MONASH University

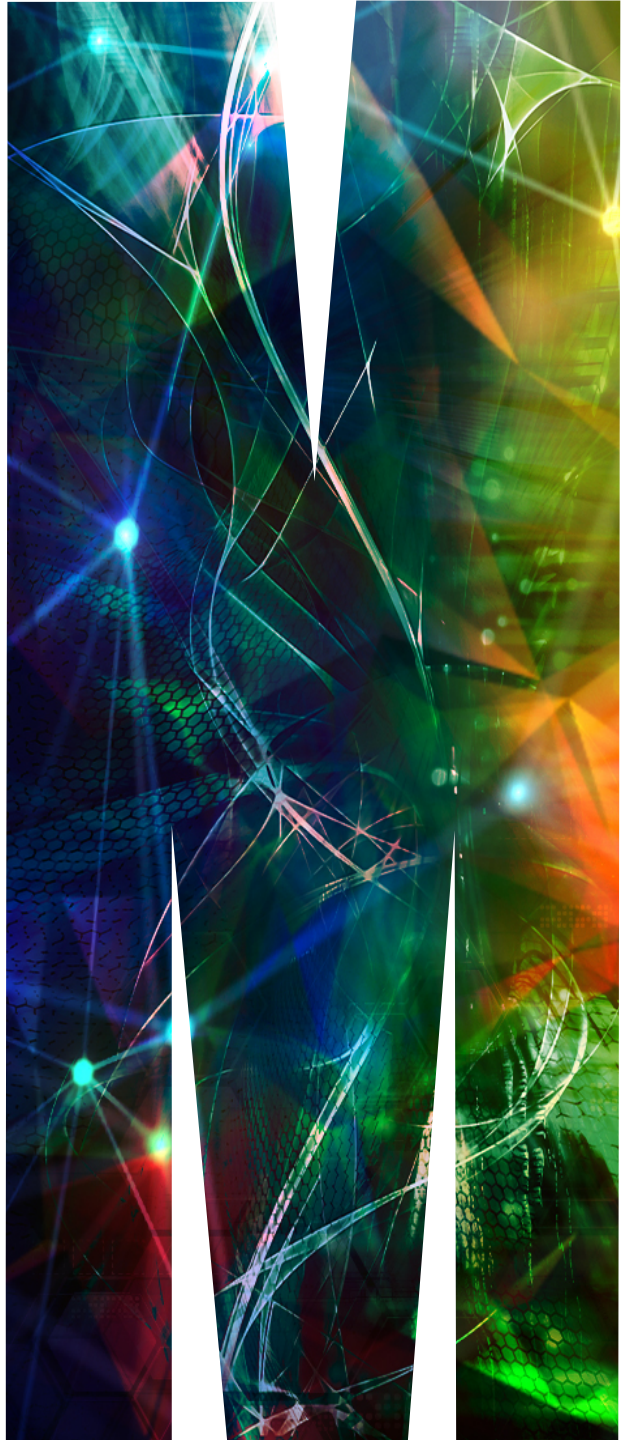
FIT5214: Blockchain

Lecture 5: Attacks on Blockchain

Lecturer: Rafael Dowsley

rafael.dowsley@monash.edu

https://dowsley.net



Unit Structure

- **Lecture 1: Introduction to Blockchain**
- **Lecture 2: Bitcoin**
- **Lecture 3: Ethereum and Smart Contracts**
- **Lecture 4: Proof-of-Work (PoW)**
- **Lecture 5: Attacks on Blockchains**
- **Lecture 6: Class Test/Alternatives to PoW**
- **Lecture 7: Proof-of-Stake (PoS)**
- **Lecture 8: Privacy**
- **Lecture 9: Byzantine Agreement**
- **Lecture 10: Blockchain Network**
- **Lecture 11: Payment Channels**
- **Lecture 12: Guest Lecture**

Unit Structure

- Lecture 1: Introduction to Blockchain
- Lecture 2: Bitcoin
- Lecture 3: Ethereum and Smart Contracts
- Lecture 4: Proof-of-Work (PoW)
- Lecture 5: Attacks on Blockchains
- Lecture 6: Class Test/Alternatives to PoW
- Lecture 7: Proof-of-Stake (PoS)
- Lecture 8: Privacy
- Lecture 9: Byzantine Agreement
- Lecture 10: Blockchain Network
- Lecture 11: Payment Channels
- Lecture 12: Guest Lecture

In-Semester Class Test

- **Next Wednesday (31st of August 2022), 10am-11am using eAssessment.**
- **The test will assess the contents that were covered until Week 5.**
- **Regarding the labs, you are not required to know Unix commands by heart, but the concepts that were covered in the labs' discussions are examinable (the part about Atomic Cross-Chain Trading from this week's lab will not be examined this semester).**
- **After the test, a shorter lecture from 11am until 11:50pm.**

In-Semester Class Test

- In the first section, there will be 7 multiple choice questions with multiple right answers (each question is worth 2 marks). Select all right answers.
- Every right answer that is selected will give positive marks, every wrong answer that is selected will deduct marks (overall the grade of each question is between 0.0 and 2.0).
- E.g., Which of the following are cities in Australia?
  - Sydney
  - Tokyo
  - Melbourne
  - Paris

In-Semester Class Test

- In the second section, there will be 2 multiple choice questions with a single right answer (1 mark each). Just select the single right answer for each question.

- E.g., What is the capital of Australia?
  - Sydney
  - Canberra
  - Melbourne
  - Brisbane

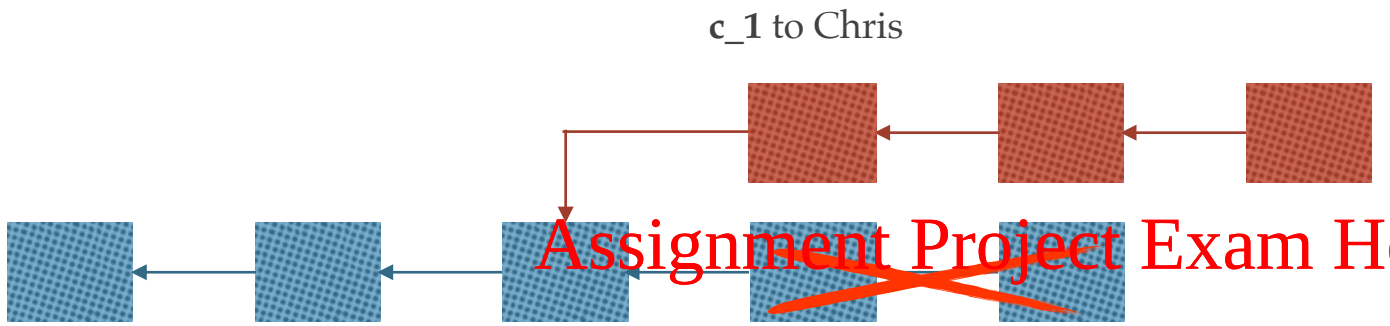
In-Semester Class Test

- **In the last section, there will be 2 short answers questions (each worth two marks). Just type the numerical answer.**
- **How much is 10 x 5?**
- **50**

Feedback

- **Preliminary Unit Design and Delivery Feedback (iSETU)**
- **https://lms.monash.edu/mod/feedback/view.php?id=10523428**
- **Your feedback is very important so that we can keep improving this unit**

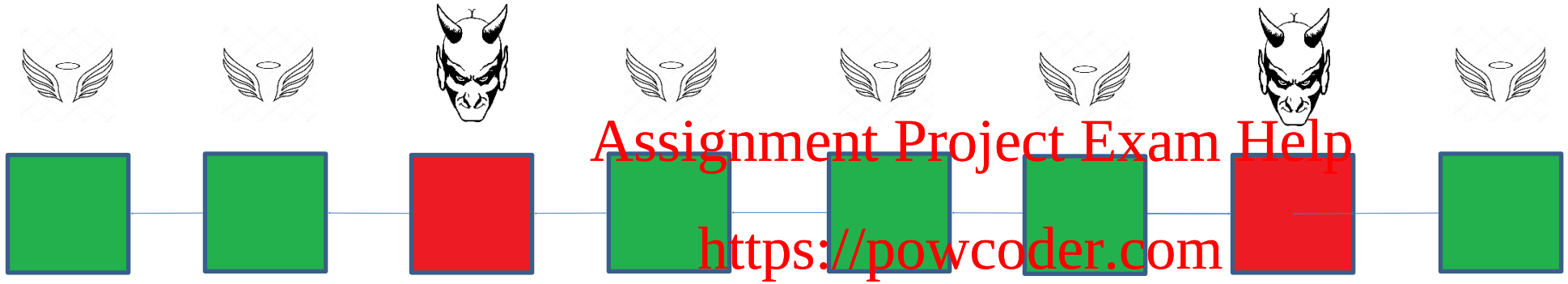
Recap: 51% attacks



If an attacker has >50% CPU power, it can spend a coin more than once.

