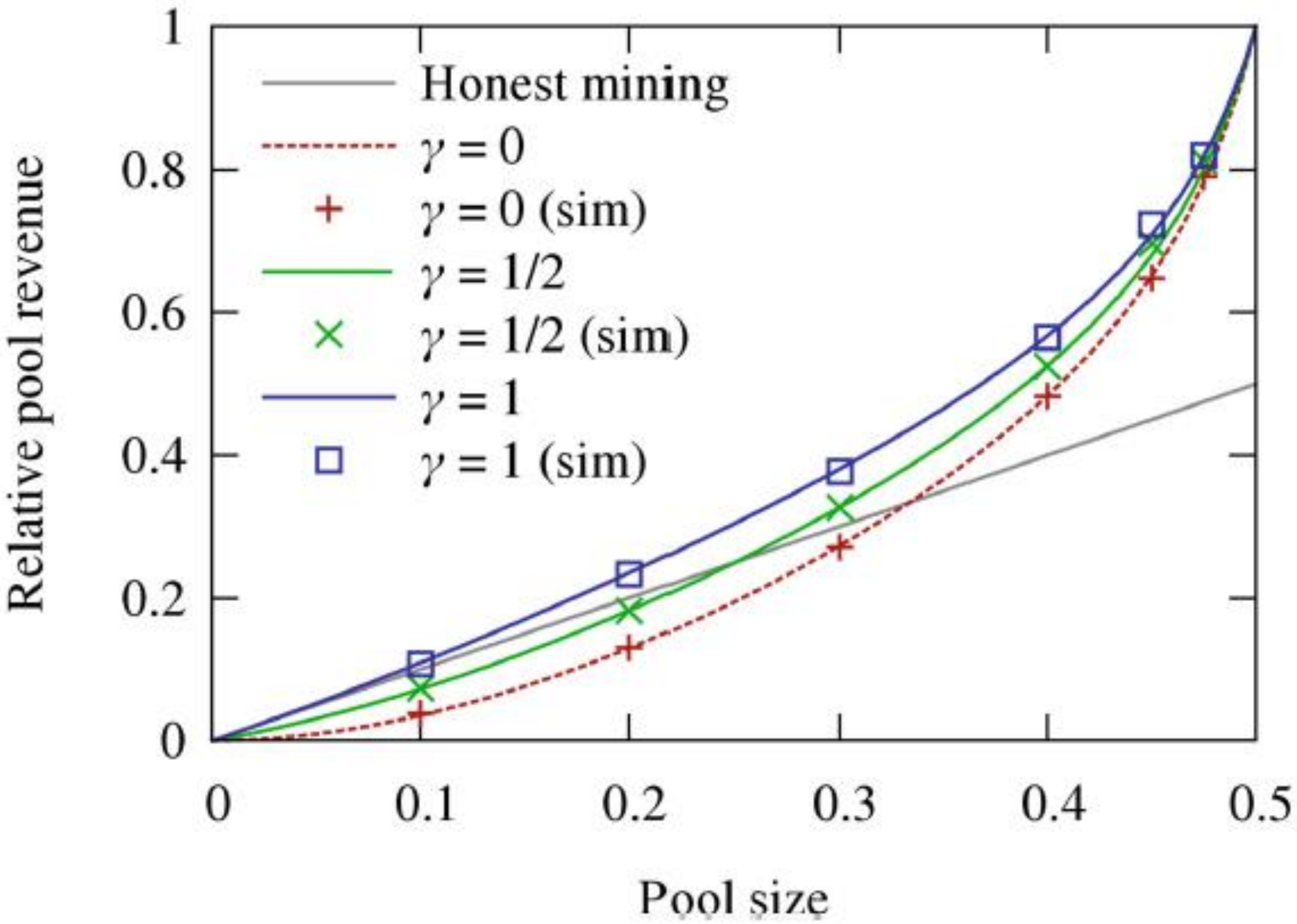


Selfish Mining

- ❖ Generate intentional forks adaptively.
  - – An attacker finds a valid block and propagates the block **when another block is found by an honest node.**

- ❖ Force the honest miners into wasting victims' computations on the stale public branch.

Selfish Mining



- ❖ γ: An attacker's network capability
- ❖ When an attacker possesses more than 33% computational power, the attacker can always earn extra rewards.

Selfish Mining

Selfish Mining

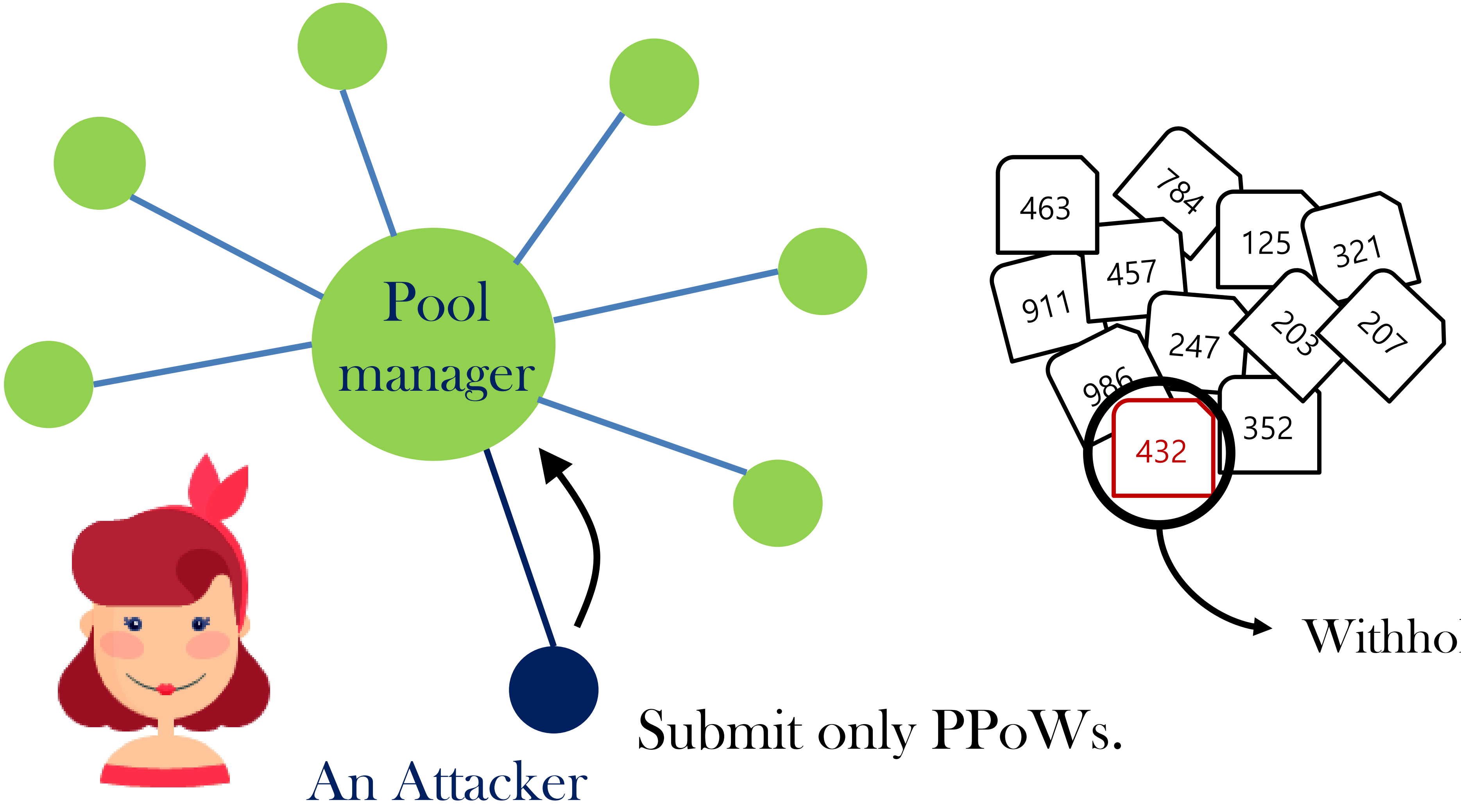
Impractical

- The value of γ cannot be 1 because when the intentional fork occurs, the honest miner who generated a block will select his block, not that of the selfish miner.

- Honest miners can easily detect that their pool manager is a selfish mining attacker.
  - If the manager does not propagate blocks immediately when honest miners generate FPoWs, the honest miners will know that their pool manager is an attacker.
  - The blockchain has an abnormal shape when a selfish miner exists.

