



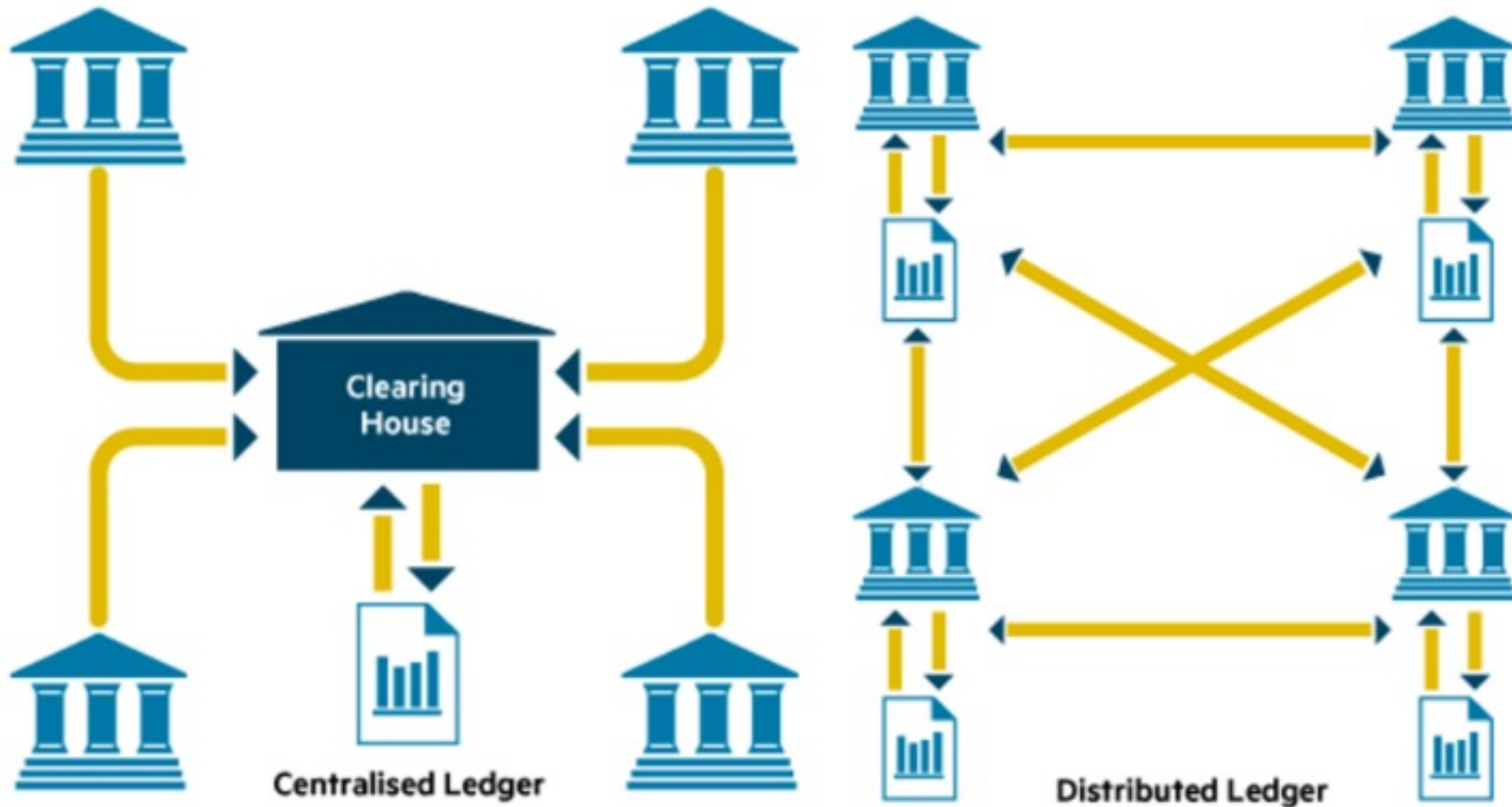
Blockchain Overview + FAW

Yongdae Kim

Distributed Ledger

Embedding distributed ledger technology

A distributed ledger is a network that records ownership through a shared registry



Bitcoin

□ Satoshi Nakamoto

- “Bitcoin: A Peer-to-peer Electronic Cash System”
- “Proof of Work”
- Peer-to-peer Network
- Secure
- Decentralized Ledger technology



Ethereum

- ❑ 2nd gen Blockchain
- ❑ Vitalek Buterin, 19 year old genius
- ❑ Turing Complete Language
- ❑ Storing and executing program on a ledger
- ❑ Smart Contract
- ❑ Implementing other blockchains on Ethereum



Cypherpunk and Blockchain

- ❑ David Chaum (1980s)
 - "Security without Identification: Transaction Systems to Make Big Brother Obsolete"
 - Anonymous Digital Cash, Pseudonymous Reputation System
- ❑ Adam Back (1997)
 - Hash cash: Anti-spam mechanism requiring cost to send email
- ❑ Wei Dai (1998)
 - B-money: Enforcing contractual agreement between two anons
 - 1. Every participant maintain separate DB: Bitcoin
 - 2. deposit some money as potential fines or rewards: PoS
- ❑ Nick Szabo (2005)
 - "Bit Gold": Values based on amount of computational work
 - Concept of "Smart Contract"

What is Bitcoin?

- ❑ Satoshi Nakamoto, who published the invention in 2008 and released it as open-source software in 2009.
 - “Bitcoin: A Peer-to-peer Electronic Cash System”
- ❑ Bitcoin is a first cryptocurrency based on a peer-to-peer network.
- ❑ Bitcoin as a form of payment for products and services has grown, and users are increasing.

Bitcoin P2P e-cash paper

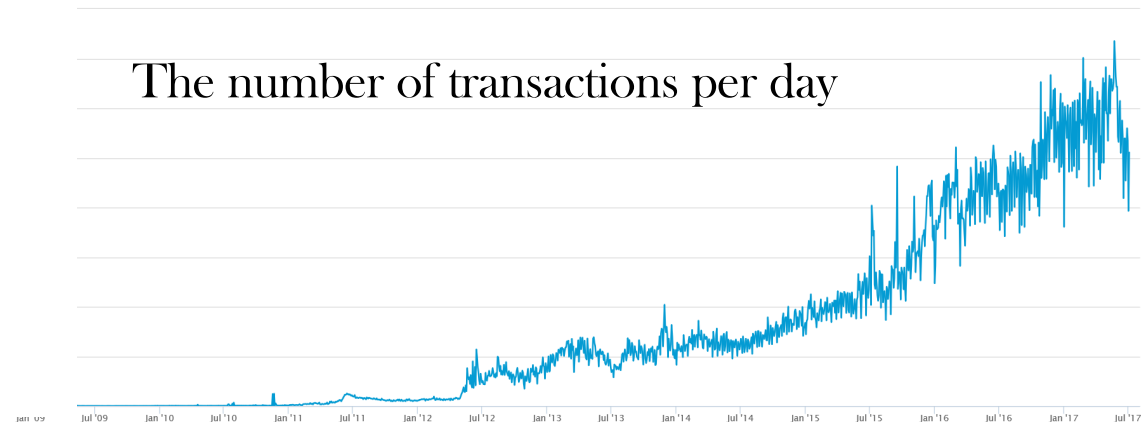
Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

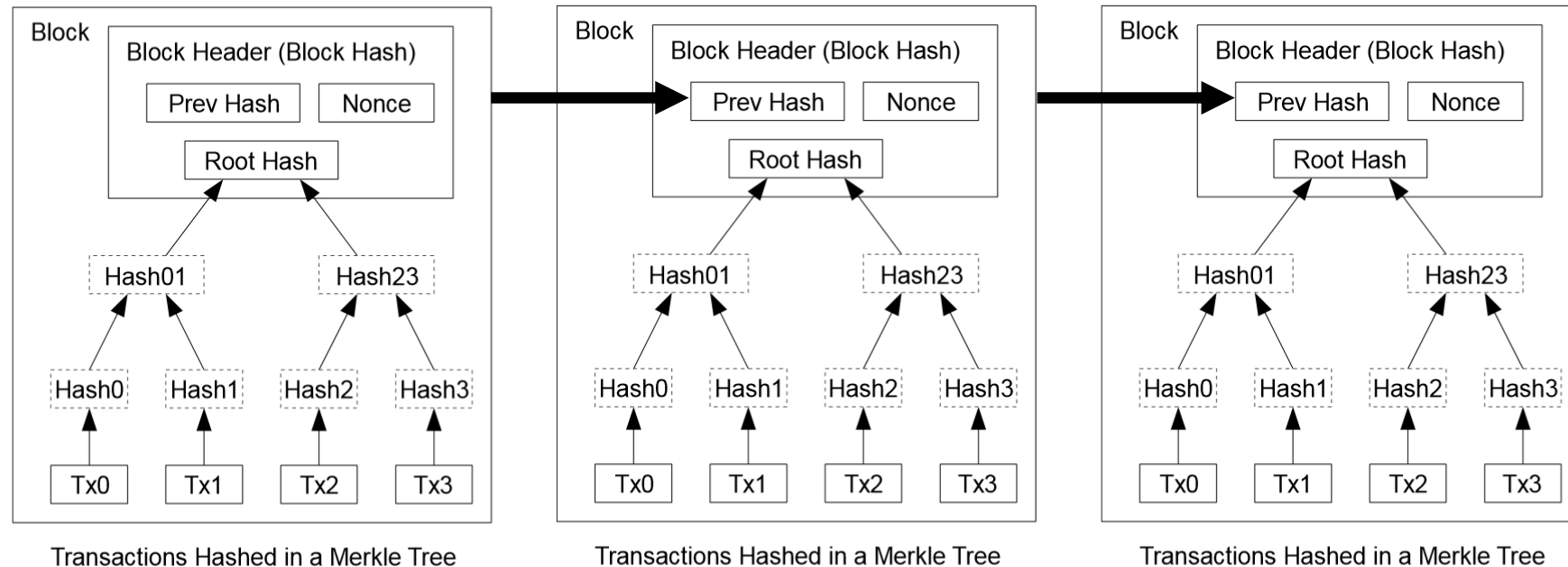
The paper is available at:
<http://www.bitcoin.org/bitcoin.pdf>

The main properties:

Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.



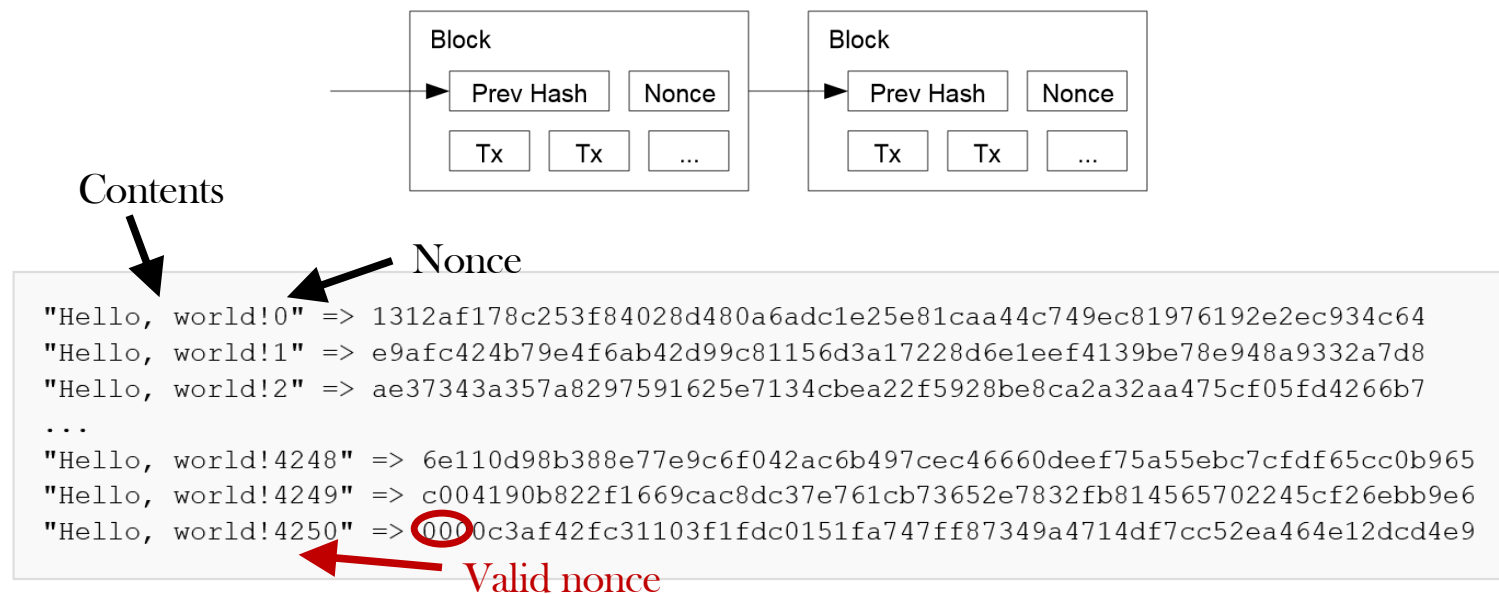
Blockchain



- ❖ Blocks connect as a chain.
- ❖ Each header of blocks includes the previous block's hash.