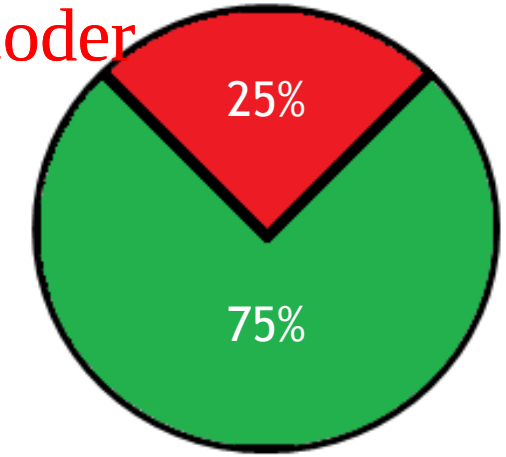
Recap: 51% attack

Recap: Chain Quality



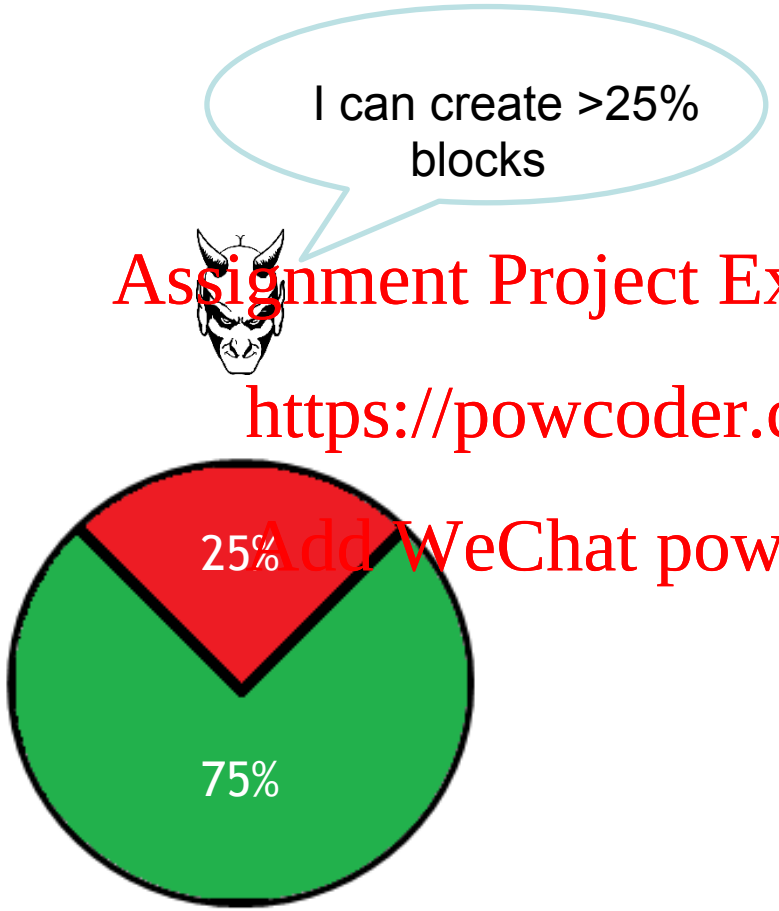
Adversarial contribution = 2/8 = 25%

Ideal Chain Quality



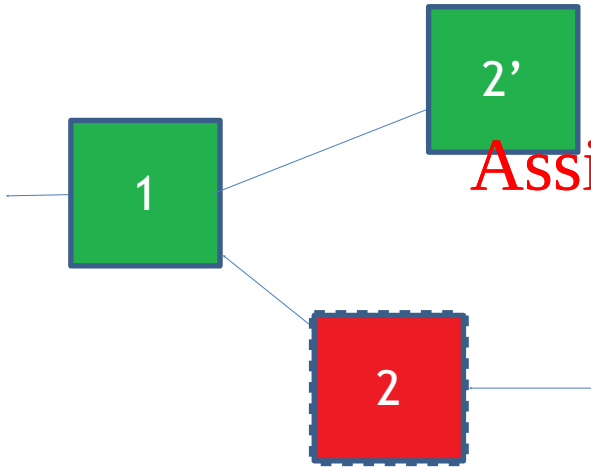
MONASH University

Non-majority attacks



Selfish mining attack

Basic idea: find a smart strategy to release blocks, to get extra advantage



Read more: https://arxiv.org/pdf/1311.0243.pdf

Selfish mining attack

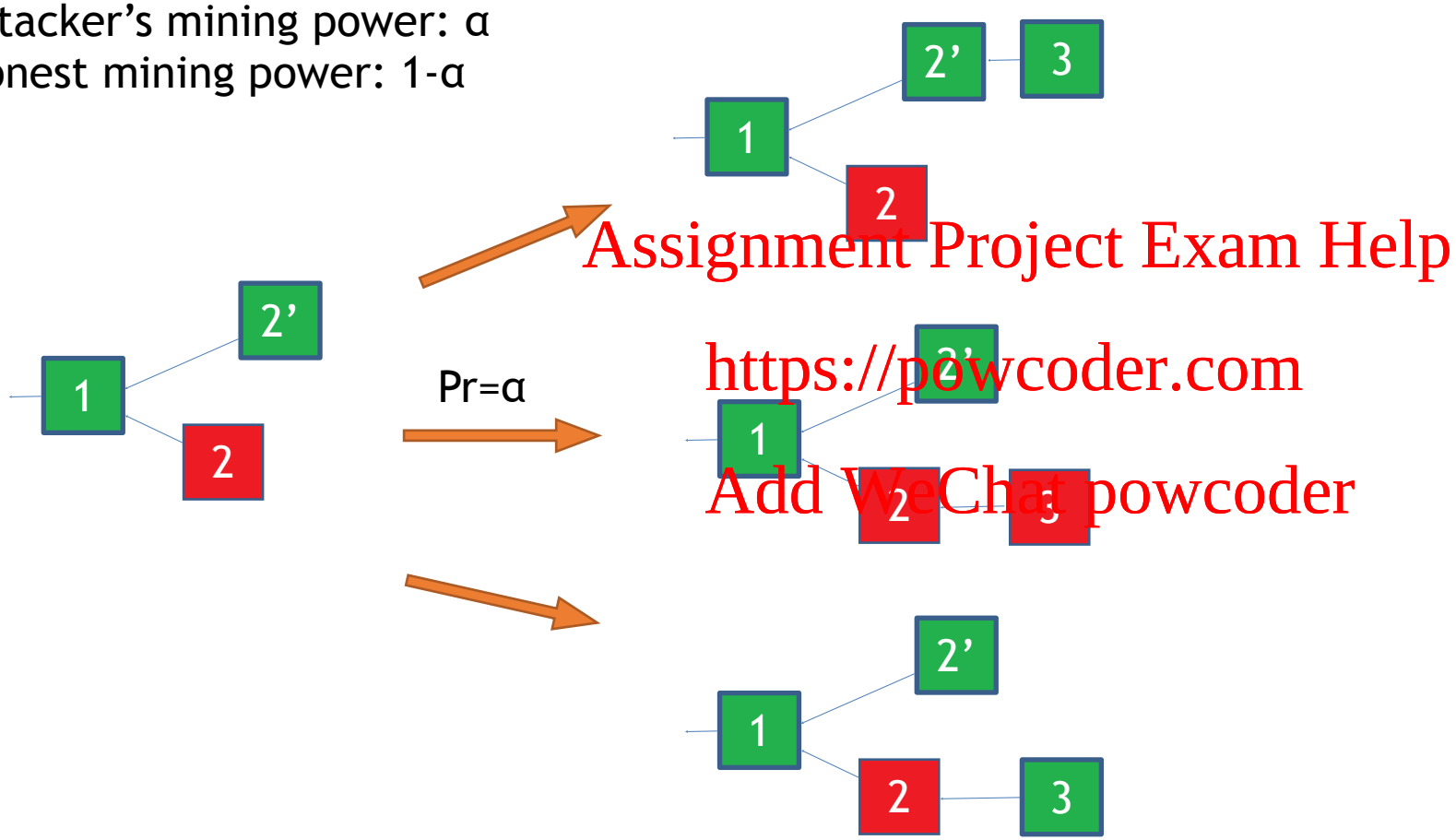
Key Idea: adversary keeps the blocks he discovers private in most situations, thereby intentionally forking the chain.

- If both public and private branches have length 1 and the adversary mines a block, he reveals both blocks of his private branch, making that the longest chain.
- In all other cases that the adversary mines a new block, he keeps it private.
- If any honest miner mines a new block and that makes both branches have length 1, then the adversary reveals his private block and tries his luck.
- If any honest miner mines a new block and that makes the public branch exactly one block smaller than the private branch, then the adversary reveals his whole private branch, making it part of the longest chain.