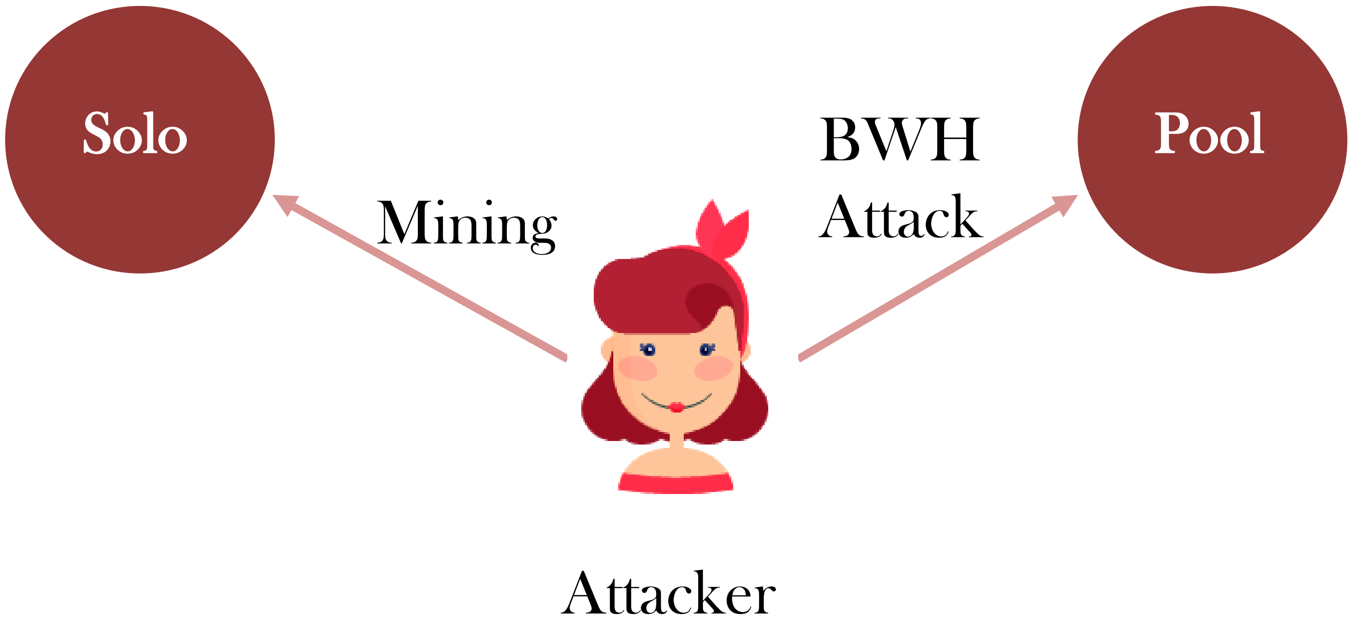
Block Withholding Attack

Block Withholding (BWH) Attack

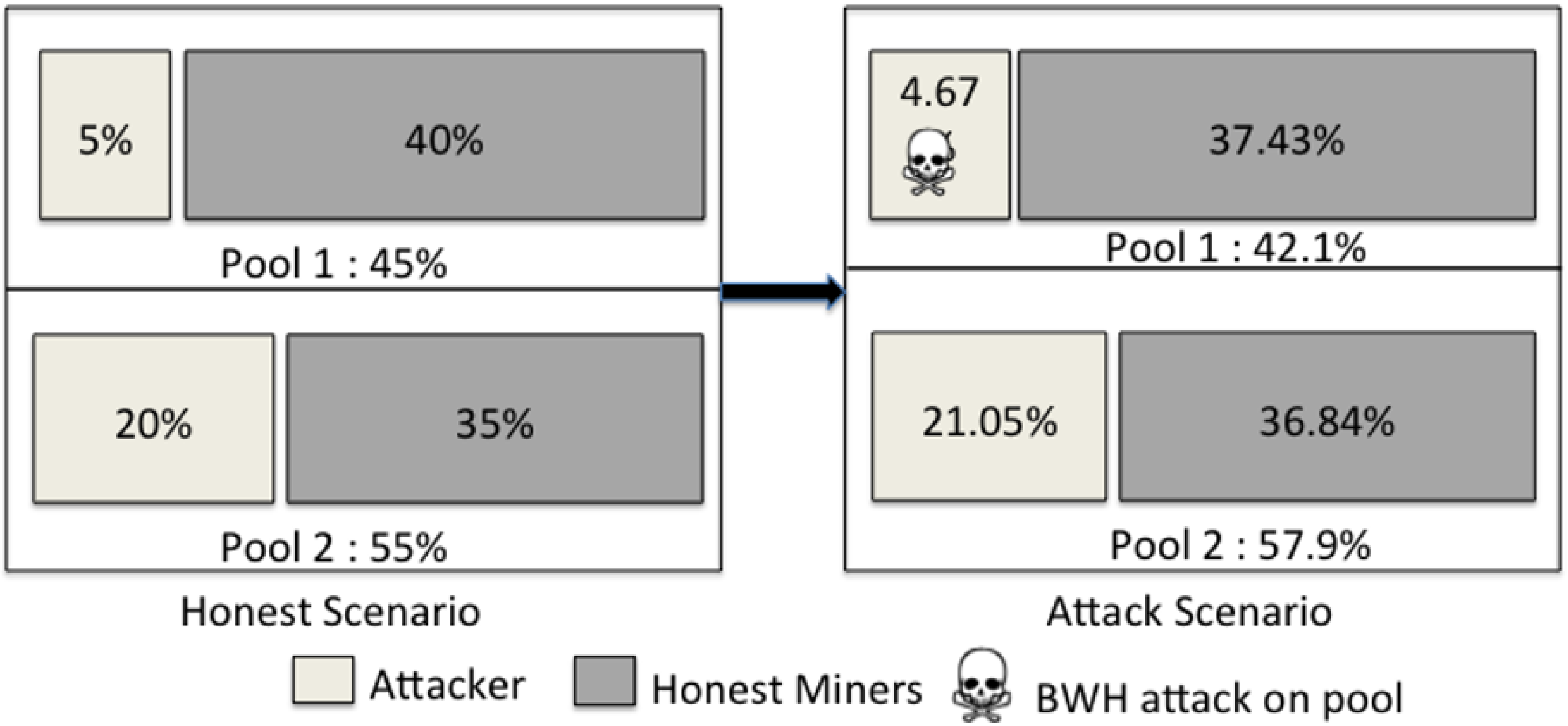


Block Withholding (BWH) Attack

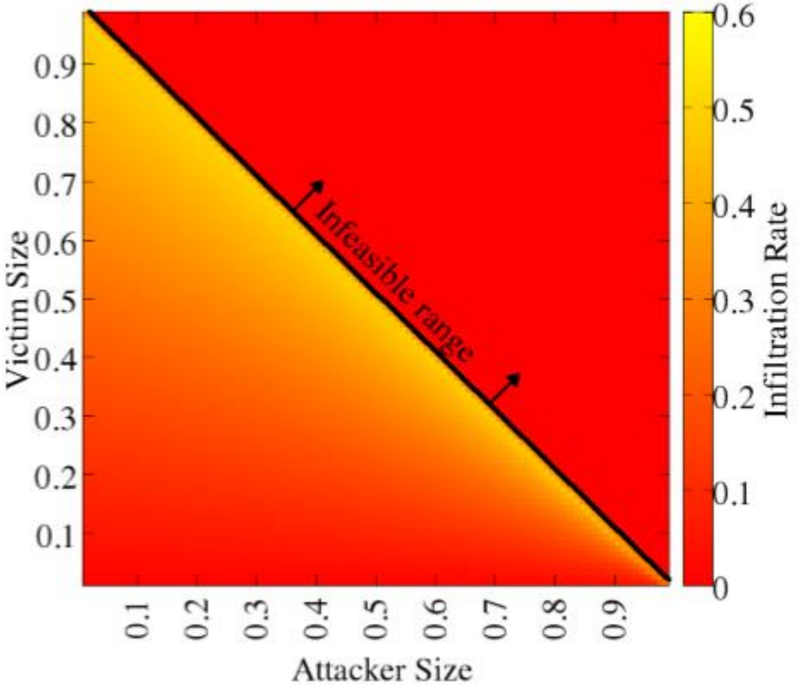
- An attacker joins the victim pool.
- She should split her computational power into solo mining and malicious pool mining (BWH attack).
- She receives unearned wages while only pretending to contribute work to the pool.



Block Withholding (BWH) Attack

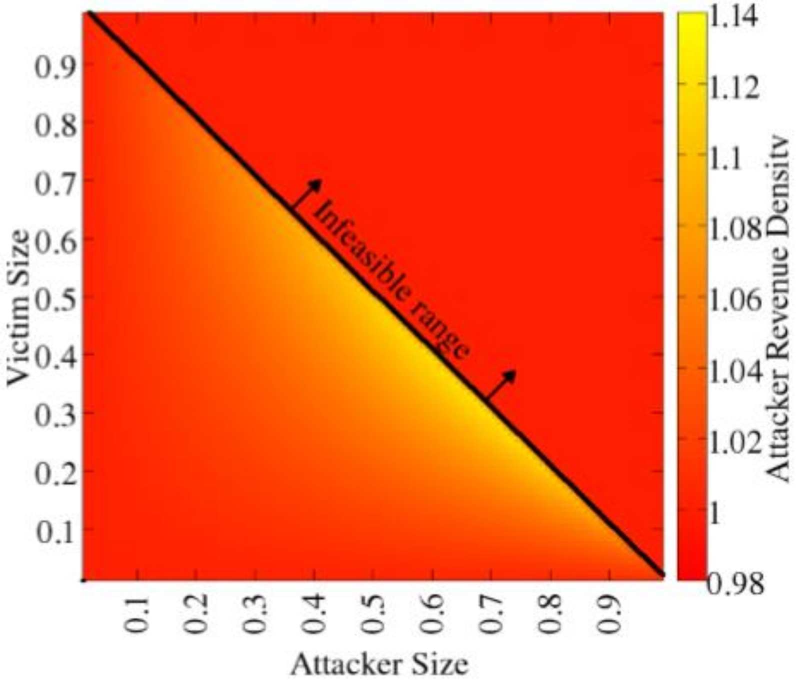


Result



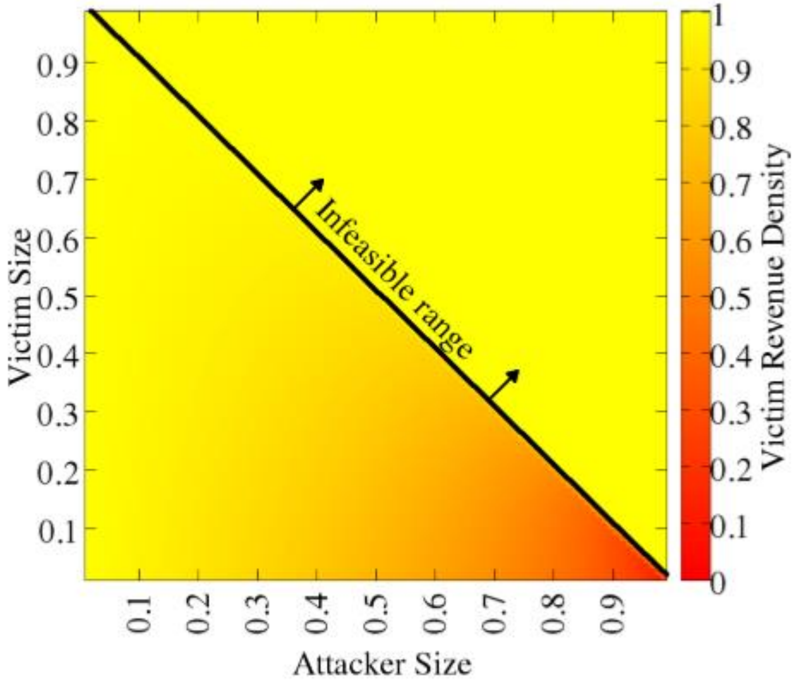
(a) $x_{1,2}$

Infiltration mining power



(b) r_1

Attacker relative reward



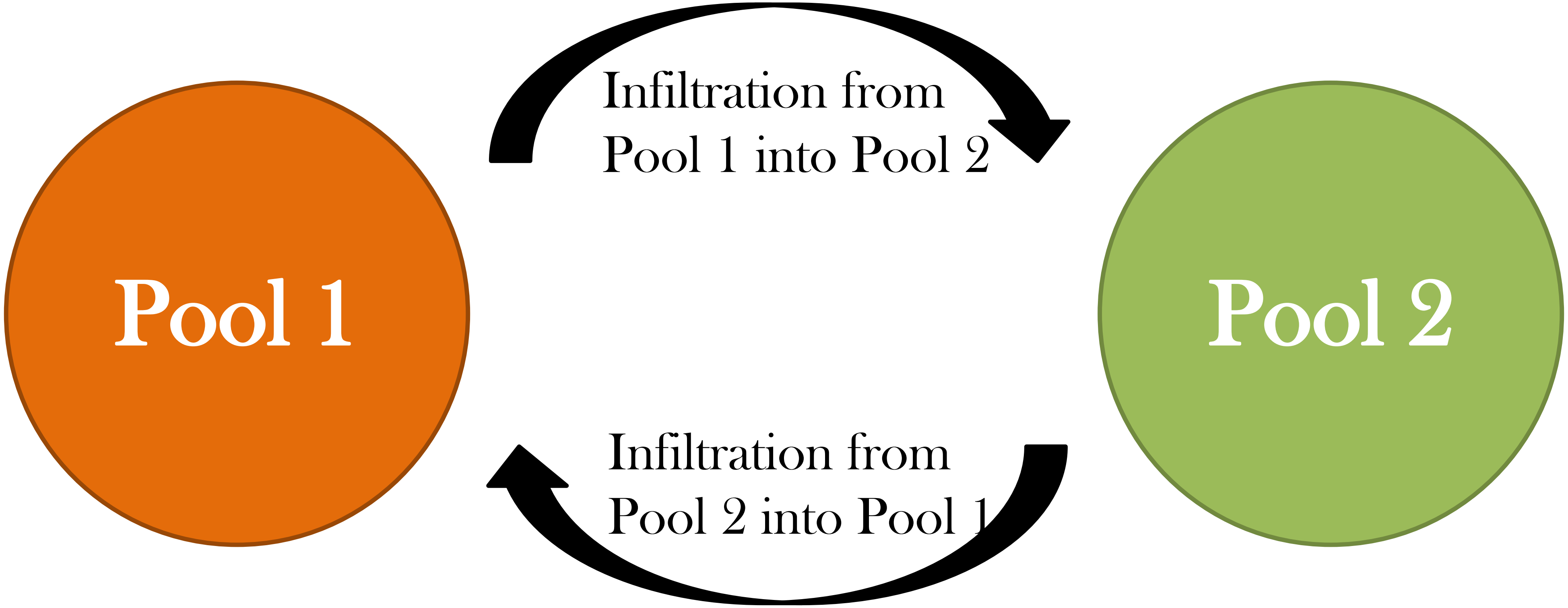
(c) r_2

Victim relative reward

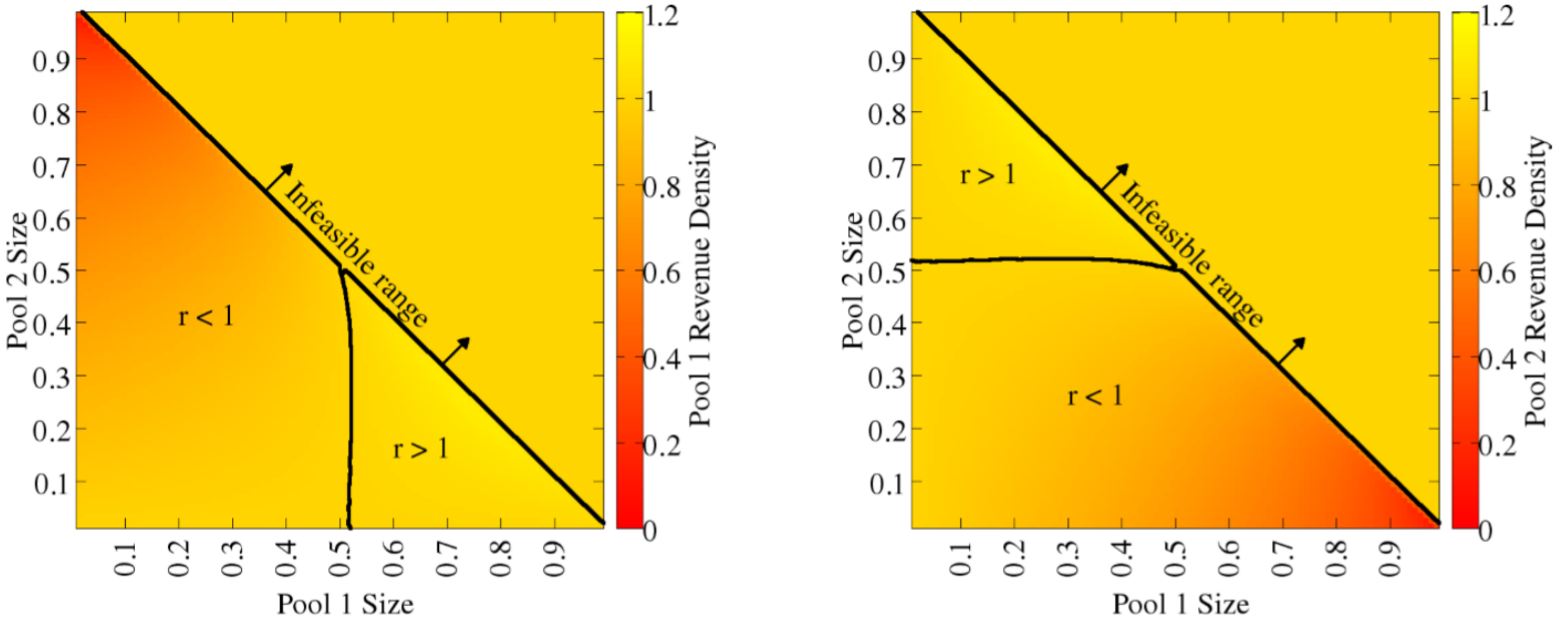
❖ The BWH attack is always profitable.

The Miners’ dilemma (S&P 2015)

❖ Pools can launch the BWH attack each other through infiltration.



Result



(c) r_1 (d) r_2

❖When they execute the BWH attack each other, both of them make a loss.