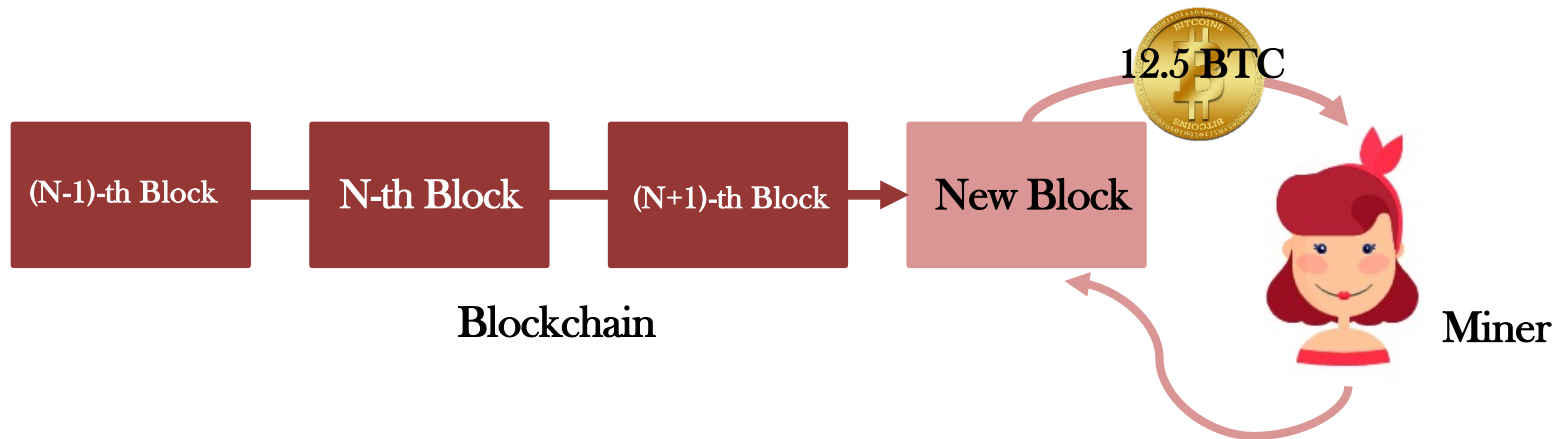
Proof-of-Work

- Proof-of-work scheme is based on SHA-256
- Proof-of-work is to find a valid Nonce by incrementing the Nonce in the block header until the block's hash value has the required prefix zero bits.



Reward

- ❑ Performing proof-of-work is called **Mining**.
- ❑ A person who does mining is called **Miner**.
- ❑ A miner can earn 12.5 BTC (\approx \$ 10k) as a reward when she succeeds to find a valid nonce.

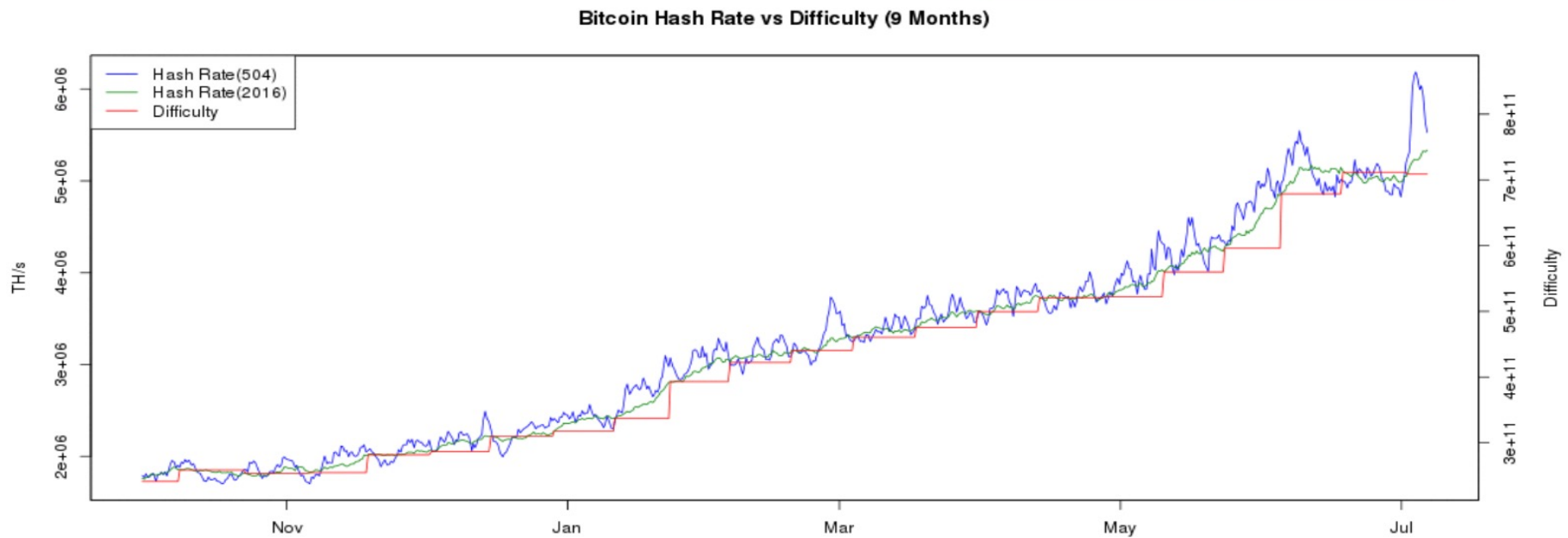


Miner's Incentive

- ❑ 12.5 BTC reward for a valid block
 - Special coin-creation transaction (first transaction in each block)
- ❑ Transaction fees (optional)
 - Offered by creator of transaction (input sum - output sum)
 - Incentive to include transaction in a block (faster processing)
- ❑ Keeping up the system
 - To preserve the value of your own bitcoin money

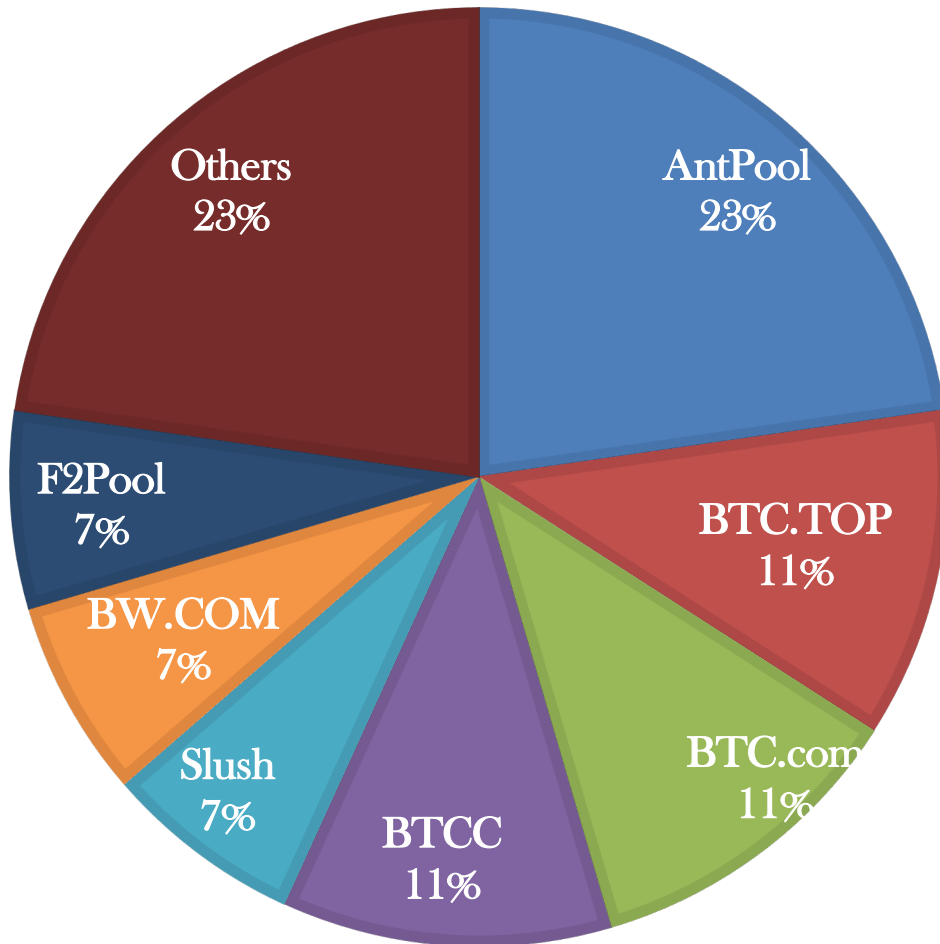
- ❑ Rewarded only if block is on eventual consensus branch!

Mining Difficulty



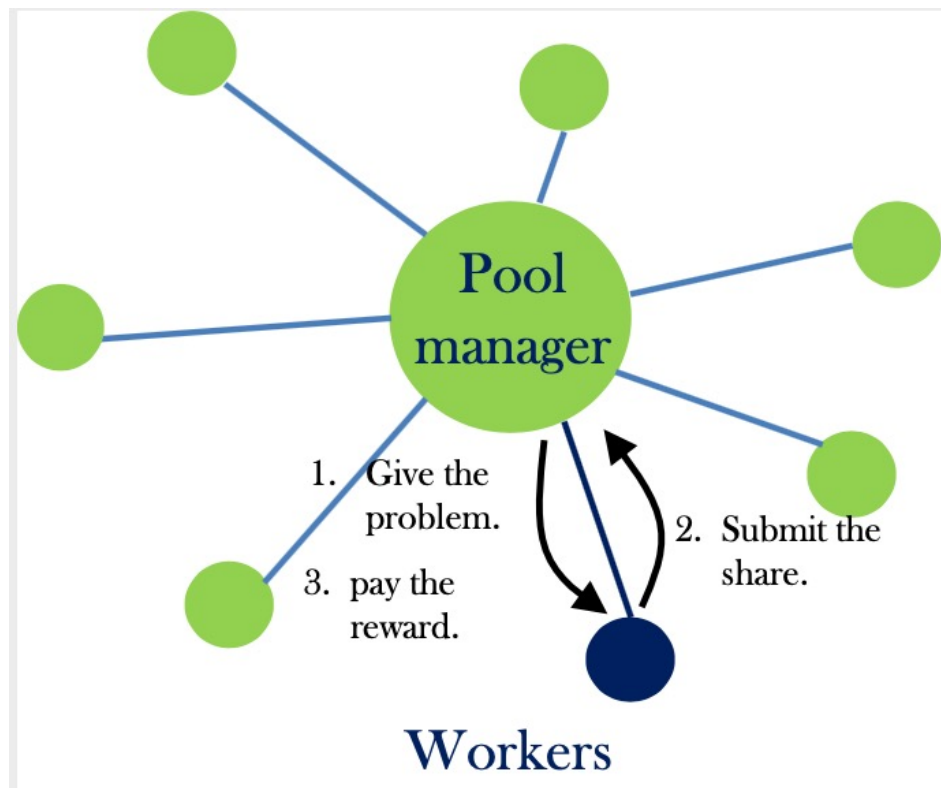
- ❖ Bitcoin adjusts automatically the mining difficulty to be an average one round period 10mins.
- ❖ The difficulty increases continuously as computing power increases.

Mining Pool



- ❖ Many miners started to do mining together.
- ❖ Most mining pools consist of a manager and miners.
- ❖ Currently, most computational power is possessed in mining pools.

Stratum



- ❑ A miner in a pool solves the easier problem than actual proofs-of-work.
- ❑ A miner submits the solution called a share to a manager.
- ❑ The manager pay the profit to a miner in proportion to an amount of shares (easier problems solved).

Bitcoin Mining Hardware



Antminer S9 13 TH/S 16nm ASIC Bitcoin Miner

by AntMiner

\$1,887⁰⁰

FREE Shipping on eligible orders
Only 12 left in stock - order soon.