Read more: https://arxiv.org/pdf/1311.0243.pdf

Selfish mining attack

Attacker's mining power: α
Honest mining power: 1-α

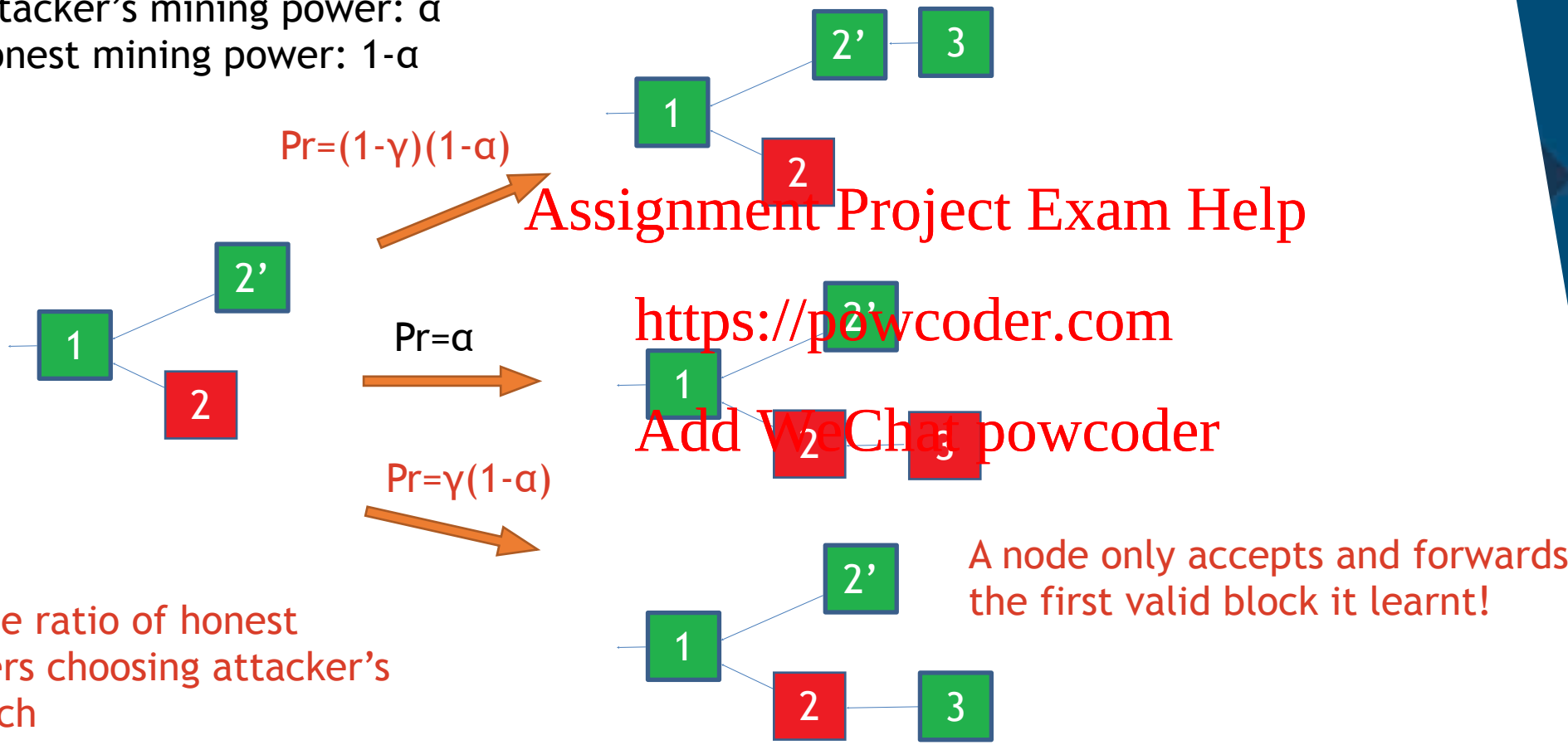


The attacker may have better network connectivity

Read more: https://arxiv.org/pdf/1311.0243.pdf

Selfish mining attack

Attacker's mining power: α
Honest mining power: 1-α



γ: the ratio of honest miners choosing attacker's branch

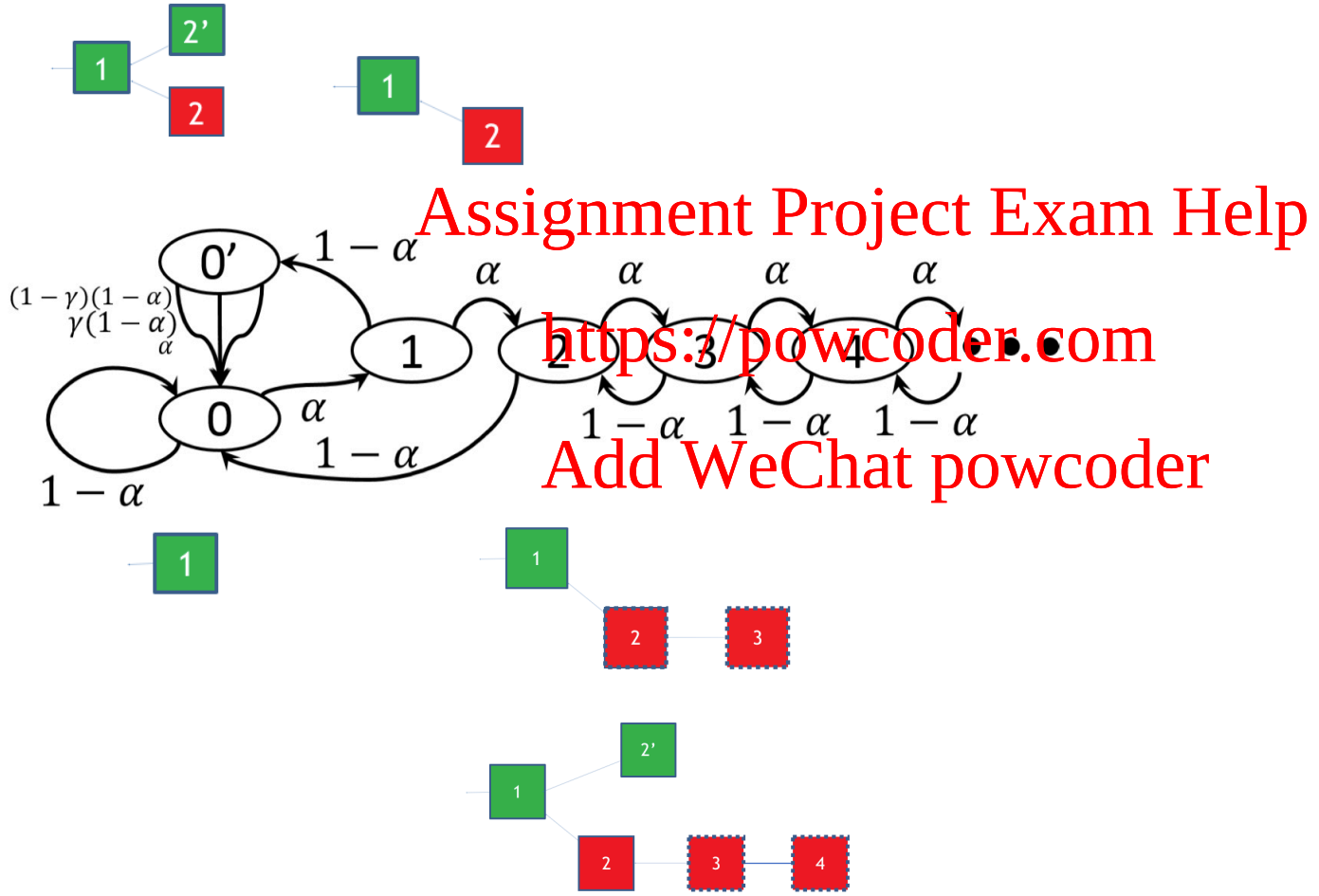
A node only accepts and forwards the first valid block it learnt!

The attacker may have better network connectivity

Read more: https://arxiv.org/pdf/1311.0243.pdf

Selfish mining attack

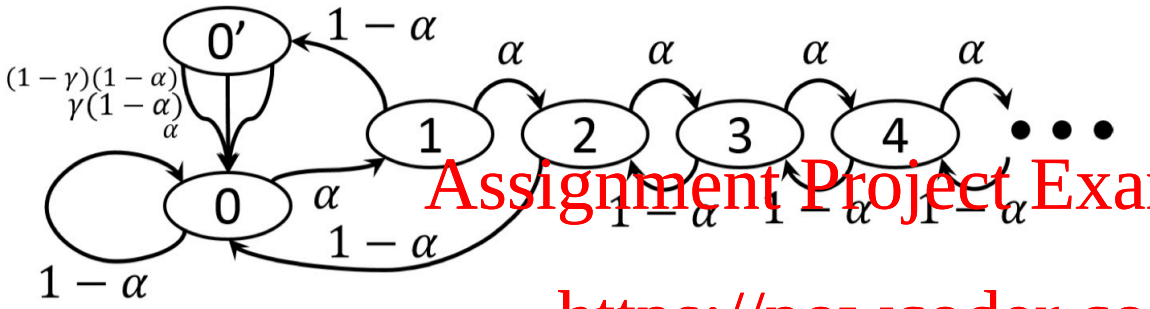
State machine with transition frequencies



Read more: https://arxiv.org/pdf/1311.0243.pdf

ACK: Thanks to Ittay Eyal for agreeing to use his figures in these slides.

Pr(state)



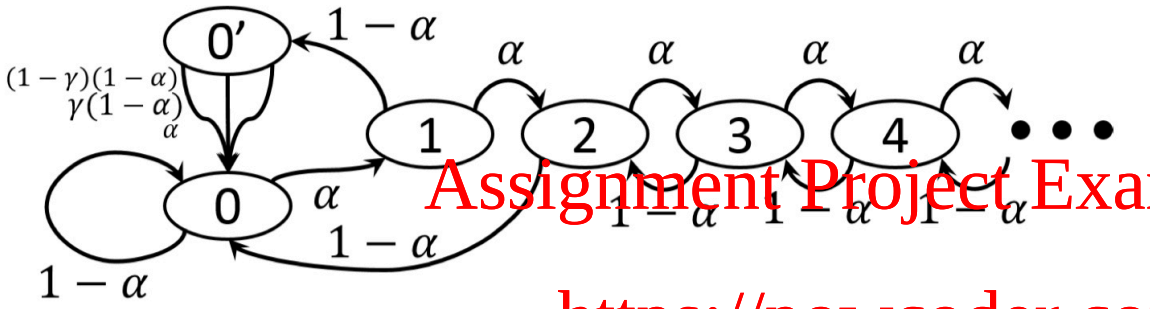
$P_1 = \alpha P_0$

$P_{0'} = ?$

$P_0 = ?$

Read more: https://arxiv.org/pdf/1311.0243.pdf

Pr(state)



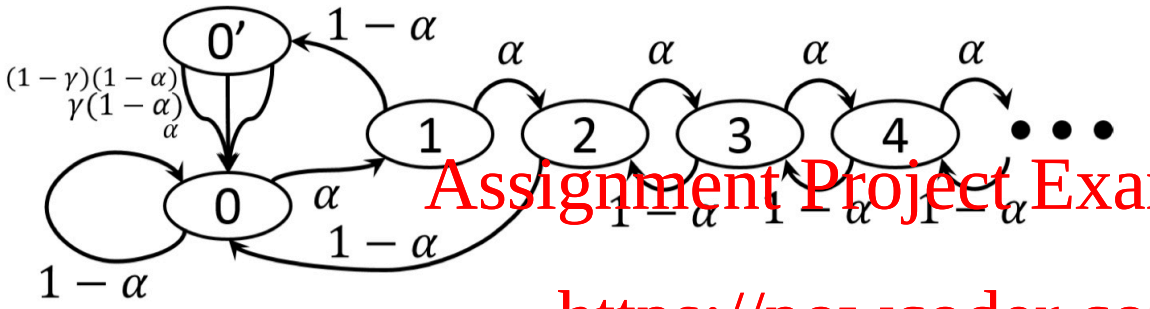
$$P_1 = \alpha P_0$$

$$P_{0'} = (1-\alpha)P_1$$

$$P_0 = P_{0'} + (1-\alpha)P_0 + (1-\alpha)P_2$$

Read more: https://arxiv.org/pdf/1311.0243.pdf

Pr(state)



$$P_1 = \alpha P_0$$

$$P_{0'} = (1-\alpha)P_1$$

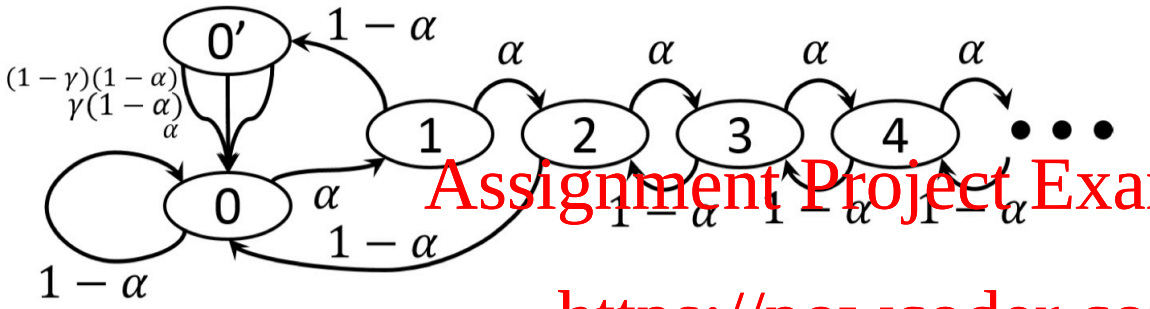
$$P_0 = P_{0'} + (1-\alpha)P_0 + (1-\alpha)P_2$$

Is the following equation true?

$$\alpha P_0 = (1-\alpha)P_1 + (1-\alpha)P_2$$

Read more: https://arxiv.org/pdf/1311.0243.pdf

Pr(state)



$$P_1 = \alpha P_0$$

$$P_{0'} = (1-\alpha)P_1$$

$$P_0 = P_{0'} + (1-\alpha)P_0 + (1-\alpha)P_2$$

$$\begin{aligned} P_0 &= P_0 + (1-\alpha)P_0 + (1-\alpha)P_2 \\ &= (1-\alpha)P_1 + (1-\alpha)P_0 + (1-\alpha)P_2 \end{aligned}$$

$$\rightarrow$$

$$\alpha P_0 = (1-\alpha)P_1 + (1-\alpha)P_2$$

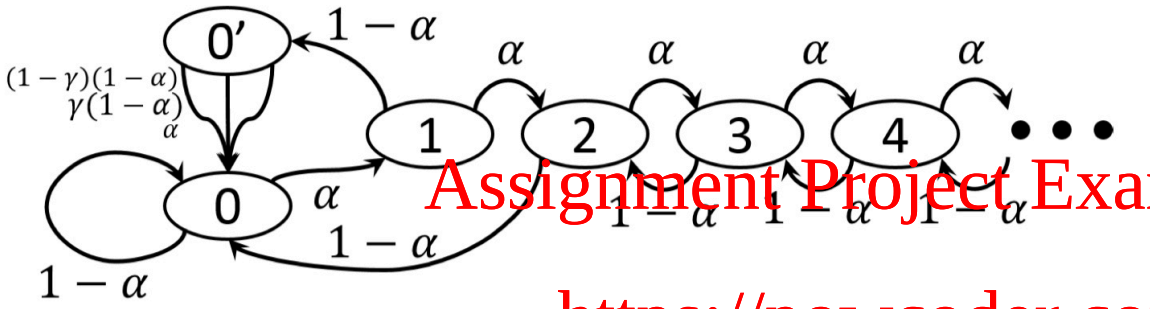
Is the following equation true?

