

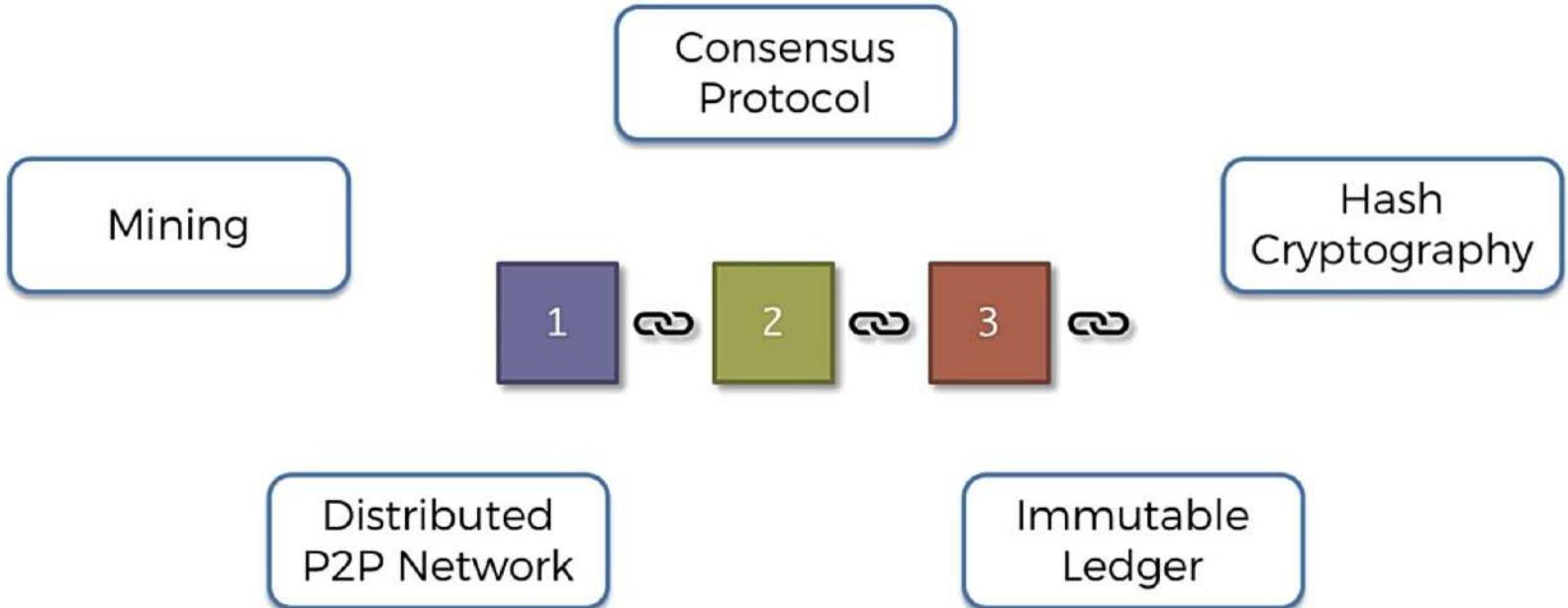


# Module 2: Consensus & Mining

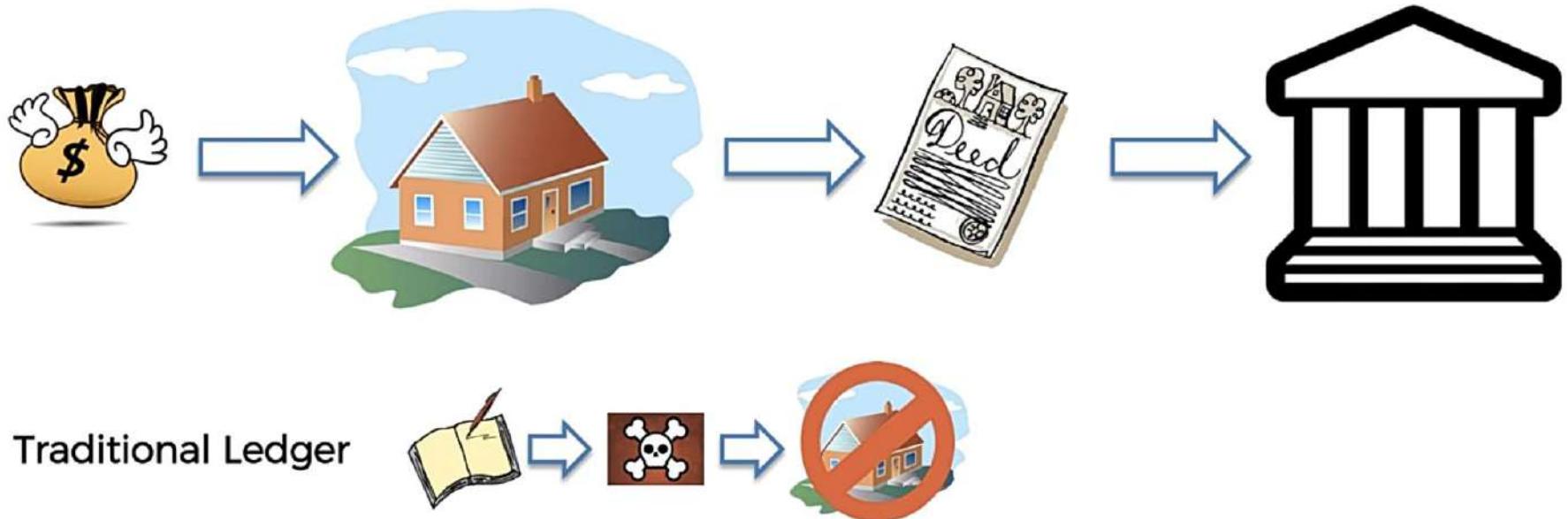
# Agenda

- Decentralized Consensus
- Byzantine Generals Problem
- Independent Verification of Transactions
- Mining Nodes
- Aggregating Transactions into Blocks
- Constructing Block Header
- Mining the Block
- Successful Mining of Block
- Validating a new Block
- Assembling and Selecting Chains of Blocks
- Blockchain Forks

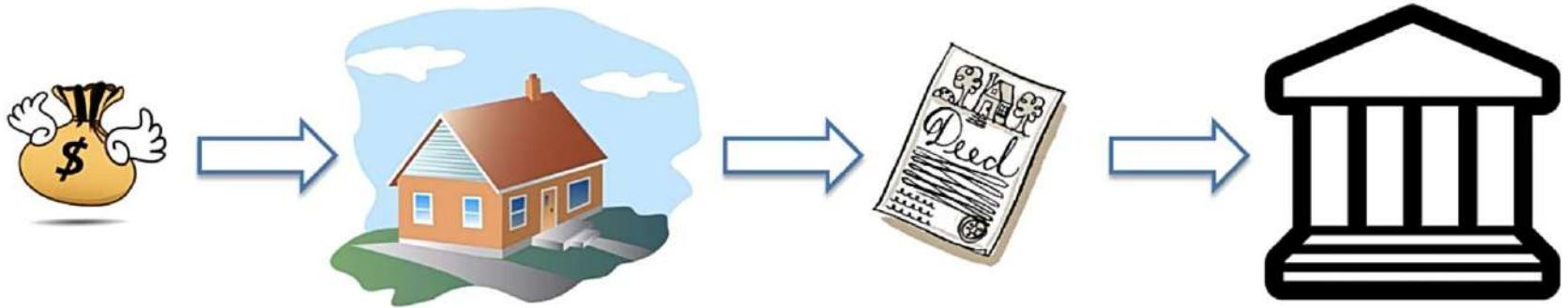
# Blockchain



# Immutable Ledger



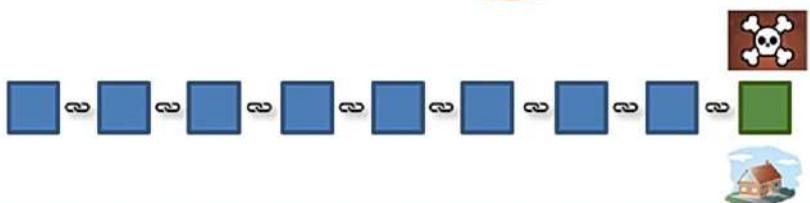
# Immutable Ledger



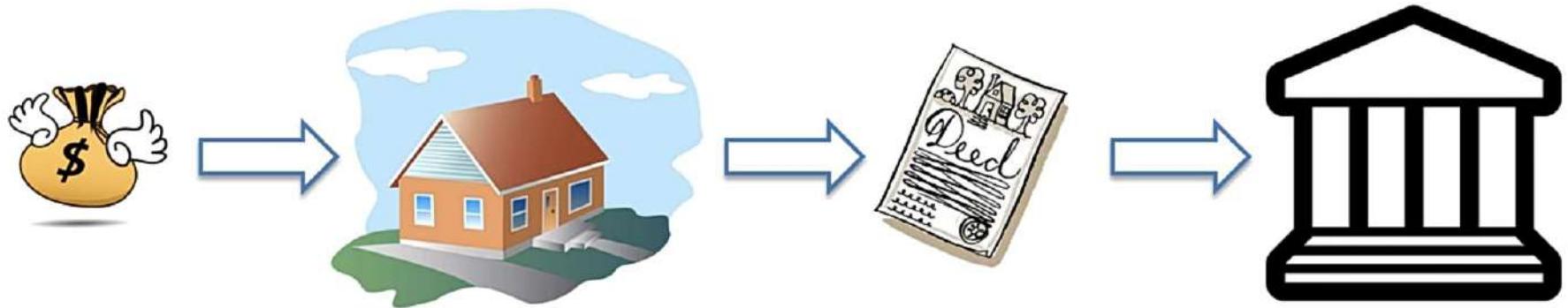
Traditional Ledger



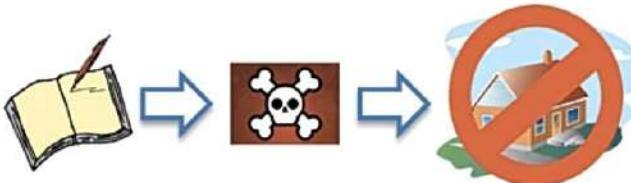
Blockchain



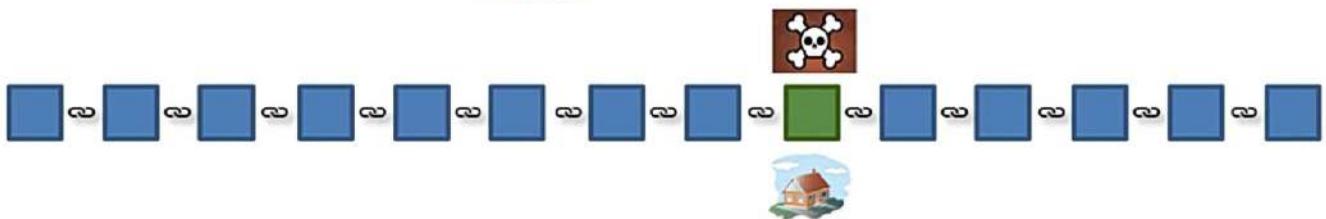
# Immutable Ledger



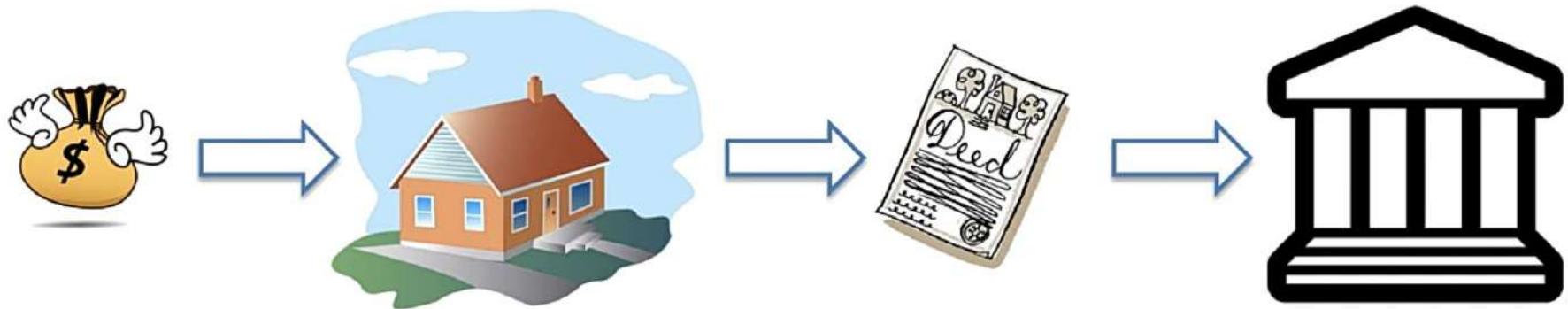
Traditional Ledger



Blockchain



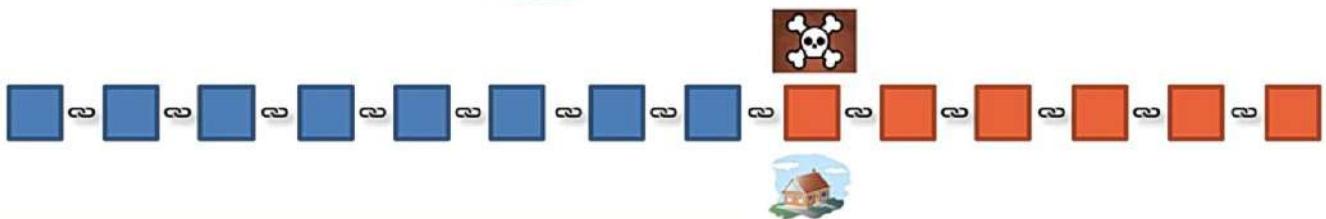
# Immutable Ledger



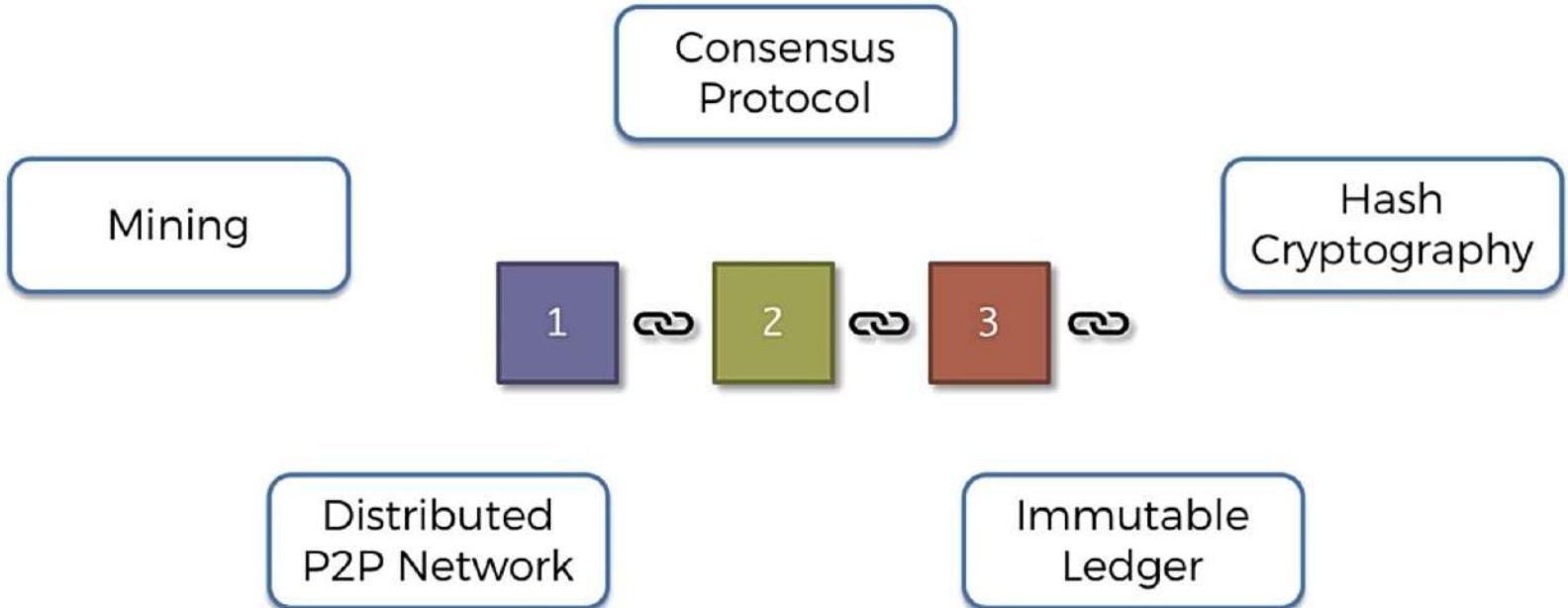
Traditional Ledger



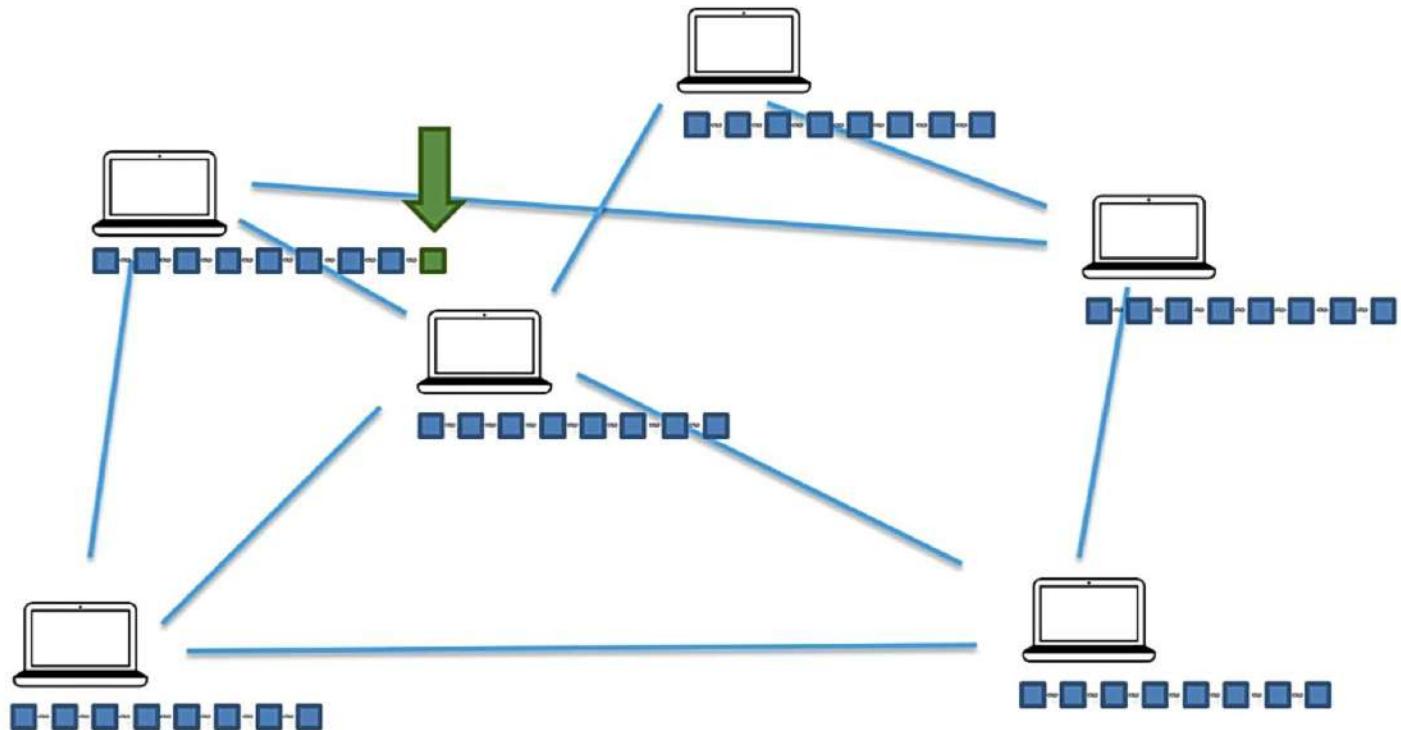
Blockchain



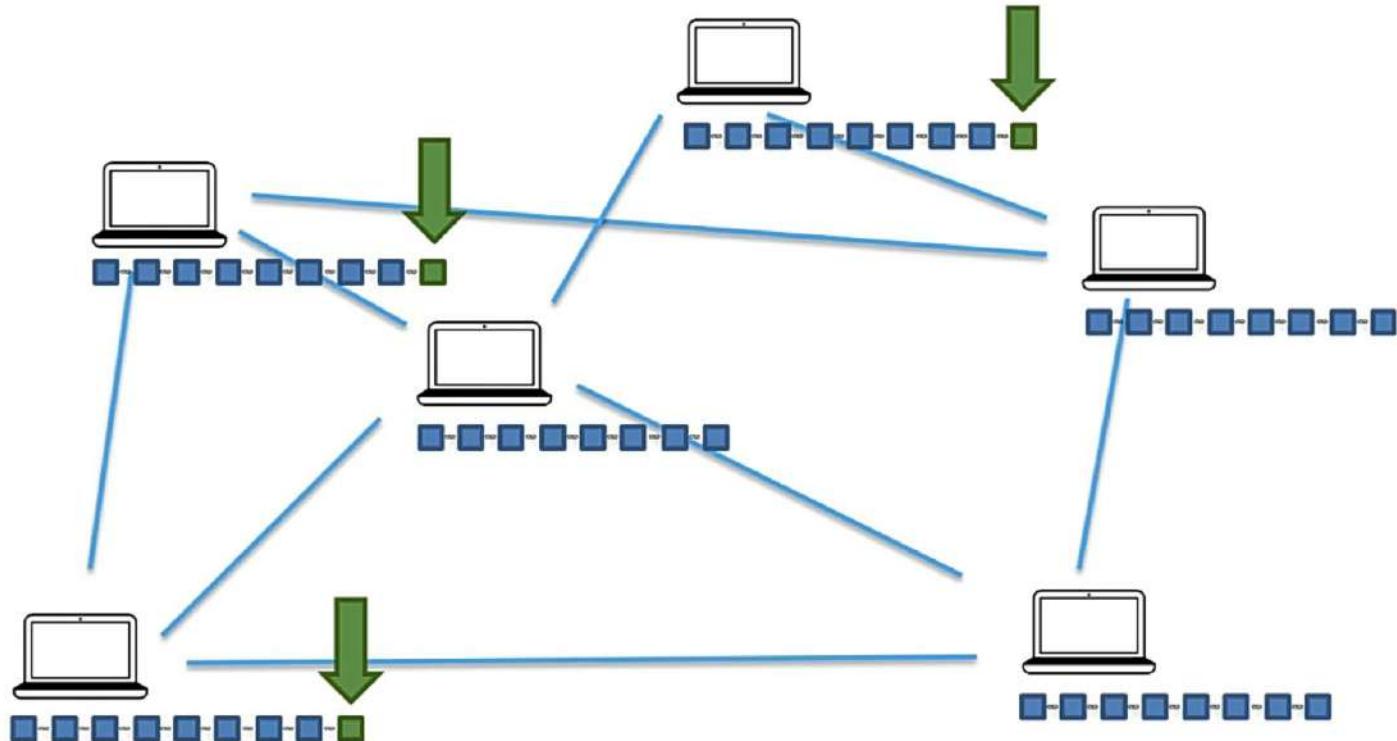
# Blockchain



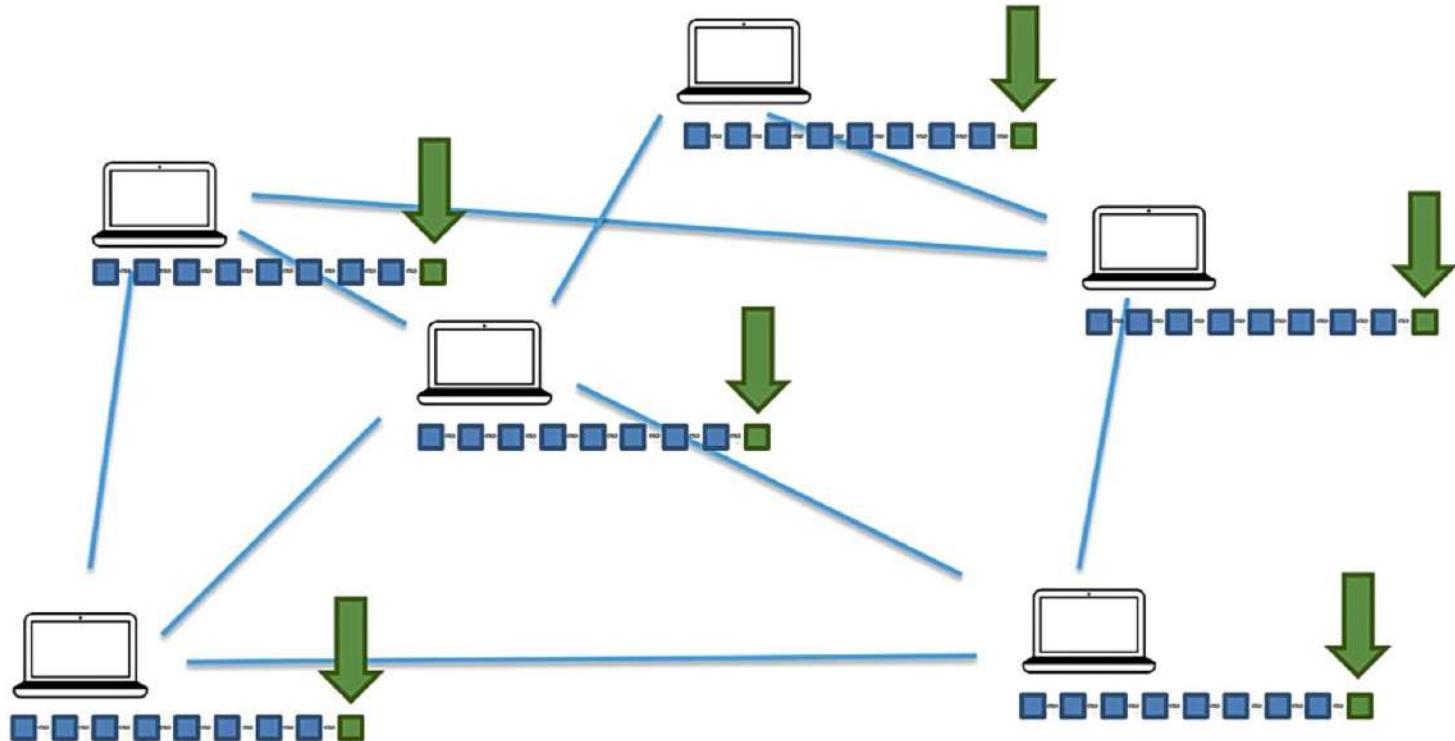
# Distributed P2P Network



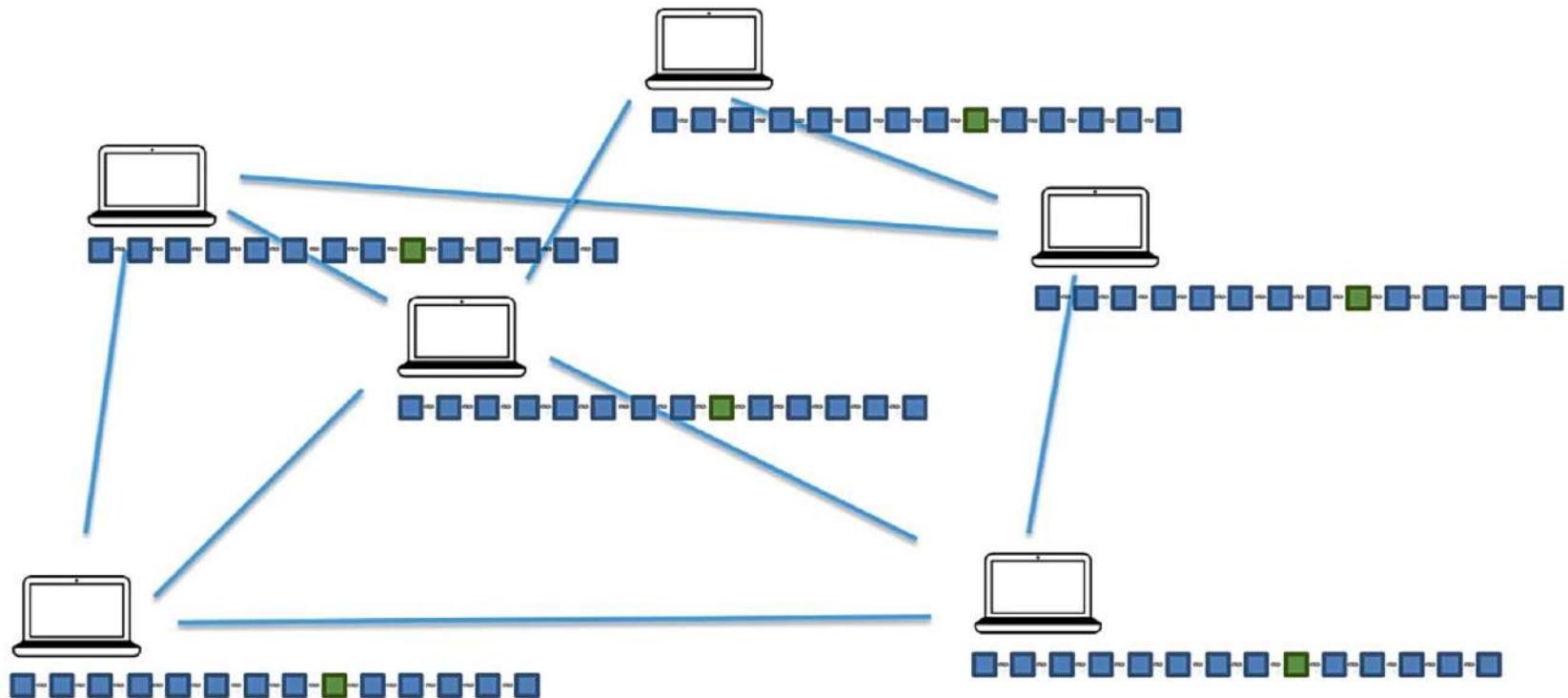
# Distributed P2P Network



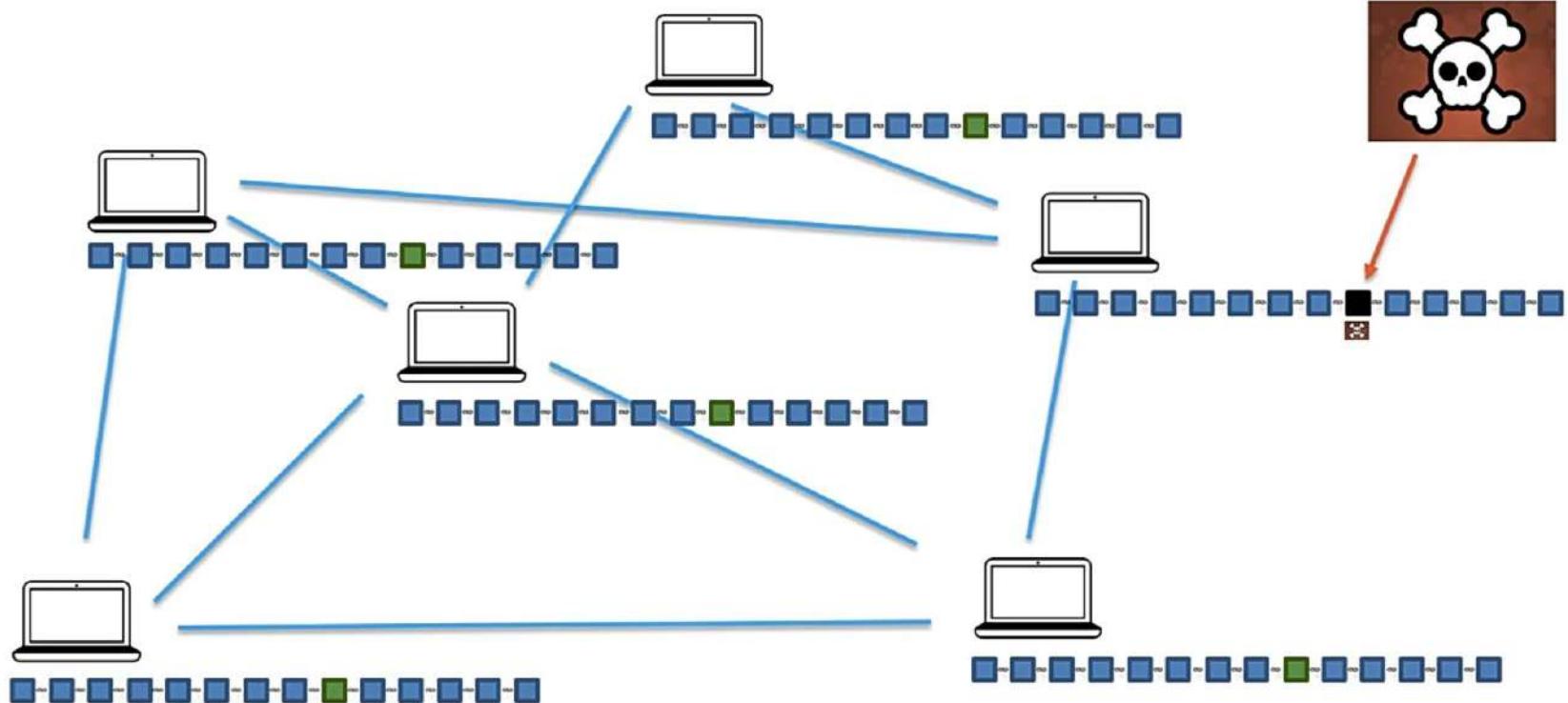
# Distributed P2P Network



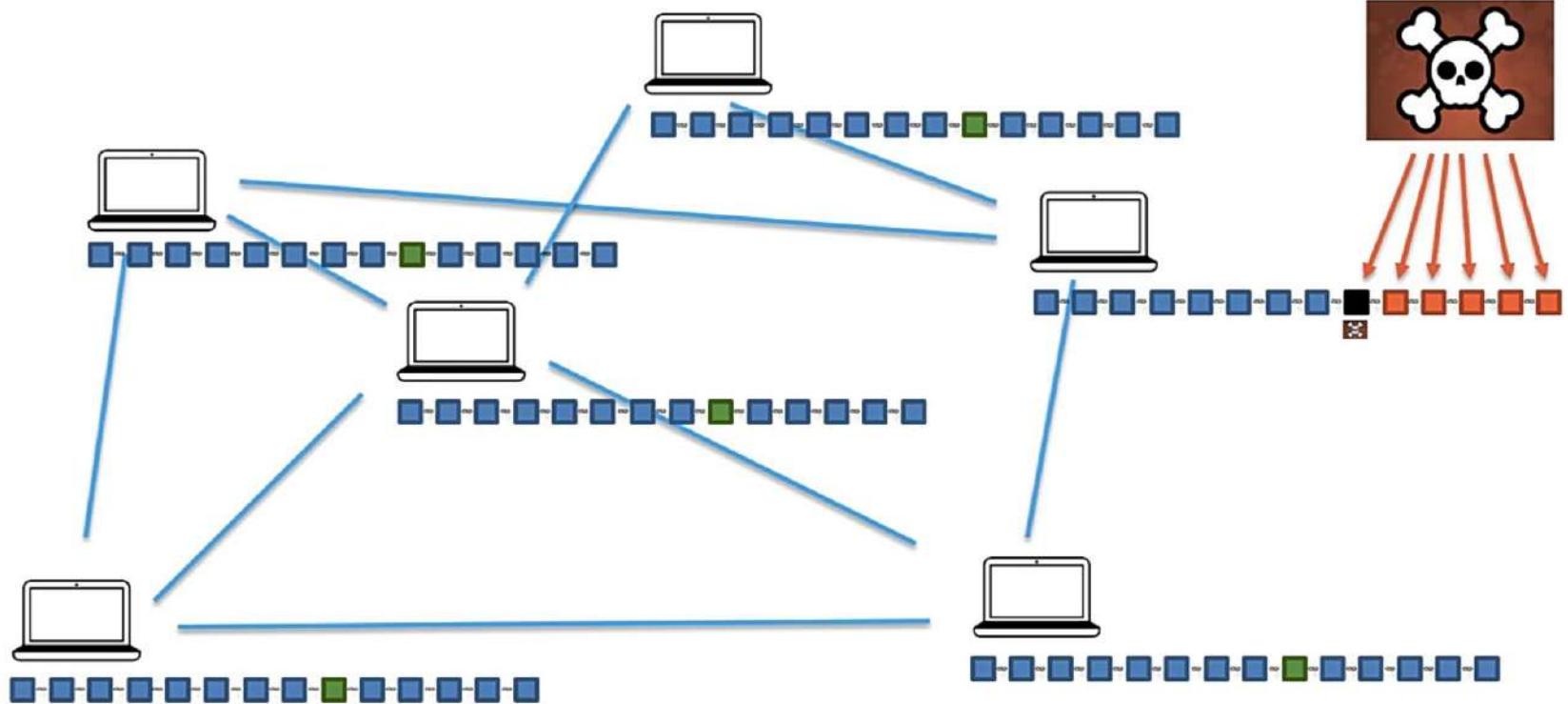
# Distributed P2P Network



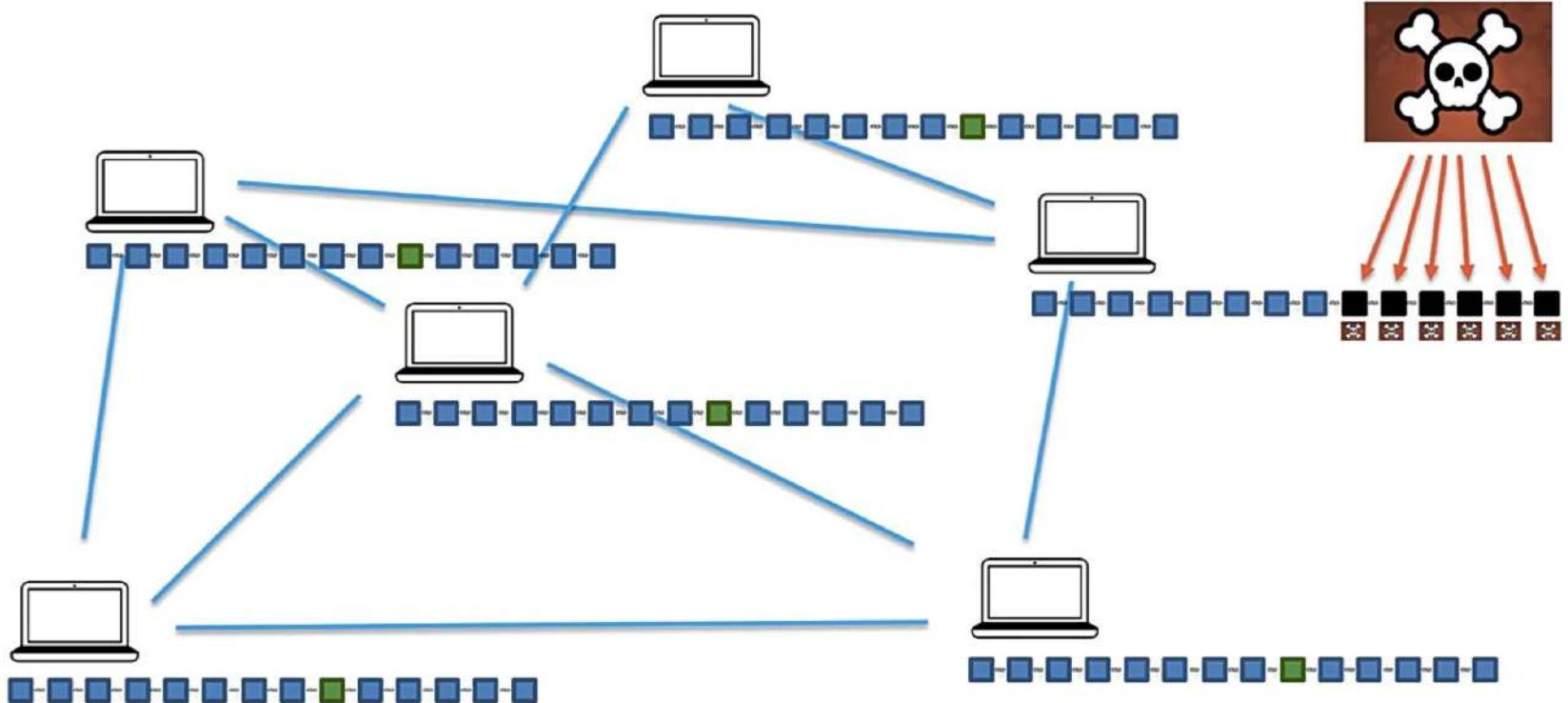
# Distributed P2P Network



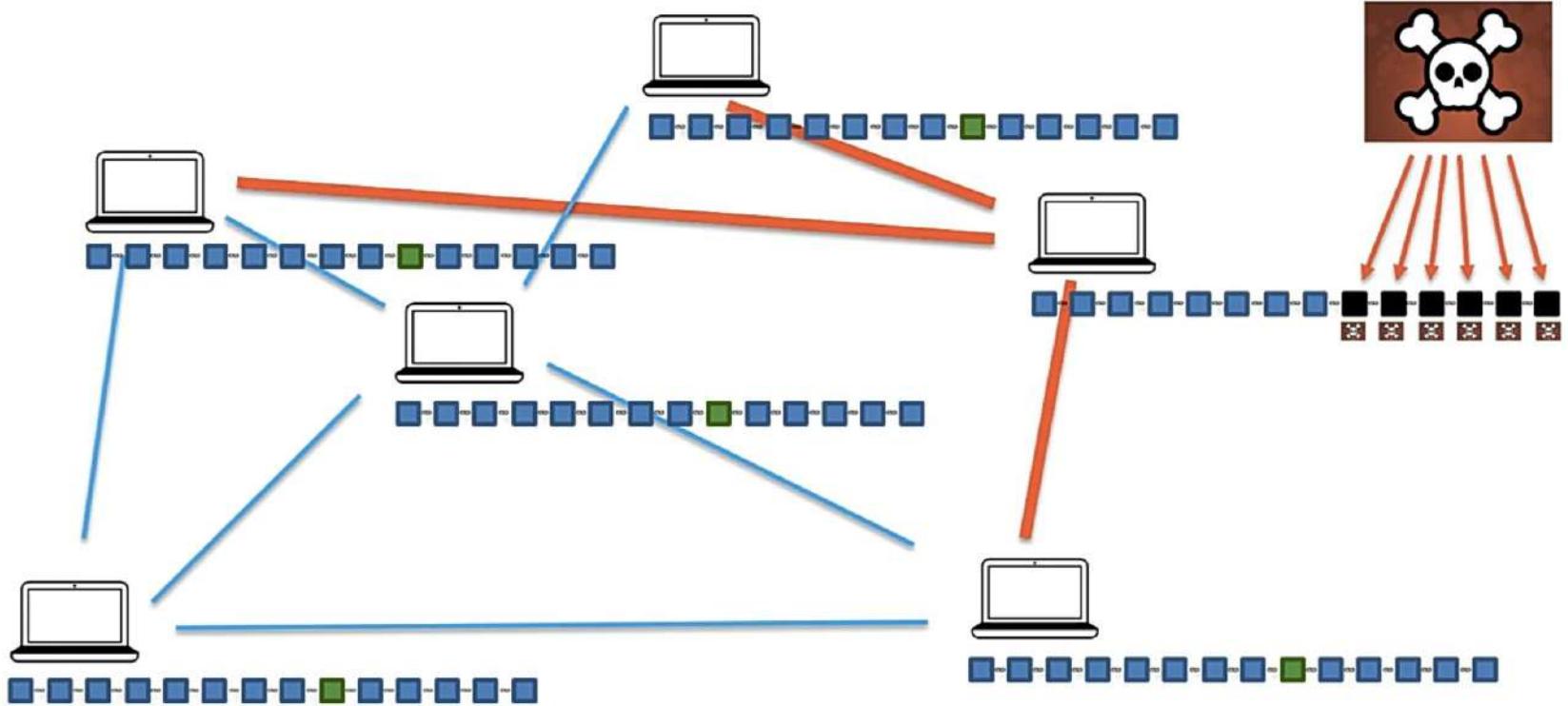
# Distributed P2P Network



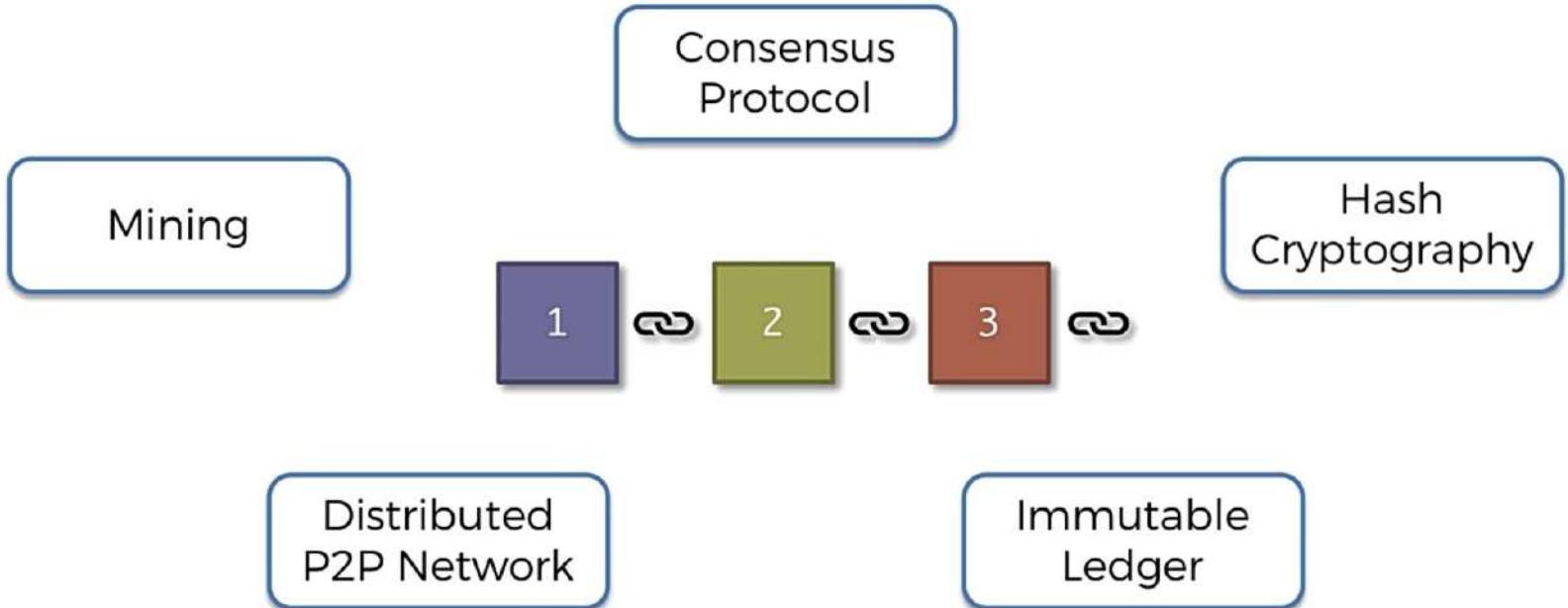
# Distributed P2P Network



# Distributed P2P Network



# Blockchain



# How Mining Works ?



Block: #3

Data:

Kirill -> Hadelin 500 hadcoins

Kirill -> Ebay 100 hadcoins

Hadelin -> Joe 70 hadcoins



# How Mining Works ?



# How Mining Works ?



Block: #3

Data:

Kirill -> Hadelin 500 hadcoins

Kirill -> Ebay 100 hadcoins

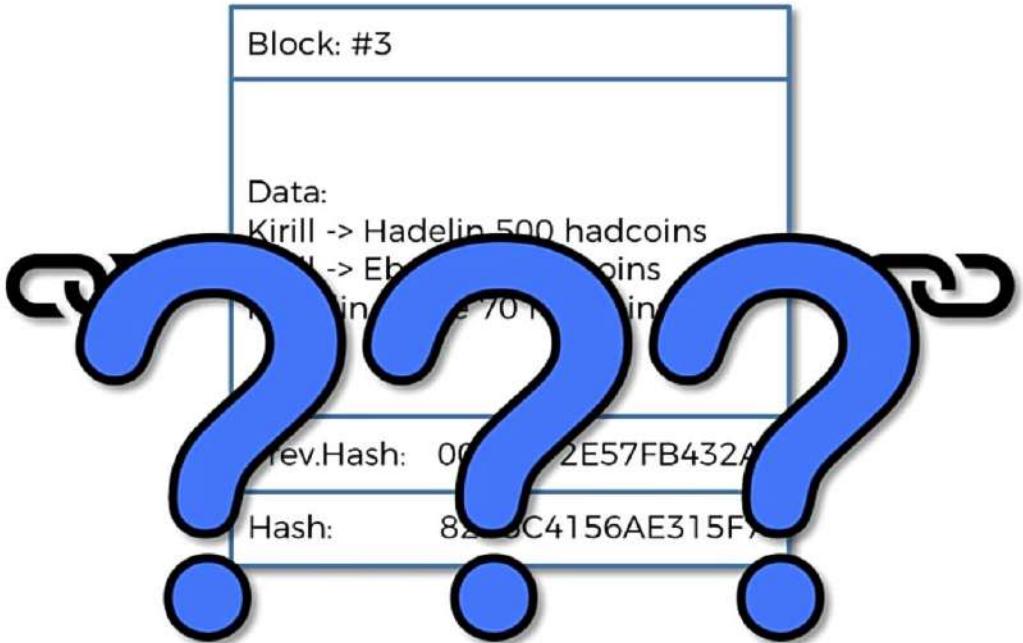
Hadelin -> Joe 70 hadcoins



Prev.Hash: 0000DF2E57FB432A

Hash: 82B5C4156AE315F7

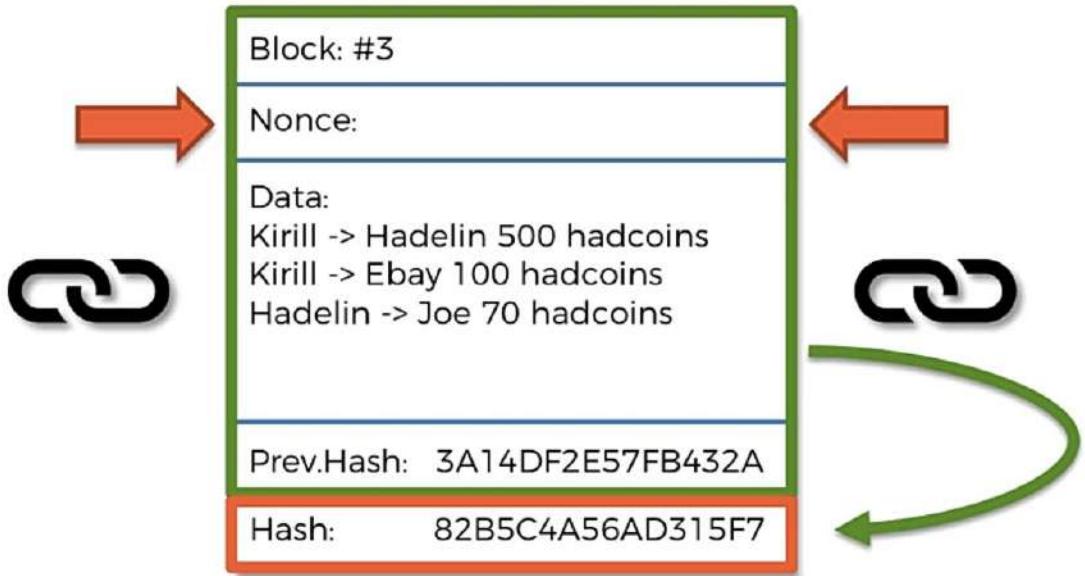
# How Mining Works ?



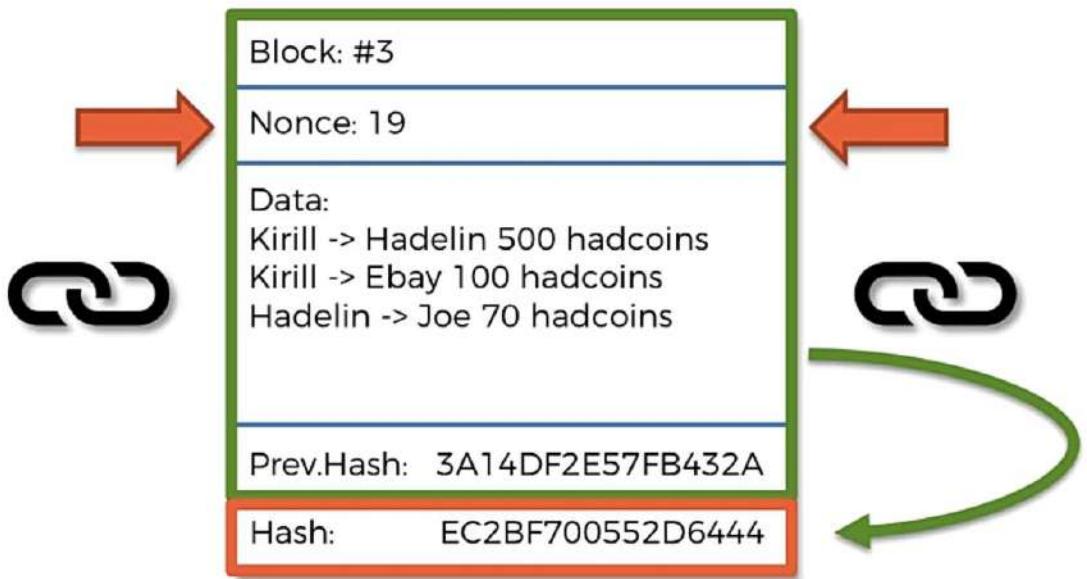
# How Mining Works ?



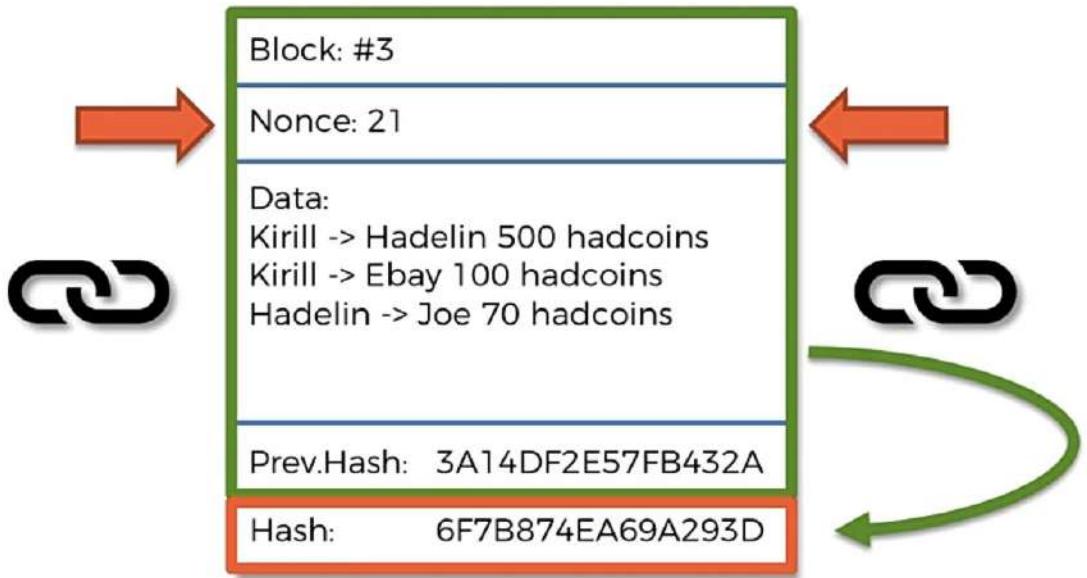
# How Mining Works ?



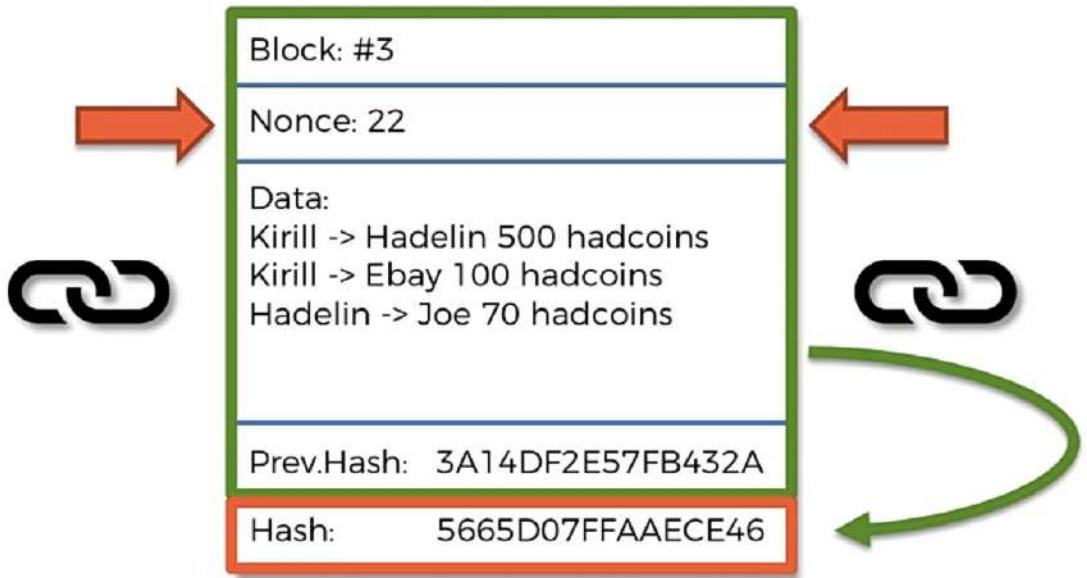
# How Mining Works ?



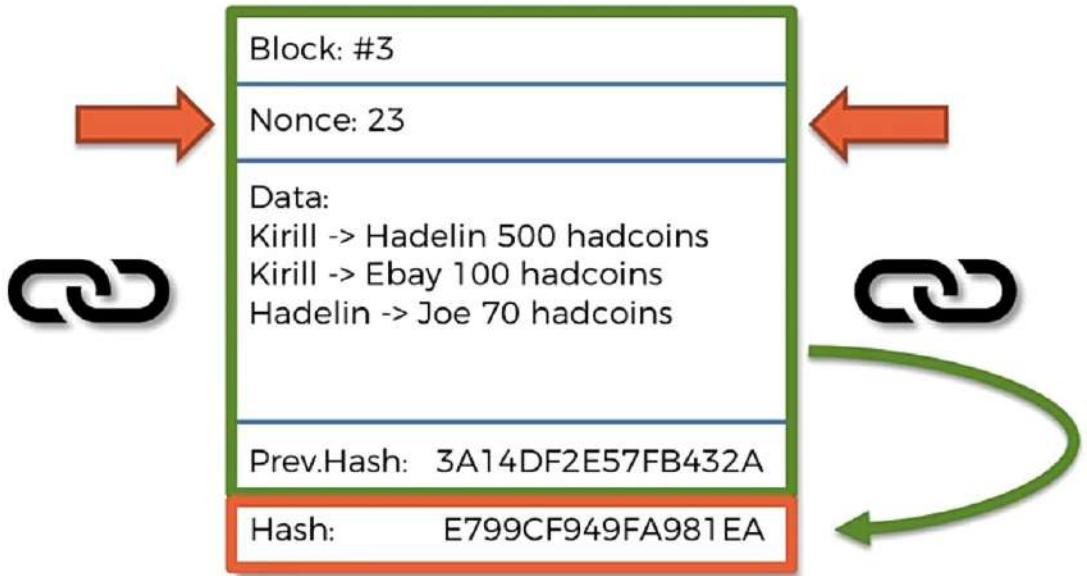
# How Mining Works ?