More Buying Choices
\$1,885.00 (5 used & new offers)



Rev 2 GekkoScience 2-Pac Compac USB Stick Bitcoin Miner 15gh/s+

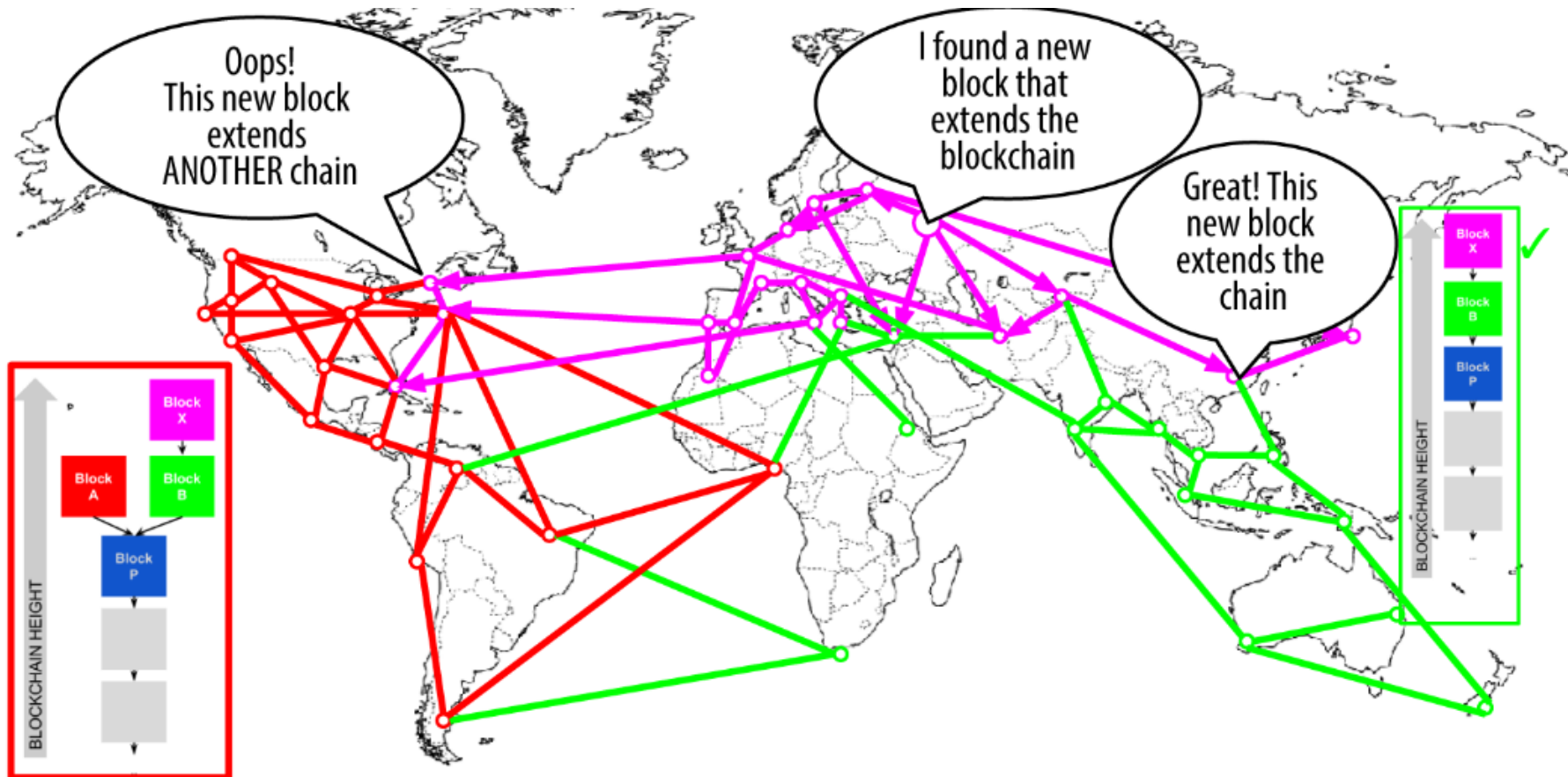
by GEKKOSCIENCE

\$69⁹⁷ + \$4.49 shipping

More Buying Choices
\$59.97 (2 new offers)

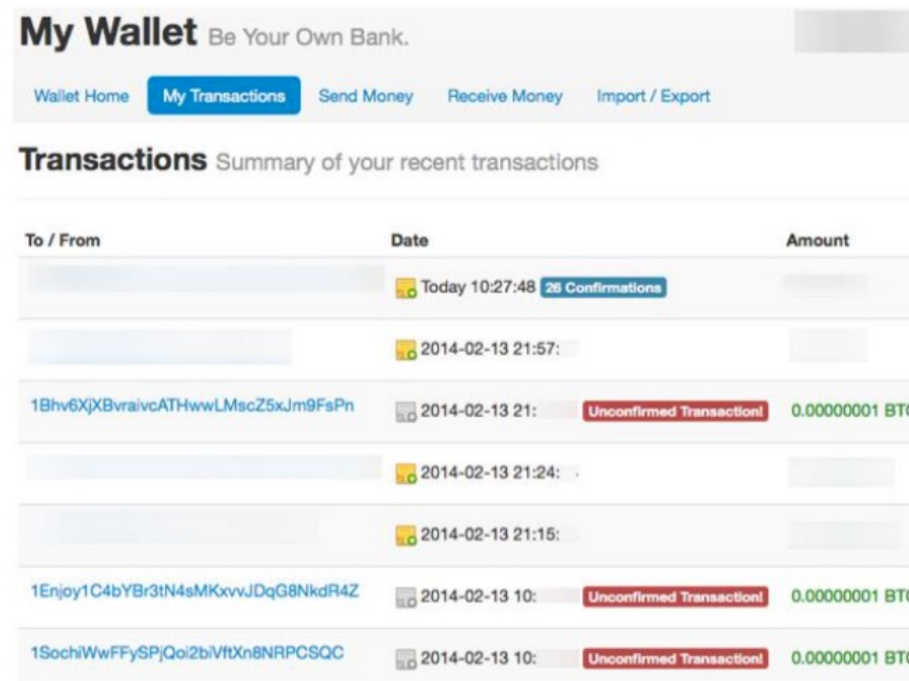


Forks



Transaction Confirmations

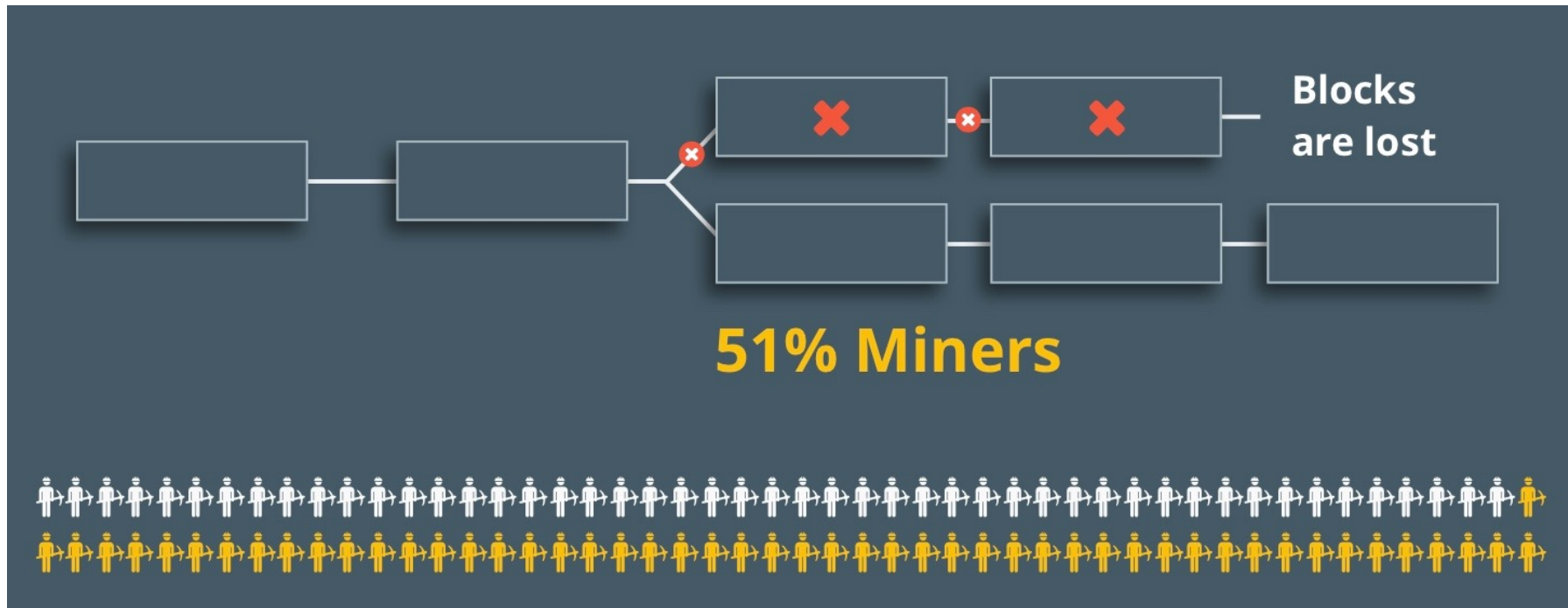
- A transactions is typically considered “confirmed” once it has 6 confirmations → Probabilistic confirmation



The screenshot shows a Bitcoin wallet interface titled "My Wallet Be Your Own Bank." with navigation buttons for "Wallet Home", "My Transactions", "Send Money", "Receive Money", and "Import / Export". Below this is a "Transactions" section with the subtitle "Summary of your recent transactions". A table lists several transactions with columns for "To / From", "Date", and "Amount".

To / From	Date	Amount
	Today 10:27:48 26 Confirmations	
	2014-02-13 21:57:	
1Bhv6XjXBvraivcATHwwLMscZ5xJm9FsPn	2014-02-13 21: Unconfirmed Transaction!	0.00000001 BTC
	2014-02-13 21:24:	
	2014-02-13 21:15:	
1Enjoy1C4bYBr3tN4sMKxvJdQg8NkdR4Z	2014-02-13 10: Unconfirmed Transaction!	0.00000001 BTC
1SochiWwFFySPjQoi2bVtXn8NRPCSQc	2014-02-13 10: Unconfirmed Transaction!	0.00000001 BTC

51% Attack



Hash Rate Comparison



BTC Pool

Pool HashRate	Network HashRate
6.103E	53.986E



ZEC Pool

Pool HashRate	Network HashRate
107.573M	2.128G



BCH Pool

Pool HashRate	Network HashRate
435.120P	3.548E



DASH Pool

Pool HashRate	Network HashRate
251.480T	2.558P



LTC Pool

Pool HashRate	Network HashRate
40.886T	247.719T



BTM Pool

Pool HashRate	Network HashRate
173.546K	1.225G



ETH Pool

Pool HashRate	Network HashRate
663.324G	205.490T



XMR Pool

Pool HashRate	Network HashRate
7.544M	399.718M



ETC Pool

Pool HashRate	Network HashRate
17.589G	13.079T

Smart Contract

- Definition: A smart contract is a computer program executed in a secure environment that directly controls digital assets

Computer Program

```
if HAS_EVENT_X_HAPPENED() is true:  
    send(party_A, 1000)  
else:  
    send(party_B, 1000)
```

Properties of Secure Environments

Correctness of execution

- The execution is done correctly, is not tampered

Integrity of code and data

Optional properties

- Confidentiality of code and data
- Verifiability of execution
- Availability for the programs running inside

Digital Assets

Domain name

Website

Money

Anything tokenisable (e.g. gold, silver, stock share etc)

Game items

Network bandwidth, computation cycles

Legal vs. Smart Contracts

Legal: "I promise to send you \$100 if my lecture is rated 1"

Smart: "I send \$100 into a computer program executed in a secure environment which sends \$100 to you if the rating of my lecture is 1*, otherwise it eventually sends \$100 back to me"

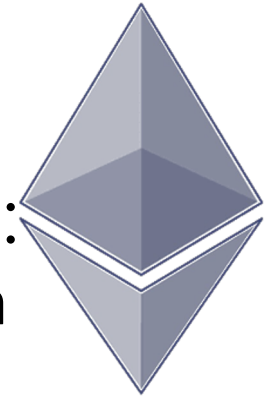
Smart vs. Legal Contracts

□ Why Smart Contracts

- Automated processing
- Trust reduction
 - » Trust the secure environments, not a very large number of contract enforcement mechanisms
- Unambiguous, terms clearly expressed in code

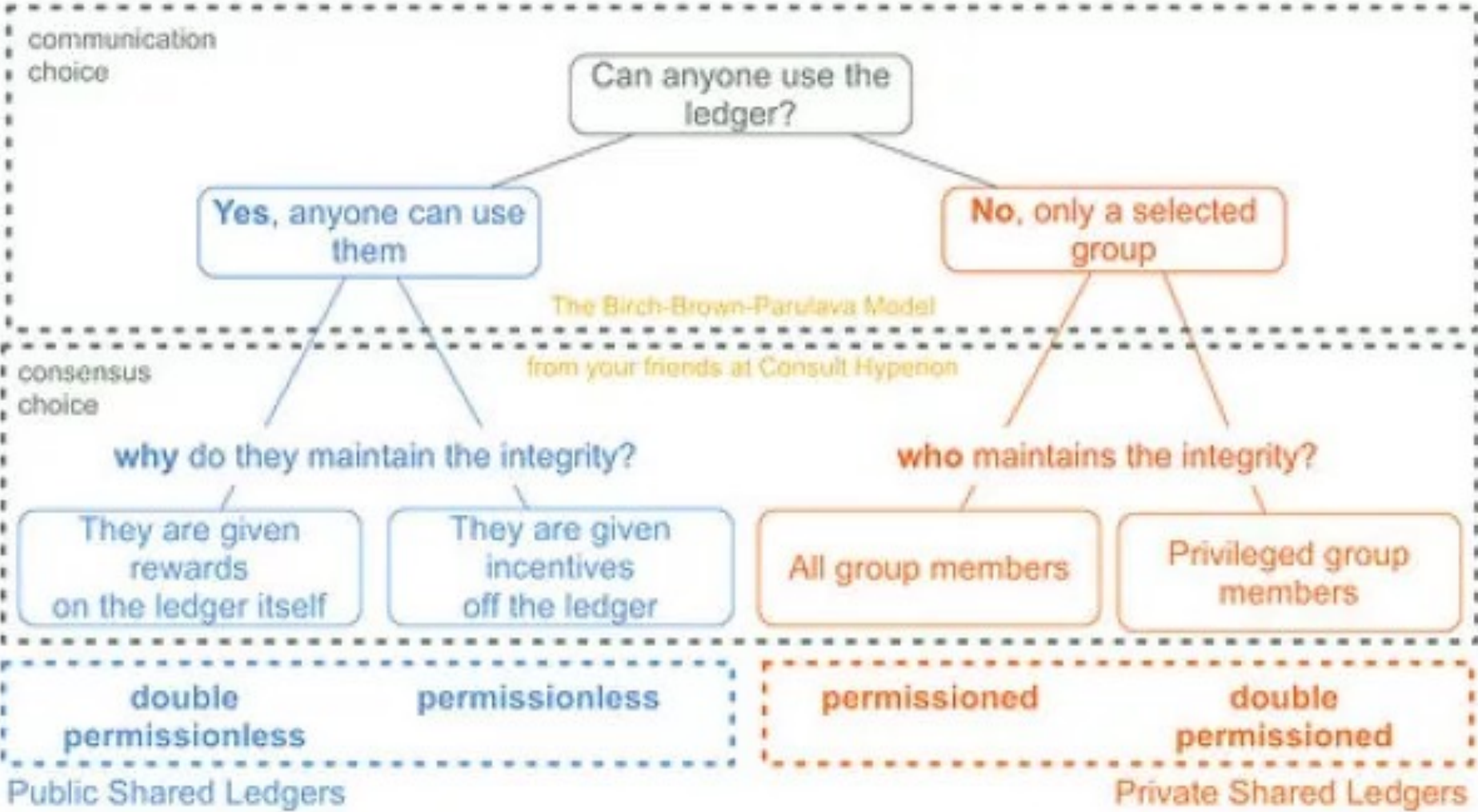
Legal contracts	Smart contracts
Good at subjective (i.e. requiring human judgement) claims	Good at objective (i.e. mathematically evaluable) claims
High cost	Low cost
May require long legal process	Fast and automated
Relies on penalties	Relies on collateral/security deposits
Jurisdiction-bound	Potentially international (“a-legal”)