The Miners' dilemma (S&P 2015)

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	$(r_1 = \tilde{r}_1 < 1, r_2 > 1)$	$(\tilde{r}_1 < r_1 < 1, \tilde{r}_2 < r_2 < 1)$

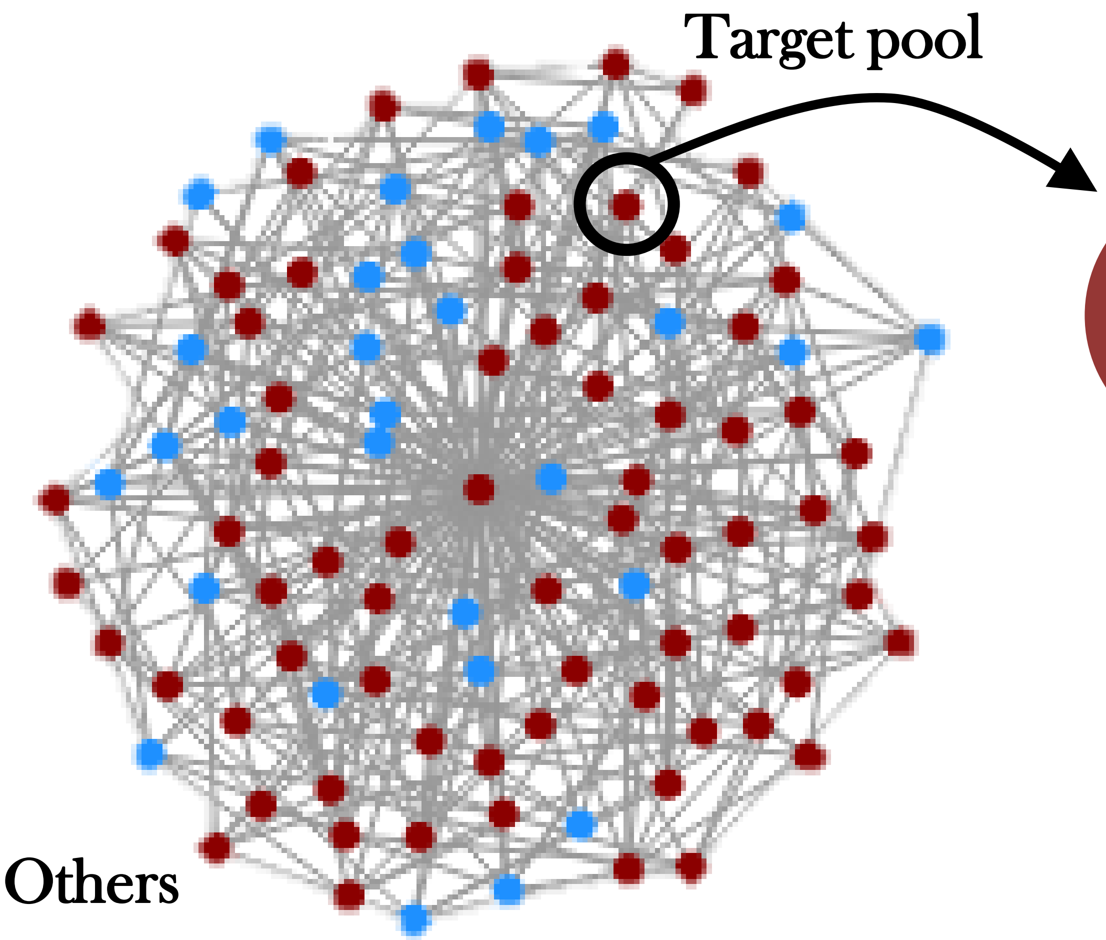
From "The Miner's Dilemma"

❖ The equilibrium reward of the pool is **inferior** compared to the no-attack scenario.

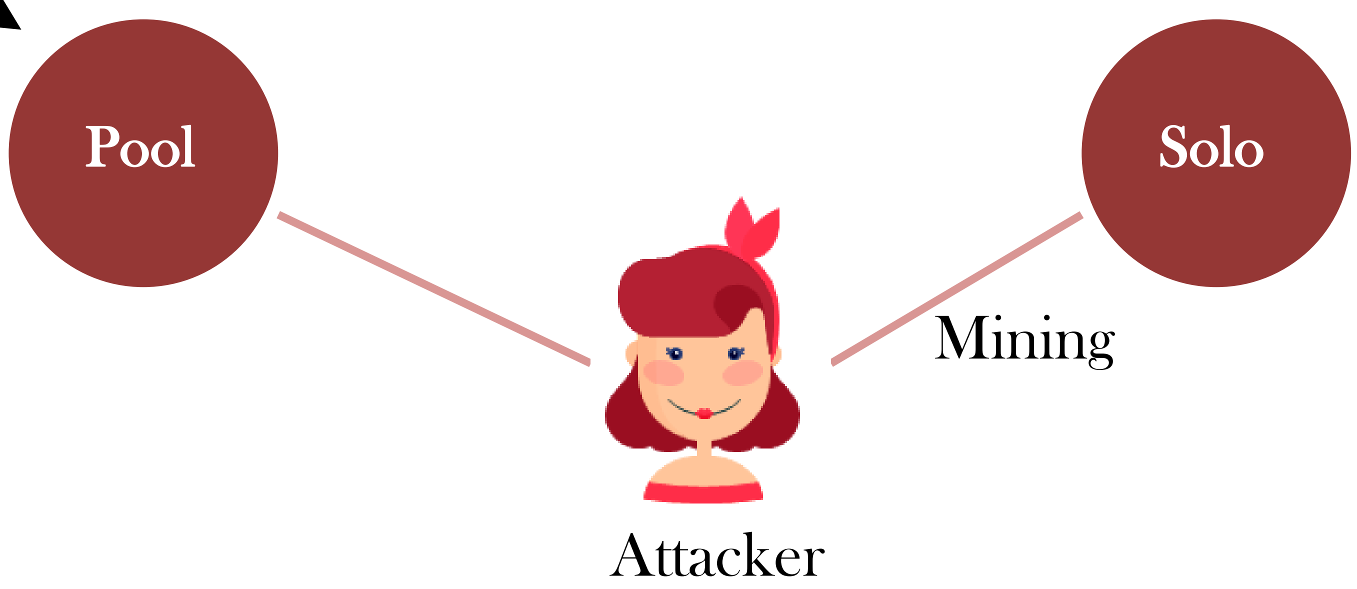
❖ The fact that the BWH attack is **not common** may be explained.

Fork After Withholding Attack

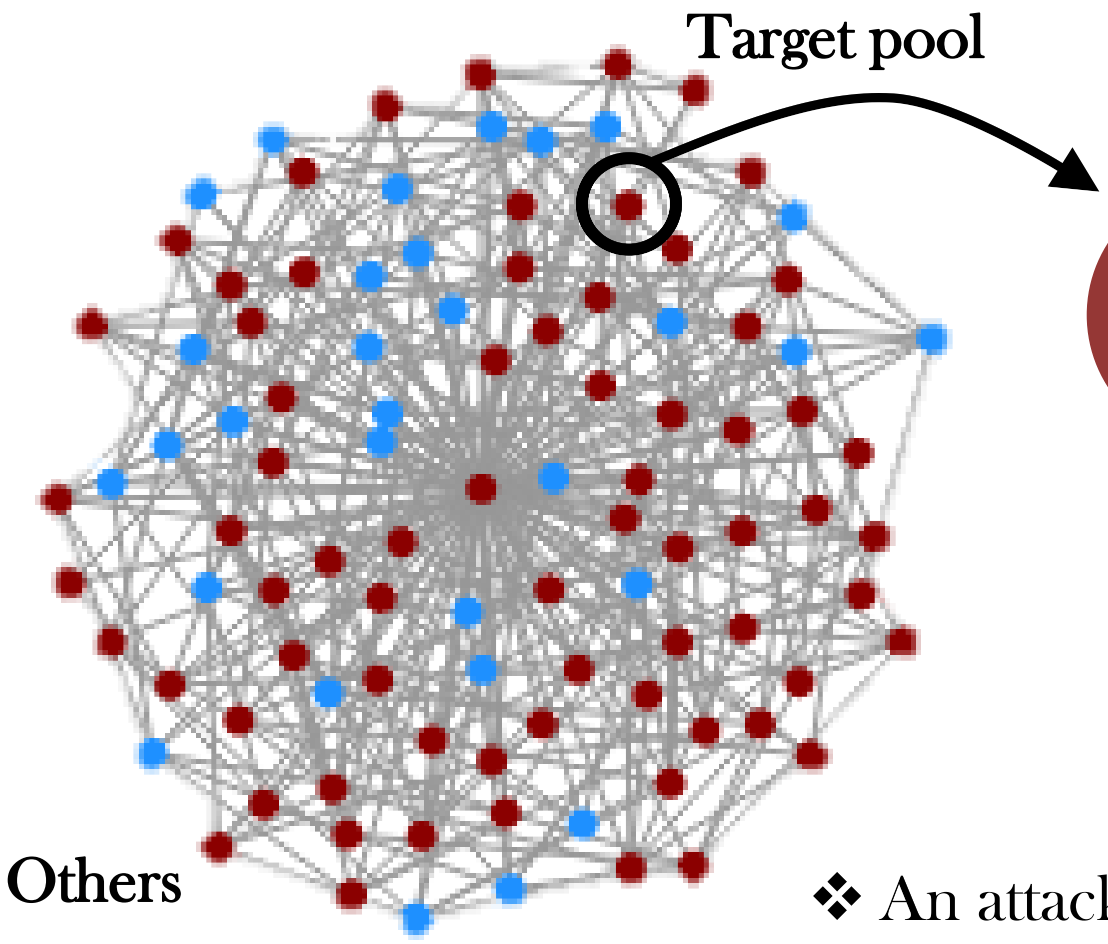
FAW Attack Against One Pool



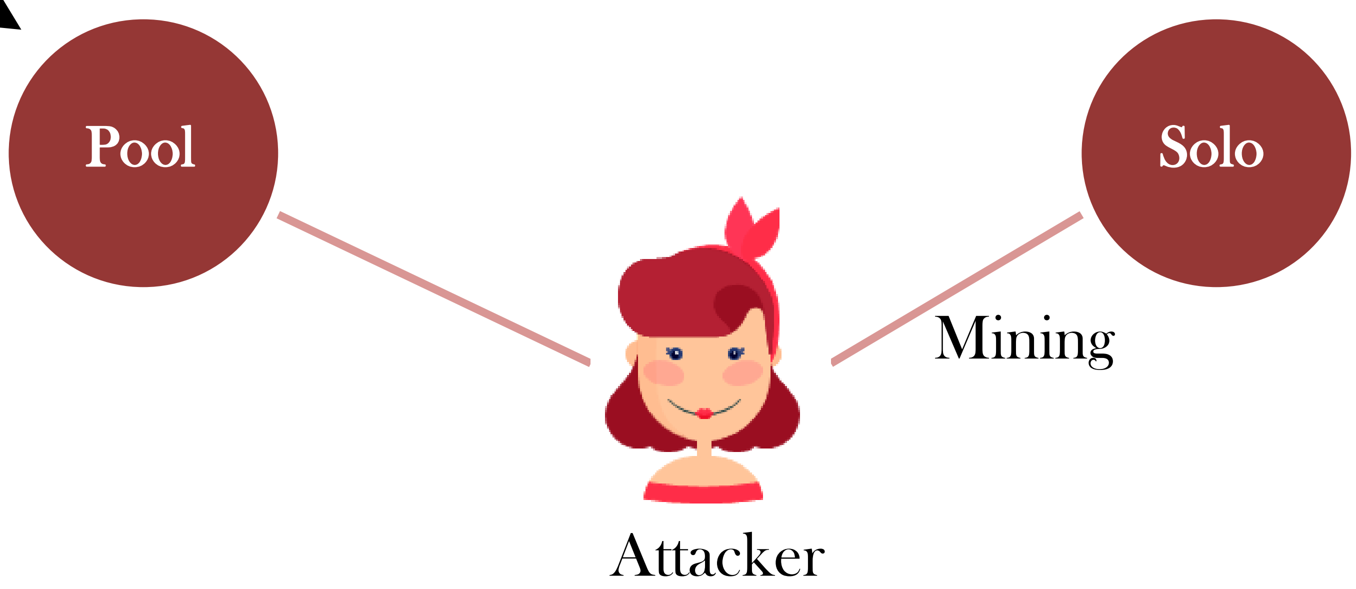
Submit an FPoW to the pool only if others generate another block. Otherwise, throw away her FPoW.



FAW Attack Against One Pool



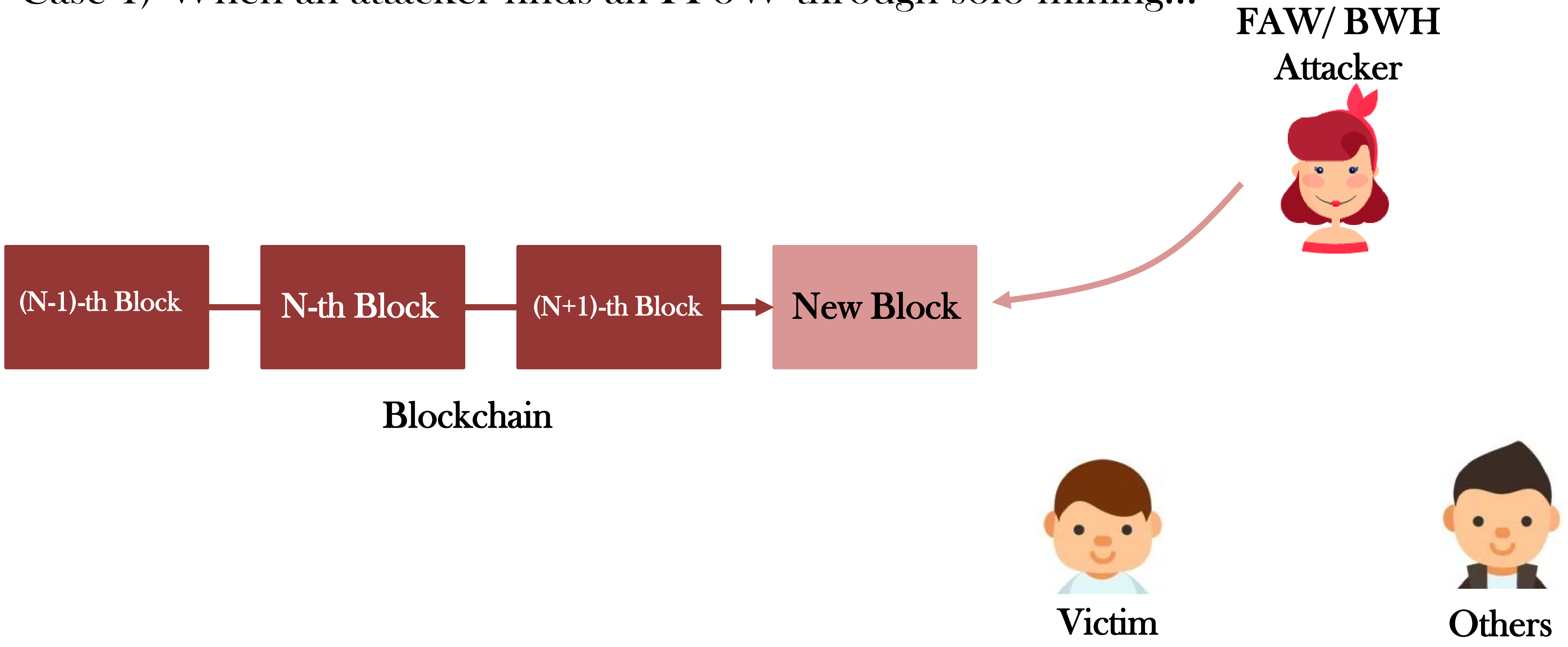
Submit an FPoW to the pool only if others generate another block. Otherwise, throw away her FPoW.



❖ An attacker generates forks intentionally through a pool!