$$\alpha P_0 = (1-\alpha)P_1 + (1-\alpha)P_2$$

Read more: https://arxiv.org/pdf/1311.0243.pdf

MONASH University

Pr(state)



$$P_1 = \alpha P_0$$

$$P_{0'} = (1-\alpha)P_1$$

$$P_0 = P_{0'} + (1-\alpha)P_0 + (1-\alpha)P_2$$

$$P_0 = P'_0 + (1-\alpha)P_0 + (1-\alpha)P_2$$

$$= (1-\alpha)P_1 + (1-\alpha)P_0 + (1-\alpha)P_2$$

$$\rightarrow$$

$$\alpha P_0 = (1-\alpha)P_1 + (1-\alpha)P_2$$

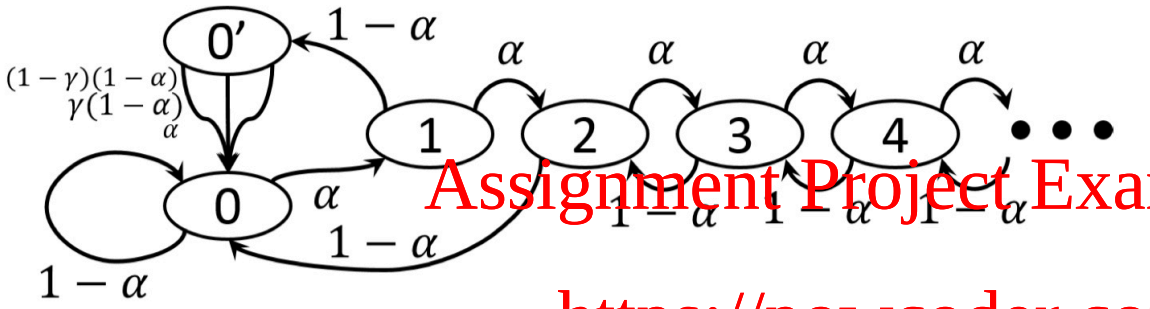
$$\alpha P_0 = (1-\alpha)P_1 + (1-\alpha)P_2$$

Given only α, what is P_0?

Read more: https://arxiv.org/pdf/1311.0243.pdf

MONASH University

Pr(state)



$$p_0 = \frac{\alpha - 2\alpha^2}{\alpha(2\alpha^3 - 4\alpha^2 + 1)}$$

$$p_{0'} = \frac{(1-\alpha)(\alpha - 2\alpha^2)}{1 - 4\alpha^2 + 2\alpha^3}$$

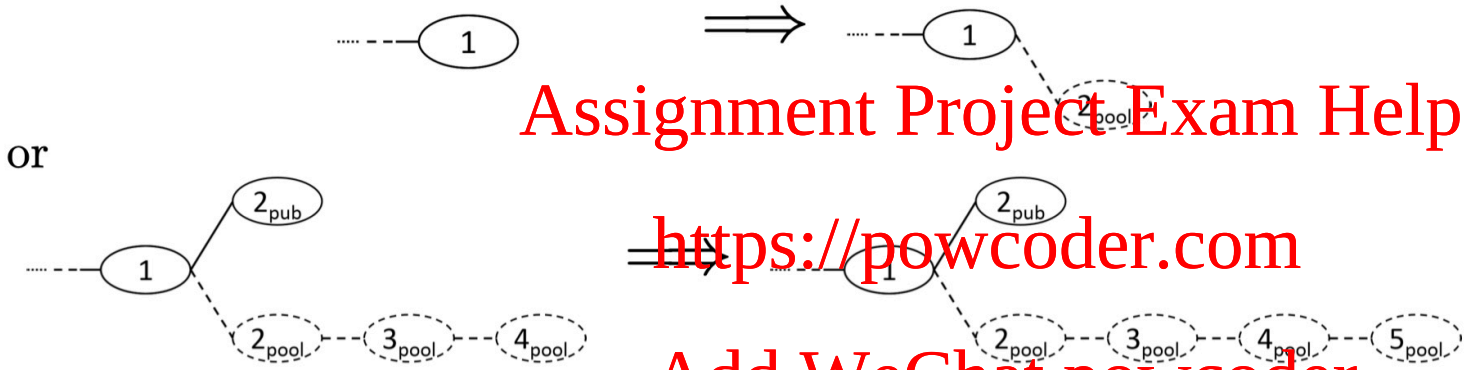
$$p_1 = \frac{\alpha - 2\alpha^2}{2\alpha^3 - 4\alpha^2 + 1}$$

$$\forall k \geq 2 : p_k = \left(\frac{\alpha}{1-\alpha}\right)^{k-1} \frac{\alpha - 2\alpha^2}{2\alpha^3 - 4\alpha^2 + 1}$$

Read more: https://arxiv.org/pdf/1311.0243.pdf

Different cases

1. Any state but two branches of length 1, attacker finds a block.



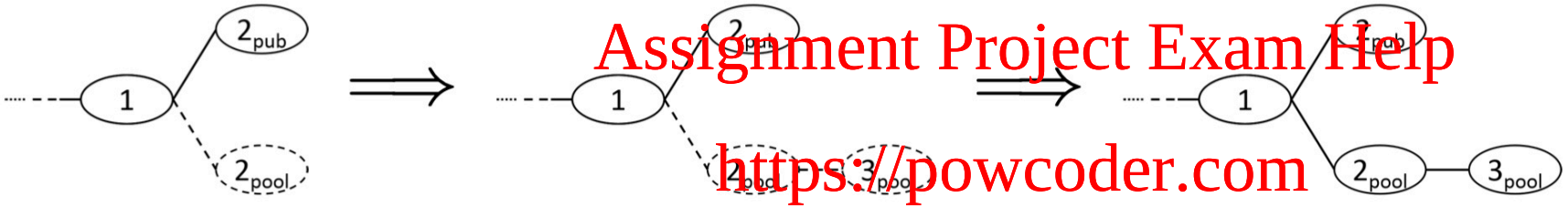
The attacker appends one block to its private branch, increasing its lead on the public branch by one.

The revenue from this block will be determined later.

Read more: https://arxiv.org/pdf/1311.0243.pdf

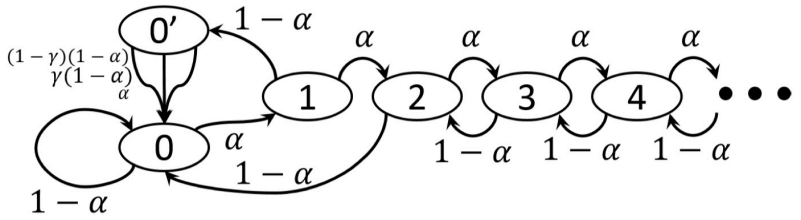
Different cases

2. Two branches of length 1, attacker finds a block



The attacker publishes its secret branch of length two, thus obtaining a revenue of two.

r(Attacker)=$P_0' \cdot \alpha \cdot 2$

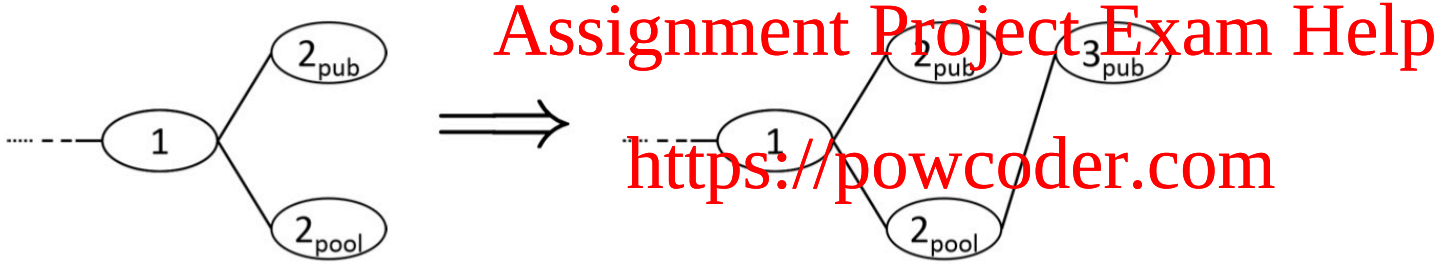


Read more: https://arxiv.org/pdf/1311.0243.pdf

MONASH University

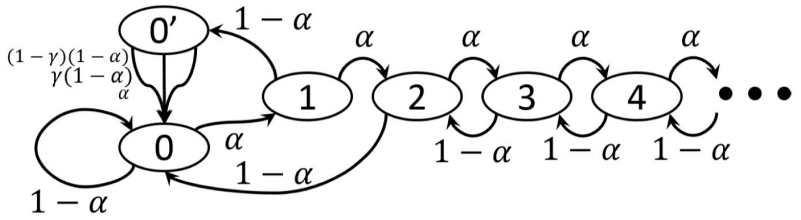
Different cases

3. Two branches of length 1, honest miner finds a block on the attacker's branch



Attacker and honest miner each obtain a revenue of one.

$r(\text{honest}) = r(\text{Attacker}) = P_0' \cdot \gamma(1-\alpha) \cdot 1$

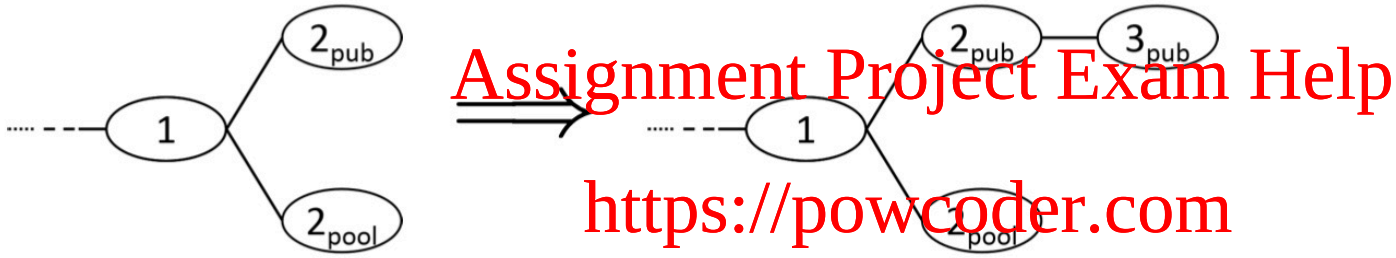


Read more: https://arxiv.org/pdf/1311.0243.pdf

MONASH University

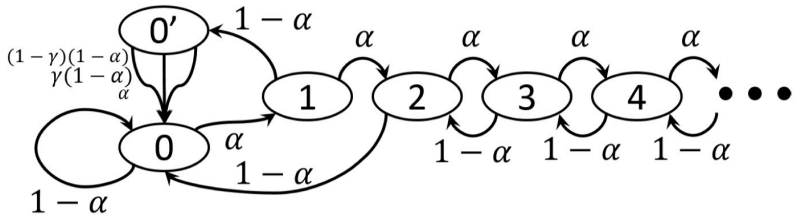
Different cases

4. Two branches of length 1, honest miner finds a block on honest branch



Honest miner obtains a revenue of two.