Ethereum

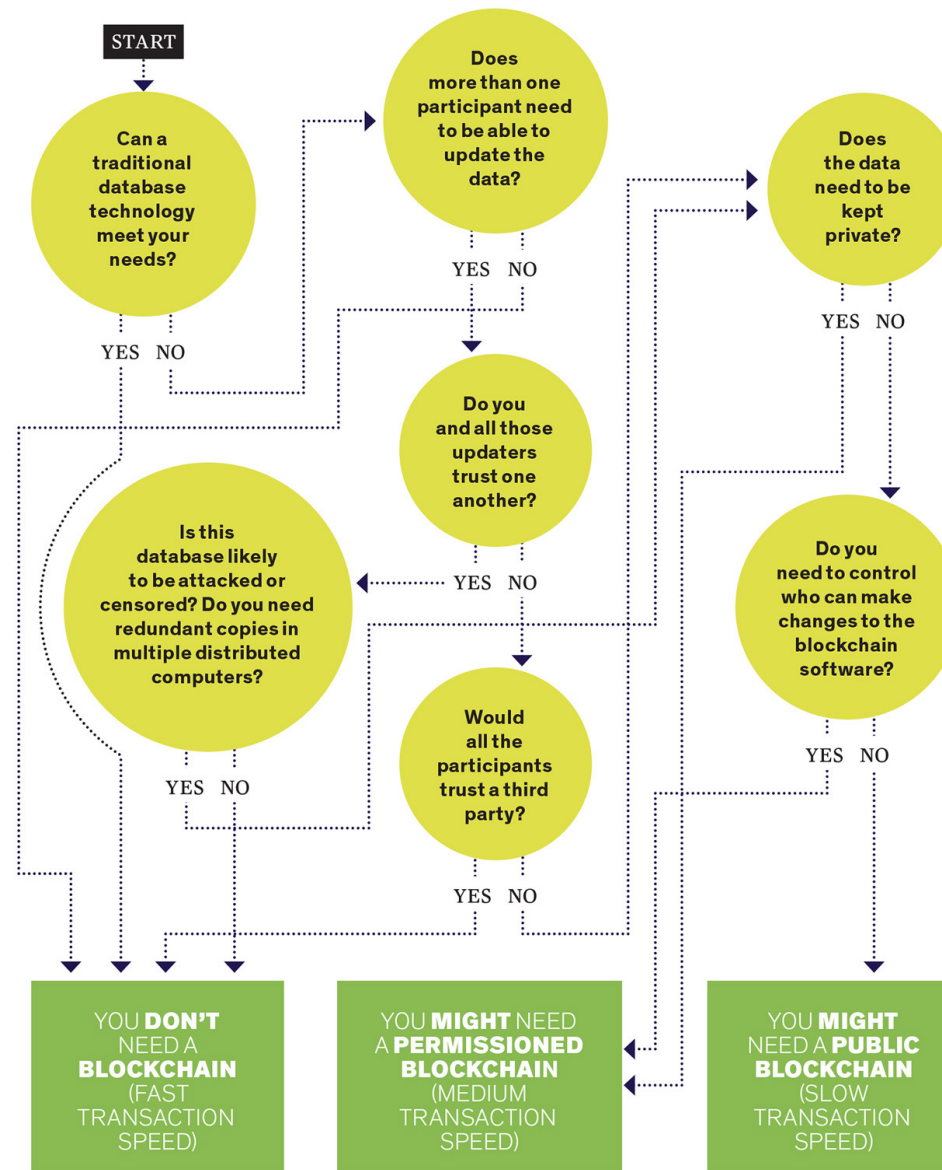


- Blockchain with expressive programming language
 - Programming language makes it ideal for smart contracts
- Why?
 - Most public blockchains are cryptocurrencies
 - » Can only transfer coins between users
 - Smart contracts enable much more applications
- Two types of account:
 - Normal account like in Bitcoin
 - » has balance and address
 - Smart Contract account
 - » like an object: containing (i) code, and (ii) private storage (key-value storage)
 - » Code can
 - Send ETH to other accounts
 - Read/write storage
 - Call (ie. start execution in) other contracts

Taxonomy of Blockchain



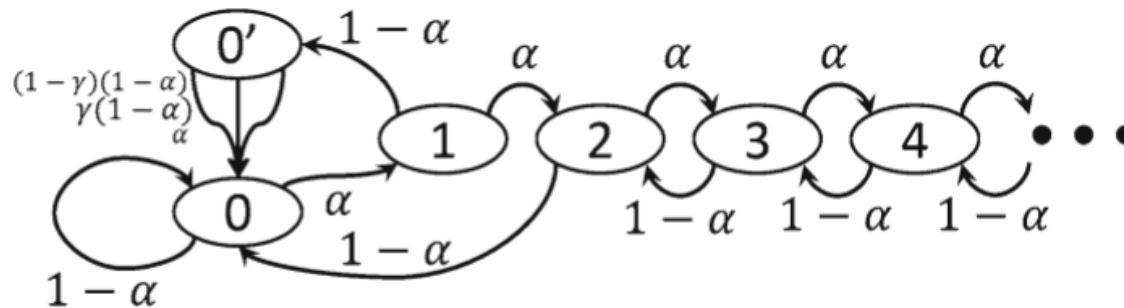
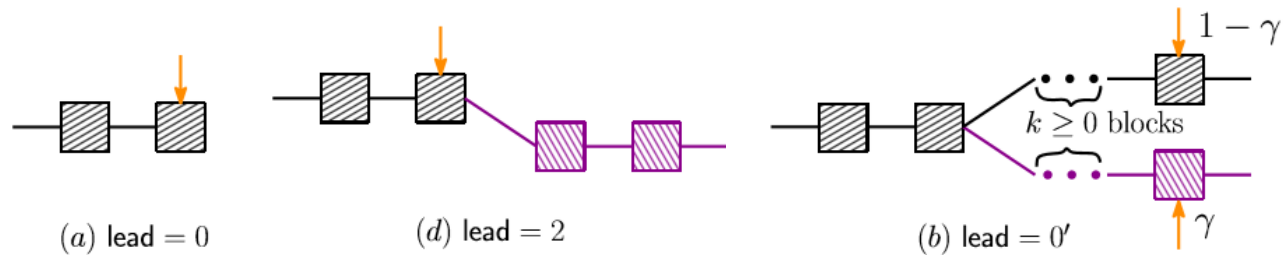
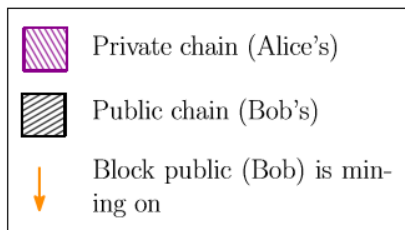
Blockchain Testing



Attacks in Bitcoin System

- ❑ Double spending
- ❑ Anonymity
- ❑ Peer-to-Peer Network
- ❑ **Mining**
 - Selfish mining: FC 2014
 - » Generate intentional forks
 - Block withholding (BWH) attacks: S&P 2015
 - » Exploit pools' protocol
 - Fork after withholding (FAW) attacks
 - » Generate intentional forks through pools

Selfish Mining

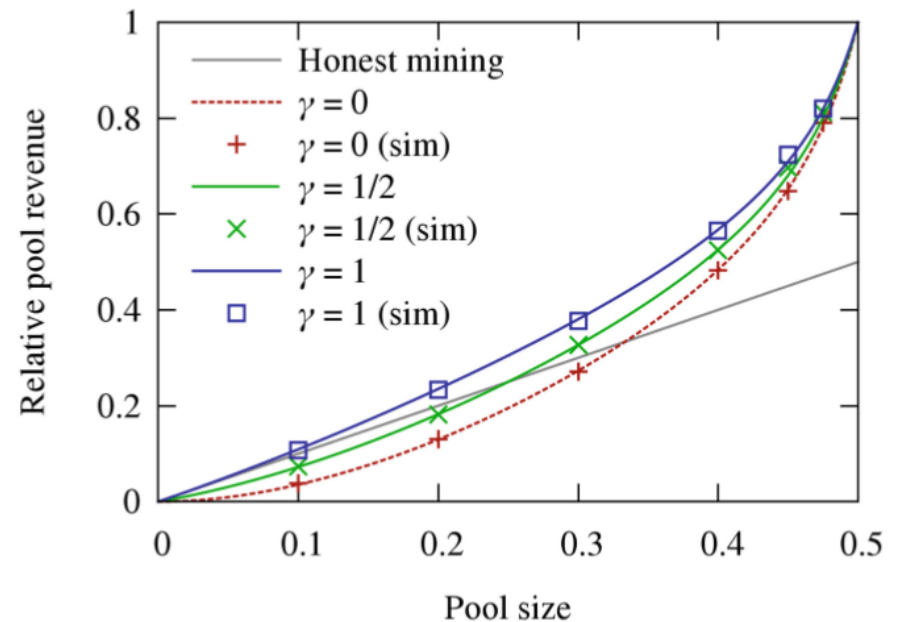


- ❖ Generate intentional forks adaptively.
- ❖ Force the honest miners into performing wasted computations on the stale public branch.

Eyal and Sirer. "Majority is not enough: Bitcoin mining is vulnerable." Financial Crypto, 2014.

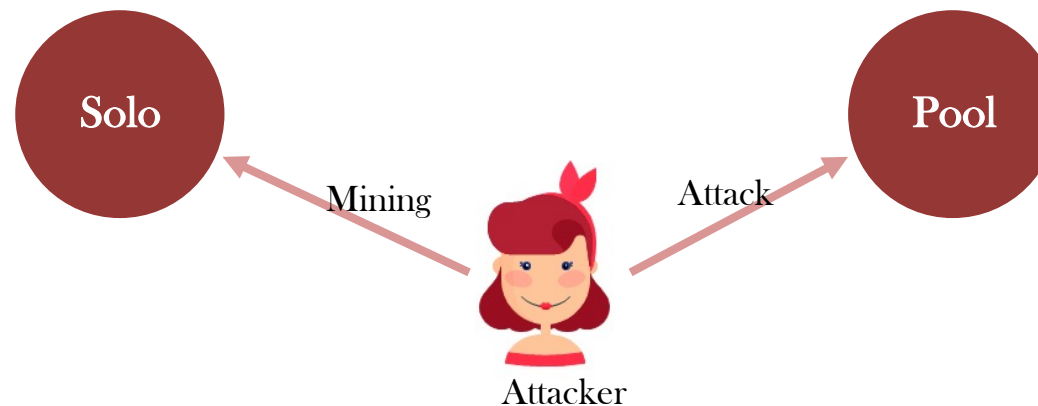
Selfish Mining

- ❖ An attacker can earn the extra reward according to her network capability.
- ❖ For example, if an attacker possesses 20% computational power, she can earn the extra reward **\$6M** at most.
- ❖ However, it is **not practical**.