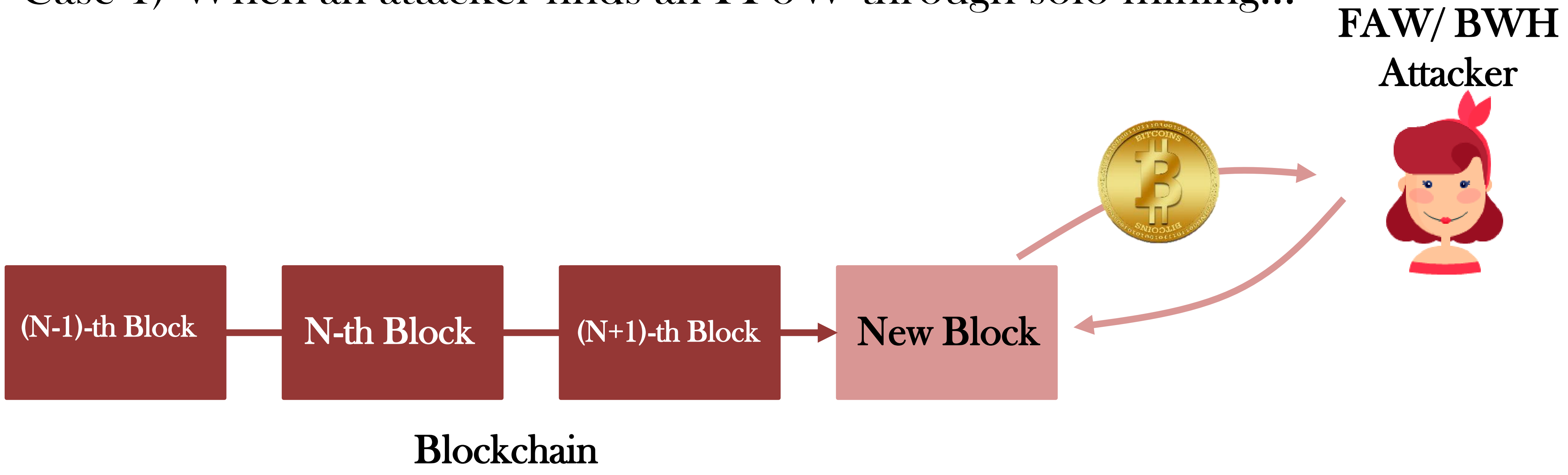
FAW vs BWH

Case 1) When an attacker finds an FPoW through solo mining...



FAW vs BWH

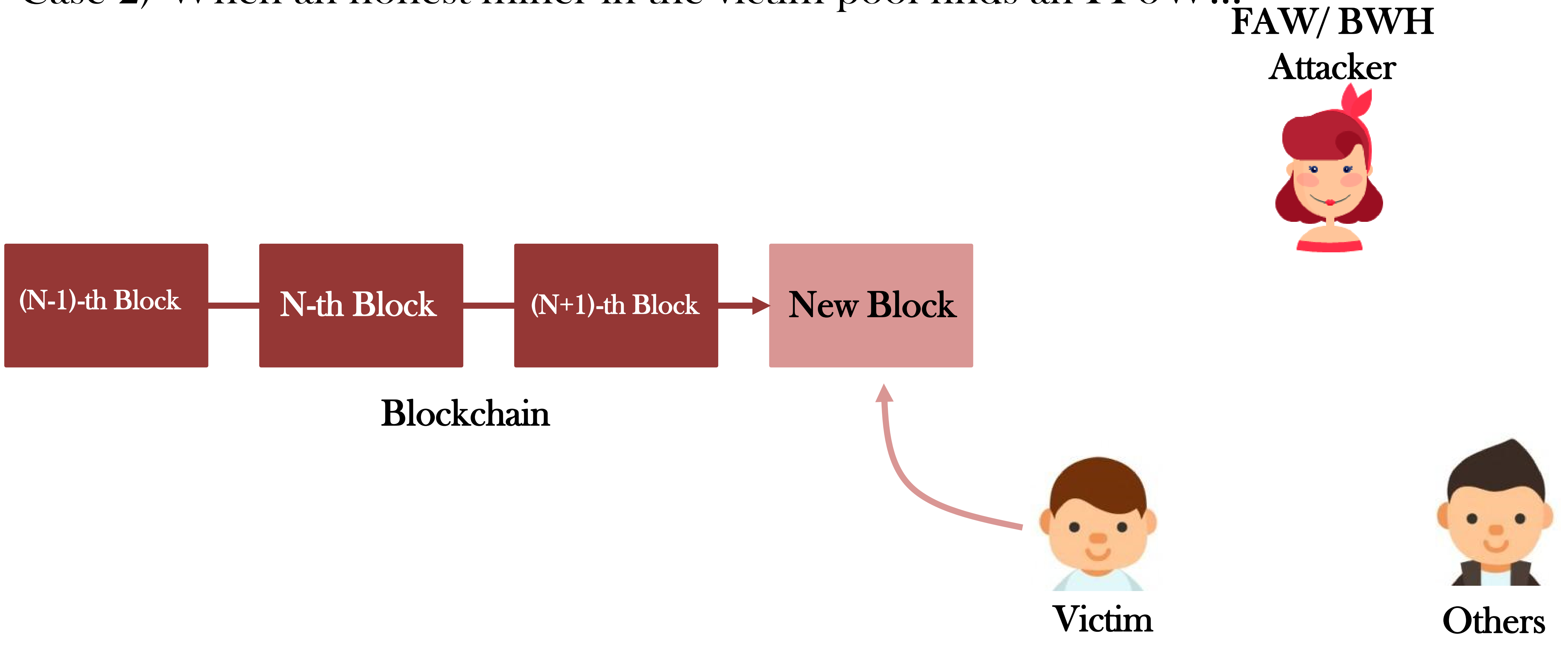
Case 1) When an attacker finds an FPoW through solo mining...



The attacker earns the block reward.

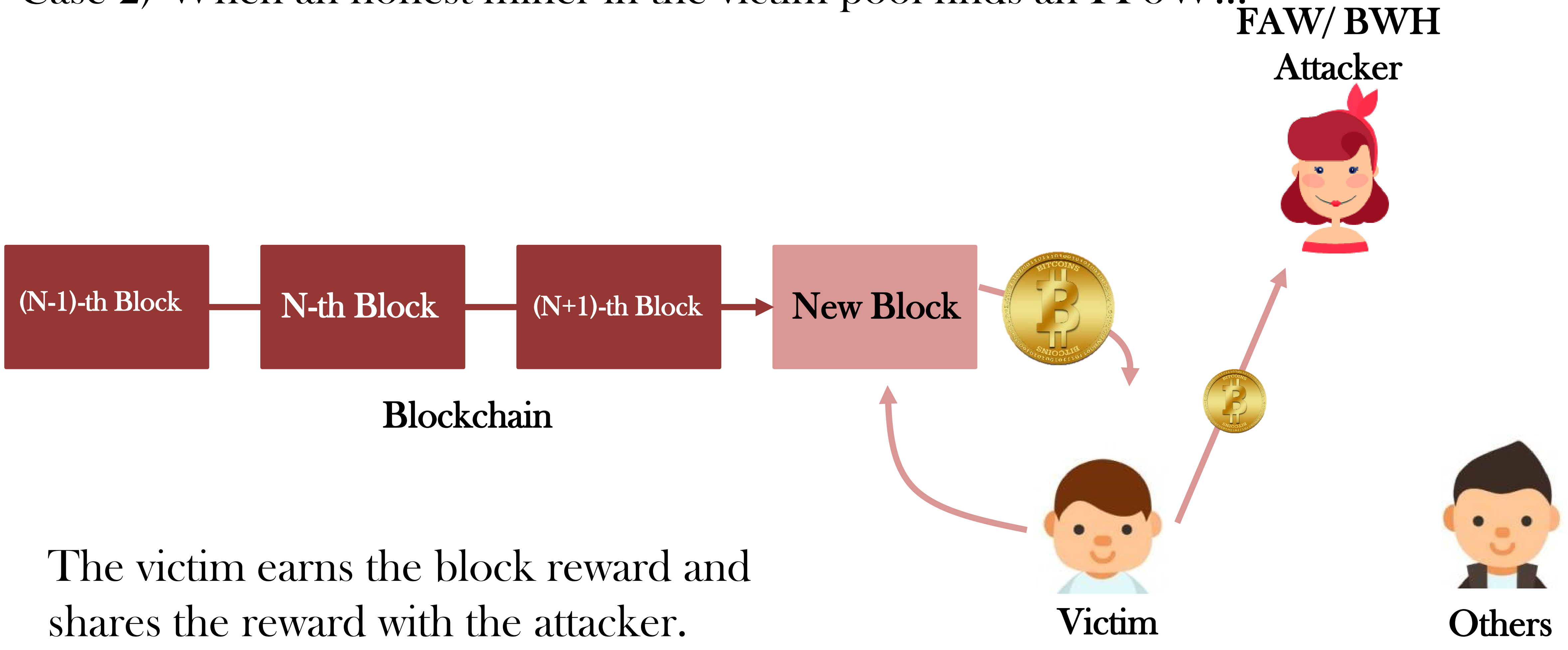
FAW vs BWH

Case 2) When an honest miner in the victim pool finds an FPoW…



FAW vs BWH

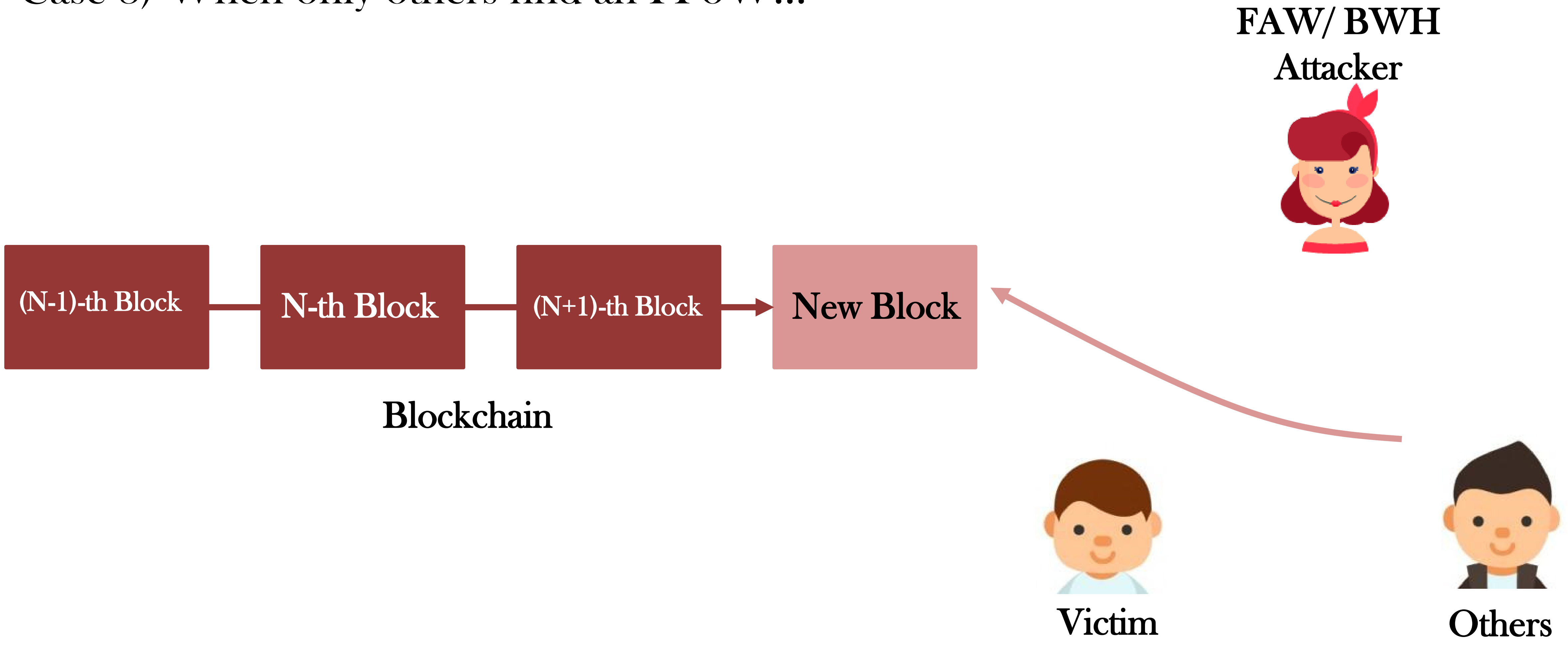
Case 2) When an honest miner in the victim pool finds an FPoW...



The victim earns the block reward and shares the reward with the attacker.