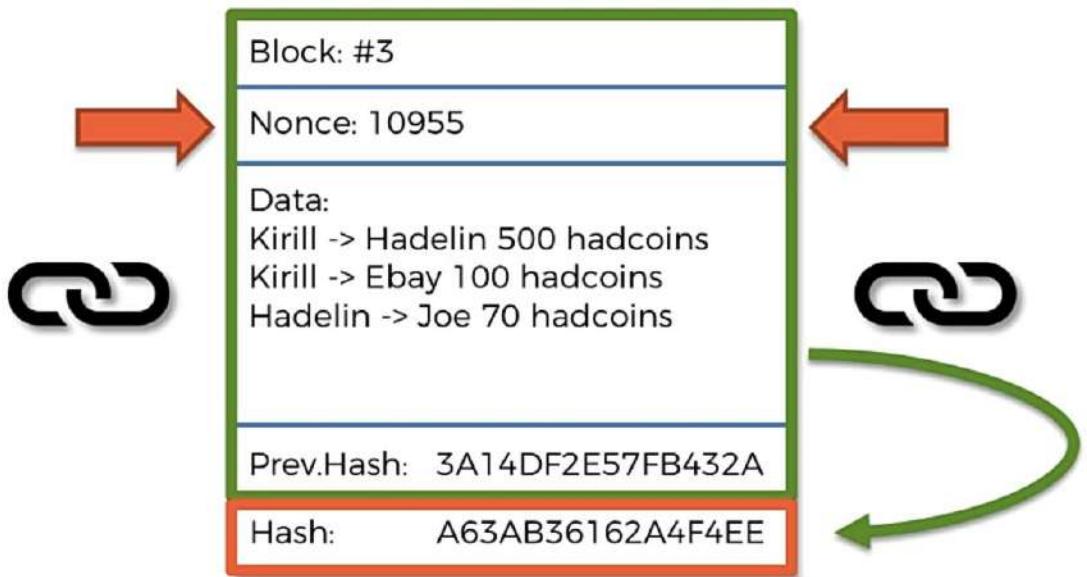
# How Mining Works ?



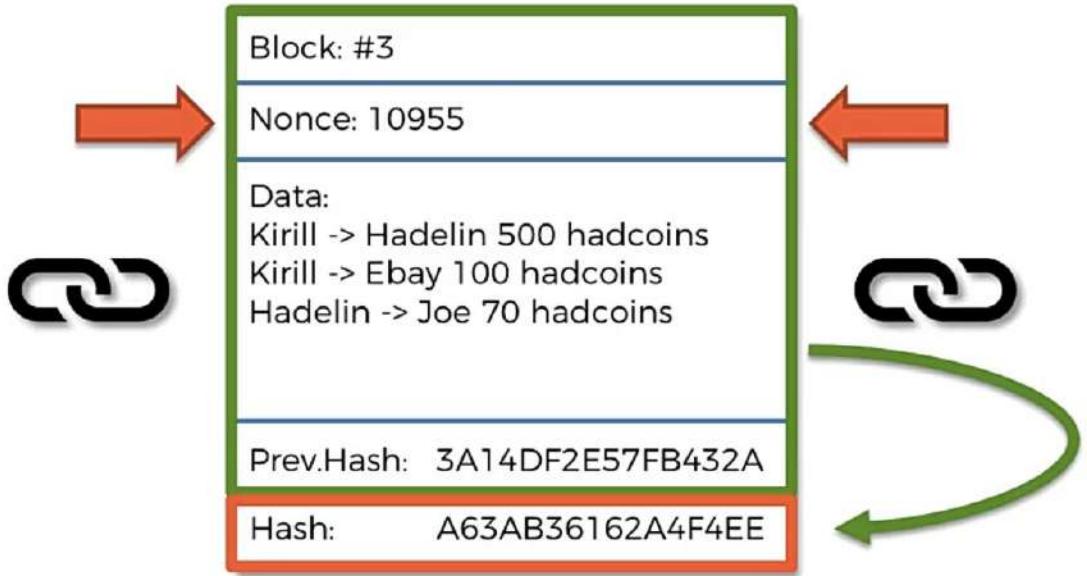
# How Mining Works ?



# How Mining Works ?



# How Mining Works ?



# How Mining Works ?

## A Hash is a Number

18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68  
=11232962686236154915841062771303455665105266333  
445130312258268457057784990824

# How Mining Works ?

## A Hash is a Number

18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68  
=11232962686236154915841062771303455665105266333  
445130312258268457057784990824

0000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923  
=00000000000000218420711603109937116824492054445  
852323869008912526075378993443

000159CAA4B1EDA0FED66CB5E915C8F  
=000438  
342898295709947707018187988111

# How Mining Works ?

- ALL POSSIBLE HASHES -

A Hash is a Number

18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

=11232962686236154915841062771303455665105266333  
445130312258268457057784990824

0000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

=000000000000000218420711603109937116824492054445  
852323869008912526075378993443

00159CAA4B1EDA0FED66CB5E915C8F

=00438  
342898295709947707018187988111

LARGEST

SMALLEST

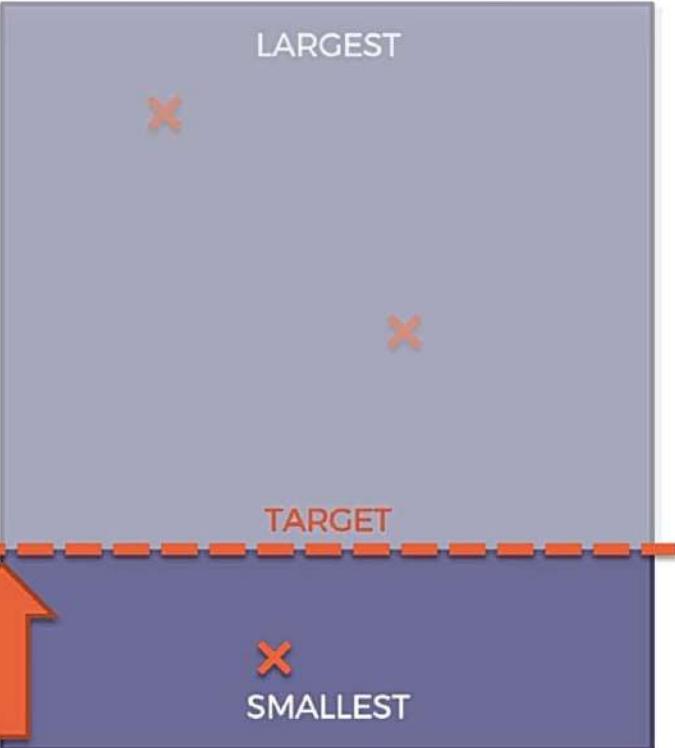
# How Mining Works ?

18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

0000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

000159CAA4B1EDA0FED66CB5E915C8F

- ALL POSSIBLE HASHES -



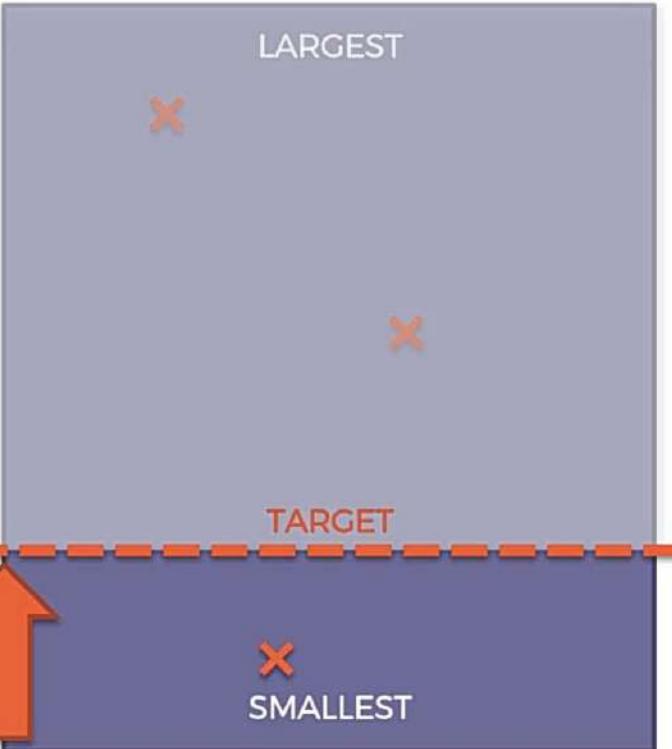
# How Mining Works ?

- ALL POSSIBLE HASHES -

✗ 18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

✗ 00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

✓ 000159CAA4B1EDA0FED66CB5E915C8F



# How Mining Works ?

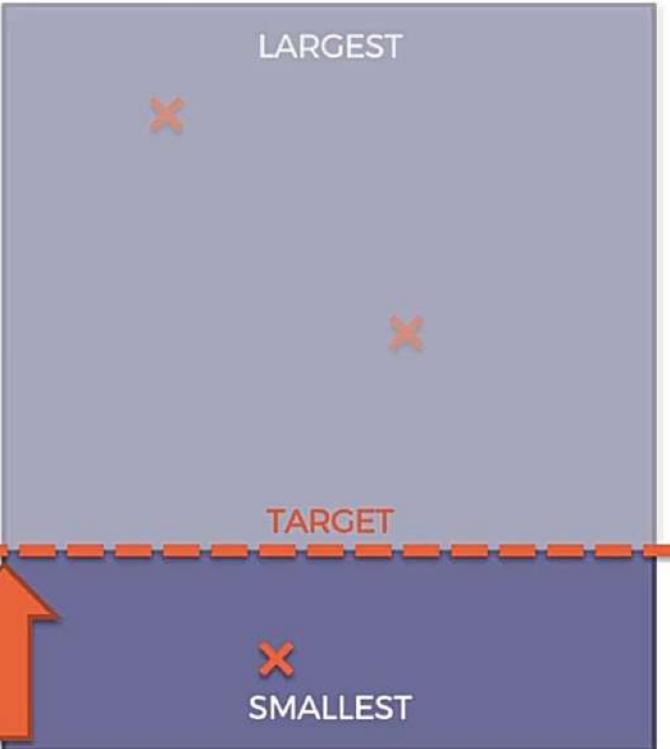
X 18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

X 0000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

✓ 00159CAA4B1EDA0FED66CB5E915C8F

TIP: Express Target with leading Zeros  
E.g. '0000'

- ALL POSSIBLE HASHES -

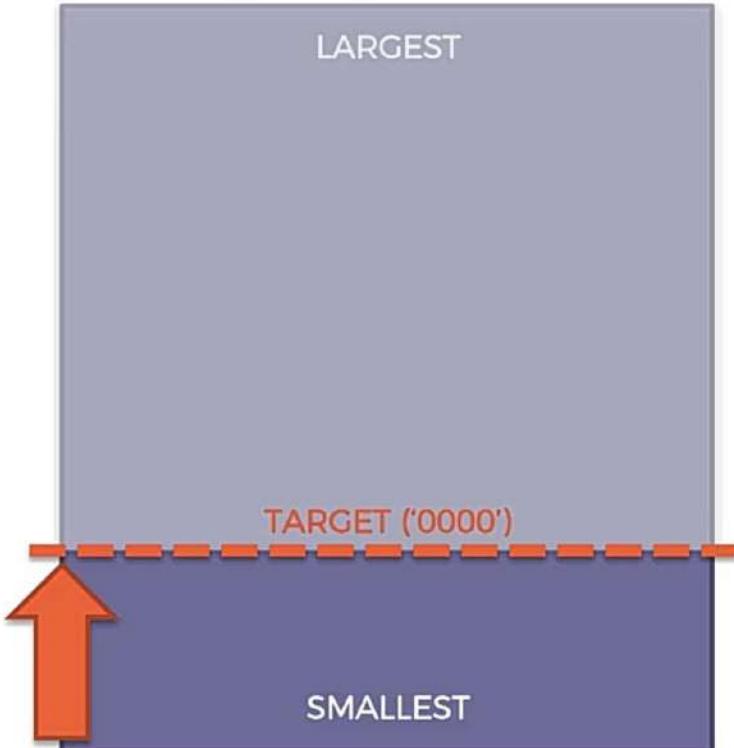


# How Mining Works ?

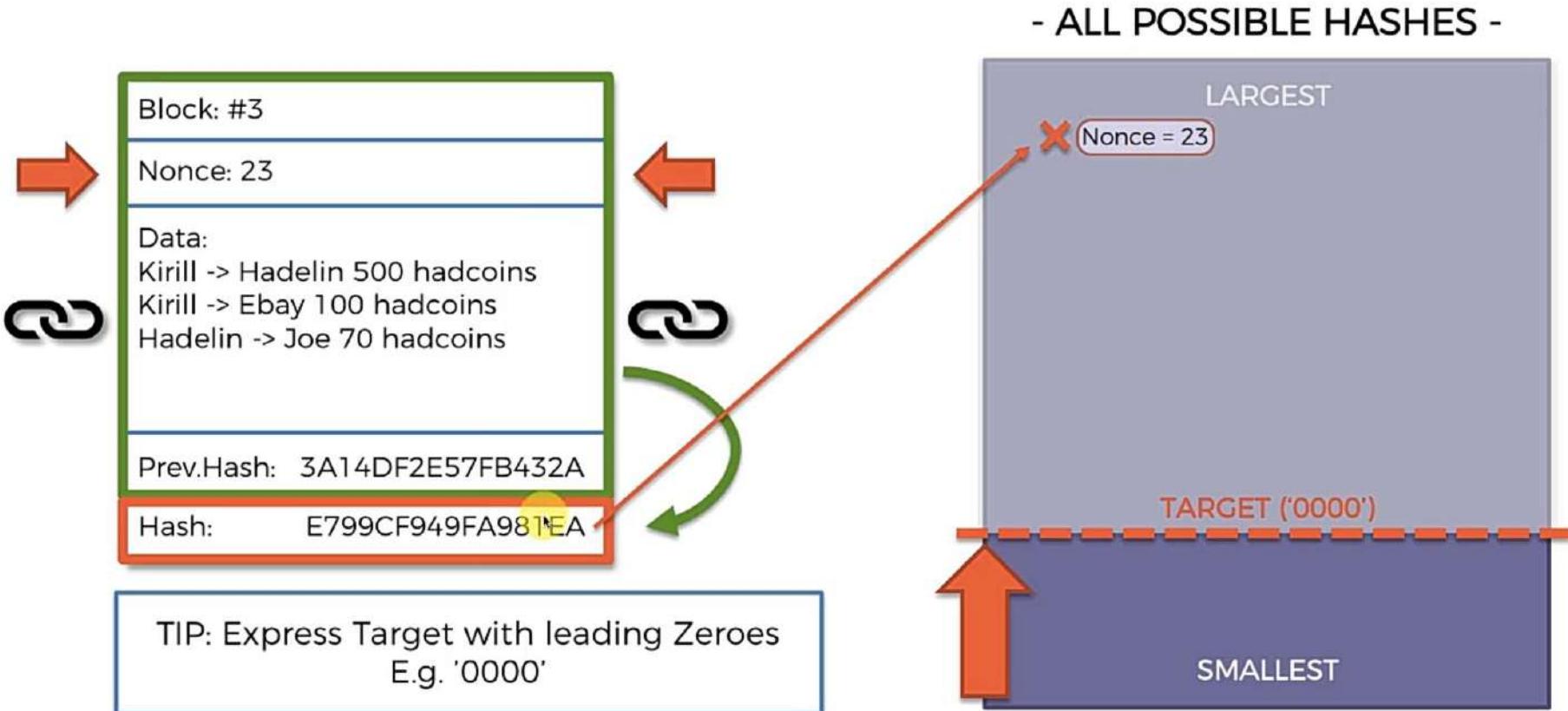


TIP: Express Target with leading Zeroes  
E.g. '0000'

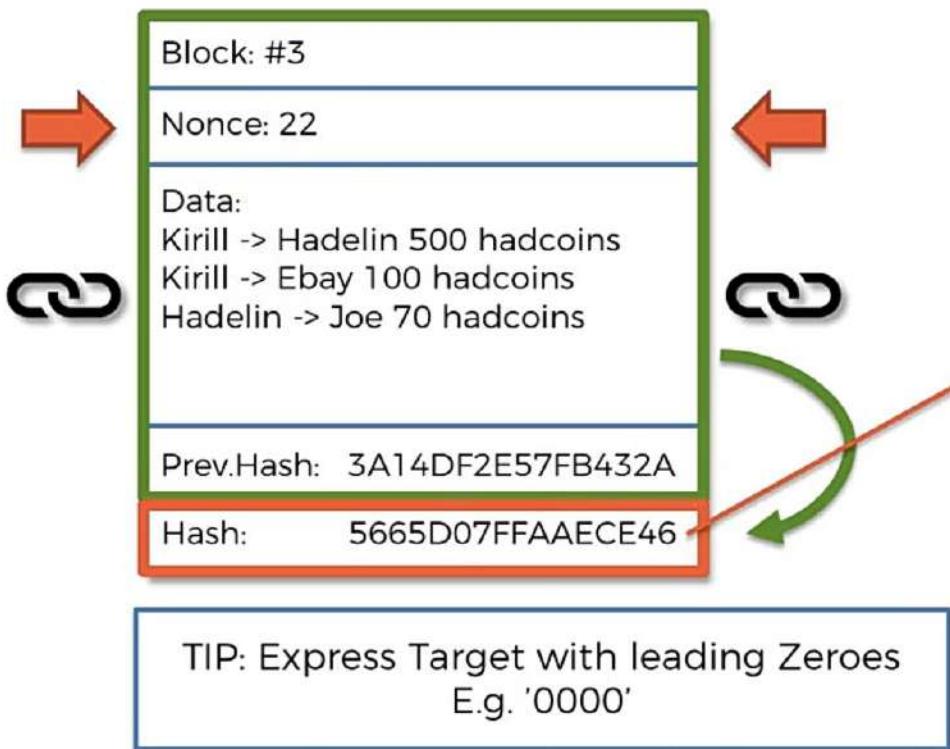
- ALL POSSIBLE HASHES -



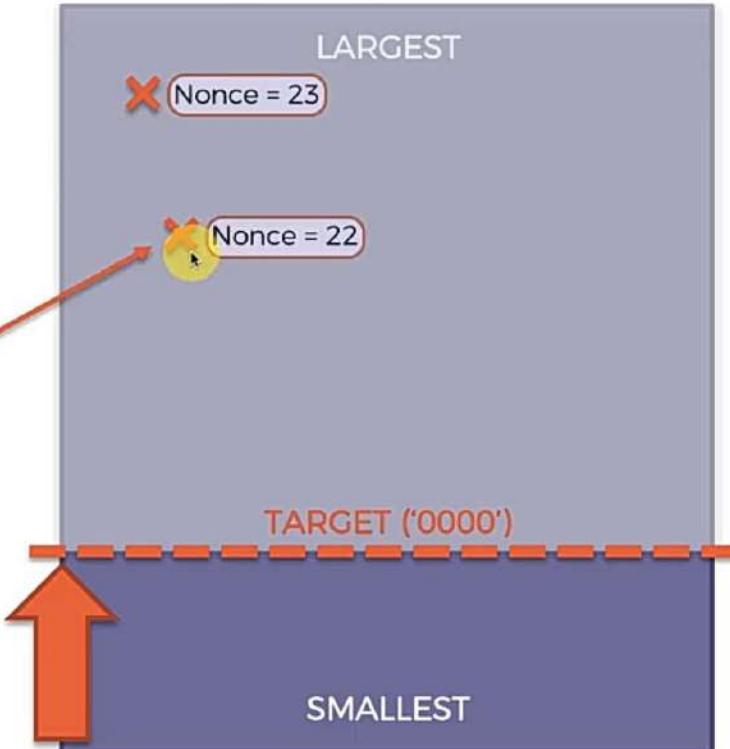
# How Mining Works ?



# How Mining Works ?

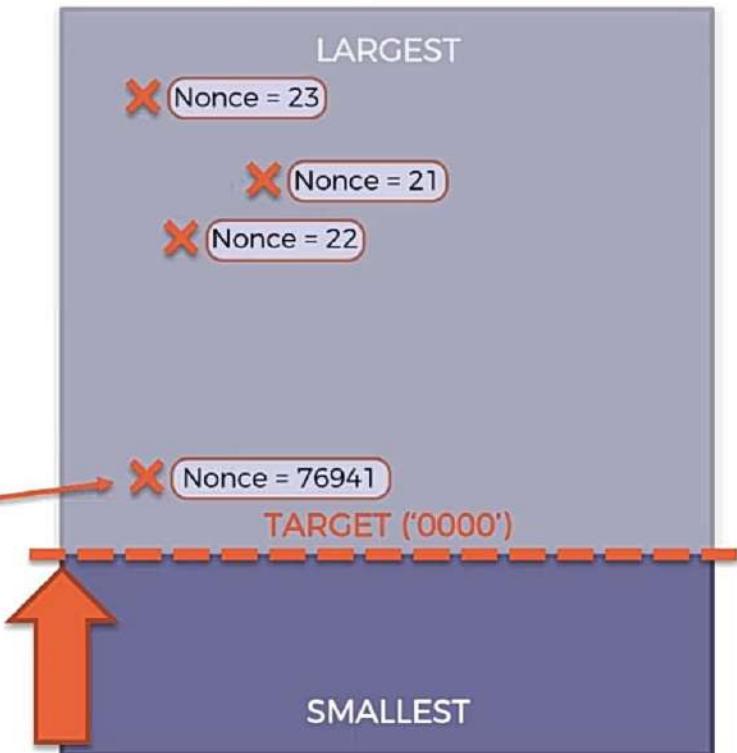
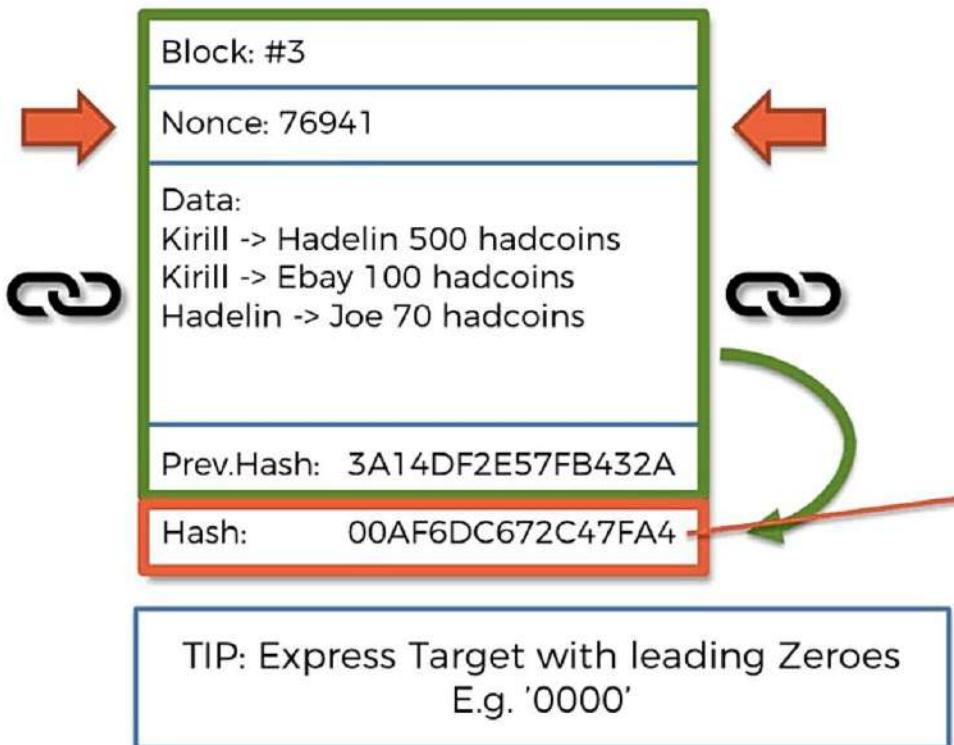


- ALL POSSIBLE HASHES -

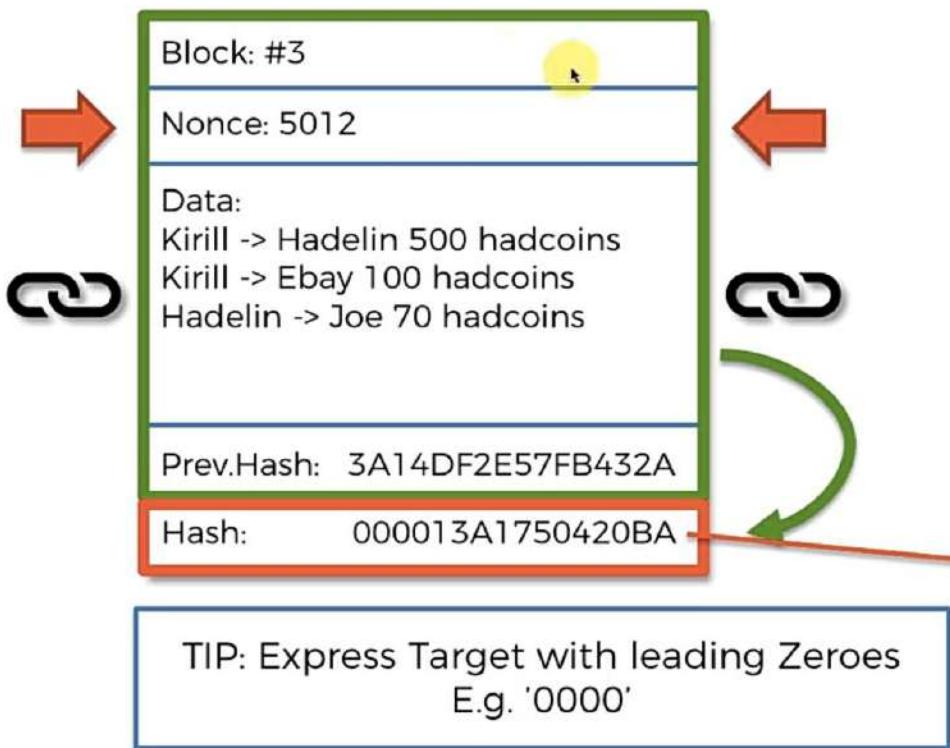


# How Mining Works ?

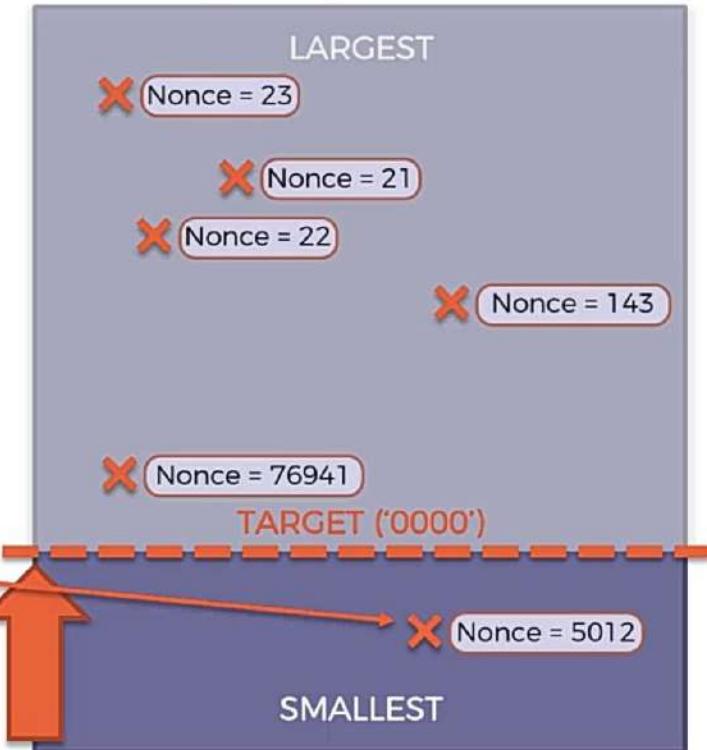
- ALL POSSIBLE HASHES -



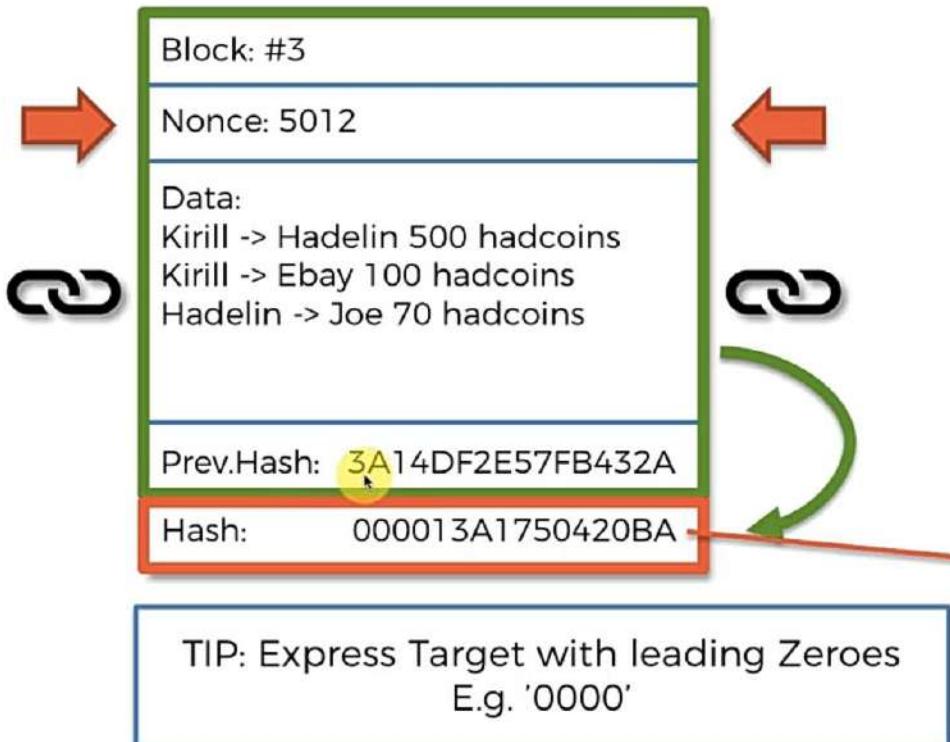
# How Mining Works ?



- ALL POSSIBLE HASHES -



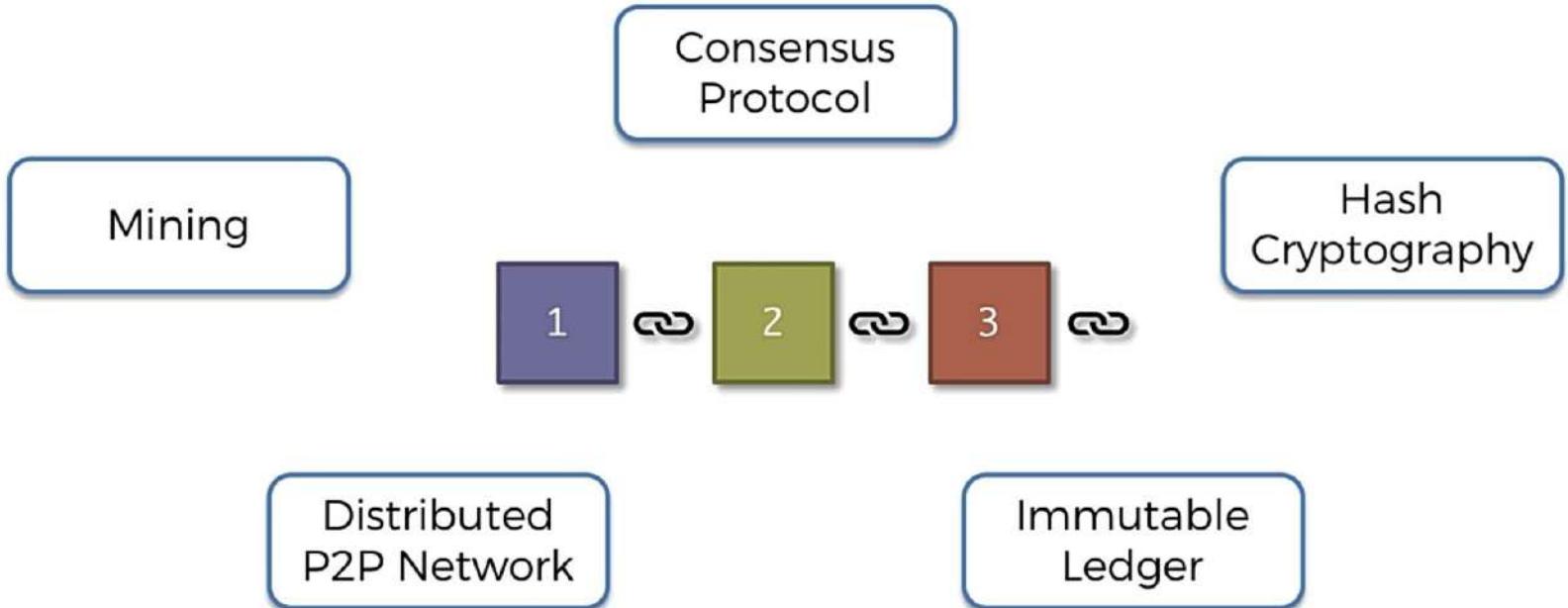
# How Mining Works ?



- ALL POSSIBLE HASHES -



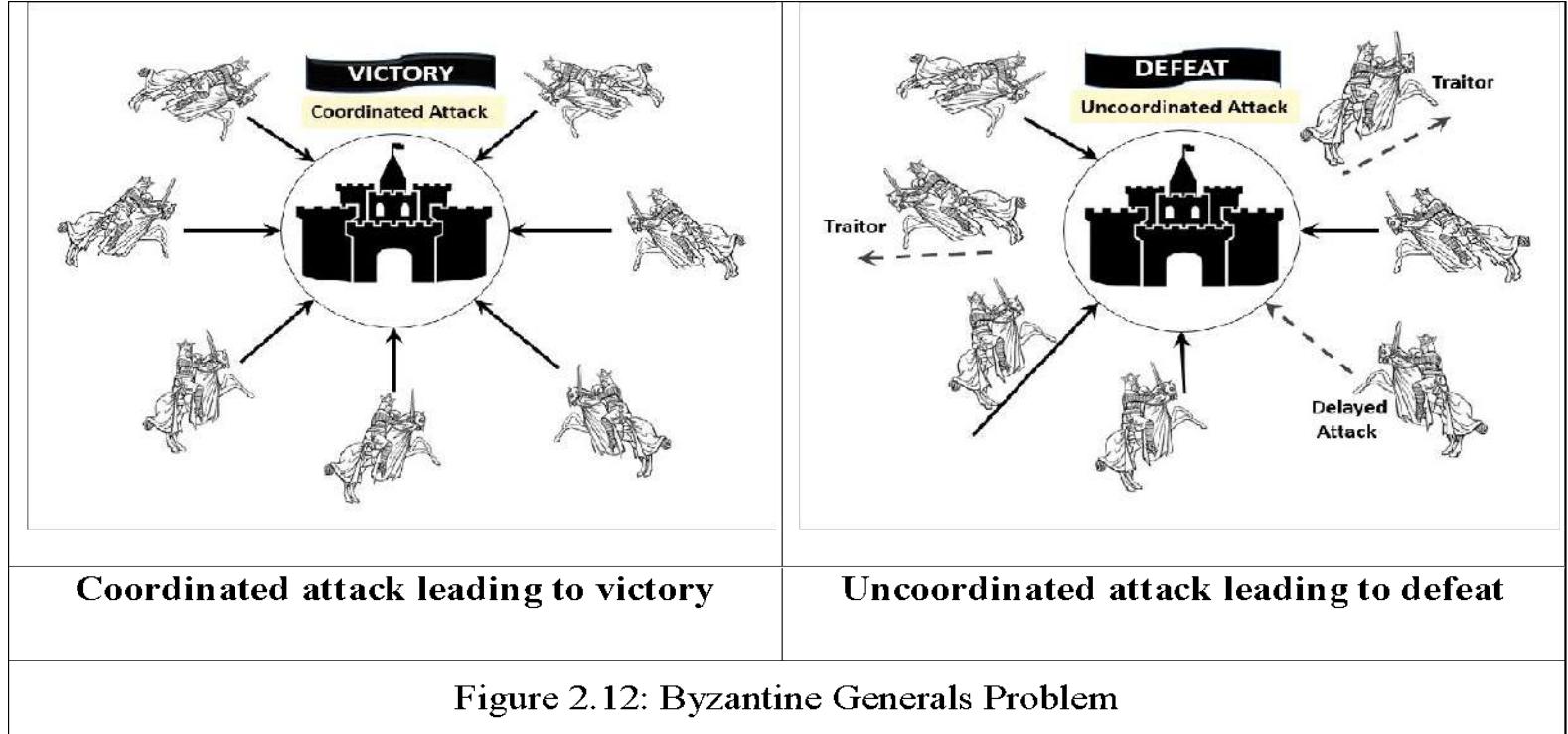
# Blockchain



# What is Consensus?

- As per Webster dictionary, a consensus is a **general agreement or opinion shared by all the people in a group.**
- A protocol is a **system of standard rules that are acceptable by all parties** to control the exchange of information in a network. Thus, a **consensus protocol** in Blockchain can be defined as **a set of rules and procedures for attaining a unified agreement (consensus) between the participating nodes** on the status of the network.
- The consensus protocol **aims to overcome the classic problem of a distributed computing system known as the Byzantine Generals Problem**