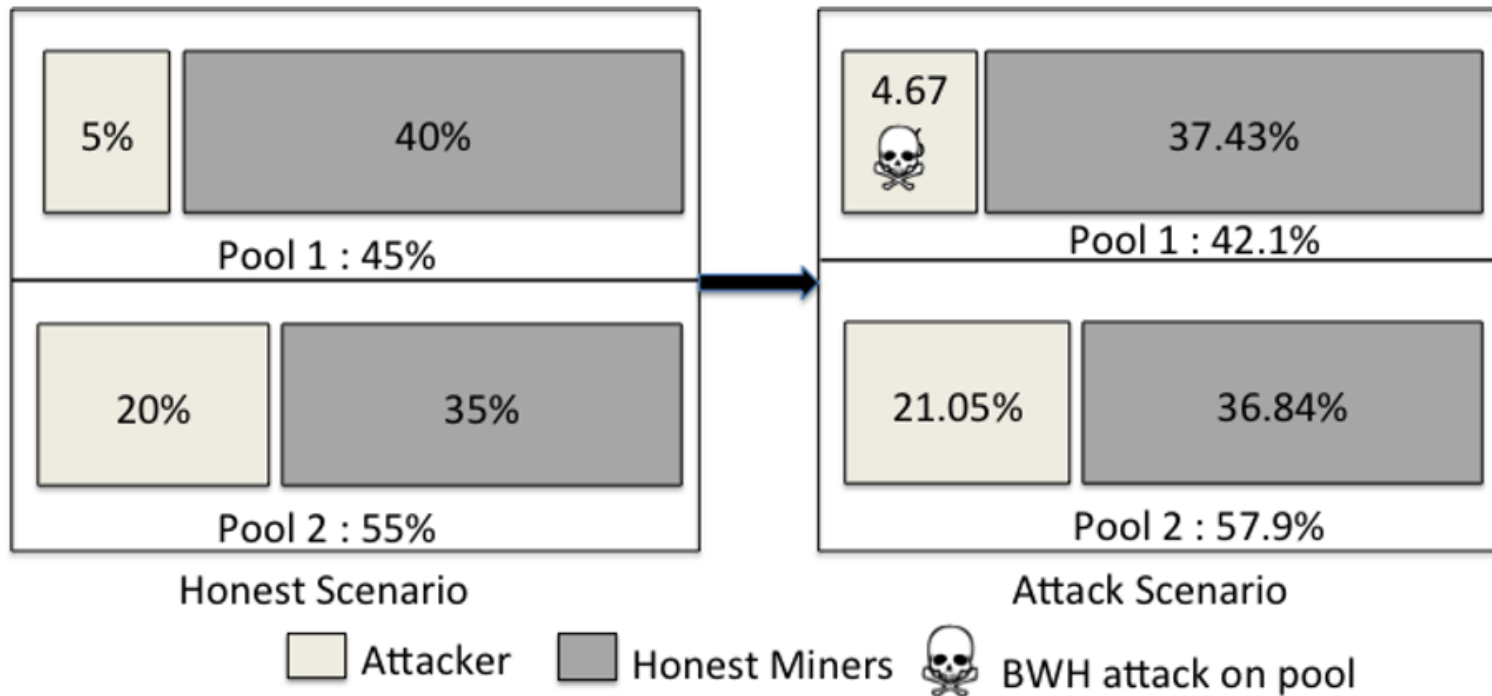


BWH Attack

- ❑ An attacker joins the target pool.
- ❑ She receives unearned wages while only pretending to contribute work in the pool.
- ❑ She submits the share which contains only partial solution but not the perfect solution.
- ❑ She should split her computational power into solo mining and malicious pool mining.



BWH Attack



FAW Attack

- ❑ In the BWH attack, the largest beneficiaries are honest miners except the target pool.
- ❑ In the FAW attack, an attacker also takes away part of miners' rewards by generating intentional forks.
- ❑ She submits only the perfect solution to the manager when external miners propagate a block.
- ❑ For example, if an attacker possesses 20% computational power, she can earn the extra reward **\$ 320k (\approx 369M Won)** and **\$ 1053k (\approx 1215M Won)** per month via BWH and FAW attacks, respectively. (Basic reward: \$ 27M \approx 31100M Won)



Back to the BWH Attack

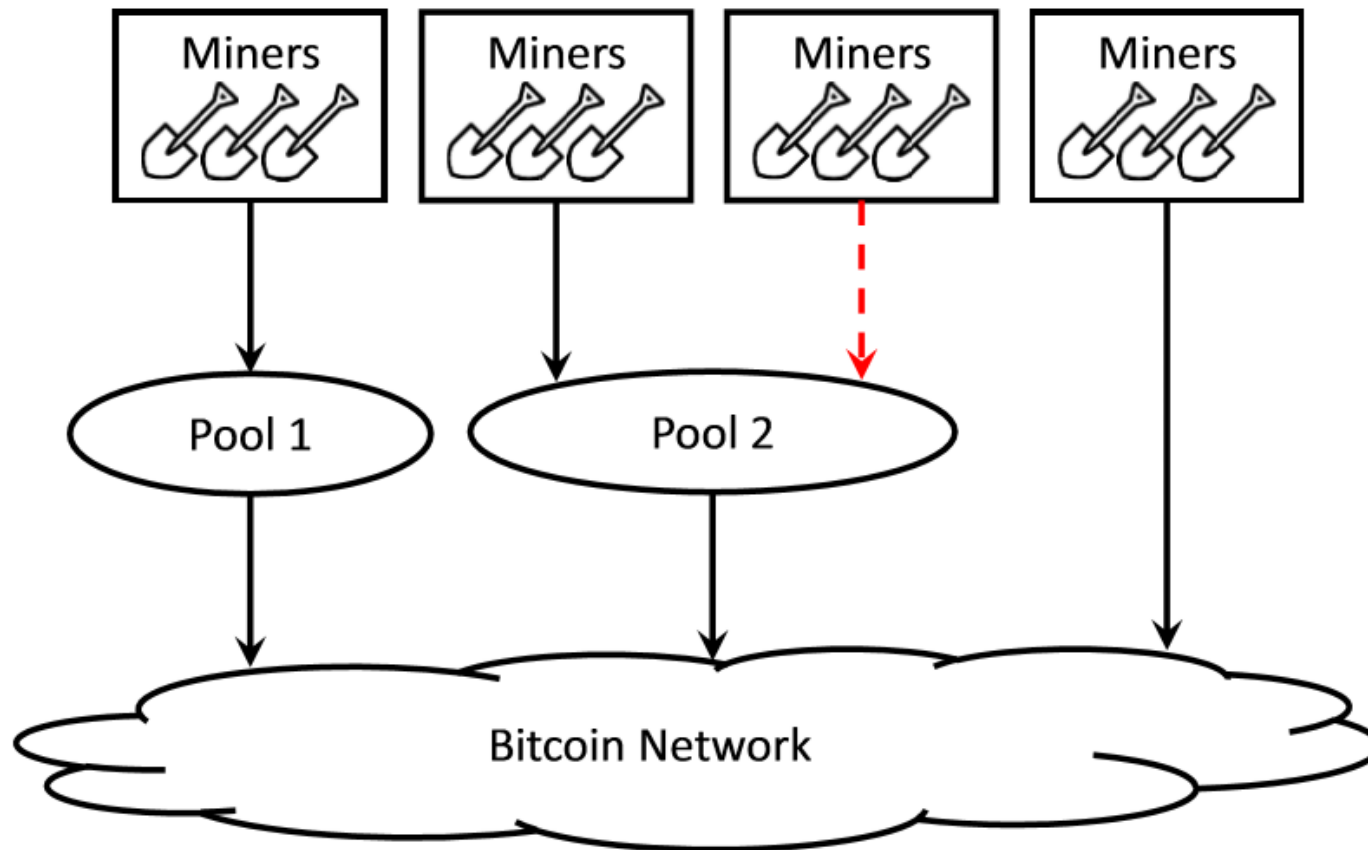
The History of the BWH Attack

- ❑ 2011: Analysis of Bitcoin Pooled Mining Reward Systems
 - “This has no direct benefit for the attacker, only causing harm to the pool operator or participants.”

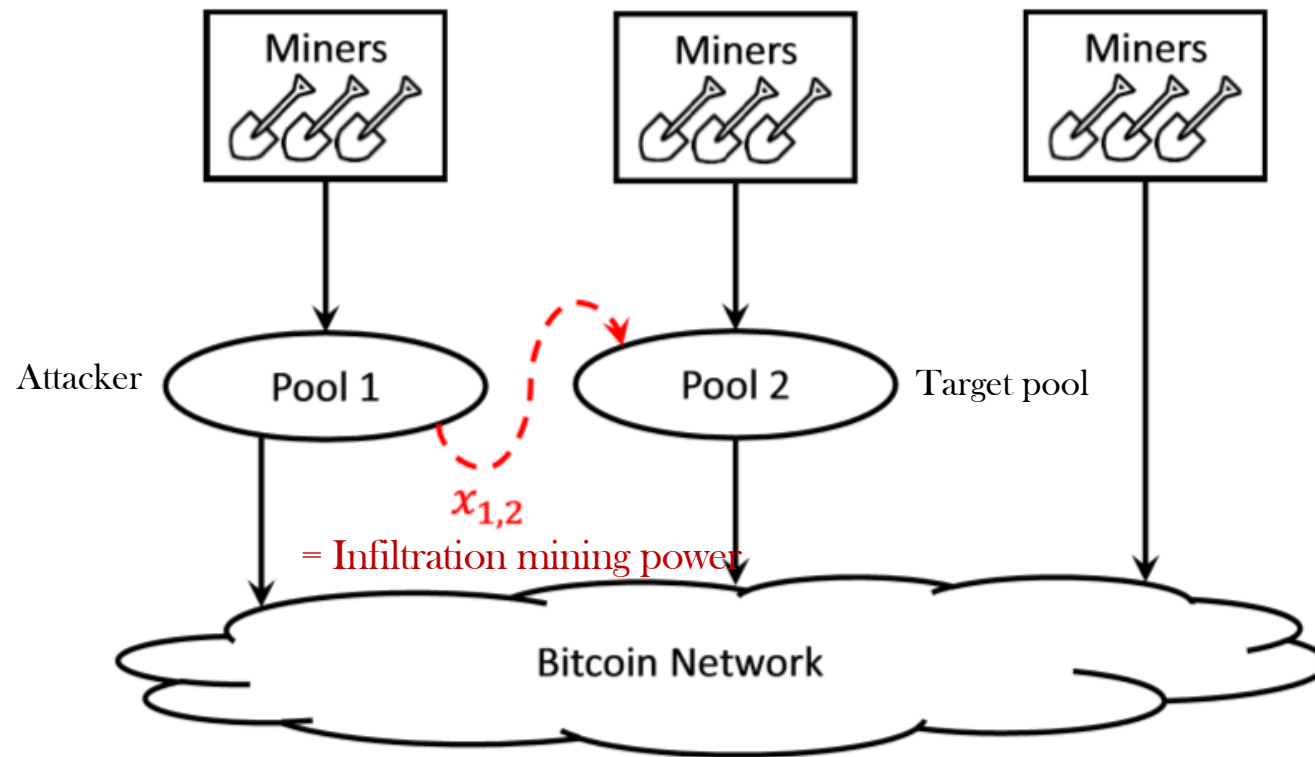
- ❑ 2014 : On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency
 - “They showed that an attacker can earn profit by this attack”
 - In June 2014, Eligius pool made a loss because of the BWH attack.

- ❑ 2015 : The miner’s dilemma
On Power Splitting Games in Distributed Computation: The Case of Bitcoin Pooled Mining
 - Attack strategy && game theory

