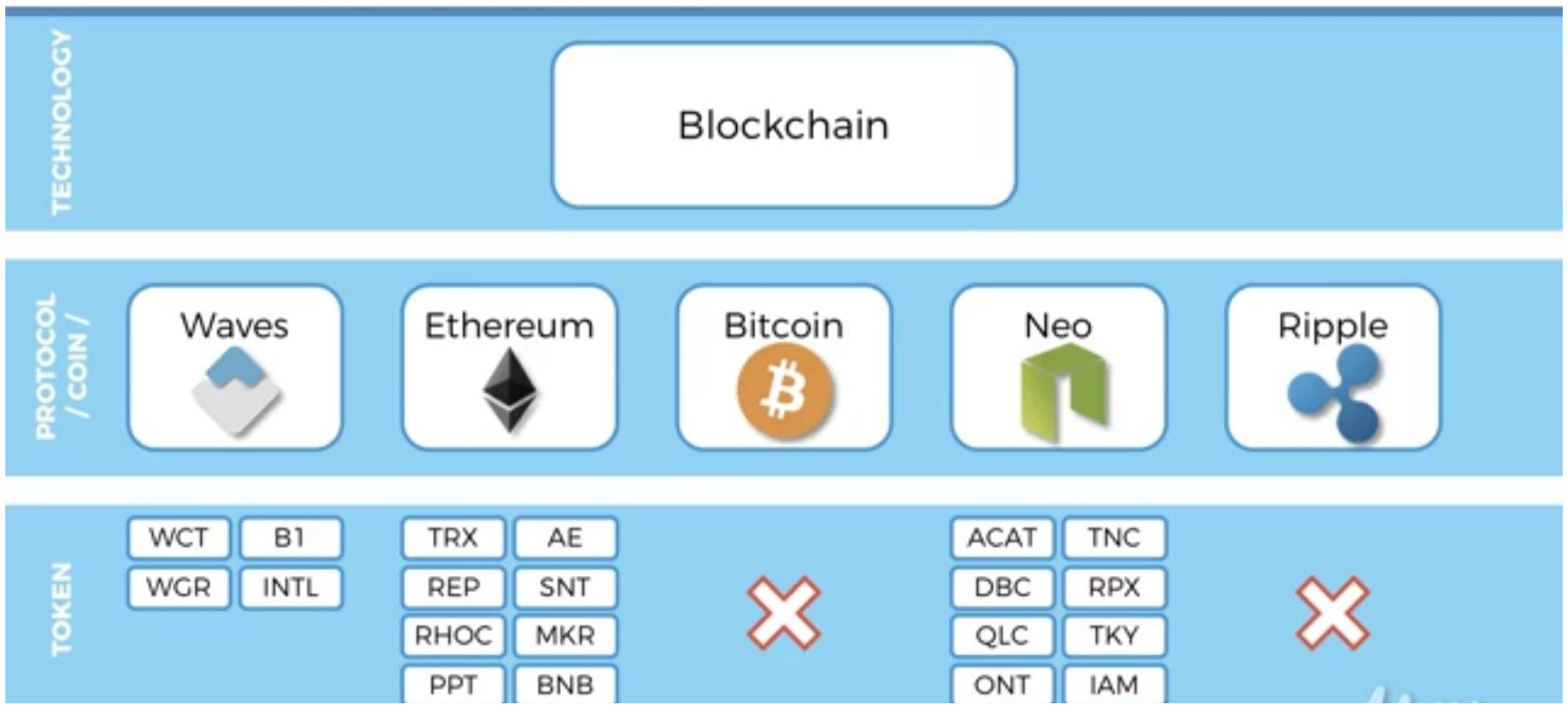
What we will learn in this section:

- What is Bitcoin?
- Bitcoin's Monetary Policy
- Understanding Mining Difficulty
- Virtual tour of a Bitcoin Mine
- Mining Pools
- Nonce Range
- How Miners Pick Transactions (Part 1)
- How Miners Pick Transactions (Part 2)
- CPUs vs GPUs vs ASICs
- How do Mempools work?
- Orphaned blocks
- The 51% Attack
- Extra: Bits to Target conversion

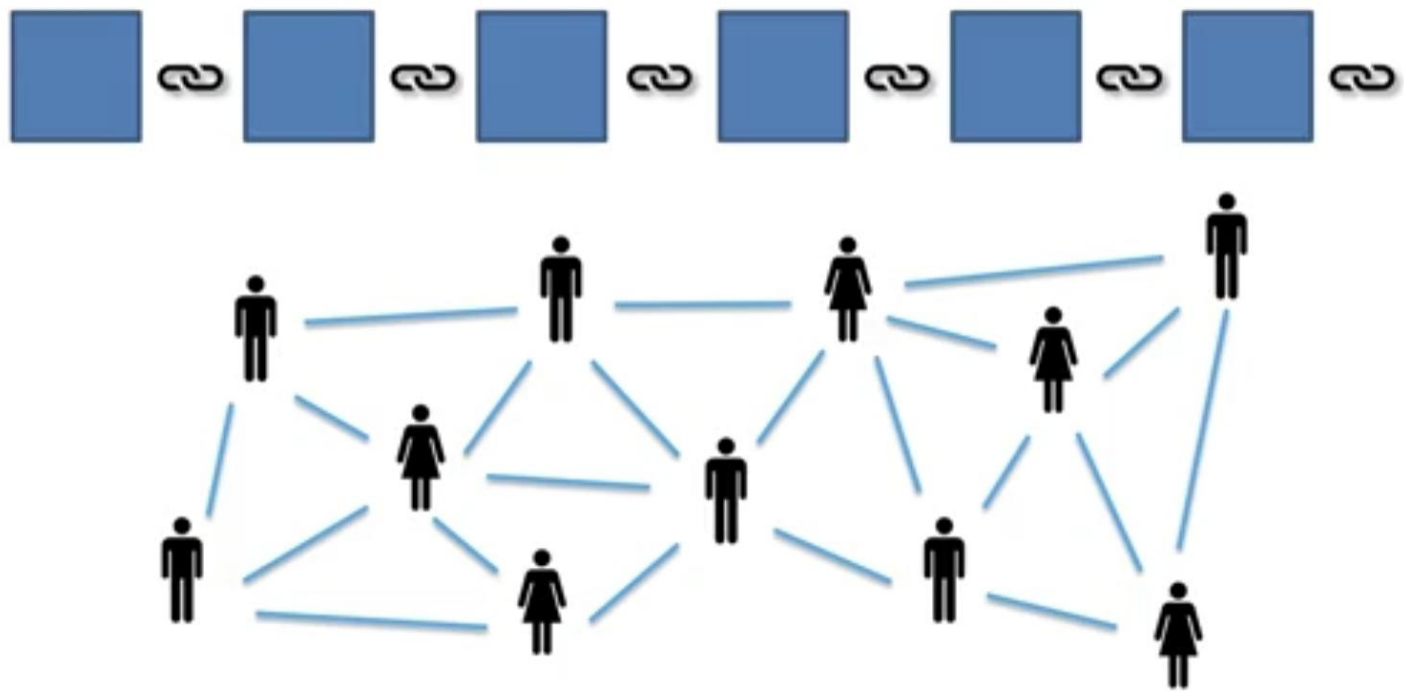
What is Bitcoin?



What is Bitcoin?

Satoshi Nakamoto

What is Bitcoin?