# Byzantine General Problem



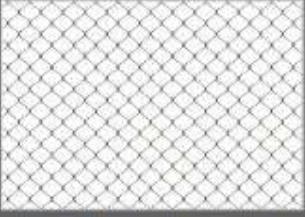
# Objectives of Consensus Protocol

1



Unified  
Agreement

2



Fault Tolerant

3



Collaborative  
and Participatory

4



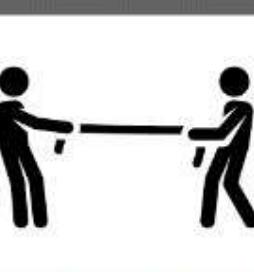
Egalitarian

5



Incentivisation

6



Prevent Double-Spend

# Byzantine Fault Tolerance



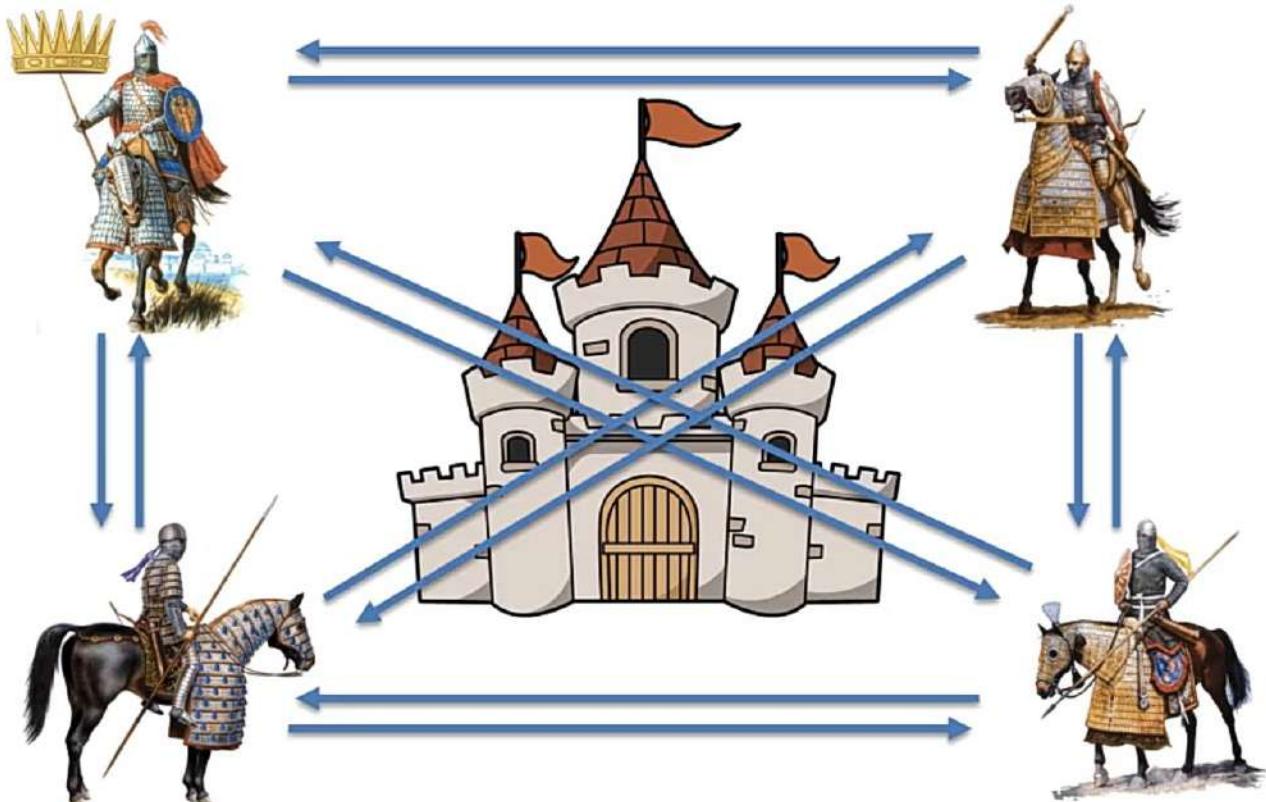
# Byzantine Fault Tolerance



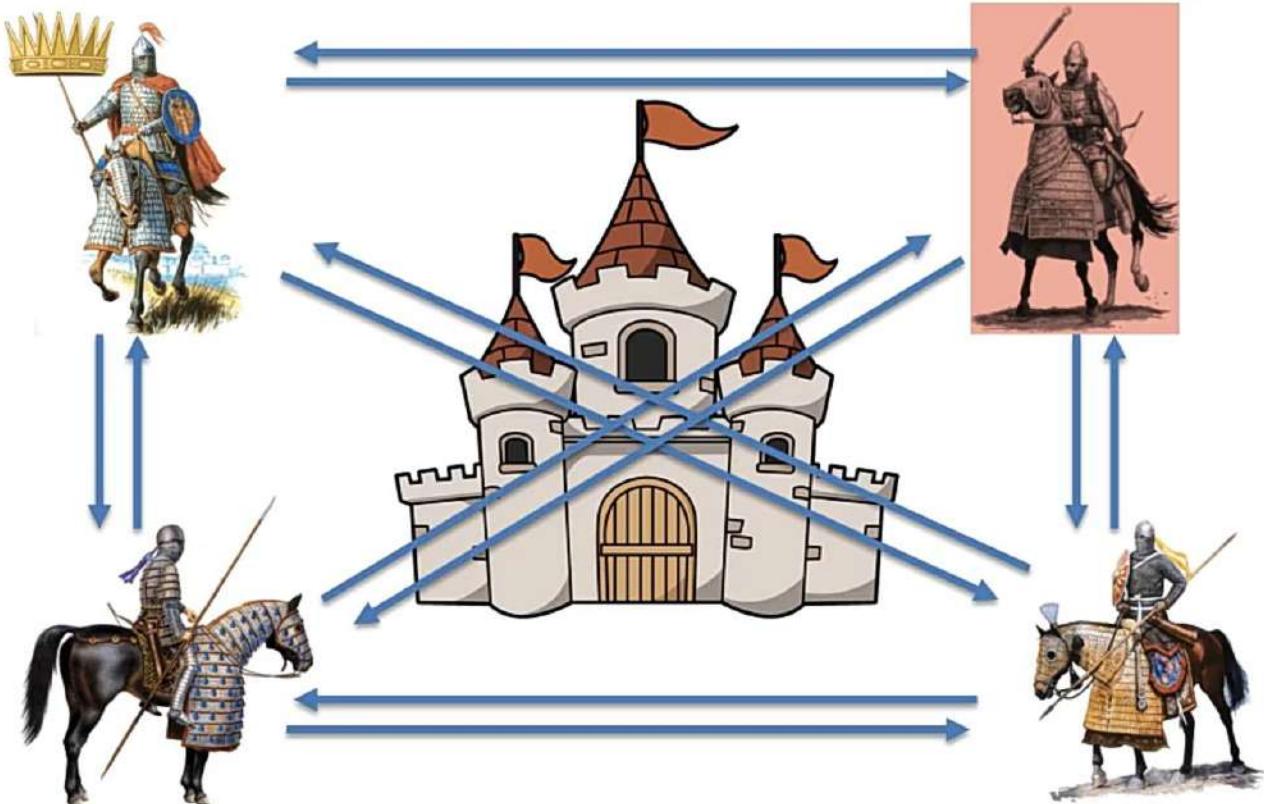
# Byzantine Fault Tolerance



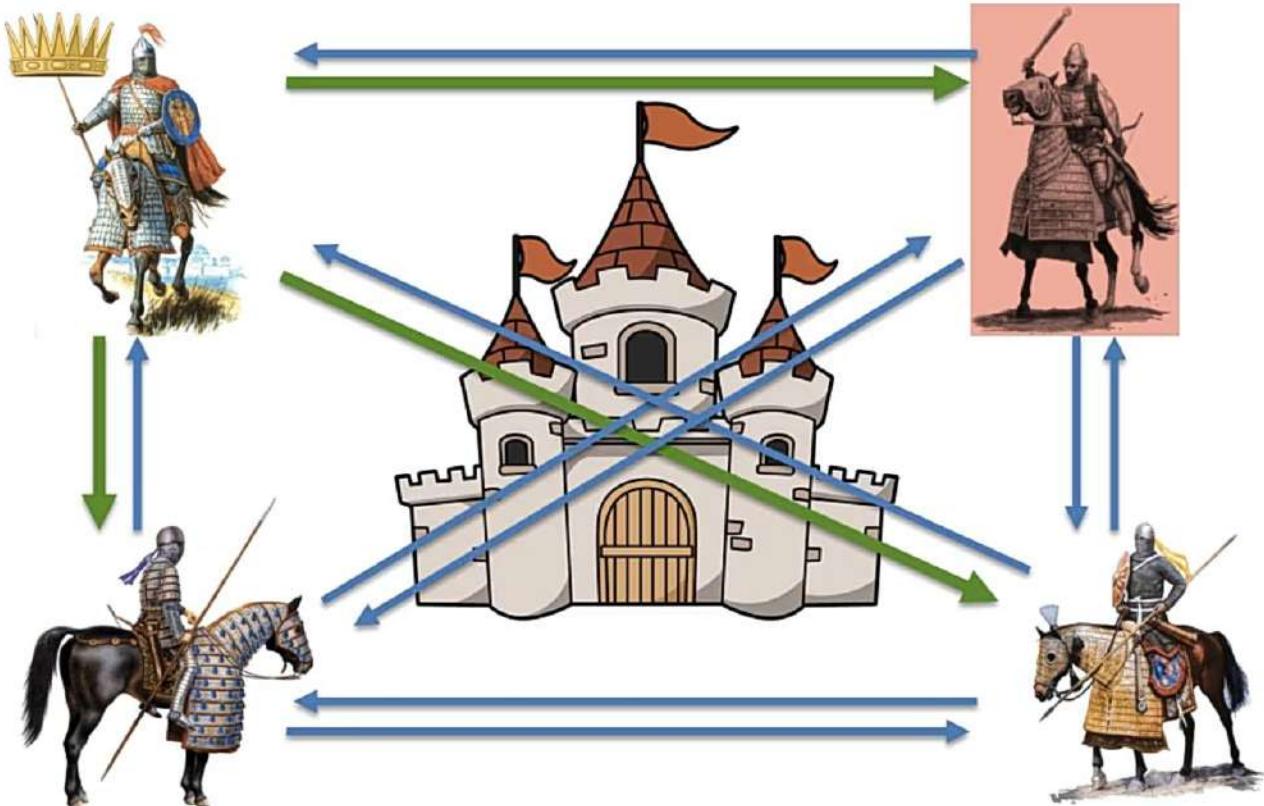
# Byzantine Fault Tolerance



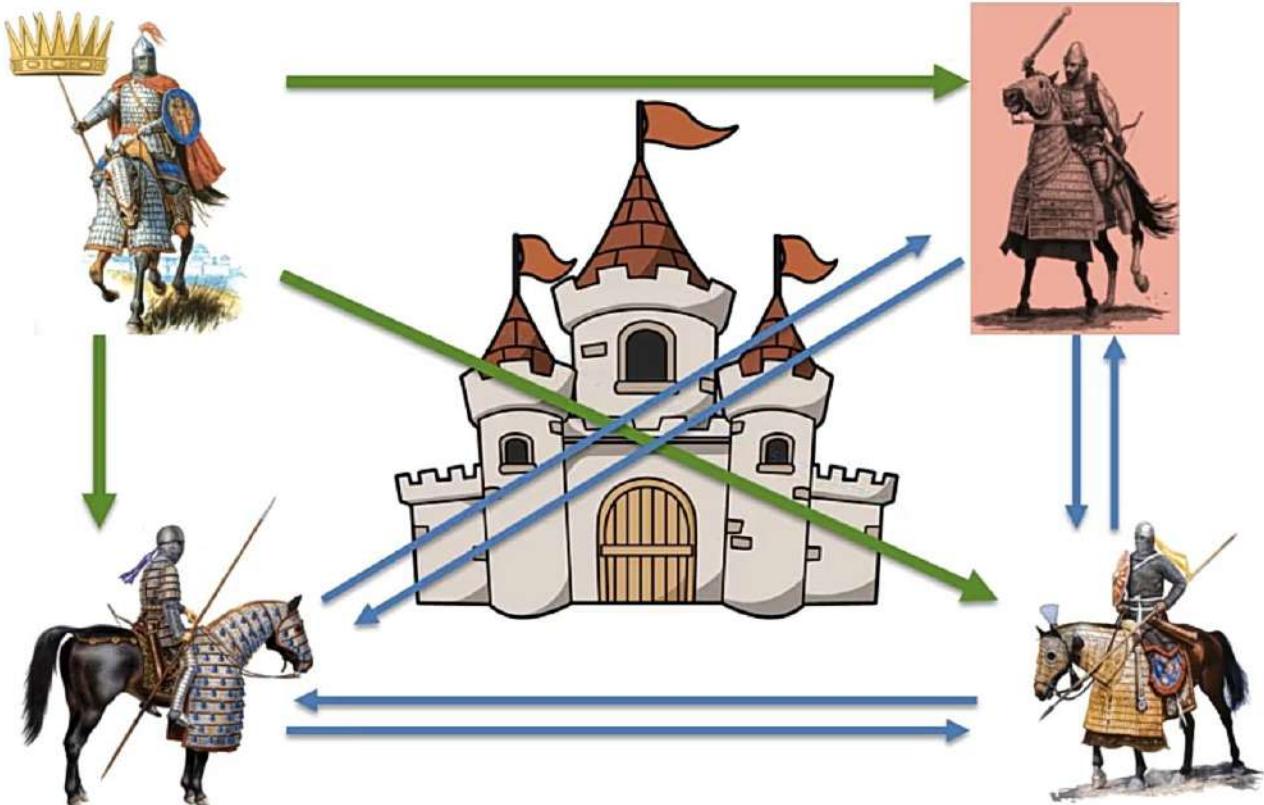
# Byzantine Fault Tolerance



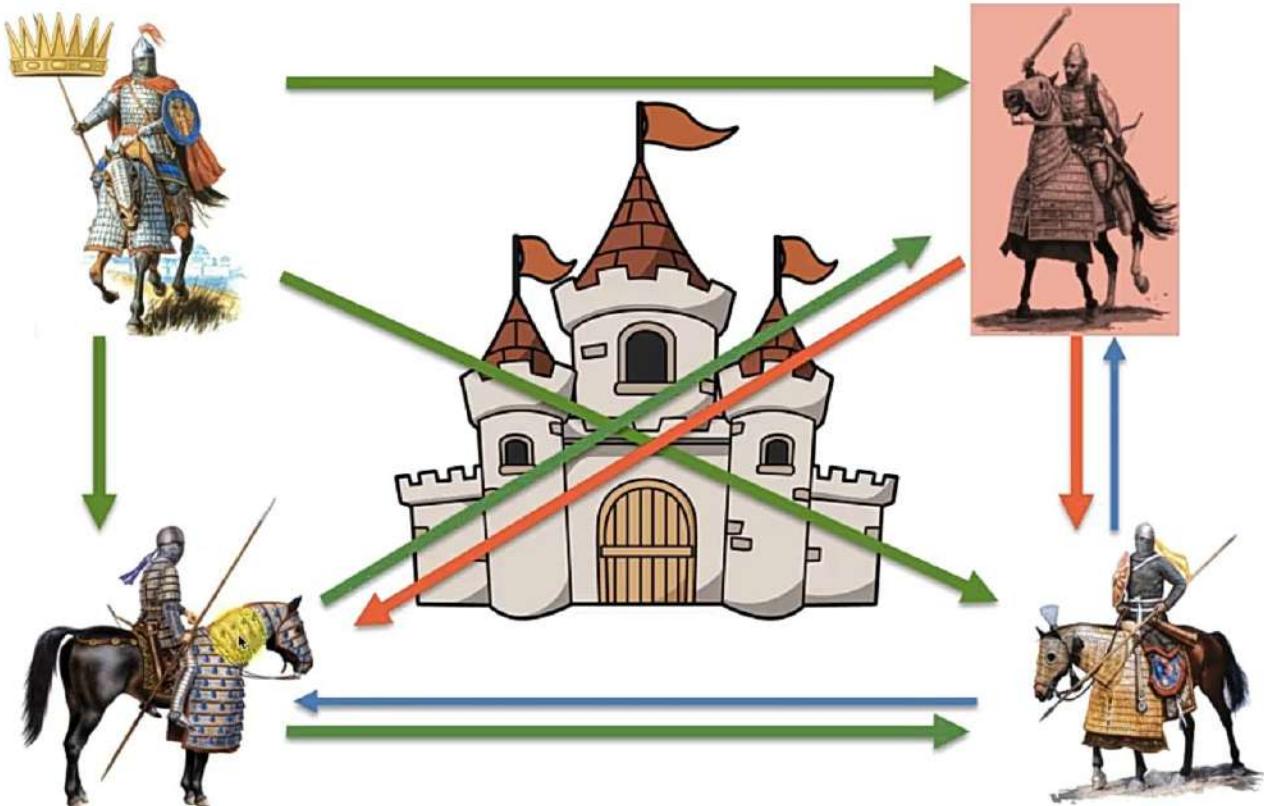
# Byzantine Fault Tolerance



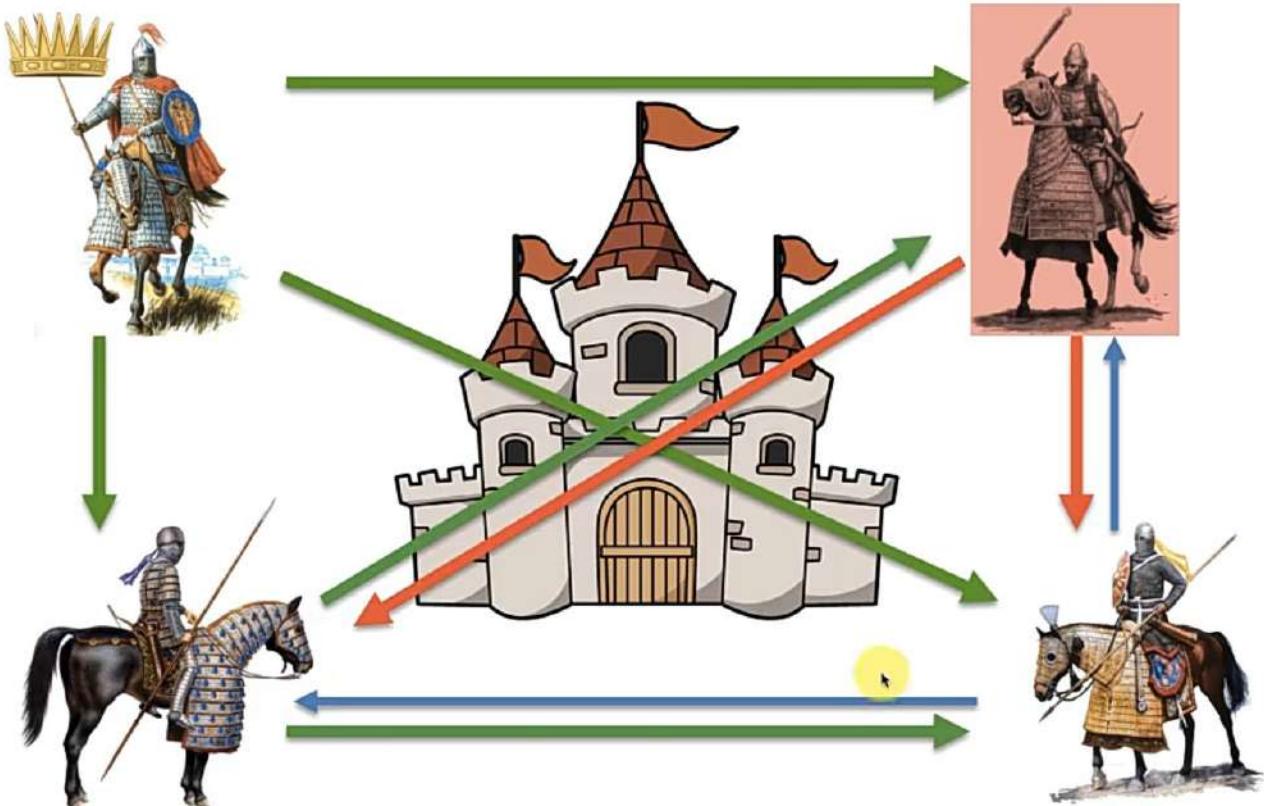
# Byzantine Fault Tolerance



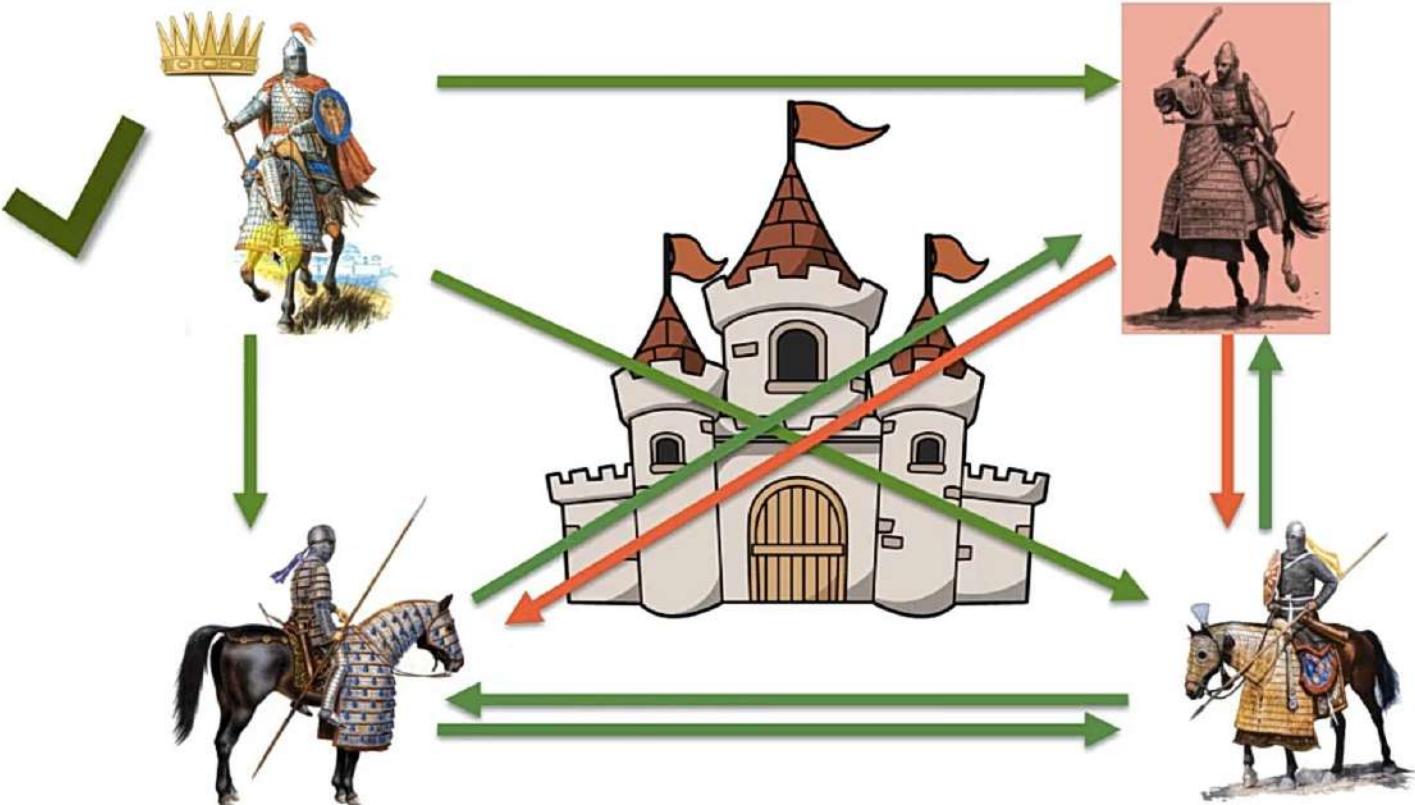
# Byzantine Fault Tolerance



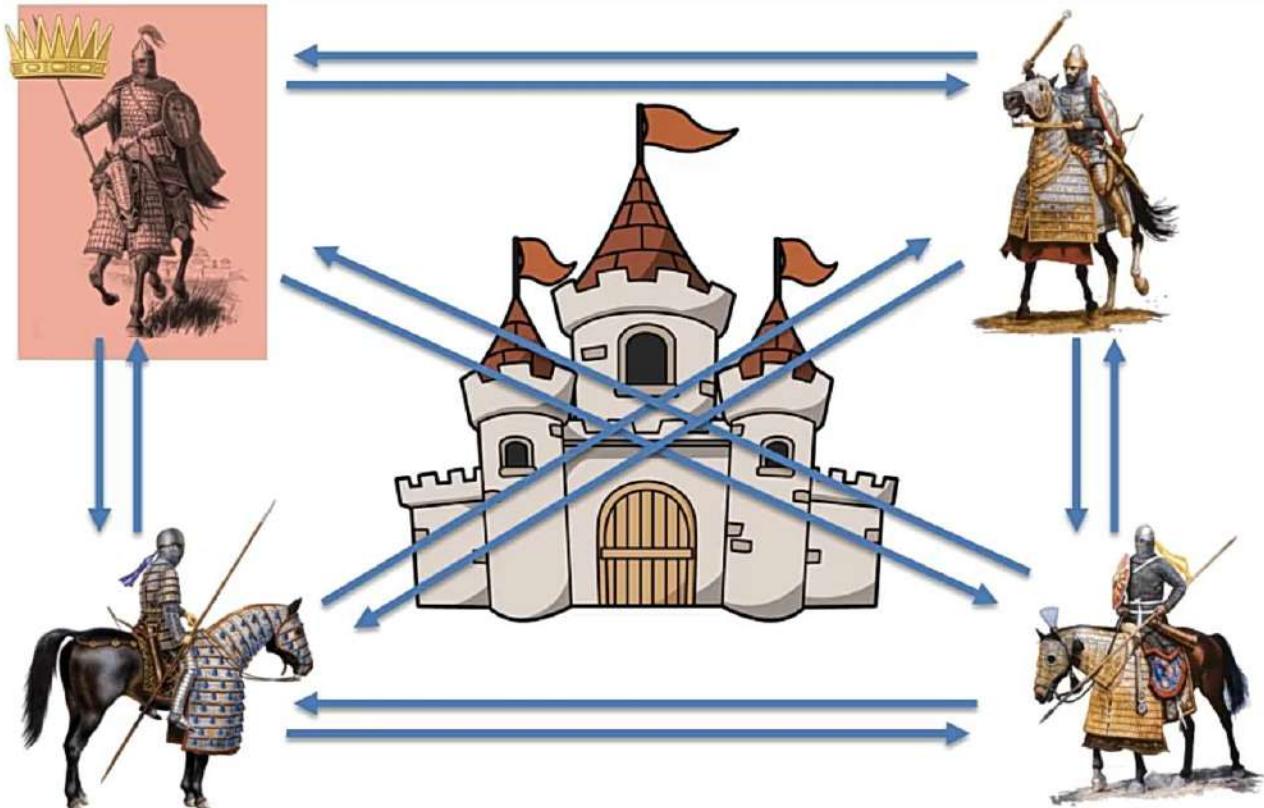
# Byzantine Fault Tolerance



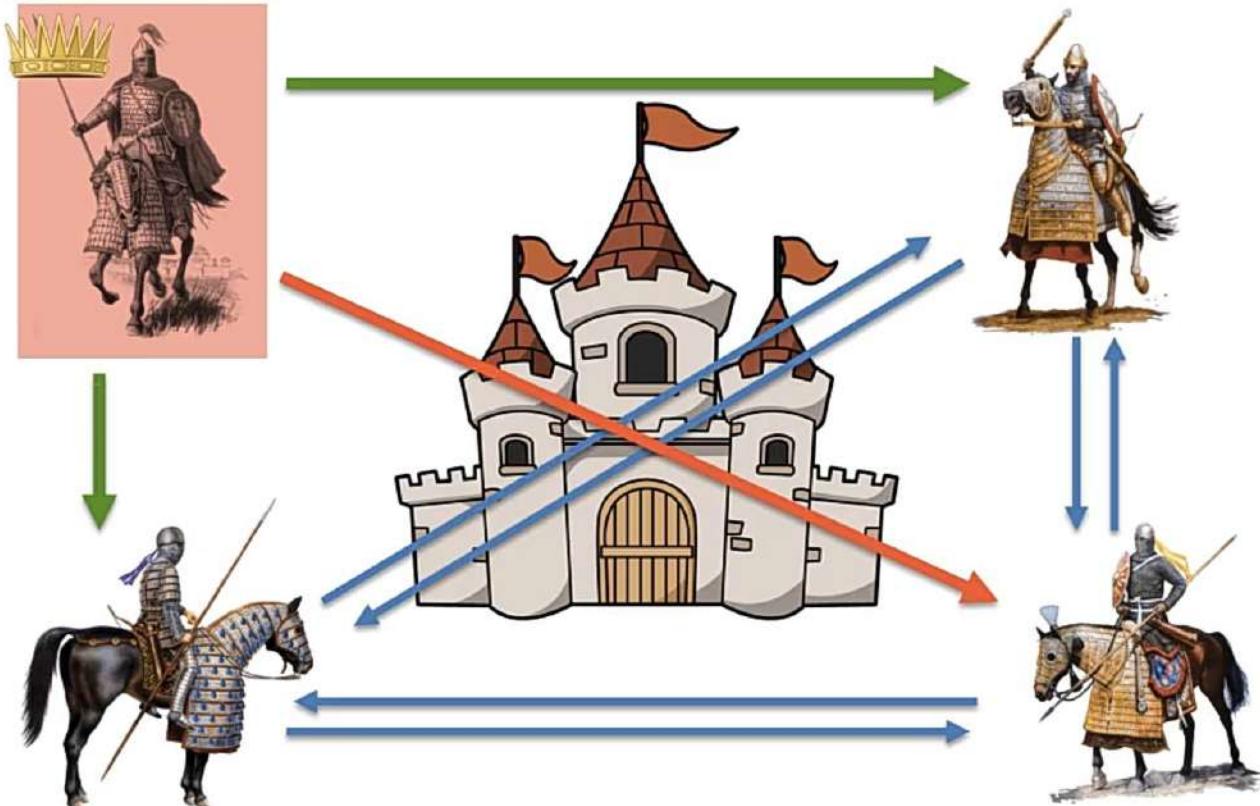
# Byzantine Fault Tolerance



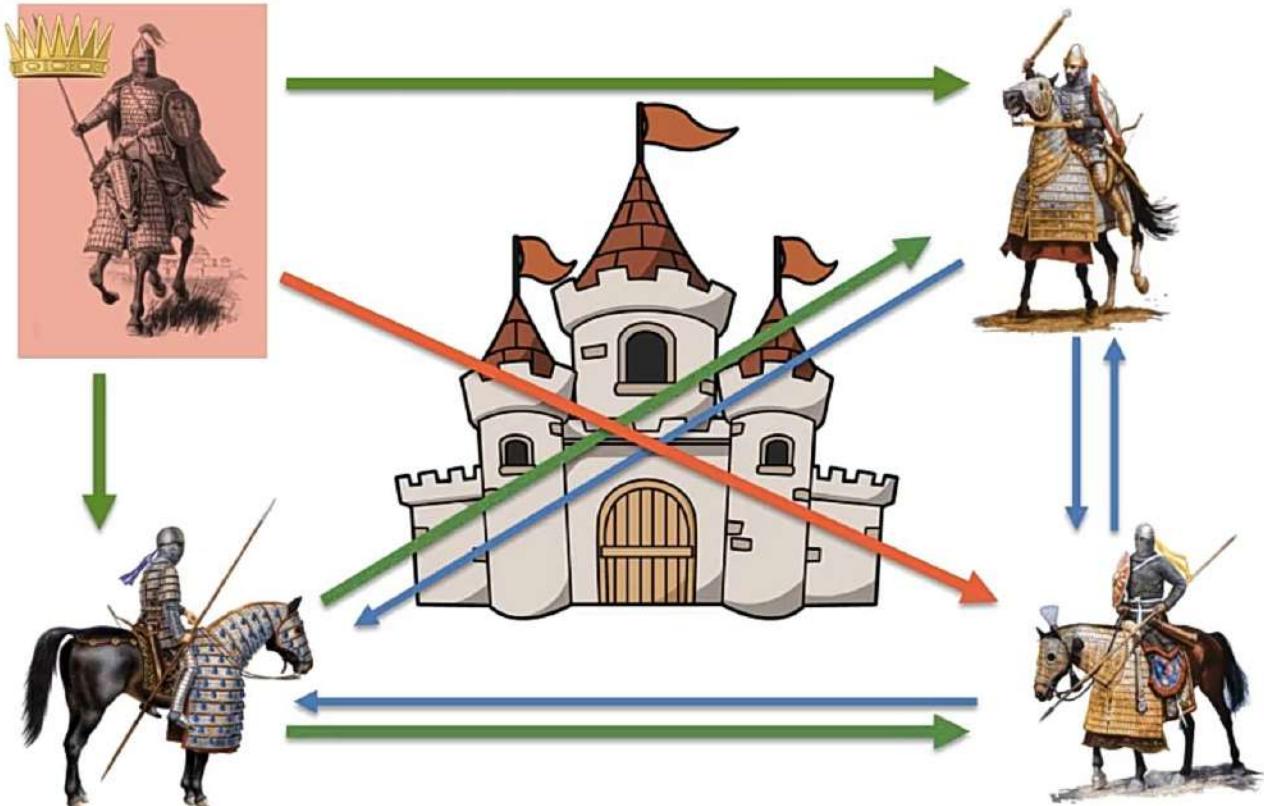
# Byzantine Fault Tolerance



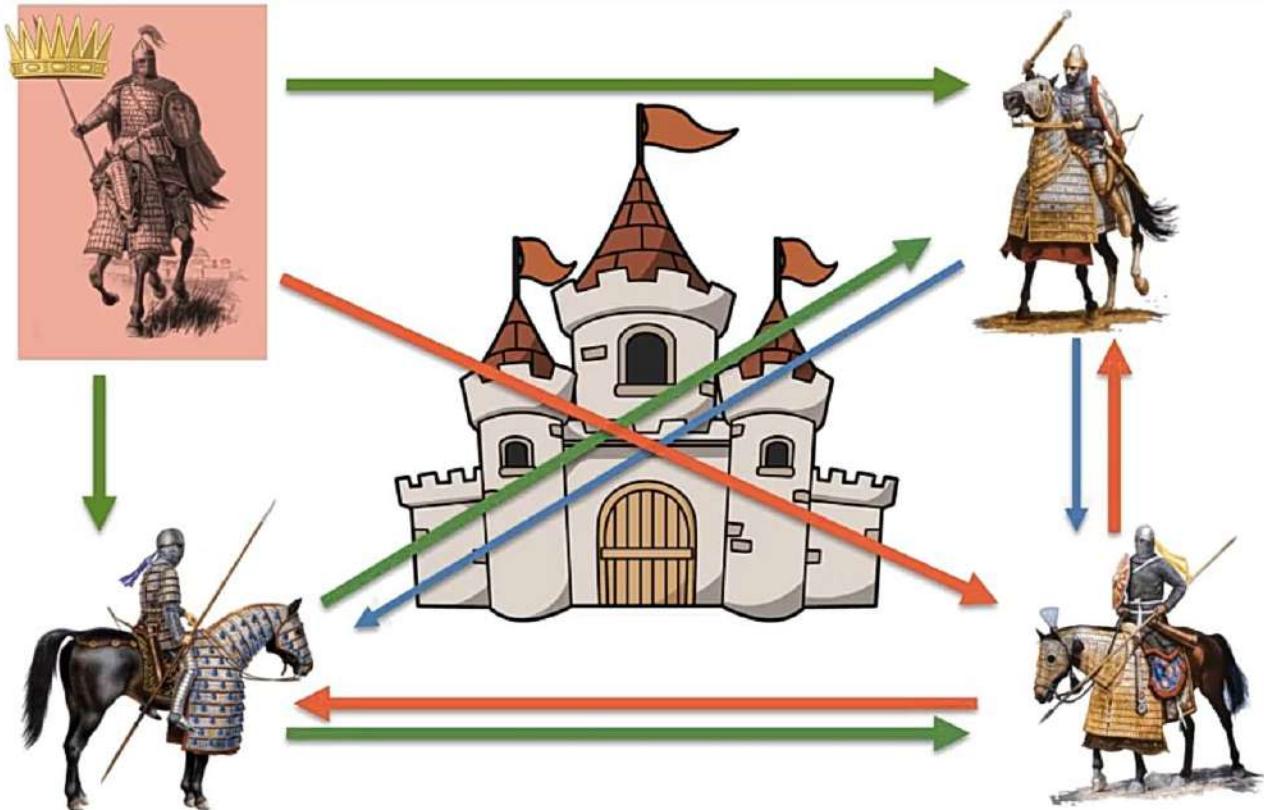
# Byzantine Fault Tolerance



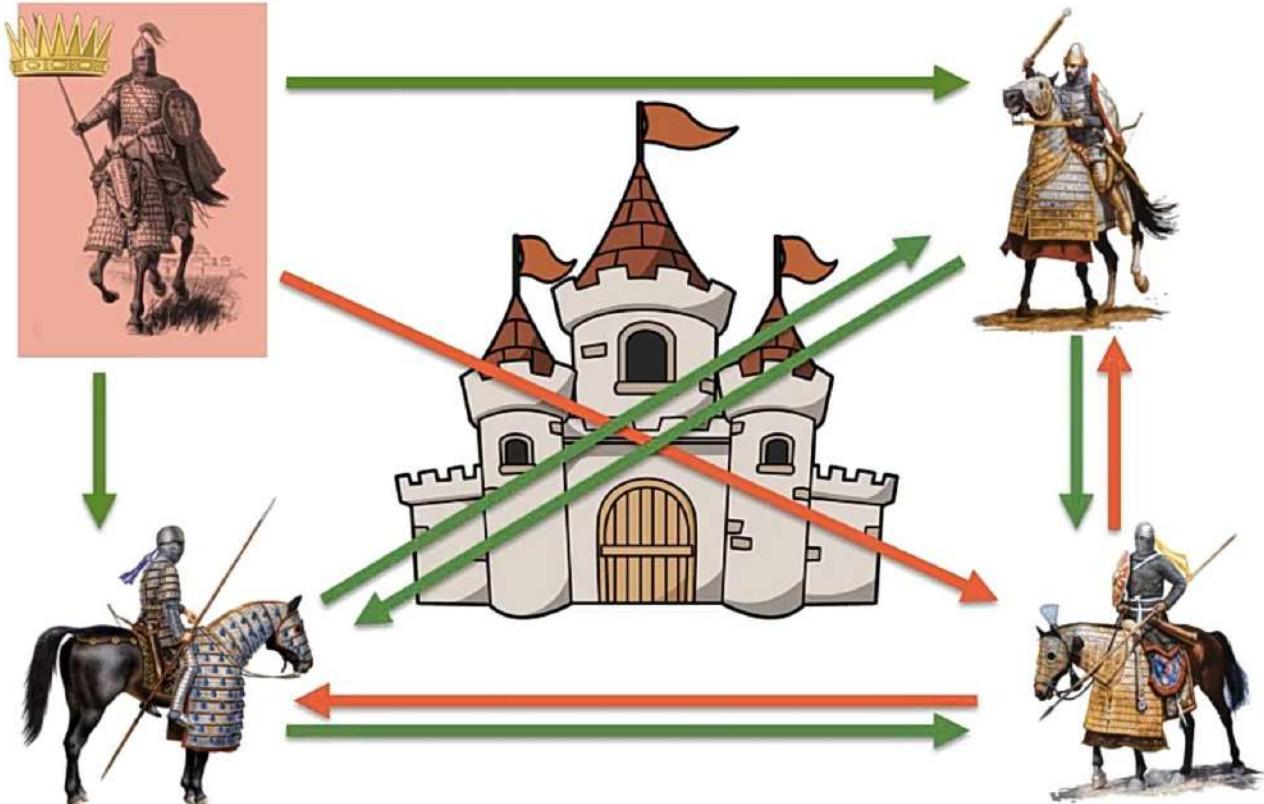
# Byzantine Fault Tolerance



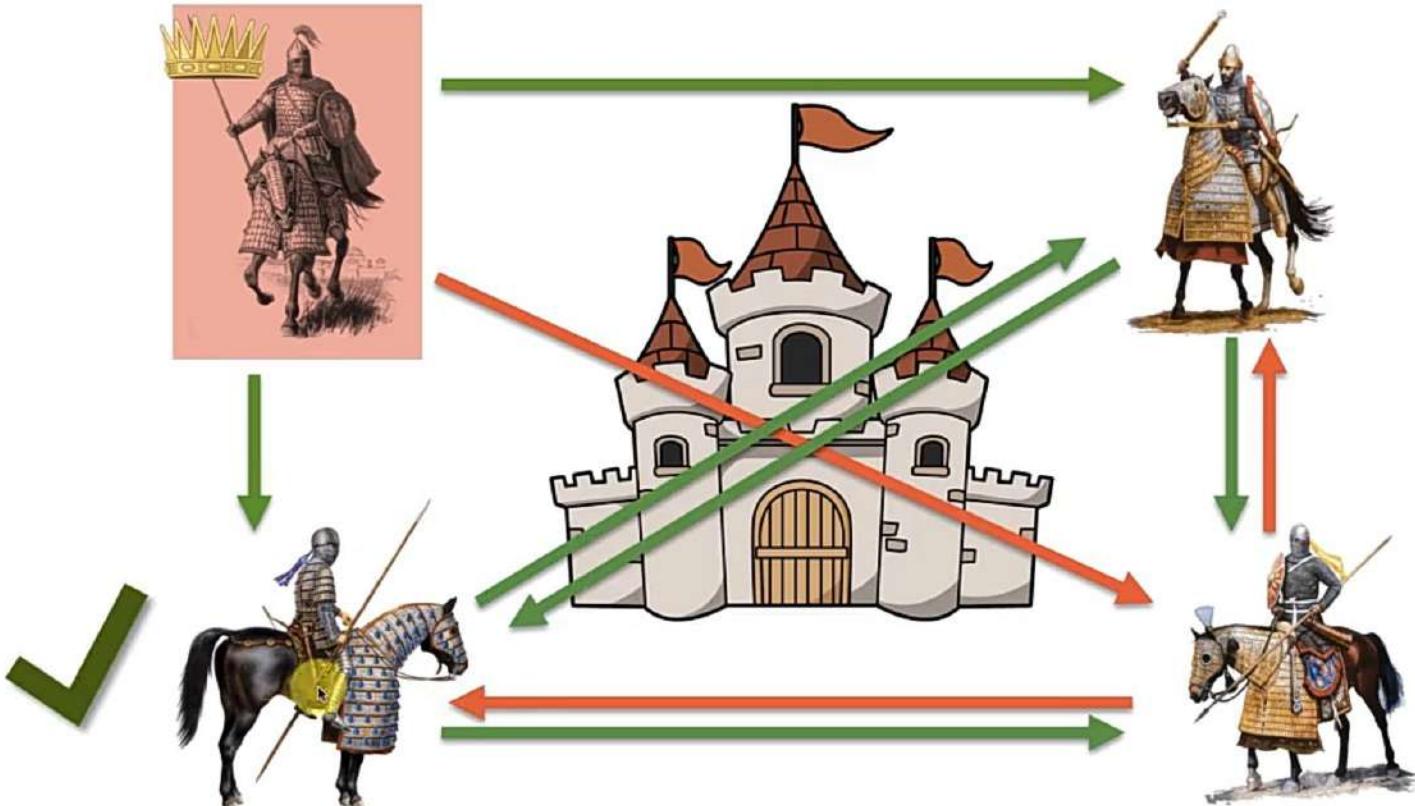
# Byzantine Fault Tolerance



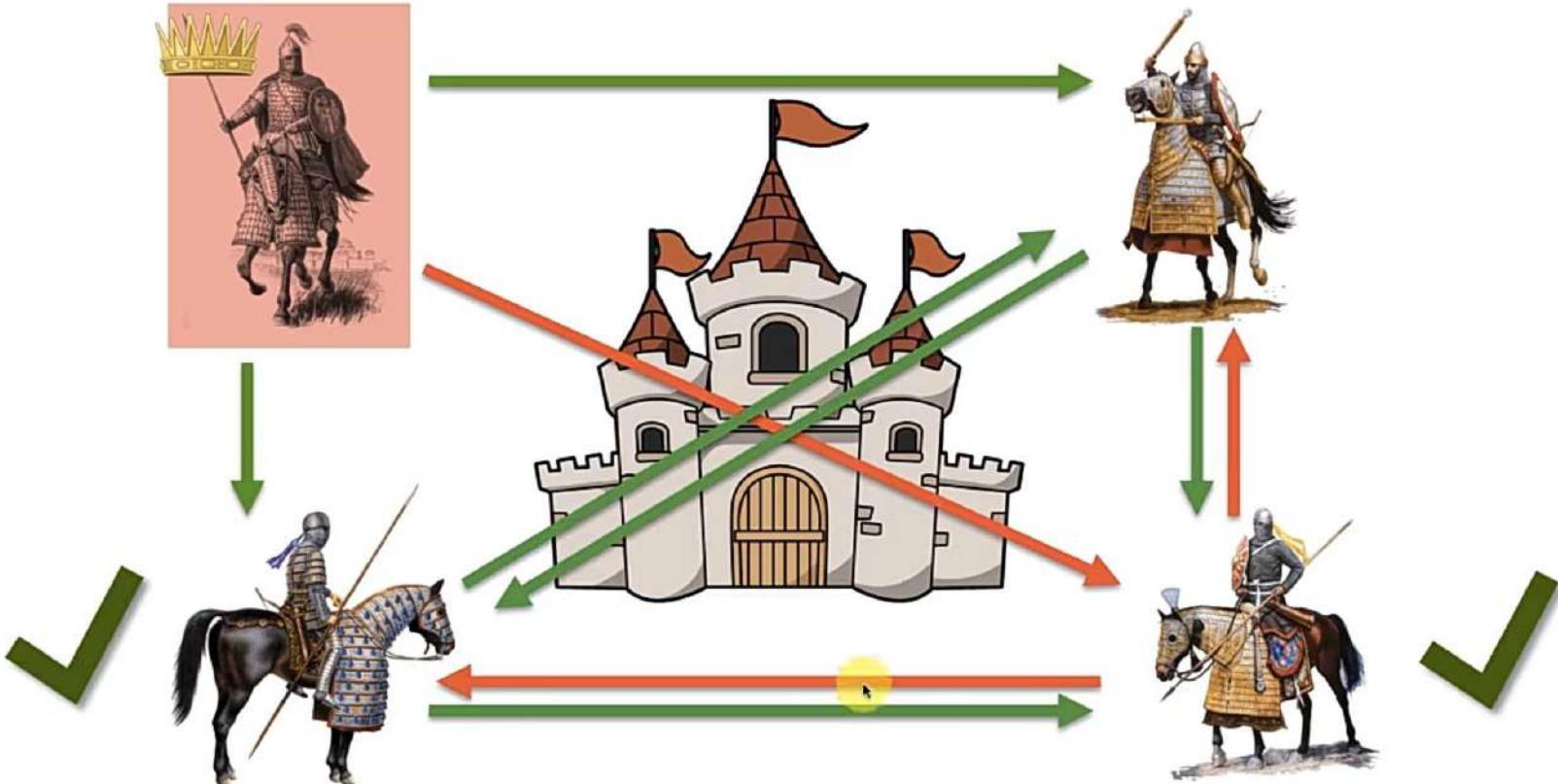
# Byzantine Fault Tolerance



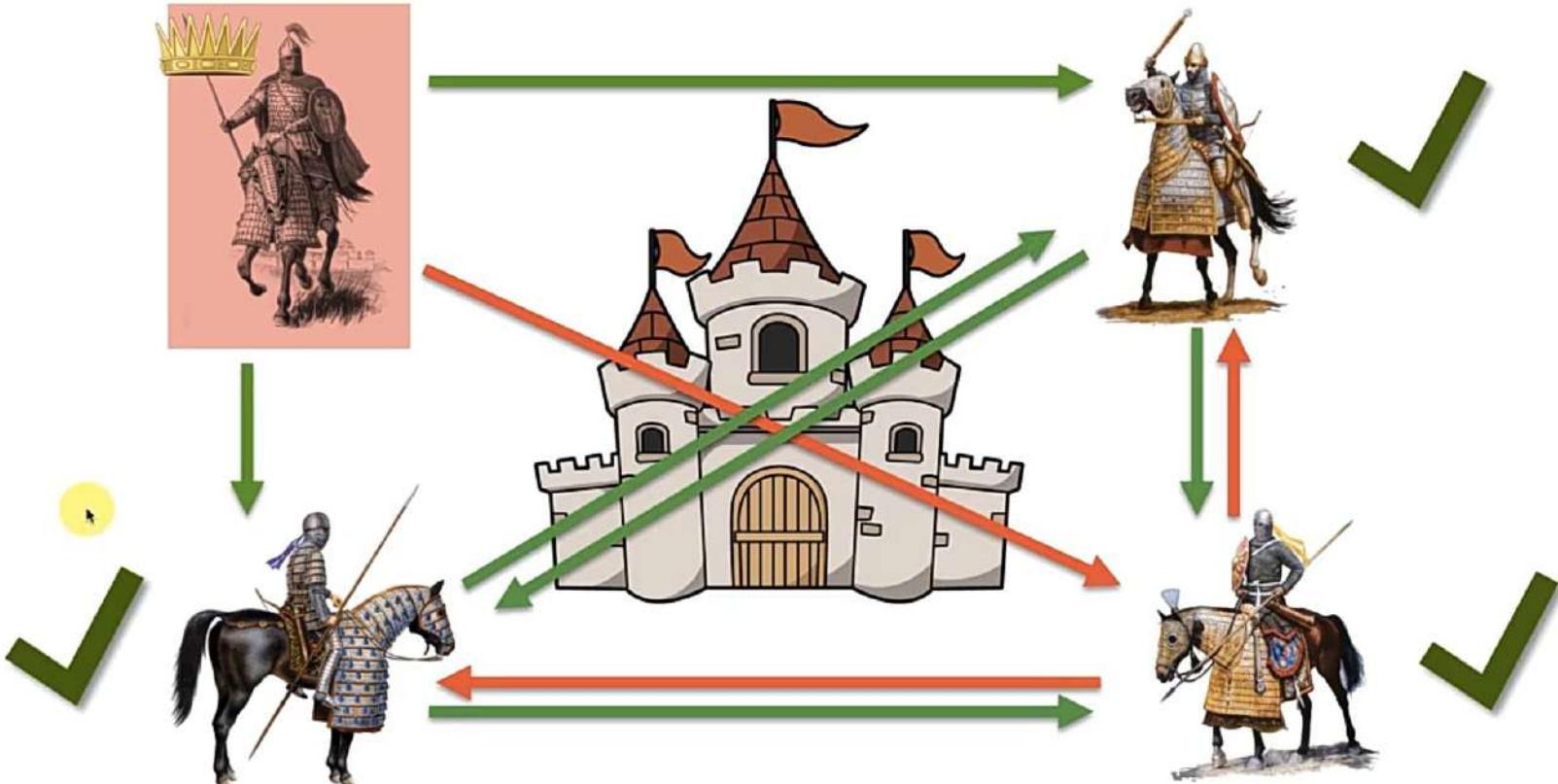
# Byzantine Fault Tolerance



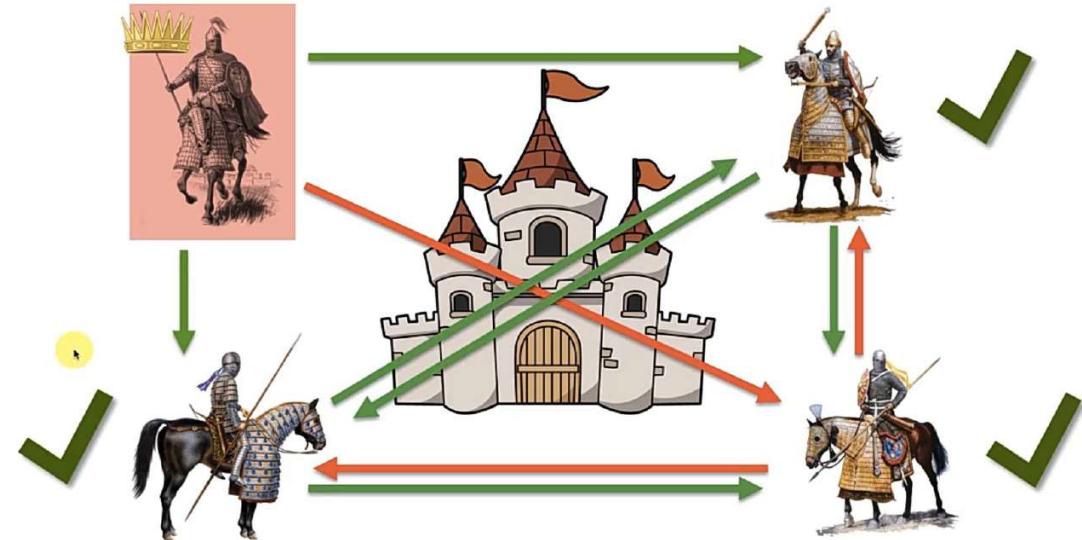
# Byzantine Fault Tolerance



# Byzantine Fault Tolerance

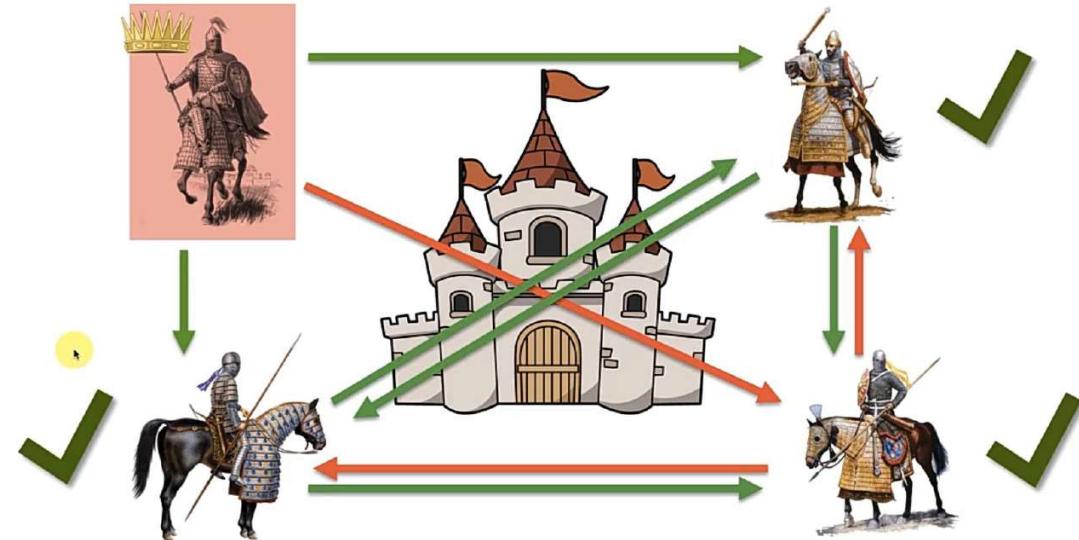


# Byzantine Fault Tolerance



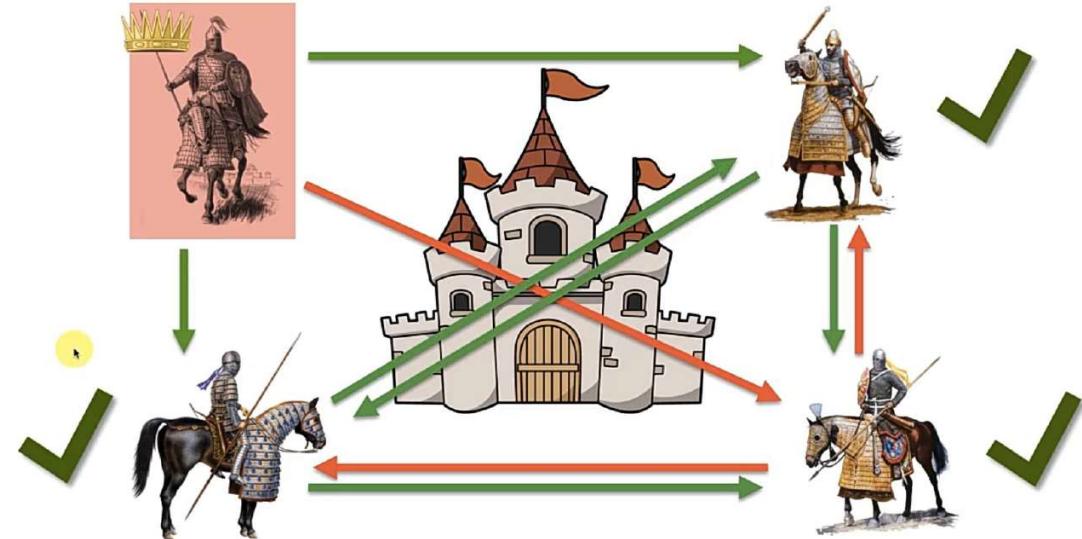
- What is the level of tolerance ?
- What if there are 2 traitors in this network ?

# Byzantine Fault Tolerance



- What is the level of tolerance ?
- What if there are 2 traitors in this network ?
- **Not more than  $\frac{1}{3}$  in the Army can be traitors.**

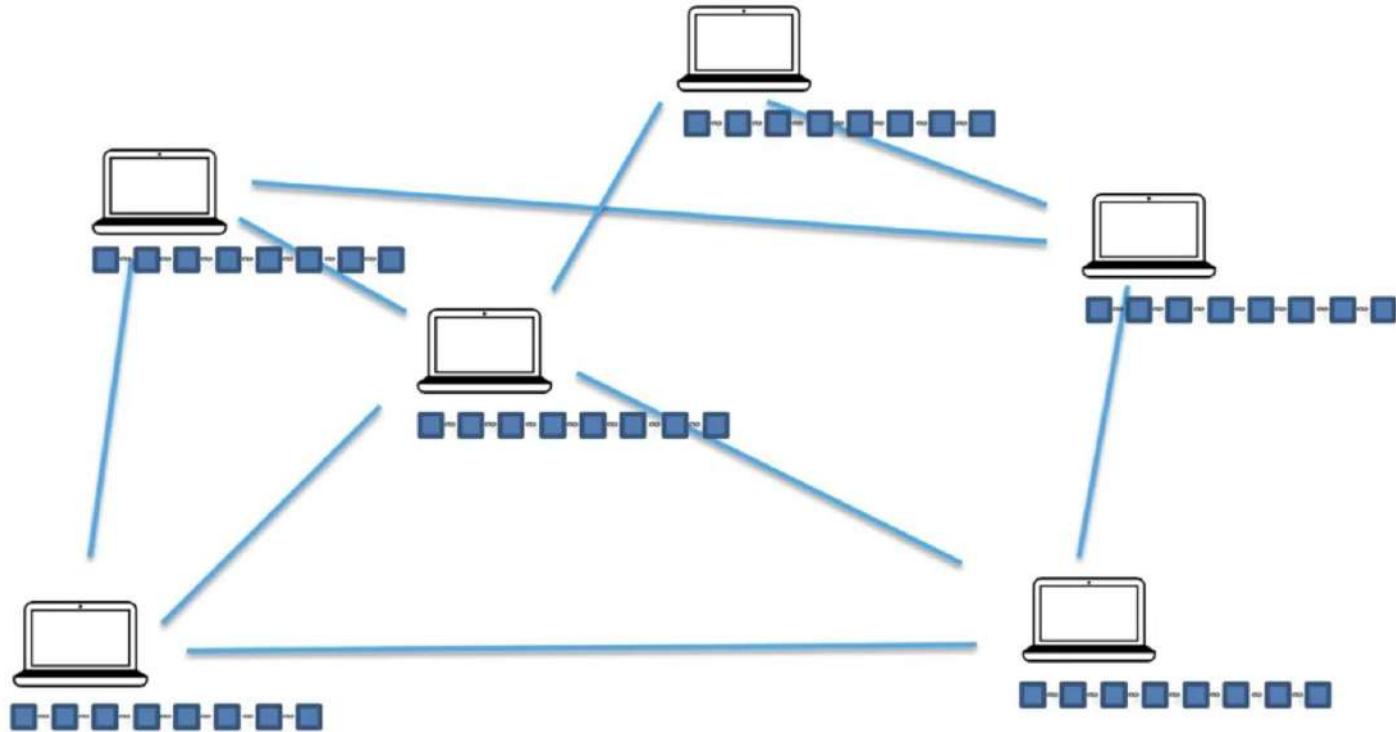
# Byzantine Fault Tolerance



## Applications of BFT

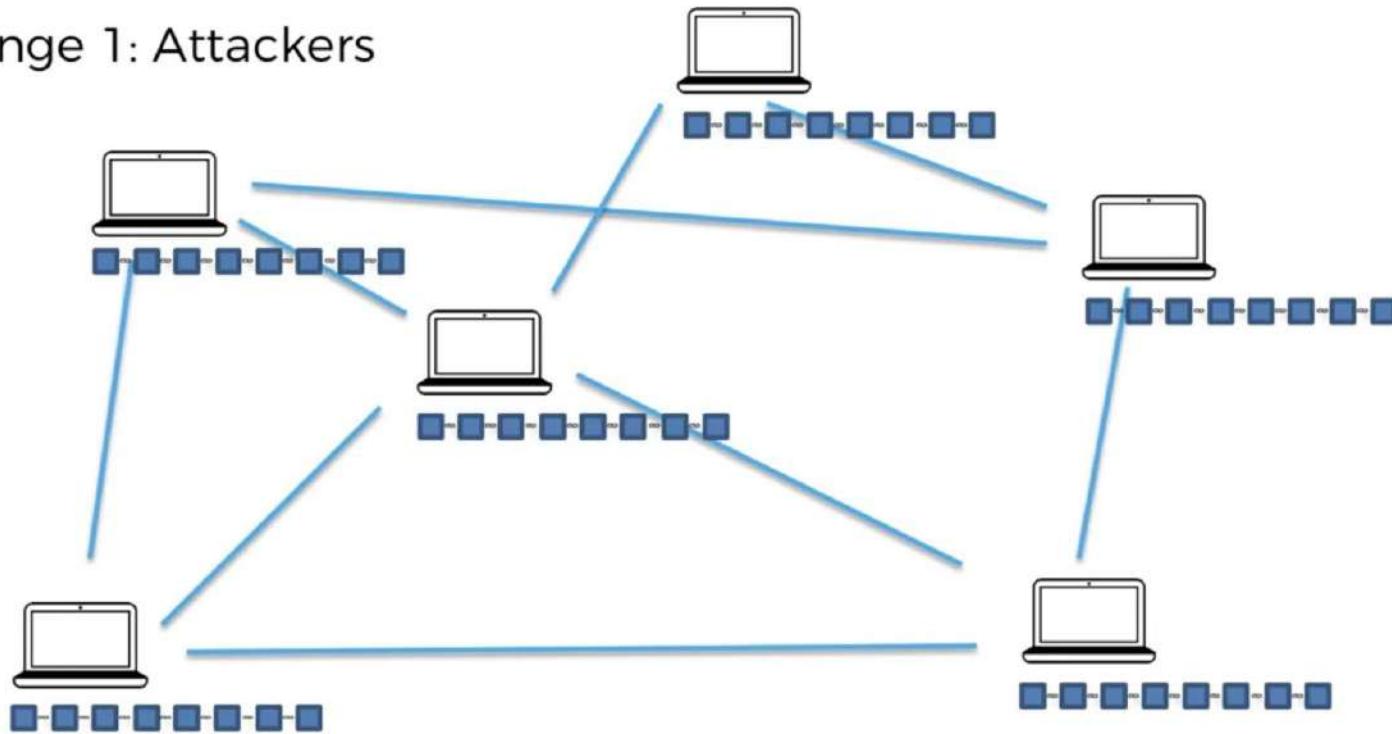
- Blockchain
- Aeroplane Circuits
- Nuclear Power Plants
- Rockets, etc ...

# Challenges Addressed by Consensus Protocol



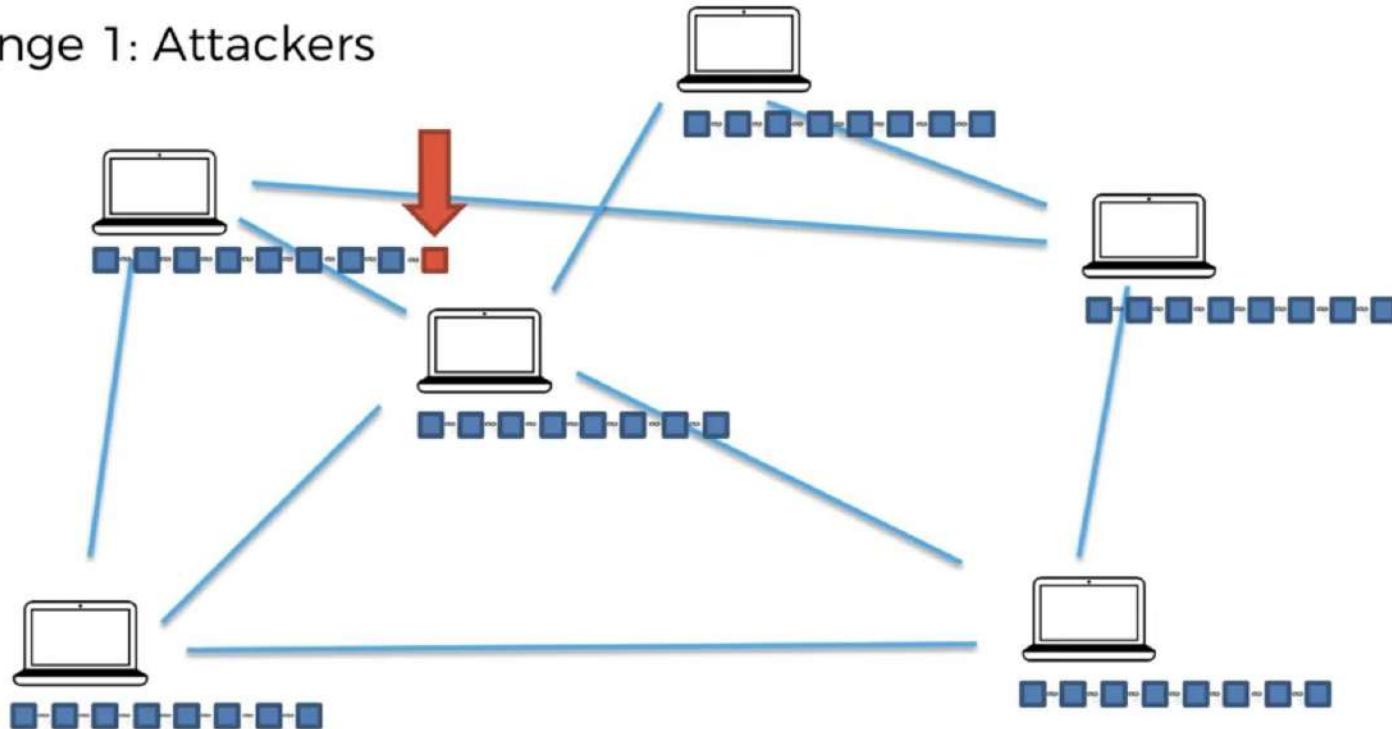
# Challenges Addressed by Consensus Protocol

Challenge 1: Attackers



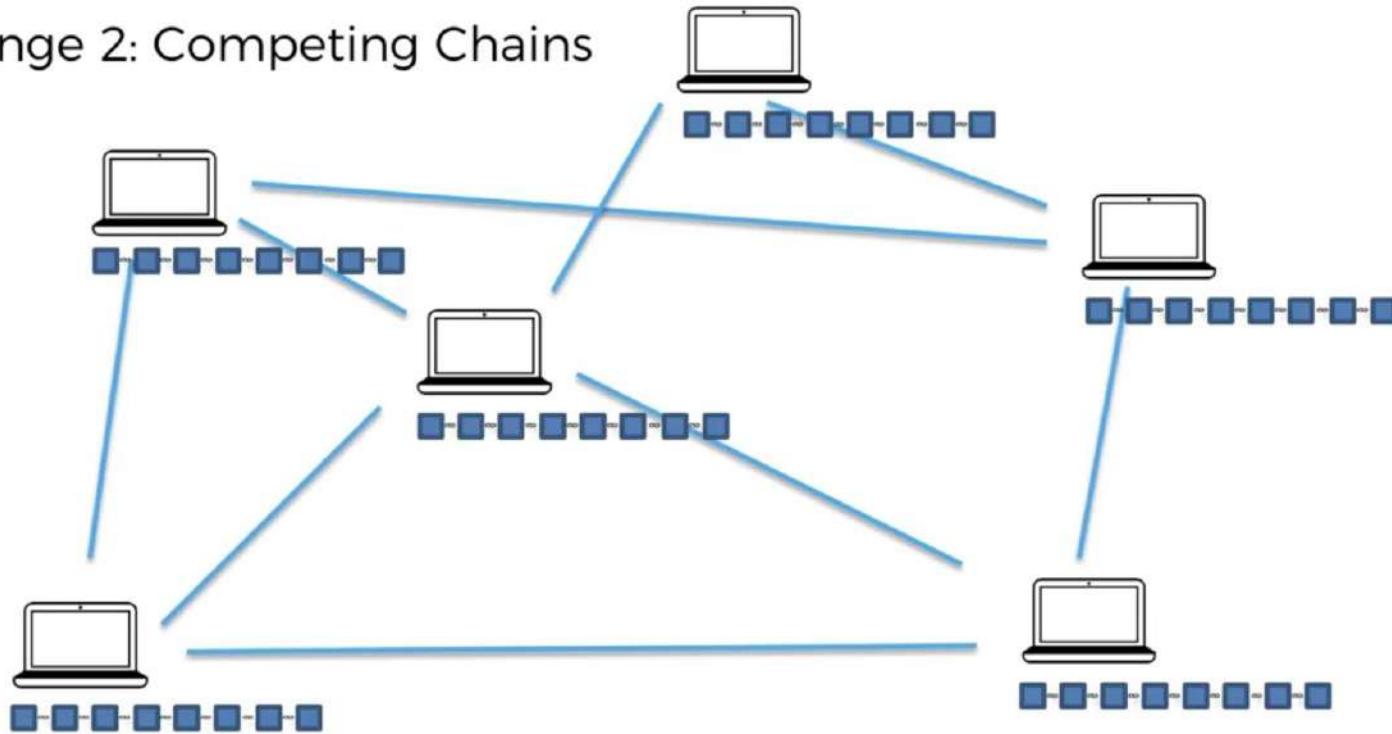
# Challenges Addressed by Consensus Protocol

Challenge 1: Attackers



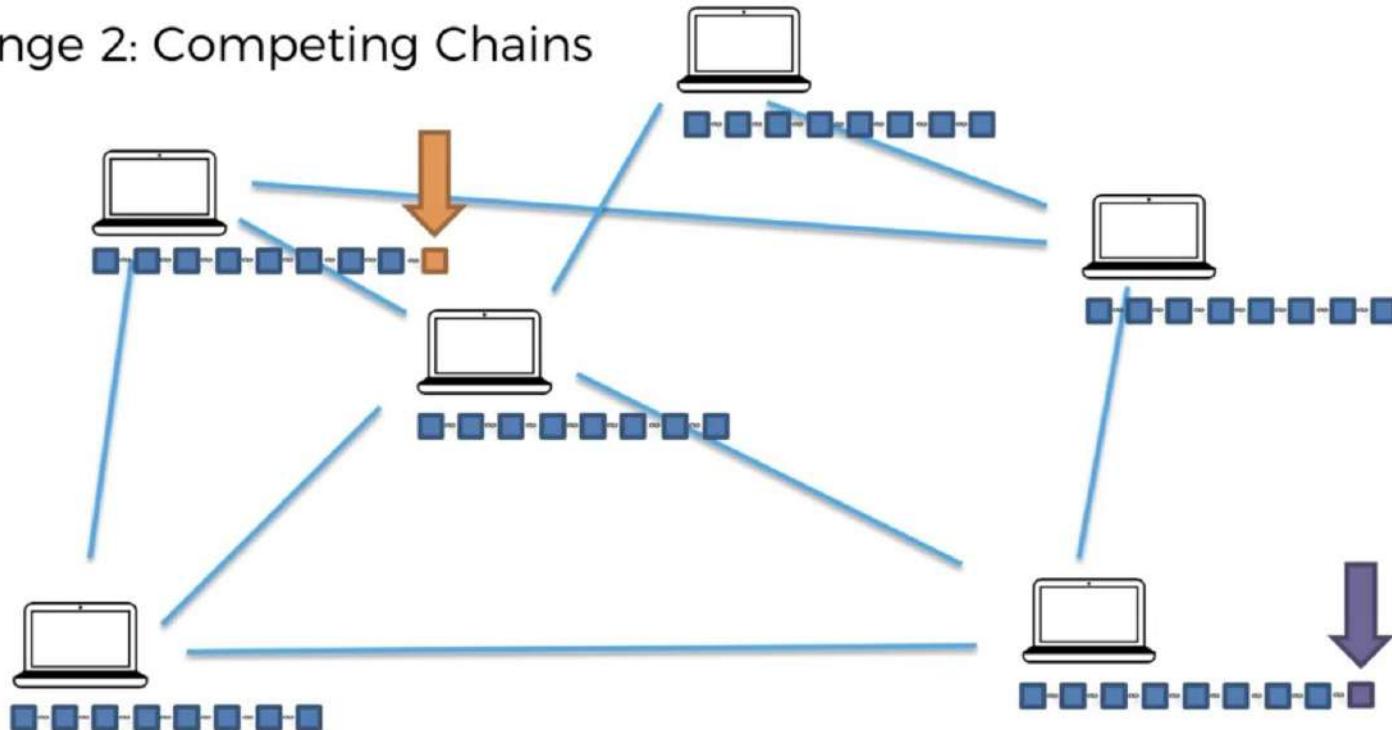
# Challenges Addressed by Consensus Protocol

Challenge 2: Competing Chains

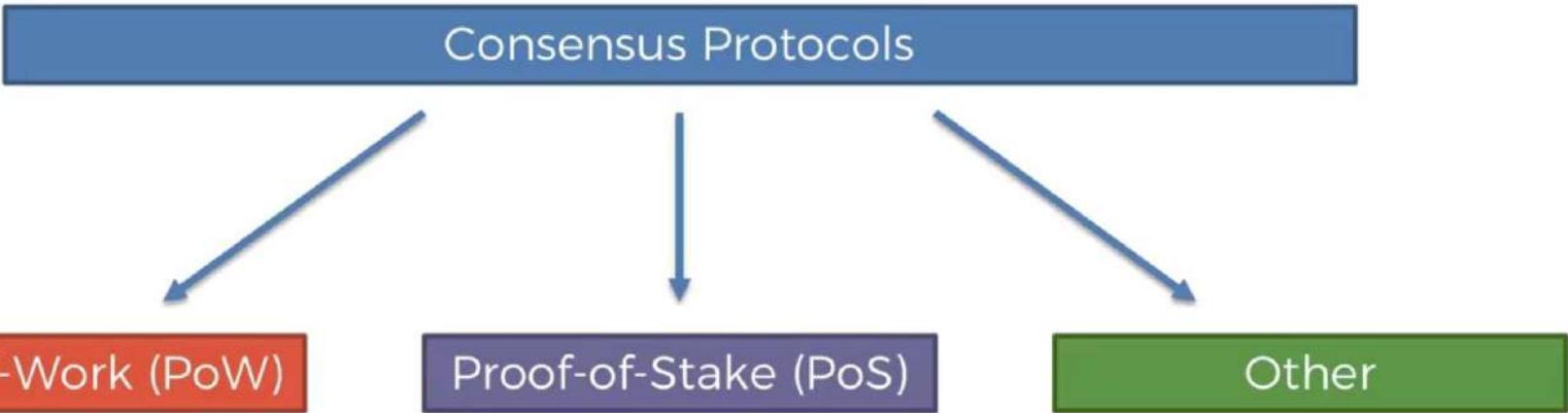


# Challenges Addressed by Consensus Protocol

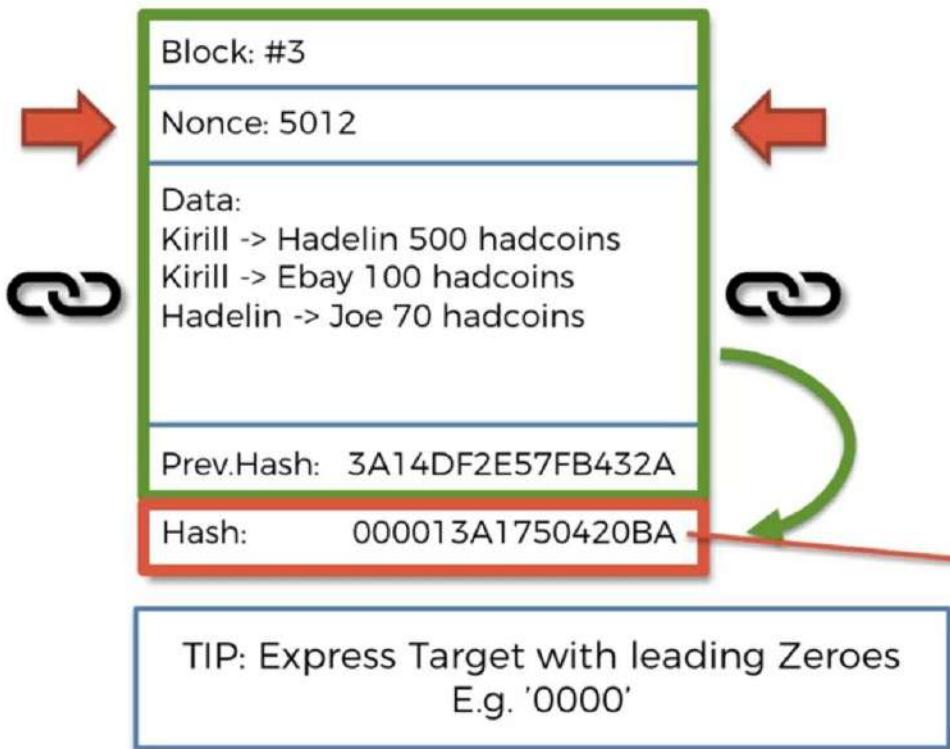
Challenge 2: Competing Chains



# Consensus Protocol



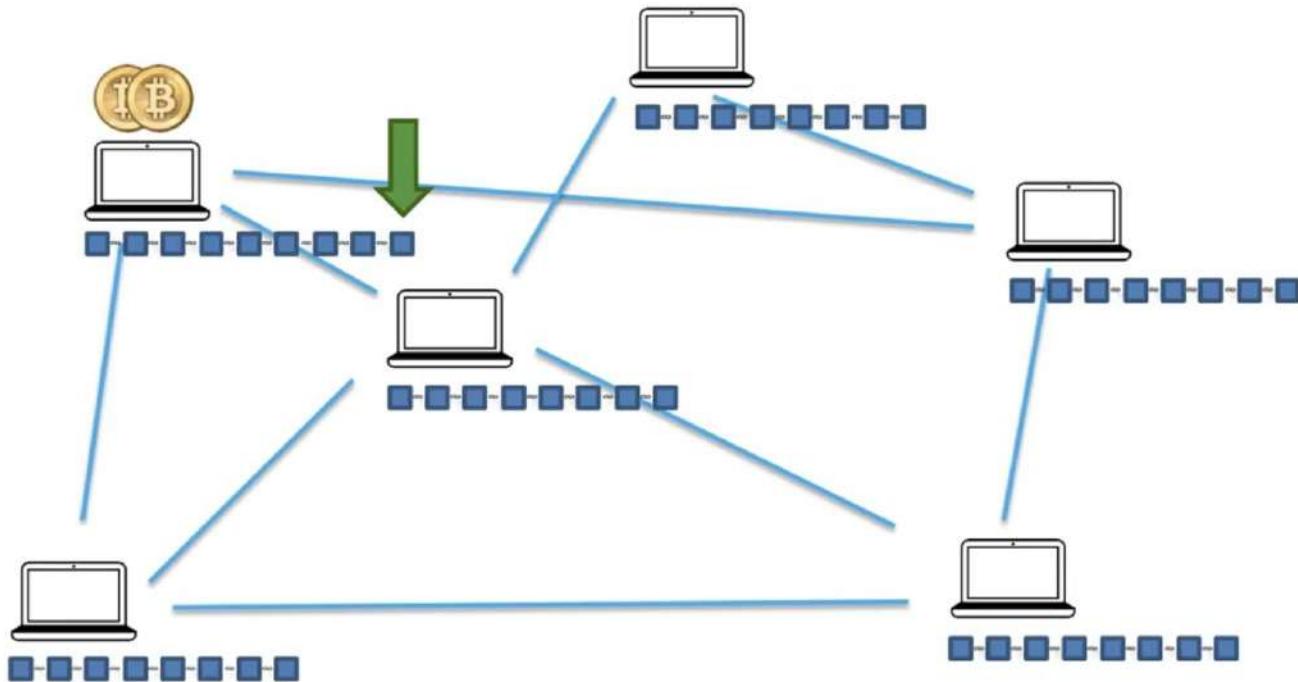
# Consensus Protocol - Cryptographic Challenge



- ALL POSSIBLE HASHES -



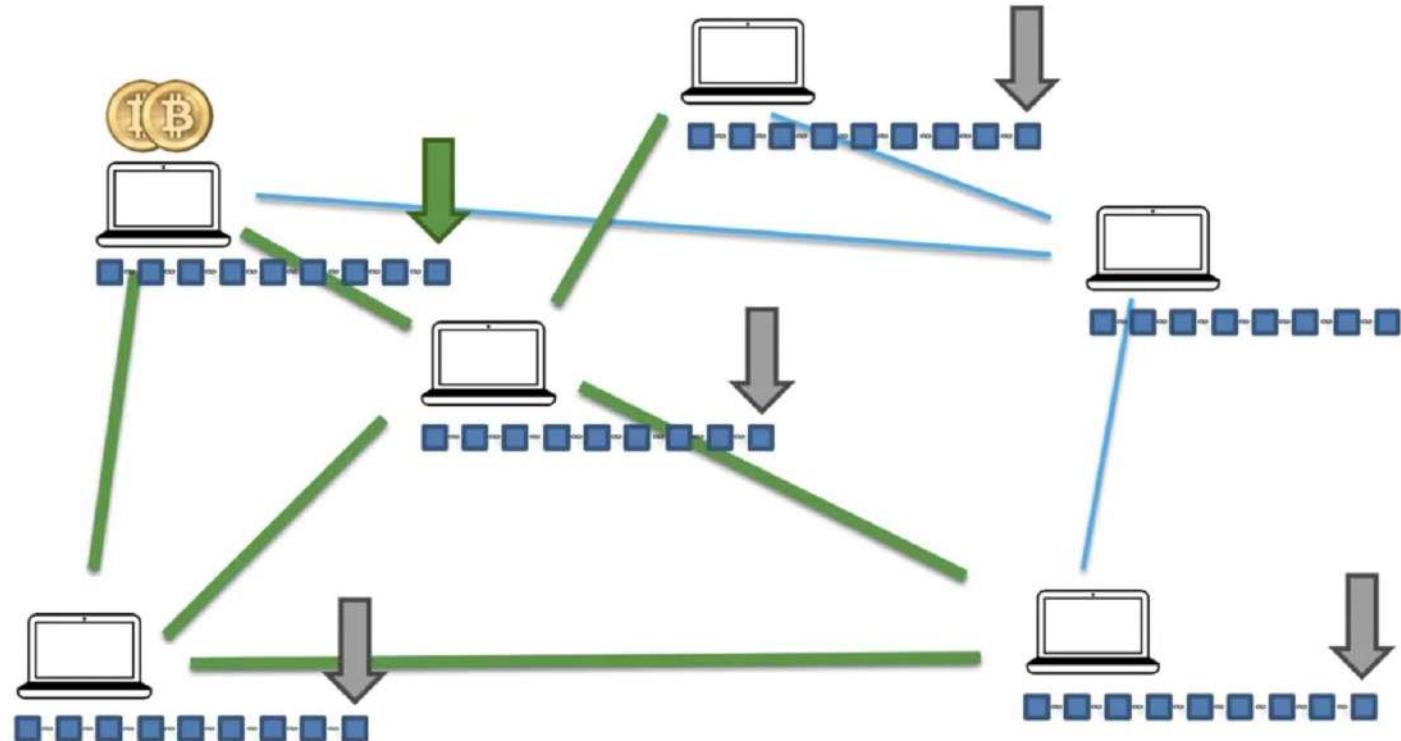
# Consensus Protocol - Attackers Challenge