$r(\text{honest}) = P_0' \cdot (1-\gamma)(1-\alpha) \cdot 2$



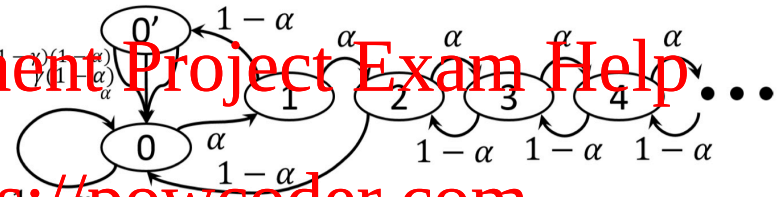
Read more: https://arxiv.org/pdf/1311.0243.pdf

MONASH University

Different cases

5. No private branch, honest miners find a block

$r(\text{honest}) = P_0 \cdot (1-\alpha) \cdot 1$



The honest miner obtains a revenue of one, all miners start from the new block.

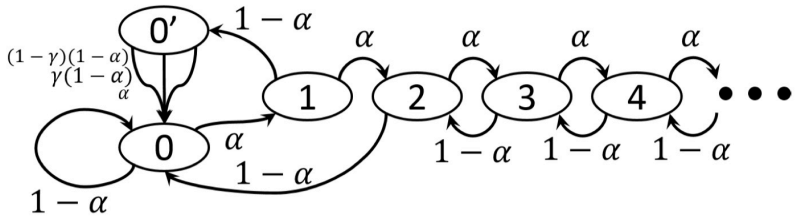
Read more: https://arxiv.org/pdf/1311.0243.pdf

Different cases

6. Lead was 1, honest miners find a block

The revenue from this block cannot be determined yet.

From P_1 to $P_{0'}$



Read more: https://arxiv.org/pdf/1311.0243.pdf

MONASH University

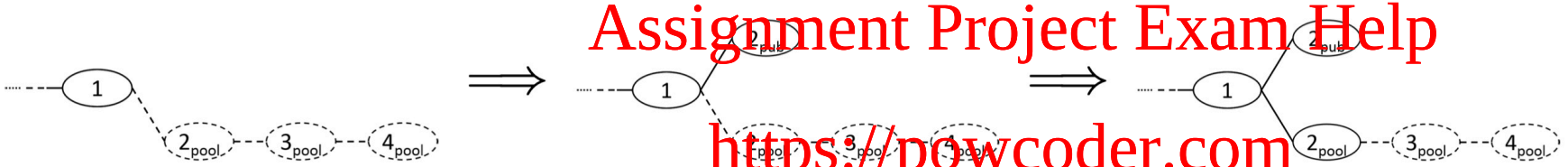
Different cases

7. Lead was 2, honest miners find a block

The attacker reveal its secret blocks and obtains a revenue of 2.

Different cases

8. Lead was more than 2, honest miners find a block



The lead of the attacker decreases by 1, but remains at least two. The new block will end outside the canonical chain once the attacker eventually reveals his entire secret branch. Therefore the honest miners do not get any revenue, and the attacker gets a revenue of 1.

Question:

If an attacker has good network connectivity, the attacker needs ____ mining power to launch selfish mining attacks to gain extra profit.

Selfish mining attack

To launch attack with extra profit:

1. Limited network connectivity: >1/3 mining power
2. With good network connectivity: any percent of mining power

Once learnt someone else's block, the attacker sends its block (faster) than the other block

* The problem: A node only accepts and forwards the first valid block it learnt!

What if we choose conflict blocks randomly?

>25% mining power is required to launch selfish mining attack, with any network connectivity

Read more: https://arxiv.org/pdf/1311.0243.pdf

Selfish mining attack

Two strategies:

1. Choosing the first valid block
2. Choosing a valid block randomly

Which proposal is better, why?

Selfish mining attack

If choosing the first valid block, then successful launching this attack requires

1. >1/3 mining power with limited network connectivity; or
2. any percent of mining power with perfect network connectivity

Advantage:

If the network connectivity is not perfect, then the attacker may need more than 25% to successfully launch the attack.

Selfish mining attack

If choosing a valid block randomly, then successful launching this attack requires >25% mining power

Advantage:

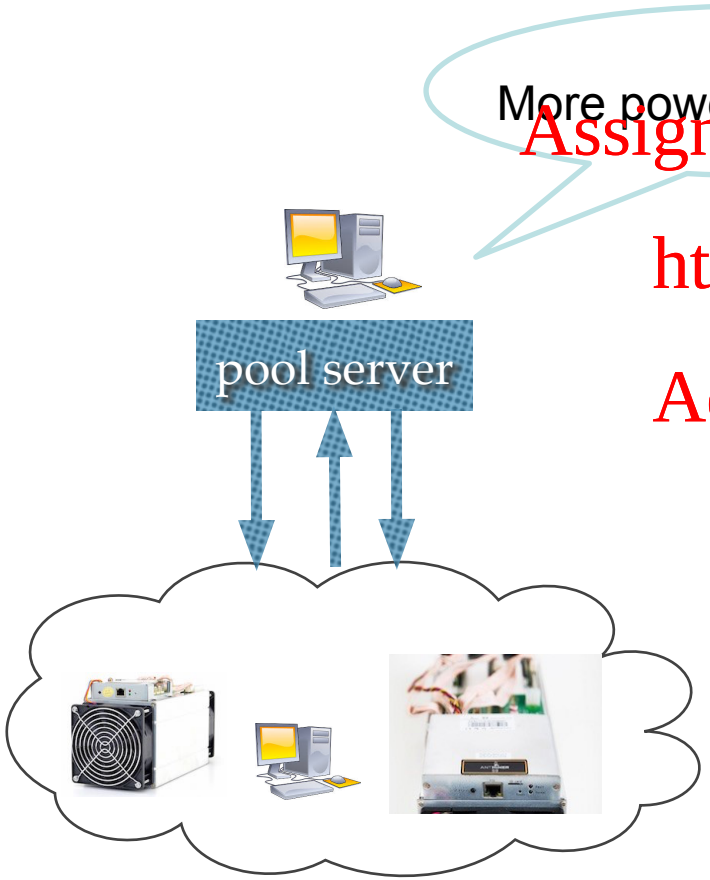
An attacker cannot launch a successful attack with less than 25% mining power.

Take home message:

By launching selfish mining attack, an attacker can obtain a ratio of revenue that is larger than its ratio of mining power.

Selfish mining attack

The larger the selfish mining power is,
the **more extra revenue per mining power unit** the attacker will gain.



This encourages a mining pool to get more mining power, which may potentially be over 50%.

Read more: https://arxiv.org/pdf/1311.0243.pdf

Quiz (multiple choice):

Which of the following properties does the selfish mining attack potentially break?

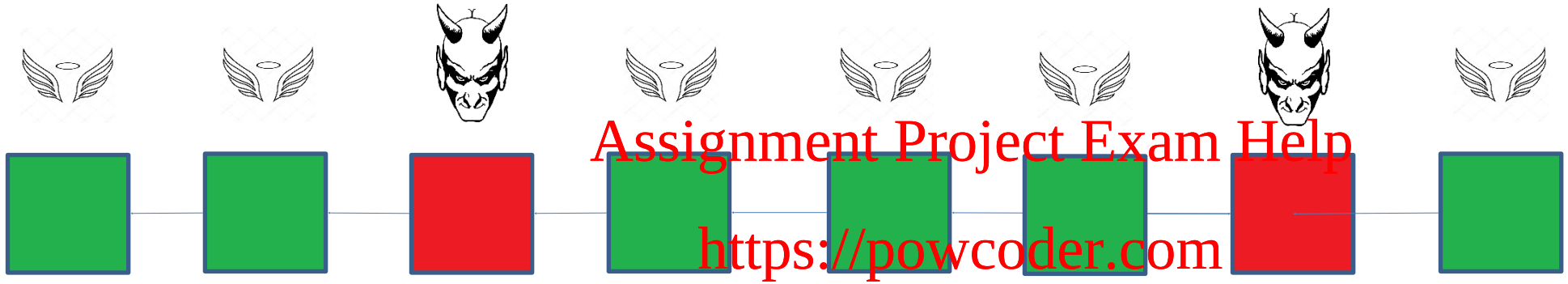
A. Consensus liveness
B. Consensus safety
C. Chain quality
D. Chain growth
E. T-consistency

Answer:

Which of the following properties does the selfish mining attack potentially break?

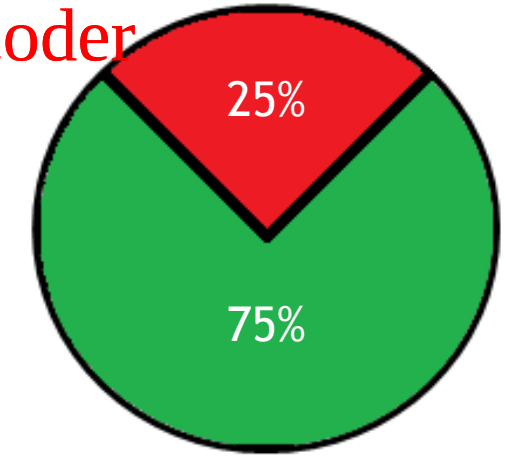
A. Consensus liveness
B. Consensus safety
C. Chain quality
D. Chain growth
E. T-consistency