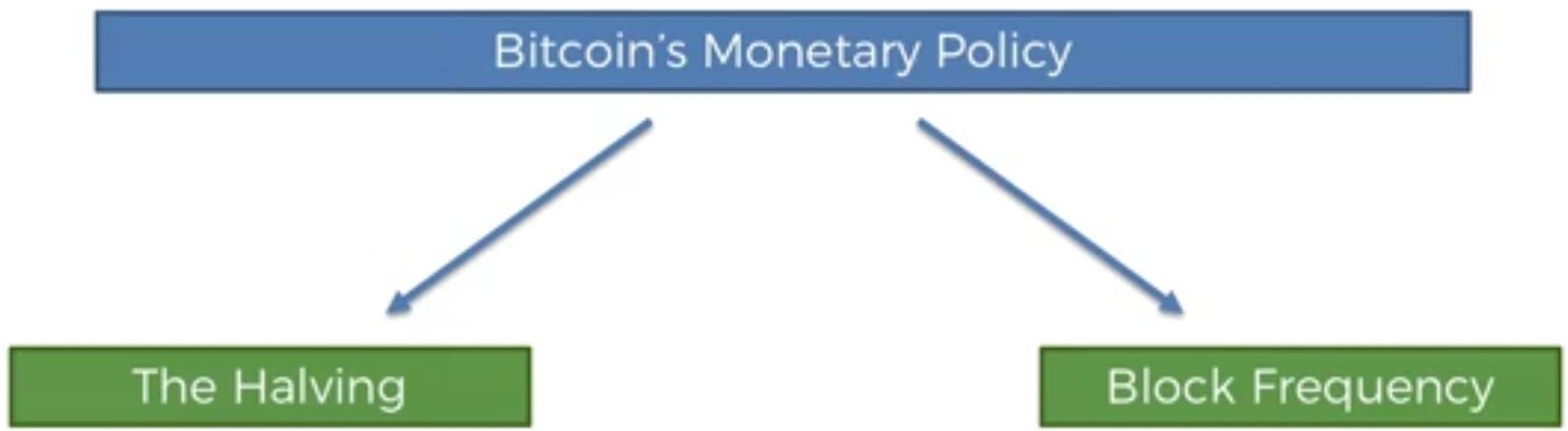


What is Bitcoin?

The Bitcoin Ecosystem:

- Nodes 
- Miners 
- Large Mines 
- Mining Pools 

Bitcoin's Monetary Policy



Bitcoin's Monetary Policy

The Halving

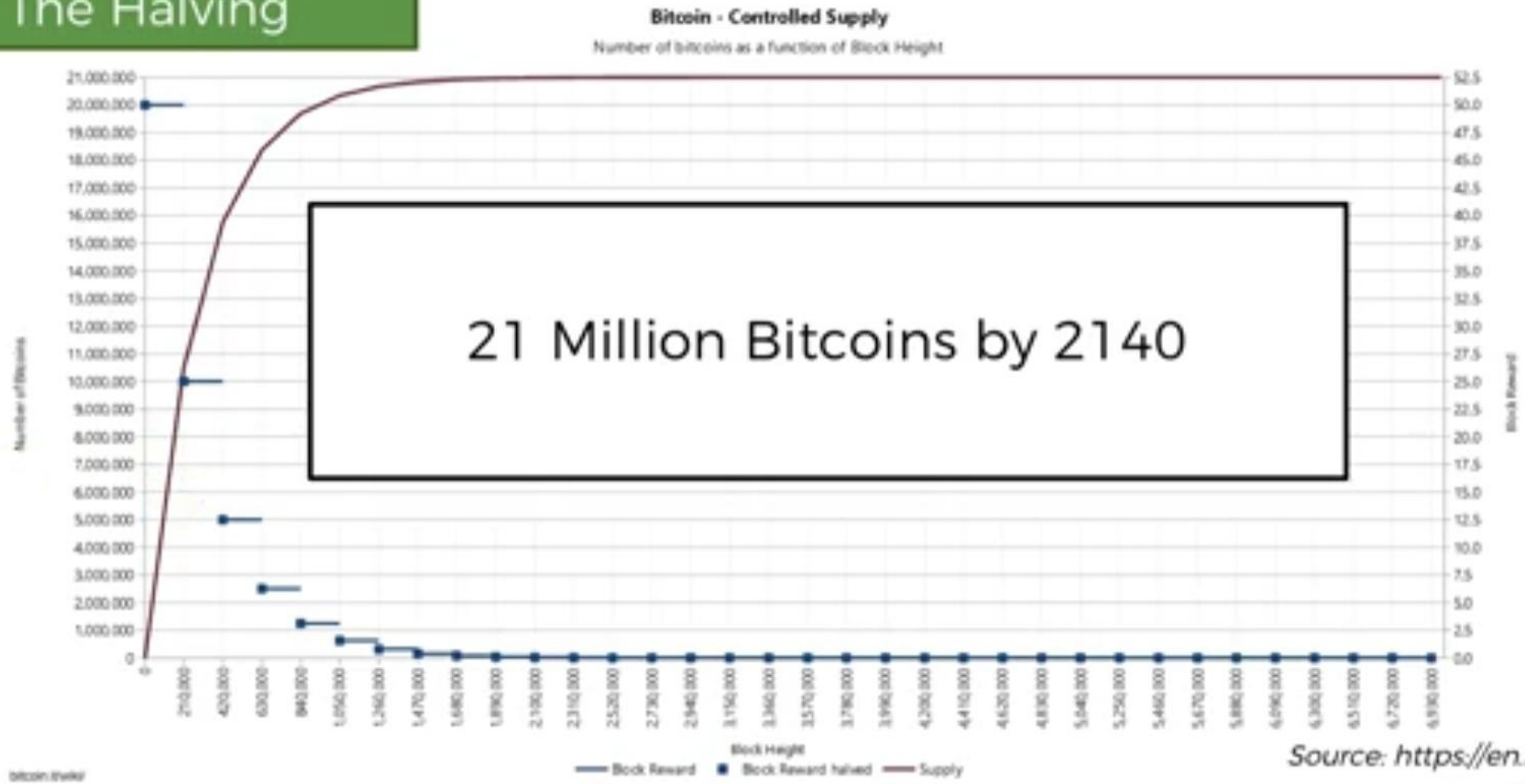
~2020: 6.25

~2024: 3.125

Date reached	Block	Reward Era	BTC/block
2009-01-03	0	1	50.00
2010-04-22	52500	1	50.00
2011-01-28	105000	1	50.00
2011-12-14	157500	1	50.00
2012-11-28	210000	2	25.00
2013-10-09	262500	2	25.00
2014-08-11	315000	2	25.00
2015-07-29	367500	2	25.00
2016-07-09	420000	3	12.50
2017-06-23	472500	3	12.50