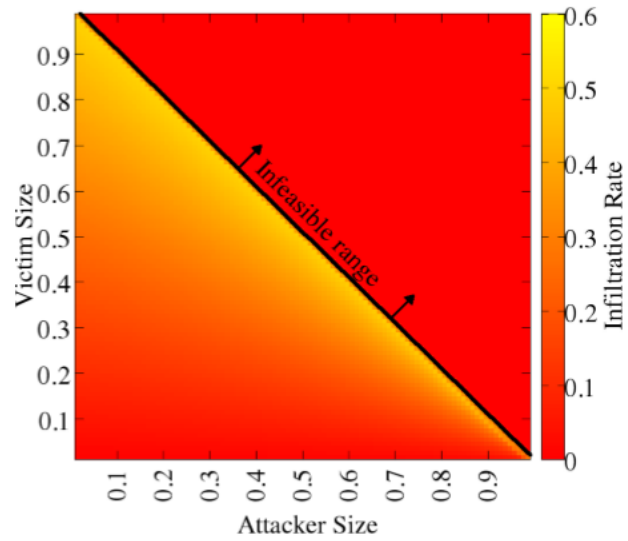
Classical BWH attack



BWH attack among pools

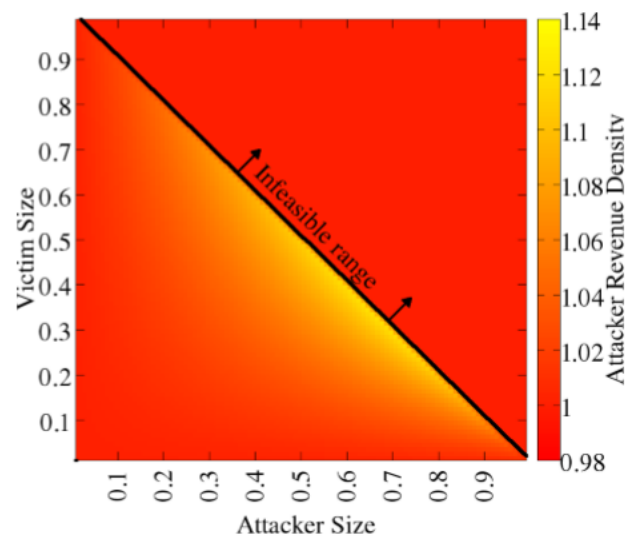


Result



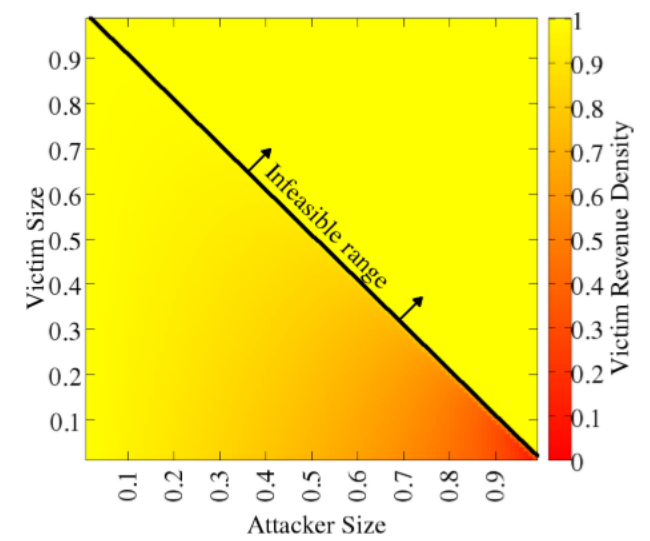
(a) $x_{1,2}$

Infiltration mining power



(b) r_1

Attacker relative reward



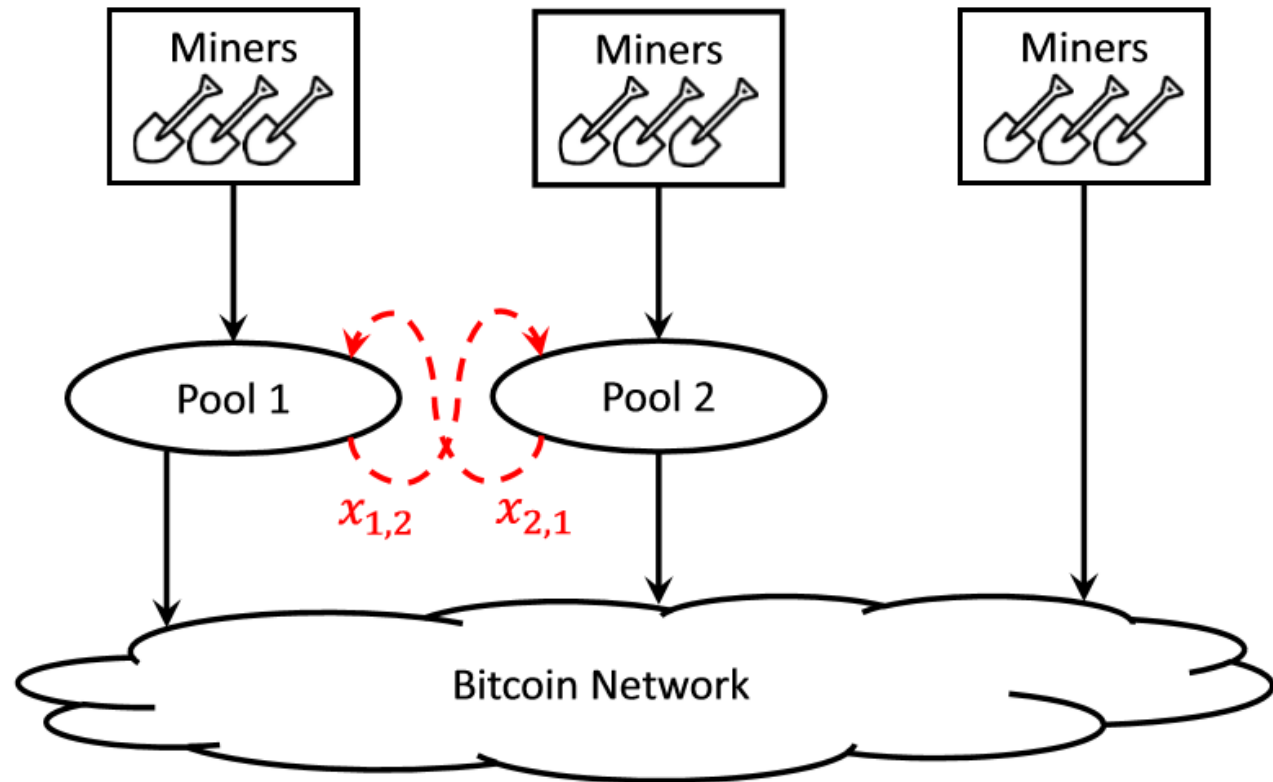
(c) r_2

Victim relative reward

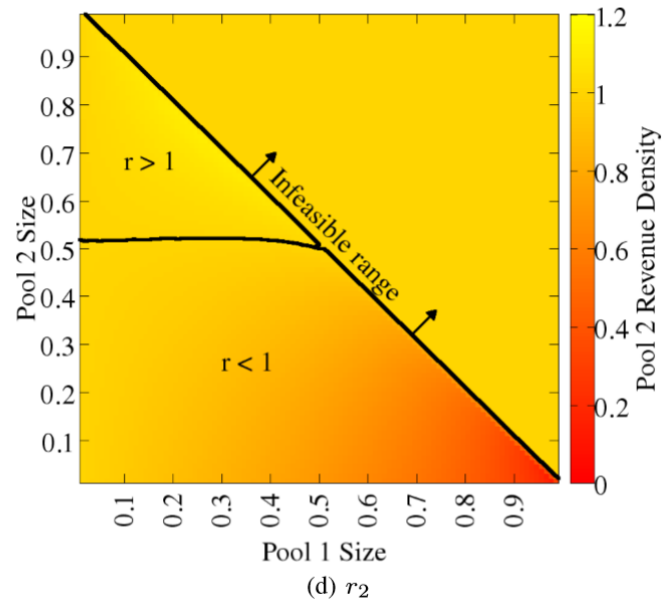
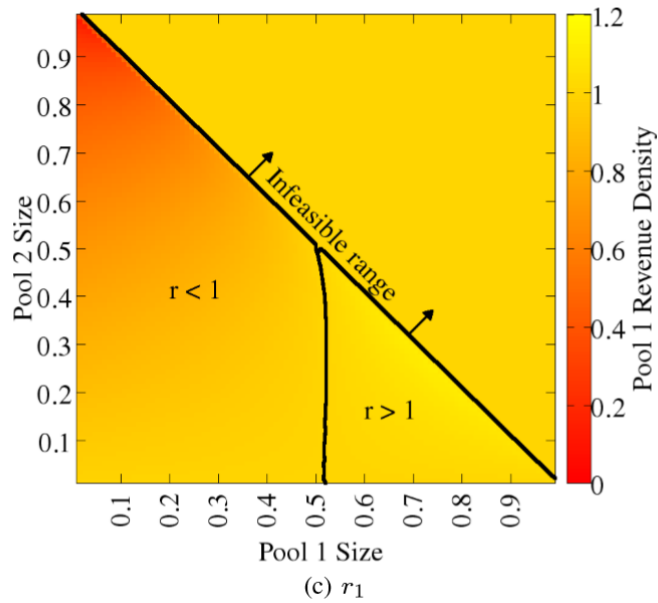
❖ The BWH attack is always profitable.

Between Two Pools

- ❖ Rational two pools can launch the BWH attack each other.
- ❖ It leads to a BWH attack game.



Result



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

Miners' dilemma

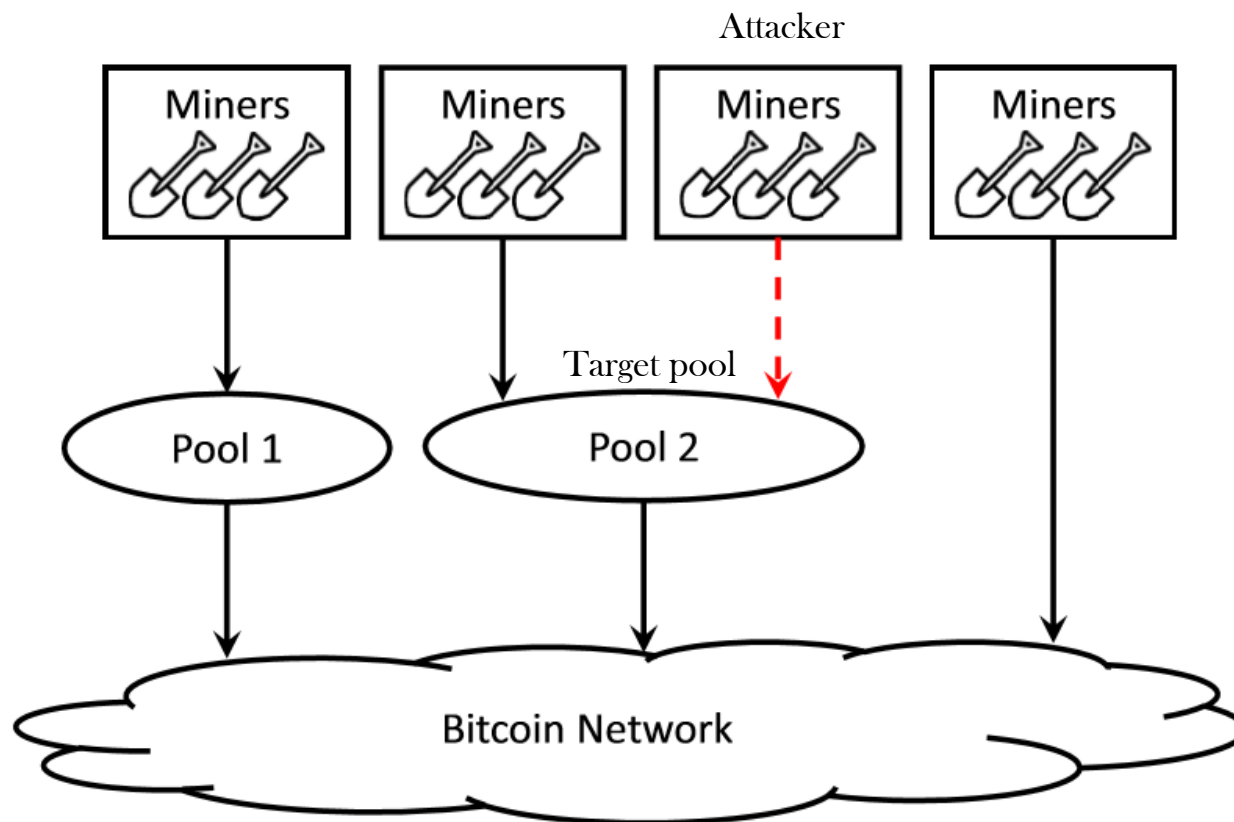
Pool 2 \ Pool 1	no attack	attack
no attack	$(r_1 = 1, r_2 = 1)$	$(r_1 > 1, r_2 = \tilde{r}_2 < 1)$
attack	$(r_1 = \tilde{r}_1 < 1, r_2 > 1)$	$(\tilde{r}_1 < r_1 < 1, \tilde{r}_2 < r_2 < 1)$

- ❖ The equilibrium revenue of the pool is **inferior** compared to the no-pool attacks scenario.
- ❖ This is equivalent to the prisoner's dilemma.
- ❖ The fact that the BWH attack is not common may be explained by modeling the attack decisions as an iterative prisoner's dilemma.