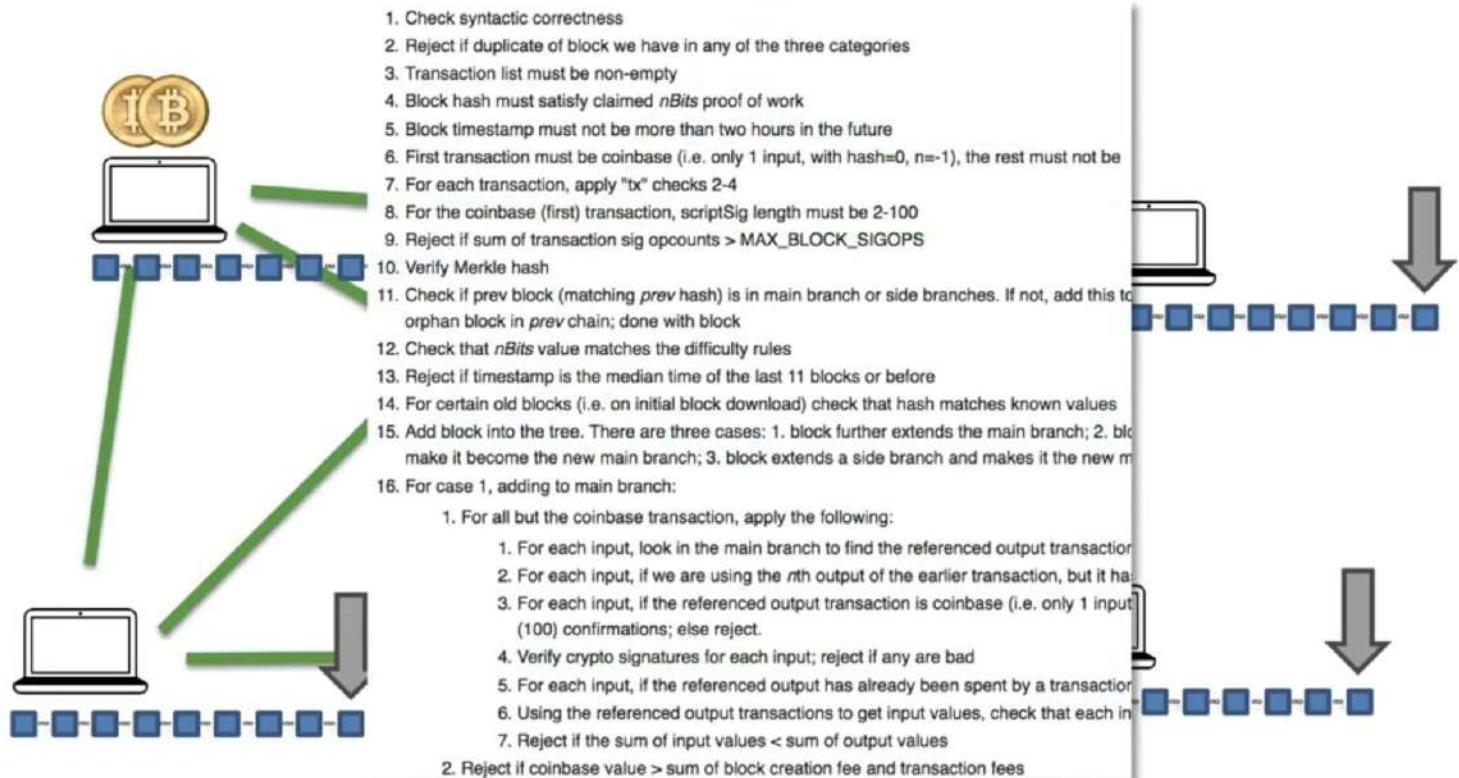
**Miners get incentives for :**

1. **Adding a block**
2. **To play fair**
3. **From the transaction fees**

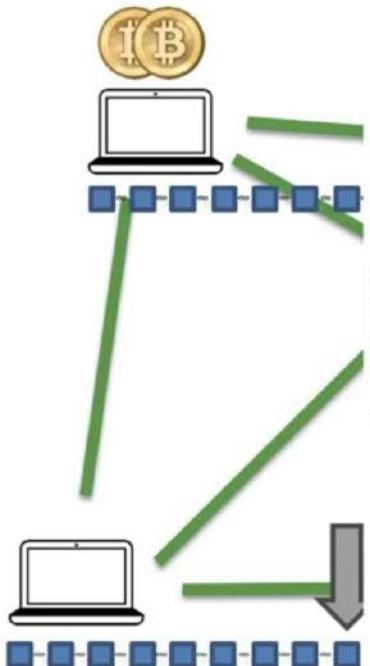
# Consensus Protocol - Attackers Challenge



# Consensus Protocol - Attackers Challenge

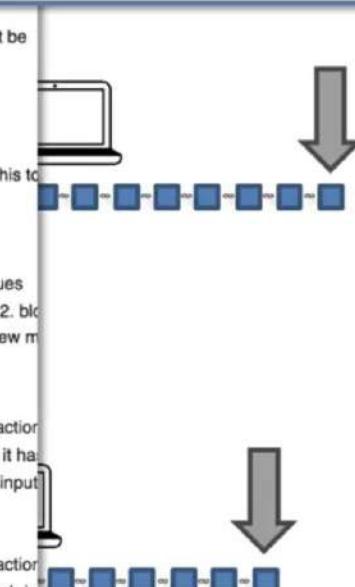


# Consensus Protocol - Attackers Challenge

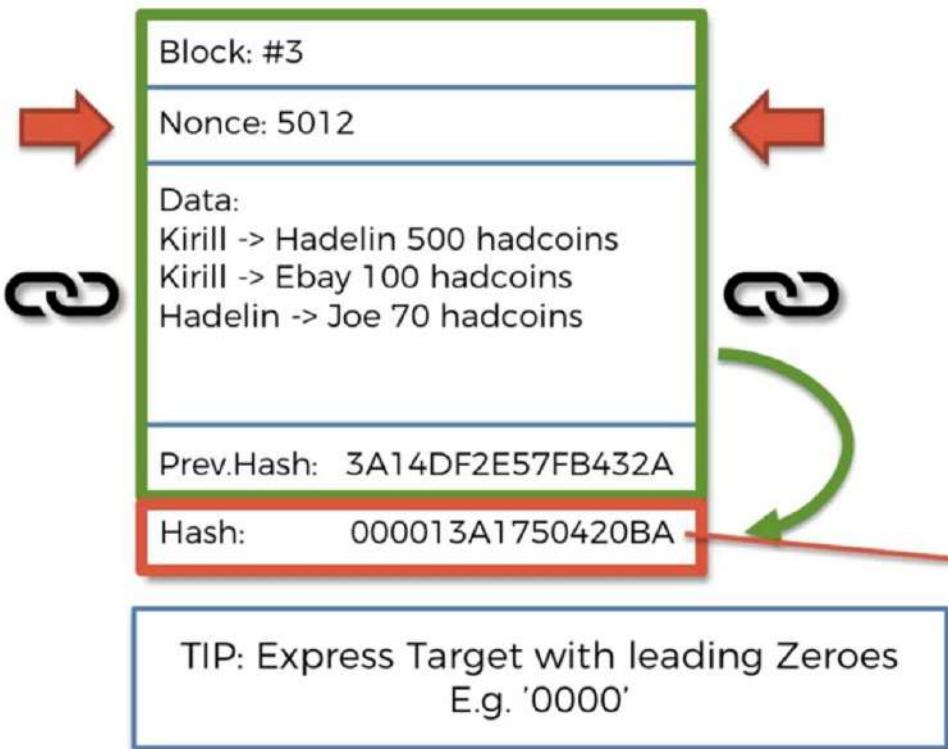


1. Check syntactic correctness
2. Reject if duplicate of block we have in any of the three categories
3. Transaction list must be non-empty
4. Block hash must satisfy claimed  $nBits$  proof of work
5. Block timestamp must not be more than two hours in the future
6. First transaction must be coinbase (i.e. only 1 input, with hash=0, n=-1), the rest must not be
7. For each transaction, apply "tx" checks 2-4
8. For the coinbase (first) transaction, scriptSig length must be 2-100
9. Reject if sum of transaction sig opcounts > MAX\_BLOCK\_SIGOPS
10. Verify Merkle hash
11. Check if prev block (matching *prev* hash) is in main branch or side branches. If not, add this to orphan block in *prev* chain; done with block
12. Check that  $nBits$  value matches the difficulty rules
13. Reject if timestamp is the median time of the last 11 blocks or before
14. For certain old blocks (i.e. on initial block download) check that hash matches known values
15. Add block into the tree. There are three cases: 1. block further extends the main branch; 2. block make it become the new main branch; 3. block extends a side branch and makes it the new m
16. For case 1, adding to main branch:
  1. For all but the coinbase transaction, apply the following:
    1. For each input, look in the main branch to find the referenced output transaction
    2. For each input, if we are using the  $i$ th output of the earlier transaction, but it ha
    3. For each input, if the referenced output transaction is coinbase (i.e. only 1 input (100) confirmations; else reject.
    4. Verify crypto signatures for each input; reject if any are bad
    5. For each input, if the referenced output has already been spent by a transaction
    6. Using the referenced output transactions to get input values, check that each in
    7. Reject if the sum of input values < sum of output values
  2. Reject if coinbase value > sum of block creation fee and transaction fees

Cryptographic puzzles:  
Hard to solve - Easy to verify



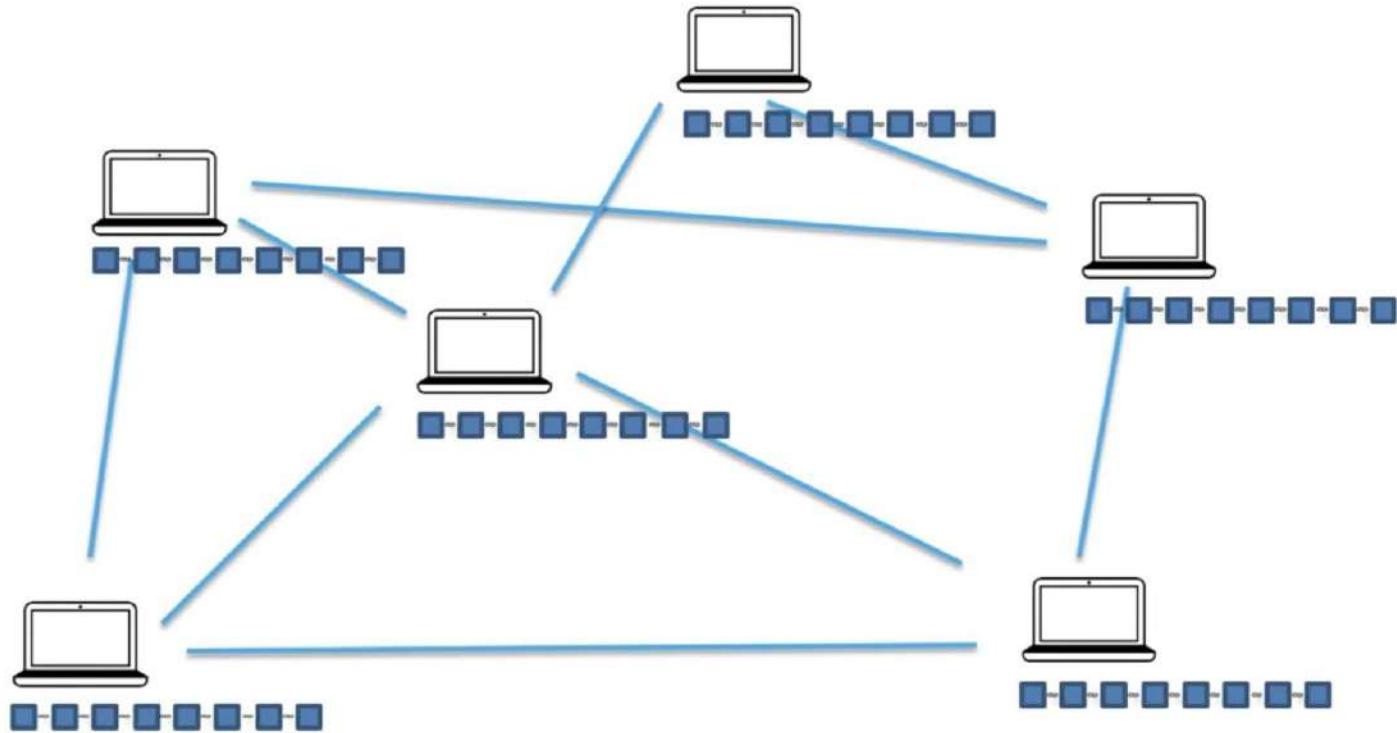
# Consensus Protocol - Attackers Challenge



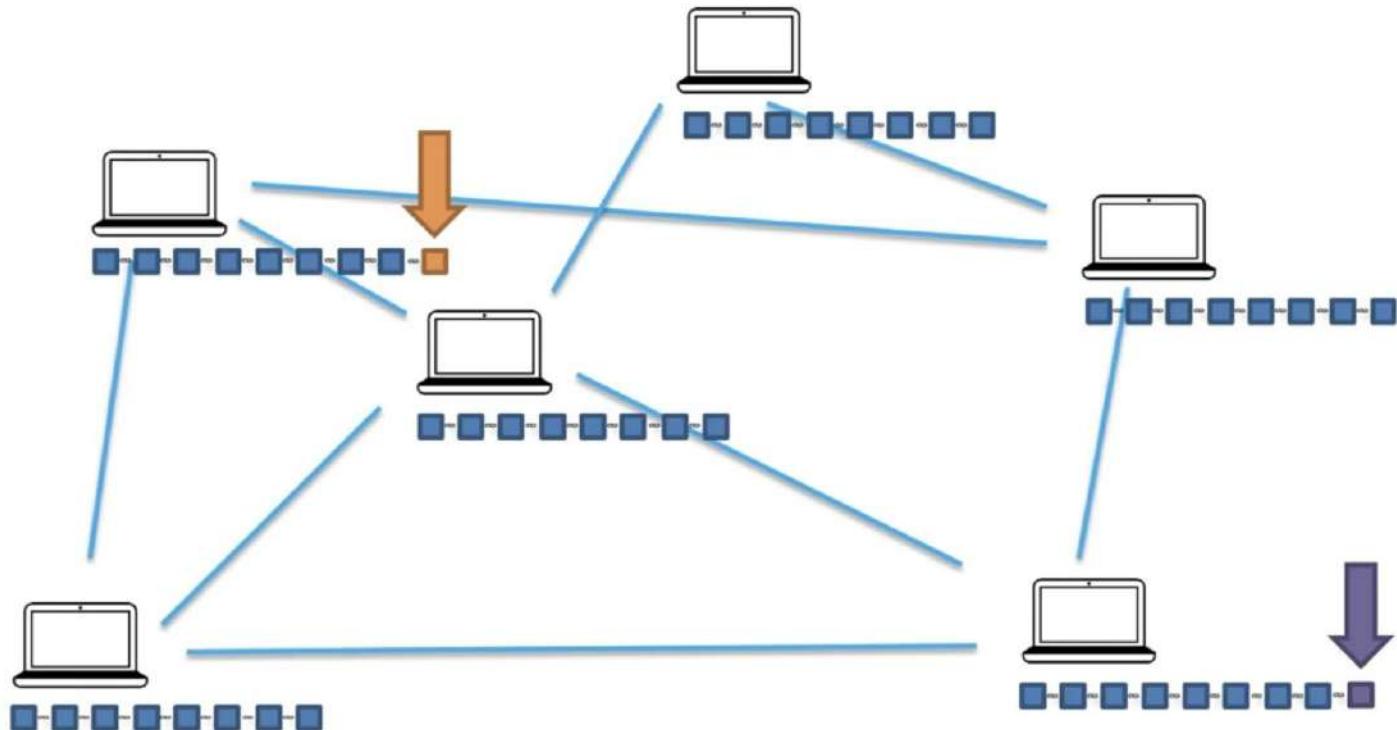
- ALL POSSIBLE HASHES -



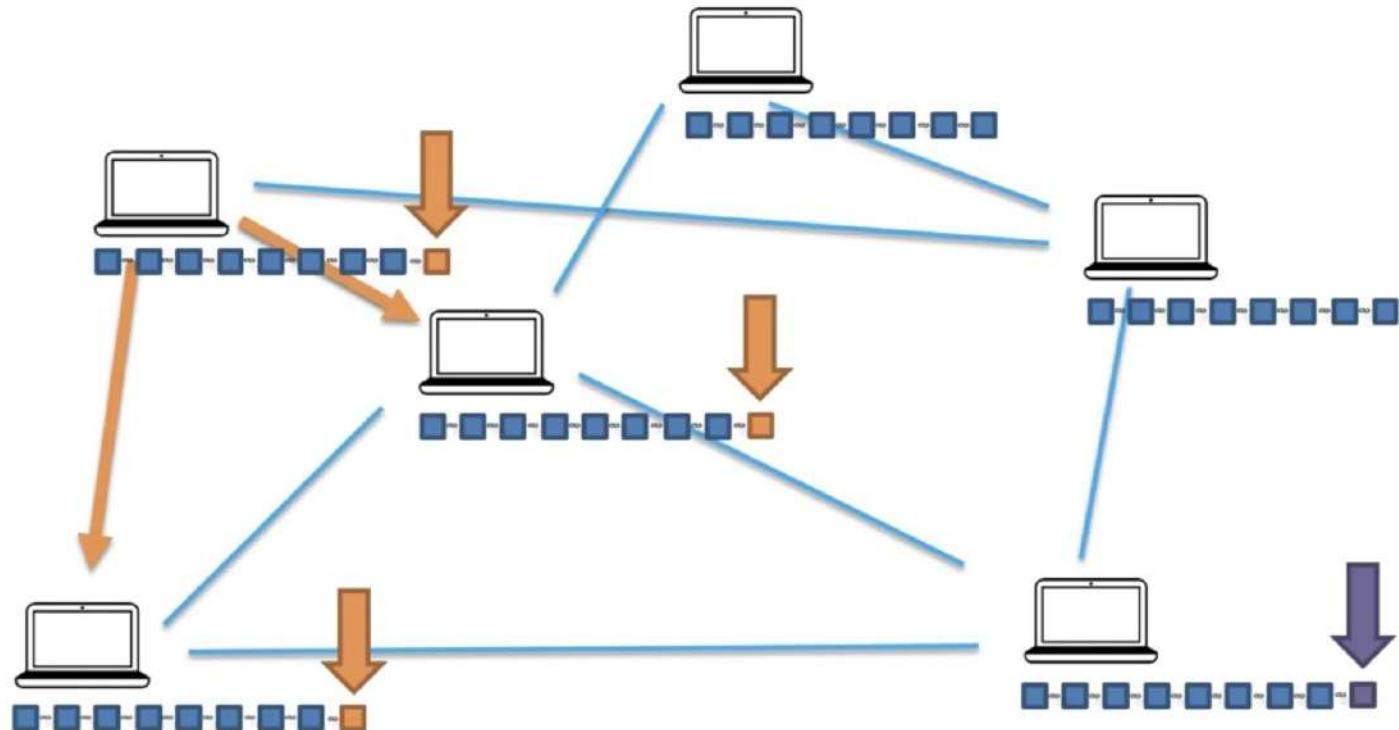
# Consensus Protocol - Competing Chains



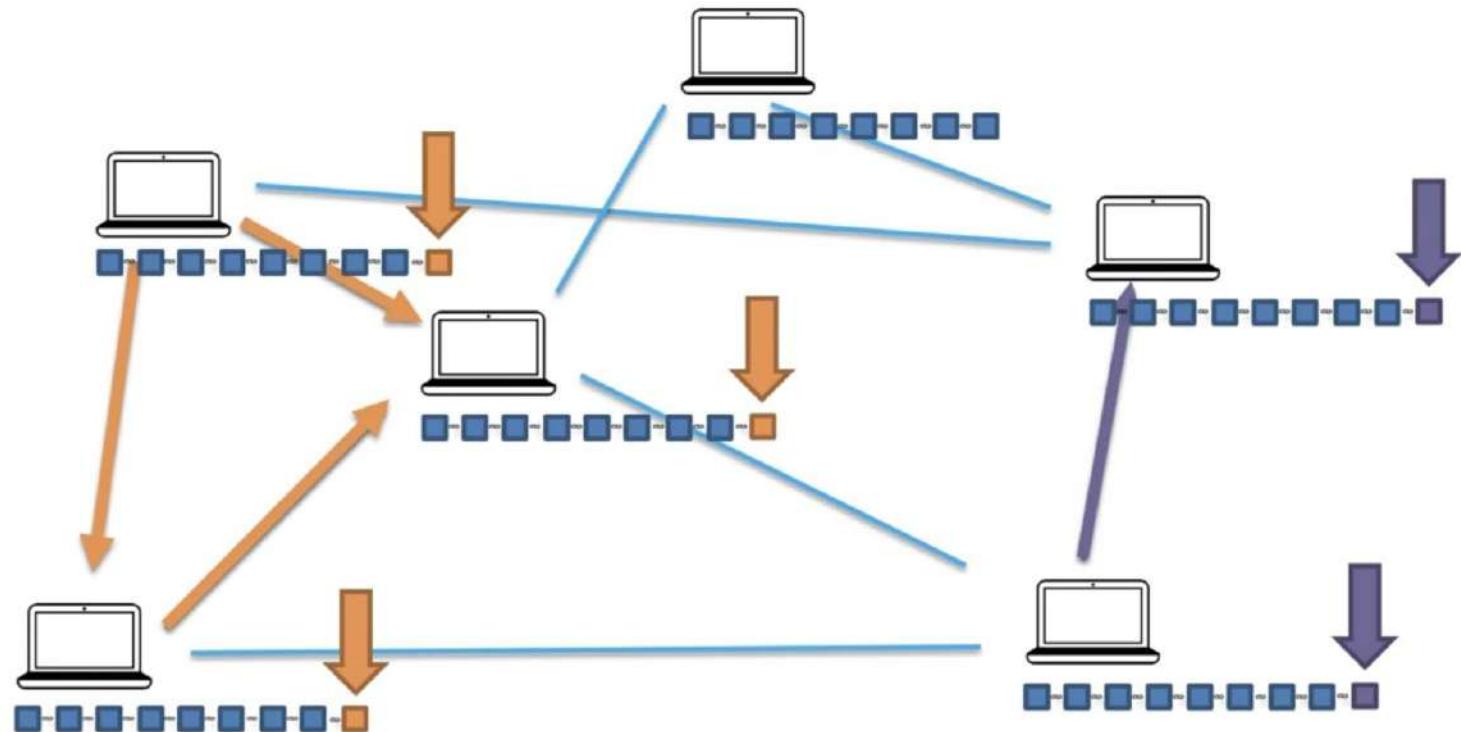
# Consensus Protocol - Competing Chains



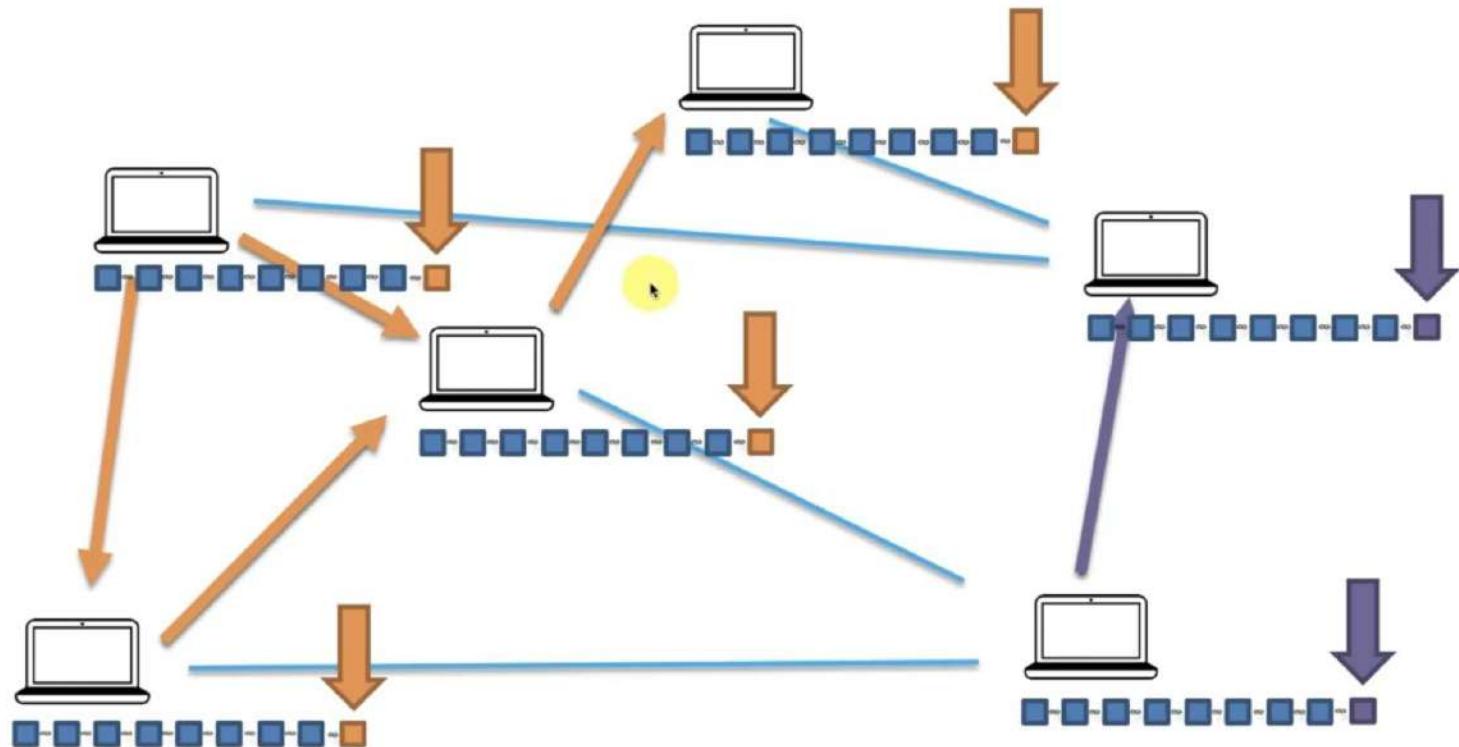
# Consensus Protocol - Competing Chains



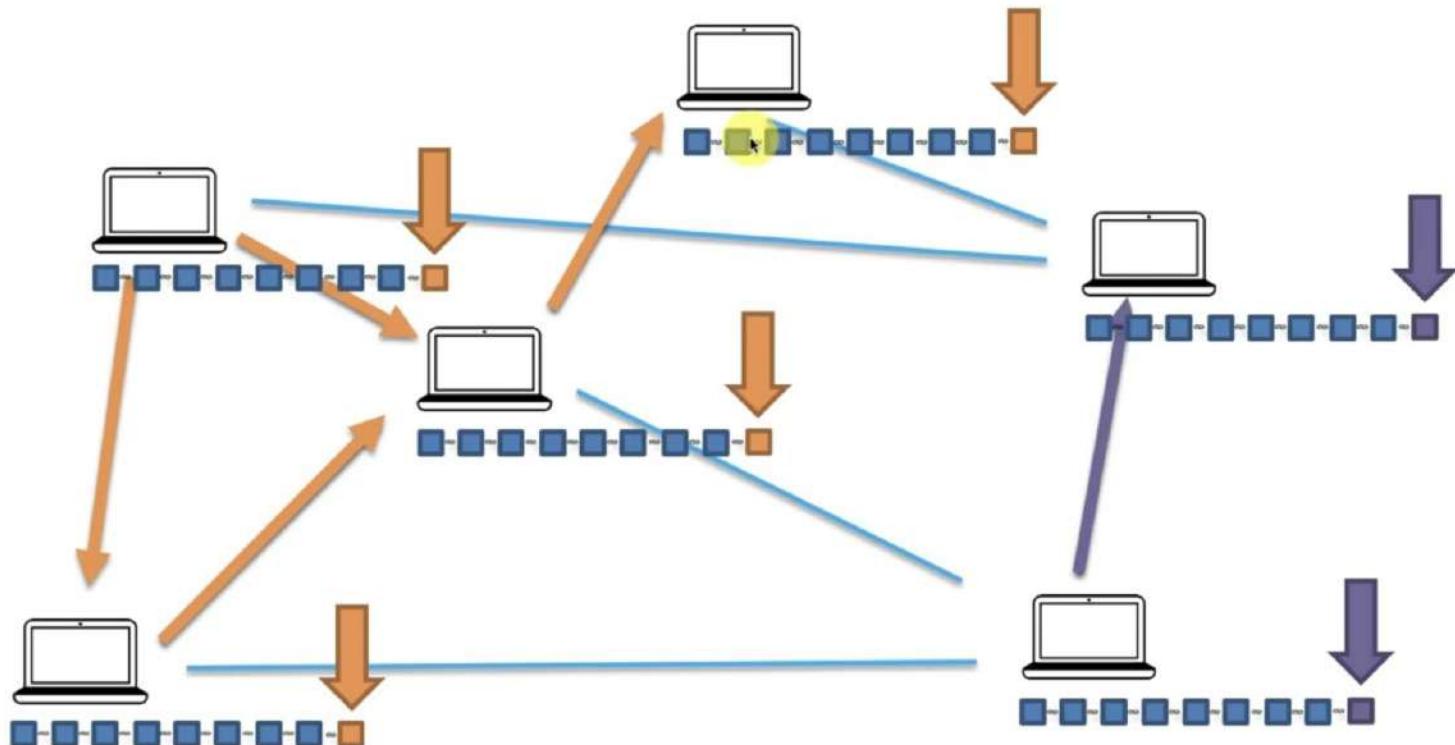
# Consensus Protocol - Competing Chains



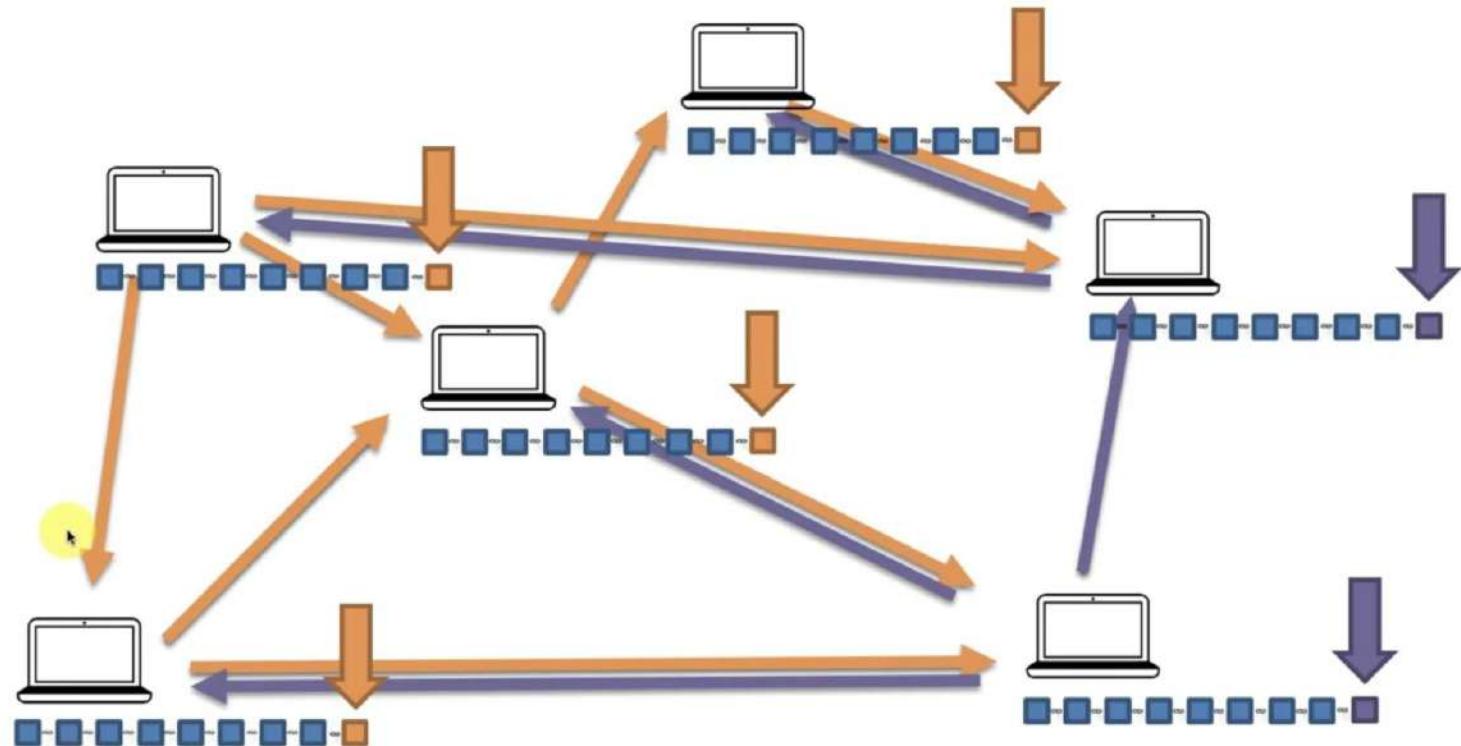
# Consensus Protocol - Competing Chains



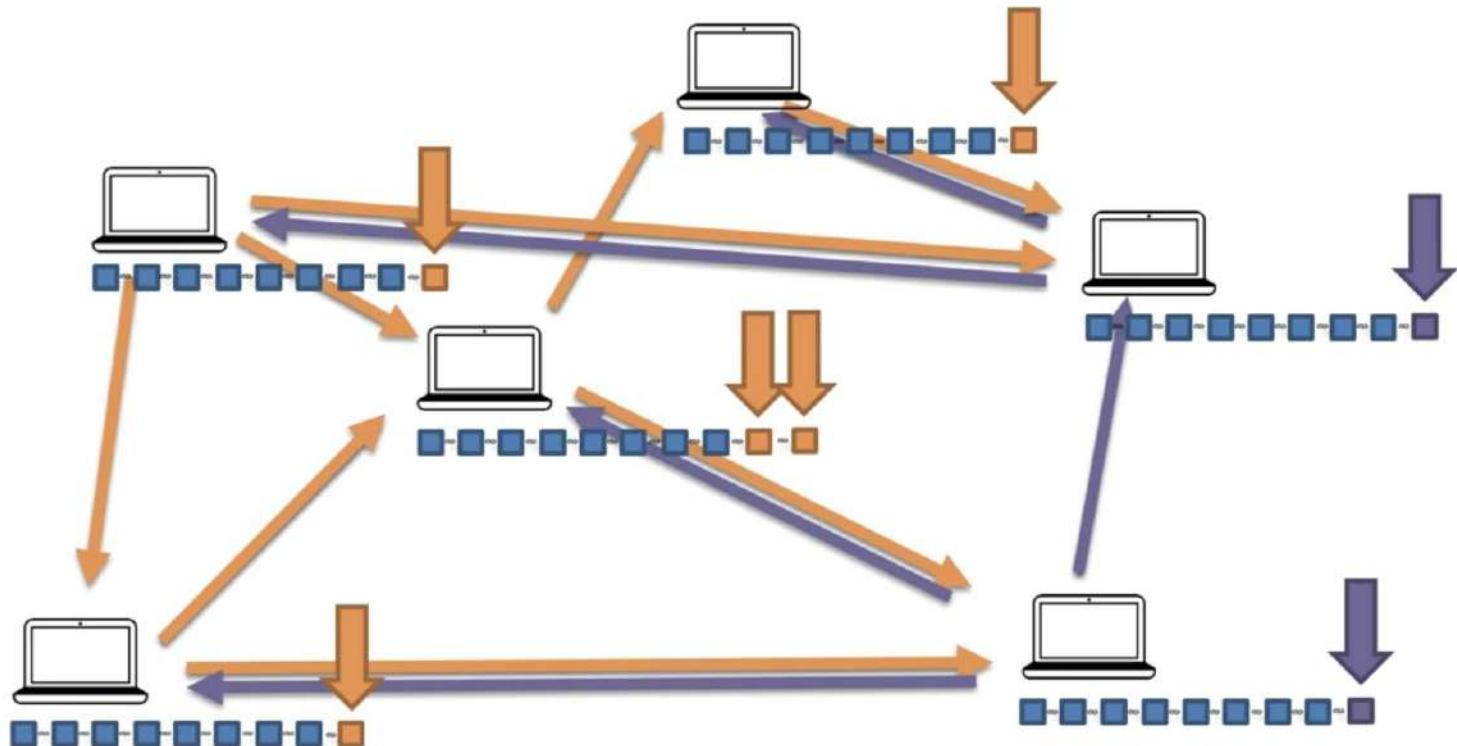
# Consensus Protocol - Competing Chains



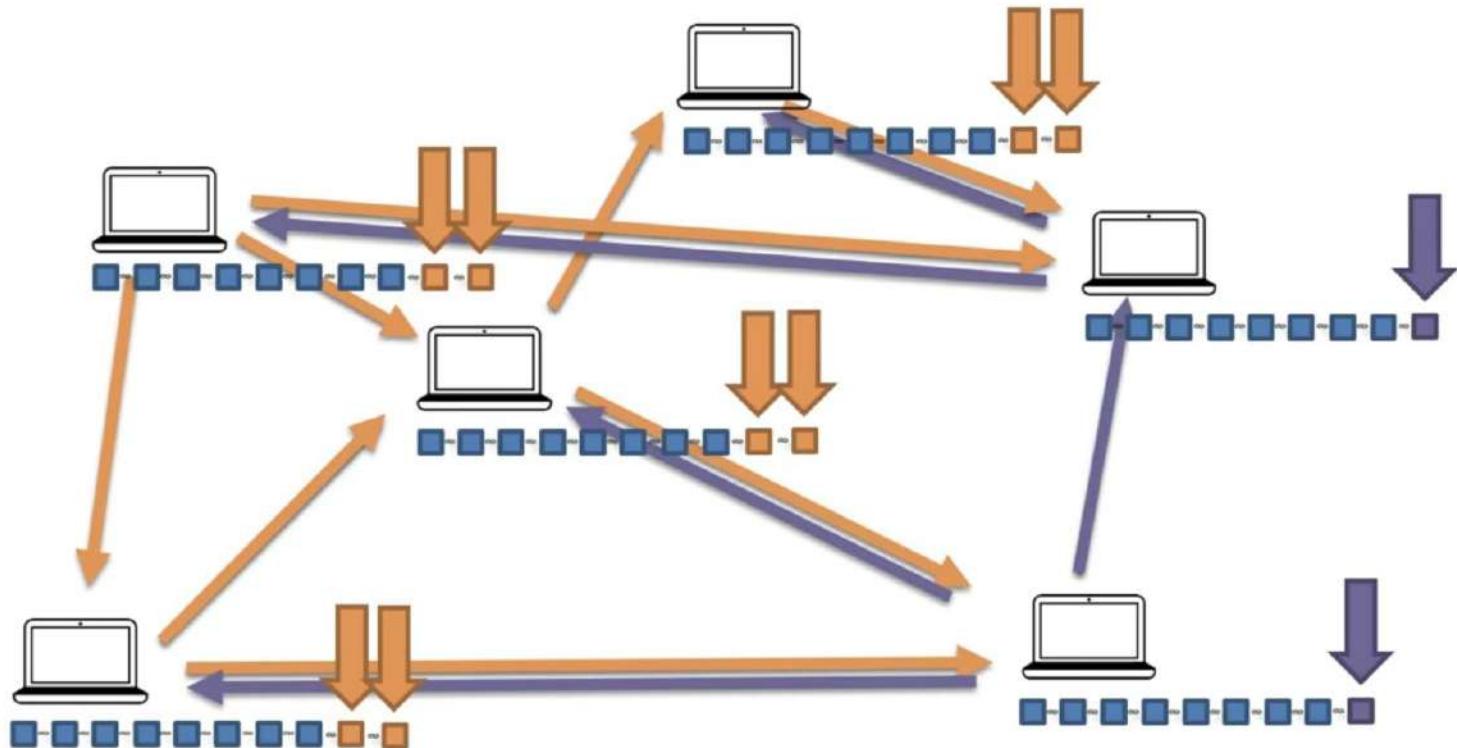
# Consensus Protocol - Competing Chains



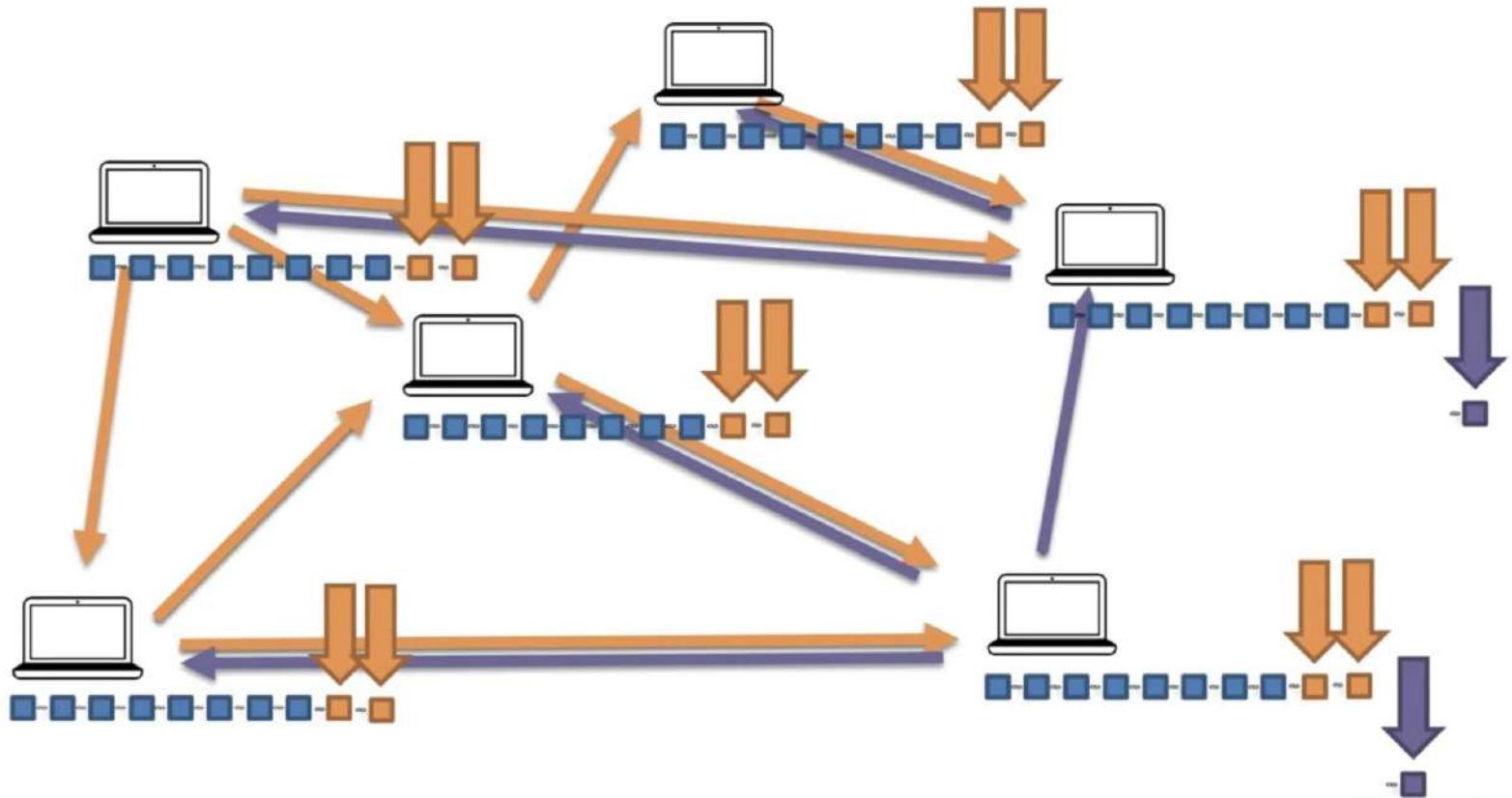
# Consensus Protocol - Competing Chains



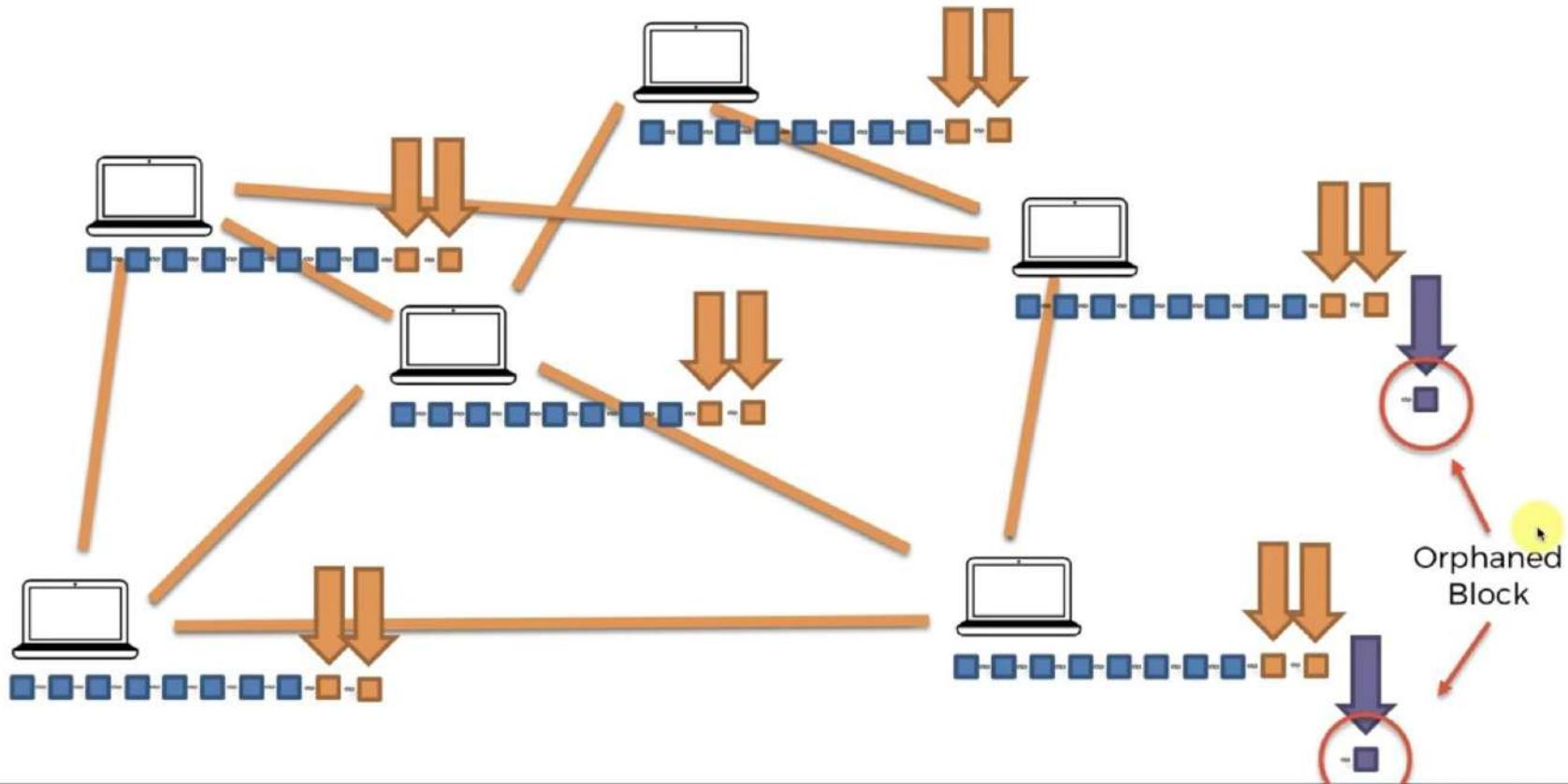
# Consensus Protocol - Competing Chains



# Consensus Protocol - Competing Chains

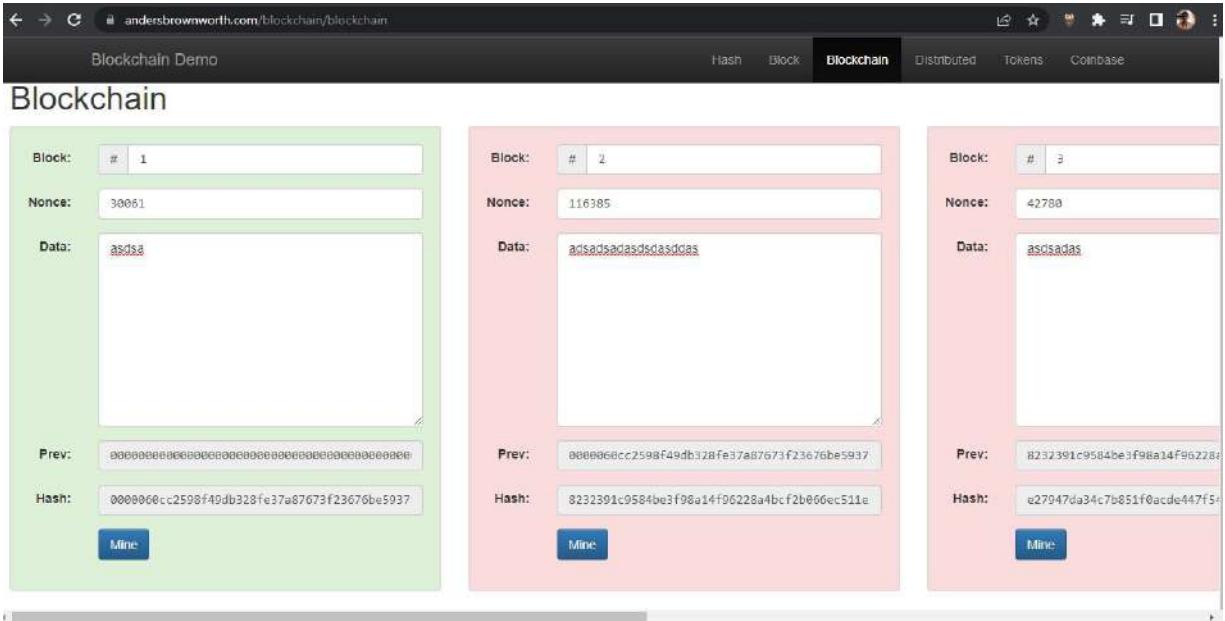


# Consensus Protocol - Competing Chains



# Blockchain - Demo

Courtesy : <https://andersbrownworth.com/blockchain/blockchain>



Block:	#	1
Nonce:	30061	
Data:	adsas	
Prev:	00	
Hash:	000000cc2598f49db328fe37a87673f23676be5937	
<button>Mine</button>		

Block:	#	2
Nonce:	116385	
Data:	adsadsadasdasdas	
Prev:	000000cc2598f49db328fe37a87673f23676be5937	
Hash:	8232391c9584be3f98a14f96228	
<button>Mine</button>		

Block:	#	3
Nonce:	42780	
Data:	ascasadas	
Prev:	8232391c9584be3f98a14f96228	
Hash:	e27947da34c7b851f0acde447f57	
<button>Mine</button>		

# Understanding Mining Difficulty

Q1: What is the Current Target  
and how does that *feel*?

# Understanding Mining Difficulty

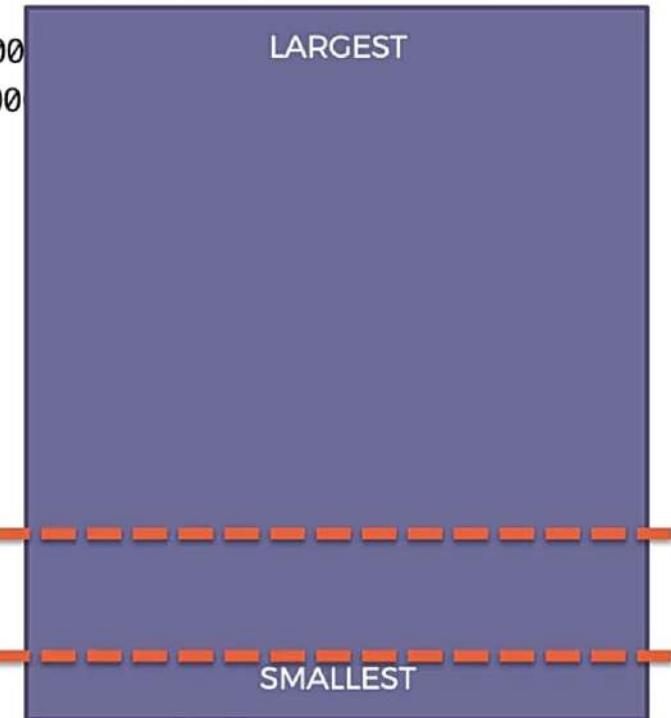
Difficulty = current target / max target

Curr target = 00000000000000005d97dc000000000000000000000000

Max target = 0000000FFFFF00

Difficulty is adjusted every 2016 blocks (2 weeks)

- ALL POSSIBLE HASHES -



# Understanding Mining Difficulty

Difficulty = current target / max target

Curr target = 00000000000000005d97dc00000000000000000000000000000000

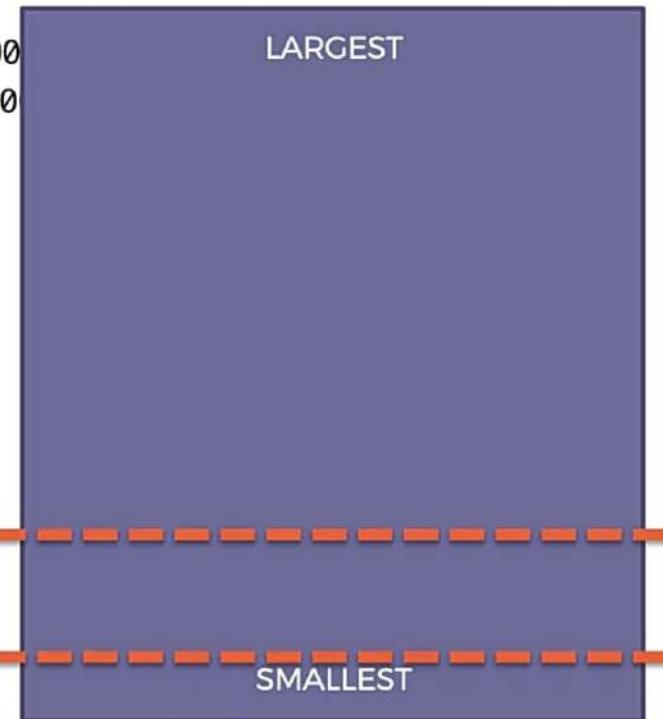
Max target = 0000000FFFFF000

Difficulty is adjusted every 2016 blocks (2 weeks)

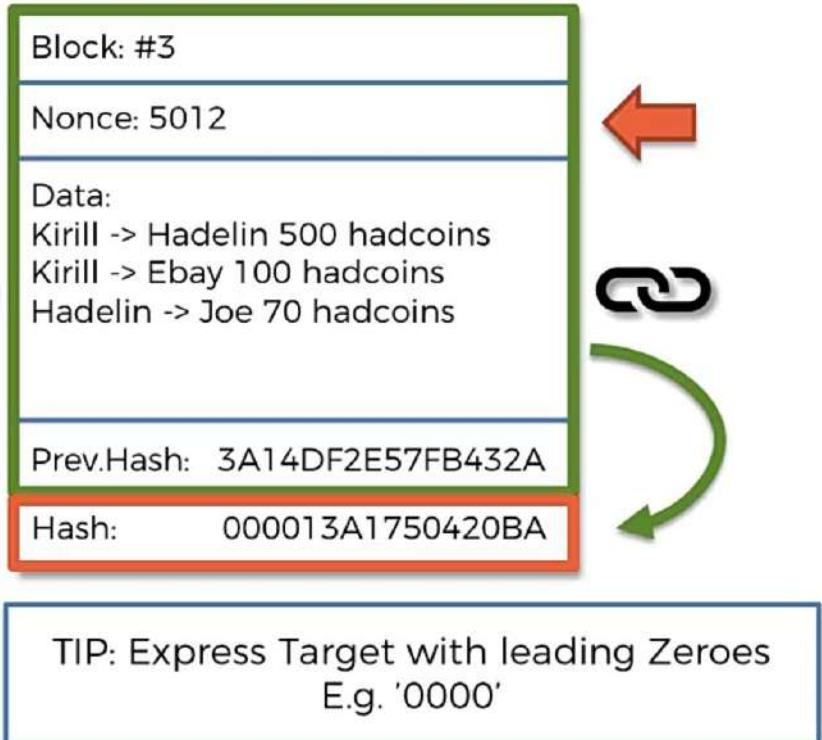
**Why 2016 ?**

# Blocks generated in 2 weeks such that one block / 10 minutes

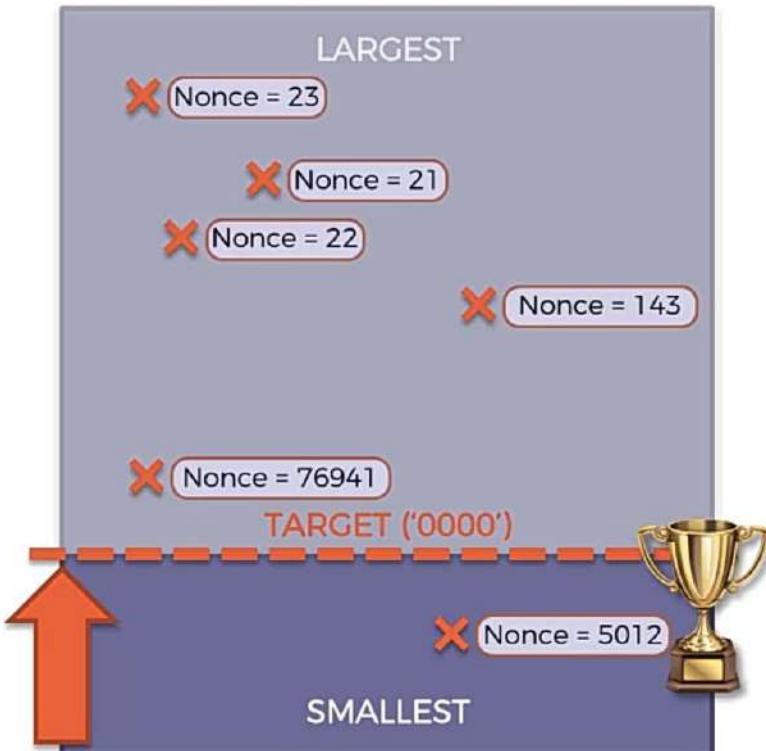
- ALL POSSIBLE HASHES -



# Understanding Mining Difficulty

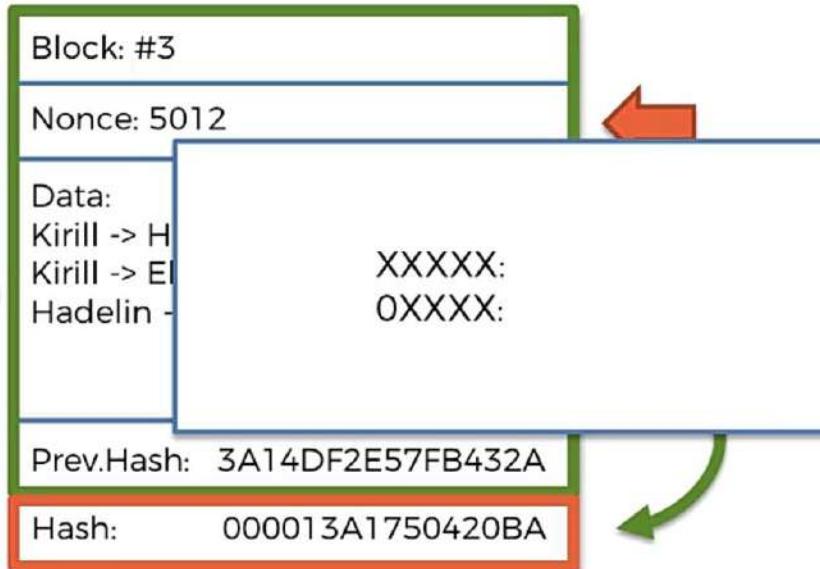


- ALL POSSIBLE HASHES -

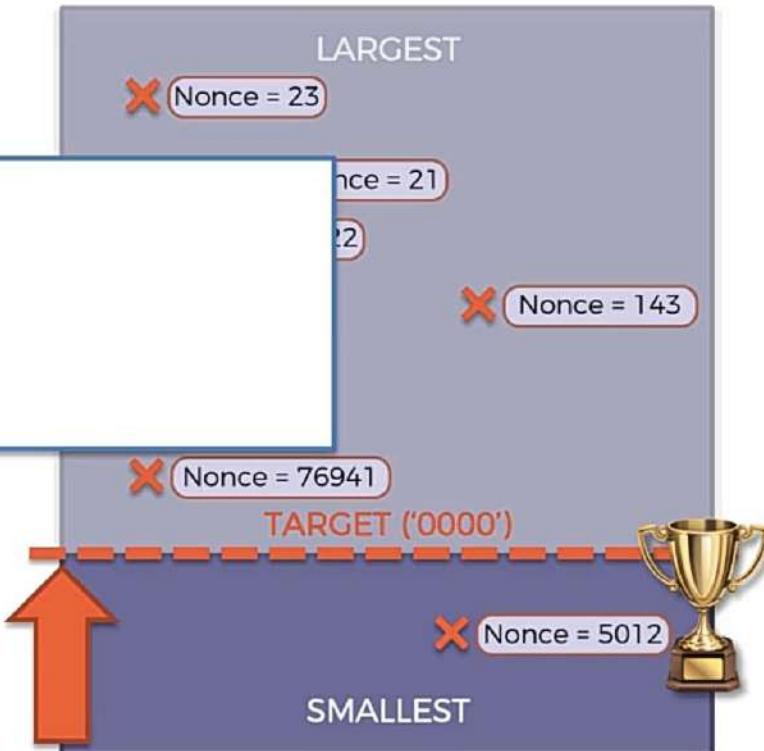


# Understanding Mining Difficulty

- ALL POSSIBLE HASHES -

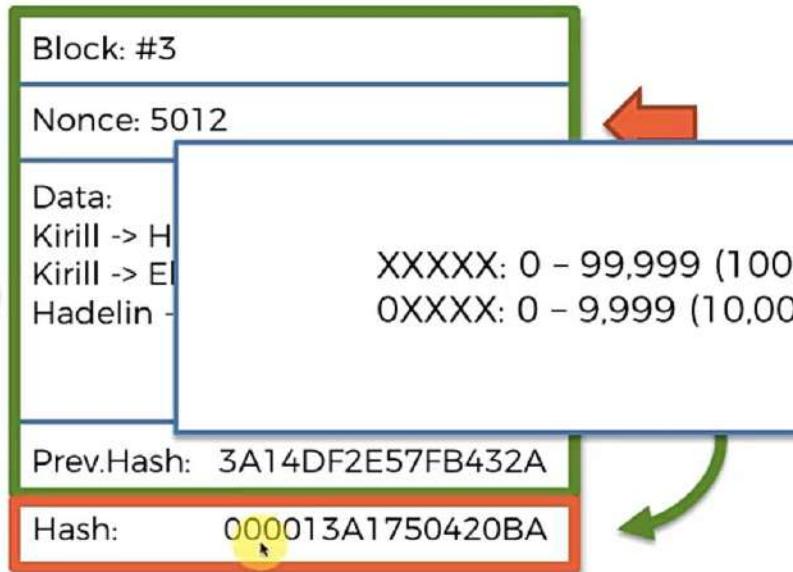


TIP: Express Target with leading Zeroes  
E.g. '0000'

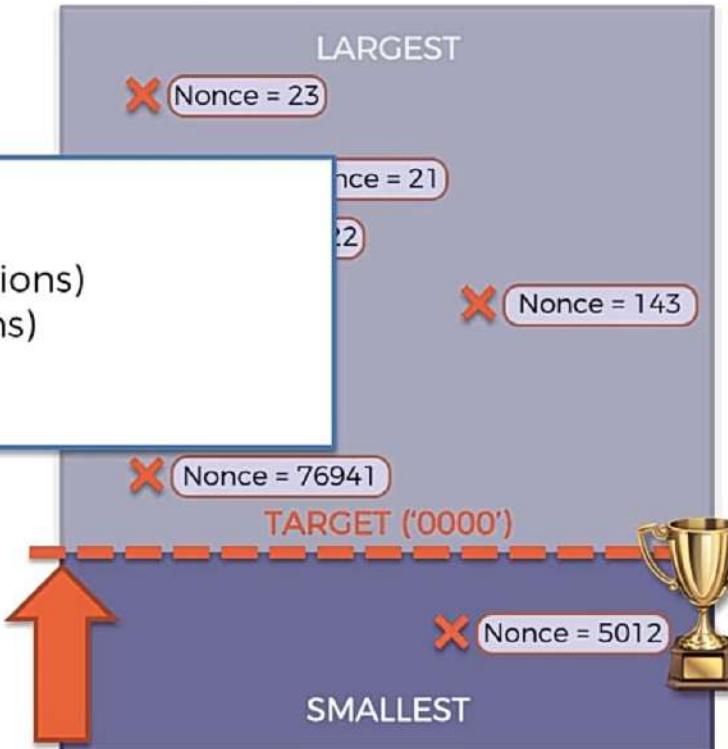


# Understanding Mining Difficulty

- ALL POSSIBLE HASHES -



TIP: Express Target with leading Zeroes  
E.g. '0000'



# Understanding Mining Difficulty

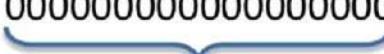
Q2: How is “Mining Difficulty” calculated?