Bitcoin's Monetary Policy

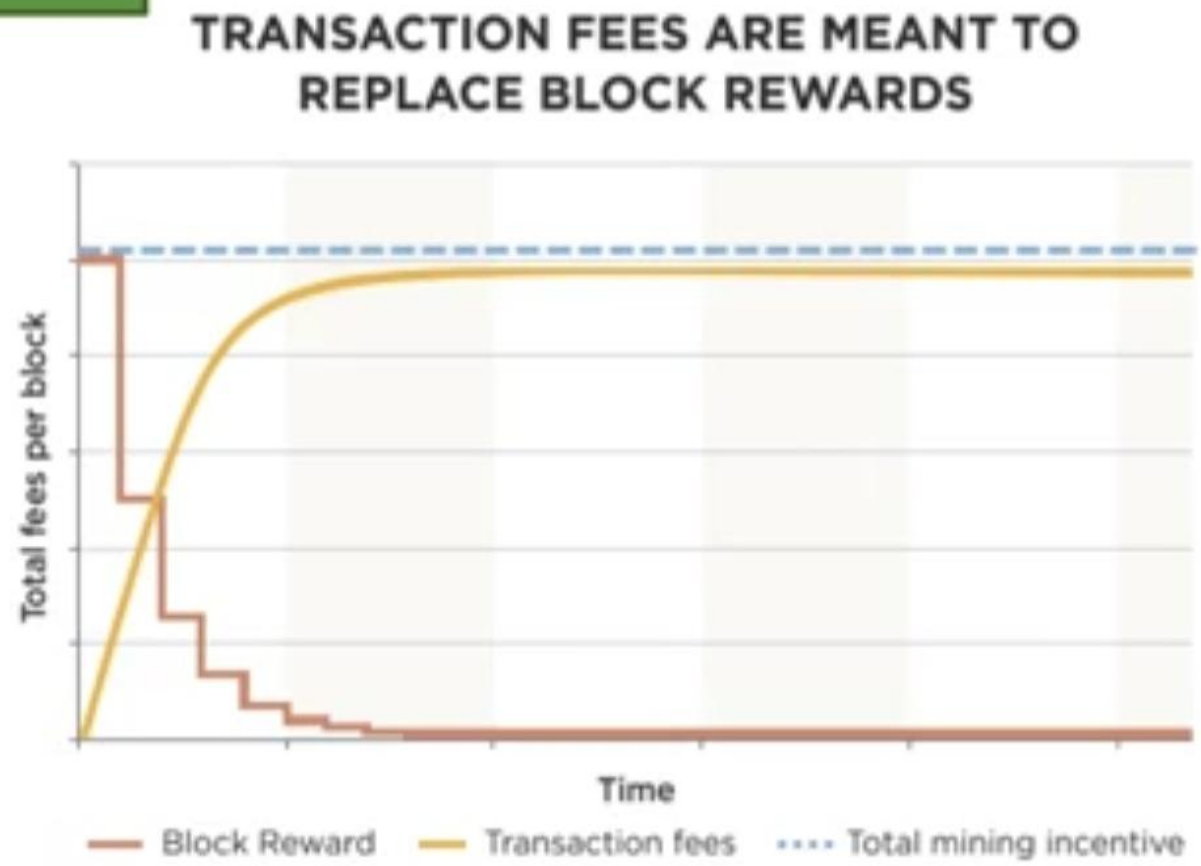
The Halving



Source: https://en.bitcoin.it/wiki/

Bitcoin's Monetary Policy

The Halving



Source: https://bitsonblocks.net

Bitcoin's Monetary Policy

Block Frequency

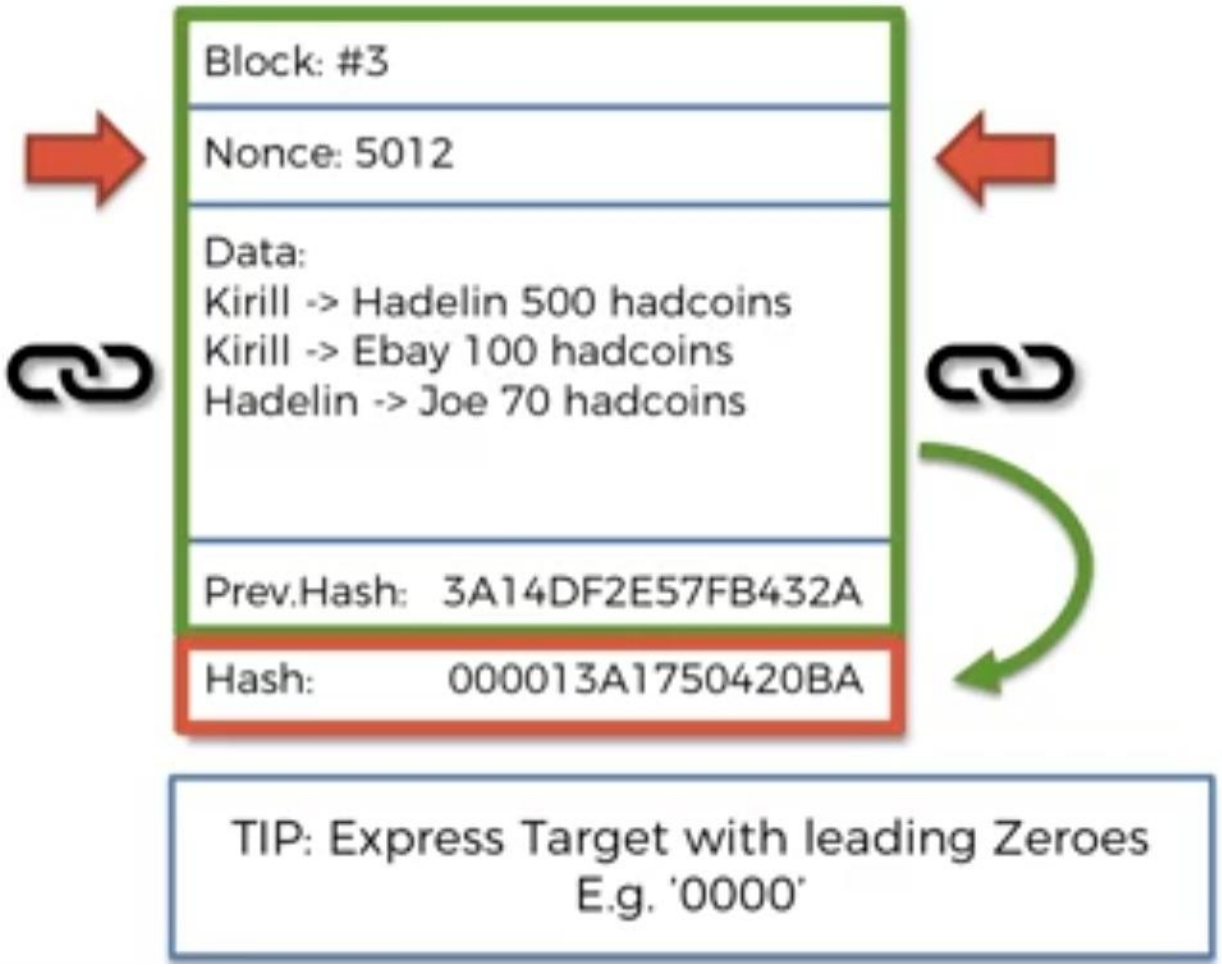
Cryptocurrency	Average block time
bitcoin	10 min
ethereum	15 sec
ripple	3.5 sec
litecoin	2.5 min

Understanding Mining Difficulty

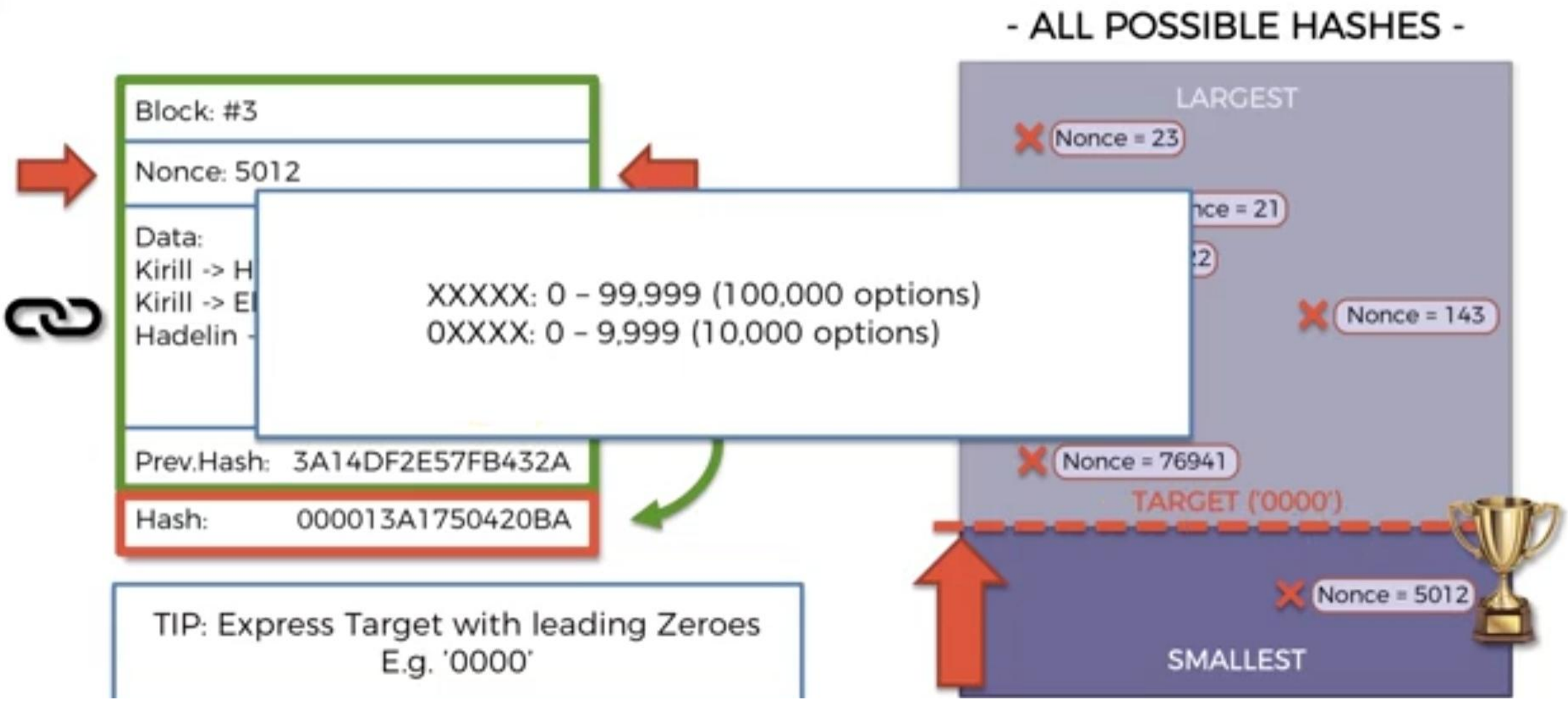
Today we will answer these questions:

- What is the Current Target and how does that *feel?*
- How is “Mining Difficulty” calculated?