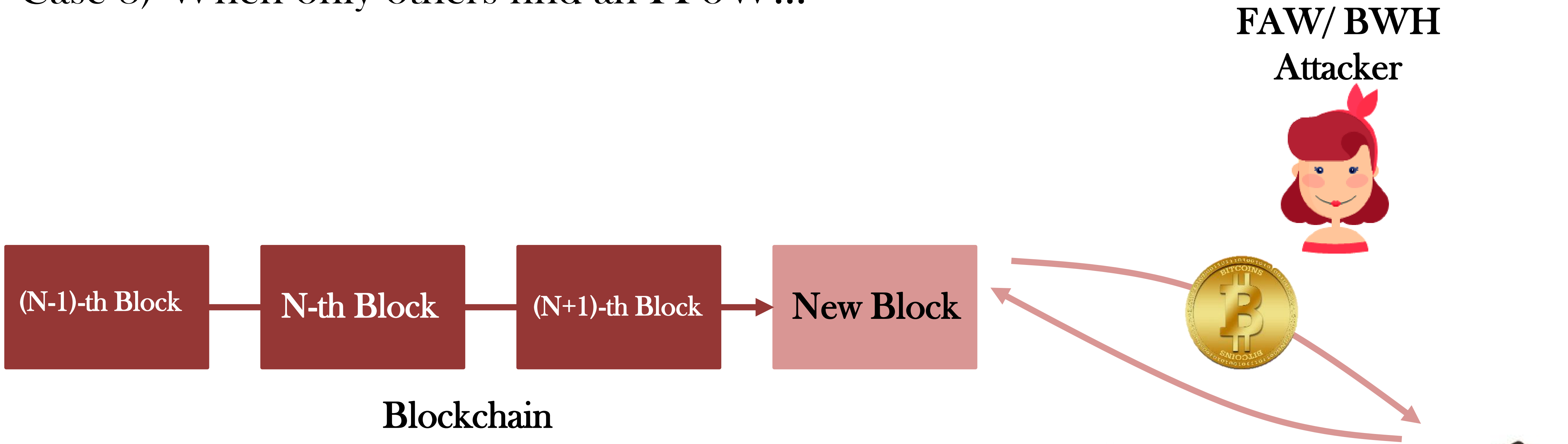
FAW vs BWH

Case 3) When only others find an FPoW…



FAW vs BWH

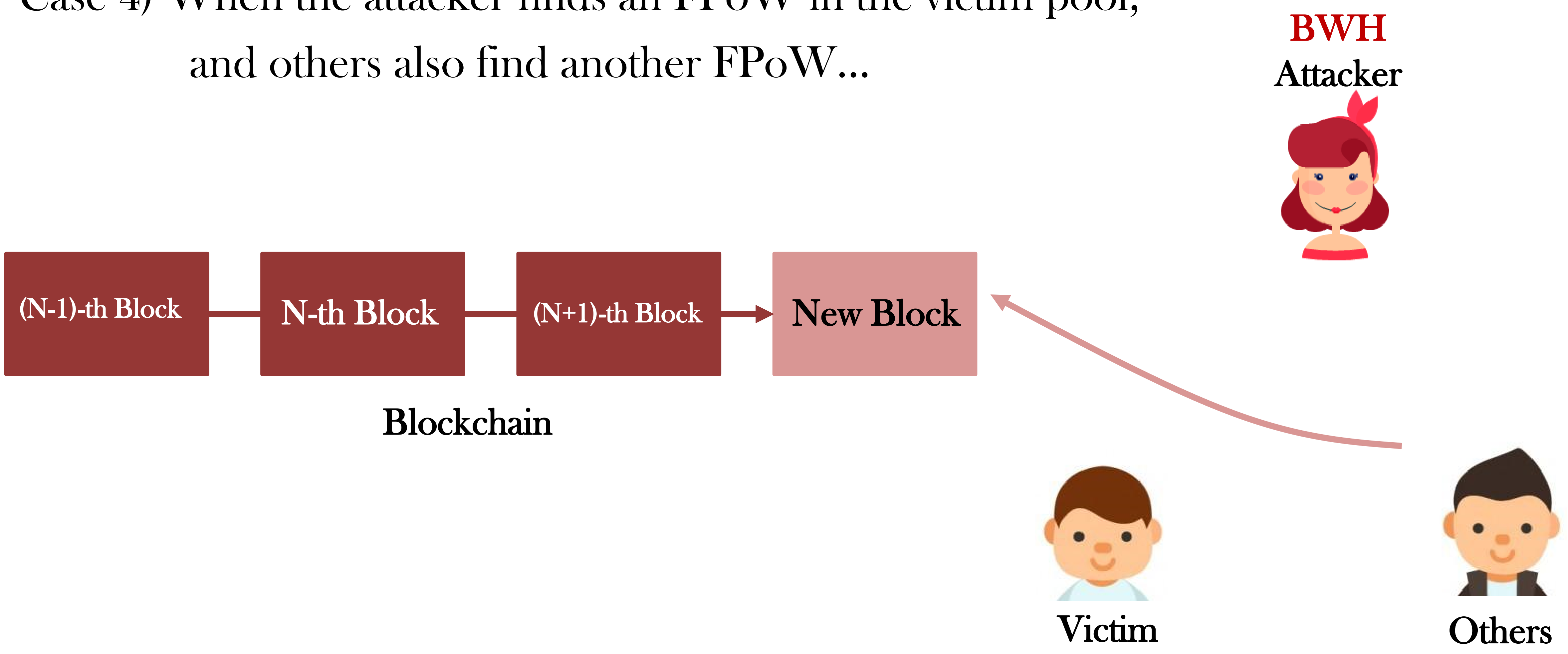
Case 3) When only others find an FPoW…



Others earn the block reward.

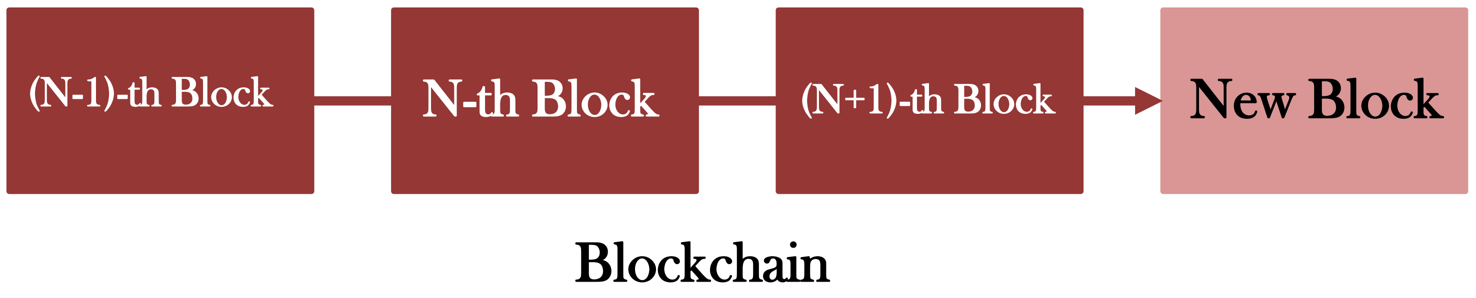
FAW vs BWH

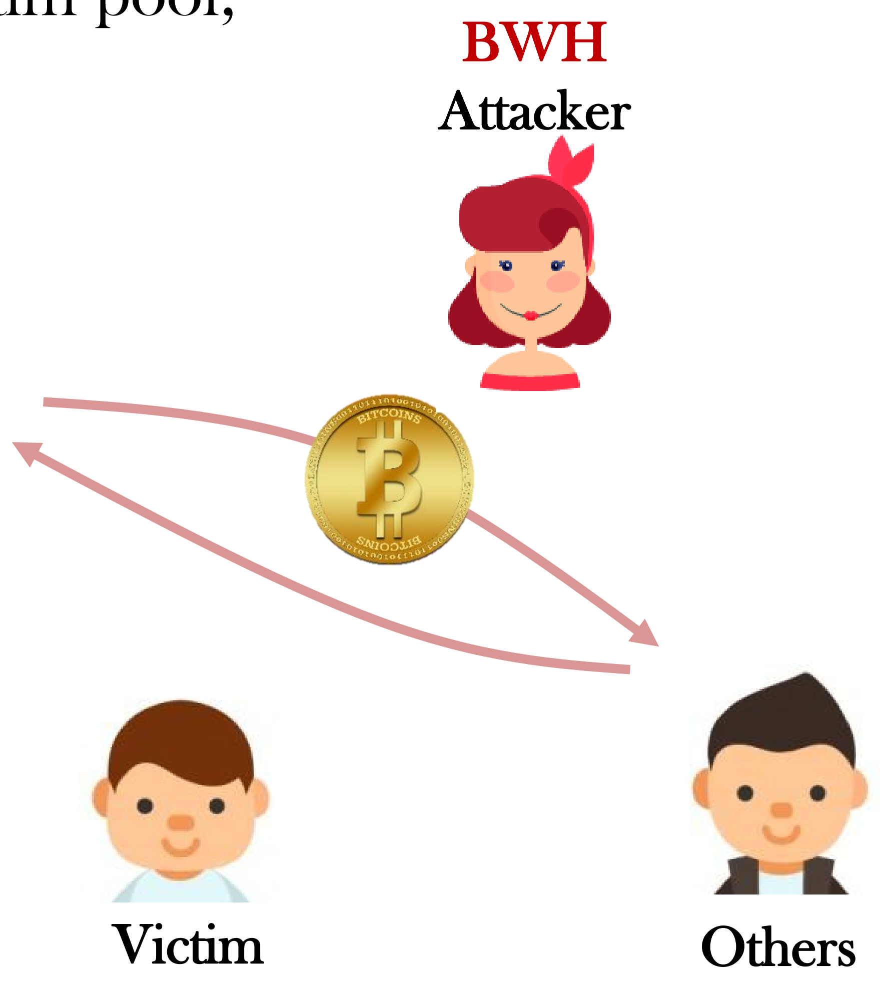
Case 4) When the attacker finds an FPoW in the victim pool,
and others also find another FPoW…



FAW vs BWH

Case 4) When the attacker finds an FPoW in the victim pool,
and others also find another FPoW…

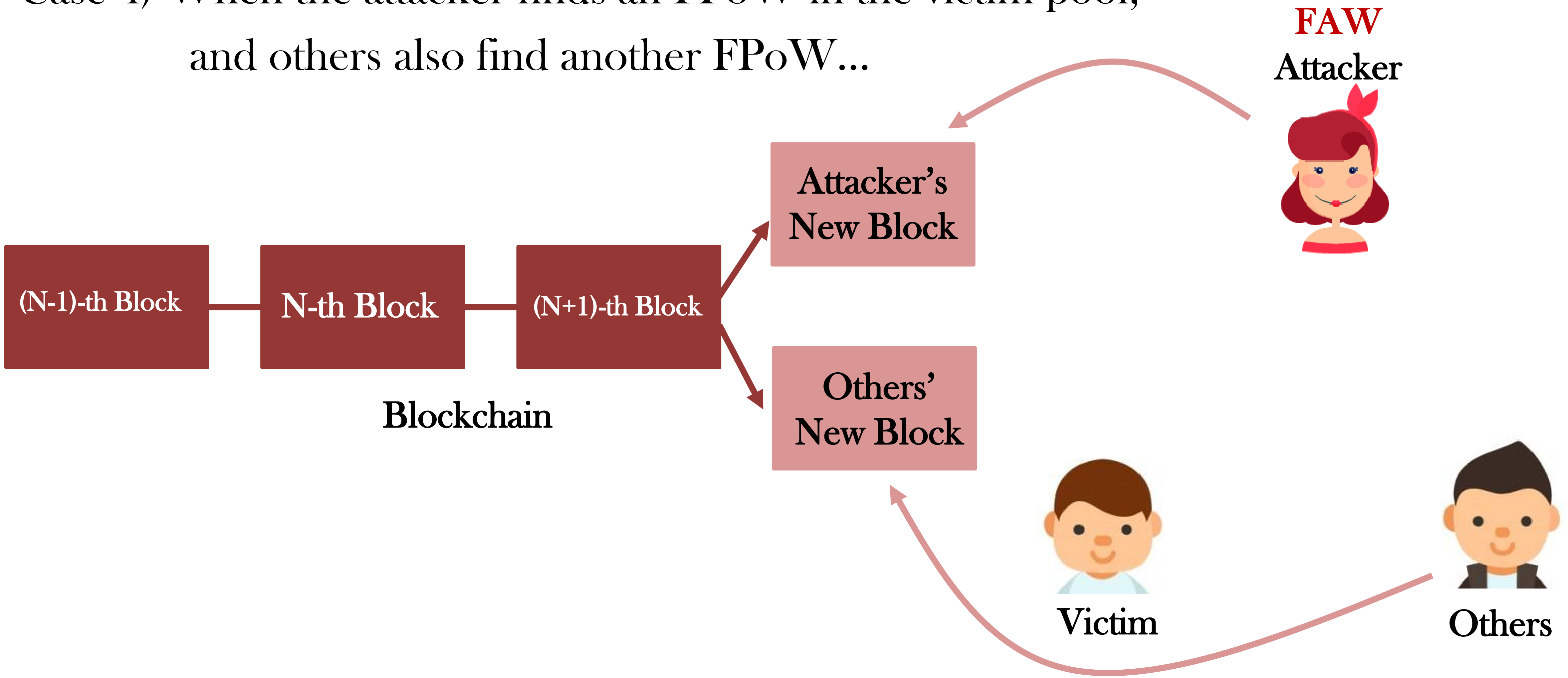




Others earn the block reward.

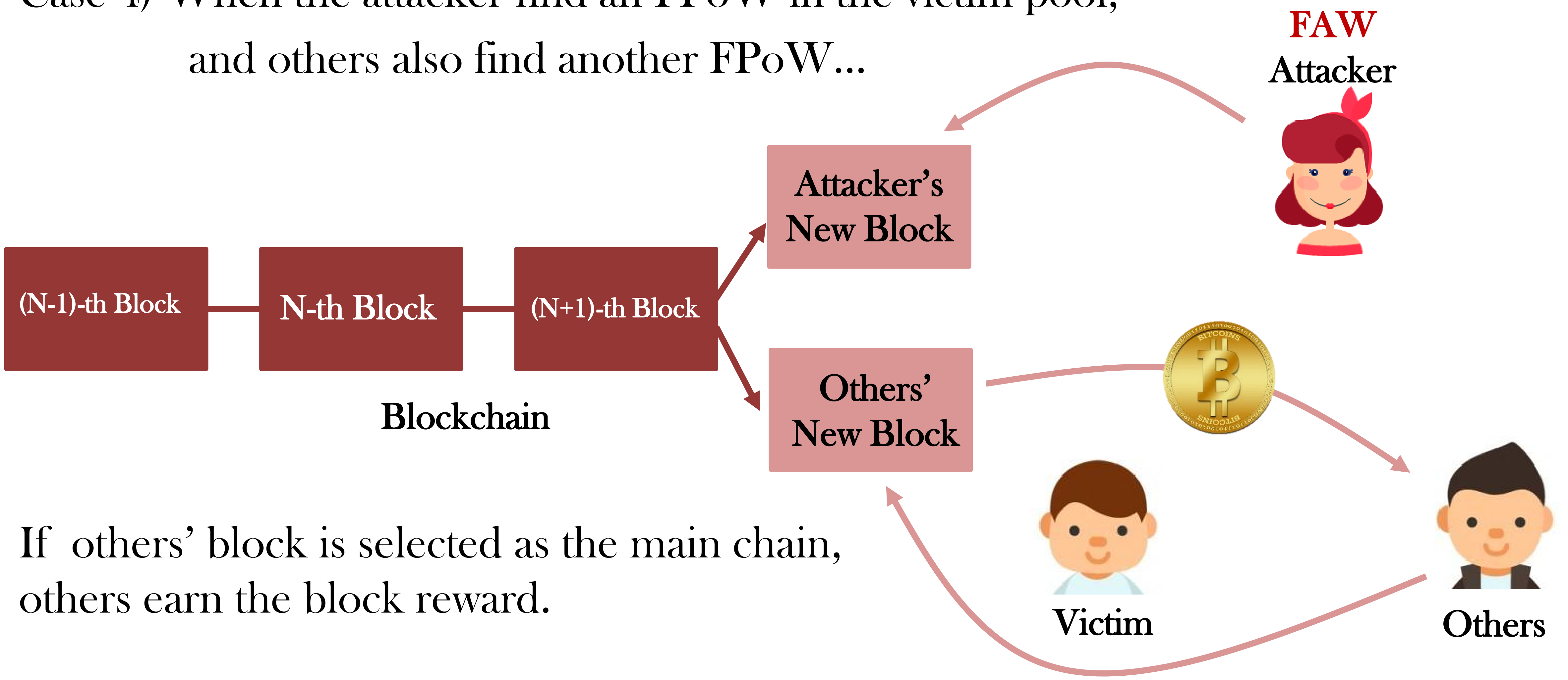
FAW vs BWH

Case 4) When the attacker finds an FPoW in the victim pool,
and others also find another FPoW…