# Understanding Mining Difficulty

Difficulty = current target / max target

Difficulty is adjusted every 2016 blocks (2 weeks)

# Understanding Mining Difficulty

Current target =  18 zeros

Let's do some estimations:

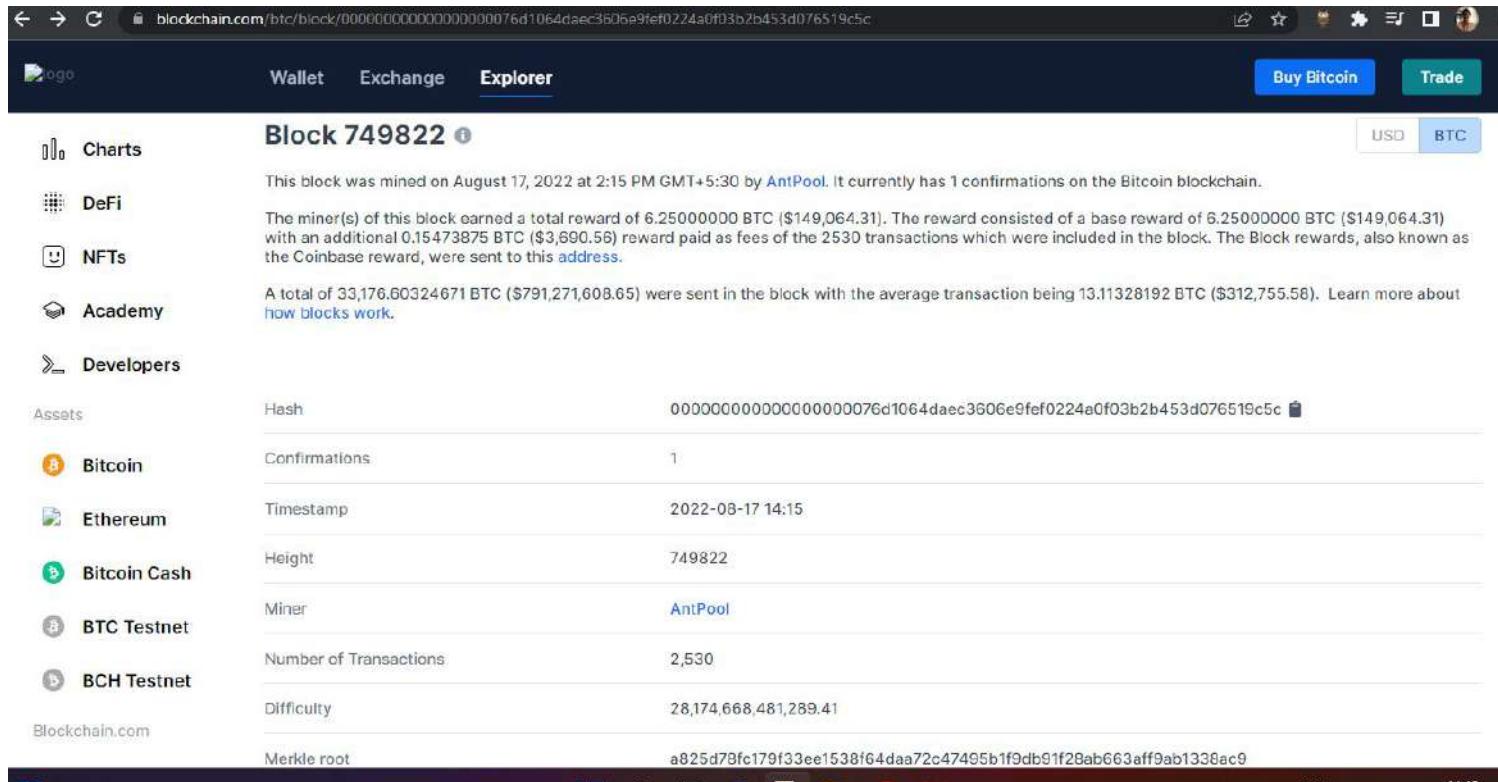
Probability:

Total possible 64-digit hexadecimal numbers:  $16 \times 16 \times \dots \times 16 = 16^{64} \approx 1.1579 \times 10^{77} \approx \underline{10^{77}}$   
Total valid hashes (with 18 leading zeros):  $16 \times 16 \times \dots \times 16 = 16^{64-18} \approx 2.4519 \times 10^{55} \approx \underline{2 \times 10^{55}}$

Probability that a Randomly picked hash is valid:  $\underline{2 \times 10^{55}} / \underline{10^{77}} = 2 \times 10^{-22} = 0.0000000000000000000002\%$

# Mining Difficulty - Demo

Courtesy : <https://www.blockchain.com/btc/block/000000000000000000000076d1064daec3606e9fef0224a0f03b2b453d076519c5c>



The screenshot shows the Blockchain.com Explorer interface for Block 749822. The block was mined on August 17, 2022, at 2:15 PM GMT+5:30 by AntPool. It currently has 1 confirmation on the Bitcoin blockchain. The miner(s) earned a total reward of 6.25000000 BTC (\$149,064.31), consisting of a base reward of 6.25000000 BTC (\$149,064.31) and an additional 0.15473875 BTC (\$3,690.56) in fees. A total of 33,176.60324671 BTC (\$791,271,608.65) were sent in the block, with an average transaction value of 13.11328192 BTC (\$312,755.58). The table below provides detailed information about the block's assets and parameters.

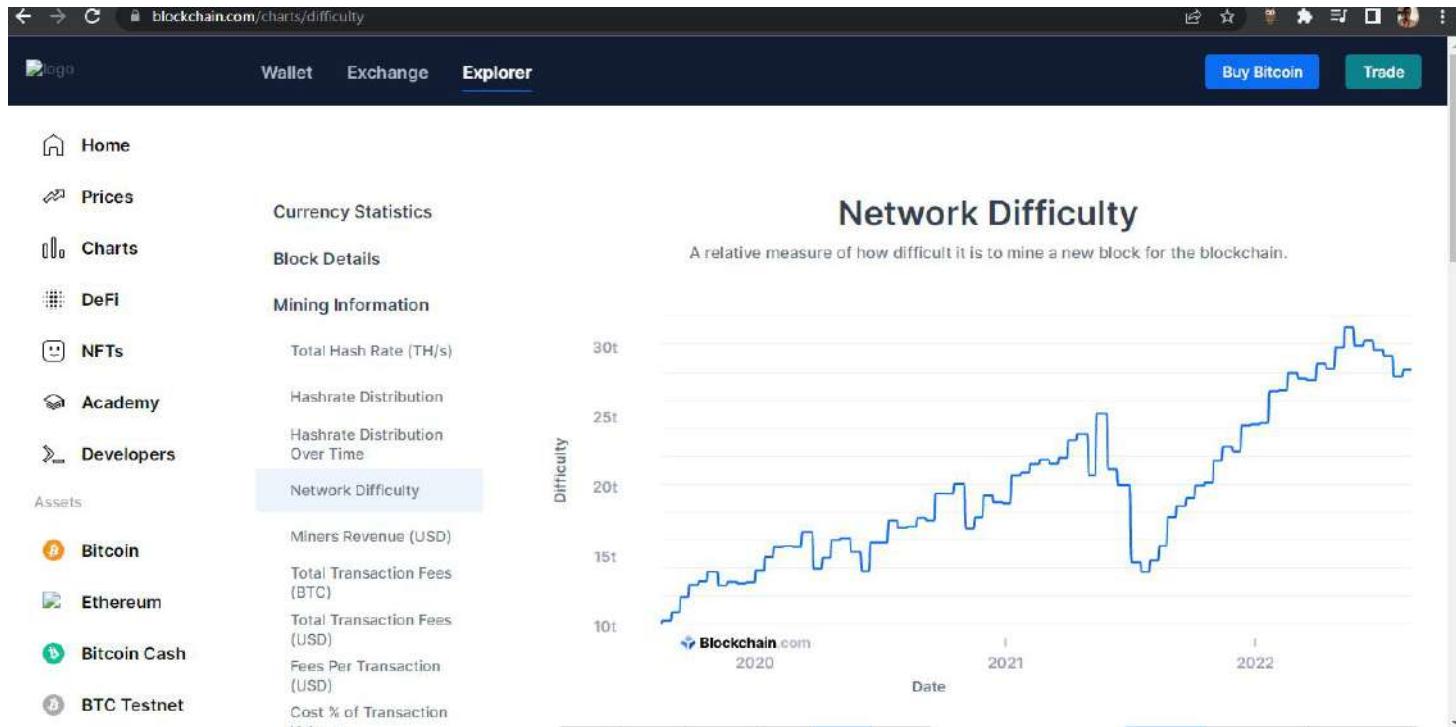
Assets	Hash
Bitcoin	000000000000000000000076d1064daec3606e9fef0224a0f03b2b453d076519c5c
Ethereum	
Bitcoin Cash	
BTC Testnet	
BCH Testnet	
Blockchain.com	

Block 749822 Details:

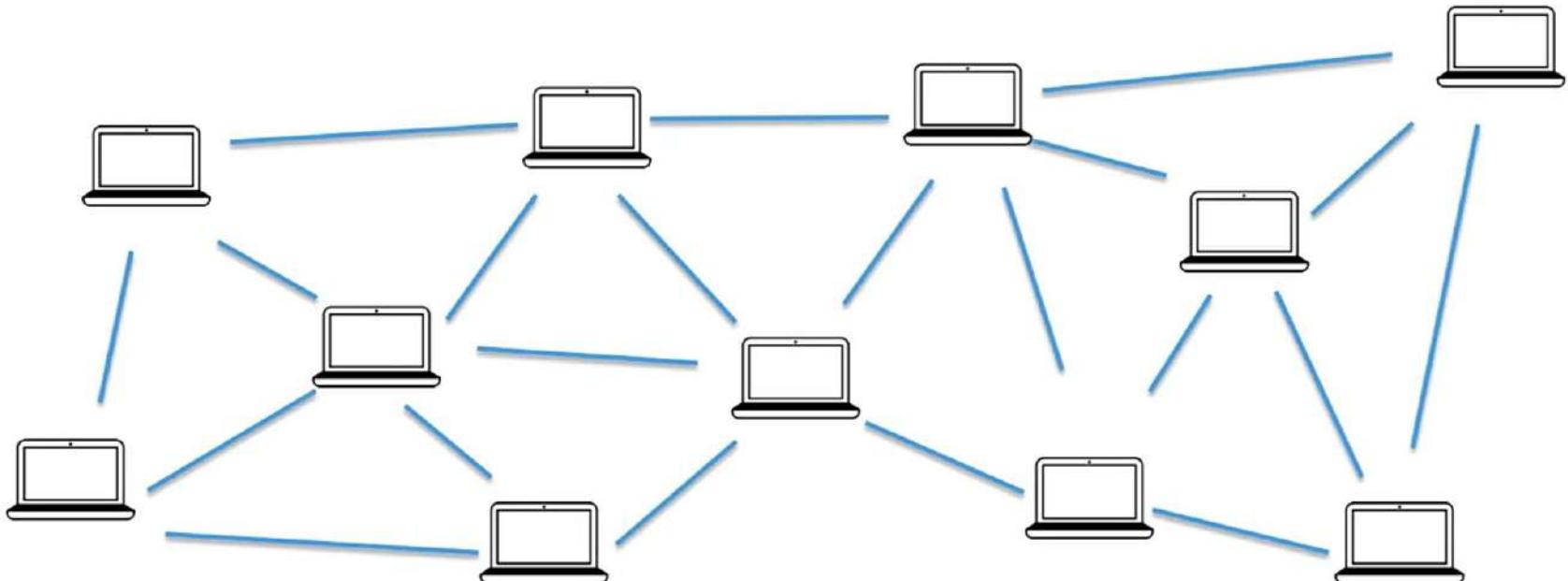
Asset	Value
Hash	000000000000000000000076d1064daec3606e9fef0224a0f03b2b453d076519c5c
Confirmations	1
Timestamp	2022-08-17 14:15
Height	749822
Miner	AntPool
Number of Transactions	2,530
Difficulty	28,174,668,481,289.41
Merkle root	a825d78fc179f33ee1538f64daa72c47495b1f9db91f28ab663aff9ab1338ac9

# Mining Difficulty - Demo

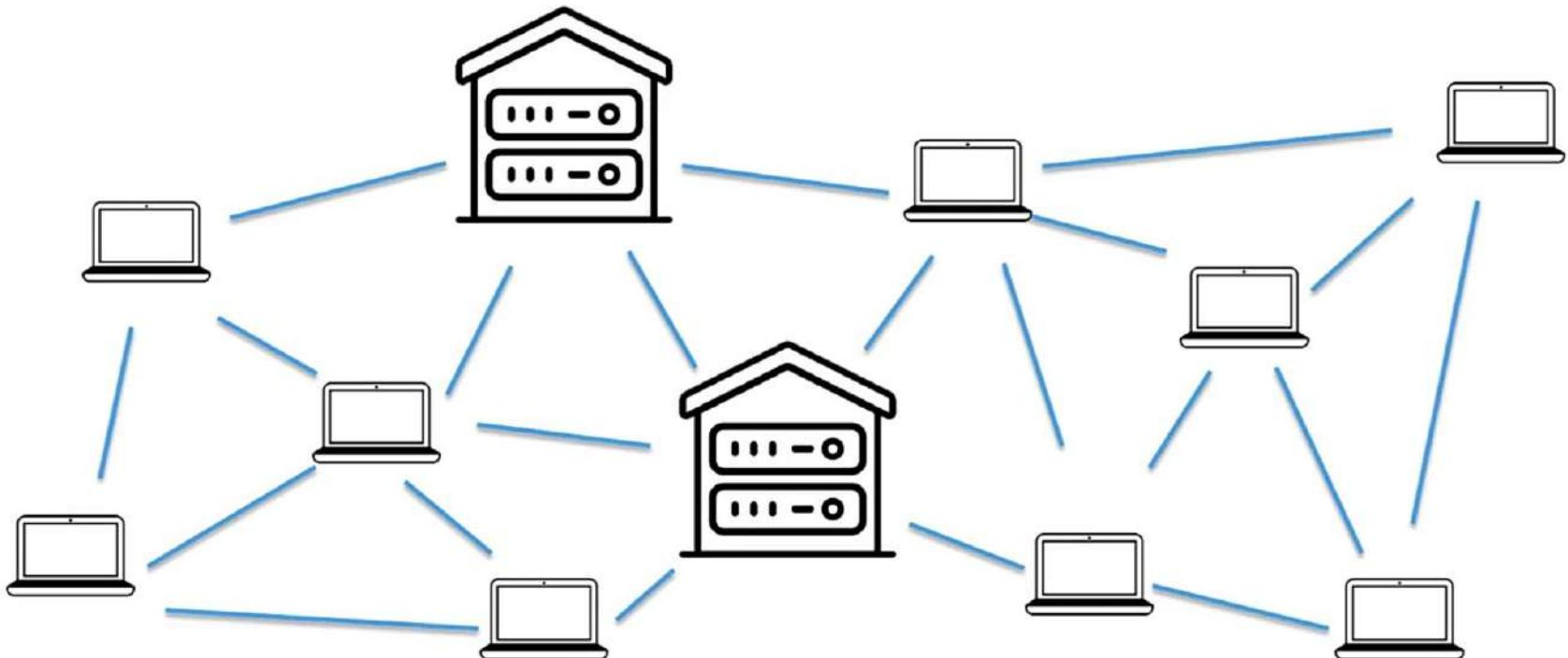
Courtesy : <https://www.blockchain.com/charts/difficulty>



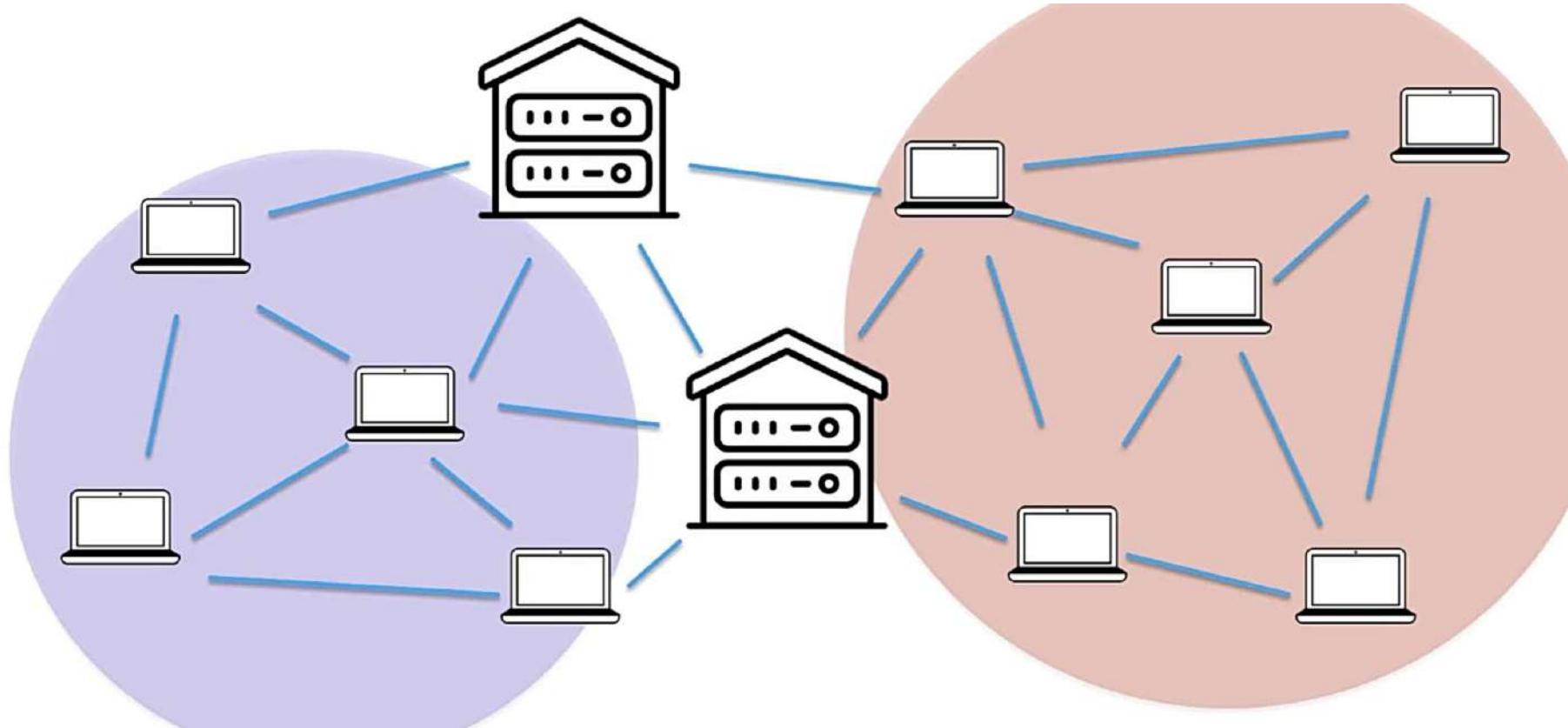
# Mining Pools



# Mining Pools



# Mining Pools



# Mining Pools

Hi! Sign in or register | Daily Deals | Gift Cards | Help & Contact [Turn Your Tax Refund Into Fun](#)

Sell | My eBay [Bell](#) [Cart](#)

**ebay** Shop by category  All Categories [Search](#) Advanced

eBay > Coins & Paper Money > Virtual Currency > Miners [Share](#)

## Cryptocurrency GPU Mining Rig 3x GTX 1080 TI Ethereum Zcash Bitcoin Extras

★★★★★ 2 product ratings | [About this product](#)



New (other): lowest price

**\$5,599.00**  
+ \$549.95 Shipping

Get it by Mon, Mar 5 - Thu, Apr 12 from New Baltimore, Michigan

- New other (see details) condition
- No returns, but backed by [eBay Money back guarantee](#)

"New  
Easily Mine Zcash or Other Equihash Coins at 2250 Sol/s (2250 h/s) @ 890W. Mine Zcash (ZEC), Bitcoin Gold (BTG),..."  
[Read full description](#)

[See details >](#)

Qty : 1

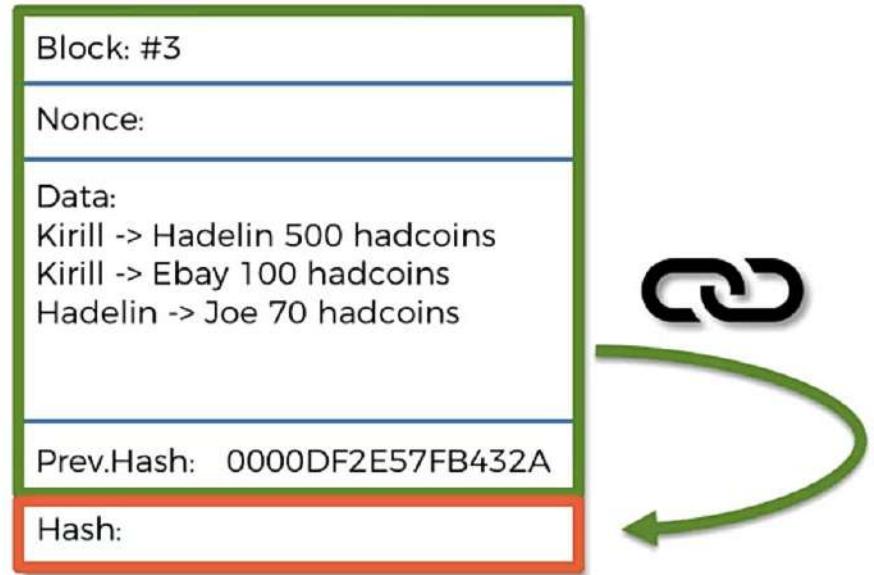
[Buy It Now](#)

[Add to cart](#)

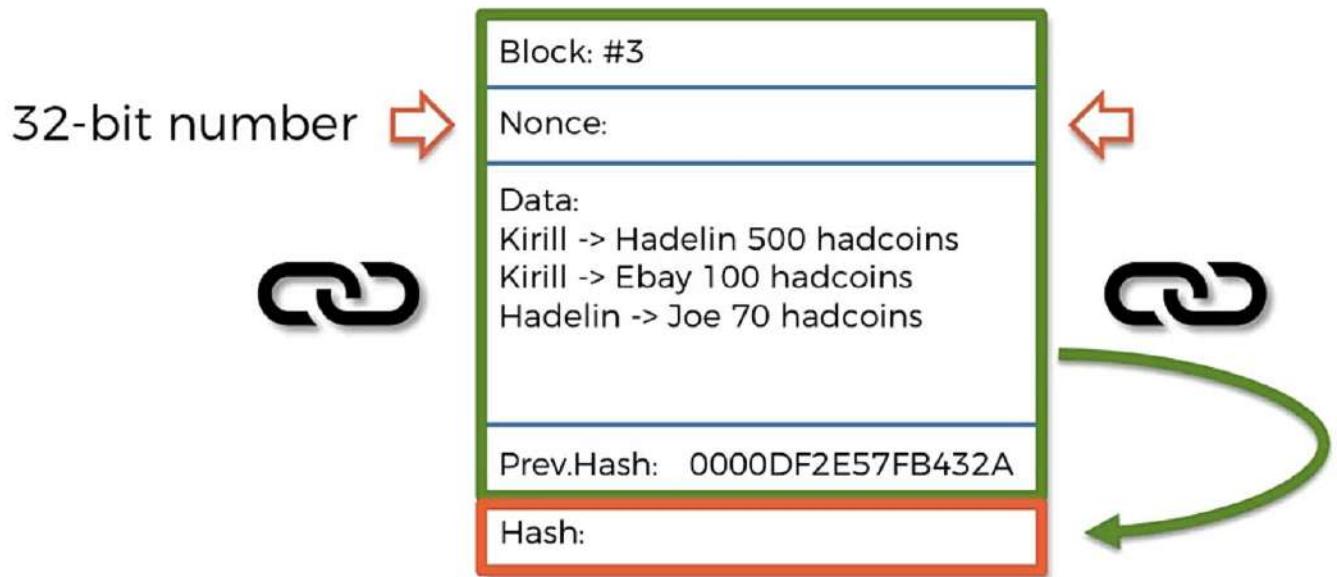
[Watch](#)

Sold by [partdiscounter \(42407\)](#)  
99.8% Positive feedback

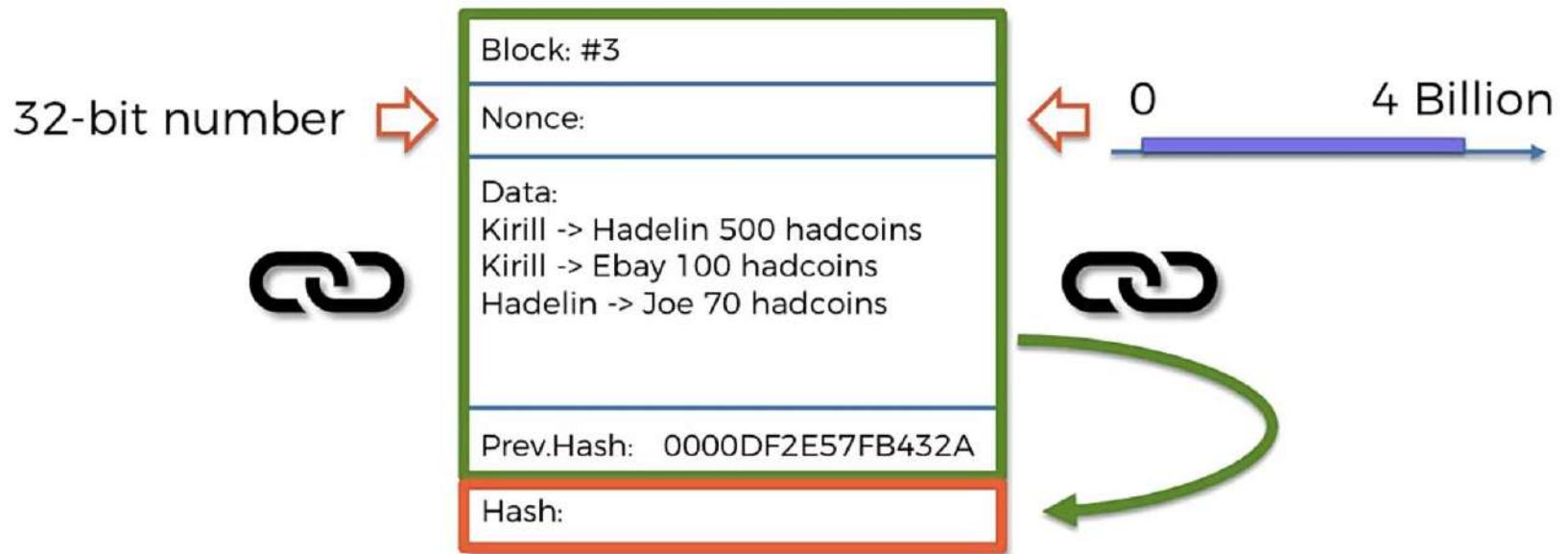
# Nonce Range



# Nonce Range

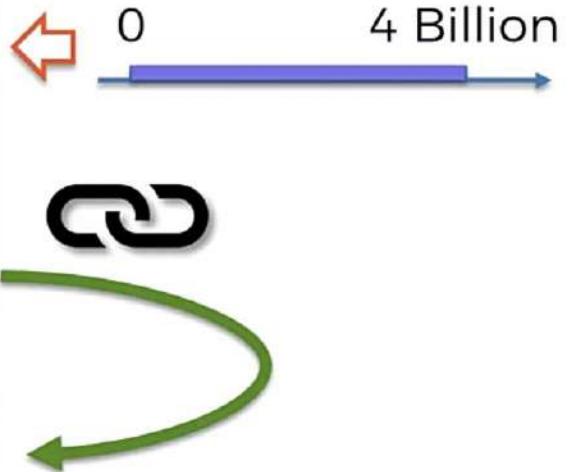
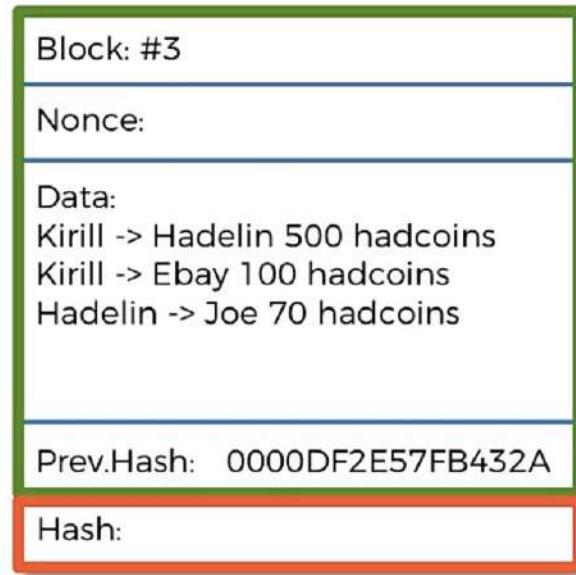


# Nonce Range



# Nonce Range

32-bit number  
(unsigned)



# Nonce Range

Let's do some estimations:

Difficulty:

Total possible 64-digit hexadecimal numbers:  $16 \times 16 \times \dots \times 16 = 16^{64} \approx 10^{77}$

Total valid hashes (with 18 leading zeros):  $16 \times 16 \times \dots \times 16 = 16^{64-18} \approx 2 \times 10^{55}$

Probability that a Randomly picked hash is valid:  $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.0000000000000000000002\%$

Nonce:

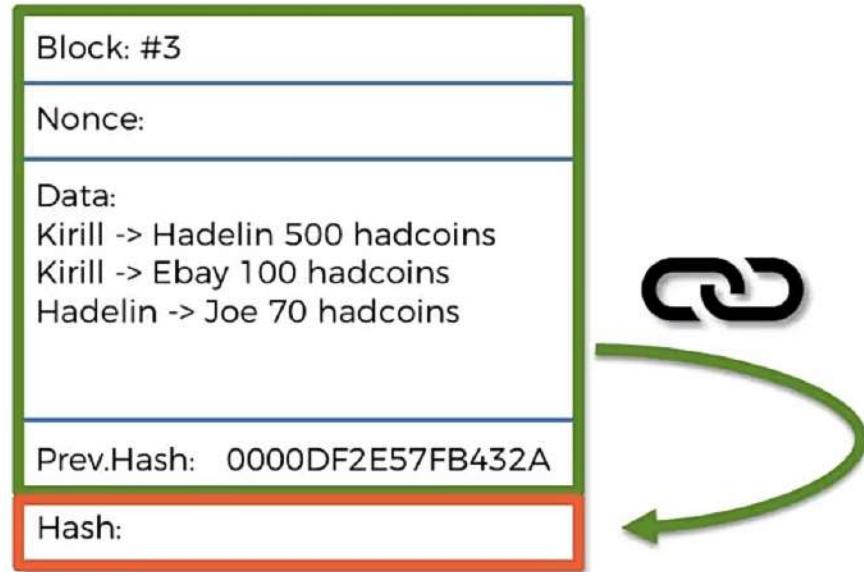
The Nonce is a 32-bit number, the Max Nonce =  $2^{32} = 4,294,967,296 = 4 \times 10^9$

Assuming no collisions, this means  $4 \times 10^9$  different hashes

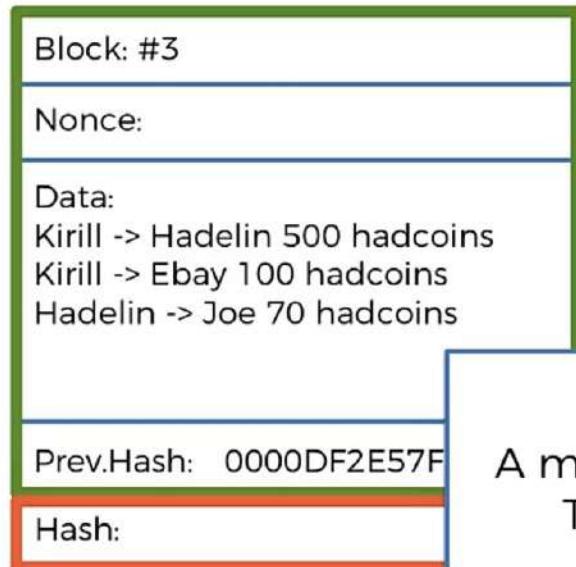
Probability that ONE of them will be valid:  $4 \times 10^9 \times 2 \times 10^{-22} = 8 \times 10^{-13} \approx 10^{-12} = 0.0000000001\%$

Conclusion: One Nonce Range is not enough

# Nonce Range



# Nonce Range

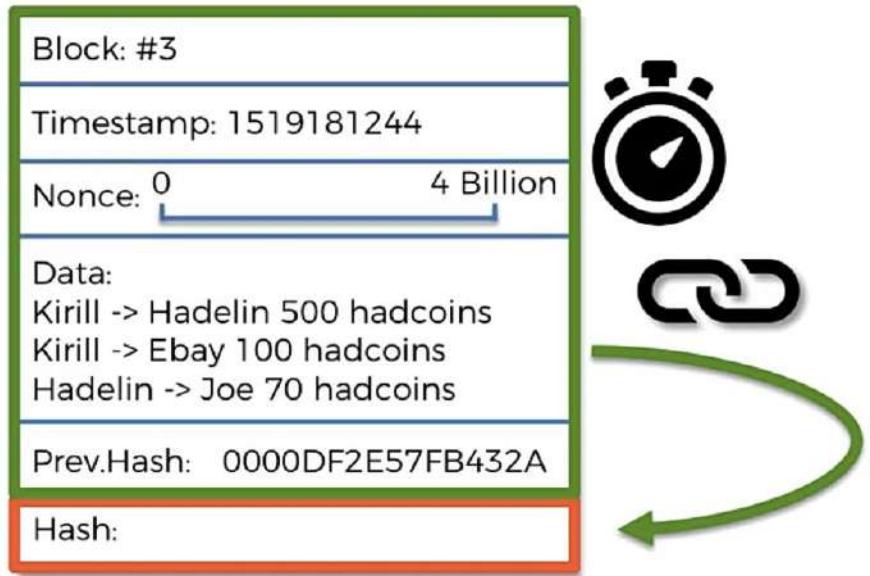


A modest miner does 100 MH/s  
That's 100 Million Hashes  
 $4\text{ Billion} / 100\text{ Million} = 40\text{ seconds}$

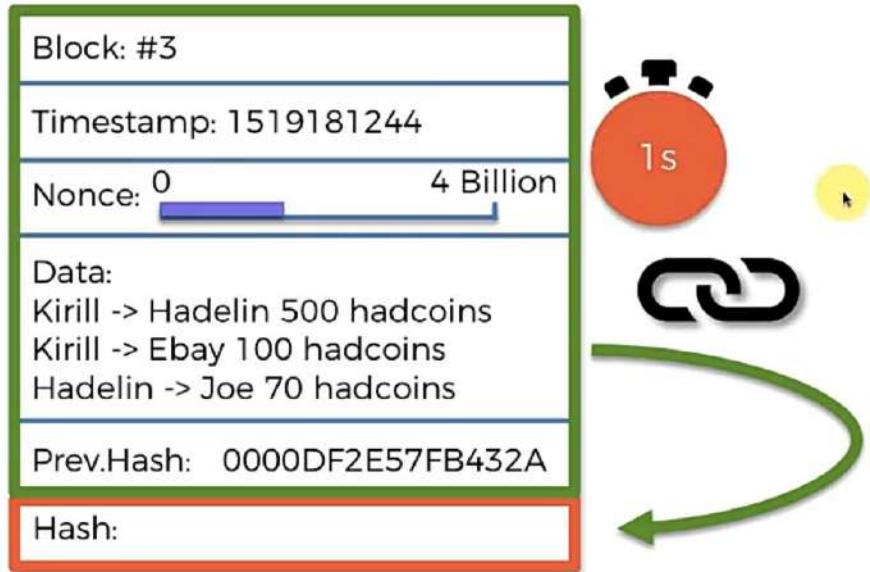
# Nonce Range



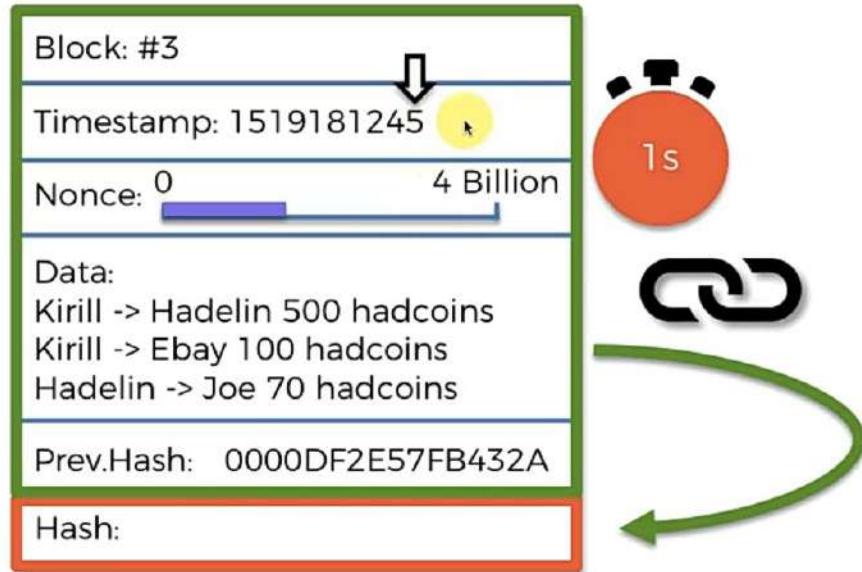
# Nonce Range



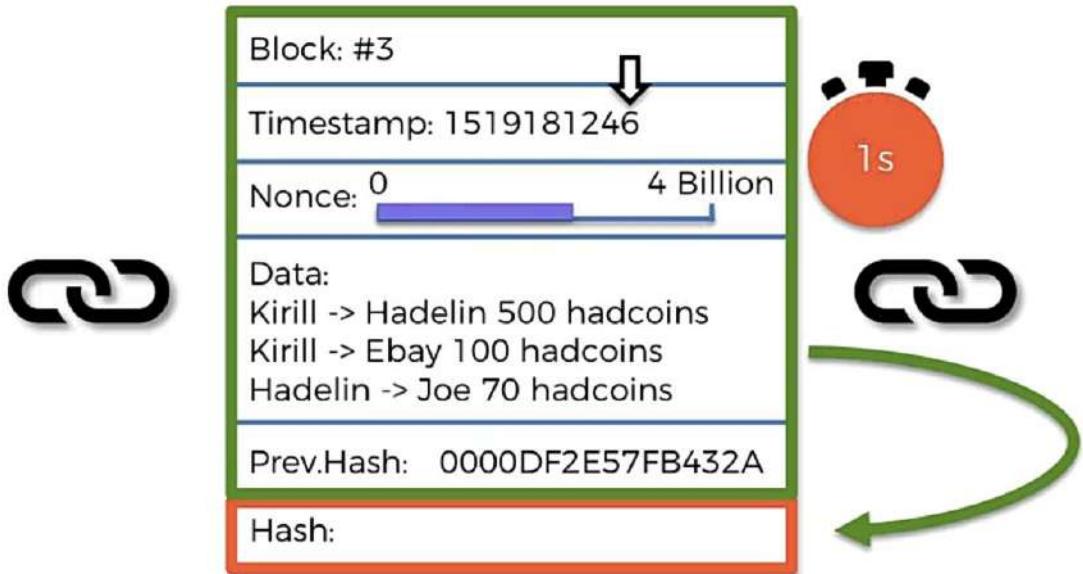
# Nonce Range



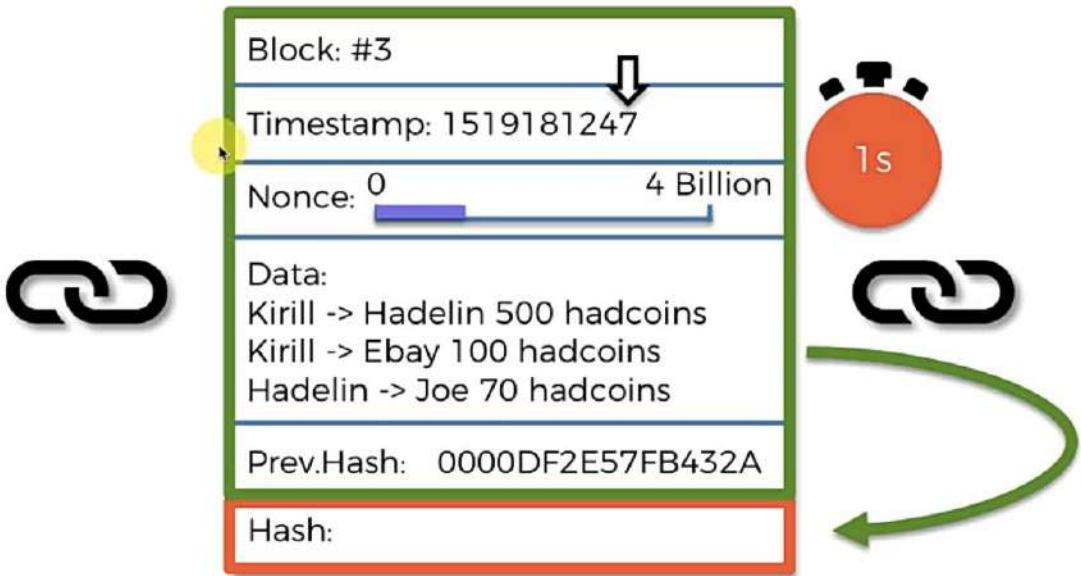
# Nonce Range



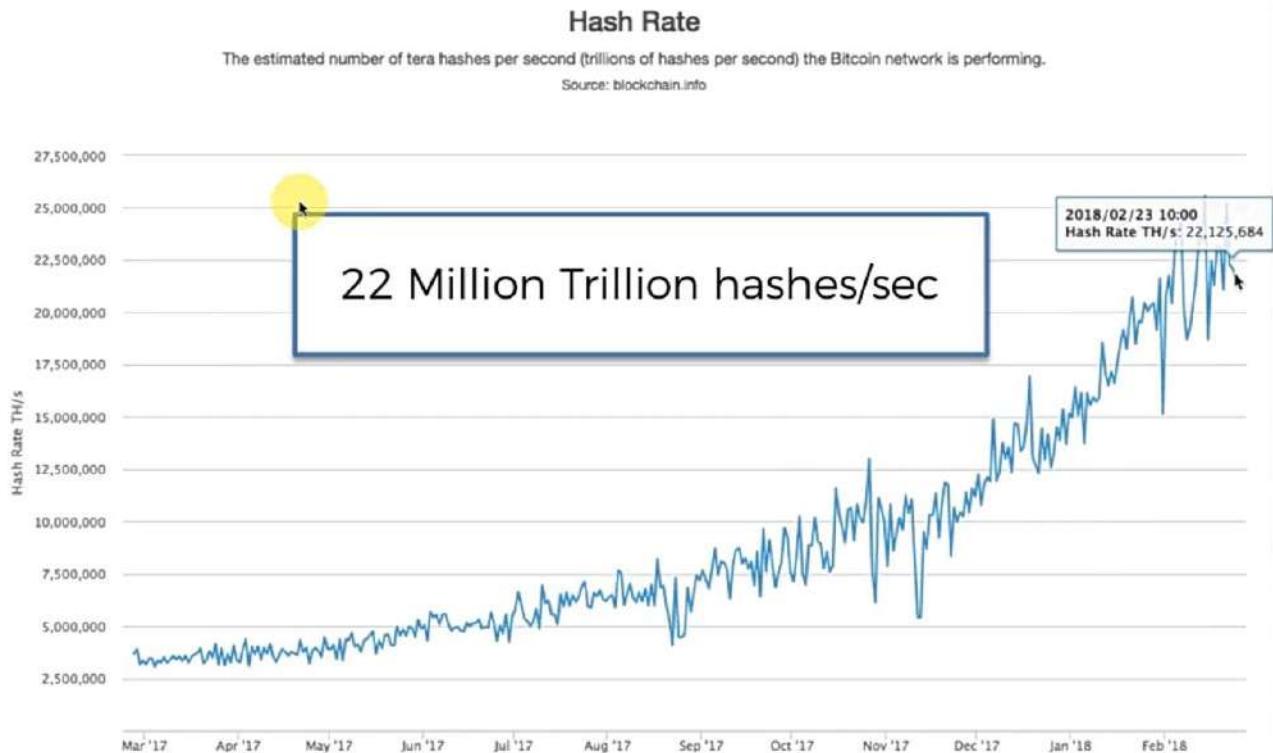
# Nonce Range



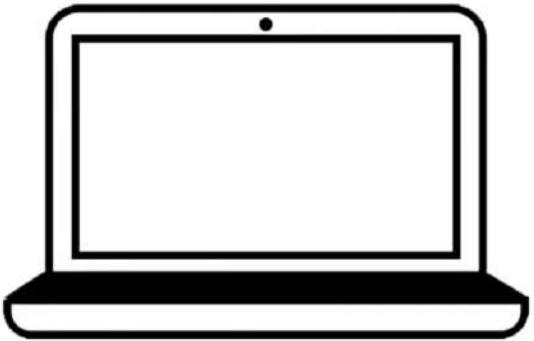
# Nonce Range



# Nonce Range



# How Miners Pick Transactions ?

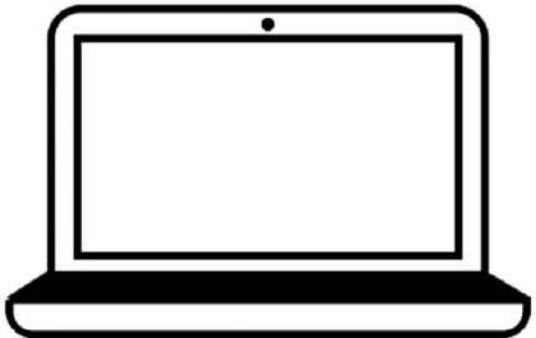


(Mining in Process)

Block: #500,112
Timestamp: 1519181244
Nonce:
Data:
Prev.Hash: 0000DF2E57FB432A
Hash:

# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC

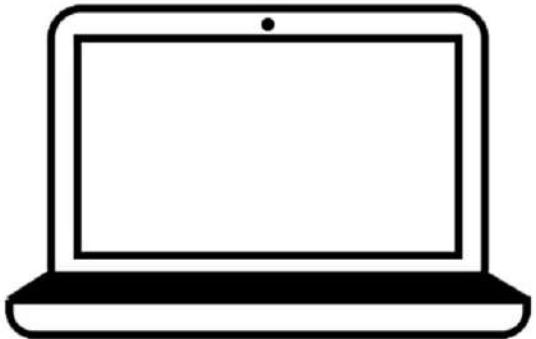


(Mining in Process)

Block: #500,112
Timestamp: 1519181244
Nonce:
Data:
Prev.Hash: 0000DF2E57FB432A
Hash:

# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC

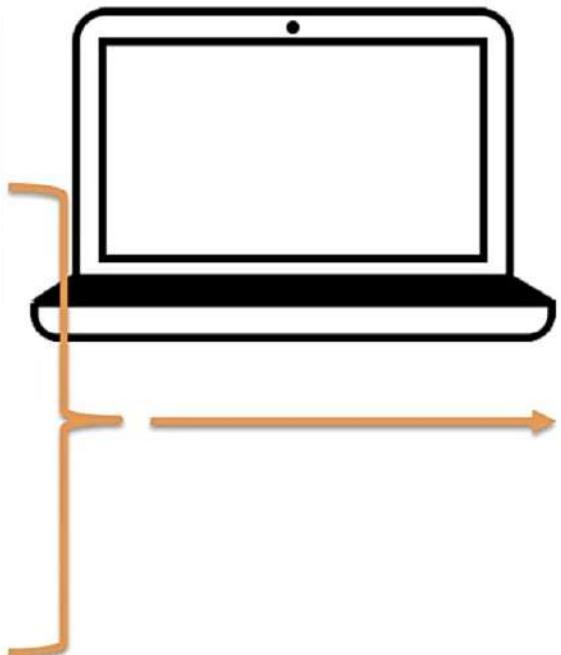


(Mining in Process)

Block: #500,112
Timestamp: 1519181244
Nonce:
Data:
Prev.Hash: 0000DF2E57FB432A
Hash:

# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC

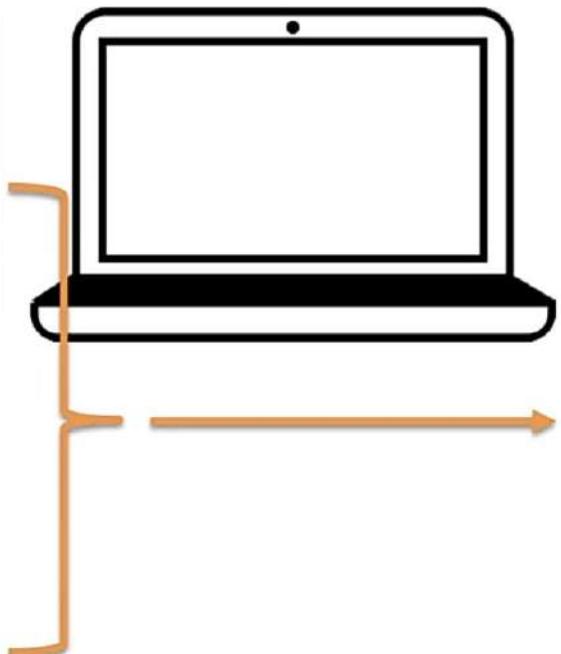


(Mining in Process)

Block: #500,112	↓
Timestamp: 1519181245	1s
Nonce: 0	4 Billion
Data:	
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
85C19D7	Fees: 0.0017 BTC
Prev.Hash: 0000DF2E57FB432A	
Hash:	

# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC

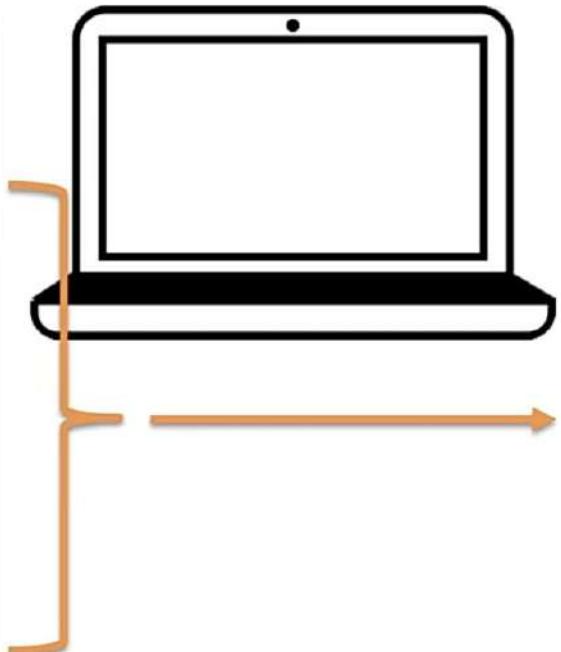


(Mining in Process)

Block: #500,112	
Timestamp: 1519181246	
Nonce: 0	4 Billion
Data:	
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
85C19D7	Fees: 0.0017 BTC
Prev.Hash: 0000DF2E57FB432A	
Hash:	

# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC

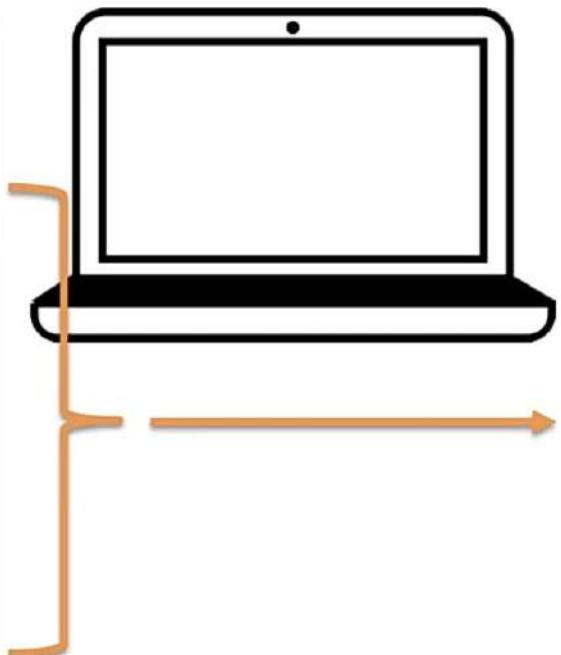


(Mining in Process)

Block: #500,112	
Timestamp: 1519181244	
Nonce: 0	4 Billion
Data:	
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
85C19D7	Fees: 0.0017 BTC
Prev.Hash: 0000DF2E57FB432A	
Hash:	

# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC

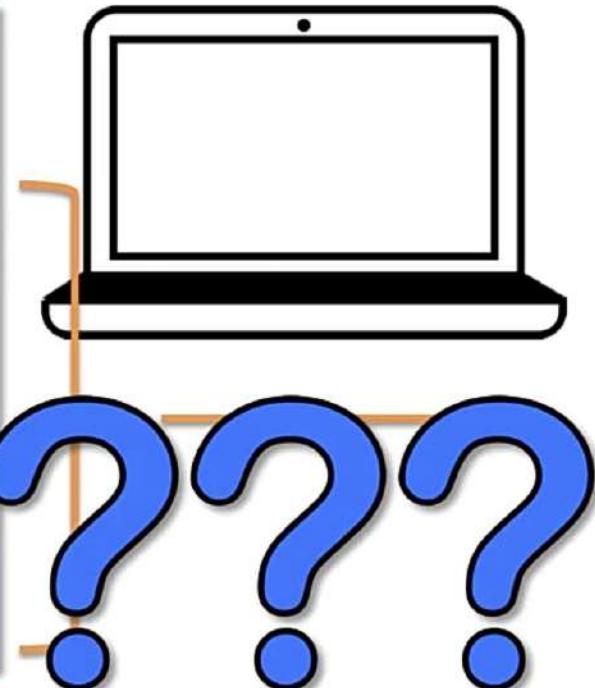


(Mining in Process)

Block: #500,112	
Timestamp: 1519181244	
Nonce: 0	4 Billion
Data:	
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
85C19D7	Fees: 0.0017 BTC
Prev.Hash: 0000DF2E57FB432A	
Hash:	