Understanding Mining Difficulty



Understanding Mining Difficulty



Understanding Mining Difficulty

Current target = 00000000000000005d97dc0000000000000000000000000000000000000000

18 zeros

Let's do some estimations:

Probability:

Total possible 64-digit hexadecimal numbers: $16 \times 16 \times \ldots \times 16 = 16^{64} \approx 1.1579 \times 10^{77} \approx 10^{77}$

Total valid hashes (with 18 leading zeros): $16 \times 16 \times \ldots \times 16 = 16^{64-18} \approx 2.4519 \times 10^{55} \approx 2 \times 10^{55}$

Probability that a Randomly picked hash is valid: $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.00000000000000000002\%$

Understanding Mining Difficulty

Q2: How is “Mining Difficulty” calculated?

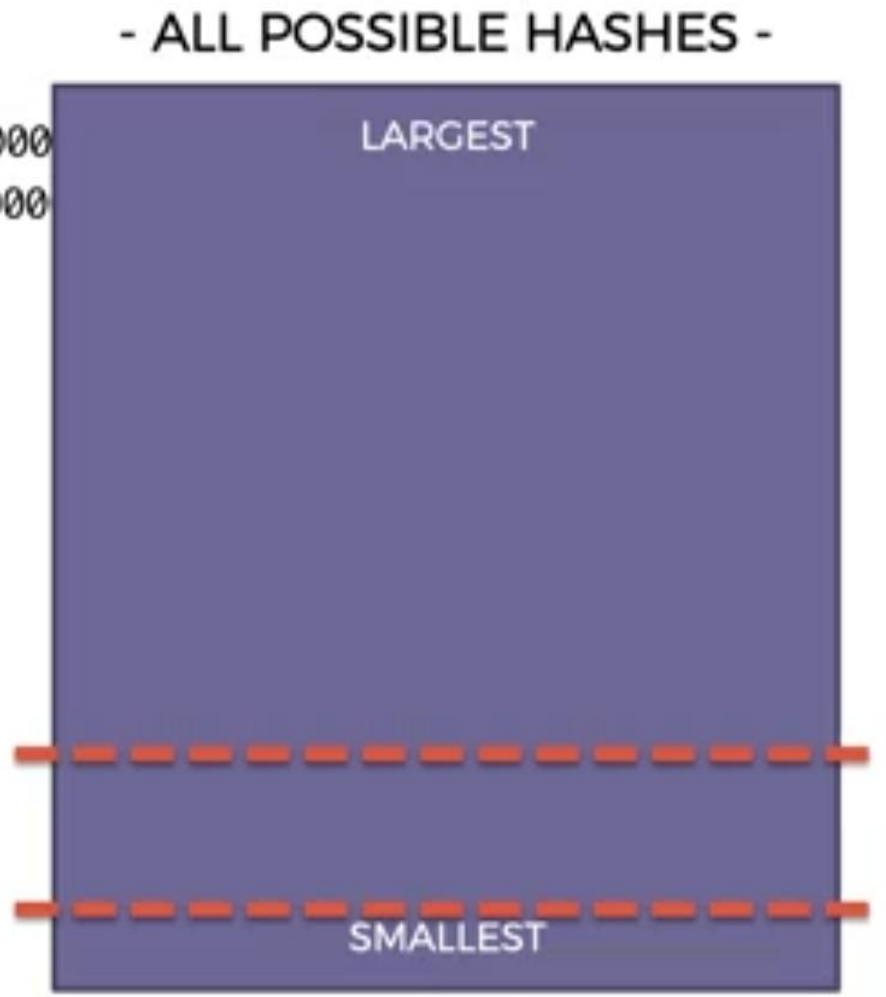
Understanding Mining Difficulty

Difficulty = current target / max target

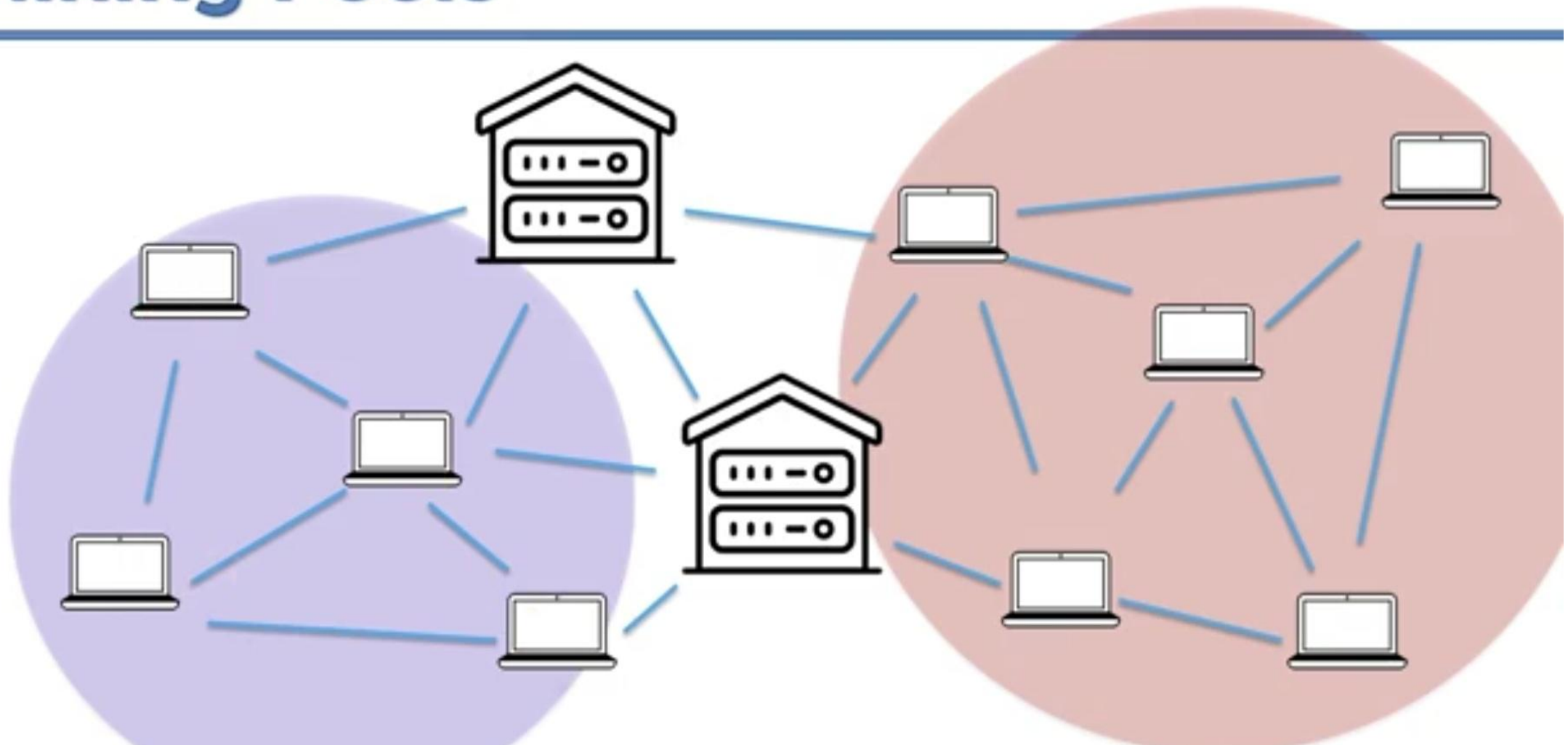
Curr target = `00000000000000005d97dc0000000000000000000000`