FAW vs BWH

Case 4) When the attacker find an FPoW in the victim pool,
and others also find another FPoW…

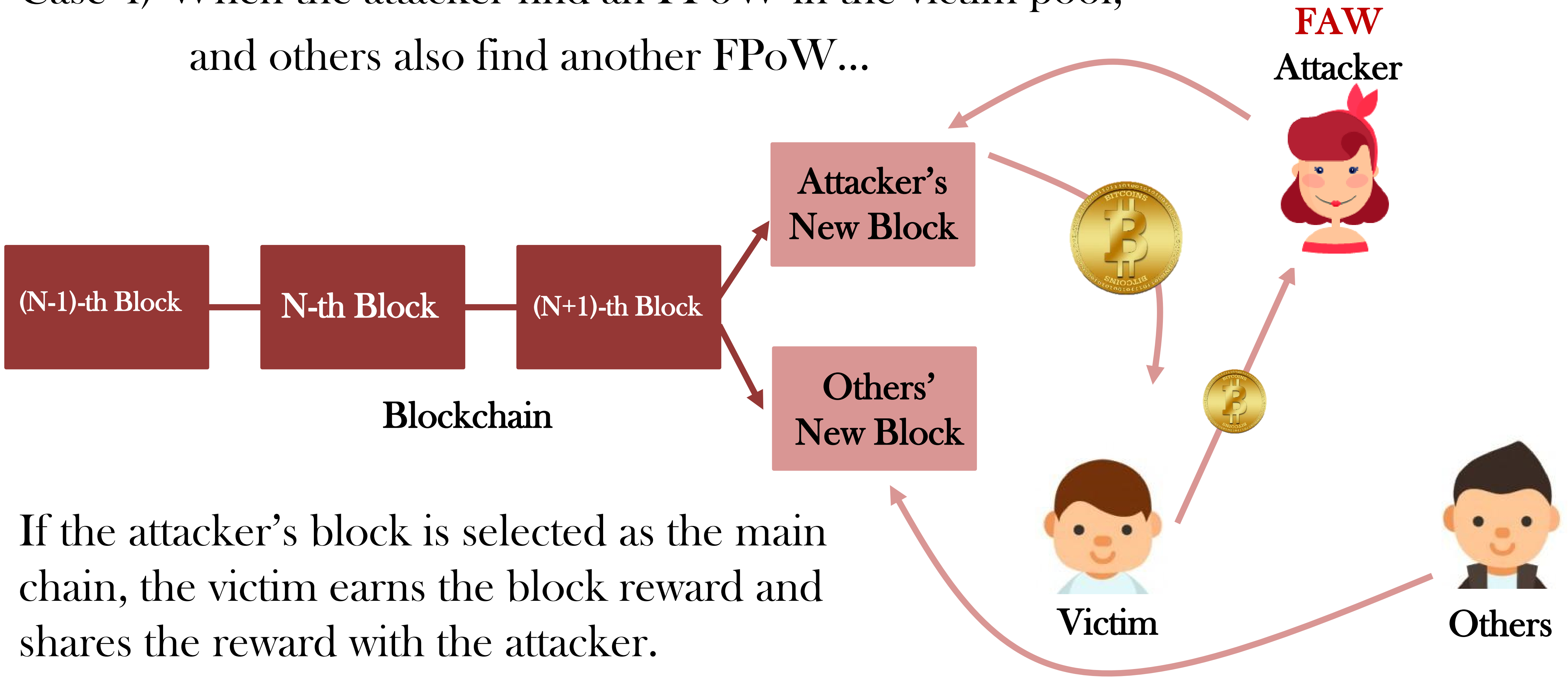


If others' block is selected as the main chain,
others earn the block reward.

FAW vs BWH

Case 4) When the attacker find an FPoW in the victim pool,

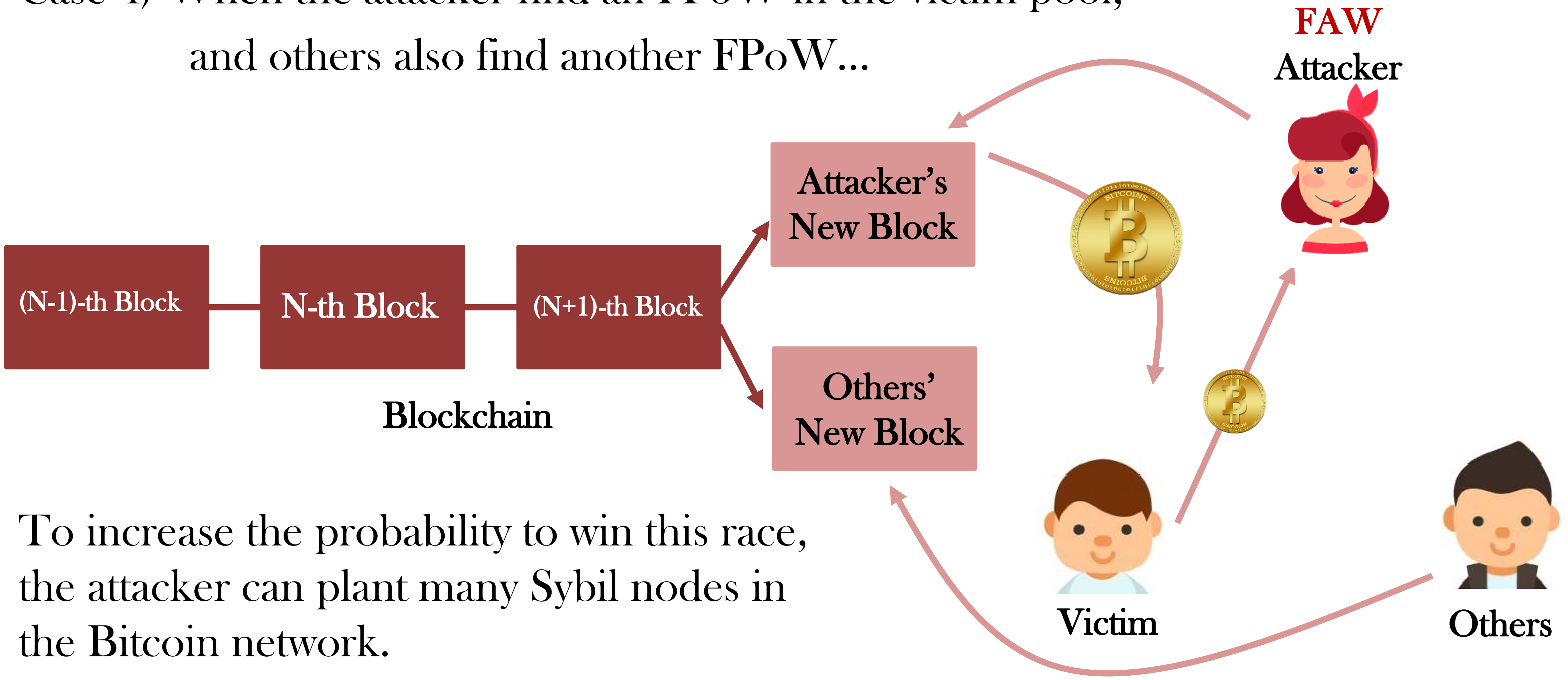
and others also find another FPoW…



If the attacker's block is selected as the main chain, the victim earns the block reward and shares the reward with the attacker.

FAW vs BWH

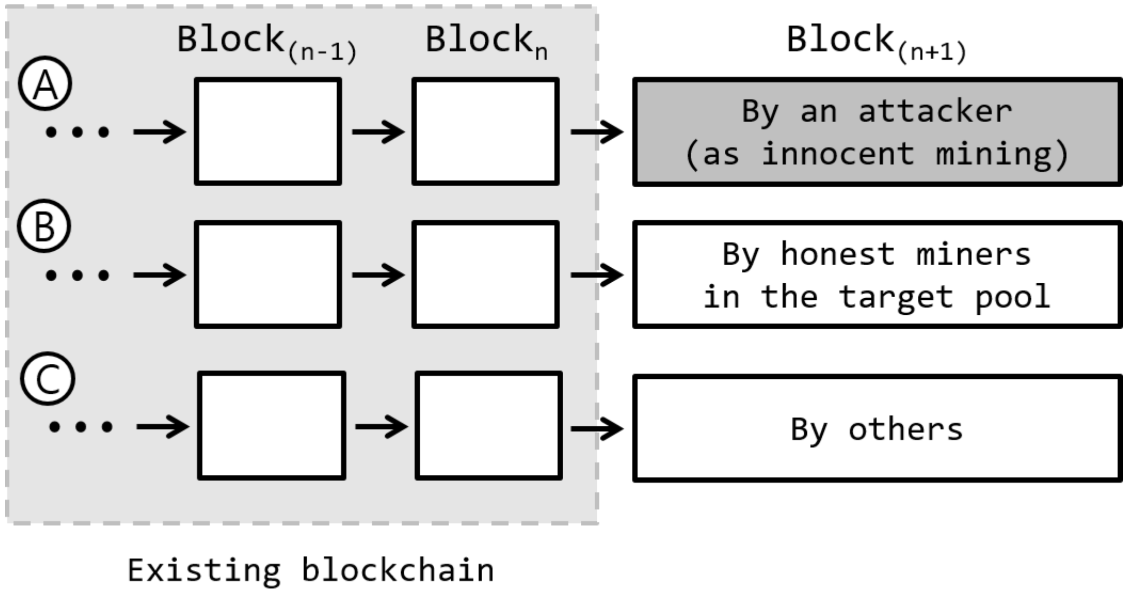
Case 4) When the attacker find an FPoW in the victim pool, and others also find another FPoW…



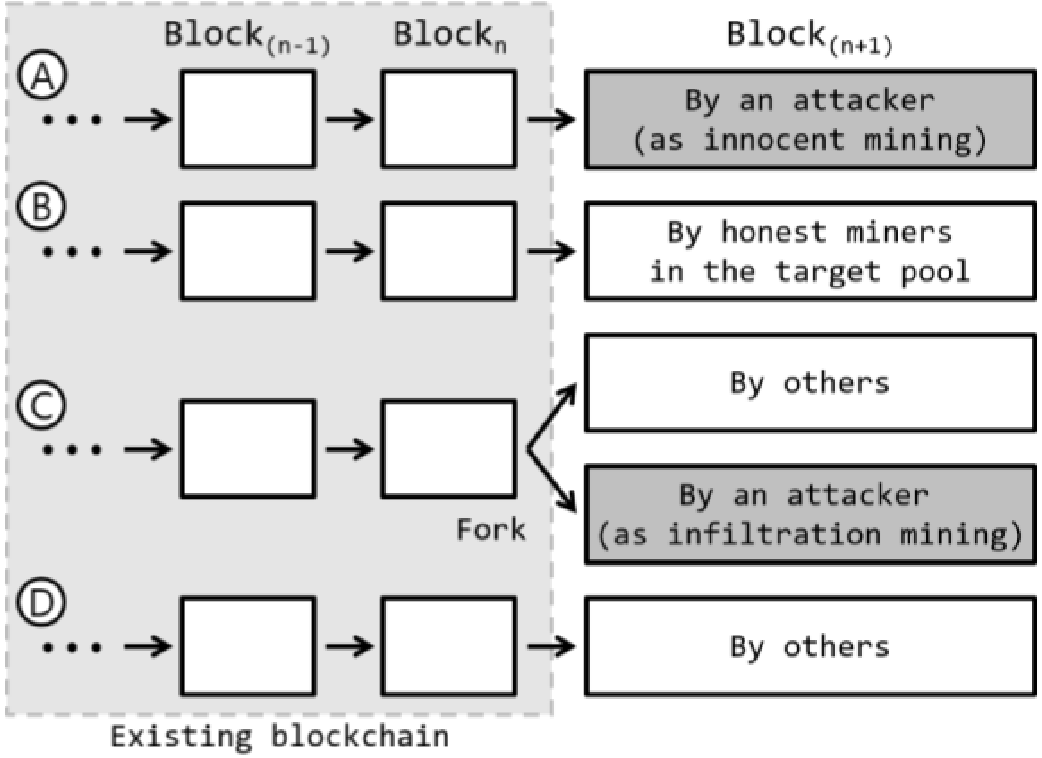
To increase the probability to win this race, the attacker can plant many Sybil nodes in the Bitcoin network.