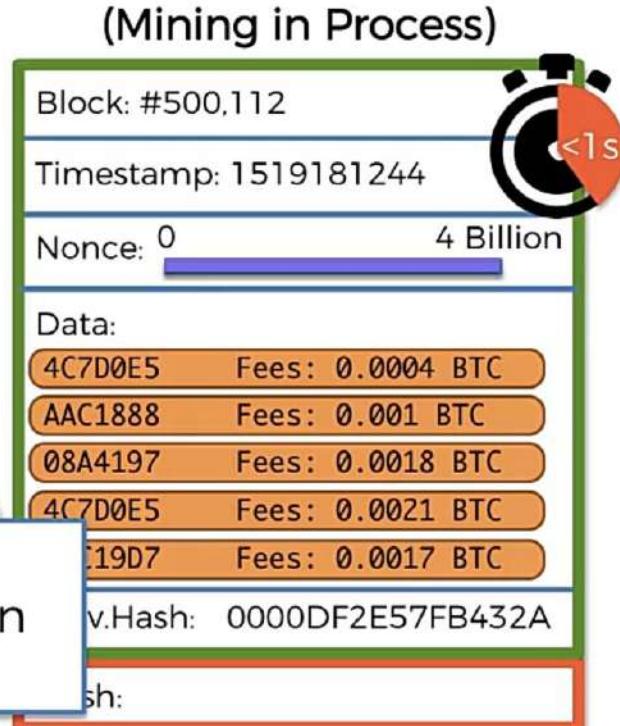
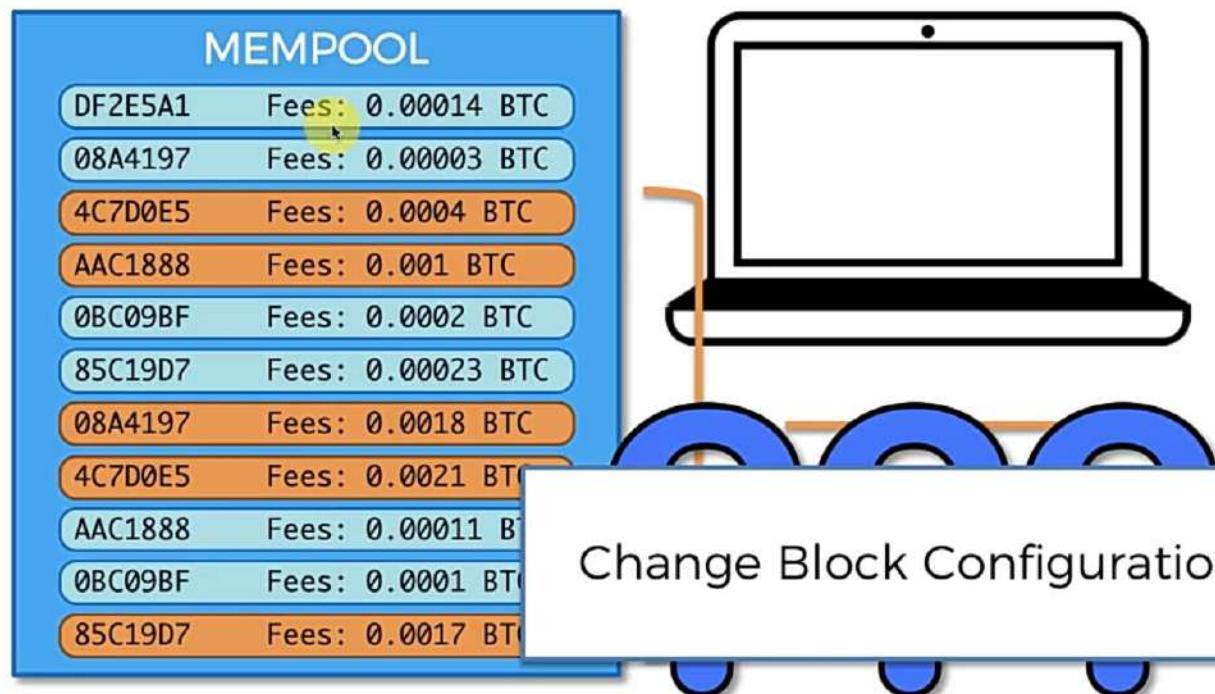
# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC



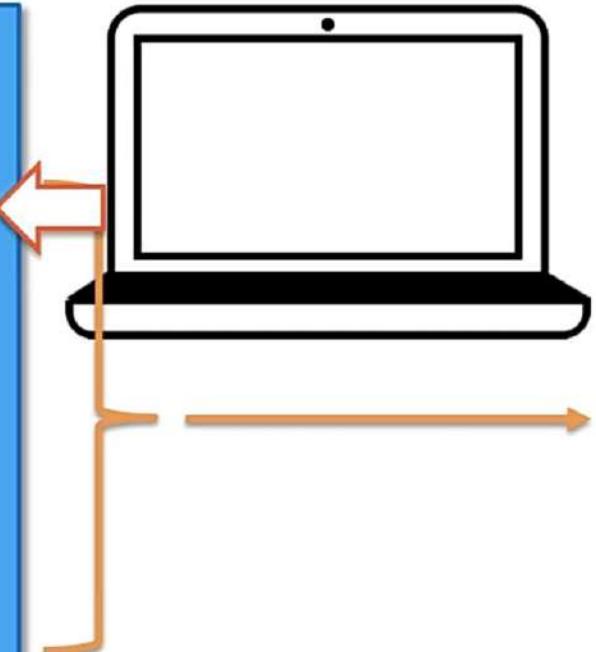
(Mining in Process)	
Block: #500,112	
Timestamp: 1519181244	
Nonce: 0	4 Billion
Data:	
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
85C19D7	Fees: 0.0017 BTC
Prev.Hash: 0000DF2E57FB432A	
Hash:	

# How Miners Pick Transactions ?



# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC

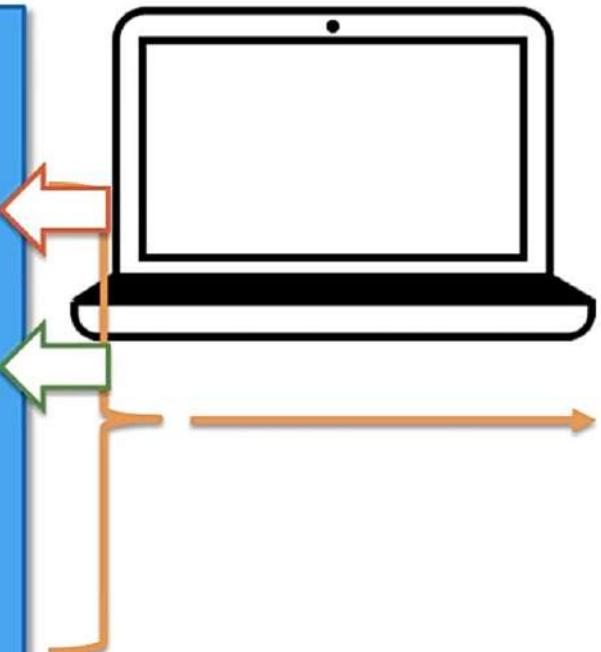


(Mining in Process)

Block: #500,112	
Timestamp: 1519181244	
Nonce: 0	4 Billion
Data:	
AAC1888 Fees: 0.001 BTC	
08A4197 Fees: 0.0018 BTC	
4C7D0E5 Fees: 0.0021 BTC	
85C19D7 Fees: 0.0017 BTC	
Prev.Hash: 0000DF2E57FB432A	
Hash:	

# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC

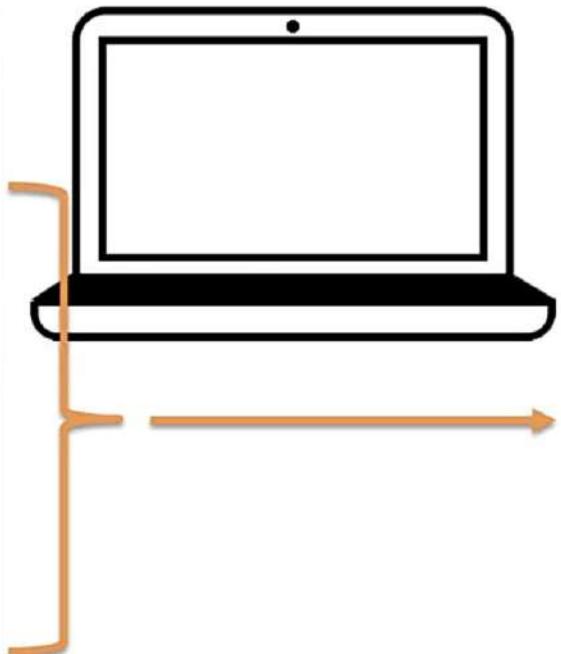


(Mining in Process)

Block: #500,112	
Timestamp: 1519181244	
Nonce: 0	4 Billion
Data:	
85C19D7	Fees: 0.00023 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
85C19D7	Fees: 0.0017 BTC
Prev.Hash: 0000DF2E57FB432A	
Hash:	

# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC

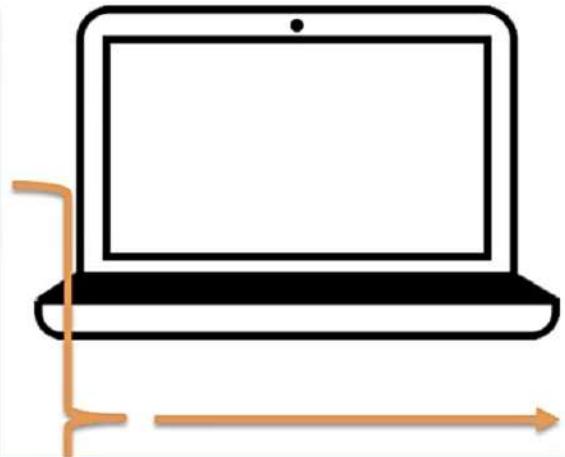


(Mining in Process)

Block: #500,112	
Timestamp: 1519181244	
Nonce: 0	4 Billion
Data:	
85C19D7	Fees: 0.00023 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
85C19D7	Fees: 0.0017 BTC
Prev.Hash: 0000DF2E57FB432A	
Hash:	

# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC

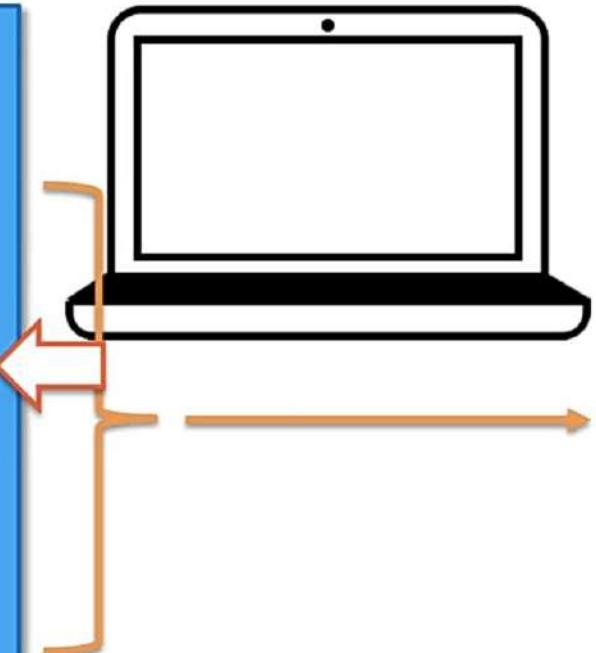


Change Block Configuration

(Mining in Process)	
Block: #500,112	 <1s
Timestamp: 1519181244	
Nonce: 0	4 Billion
Data:	
85C19D7	Fees: 0.00023 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
85C19D7	Fees: 0.0017 BTC
v.Hash:	0000DF2E57FB432A
sh:	

# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC

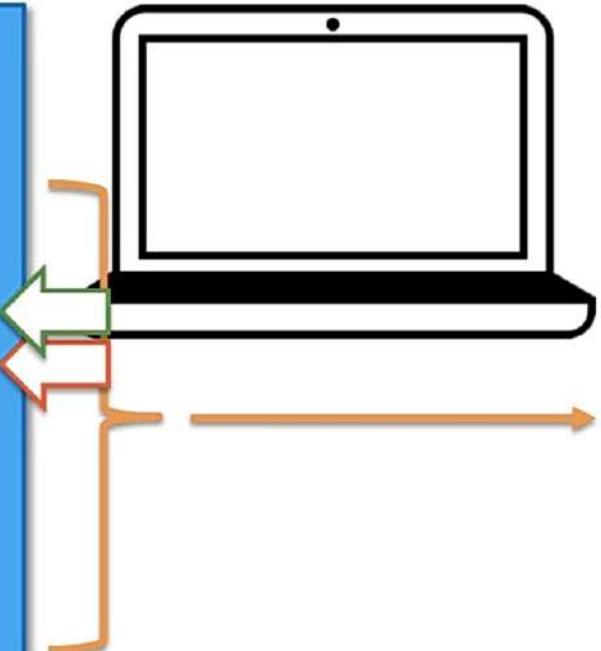


(Mining in Process)

Block: #500,112	
Timestamp: 1519181244	
Nonce: 0	4 Billion
Data:	
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
85C19D7	Fees: 0.0017 BTC
Prev.Hash: 0000DF2E57FB432A	
Hash:	

# How Miners Pick Transactions ?

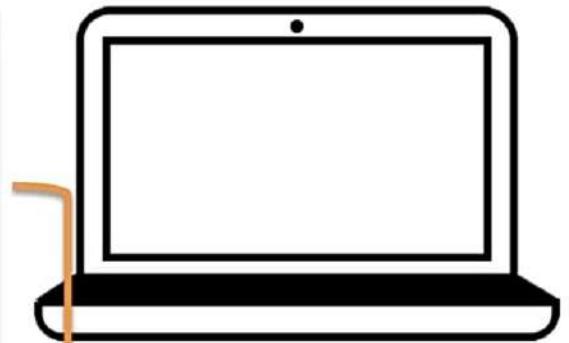
MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC



(Mining in Process)	
Block: #500,112	
Timestamp: 1519181244	
Nonce: 0	4 Billion
Data:	
0BC09BF	Fees: 0.0002 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
85C19D7	Fees: 0.0017 BTC
Prev.Hash: 0000DF2E57FB432A	
Hash:	

# How Miners Pick Transactions ?

MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC



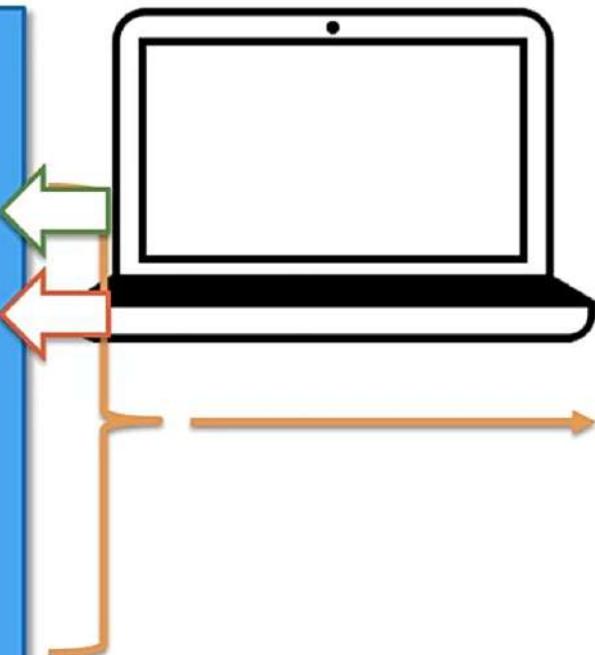
(Mining in Process)

Block: #500,112	↓	1s
Timestamp: 1519181245		
Nonce: 0	4 Billion	
Data:		
0BC09BF	Fees: 0.0002 BTC	
AAC1888	Fees: 0.001 BTC	
08A4197	Fees: 0.0018 BTC	
4C7D0E5	Fees: 0.0021 BTC	
85C19D7	Fees: 0.0017 BTC	
v.Hash: 0000DF2E57FB432A		
sh:		

Start Over

# How Miners Pick Transactions ?

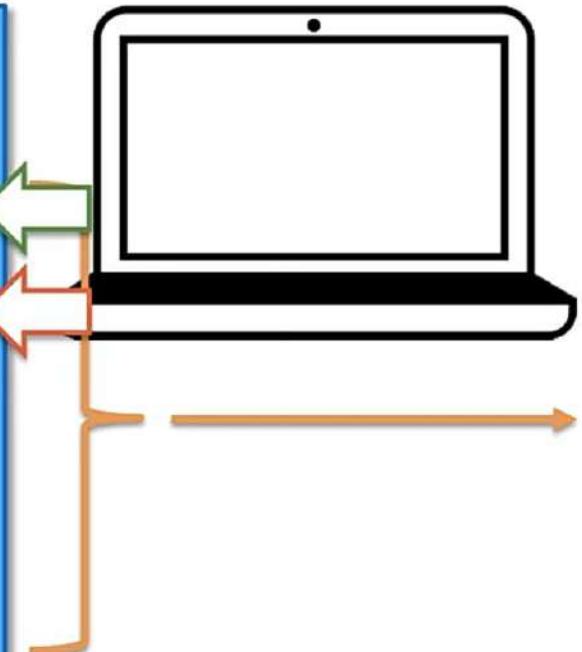
MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC



(Mining in Process)	
Block: #500,112	
Timestamp: 1519181245	
Nonce: 0	4 Billion
Data:	
0BC09BF	Fees: 0.0002 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
85C19D7	Fees: 0.0017 BTC
Prev.Hash:	0000DF2E57FB432A
Hash:	

# How Miners Pick Transactions ?

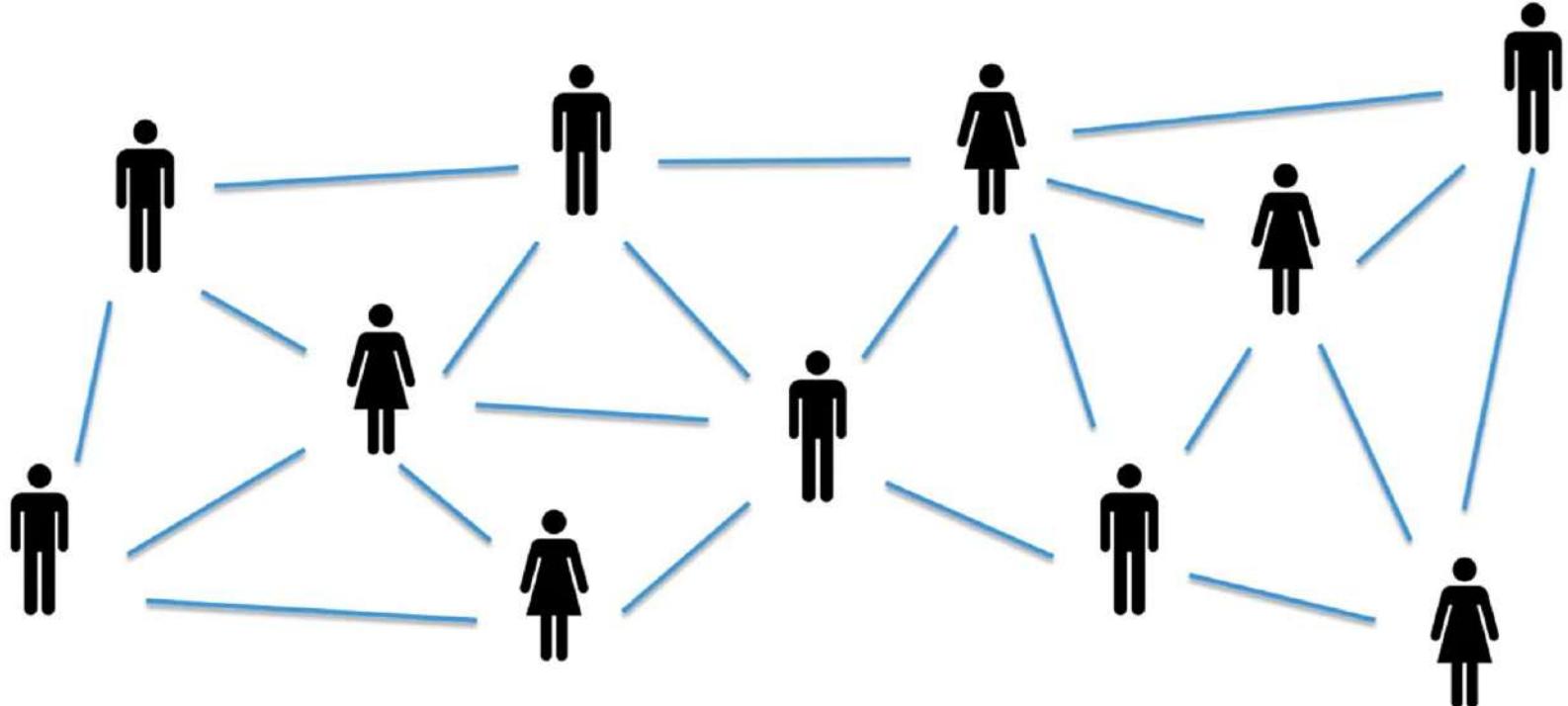
MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC



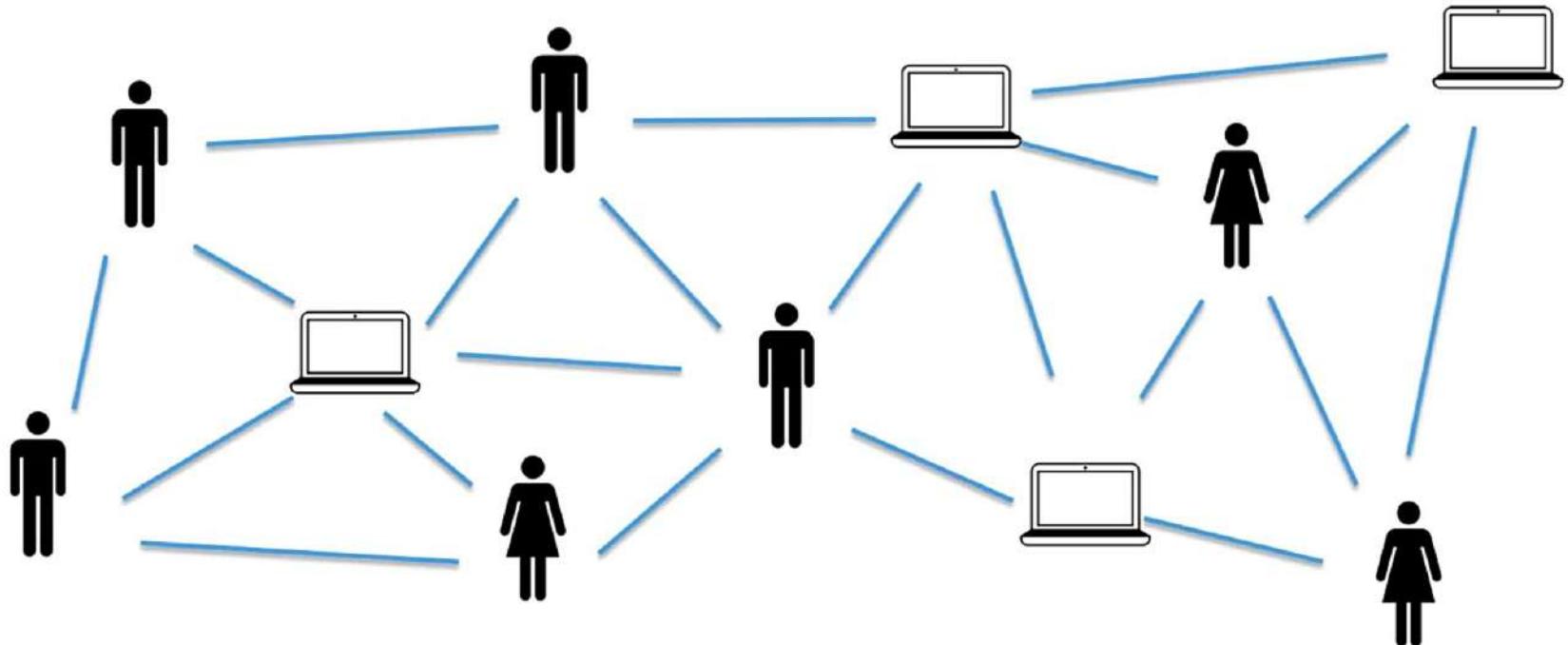
(Mining in Process)

Block: #500,112	
Timestamp: 1519181245	
Nonce: 0	4 Billion
Data:	
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
85C19D7	Fees: 0.0017 BTC
Prev.Hash: 0000DF2E57FB432A	
Hash:	

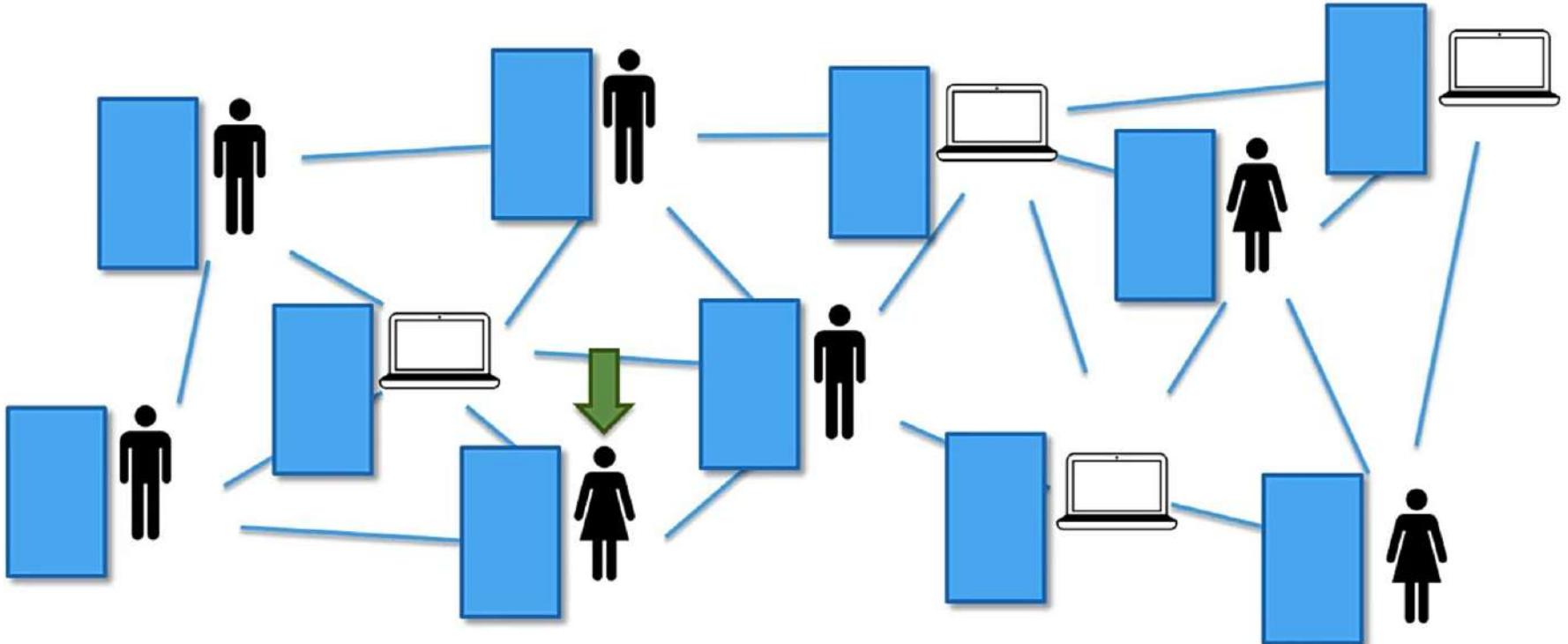
# How do Mempools work?



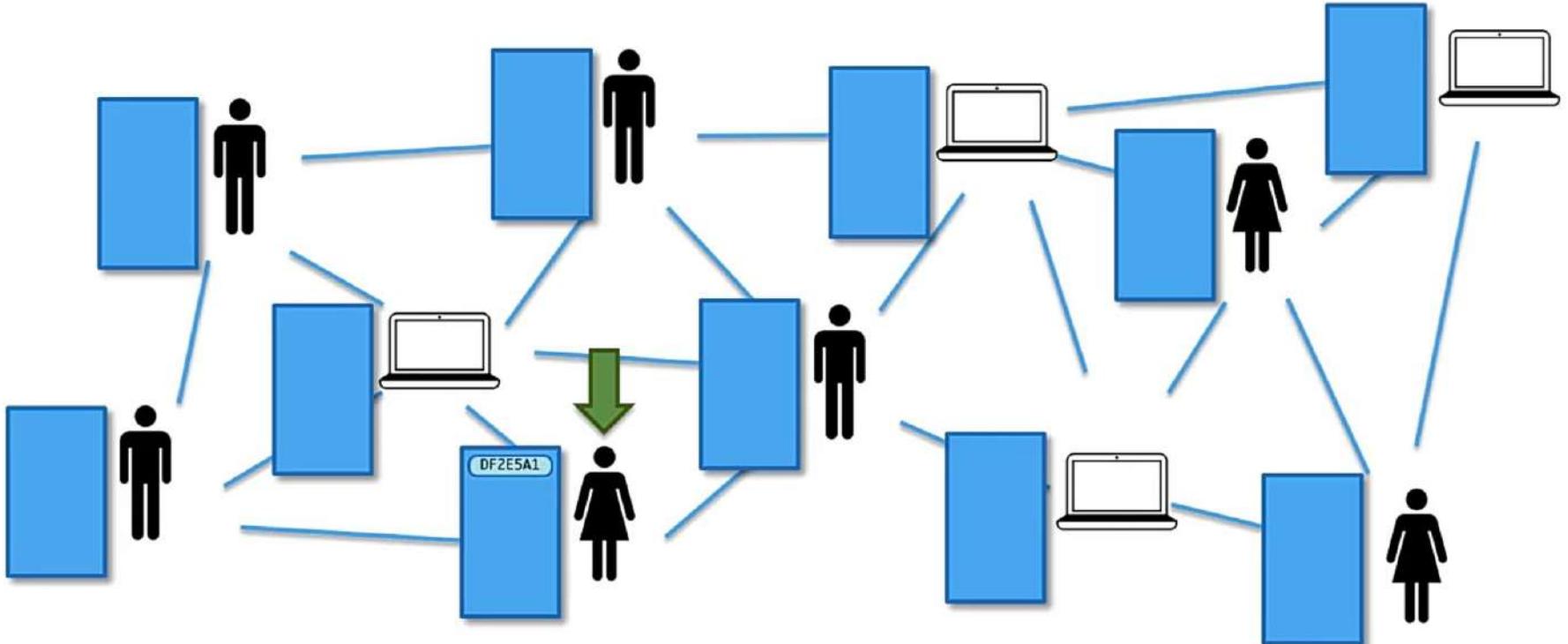
# How do Mempools work?



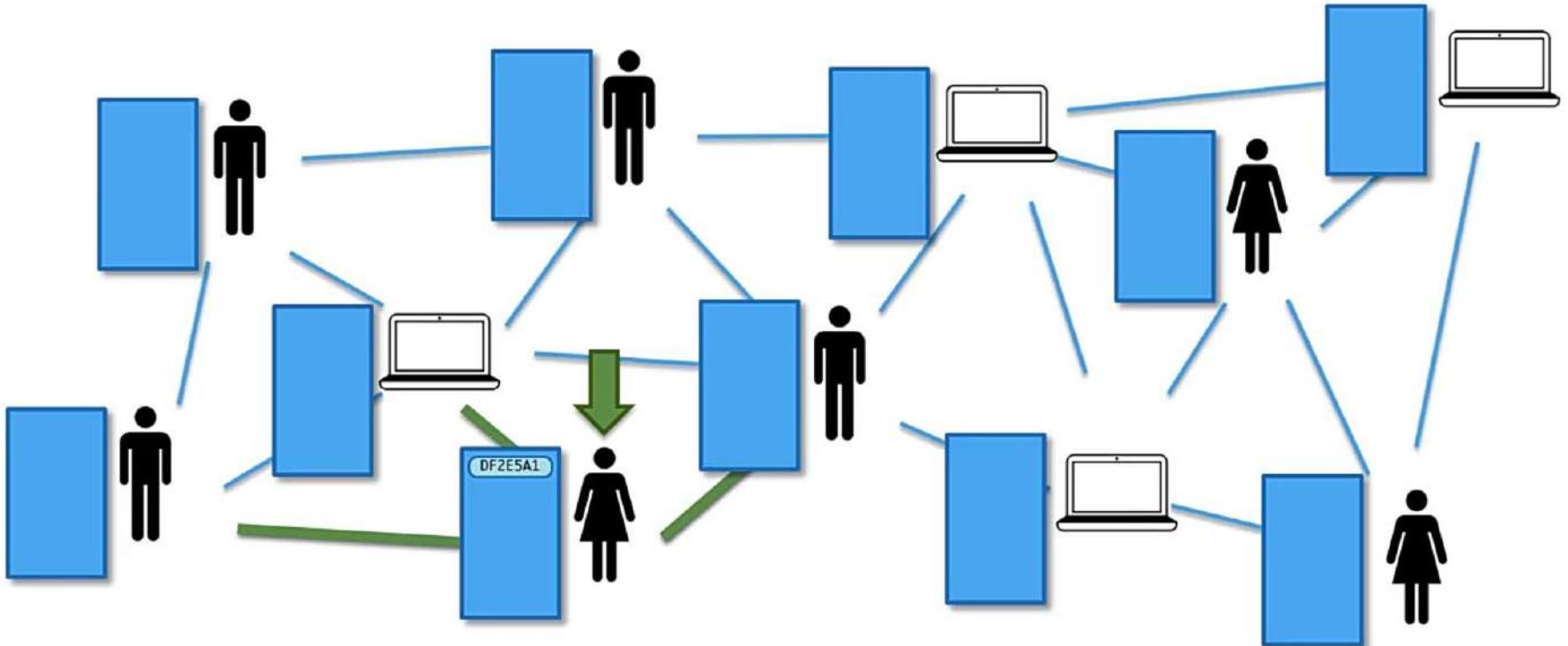
# How do Mempools work?



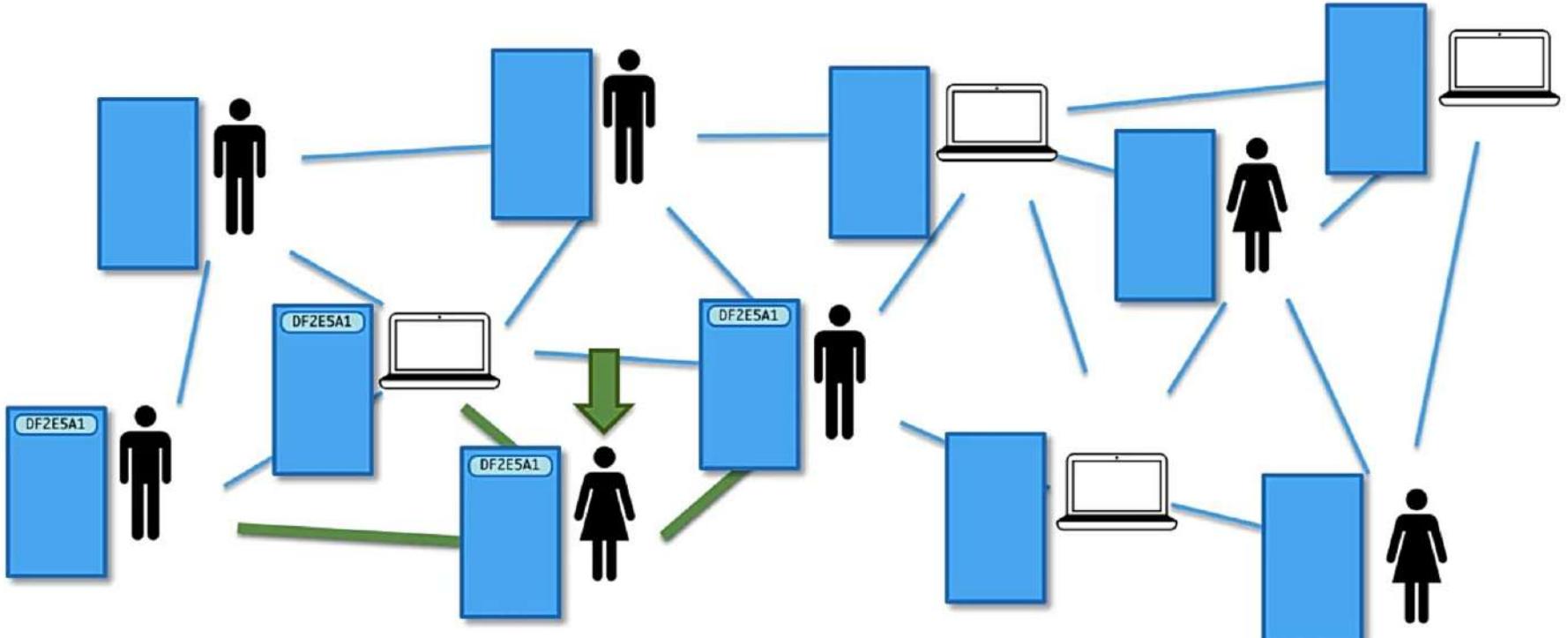
# How do Mempools work?



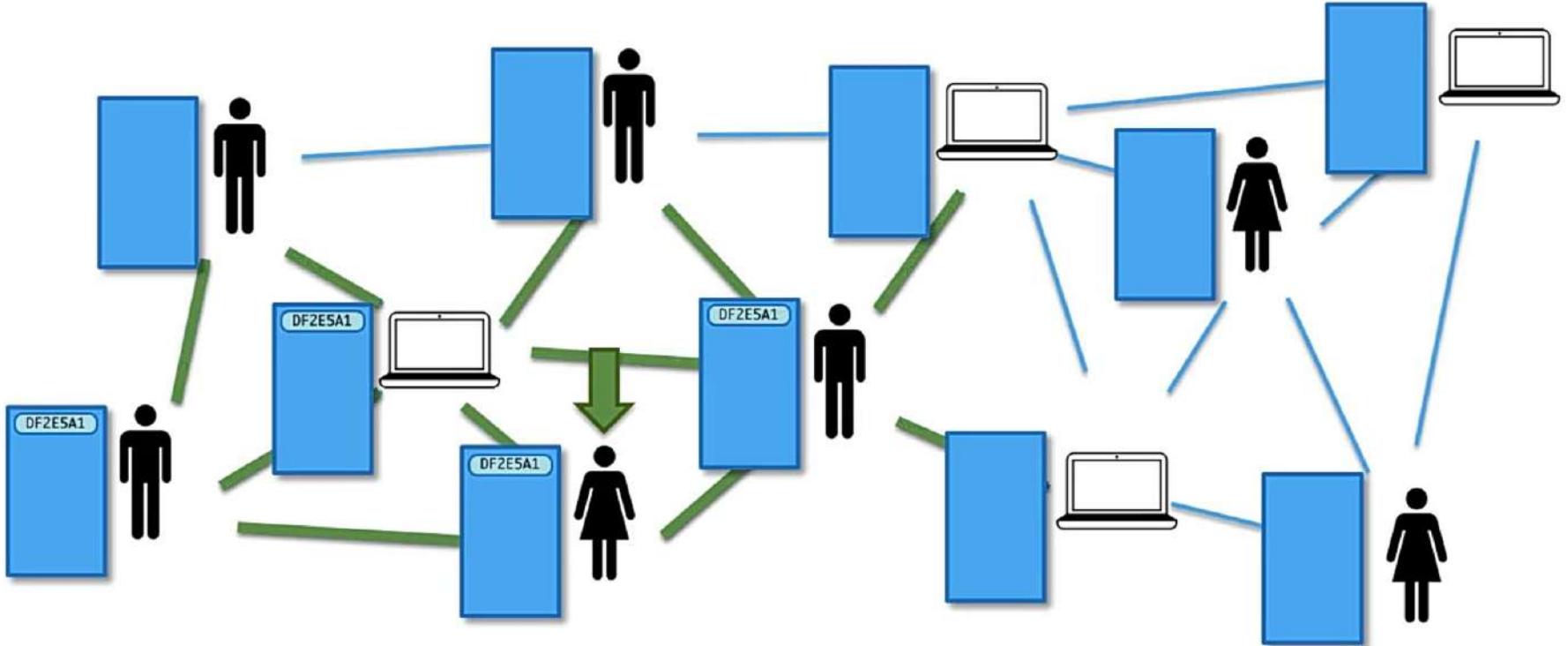
# How do Mempools work?



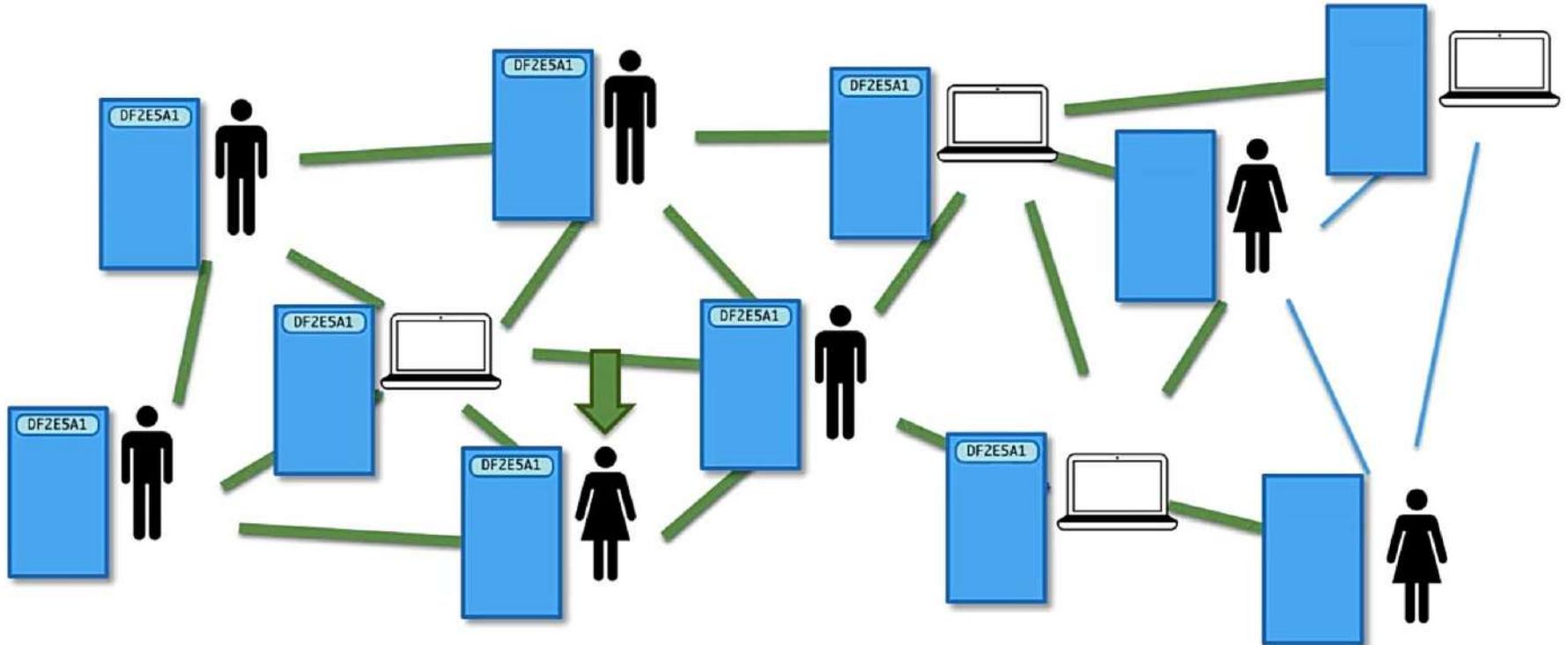
# How do Mempools work?



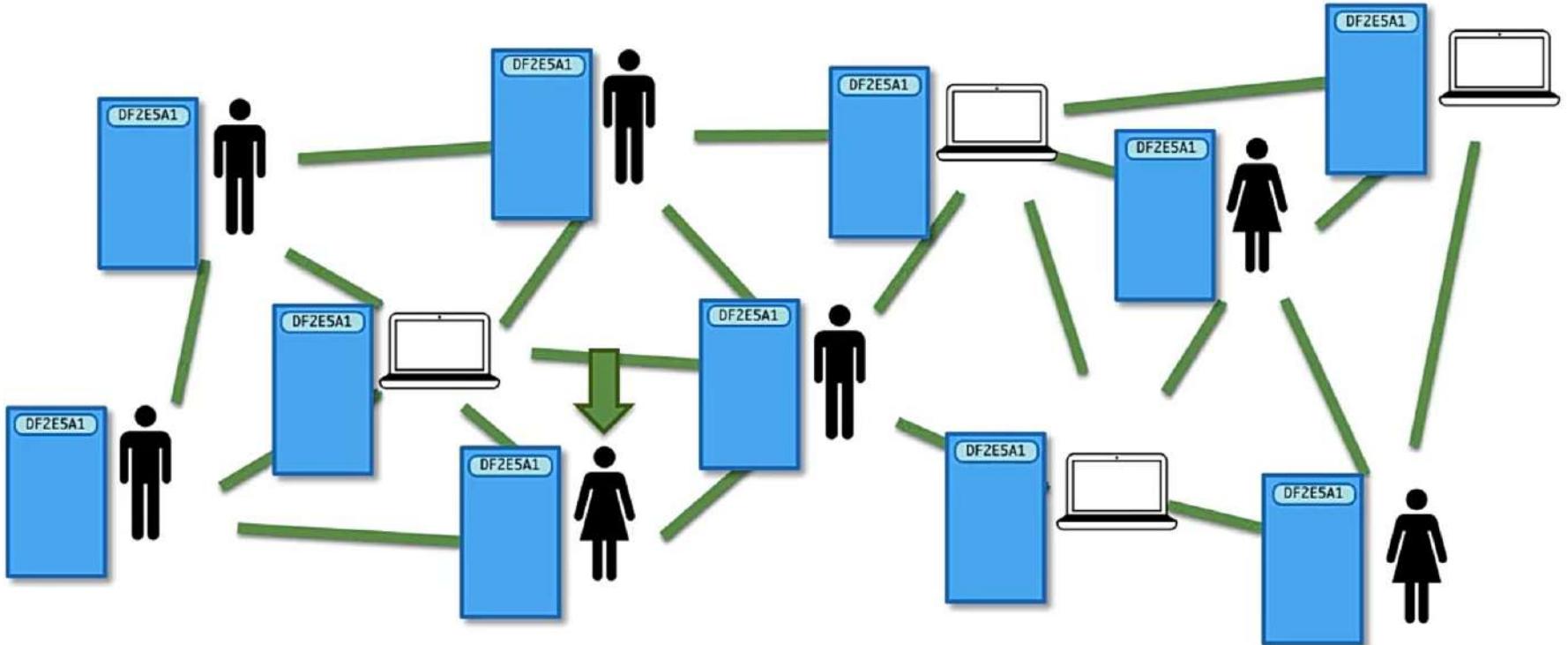
# How do Mempools work?



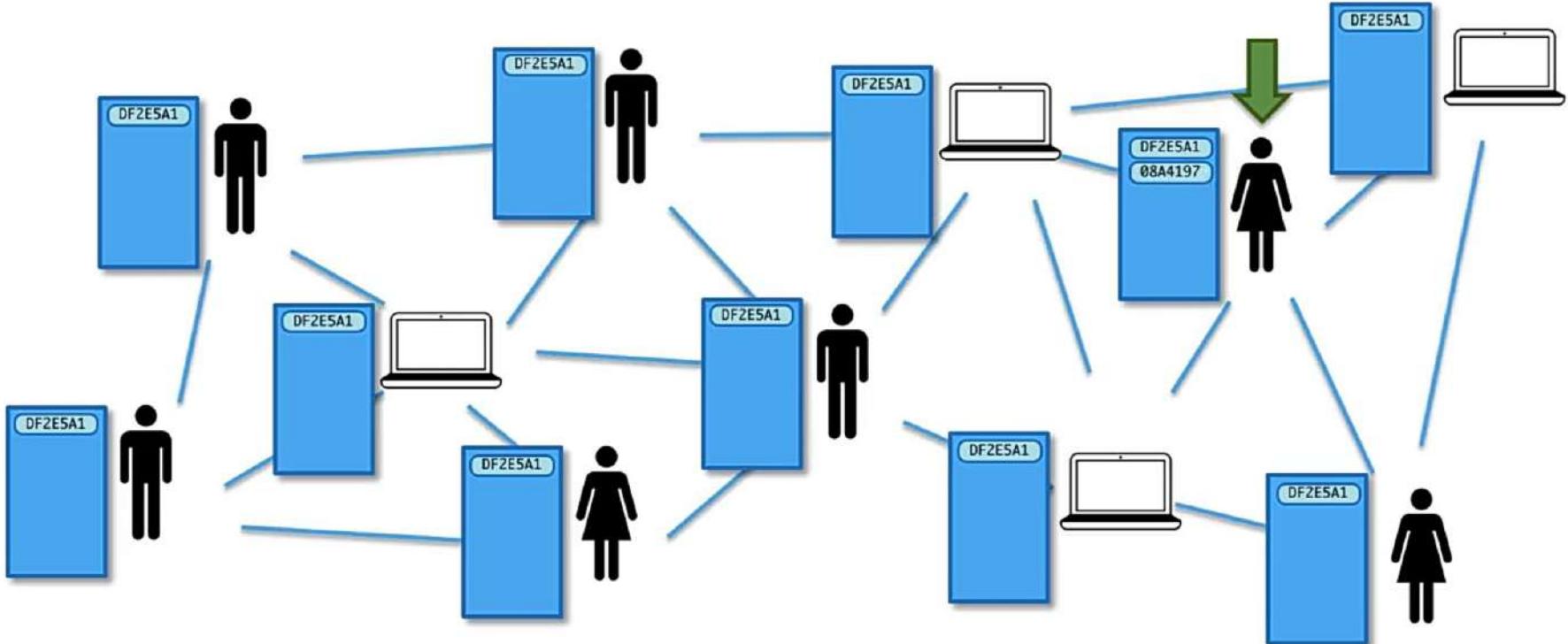
# How do Mempools work?



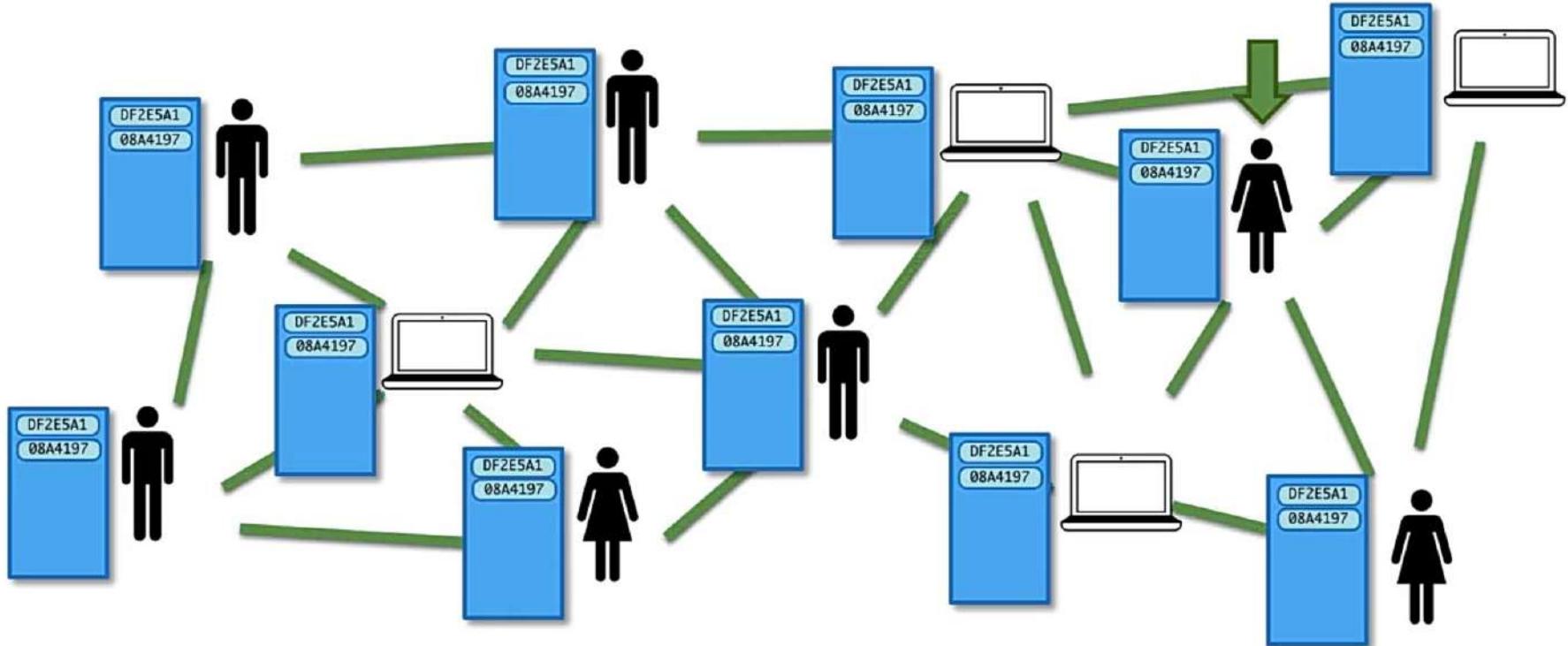
# How do Mempools work?



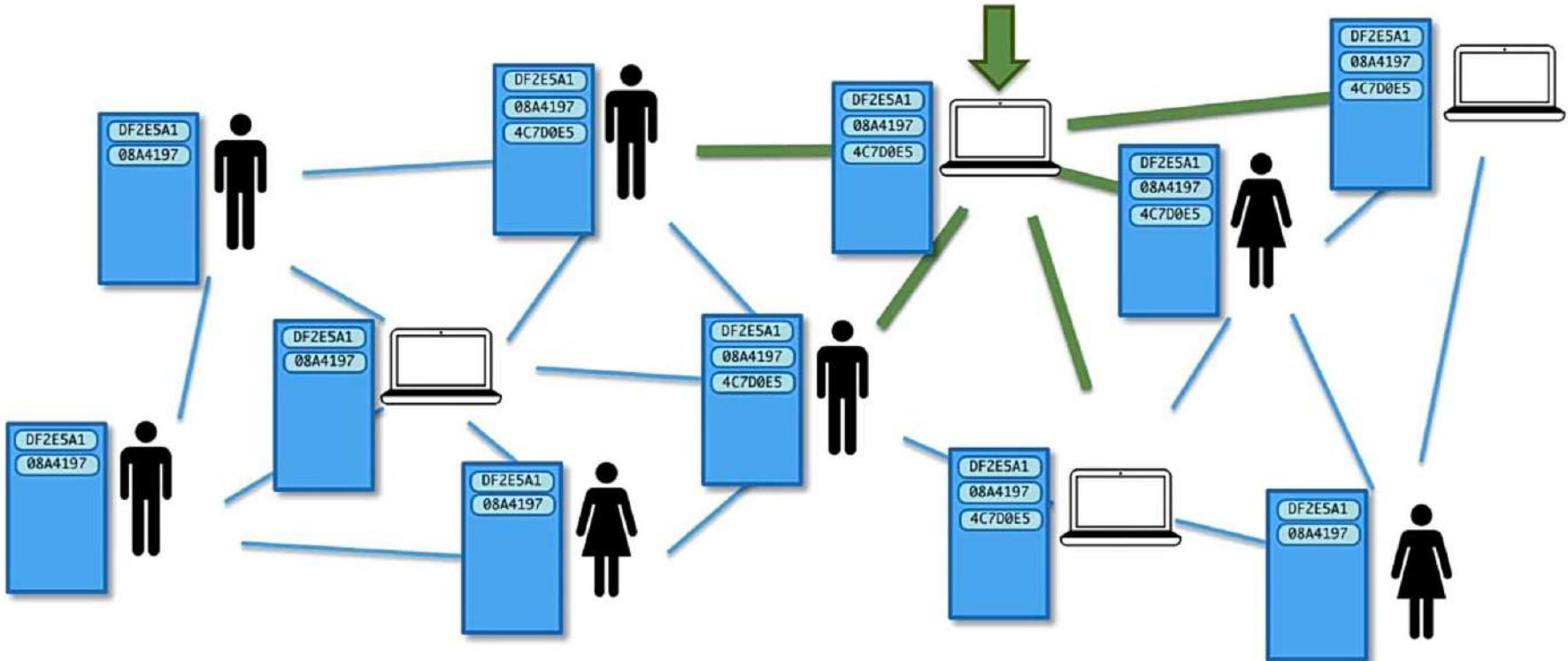
# How do Memools work?



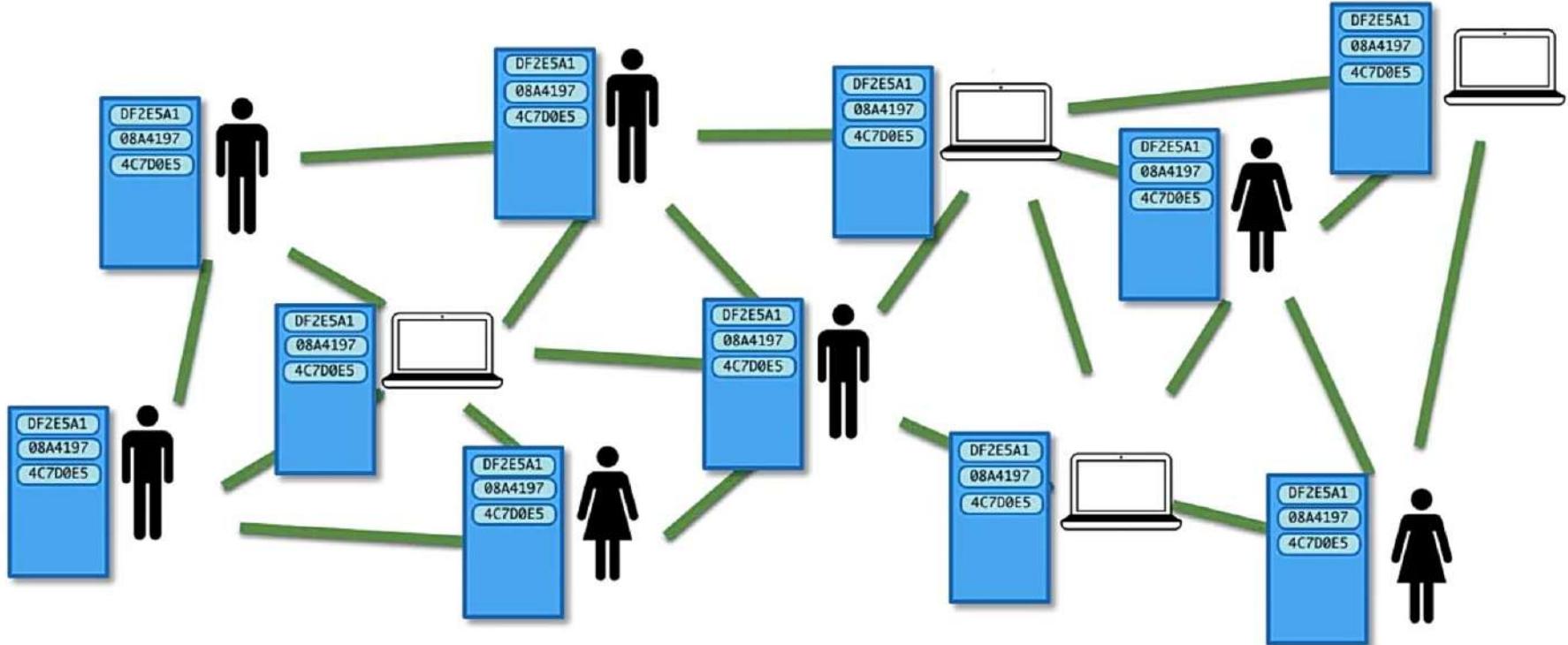
# How do Mempools work?