Max target = `00000000FFFF0000000000000000000000000000000000`

Difficulty is adjusted every 2016 blocks (2 weeks)



Mining Pools



Mining Pools

Hi! Sign in or register | Daily Deals | Gift Cards | Help & Contact | Turn Your Tax Refund Into Fun | Sell | My eBay

ebay Shop by category | Search for anything | All Categories | Search | Advanced

eBay > Coins & Paper Money > Virtual Currency > Miners | Share

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

★★★★½ 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) @ 8POW. Mine Zcash (ZEC), Bitcoin Gold (BTG)..."
Read full description

See details >

Qty: 1

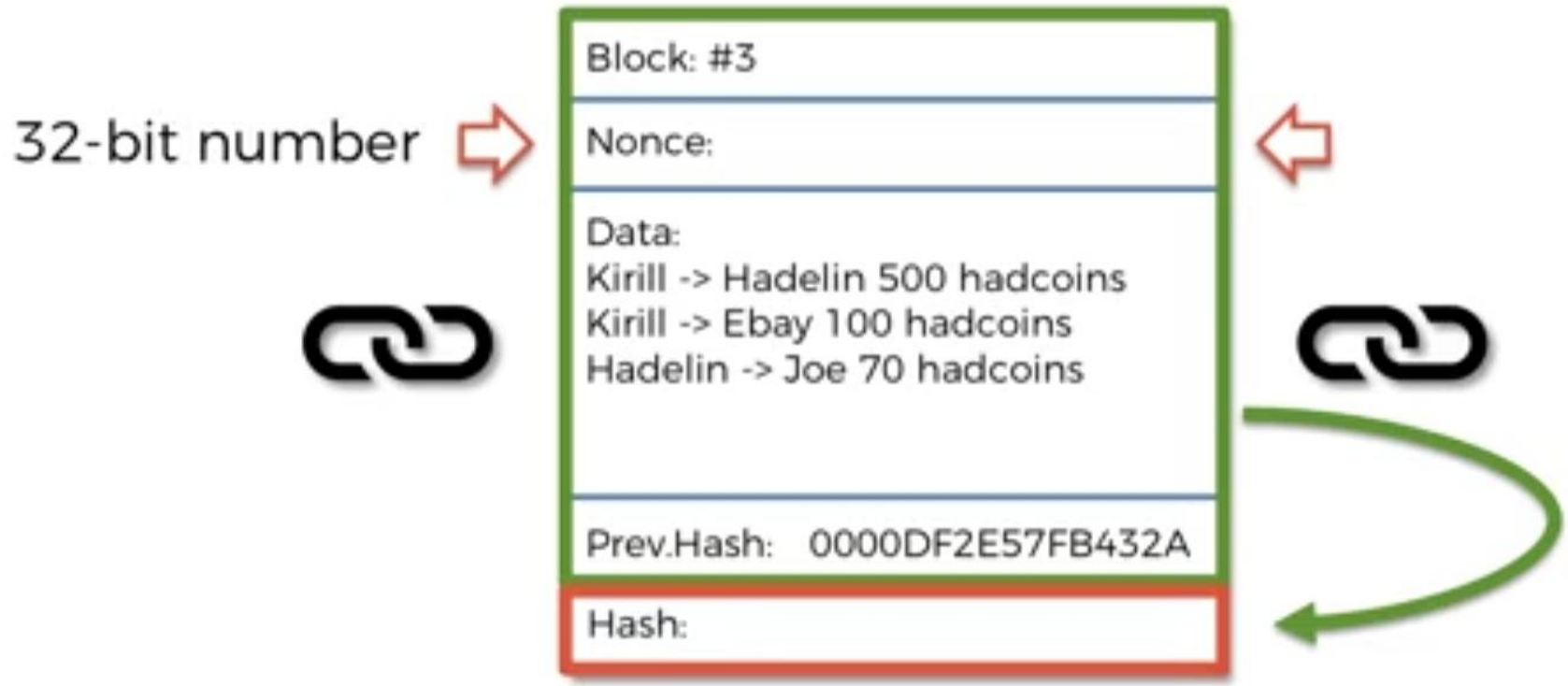
Buy It Now

Add to cart

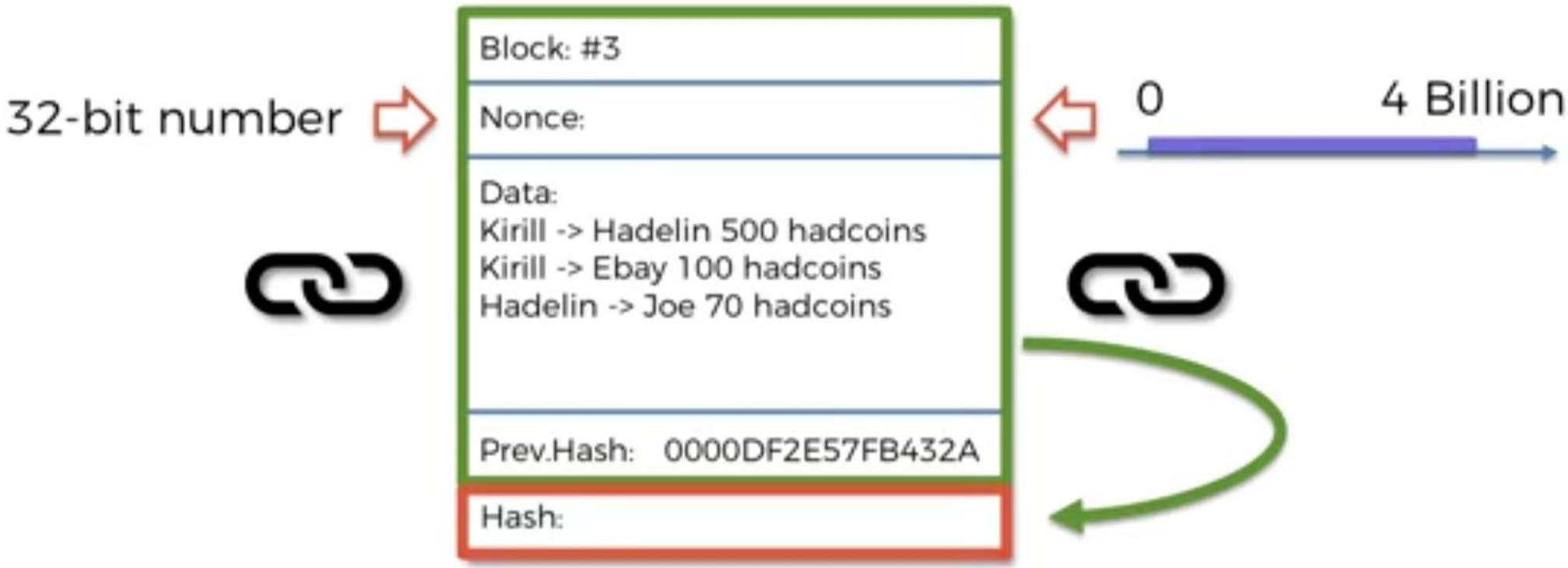
Watch

Sold by
partdiscounter (42407)
99.8% Positive feedback

Nonce Range


32-bit number
Block: #3
Nonce:
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 0000DF2E57FB432A
Hash:

Nonce Range


32-bit number
Block: #3
Nonce:
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 0000DF2E57FB432A
Hash:
0
4 Billion

Nonce Range

Let's do some estimations:

Difficulty:
Total possible 64-digit hexadecimal numbers: $16 \times 16 \times \ldots \times 16 = 16^{64} \approx 10^{77}$
Total valid hashes (with 18 leading zeros): $16 \times 16 \times \ldots \times 16 = 16^{64-18} \approx 2 \times 10^{55}$
Probability that a Randomly picked hash is valid: $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.00000000000000000002\%$