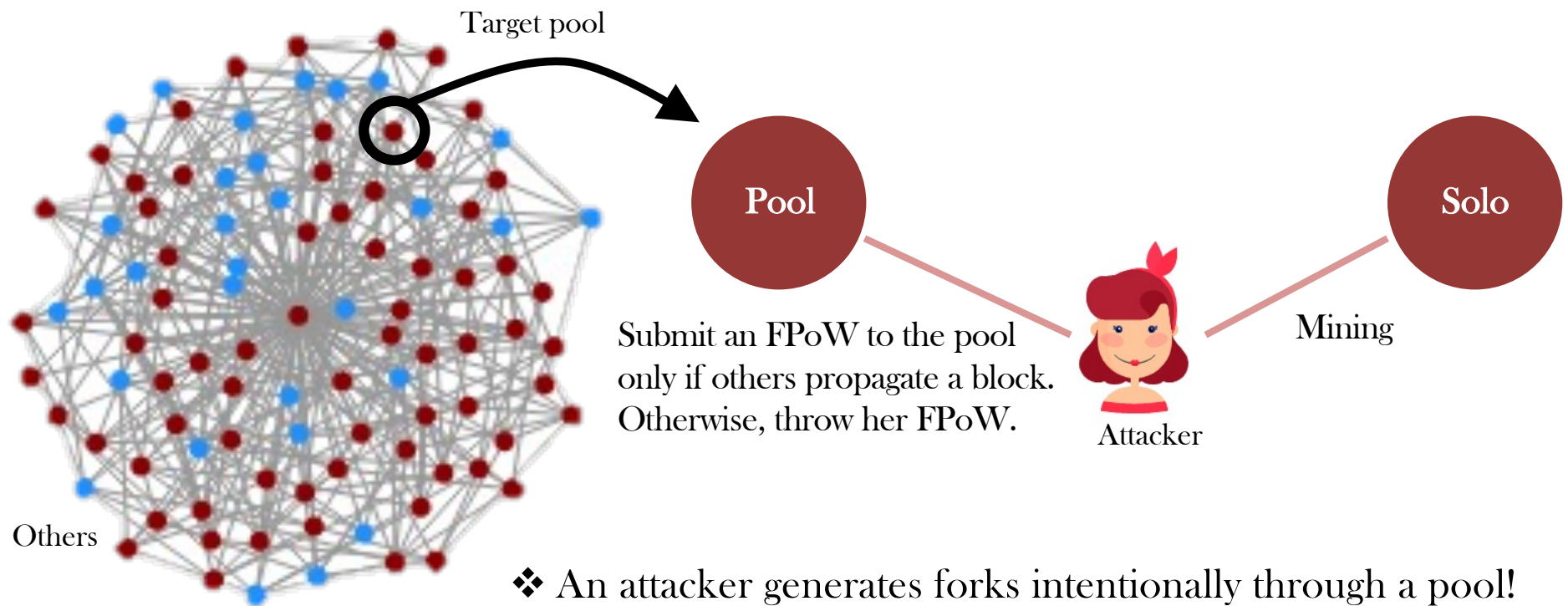


Do exist an attack which breaks the dilemma? FAW Attack

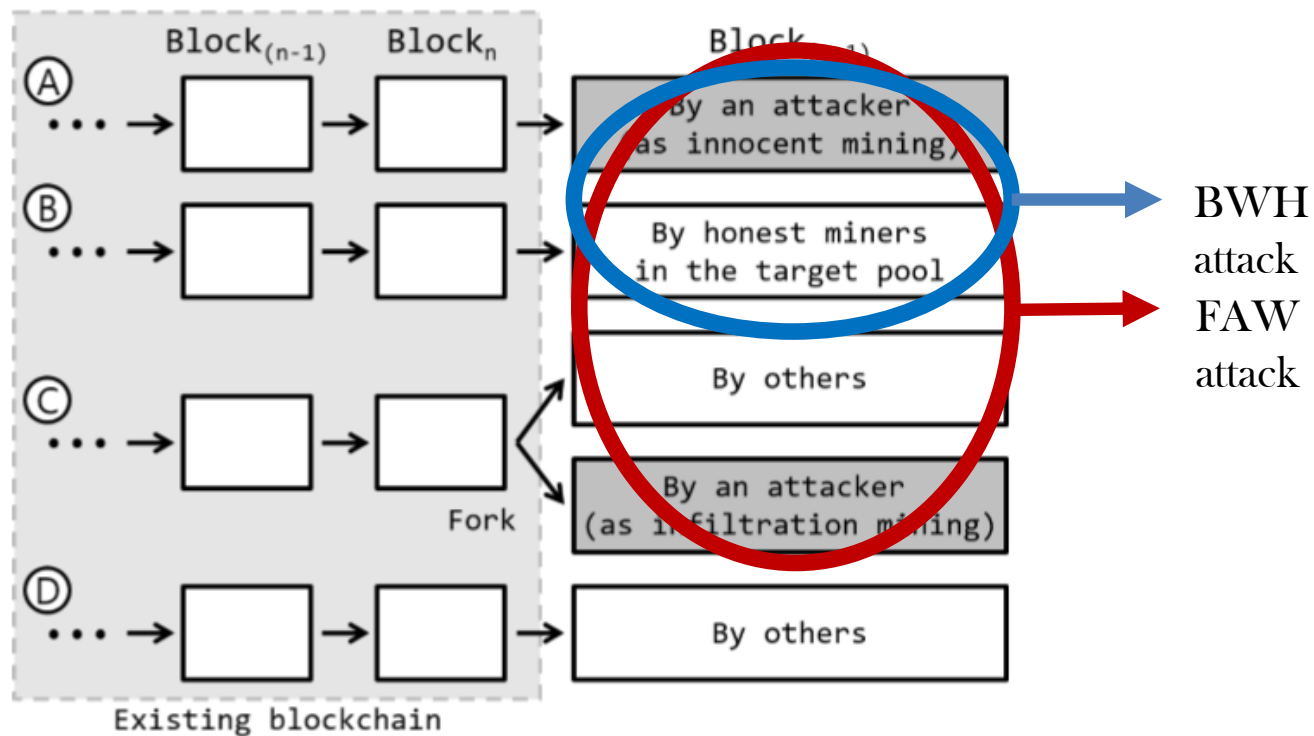
FAW Attack



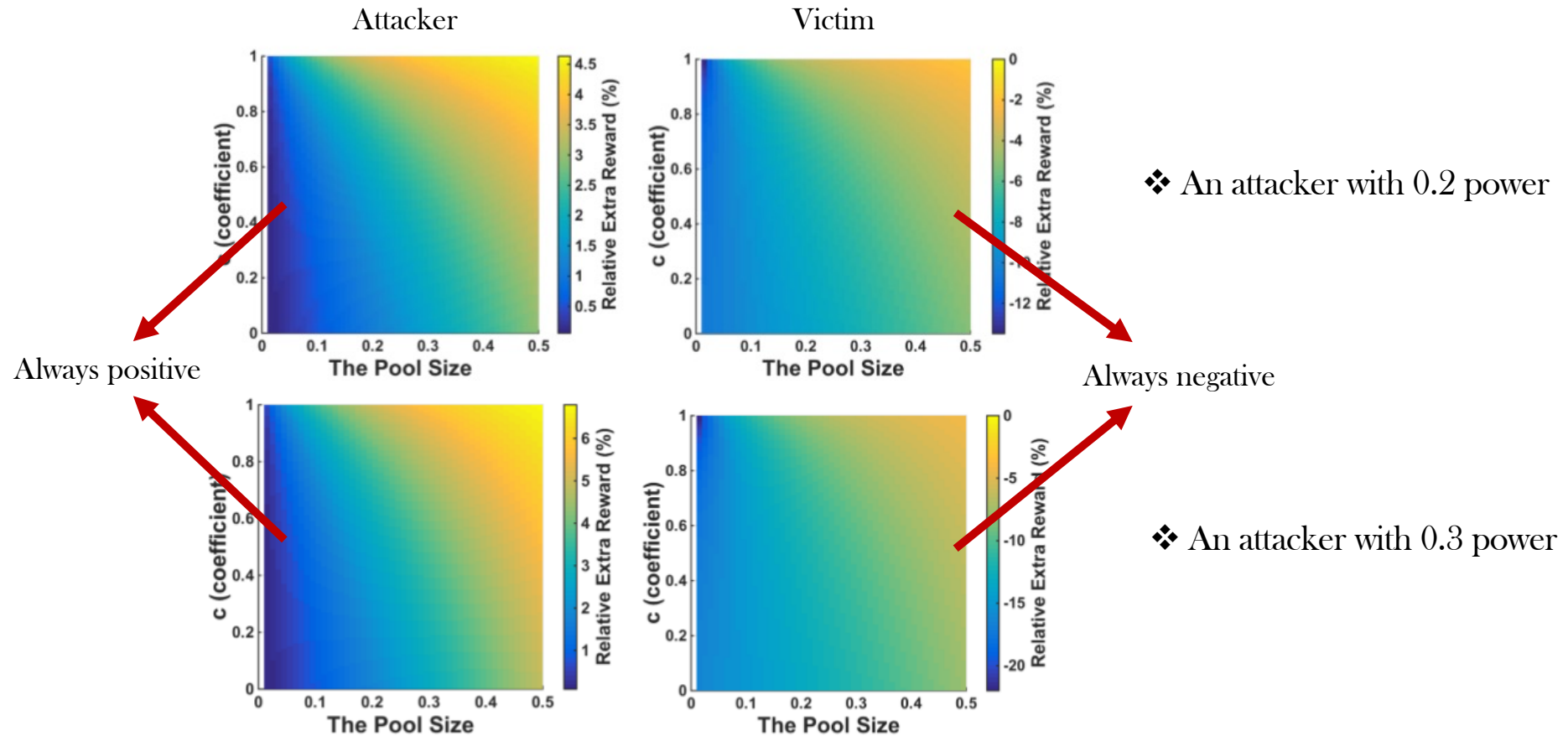
FAW Attack



FAW Attack Against One Pool



Result



Result

The case is equivalent to the case of the BWH attack

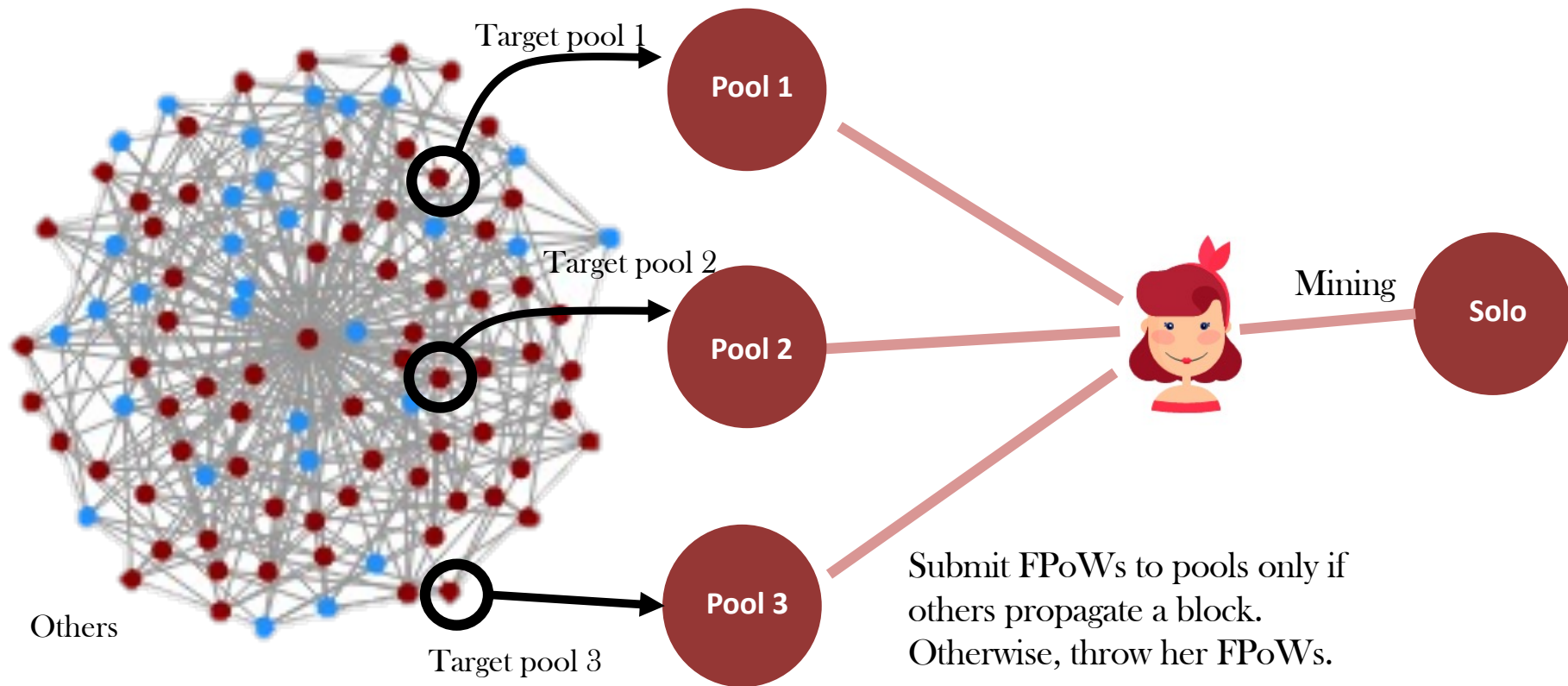
$c \backslash \alpha$	0.1	0.2	0.3	0.4
0	0.53 (0.53)	1.14 (1.14)	1.85 (1.85)	2.70 (2.70)
0.25	0.65 (0.67)	1.38 (1.38)	2.20 (2.20)	3.1 (3.13)
0.5	0.85 (0.85)	1.74 (1.74)	2.70 (2.70)	3.75 (3.75)
0.75	1.21 (1.22)	2.37 (2.37)	3.52 (3.52)	4.69 (4.70)
1	2.12 (2.12)	3.75 (3.75)	5.13 (5.13)	6.37 (6.36)

Increasing g

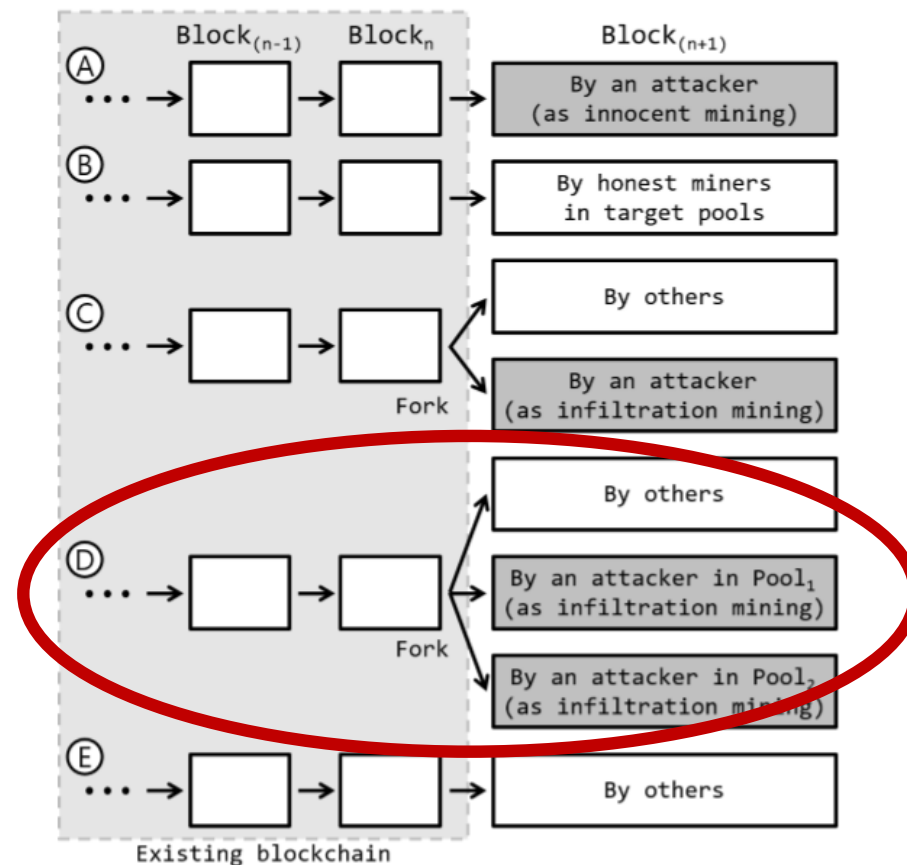
Increasing c

- We simulated an FAW attack against one pool which possesses a computational power of 0.2, using a Monte Carlo method.