FAW vs BWH

❖ The BWH Attack

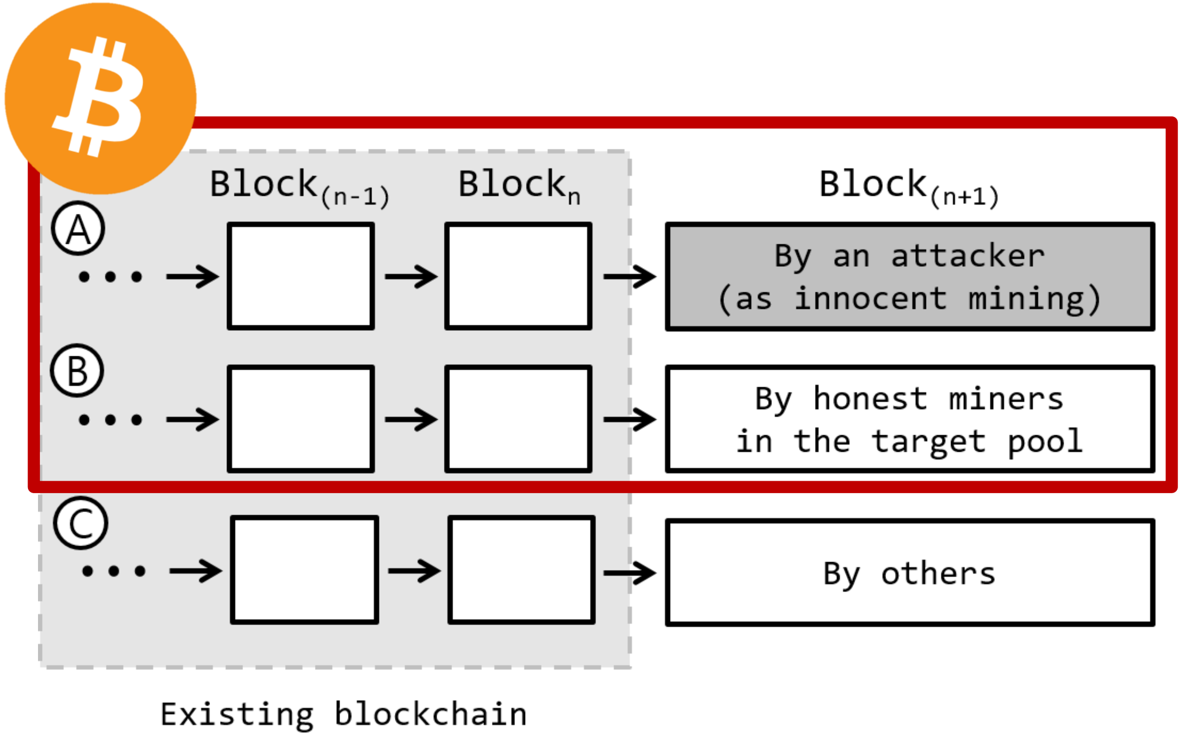


❖ The FAW Attack

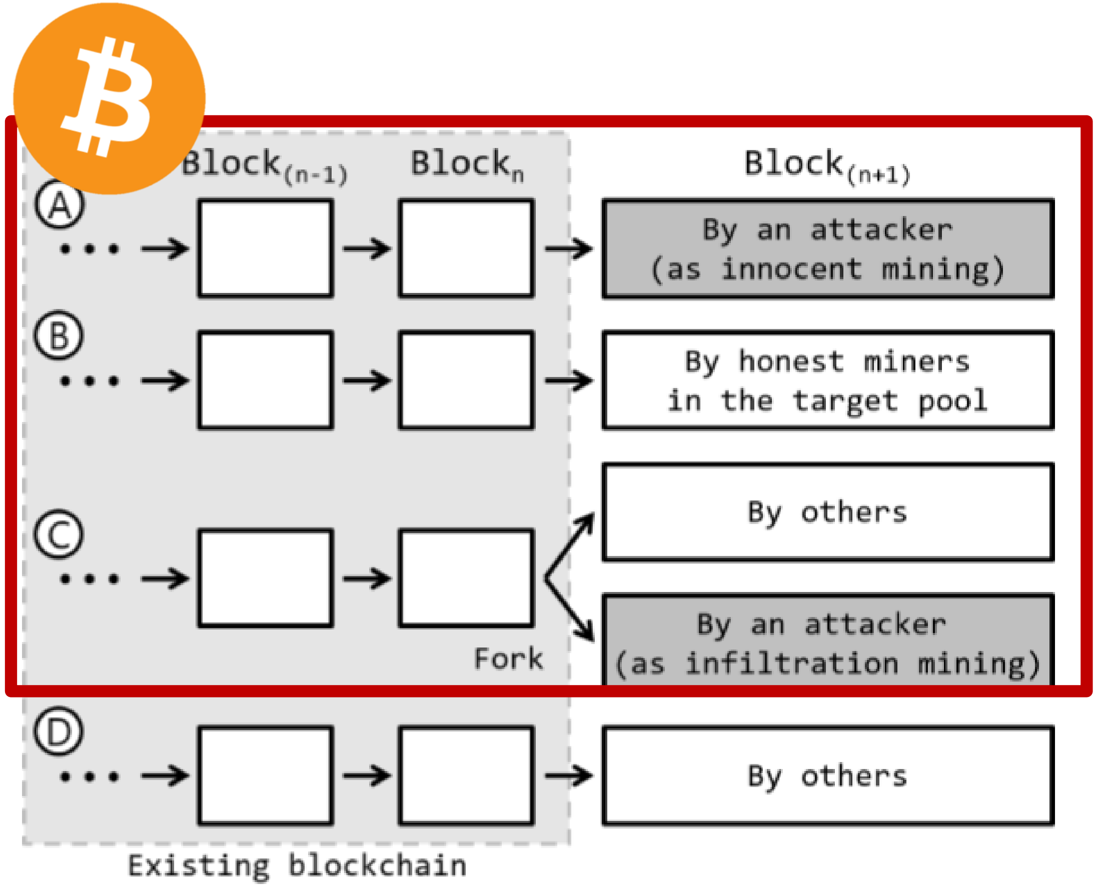


FAW vs BWH

❖ The BWH Attack



❖ The FAW Attack



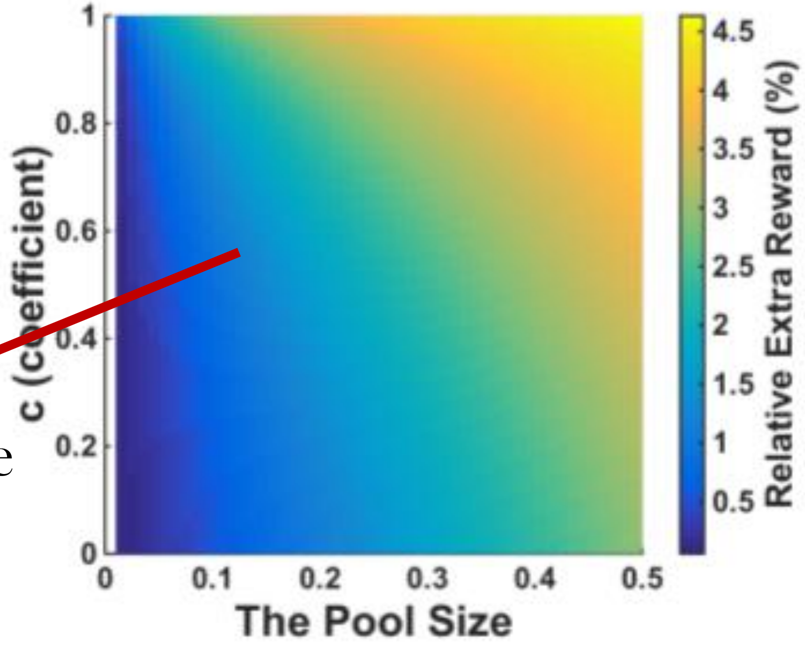
FAW vs BWH

	Attacker	Victim	Others
FAW			
BWH			

Numerical Analysis

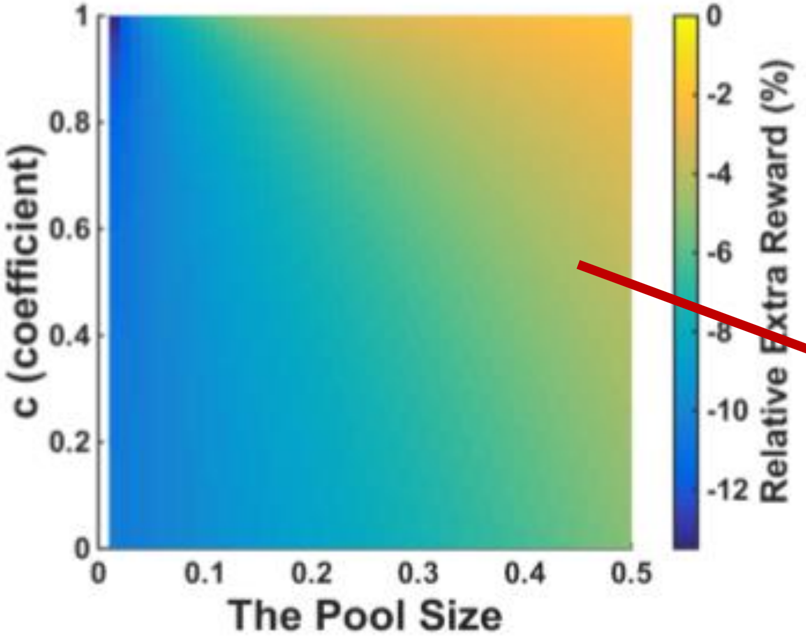
- An attacker possesses 20% power (0.2).
- A variable *c* represents a probability that an attacker's FPoW will be selected as the main chain.

Attacker



Always positive

Victim



Always negative

Numerical Analysis

An attacker's power — Increasing →

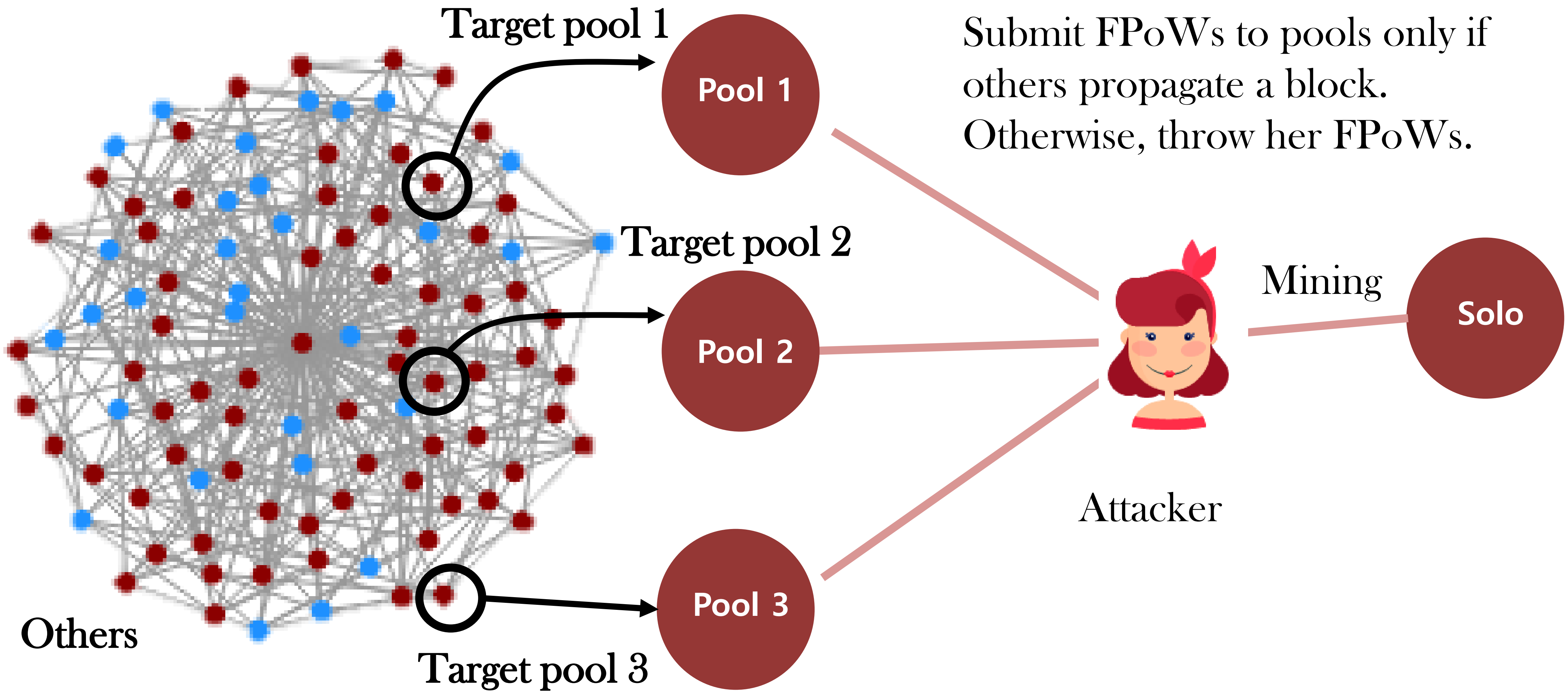
c \ α	0.1	0.2	0.3	0.4
0	0.53 (%)	1.14 (%)	1.85 (%)	2.7 (%)
0.25	0.65 (%)	1.38 (%)	2.2 (%)	3.1 (%)
0.5	0.85 (%)	1.74 (%)	2.7 (%)	3.75 (%)
0.75	1.21 (%)	2.37 (%)	3.52 (%)	4.69 (%)
1	2.12 (%)	3.75 (%)	5.13 (%)	6.37 (%)

The case is equivalent to the case of the BWH attack.

Increasing

❖ We can see that the FAW attack is more profitable than the BWH attack numerically.