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 4×10^{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

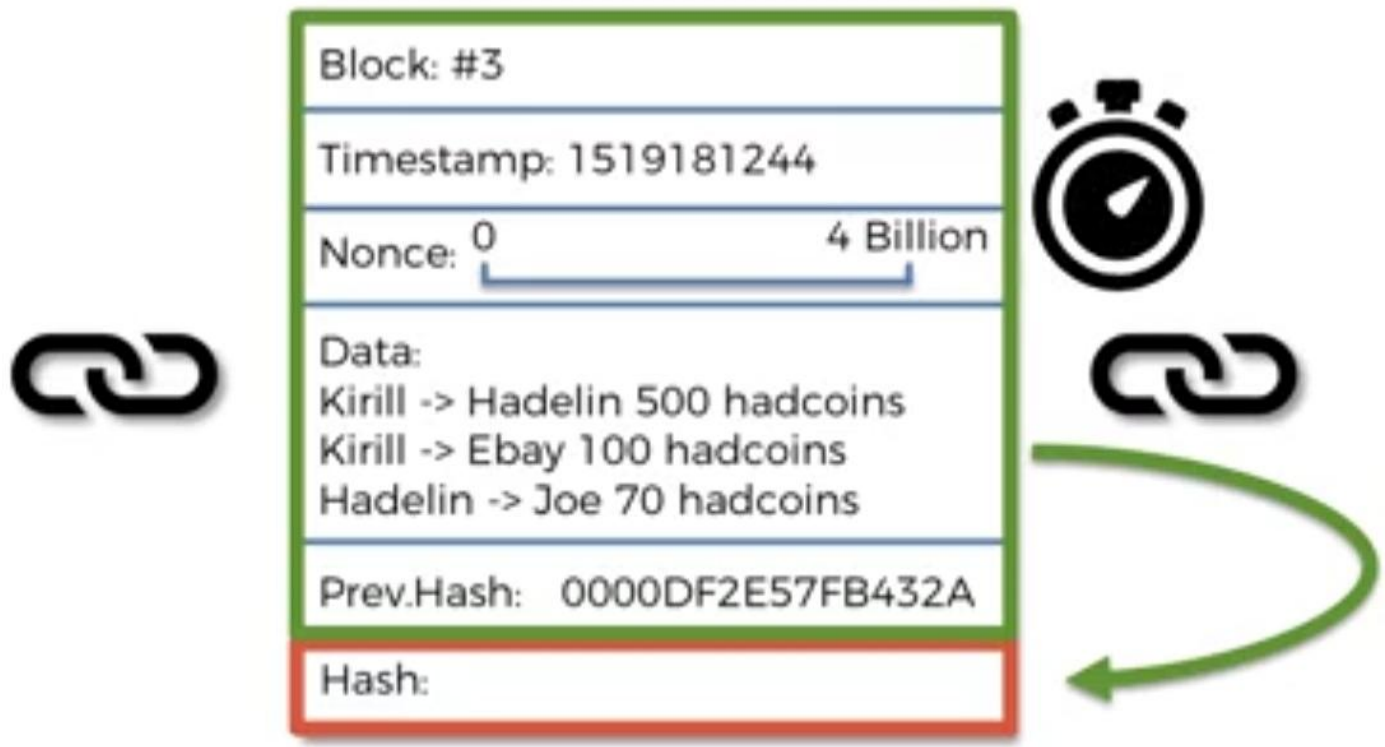
Let's do some estimations:

Difficulty:
Total possible 64-digit hexadecimal numbers: $16 \times 16 \times \ldots \times 16 = 16^{64} \approx 10^{77}$
Total valid hashes (with 18 leading zeros): $16 \times 16 \times \ldots \times 16 = 16^{64-18} \approx 2 \times 10^{55}$
Probability that a Randomly picked hash is valid: $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.00000000000000000002\%$

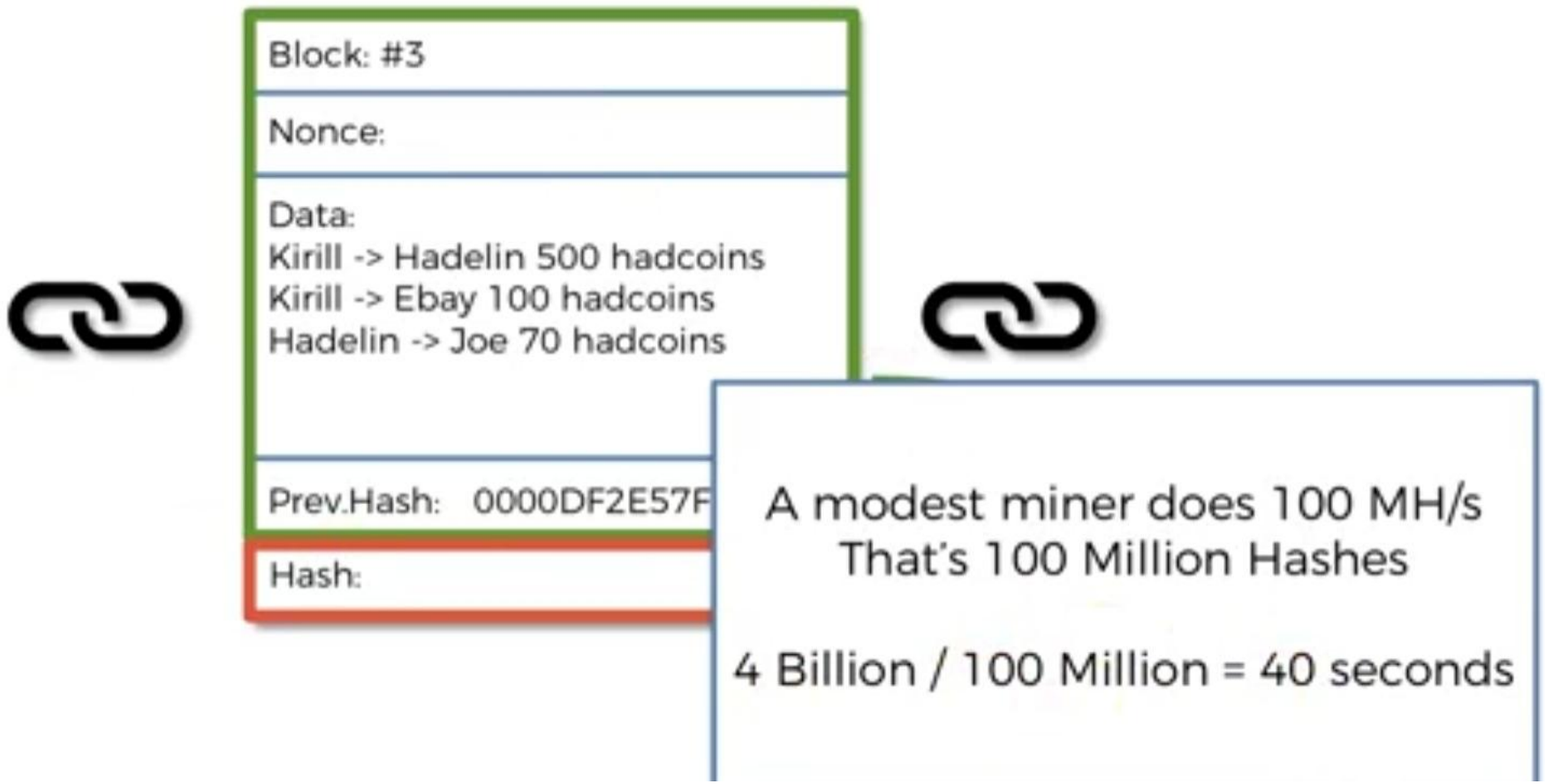
Nonce:
The Nonce is a 32-bit number, the Max Nonce = $2^{32} = 4{,}294{,}967{,}296 = 4 \times 10^{9}$
Assuming no collisions, this means 4×10^{9} different hashes
Probability that ONE of them will be valid: $4 \times 10^{9} \times 2 \times 10^{-22} = 8 \times 10^{-13} \approx 10^{-12} = 0.0000000001\%$