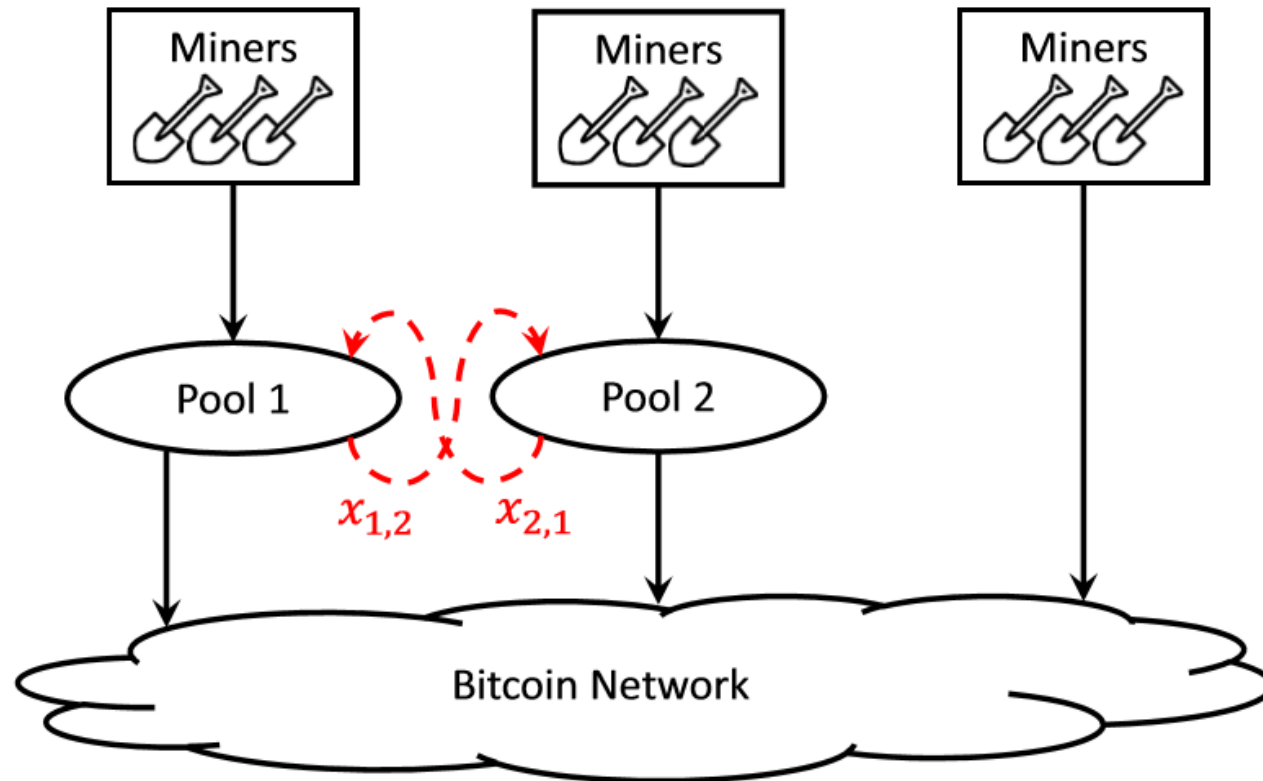
FAW Attack Against Multiple Pools



FAW Attack Against Two Pools



FAW Attack Game

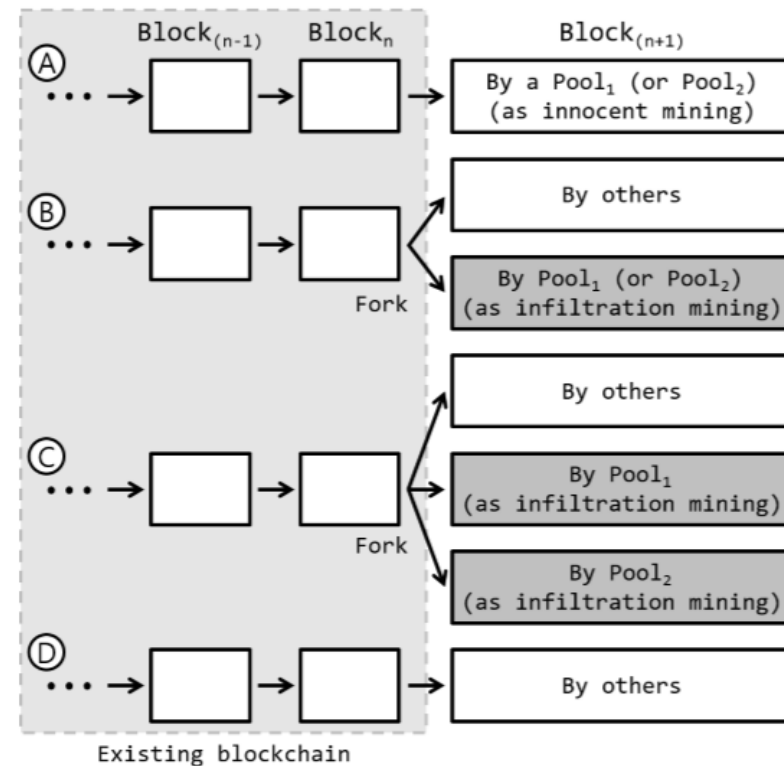


FAW Attack Game

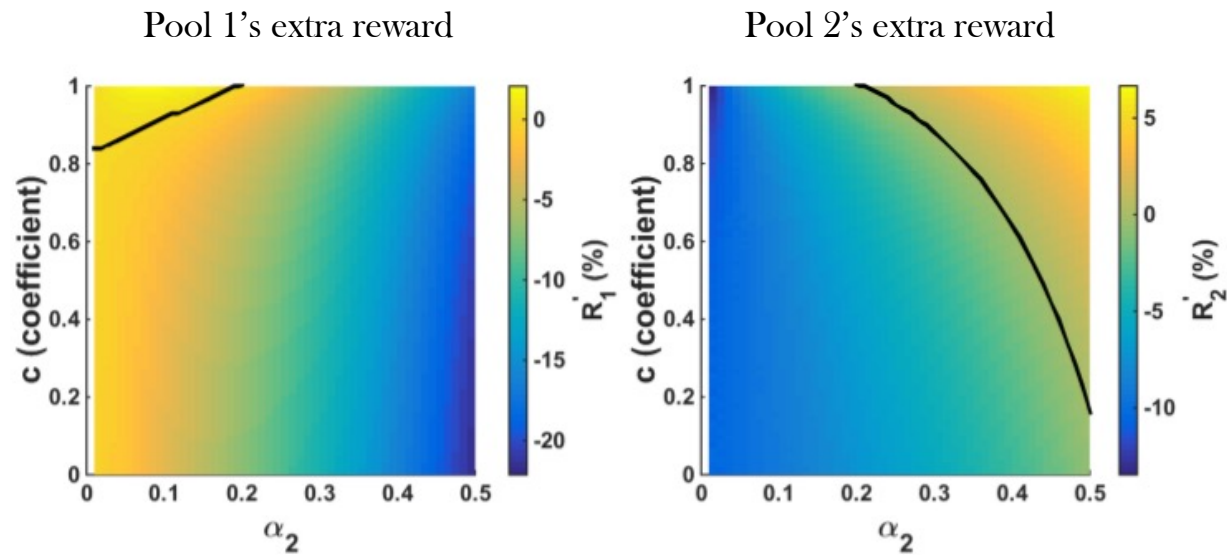
- Two pools attack each other. \Rightarrow *FAW Attack Game between two pools*

$$R_1 = \frac{\alpha_1 - f_1}{1 - f_1 - f_2} + c_2 f_2 \frac{1 - \alpha_1 - \alpha_2}{1 - f_2} + c_2' f_1 f_2 \left(\frac{1}{1 - f_1} + \frac{1}{1 - f_2} \right) \frac{1 - \alpha_1 - \alpha_2}{1 - f_1 - f_2} + R_2 \frac{f_1}{\alpha_2 + f_1}$$

$$R_2 = \frac{\alpha_2 - f_2}{1 - f_1 - f_2} + c_1 f_1 \frac{1 - \alpha_1 - \alpha_2}{1 - f_1} + c_1' f_1 f_2 \left(\frac{1}{1 - f_1} + \frac{1}{1 - f_2} \right) \frac{1 - \alpha_1 - \alpha_2}{1 - f_1 - f_2} + R_1 \frac{f_2}{\alpha_1 + f_2}$$

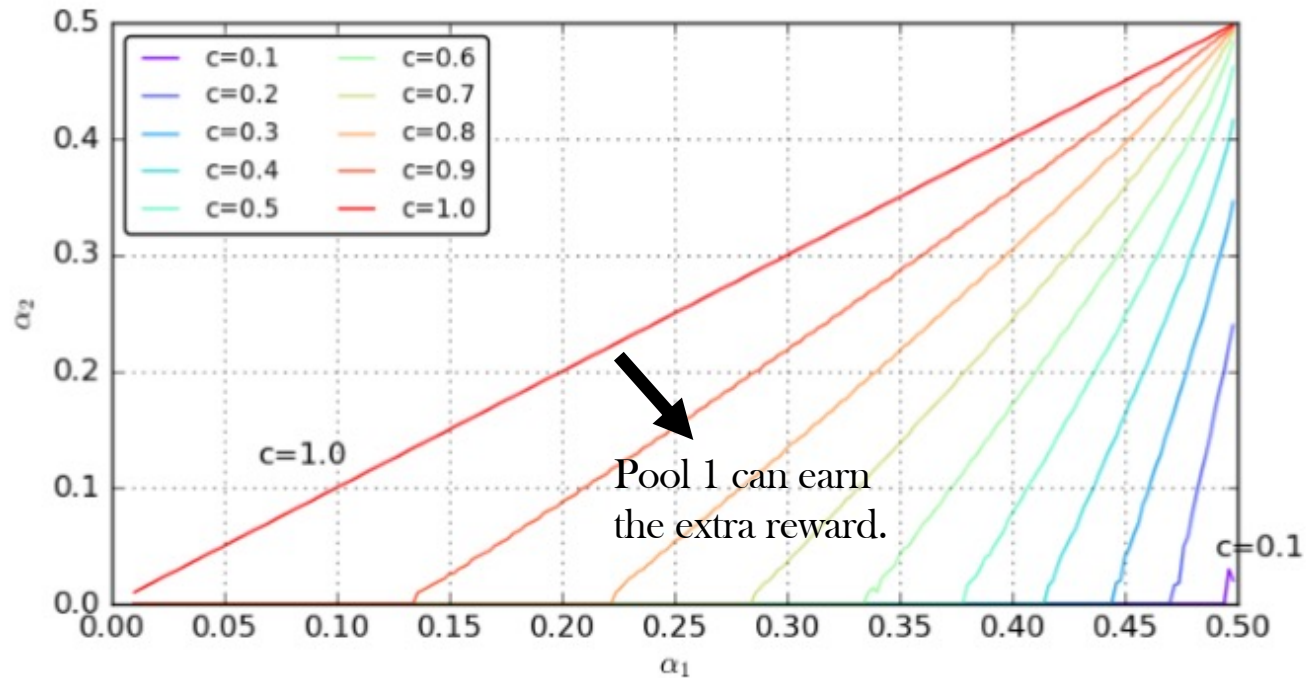


Result



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

Break Dilemma



- ❖ The FAW attack game leads to a pool size game: the larger pool can always earn the extra reward.

Detection

- ❑ The FAW attack is easier to detect than the BWH attack because of the high fork rate.
- ❑ The manager should suspect and expel any miner who submits stale FPoWs, rather than paying out the reward for the current round.
- ❑ The attacker may easily launch the attack using many Sybil nodes with many churns, replacing the expelled miner.
- ❑ The behavior makes detection useless.

No Silver Bullet

- ❑ Detection
 - Beacon value
 - Honeypots
 - An attacker can be rarely affected by the detection.

- ❑ New reward system
 - High variance of rewards

- ❑ Change Bitcoin protocol
 - Two-phase proof-of-work
 - Not backward compability

- ❑ **There is no one silver bullet.**



The FAW Attack is Stronger Than Existing Attacks.

Questions?

□ Yongdae Kim

- ▶ email: yongdaek@kaist.ac.kr
- ▶ Home: <http://syssec.kaist.ac.kr/~yongdaek>
- ▶ Facebook: <https://www.facebook.com/y0ngdaek>
- ▶ Twitter: <https://twitter.com/yongdaek>
- ▶ Google “Yongdae Kim”