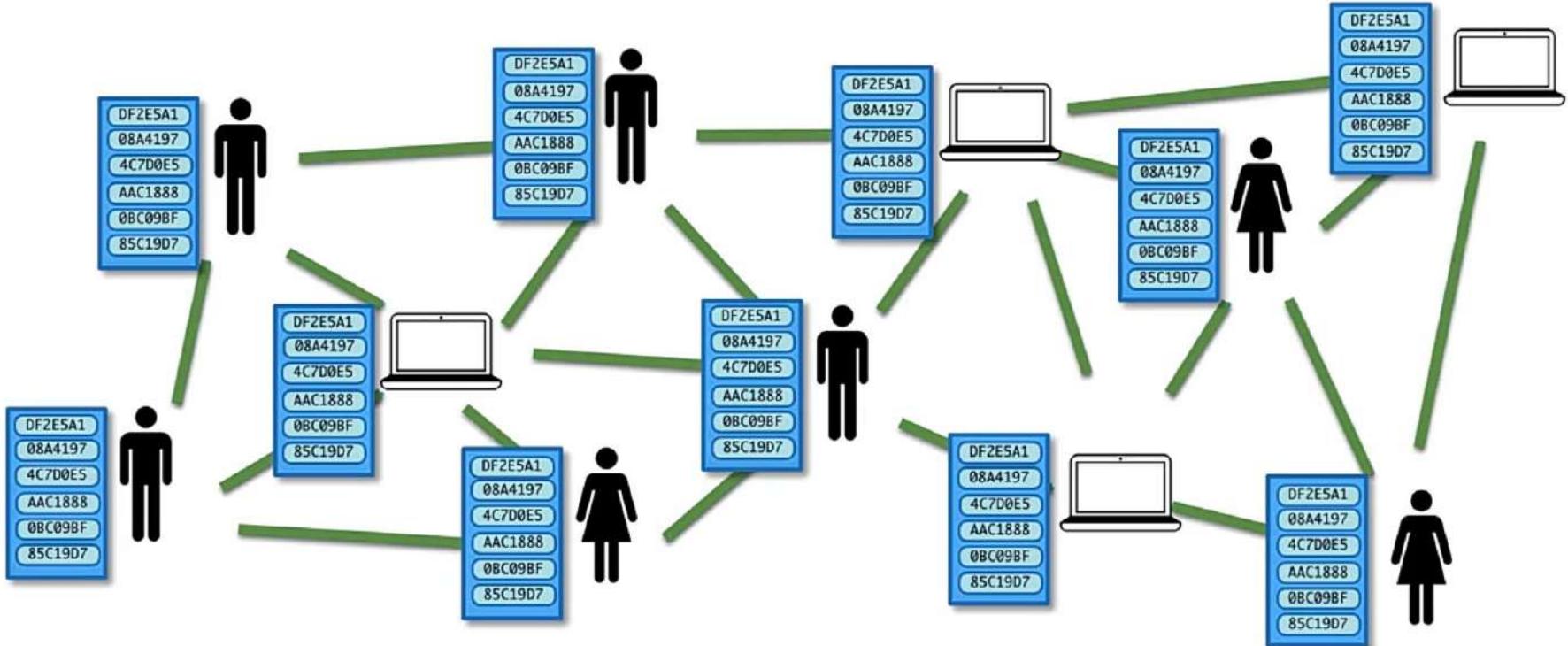
# How do Mempools work?



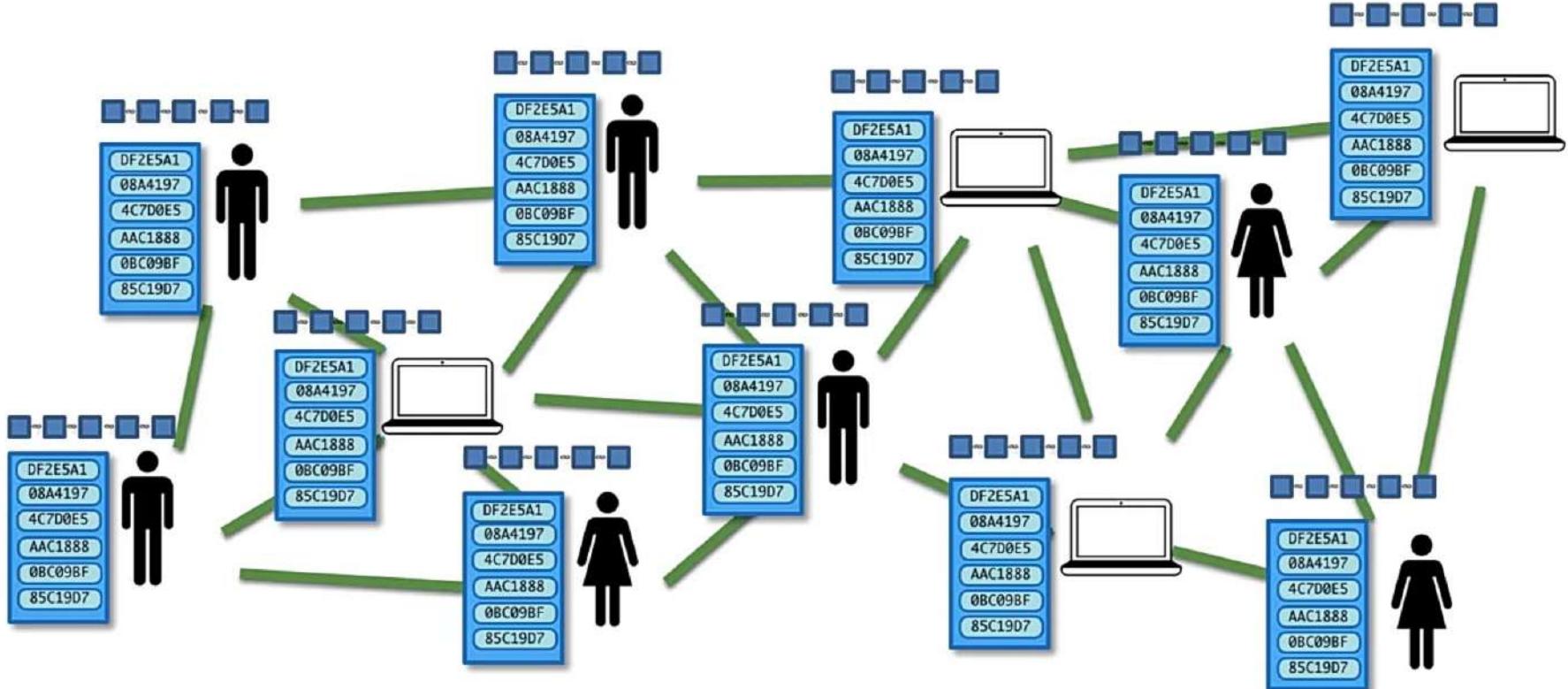
# How do Mempools work?



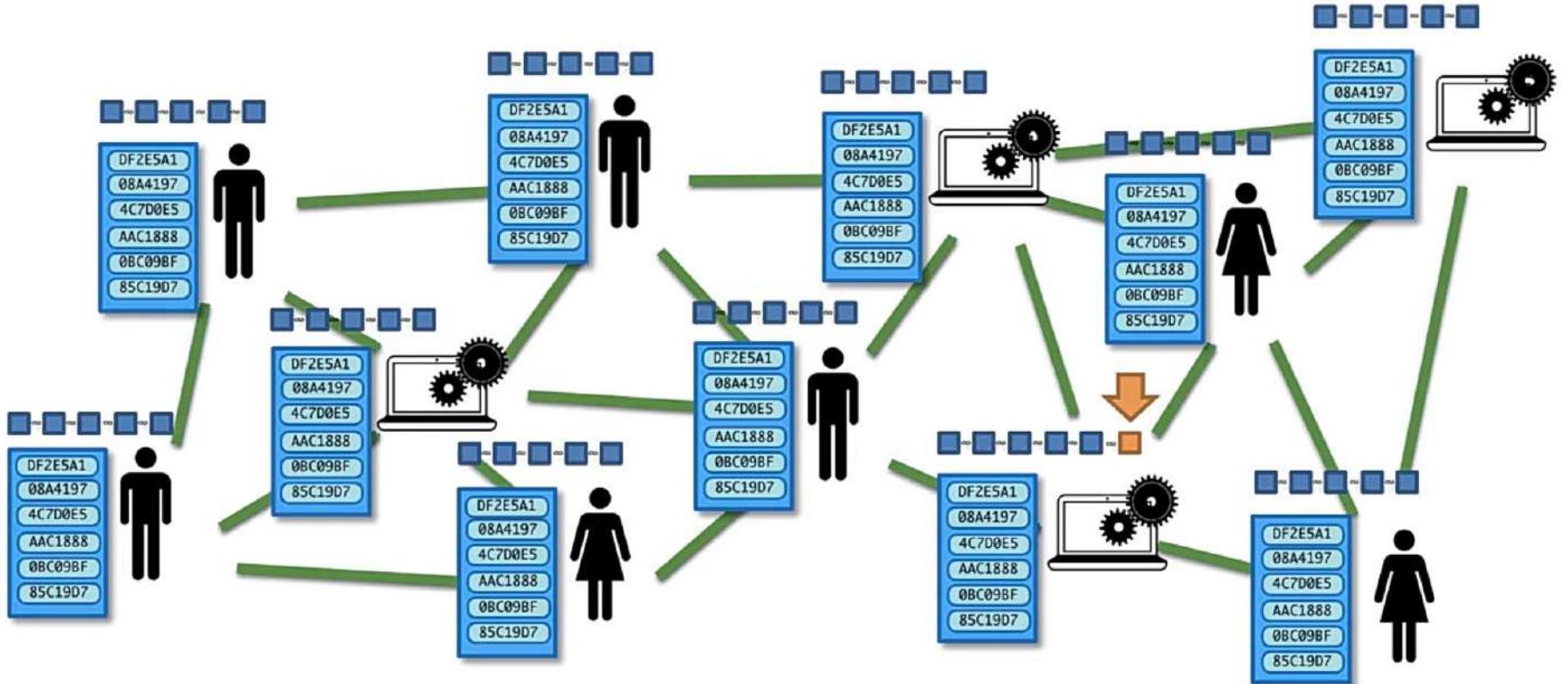
# How do Mempools work?



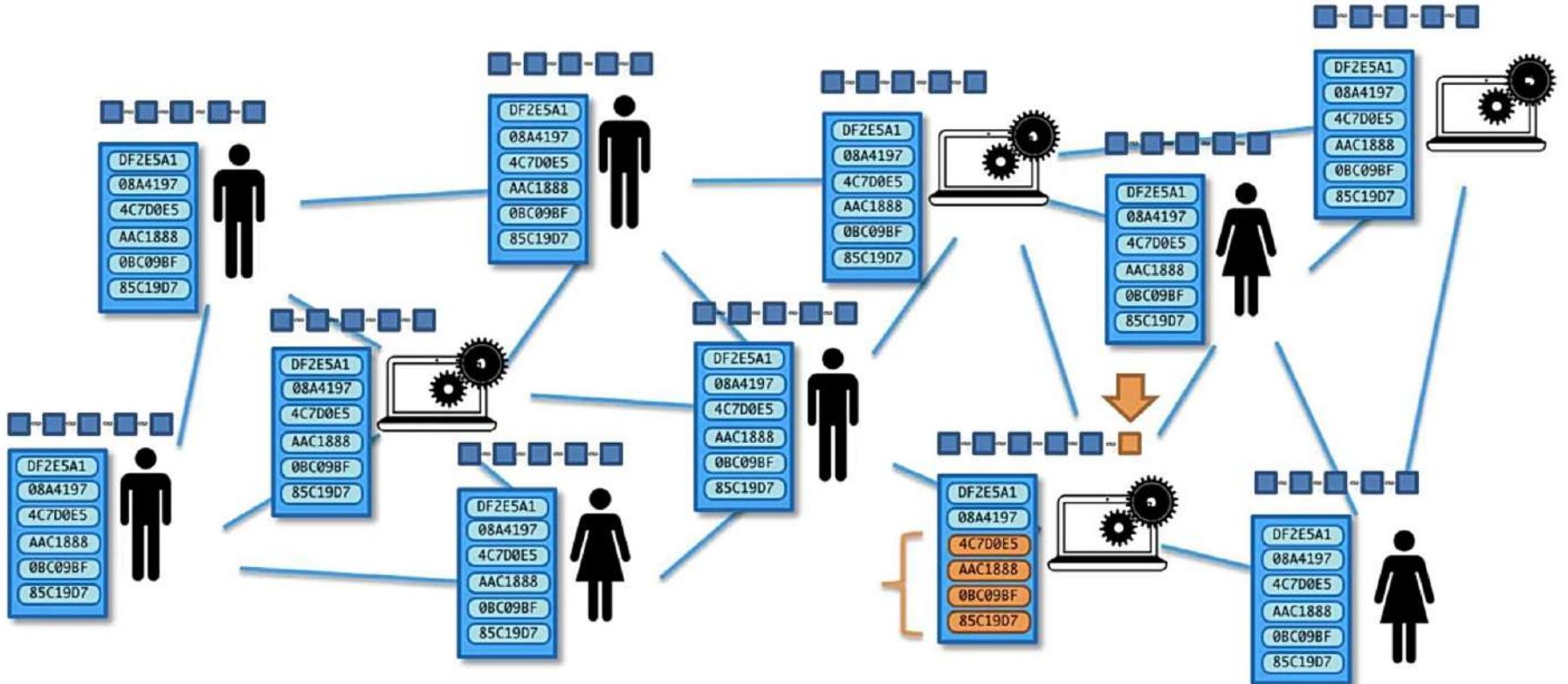
# How do Mempools work?



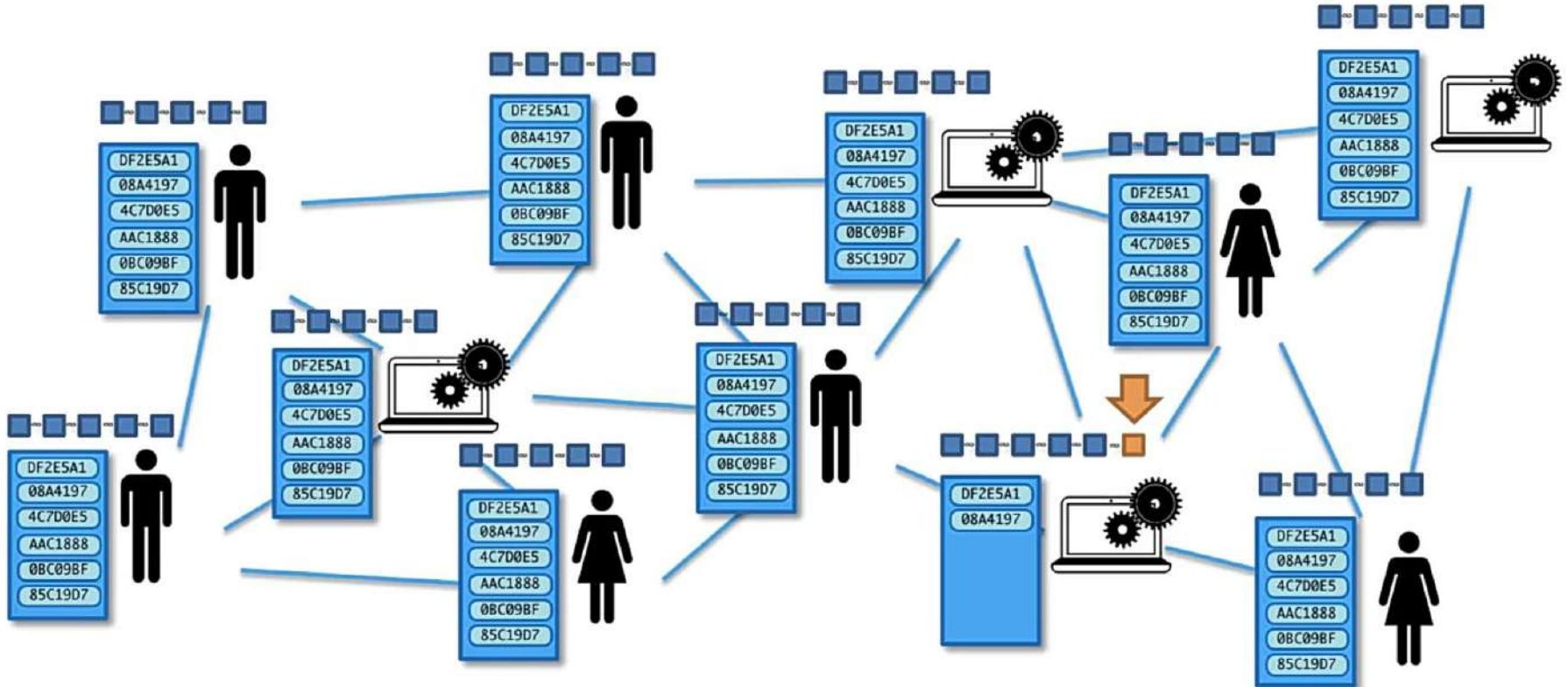
# How do Mempools work?



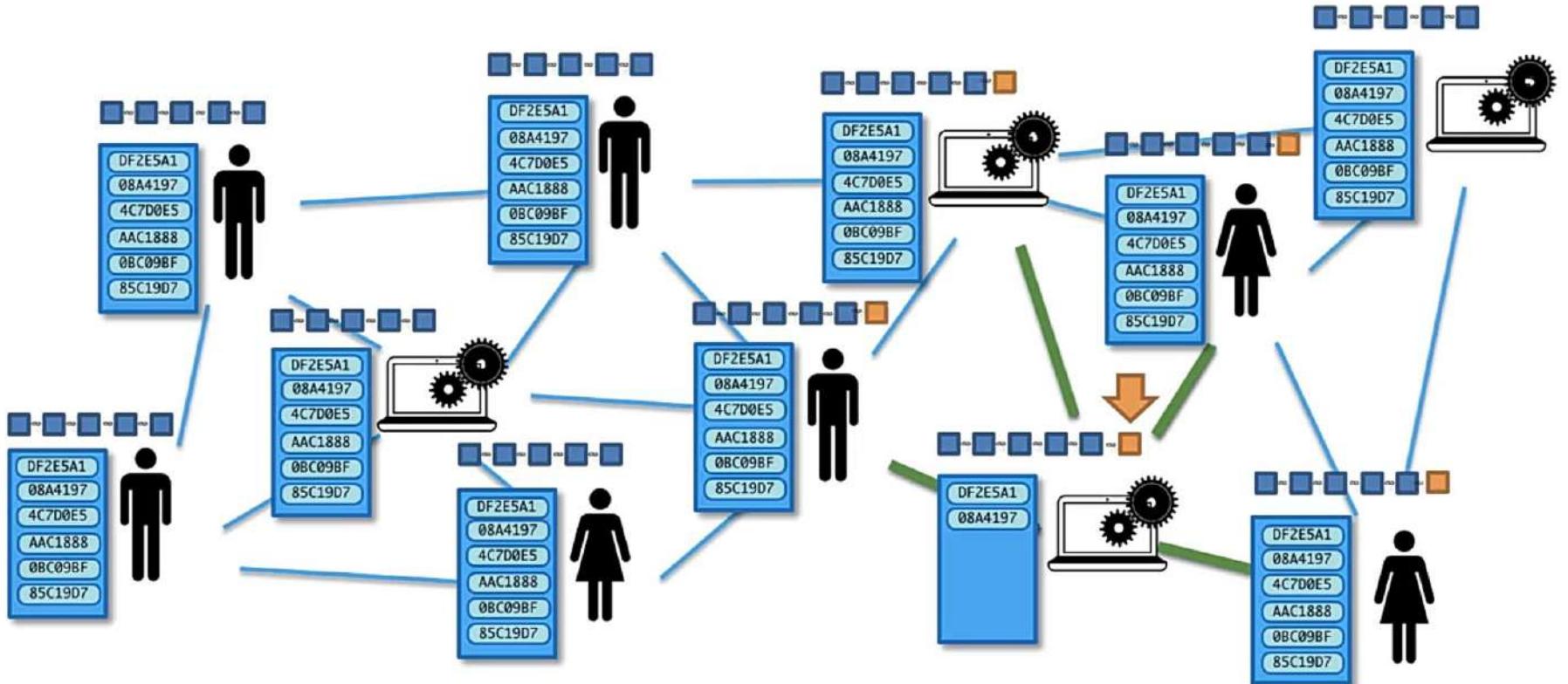
# How do Mempools work?



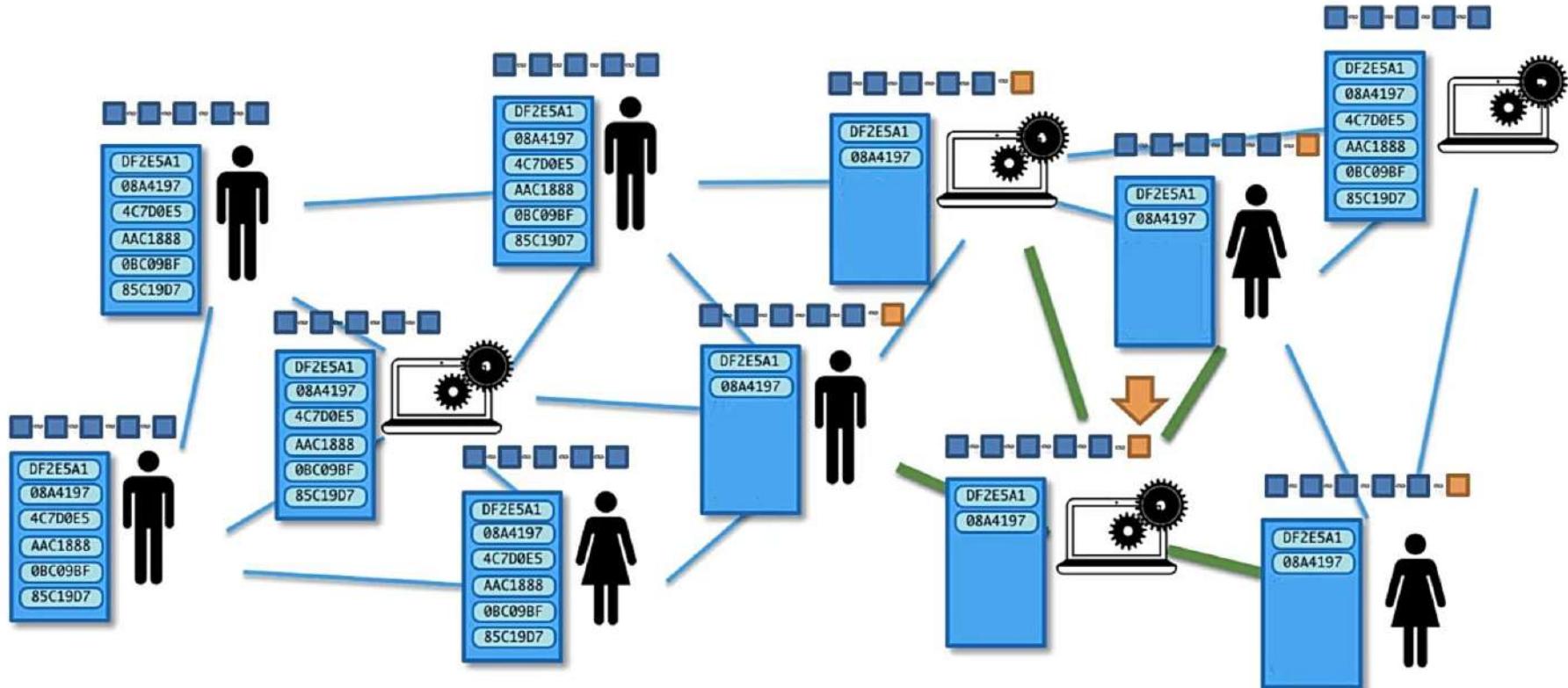
# How do Mempools work?



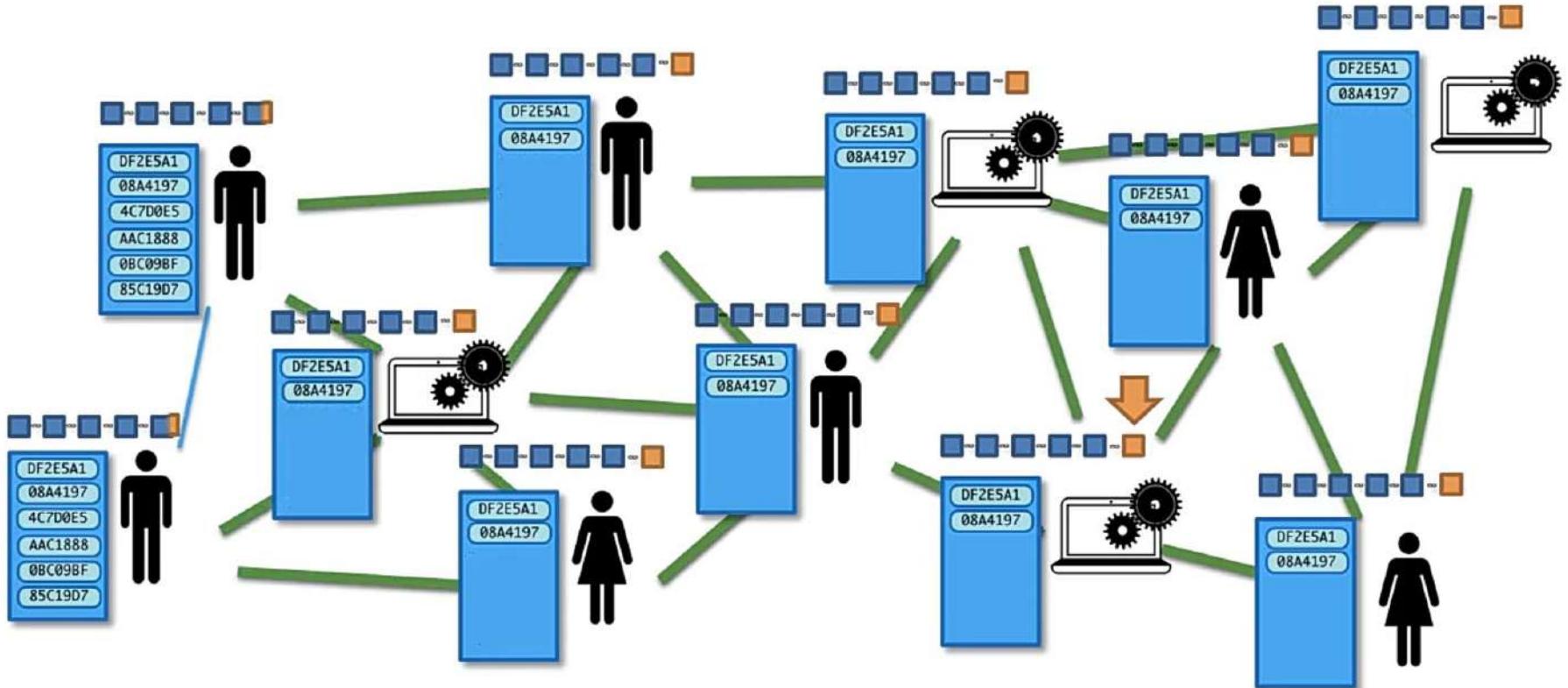
# How do Mempools work?



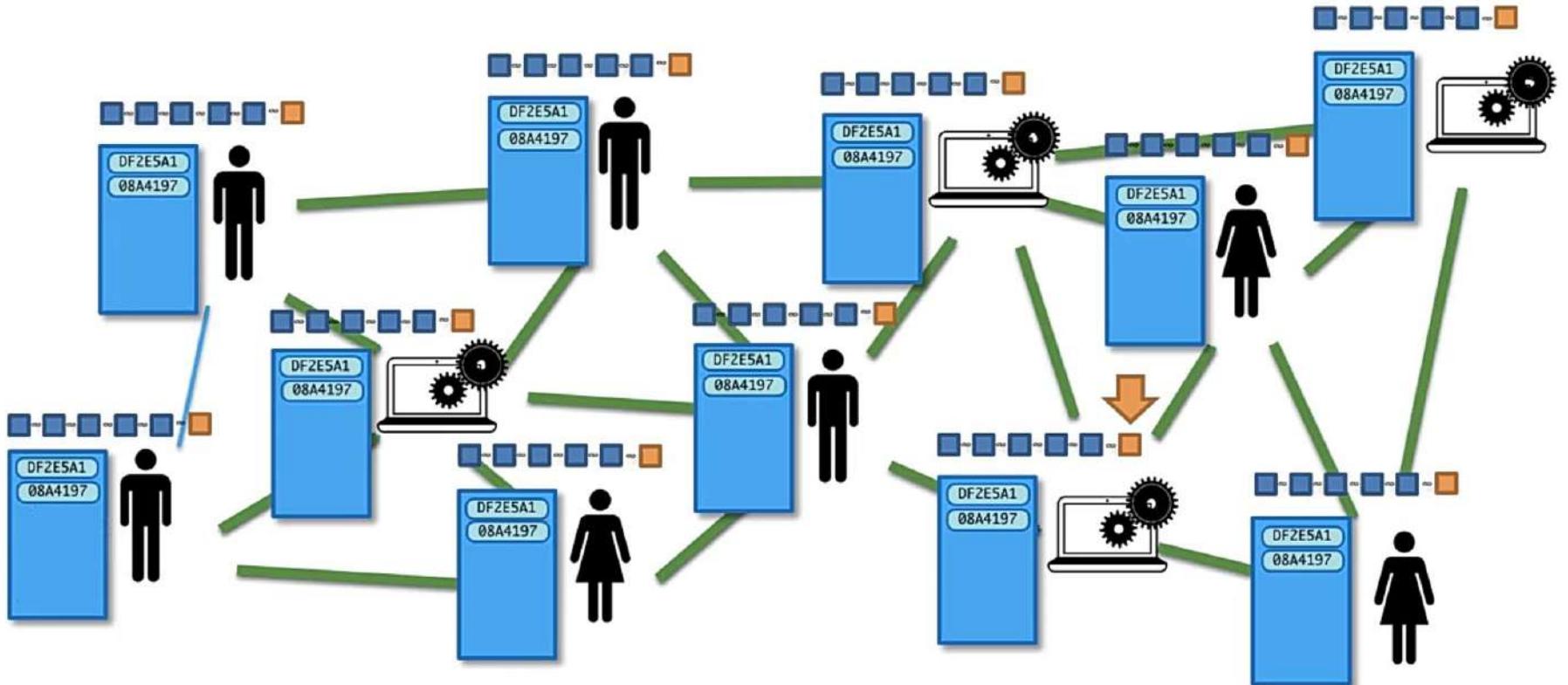
# How do Mempools work?



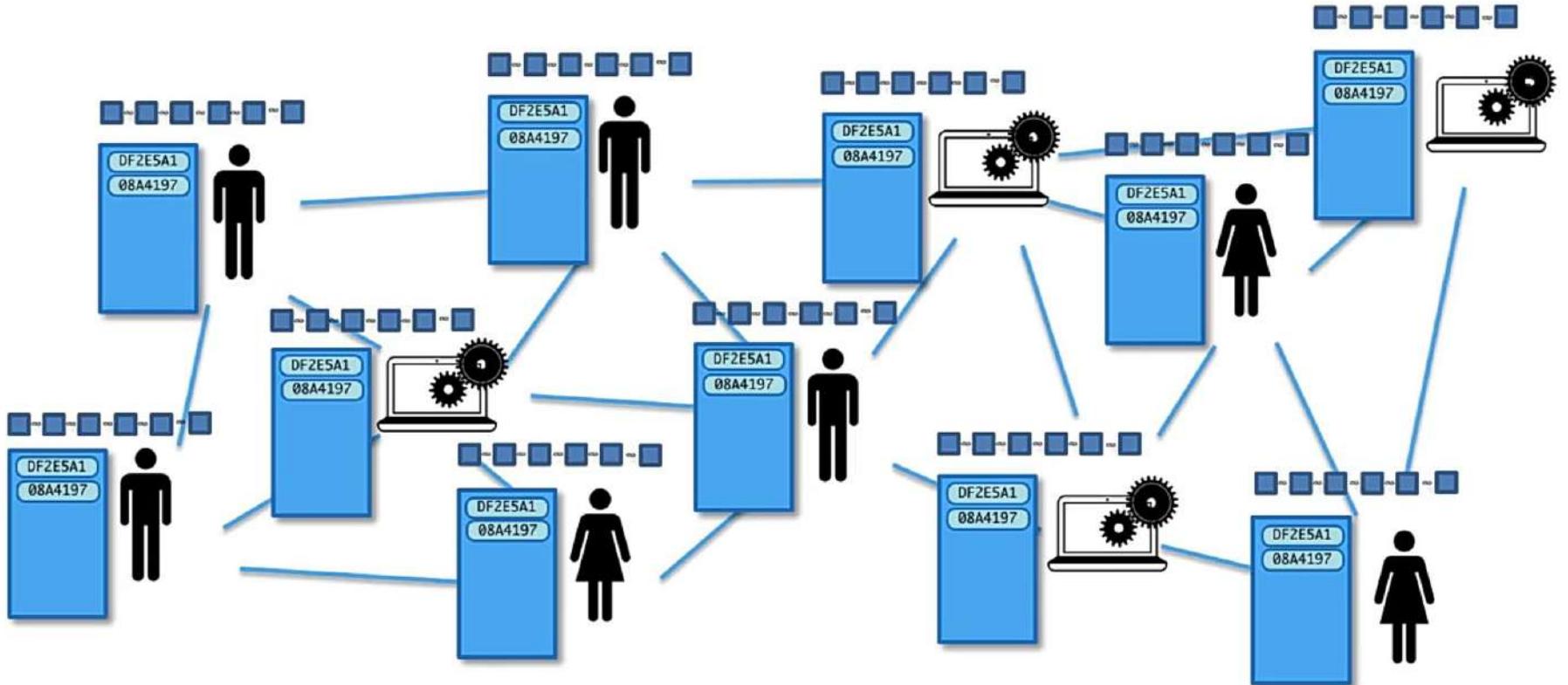
# How do Mempools work?



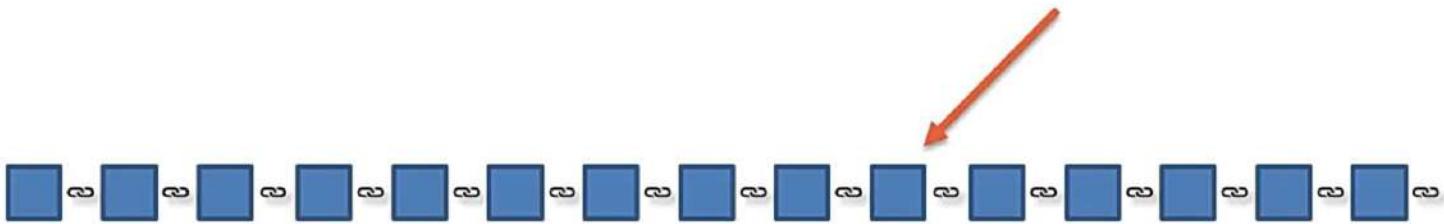
# How do Mempools work?



# How do Mempools work?

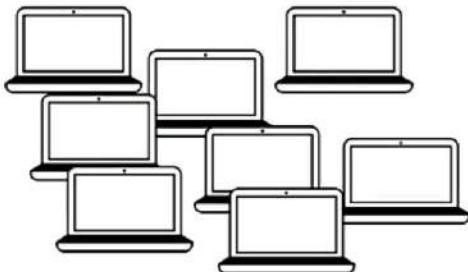


# 51% Attack

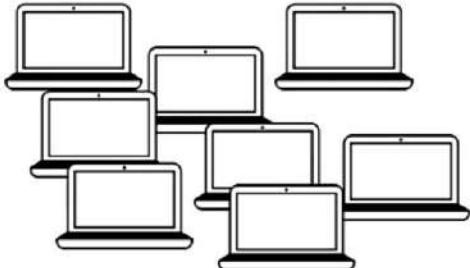


This is NOT the 51% attack

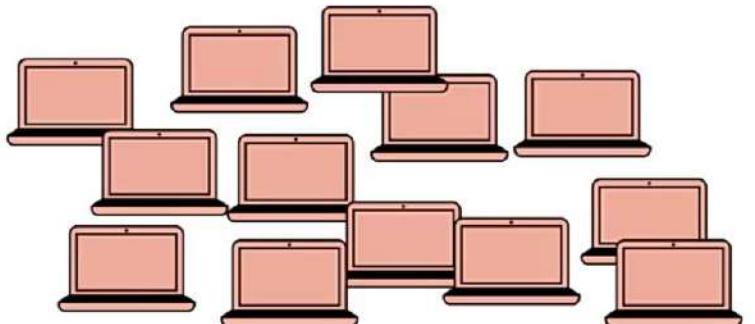
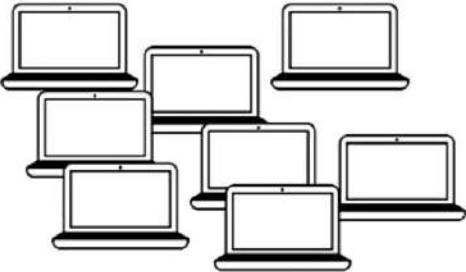
# 51% Attack



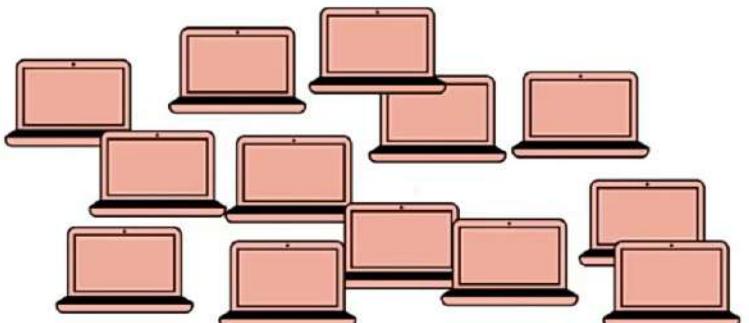
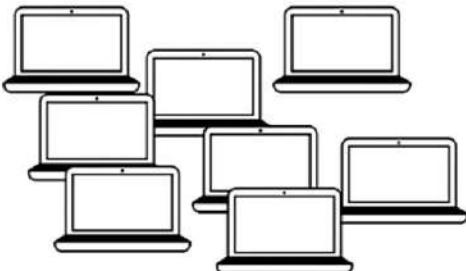
# 51% Attack



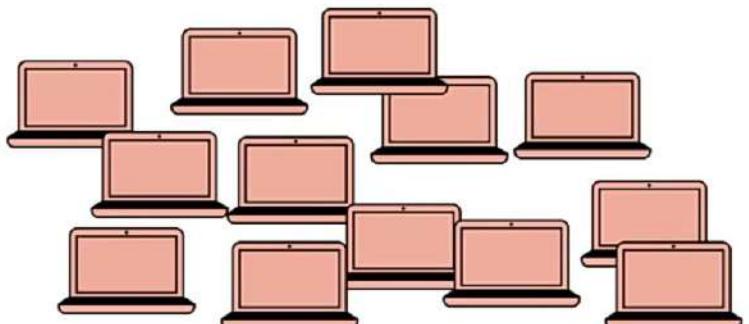
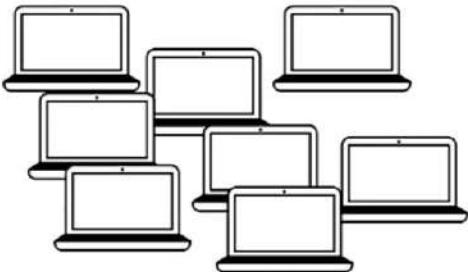
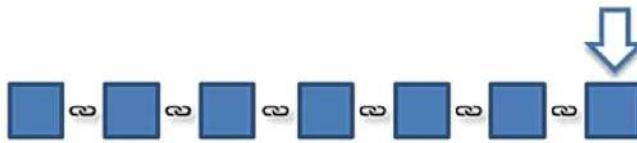
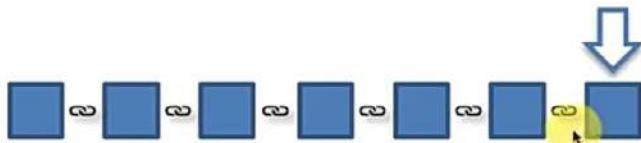
# 51% Attack



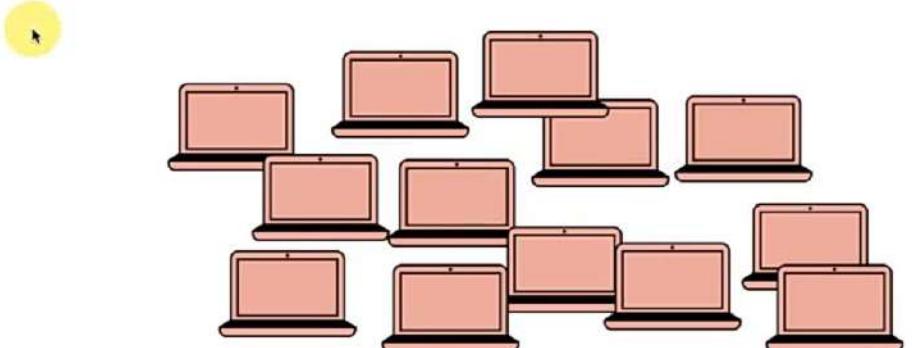
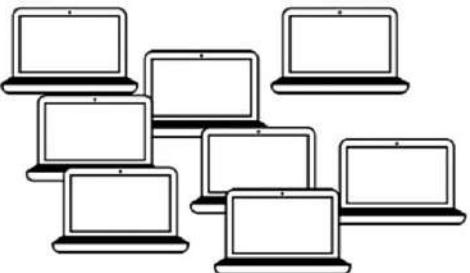
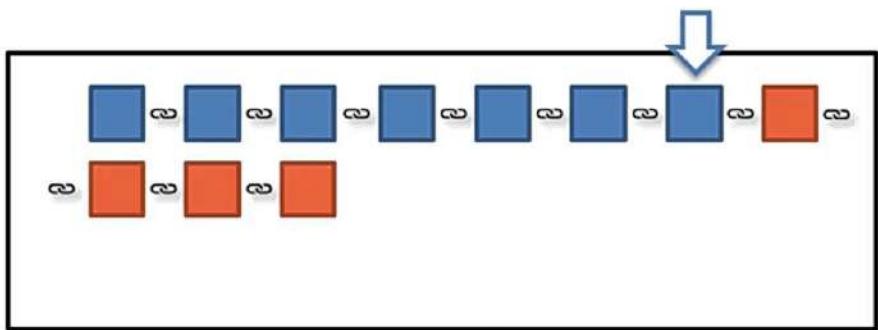
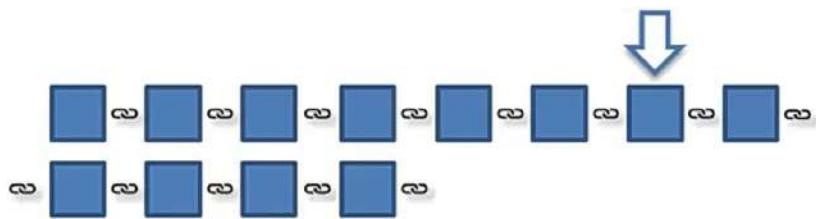
# 51% Attack



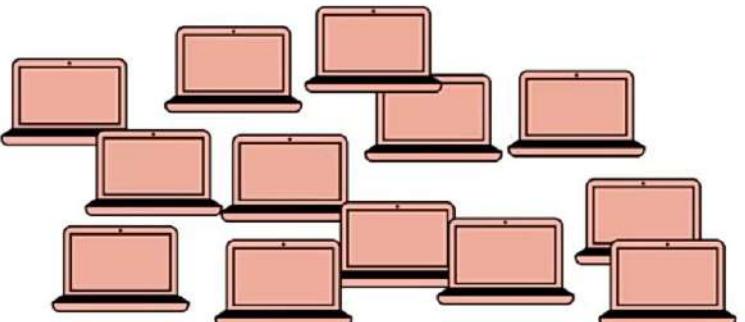
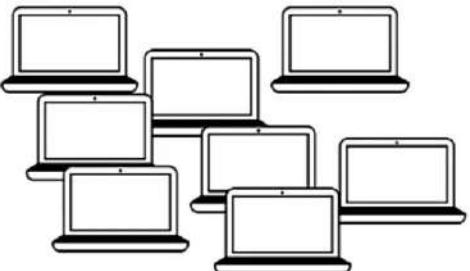
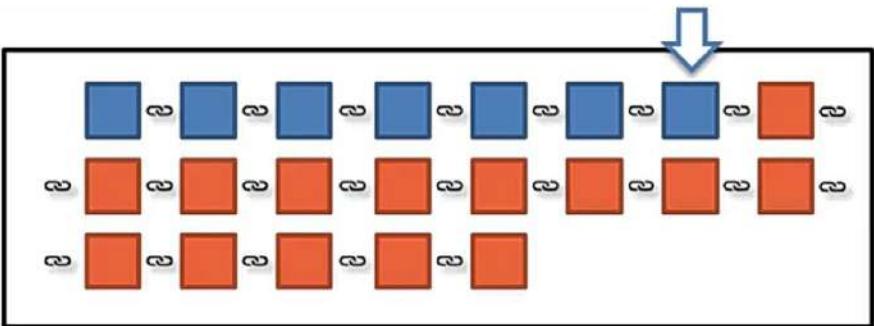
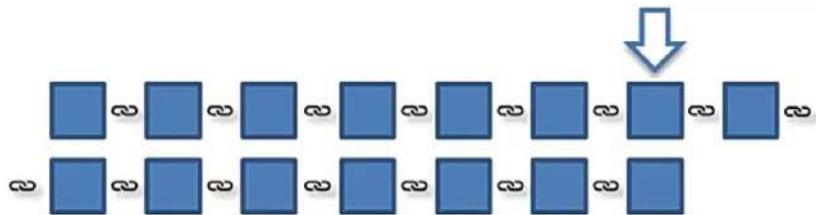
# 51% Attack



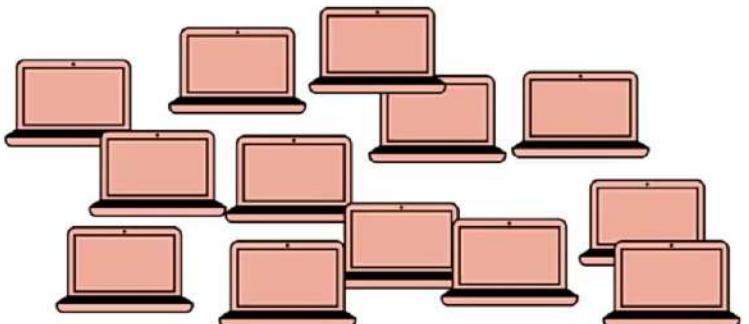
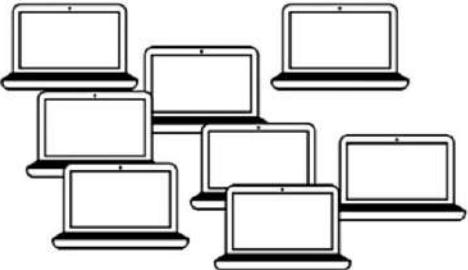
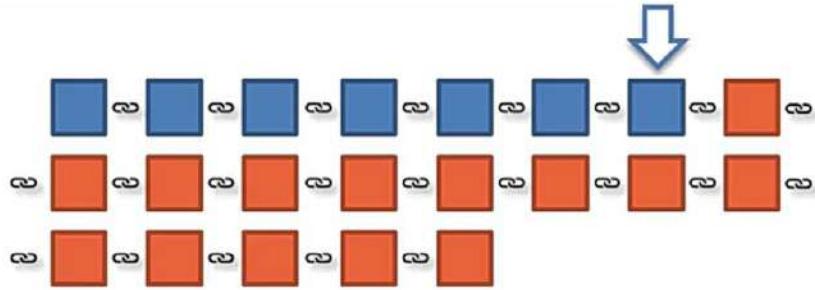
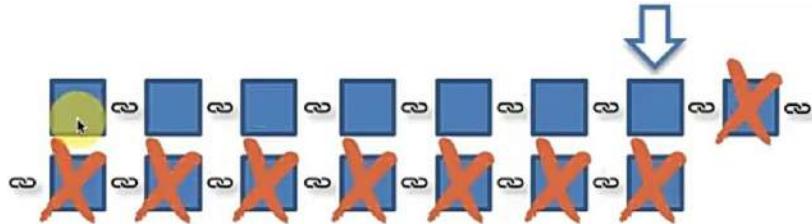
# 51% Attack



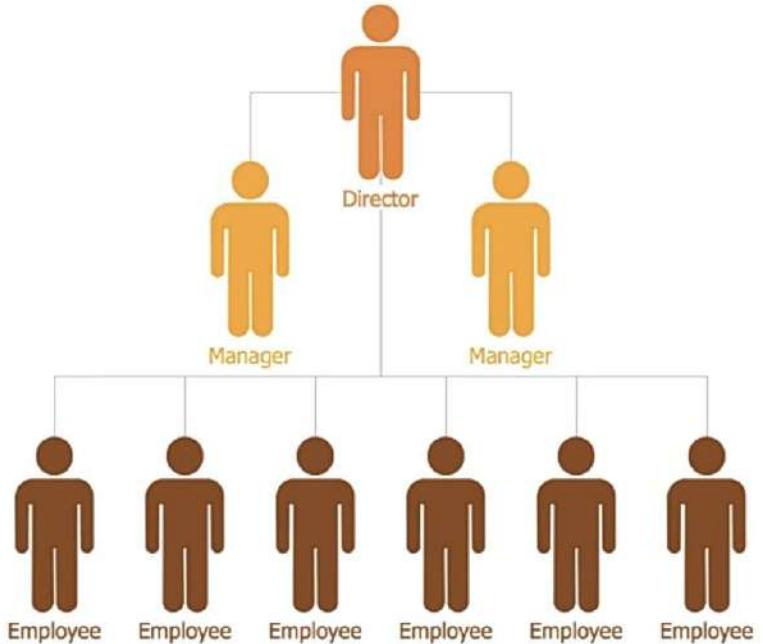
# 51% Attack



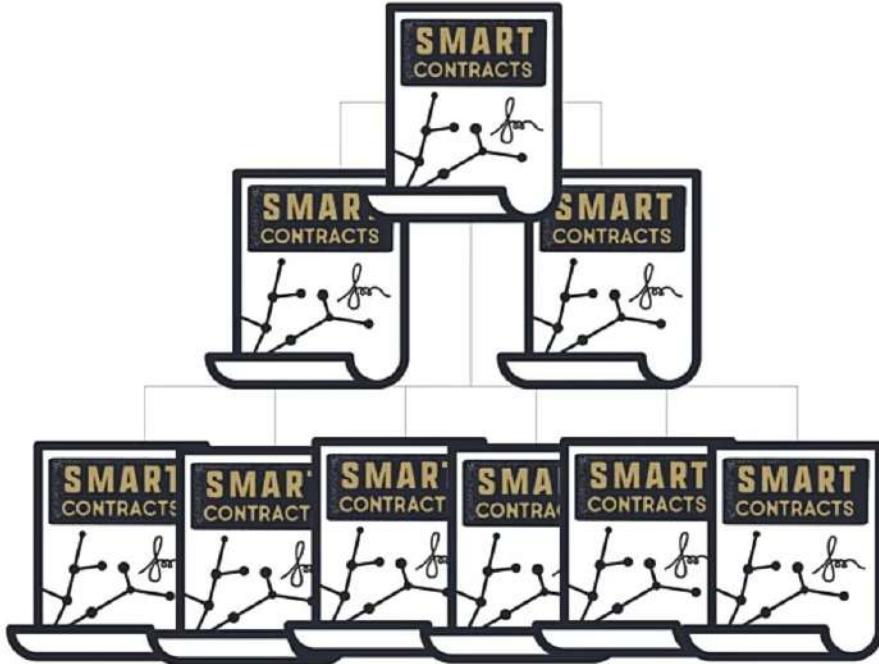
# 51% Attack



# Decentralized Autonomous Organizations



# Decentralized Autonomous Organizations



# Decentralized Autonomous Organizations



# Decentralized Autonomous Organizations



# Decentralized Autonomous Organizations



# Decentralized Autonomous Organizations



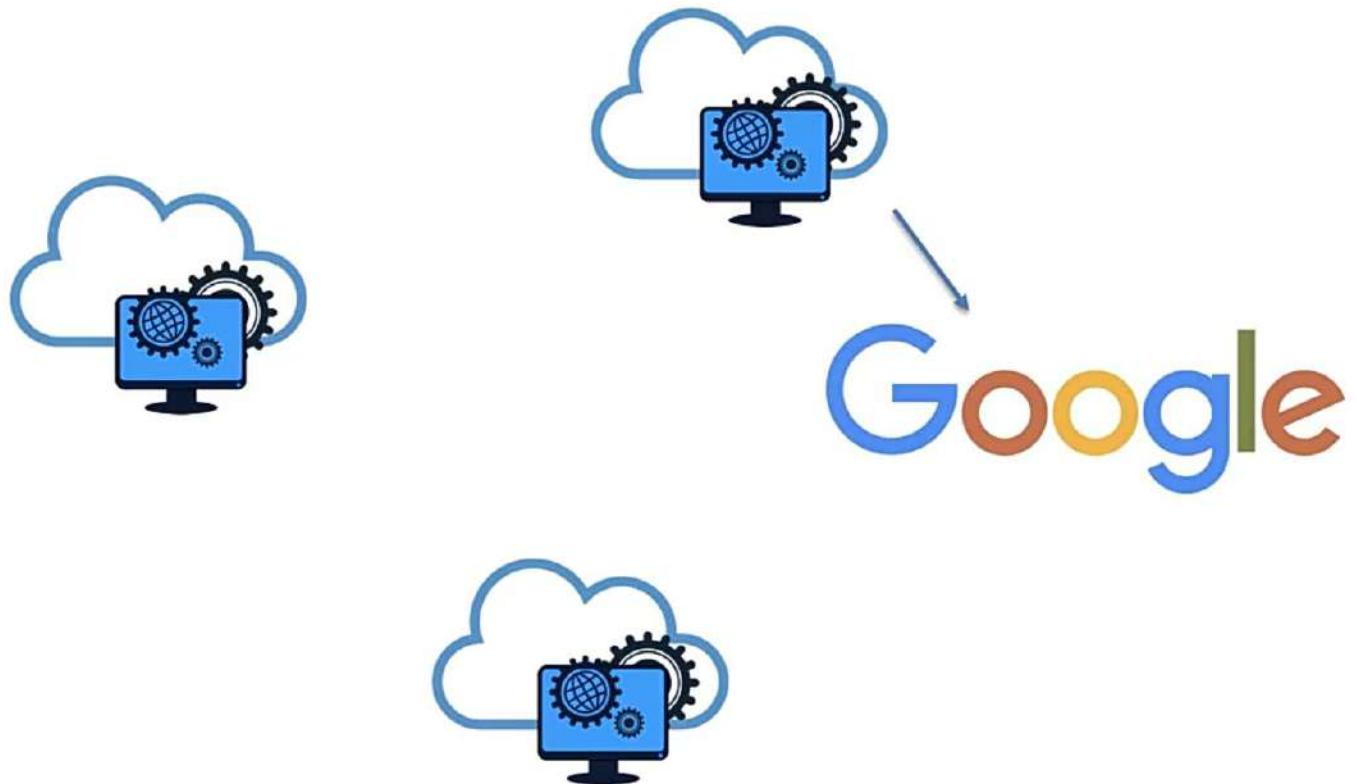
# Decentralized Autonomous Organizations



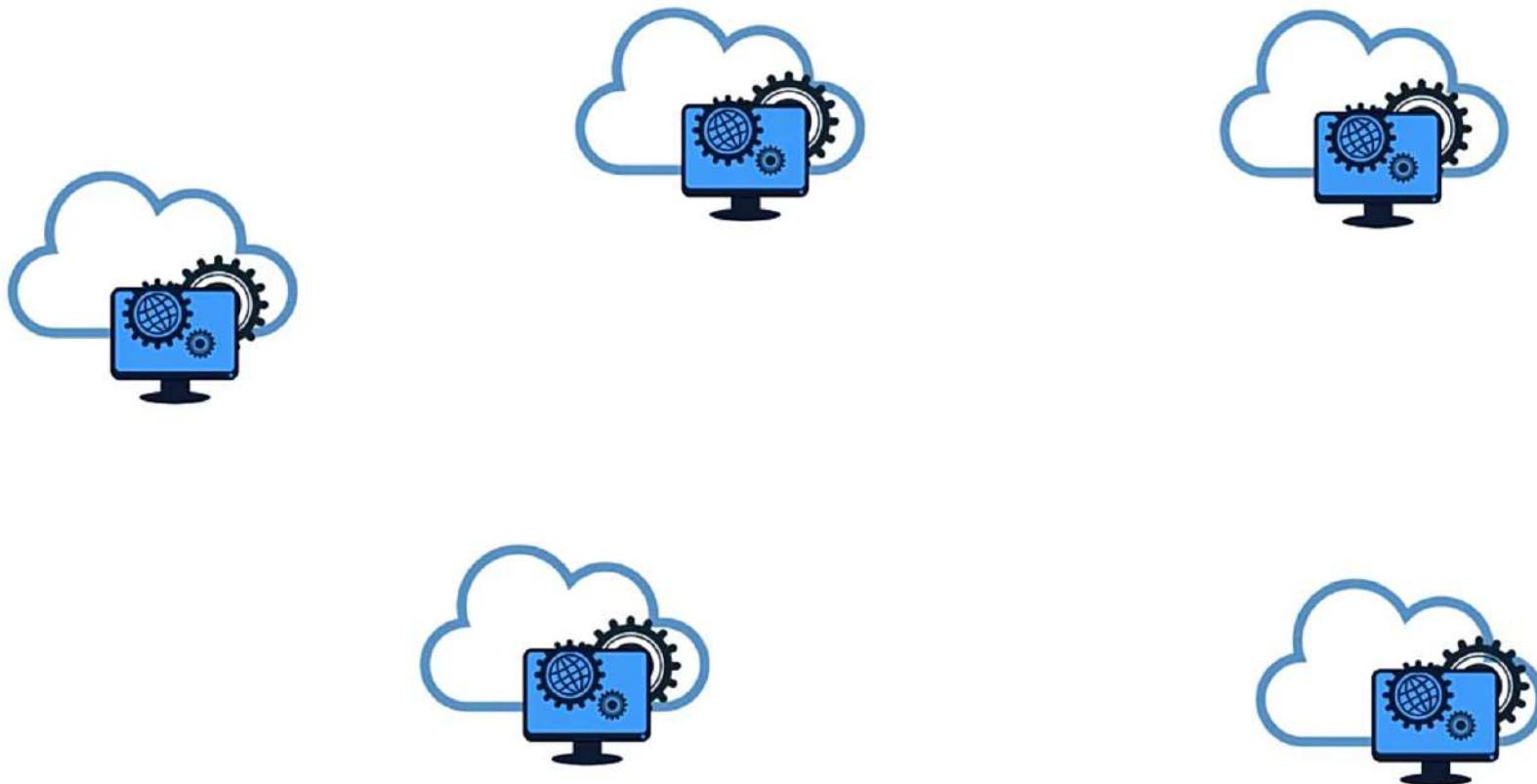
# Decentralized Autonomous Organizations



# Decentralized Autonomous Organizations



# Decentralized Autonomous Organizations



# Decentralized Autonomous Organizations

2016

On Ethereum

Investor-directed venture capital fund

Stateless

May 2016 Crowdfunded ~\$150,000,000

June 2016 Hacked for ~\$50,000,000

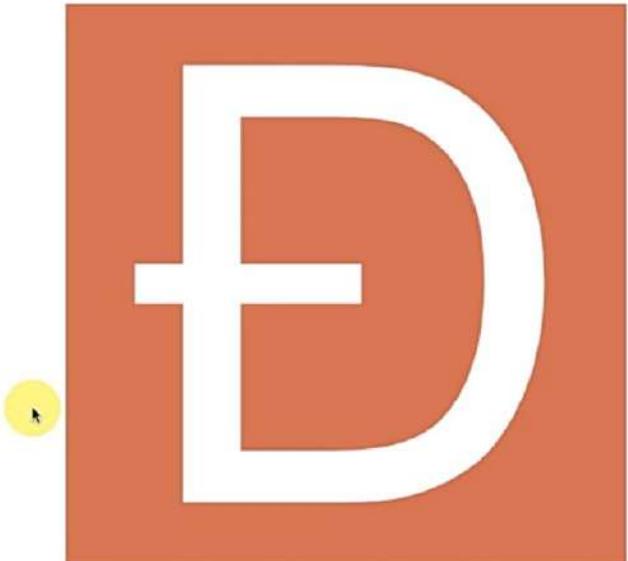
Dilemma: "*Code Is Law?*"

Hard fork

Ethereum split into ETH and ETC

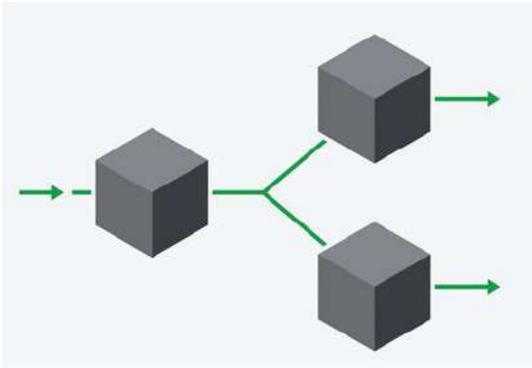
Hacker walked away with ~\$67,000,000 in ETC

Problem in DAO code not Ethereum



# Blockchain Forks

- A blockchain split that produces two competing branches.
- Can be **accidental** or **intentional**.
- **Accidental forks** are resolved by the blockchain.
- Intentional forks are used to implement new consensus rules.
  - a. **Hard forks** require nodes to be upgraded to the new consensus rules or to rollback the state.
  - b. **Soft forks** don't require nodes to be upgraded to the new consensus rules.