Conclusion: One Nonce Range is not enough

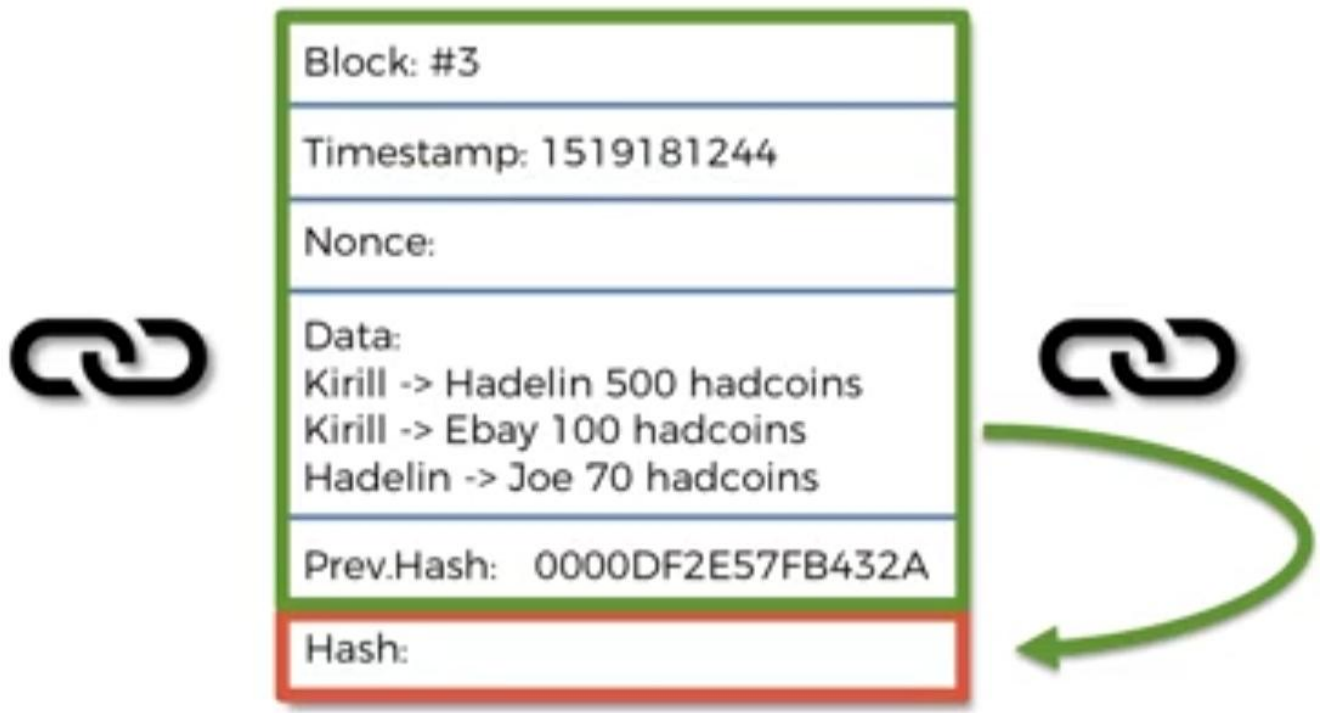
Nonce Range


Block: #3
Timestamp: 1519181244
Nonce: 0
4 Billion
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 0000DF2E57FB432A
Hash:

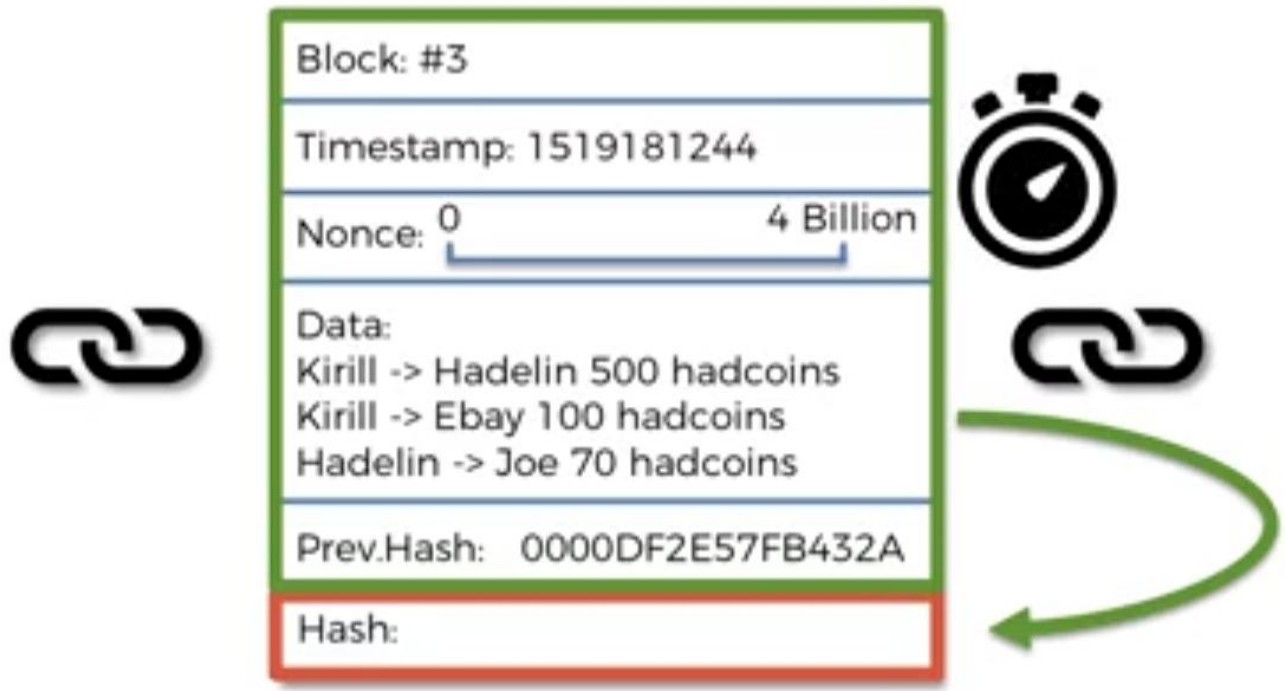
Nonce Range


Block: #3
Nonce:
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 0000DF2E57F
Hash:
A modest miner does 100 MH/s
That's 100 Million Hashes
4 Billion / 100 Million = 40 seconds