Recap: Chain Quality



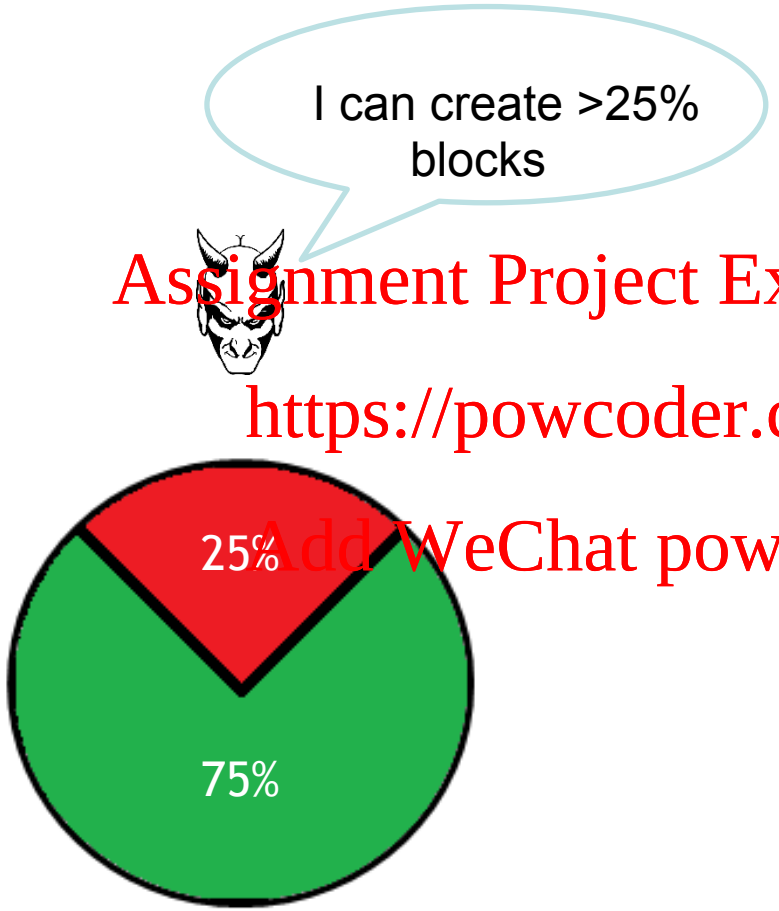
Adversarial contribution = 2/8 = 25%

Ideal Chain Quality



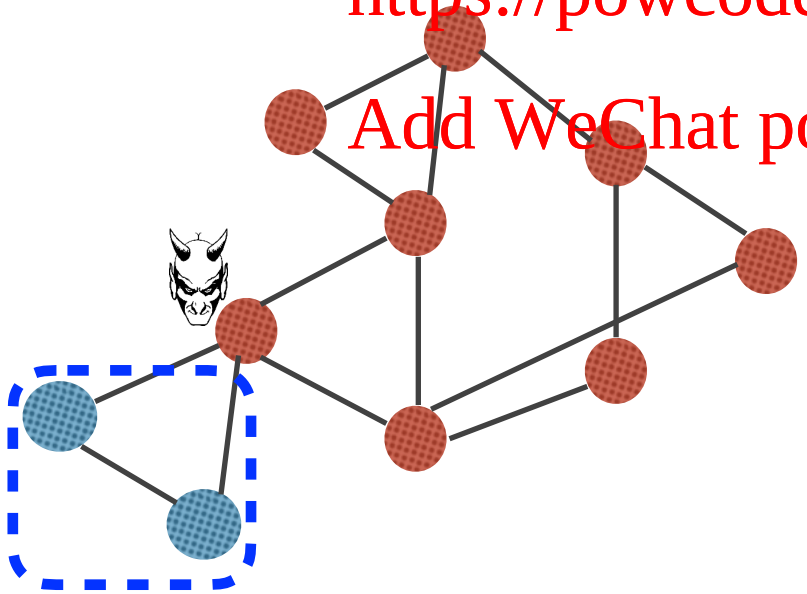
MONASH University

Non-majority attacks

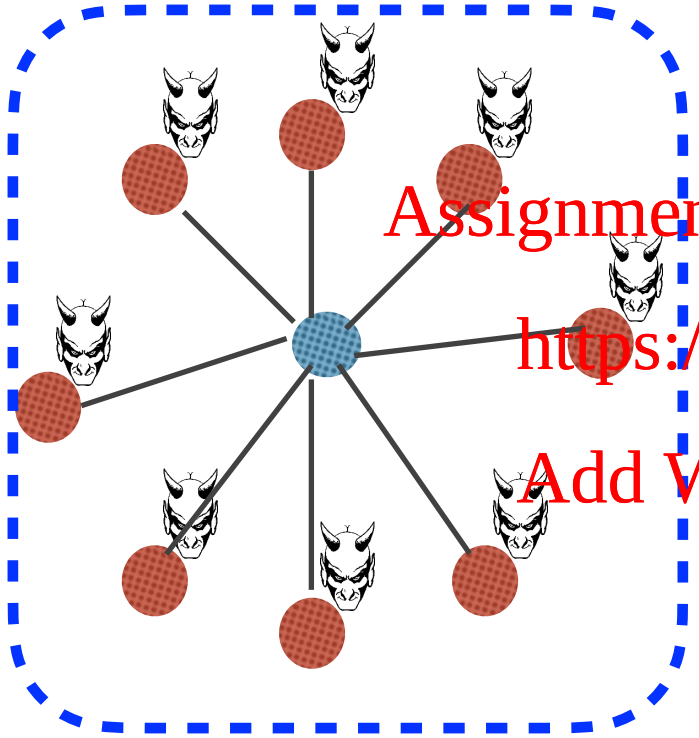


Peer-to-peer network

1. Each peer has at most 125 connections
    1. At most 8 outgoing TCP connections by default
    2. At most 117 incoming connections by default
2. Outgoing connections are used to sent out messages to the P2P network
3. Incoming connections are used to receive messages from the P2P network
4. All information about peers are maintained in a peer table locally

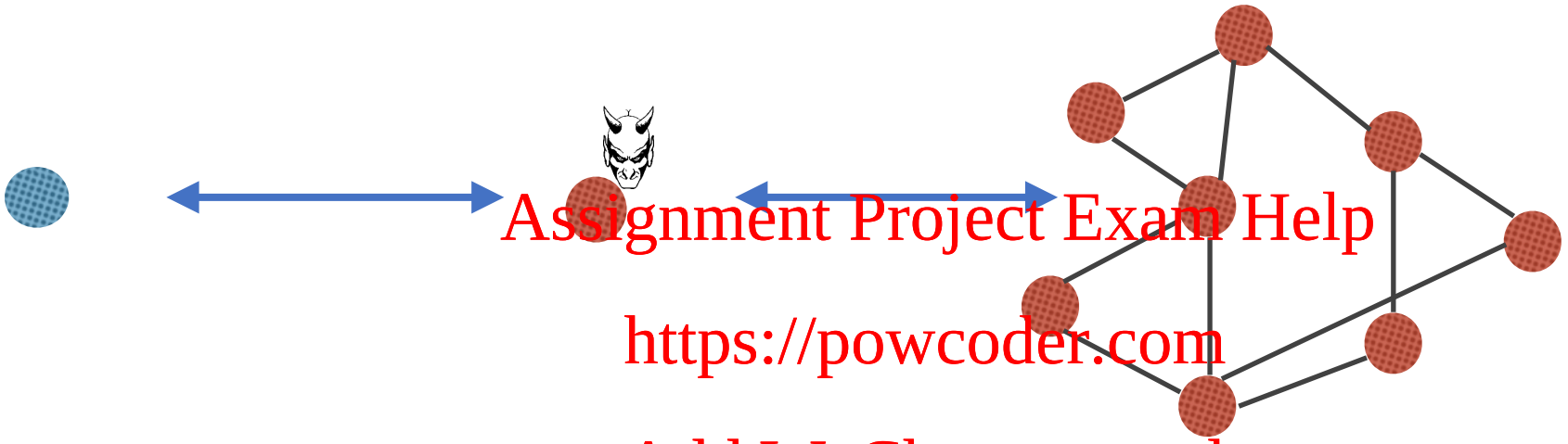


Eclipse attack



network isolated by an attacker

Eclipse attack

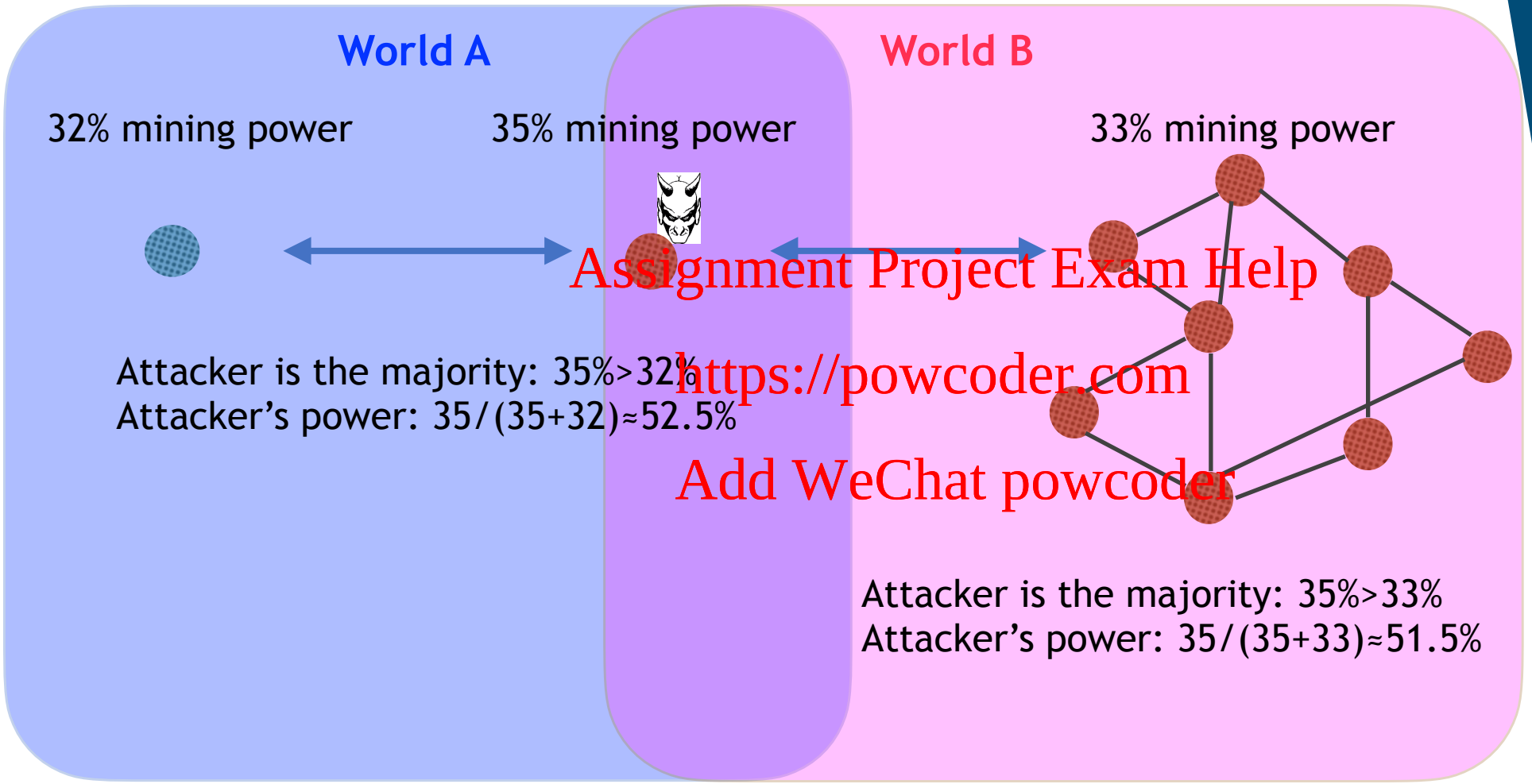


Eclipse attack

Group discussion:

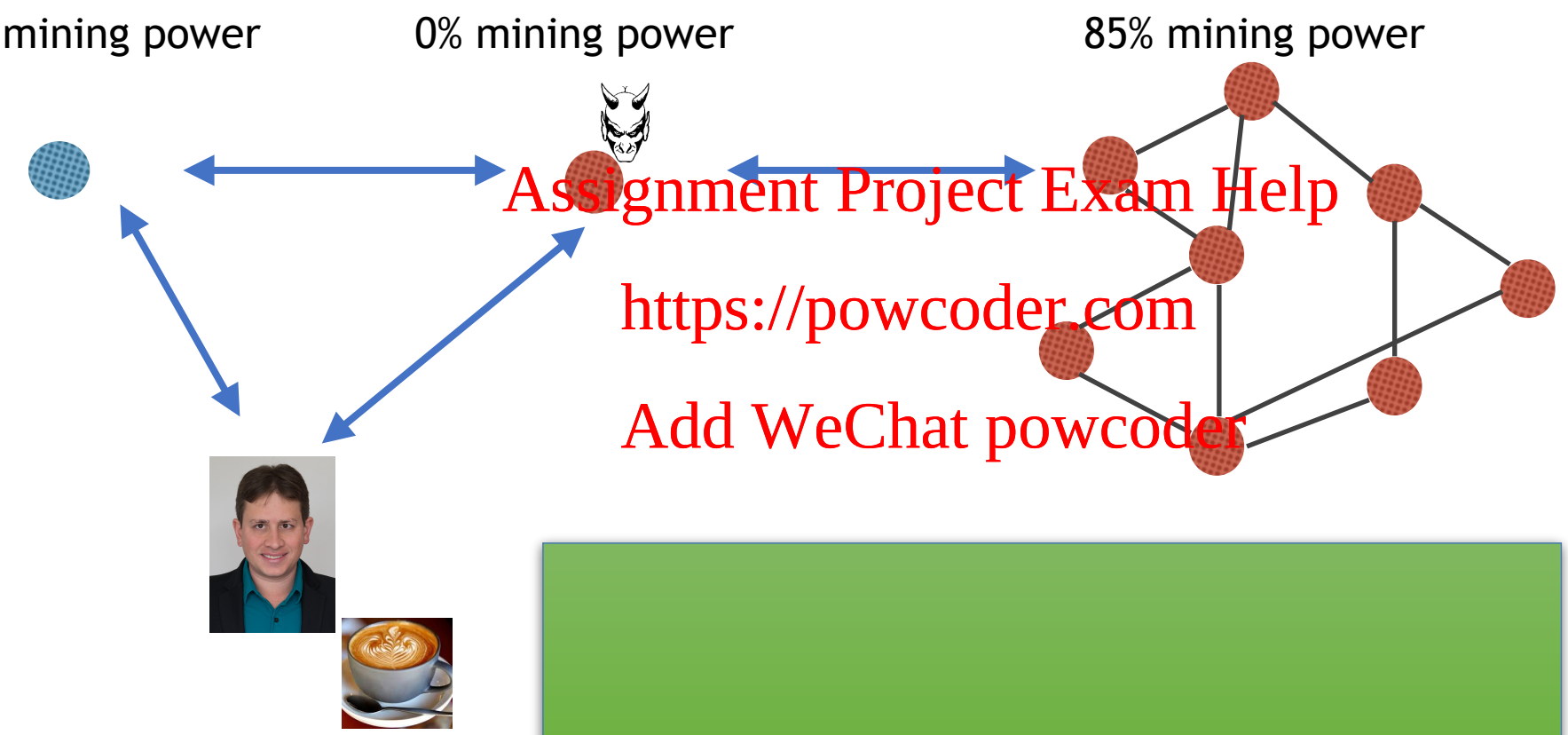
Can you attack this system to double spend?

Eclipse attack



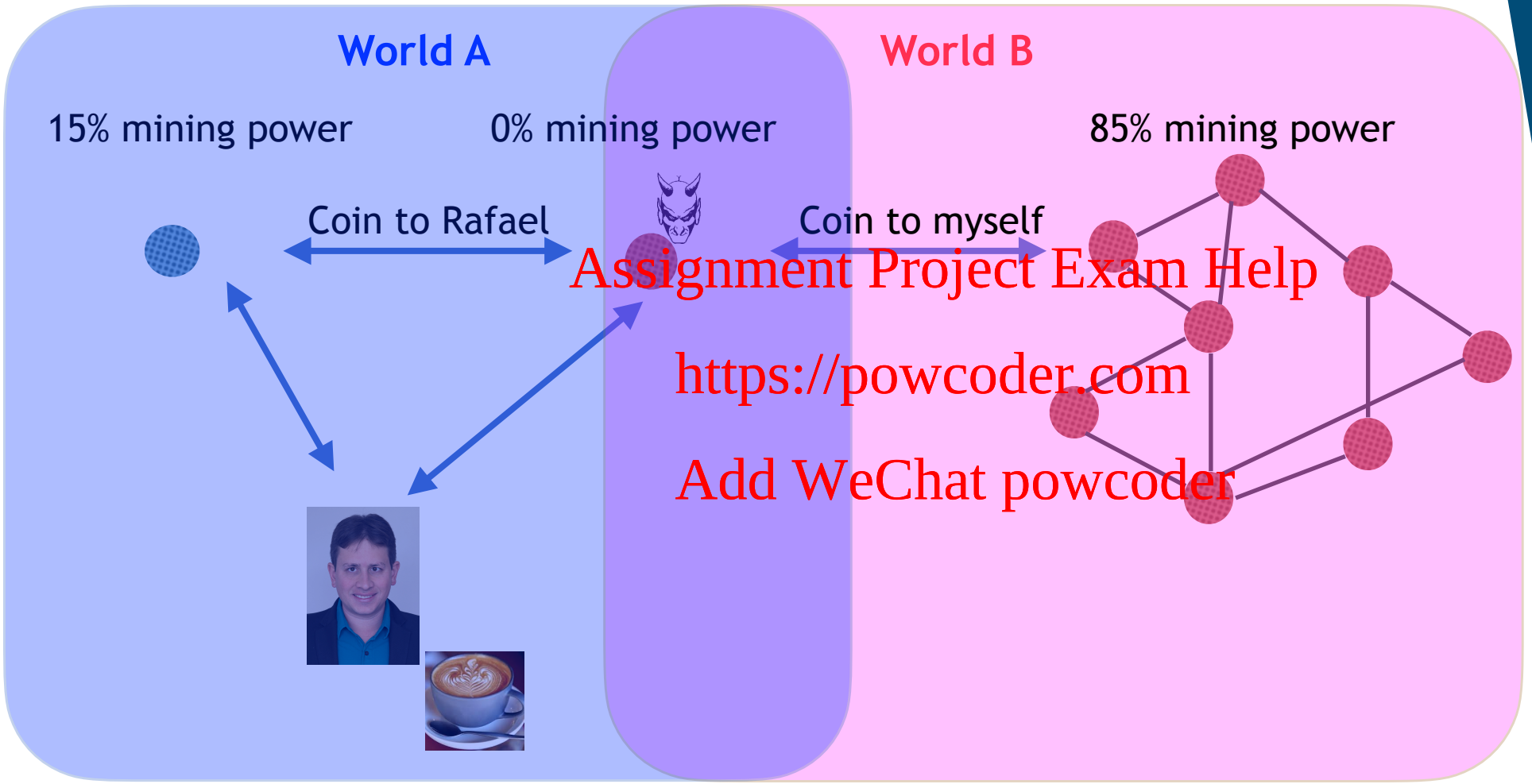
Both worlds accept the attacker's chain!
With less than 50% mining power, the attacker is able to launch majority (51%) attack!!!

Eclipse attack



Can you get free coffee?

Eclipse attack



World B will win!
With no miming power, I double spent a coin and got free coffee!

Eclipse attack

Attacking strategy:

1. Create a lot of IPs
2. Fill the peer table of a victim by flooding IP tables
3. Wait/Force the victim to drop its current connections due to
    1. Rebooting the system due to system update
    2. Network failures
    3. Power failures
    4. DoS attacks
    5. …
4. The victim will need to connect to new nodes selected from the peer table

As all peers in the peer table is controlled by the attacker, the victim is isolated.

Eclipse attack

This vulnerability is patched by Bitcoin!

Real-world attack is much more complicated and application specific:

1. How the peer table works
2. How to select new peers

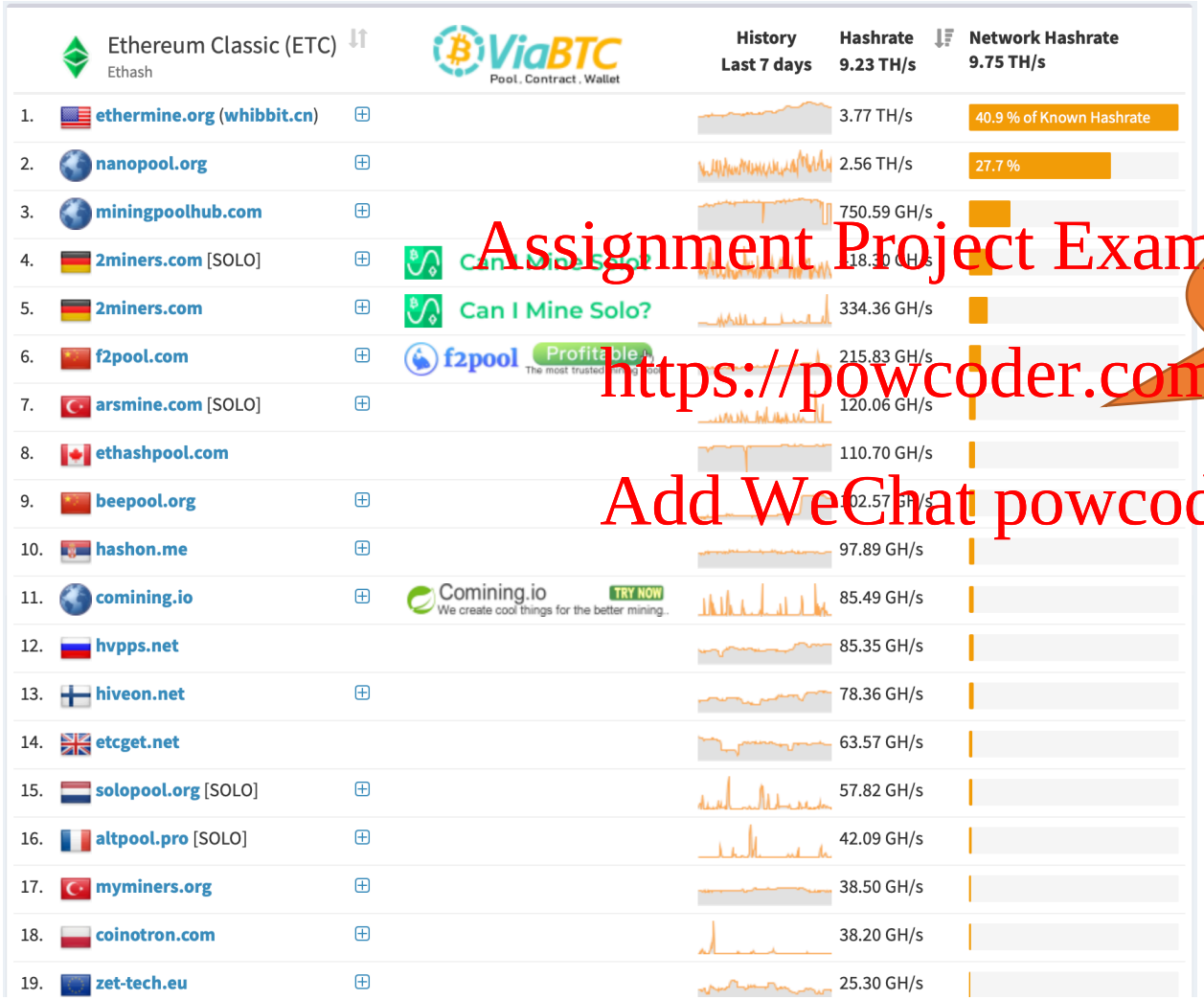
Possible fixes:

1. Anchor connections
2. Randomly select peers from the network

51% attack

How difficult is it to launch 51% attack?