NB: Some cryptocurrencies, like **Bitcoin Cash**, are created using hard forks.

Courtesy : <https://blog.bitstamp.net/post/what-are-blockchain-forks/>

# Blockchain Forks

## Accidental Forks

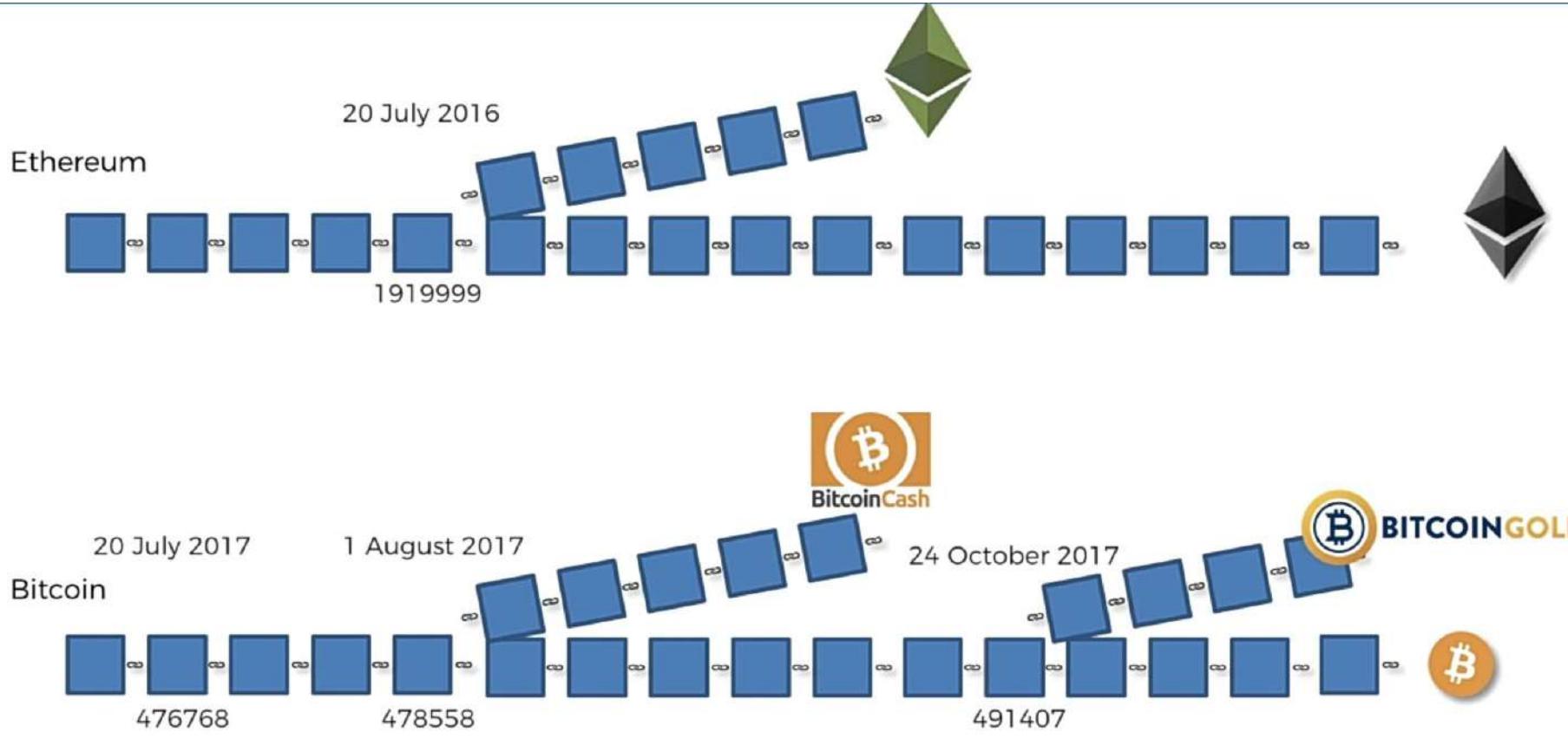
- At any given moment, thousands of miners are competing to create a new block.
- With so much mining going on at once, two or more miners sometimes mine a new block at the same time.
- When this happens, an **accidental fork** is created.
- The problem is solved when new blocks are added to one of the chains. When that happens, the network continues working on the longer chain and abandons the shorter one.

# Blockchain Forks

## Intentional forks

- When an **intentional fork** is made, the network doesn't reconverge on a single chain.
- This type of a fork is used by blockchain developers to implement changes to the protocol.
- For instance, developers may use an intentional fork to increase block size, reduce block time, or even implement an entirely new consensus algorithm.
- An intentional fork can be **hard** or **soft**. The two differ from each other in terms of compatibility with the other chain and their applications.

# Soft & Hard Forks

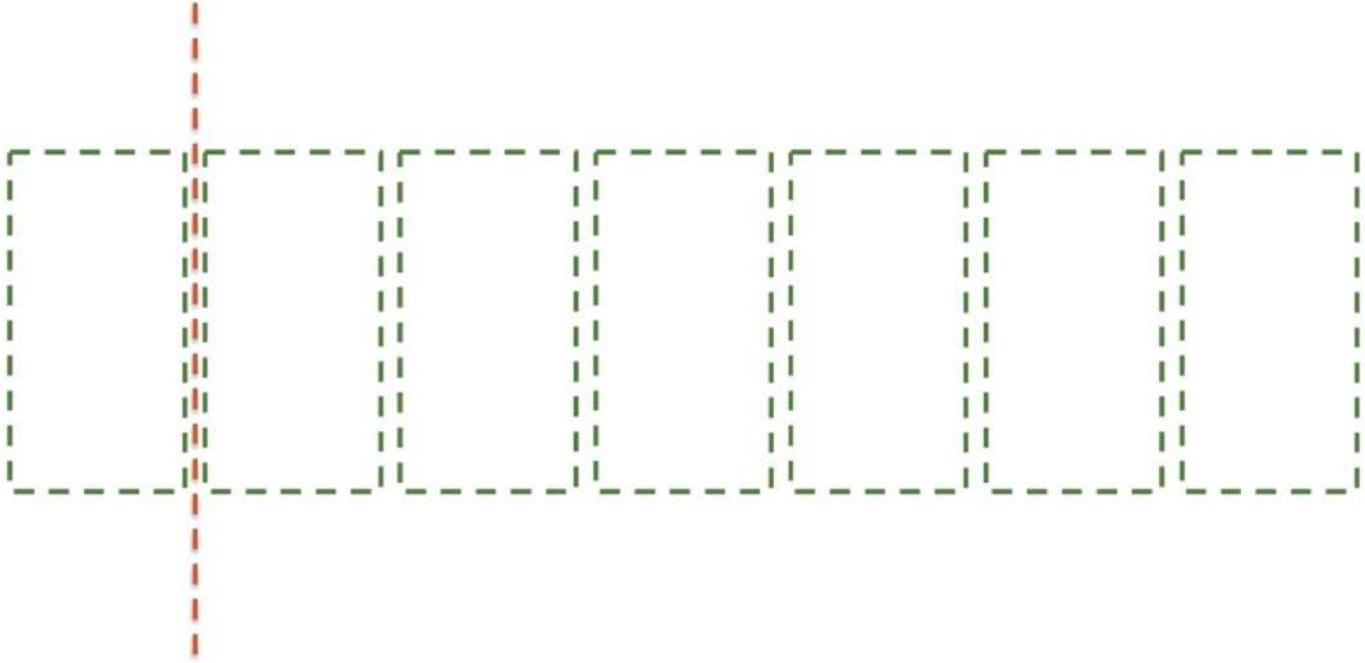


# Soft & Hard Forks

Hard Forks = Loosen Rules

Soft Forks = Tighten Rules

# Soft & Hard Forks



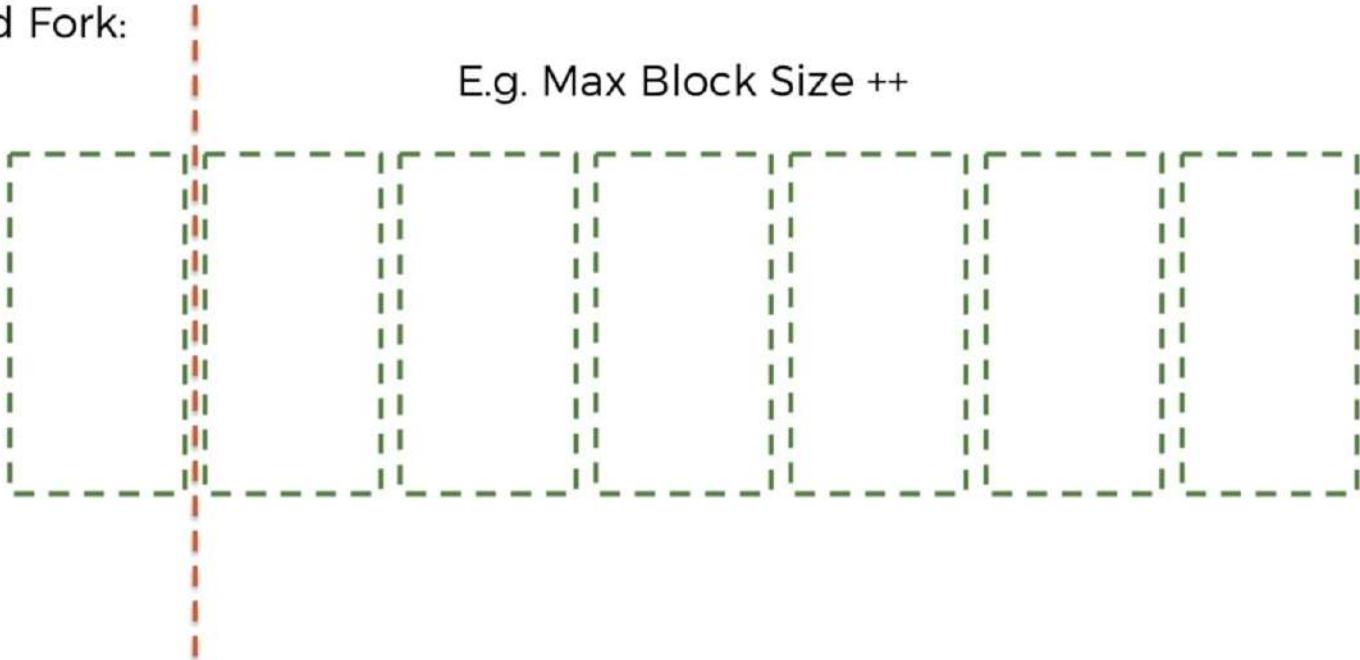
# Soft & Hard Forks

Hard Fork:

E.g. Max Block Size ++

Haven't  
upgraded

Have  
upgraded



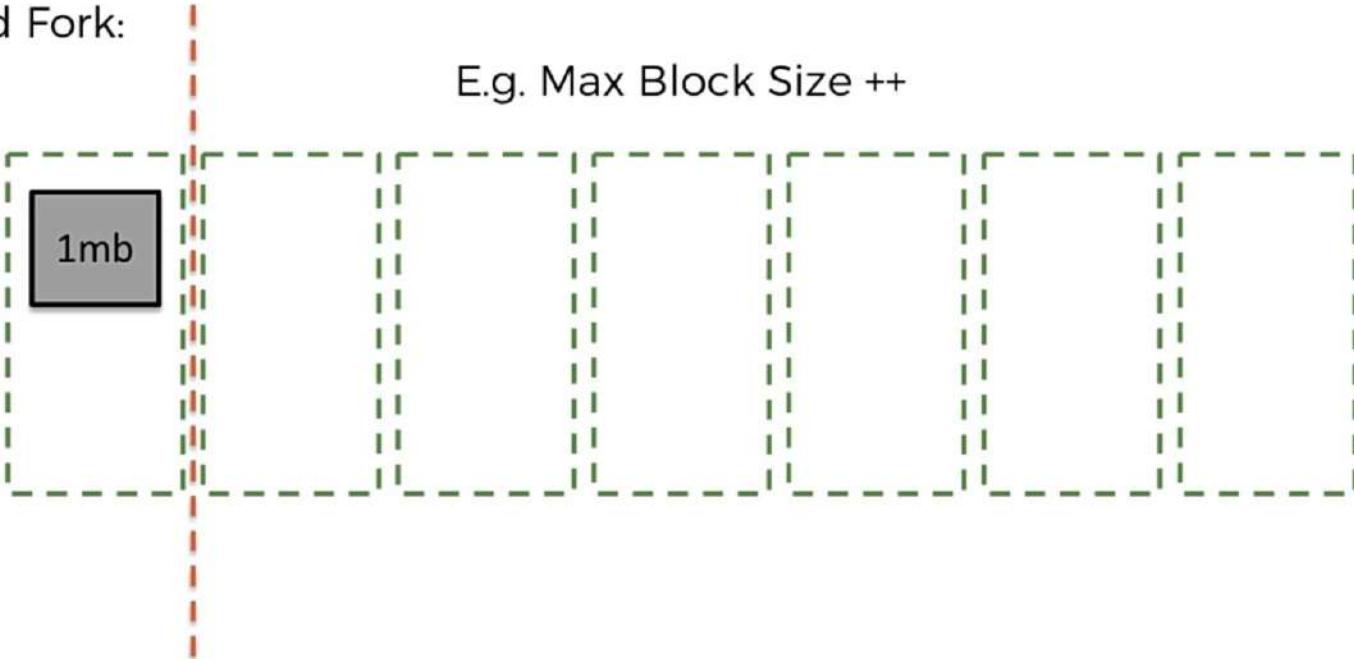
# Soft & Hard Forks

Hard Fork:

E.g. Max Block Size ++

Haven't upgraded

Have upgraded



# Soft & Hard Forks

Hard Fork:

E.g. Max Block Size ++

Haven't  
upgraded



Have  
upgraded



# Soft & Hard Forks

Hard Fork:

E.g. Max Block Size ++

Haven't upgraded



Have upgraded



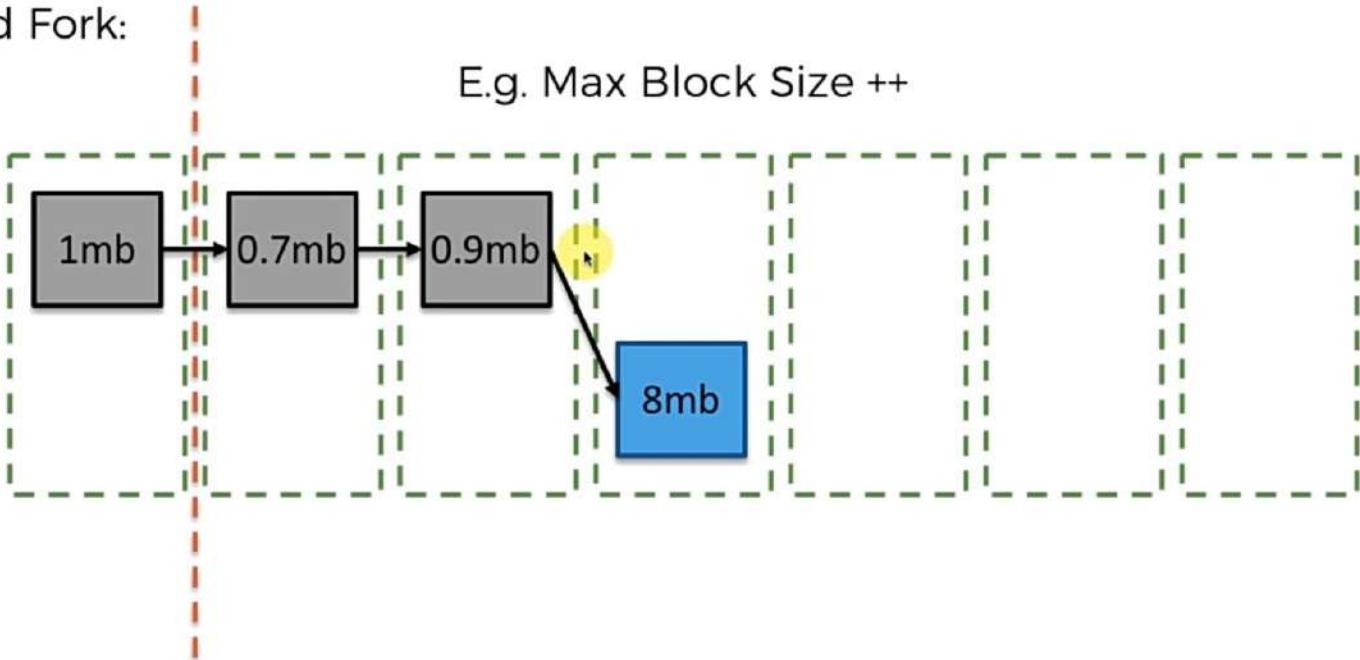
# Soft & Hard Forks

Hard Fork:

E.g. Max Block Size ++

Haven't upgraded

Have upgraded



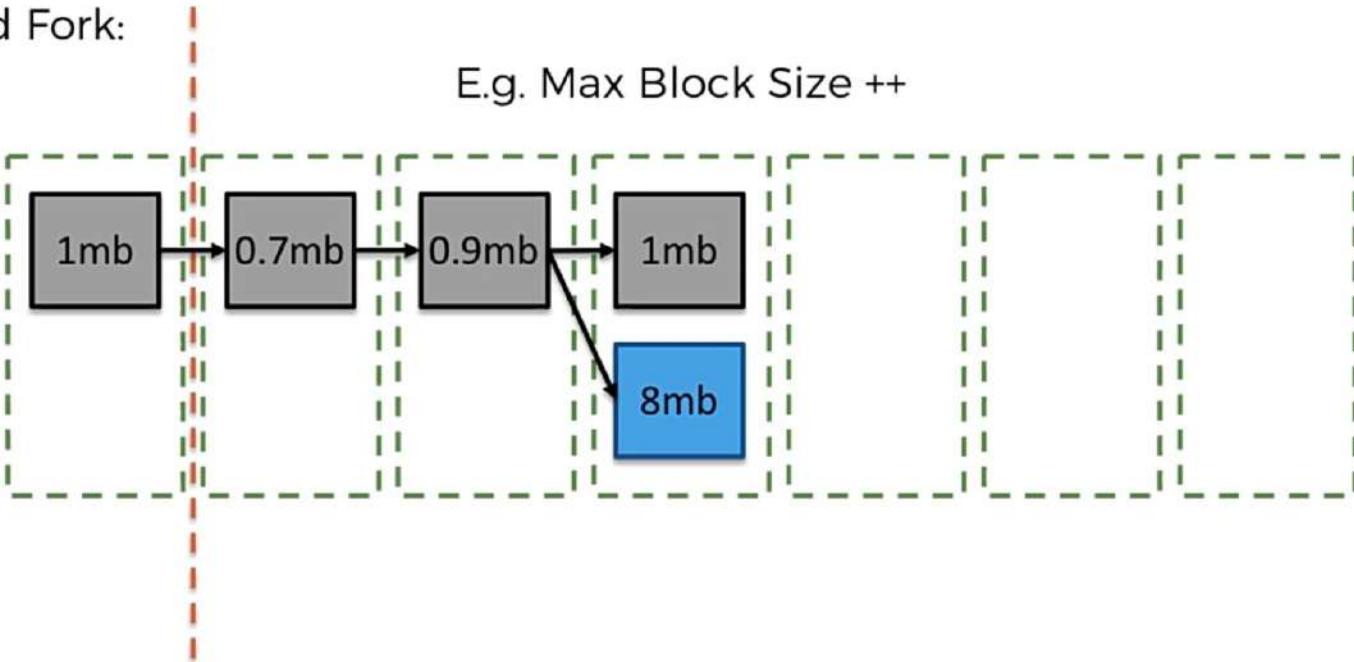
# Soft & Hard Forks

Hard Fork:

E.g. Max Block Size ++

Haven't  
upgraded

Have  
upgraded



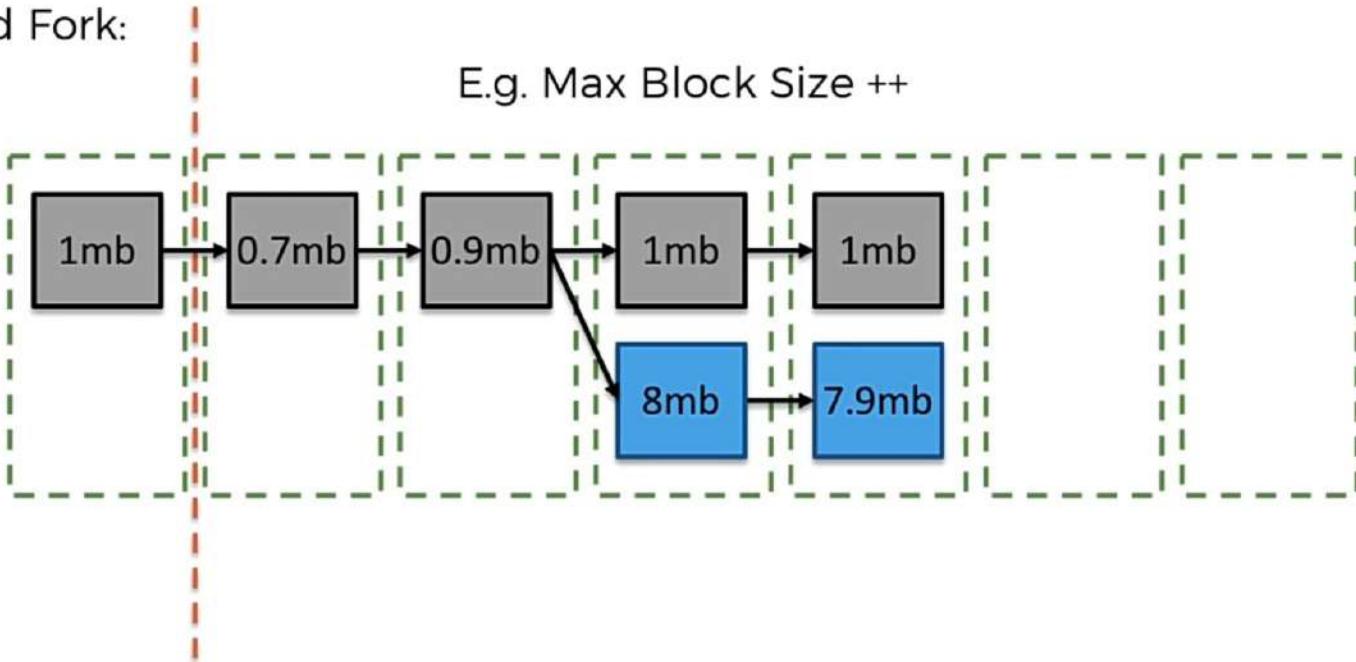
# Soft & Hard Forks

Hard Fork:

E.g. Max Block Size ++

Haven't  
upgraded

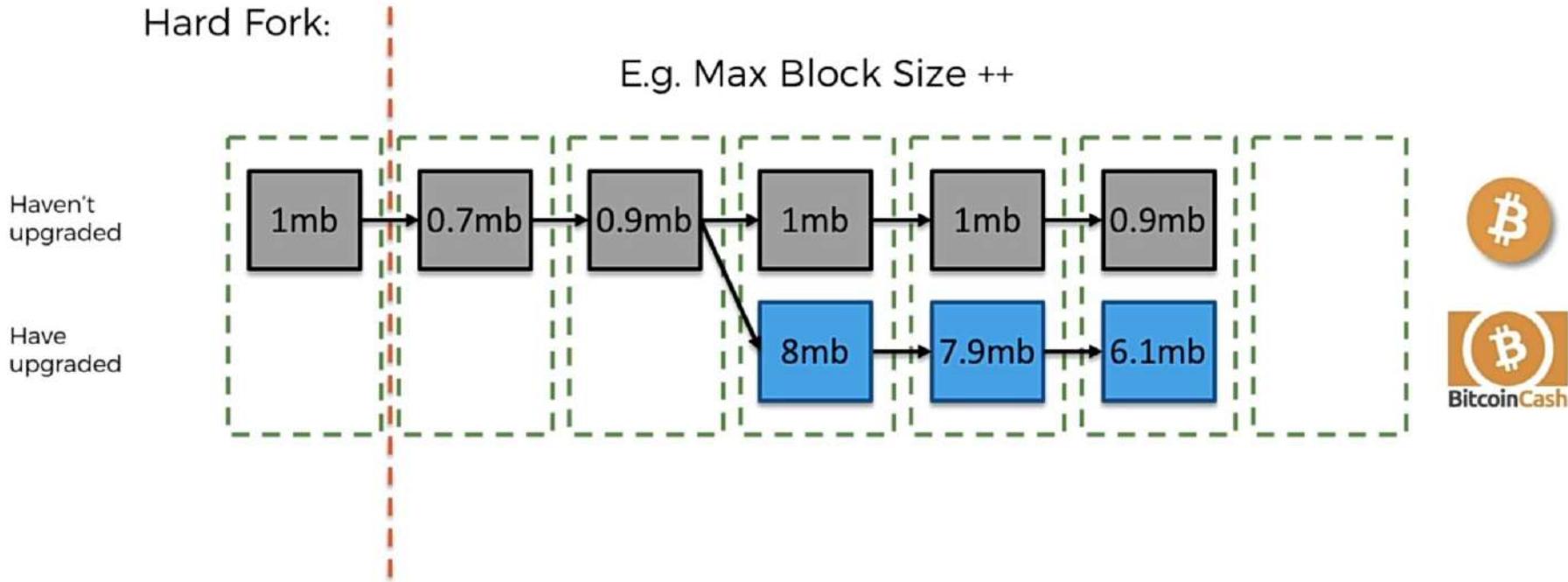
Have  
upgraded



# Soft & Hard Forks

## Hard Fork:

E.g. Max Block Size ++



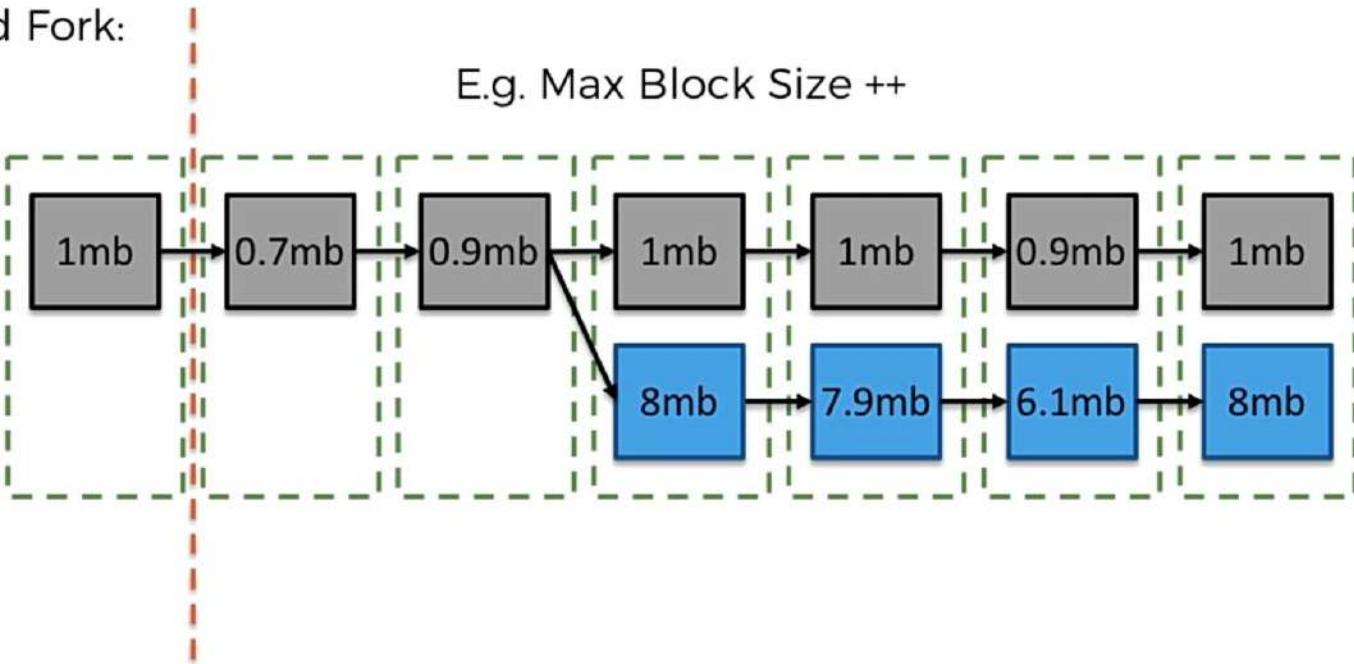
# Soft & Hard Forks

Hard Fork:

E.g. Max Block Size ++

Haven't upgraded

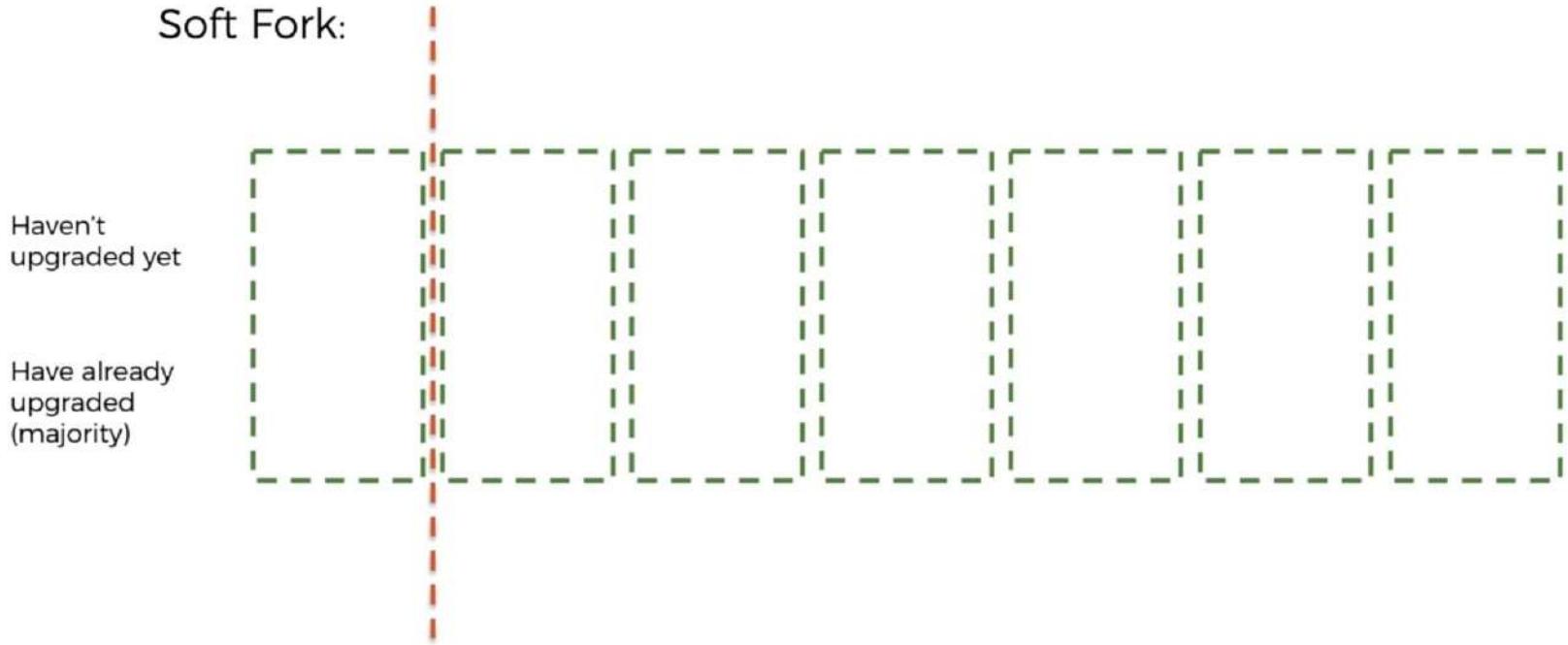
Have upgraded



BitcoinCash

# Soft & Hard Forks

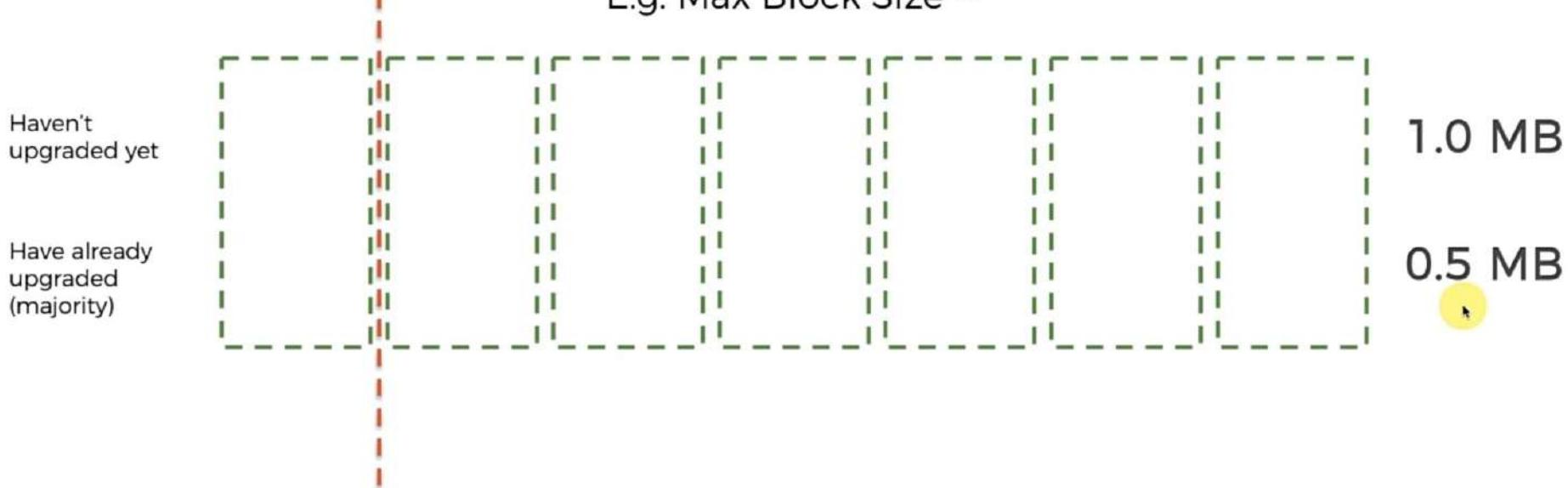
Soft Fork:



# Soft & Hard Forks

Soft Fork:

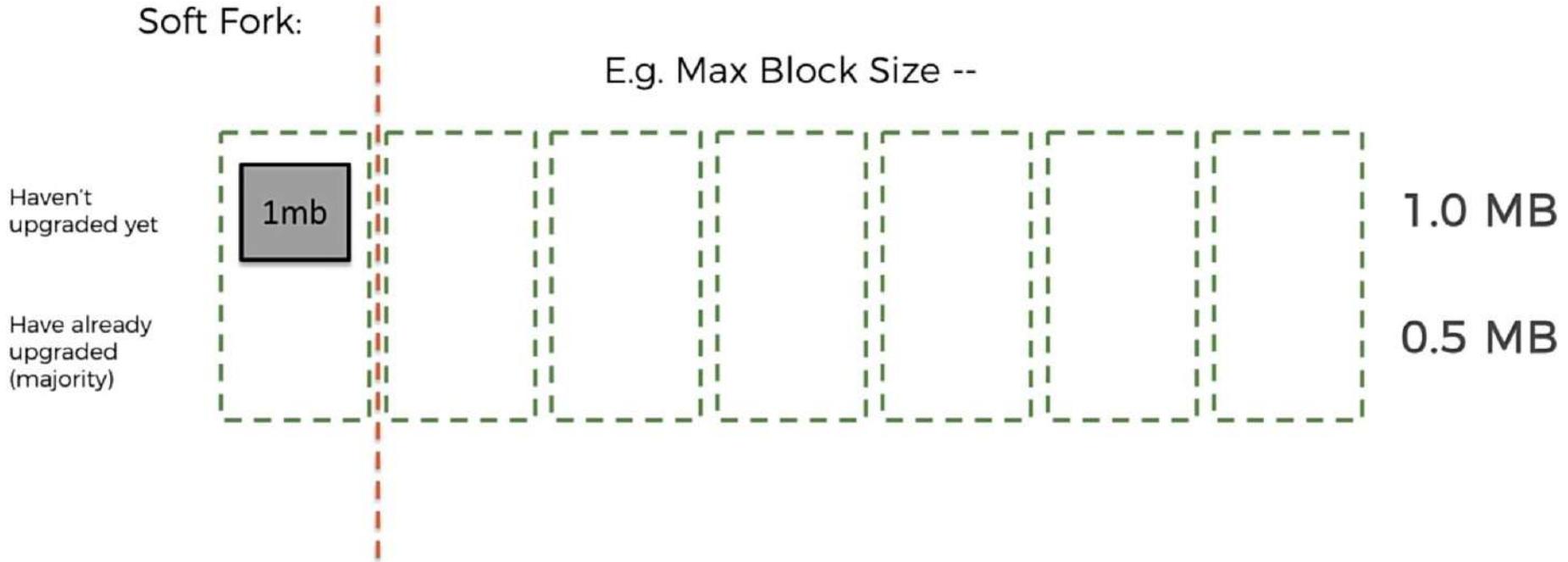
E.g. Max Block Size --



# Soft & Hard Forks

Soft Fork:

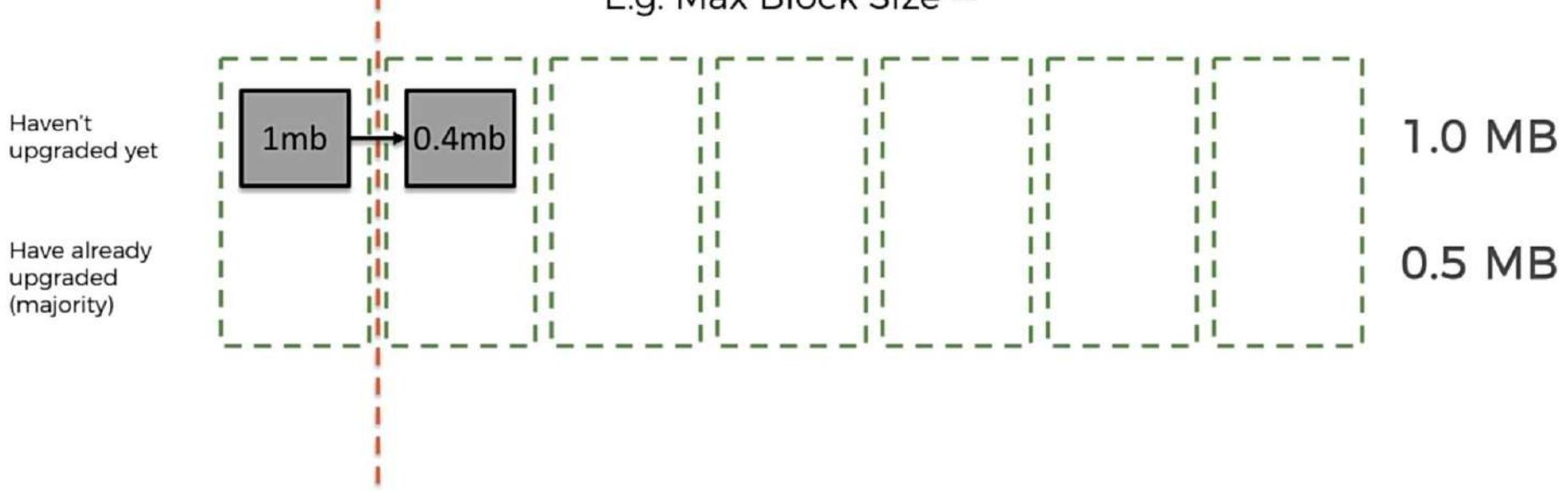
E.g. Max Block Size --



# Soft & Hard Forks

Soft Fork:

E.g. Max Block Size --



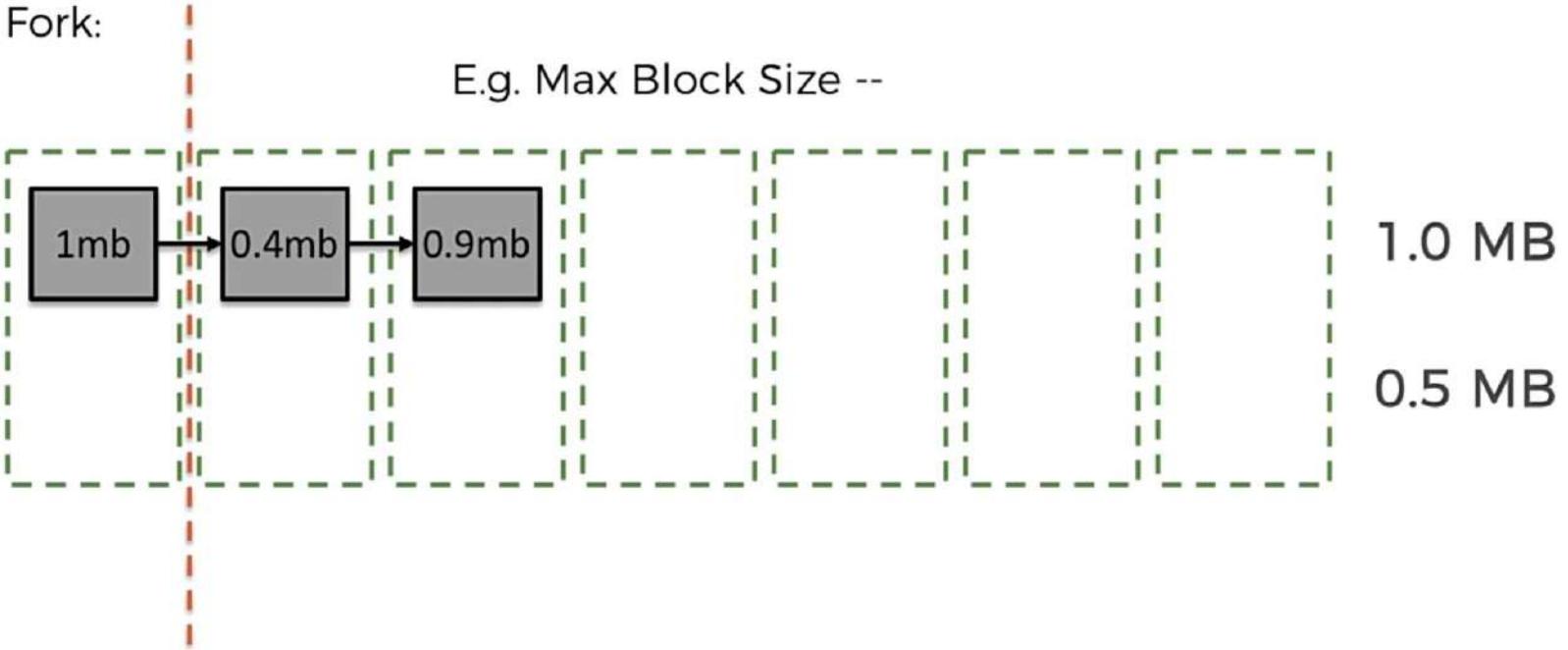
# Soft & Hard Forks

Soft Fork:

E.g. Max Block Size --

Haven't upgraded yet

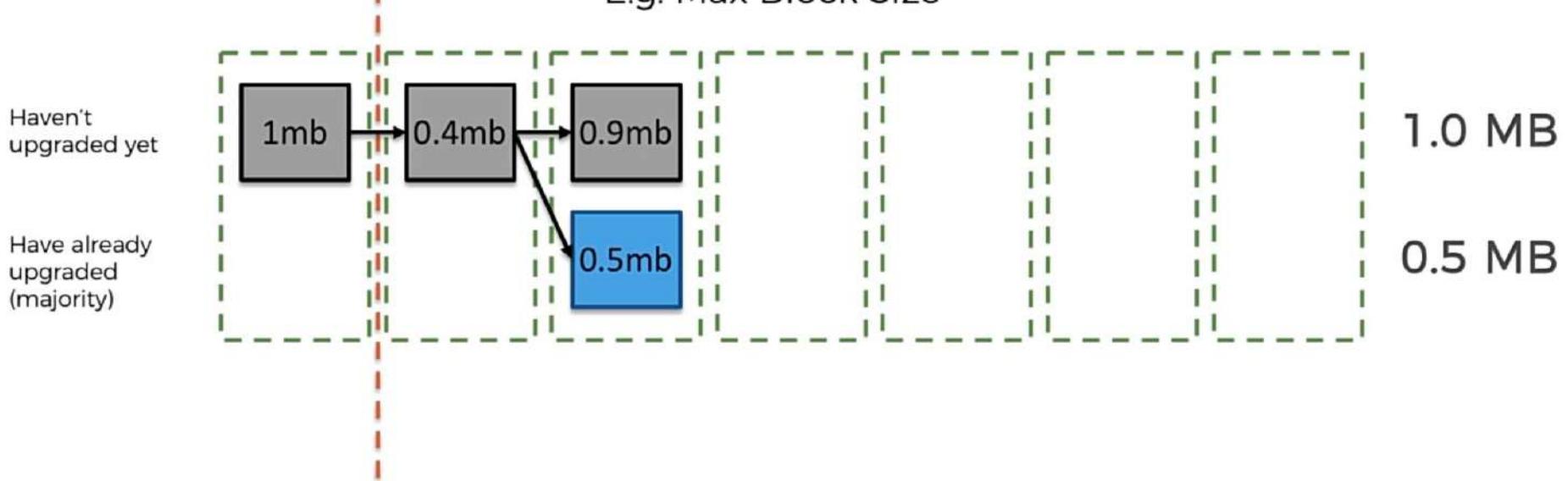
Have already upgraded (majority)



# Soft & Hard Forks

Soft Fork:

E.g. Max Block Size --



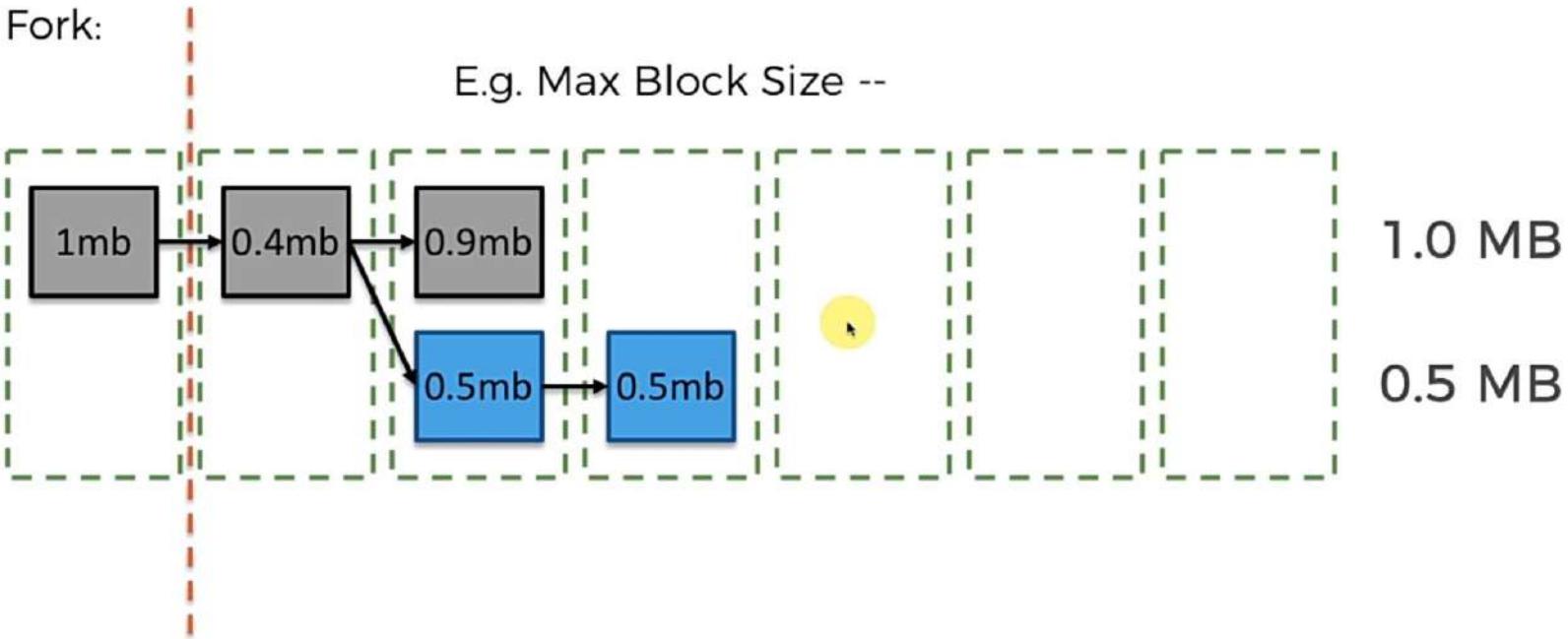
# Soft & Hard Forks

Soft Fork:

E.g. Max Block Size --

Haven't upgraded yet

Have already upgraded  
(majority)



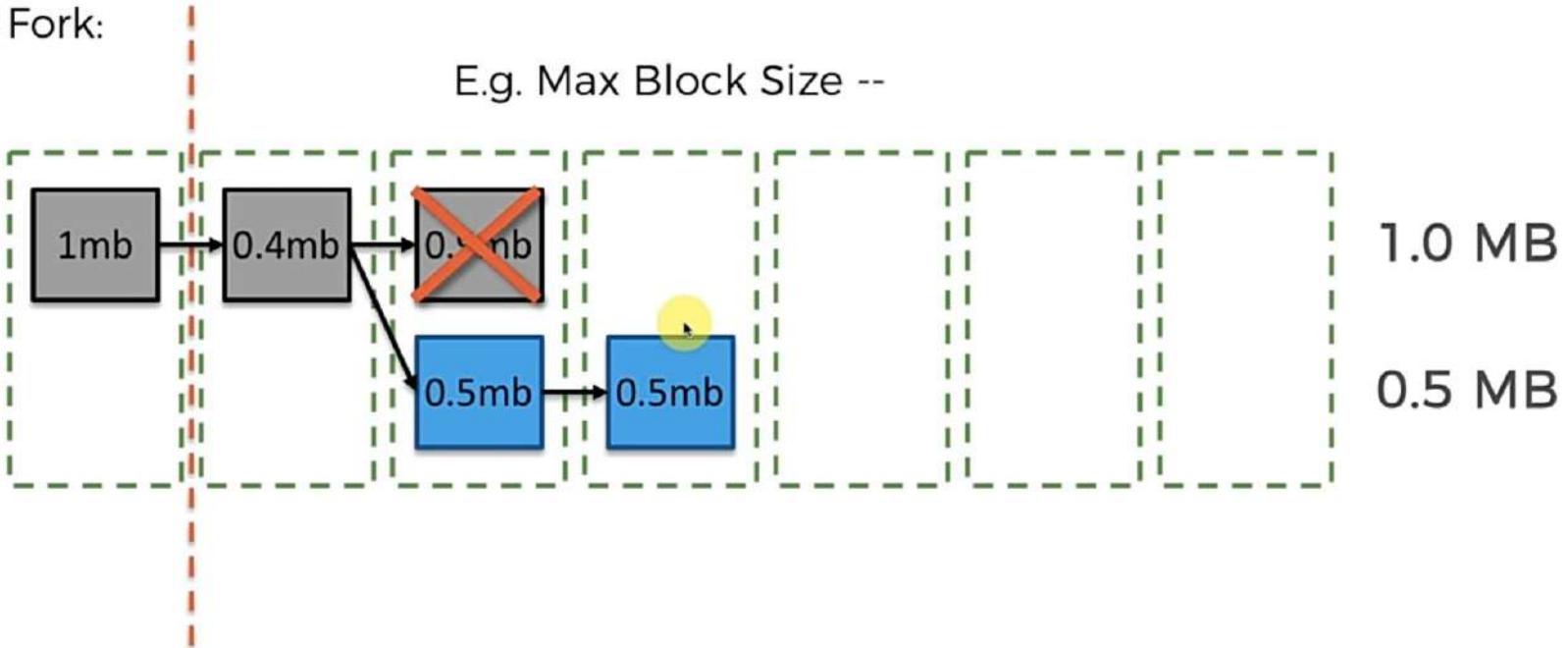
# Soft & Hard Forks

Soft Fork:

E.g. Max Block Size --

Haven't upgraded yet

Have already upgraded  
(majority)



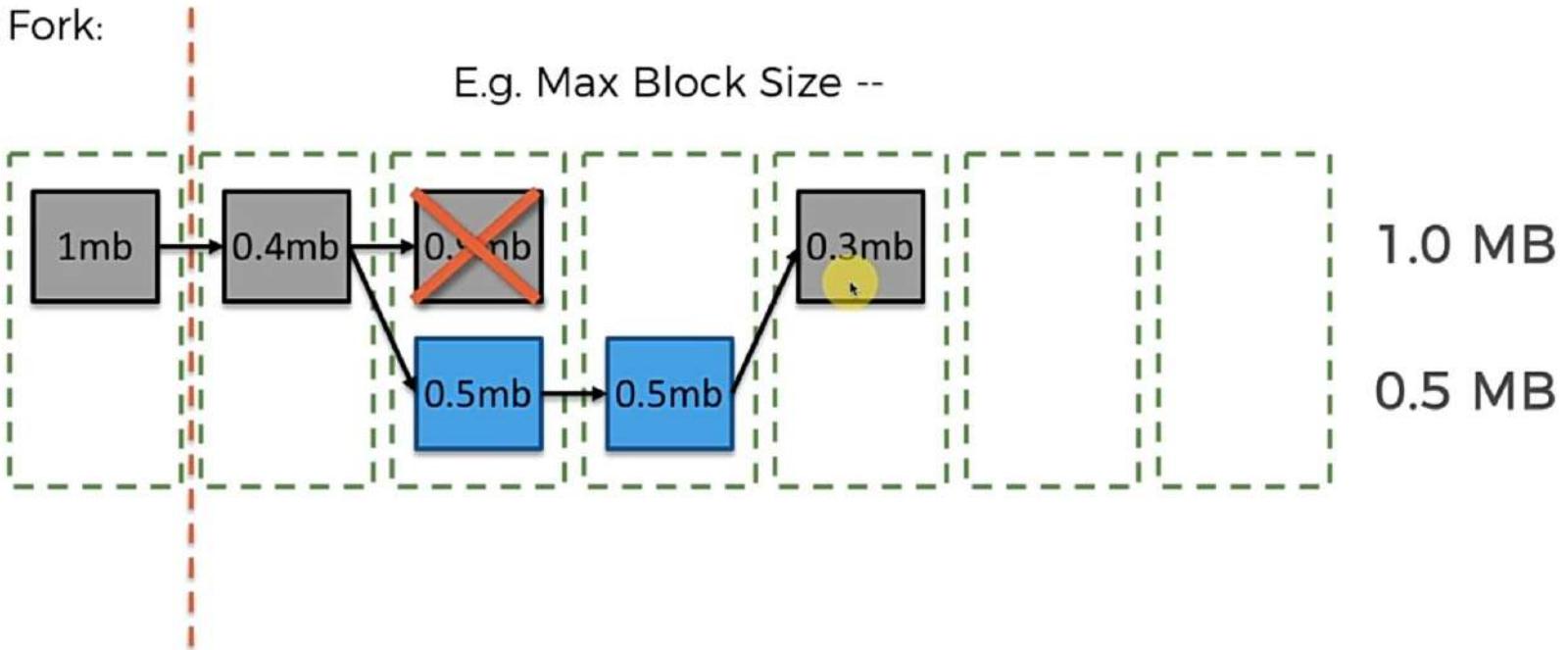
# Soft & Hard Forks

Soft Fork:

E.g. Max Block Size --

Haven't upgraded yet

Have already upgraded (majority)



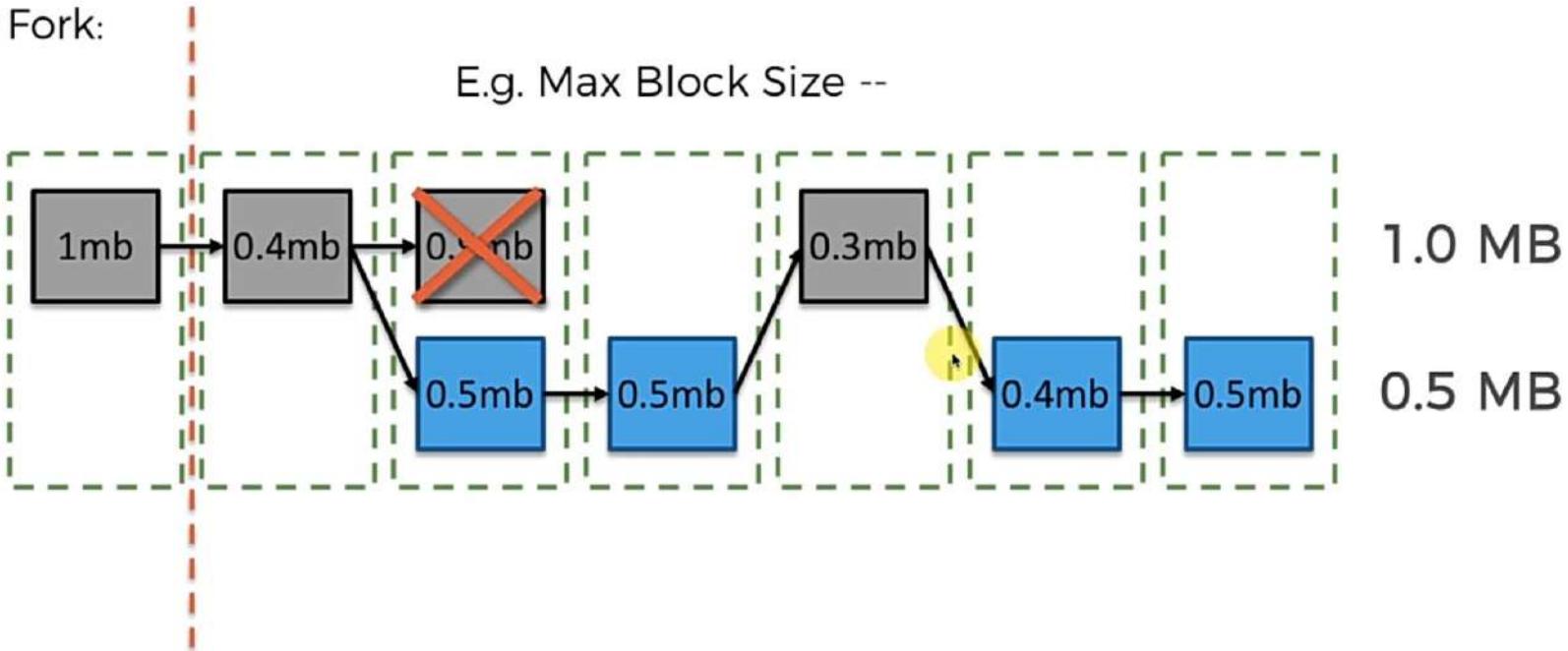
# Soft & Hard Forks

Soft Fork:

E.g. Max Block Size --

Haven't upgraded yet

Have already upgraded  
(majority)



# Different Consensus Algorithms

1. Proof of Work (PoW)
2. Proof of Elapsed Time(PoET)
3. Proof of Stake (PoS)
4. Delegated Proof of Stake (DPoS)
5. Proof of Authority (PoA)
6. Practical Byzantine Fault Tolerance
7. RAFT

# Other Consensus Algorithms

1. Proof of Stake Anonymous (PoSA):
2. Leased Proof of Stake (LPoS):
3. Proof of Importance (PoI):
4. Proof of Storage
5. Proof of Burn
6. Proof of Activity
7. Proof of Capacity
8. Directed Acyclic Graph (DAG)