FAW Attack Against Multiple Pools



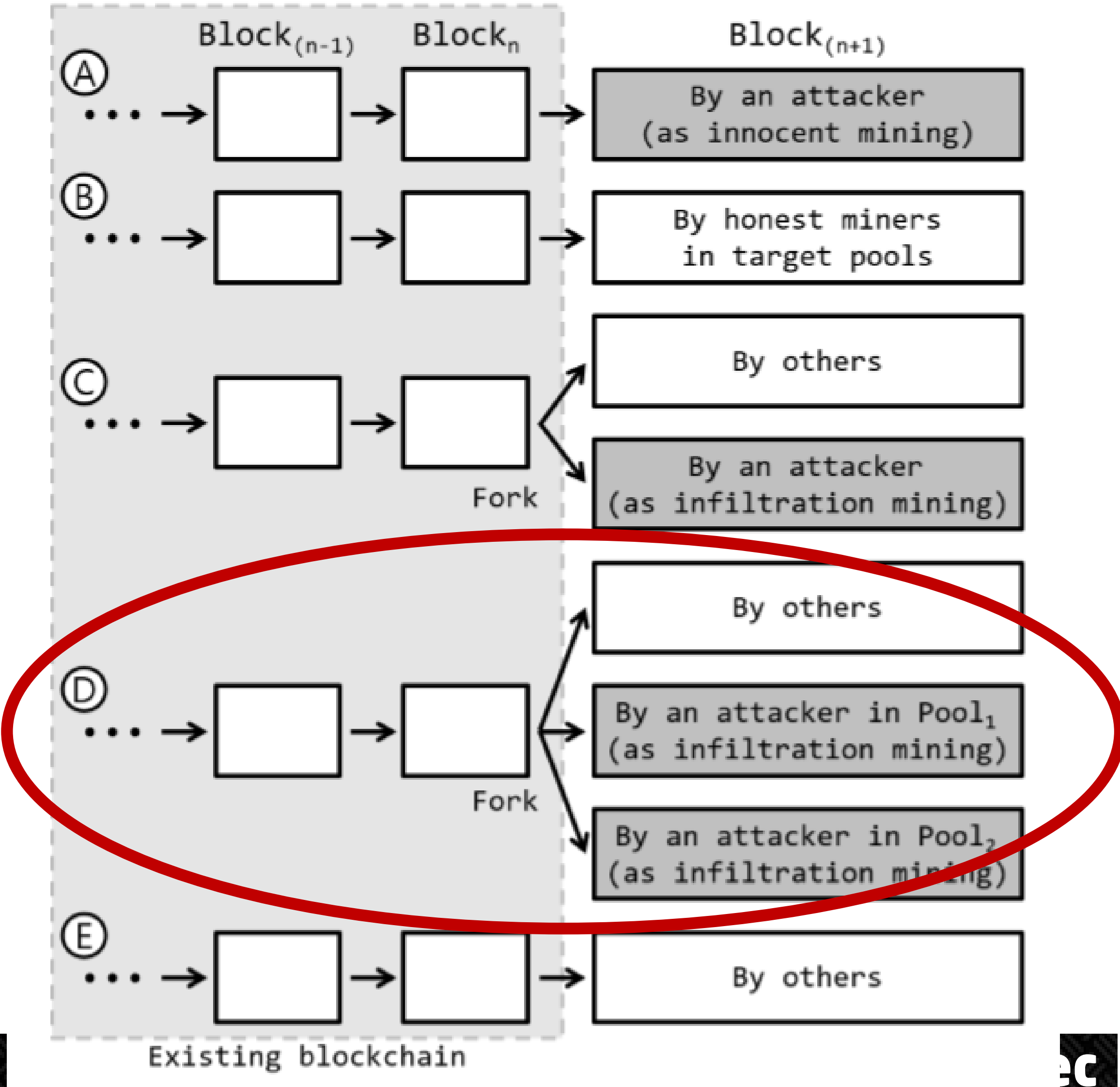
Submit FPoWs to pools only if others propagate a block. Otherwise, throw her FPoWs.

FAW Attack Against Two Pools

❖ When the attacker finds an FPoW in each of pools, a fork with three branches occurs.

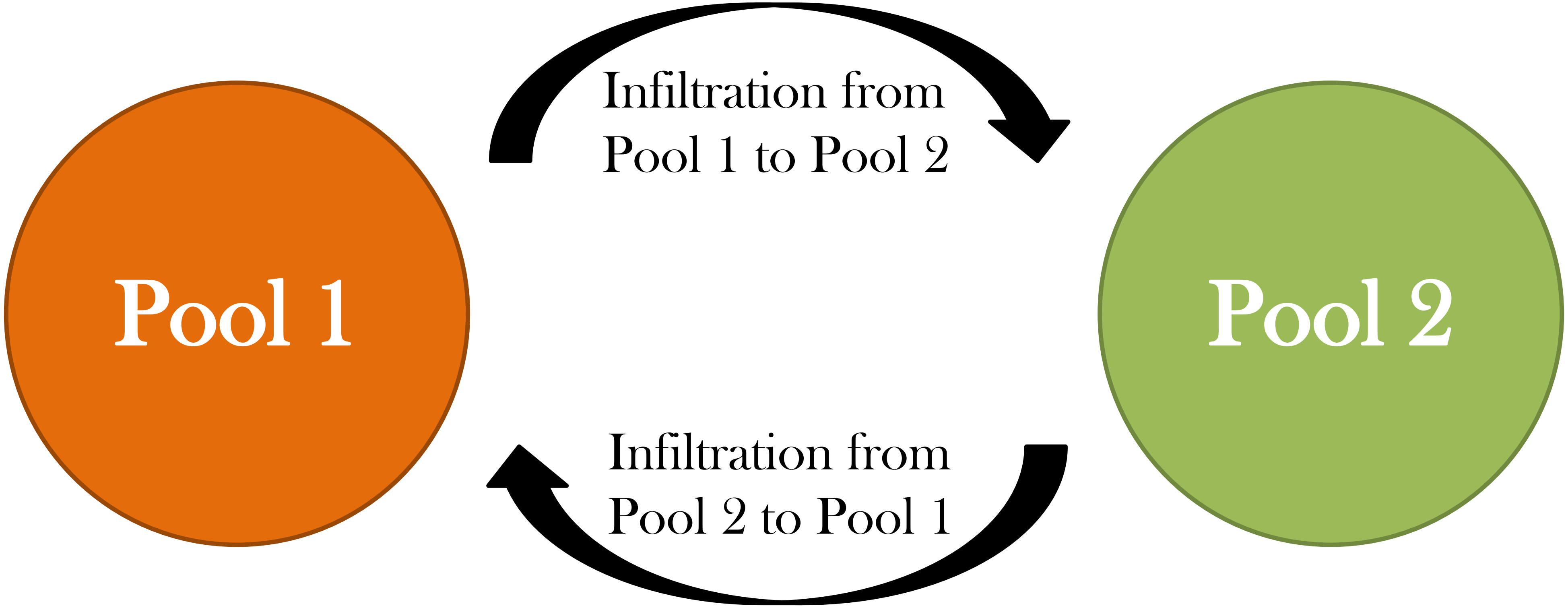
❖ In general, when n pools are targeted, a fork with $n + 1$ branches can occur.

❖ When considering the power distribution, the attacker can earn the extra reward 56% more than the BWH attacker.



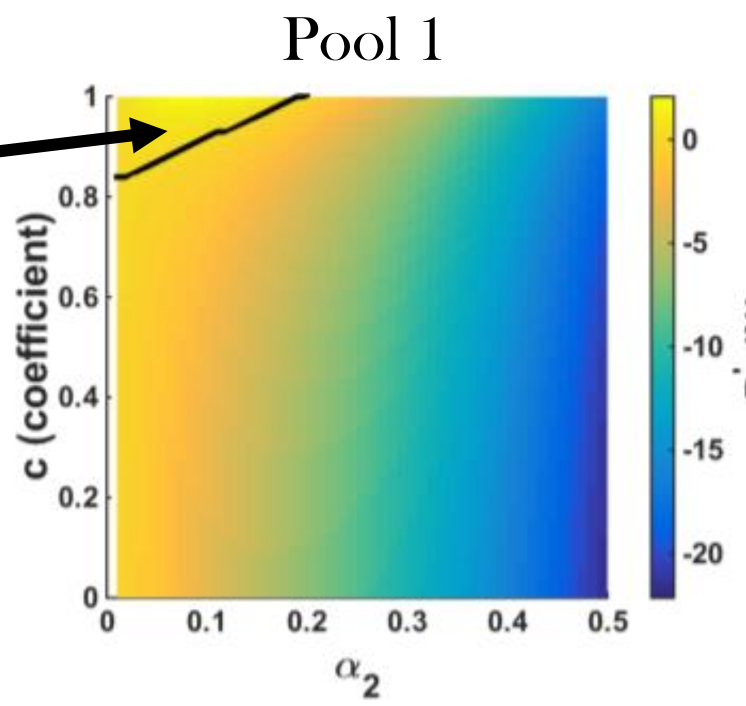
FAW Attack Game

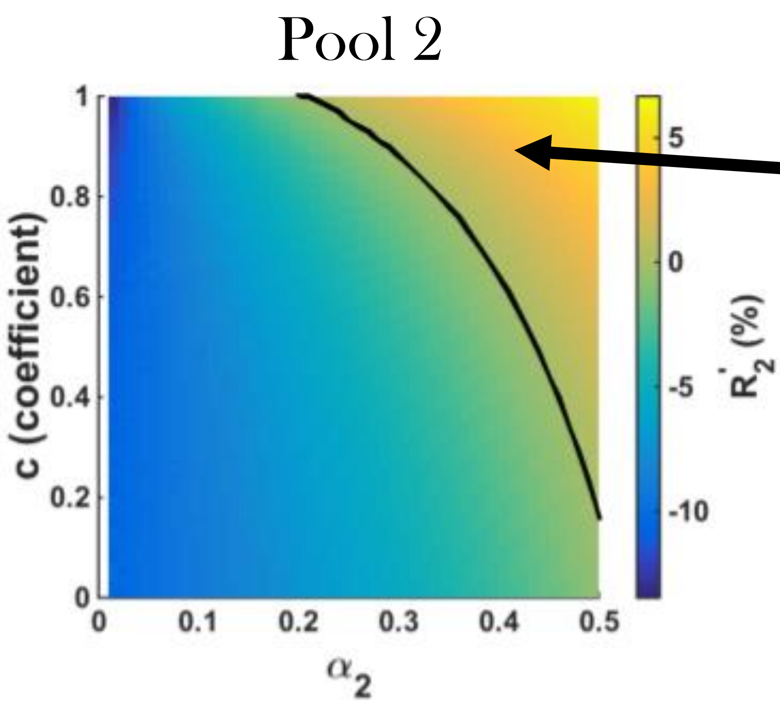
- Pools can launch the FAW attack each other through infiltration.



Dilemma? Not Always

Pool 1 can earn the extra reward in the Nash equilibrium.

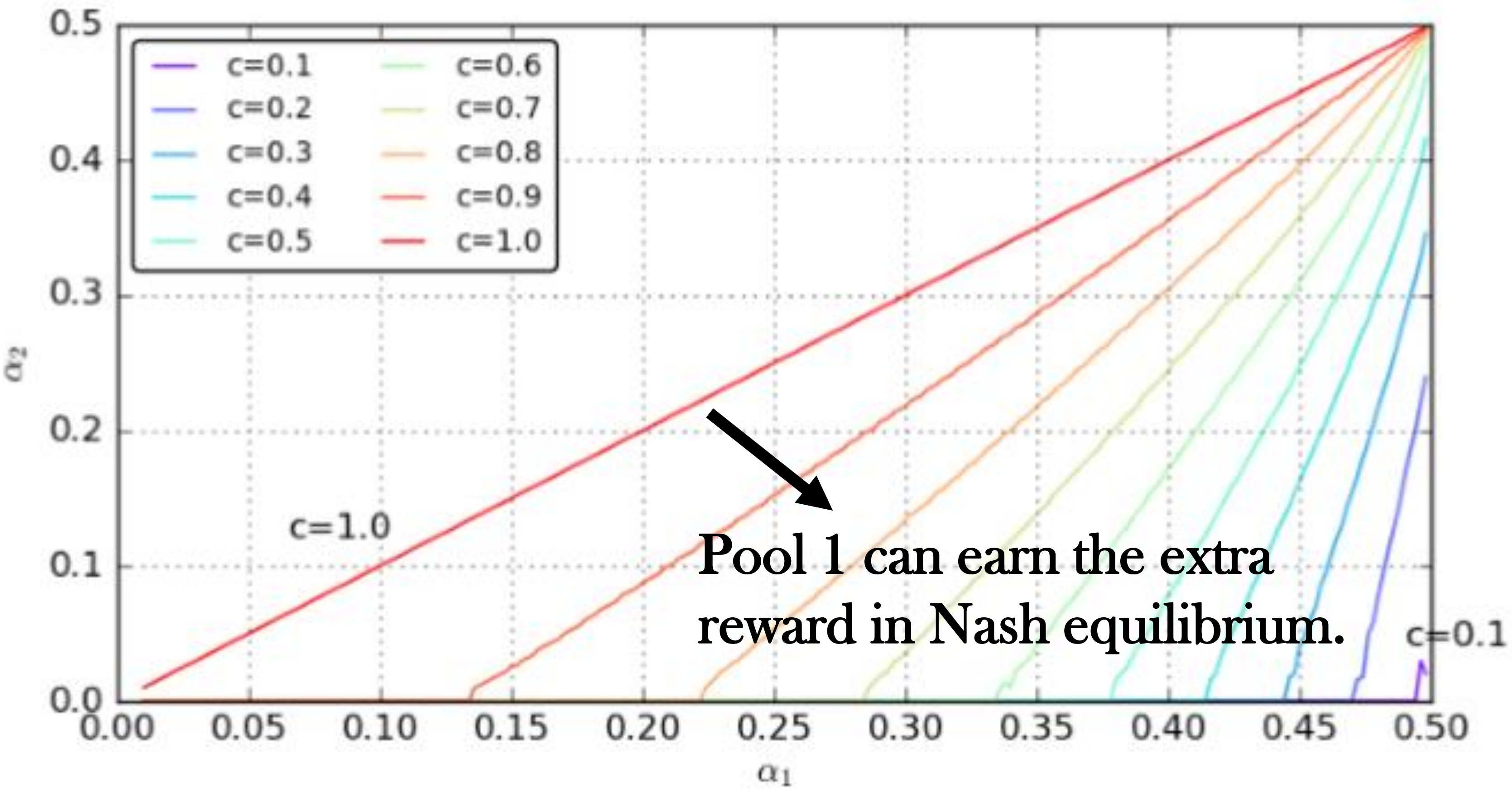




Pool 2 can earn the extra reward in the Nash equilibrium.

- ❖ Pool 1 possesses 0.2 computational power.
- ❖ The bigger pool can earn the extra reward **unlike the miner's dilemma.**

Break Dilemma



❖ FAW attacks between two pools lead to a pool size game: the larger pool can always earn the extra reward.

Detection of FAW Attack

- The FAW attack causes high fork rate.
- The FAW attacker leaves a trace of the only victim pools' identities but not the attacker's identity unlike selfish mining.
- The manager can identify the miner who submits the FPoW causing the fork.
- The FAW attacker can use many **Sybil nodes** in the victim pool.

→ **The FAW attacker can make the detection useless.**

No Silver Bullet

- New reward systems for mining pools
  - High variance of rewards
- Change Bitcoin protocol
  - Two-phase proof-of-work
  - Not backward compatibility
- **There is no one silver bullet.** 

Conclusion

- Currently, the most main coins have the proof-of-work mechanism.

- The proof-of-work mechanism is vulnerable to several attacks.

- There are still open problems.

Thank You!

Yujin Kwon
dbwls8724@kaist.ac.kr