Ethereum Classic



Ethereum Classic (ETC)
Ethash

ViaBTC
Pool. Contract. Wallet

		History Last 7 days	Hashrate 9.23 TH/s	Network Hashrate 9.75 TH/s
1.	ethermine.org (whibbit.cn)		3.77 TH/s	40.9 % of Known Hashrate
2.	nanopool.org		2.56 TH/s	27.7 %
3.	miningpoolhub.com		750.59 GH/s	
4.	2miners.com [SOLO]		118.30 GH/s	
5.	2miners.com		334.36 GH/s	
6.	f2pool.com		215.83 GH/s	
7.	arsmine.com [SOLO]		120.06 GH/s	
8.	ethashpool.com		110.70 GH/s	
9.	beepool.org		102.57 GH/s	
10.	hashon.me		97.89 GH/s	
11.	comining.io		85.49 GH/s	
12.	hvpps.net		85.35 GH/s	
13.	hiveon.net		78.36 GH/s	
14.	etcget.net		63.57 GH/s	
15.	solopool.org [SOLO]		57.82 GH/s	
16.	altpool.pro [SOLO]		42.09 GH/s	
17.	myminers.org		38.50 GH/s	
18.	coinotron.com		38.20 GH/s	
19.	zet-tech.eu		25.30 GH/s	

Can I Mine Solo?

f2pool Profitable!

Comining.io TRY NOW
We create cool things for the better mining.

Yay! No pool has >50% mining power!

https://miningpoolstats.stream/ethereumclassic

MONASH University

Question:

Can a pool of blockchain B has 51% mining power equivalent in blockchain A?

What about mining pools of other blockchains?

MONASH University

Conditions:

1. Mining power in blockchain B is compatible in blockchain A e.g. blockchain A and B share the same mining algorithm

2. Mining power in blockchain B might be less than 50%, but it will be more than 50% in blockchain A.

A mining pool in blockchain B has X unit of mining power, and the total mining power in blockchain A is Y unit.

The mining power of this mining pool in A will be: $\frac{X}{X+Y}$

51% attack: migrating mining power

Summary of the blockchains sharing the same hash algorithm

Type	Mining Algorithm	Coin	Rank	Hashrate (h/s)	Portion	Top Miners		
						#1	#2	#3
ASIC-resistant	Ethash	Ethreum (ETH)	3	1.42E+14	N/A	27.7%	22.2%	12.5%
		EthereumClassic (ETC)	18	8.62E+12	1647.4%	344.6%	305.7%	205.9%
	CryptoNight	Monero (XMR)	14	9.29E+08	N/A	37%	26%	12%
		ByteCoin (BCN)	38	3.35E+08	277.3%	102.6%	72.1%	33.3%
	Equihash	Zcash (ZEC)	20	3.36E+09	N/A	33.4%	19.2%	17.8%
		BitcoinGold (BTG)	26	3.17E+06	111111.1%	37111.1%	21333.3%	19777.8%
		Komodo (KMD)	55	4.48E+07	778.8%	451.3%	1443.6%	1338.3%
		Aion (AION)	84	7.22E+05	1000000.0%	334000.0%	192000.0%	178000.0%
ASIC-friendly	Sha256d	Bitcoin (BTC)	1	4.00E+19	N/A	23%	16.4%	11.6%
		BitcoinCash (BCH)	4	1.44E+18	2777.8%	638.8%	455.6%	322.2%
	Scrypt	Dogecoin (DOGE)	23	3.76E+14	N/A	18.0%	16.0%	10.0%
		Litecoin (LTC)	8	2.77E+14	135.7%	24.4%	21.7%	13.6%
	X11	Dash (DASH)	15	2.32E+15	N/A	13.0%	11.0%	11.0%
		WaltonChain (WTC)	73	1.14E+15	203.5%	26.5%	22.4%	22.4%

19/Feb/2019

Marketplace for mining power

Miners sell their hashing power; buyers purchase hashing power.

It's like eBay for blockchain mining!

Marketplace for mining power

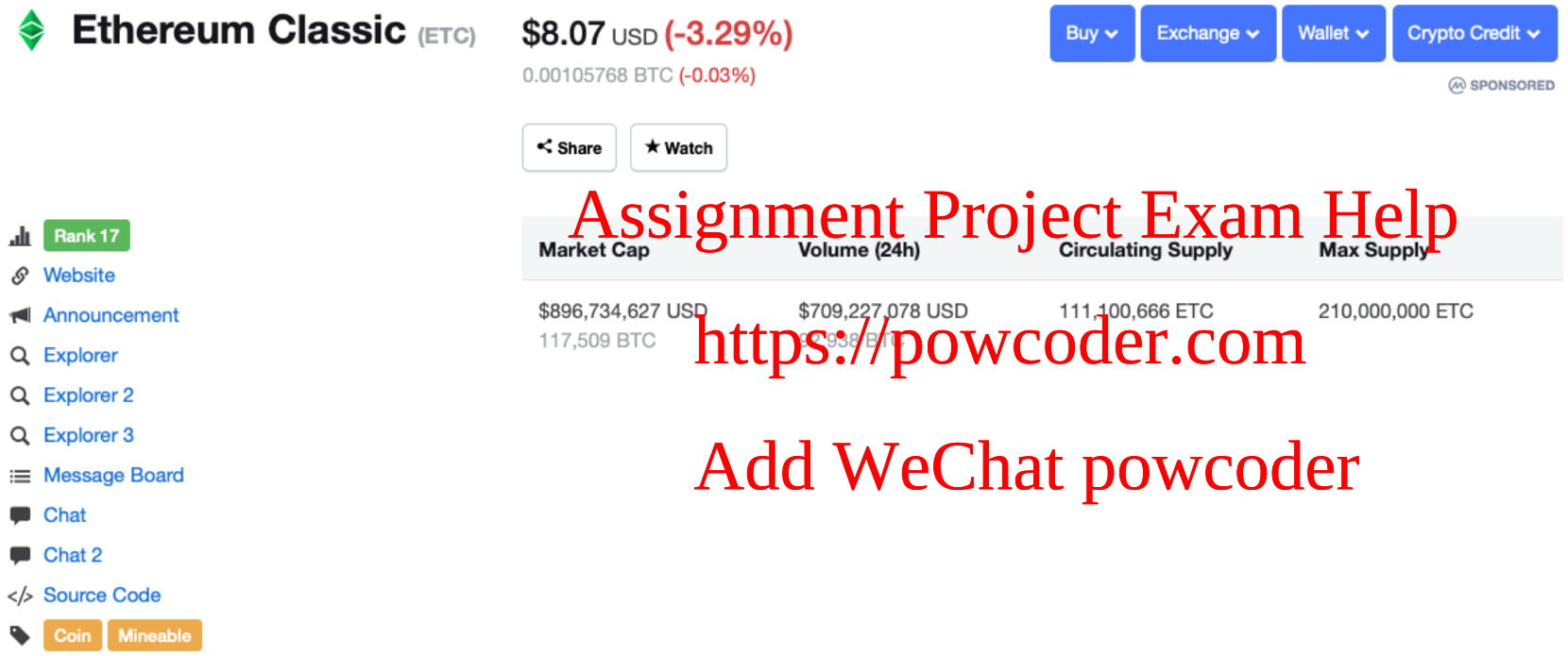
MONASH University

Some 51% attacks

- April 4, 2018: Verge (XVG) 51% attacked for a loss of ~$1.1 Million.
- May 14, 2018: Monacoin (MONA) 51% attacked for a loss of ~$90,000.
- May 22, 2018: Verge (XVG) 51% attacked again for a loss of ~$1.75 Million.
- May 29, 2018: Bitcoin Gold (BTG) 51% attacked for a loss of ~$18 Million.
- June 2, 2018: ZenCash (ZEN) 51% attacked for a loss of ~$550,000.
- June 4, 2018: Litecoin Cash (LCC) 51% attacked for unknown losses.
- September 8, 2018: FLO Blockchain (FLO) 51% attacked for a loss of ~$27,500.
- November 8, 2018: Aurum Coin (AU) 51% attacked for a loss of ~$500,000.
- December 2, 2018: Vertcoin (VTC) 51% attacked for a loss of ~$100,000.
- January 7, 2019: Ethereum Classic 51% attacked for a loss of ~$1.1 Million.
- …

Total loss: >$23 Million
Average loss: $2.5 Million/attack.

ETC Jan. 2019 attack



Ethereum Classic (ETC) is the first Ethereum still using the original blockchain, after hard forks.

ETC Jan. 2019 attack

What happened?

- 51% attacks on Ethereum Classic (ETC) in January 2019
- The attack lasted 4 hours
  (0:40am - 4:20am UTC, Jan. 7th, 2019)
- News reported that more than 1.1 million dollars were stolen
- $100,000 USD was returned

ETC Jan. 2019 attack

Attack detail:

- 12 transactions were successfully double-spent
- The source of the mining power for this attack remains uncertain, but NiceHash cloud mining platform is highly suspected;

  One day before the attack, an anonymous person rents all available Ethash (the hash algorithm used by ETH and ETC) mining power from NiceHash

Renting mining power attack?

> Ethereum's hashrate has also dropped, but less dramatically, and now stands at roughly 22 times ETC's. That is itself a major problem for Classic: Because ETC uses the same mining algorithm as Ethereum, attackers can temporarily rent existing Ethereum mining equipment, making it much easier to mount a takeover attack than if attackers had to buy equipment specific to the ETC chain. The cloud mining service NiceHash has been increasingly cited as a factor in that sort of attack, to the point that the site Crypto51 treats the degree to which a chain is "NiceHash-able" as one measure of its overall vulnerability to 51 percent attack. It's not yet clear if NiceHash or other cloud mining played a role in the Ethereum Classic attack, but it seems highly likely.

https://breakermag.com/the-ethereum-classic-51-attack-is-the-height-of-crypto-irony/

Next week: Class Test/Alternatives to PoW