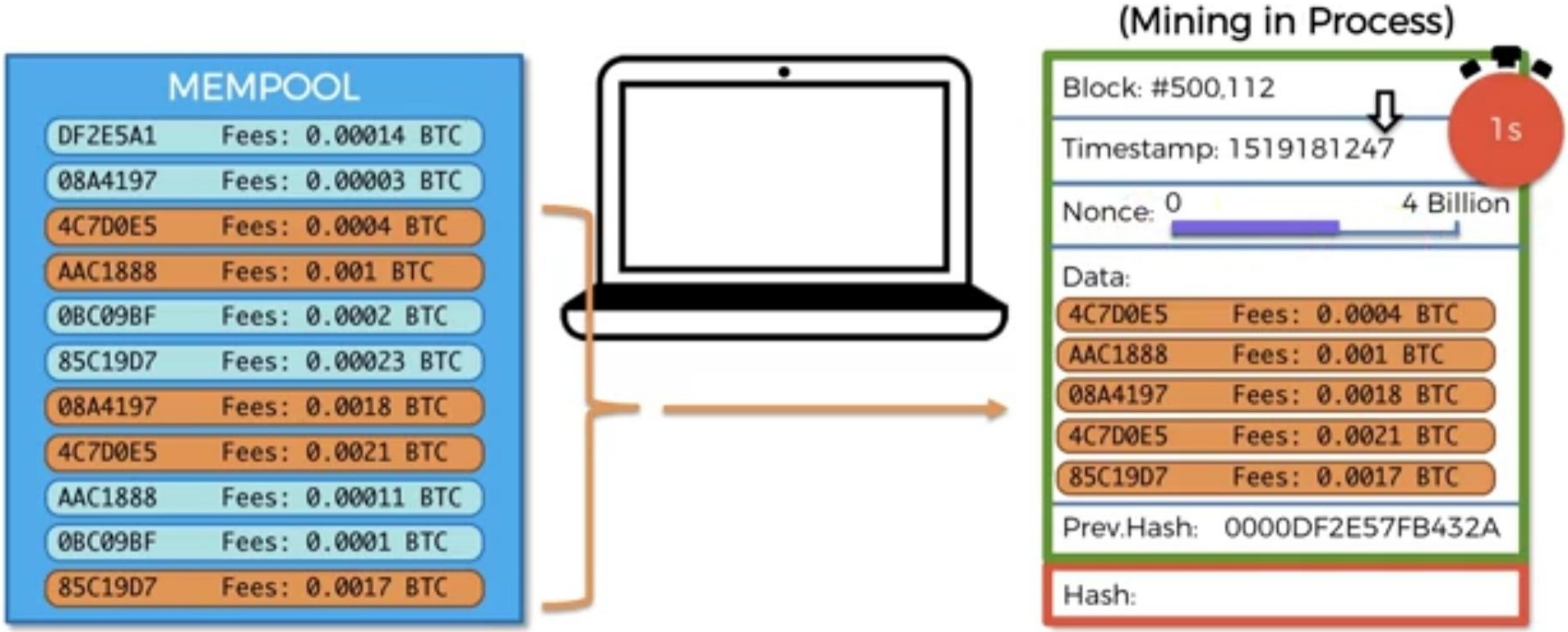
Nonce Range


Block: #3
Timestamp: 1519181244
Nonce:
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 0000DF2E57FB432A
Hash:

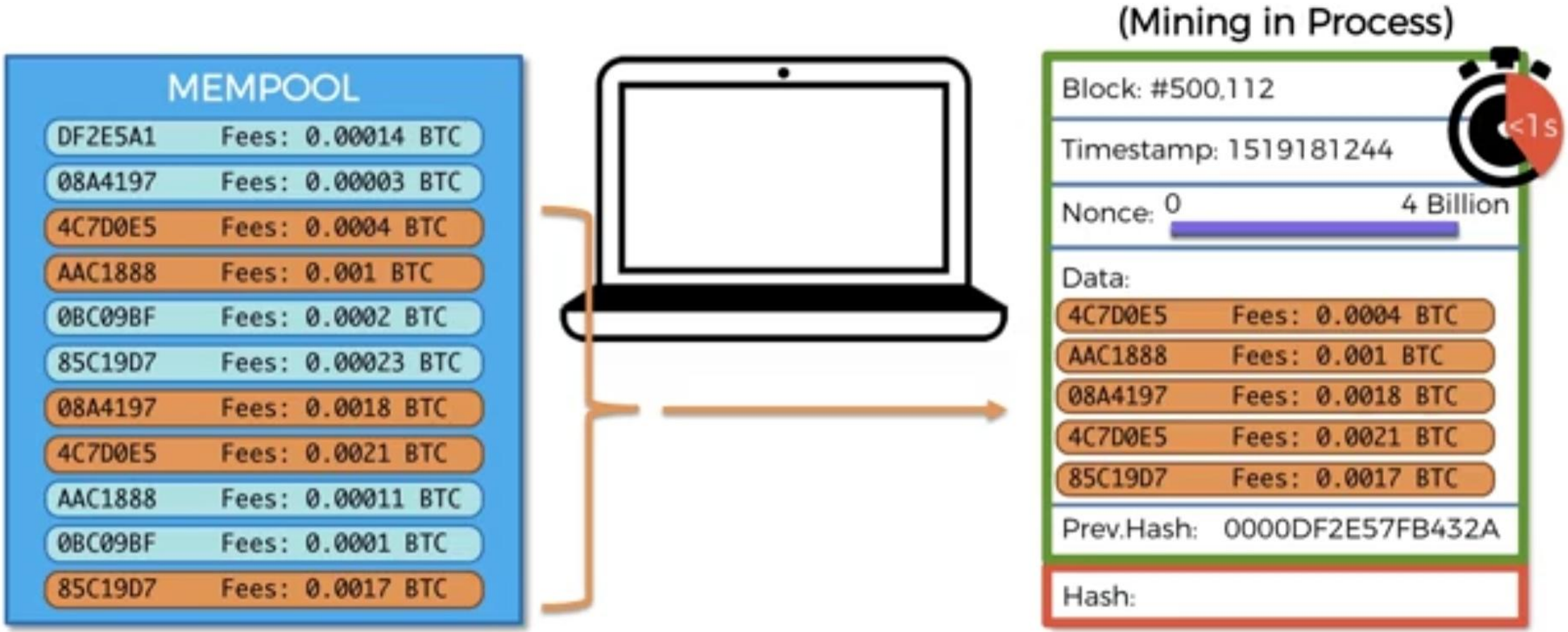
Nonce Range


Block: #3
Timestamp: 1519181244
Nonce: 0
4 Billion
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 0000DF2E57FB432A
Hash:

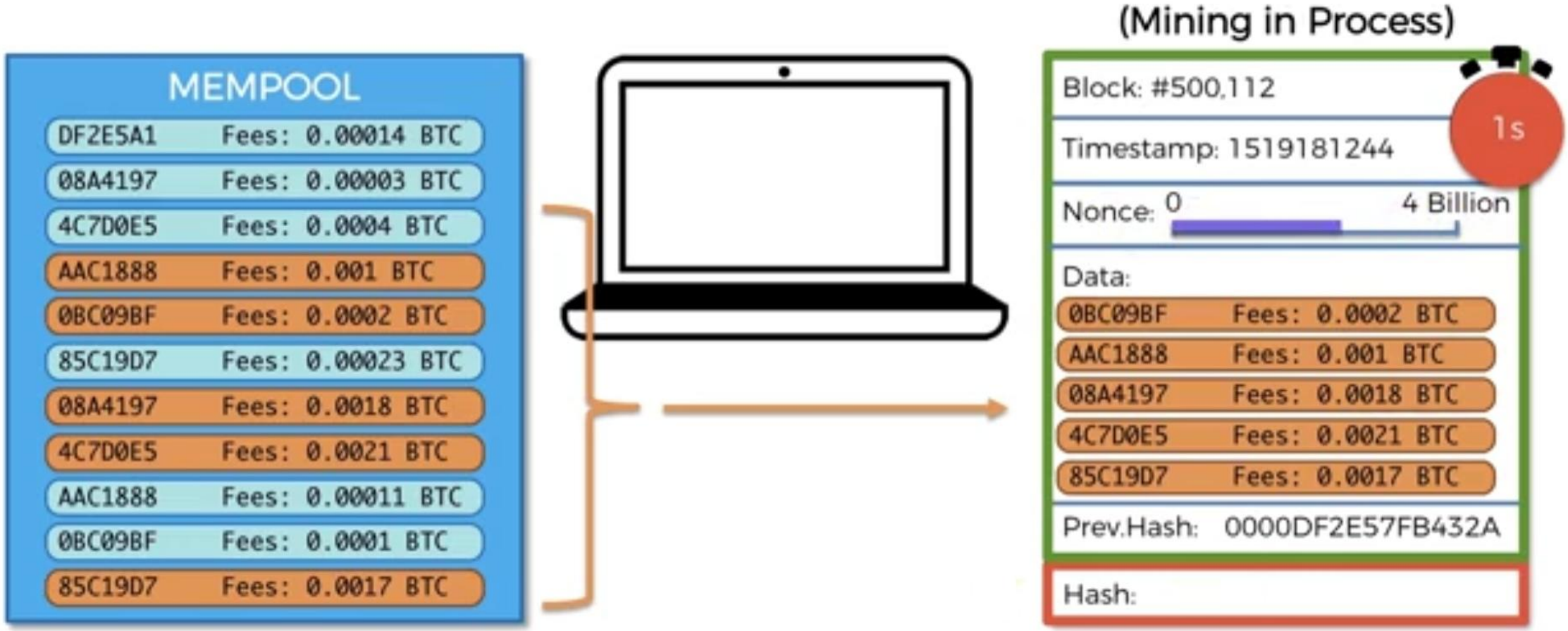
How Miners Pick Transactions



How Miners Pick Transactions



How Miners Pick Transactions

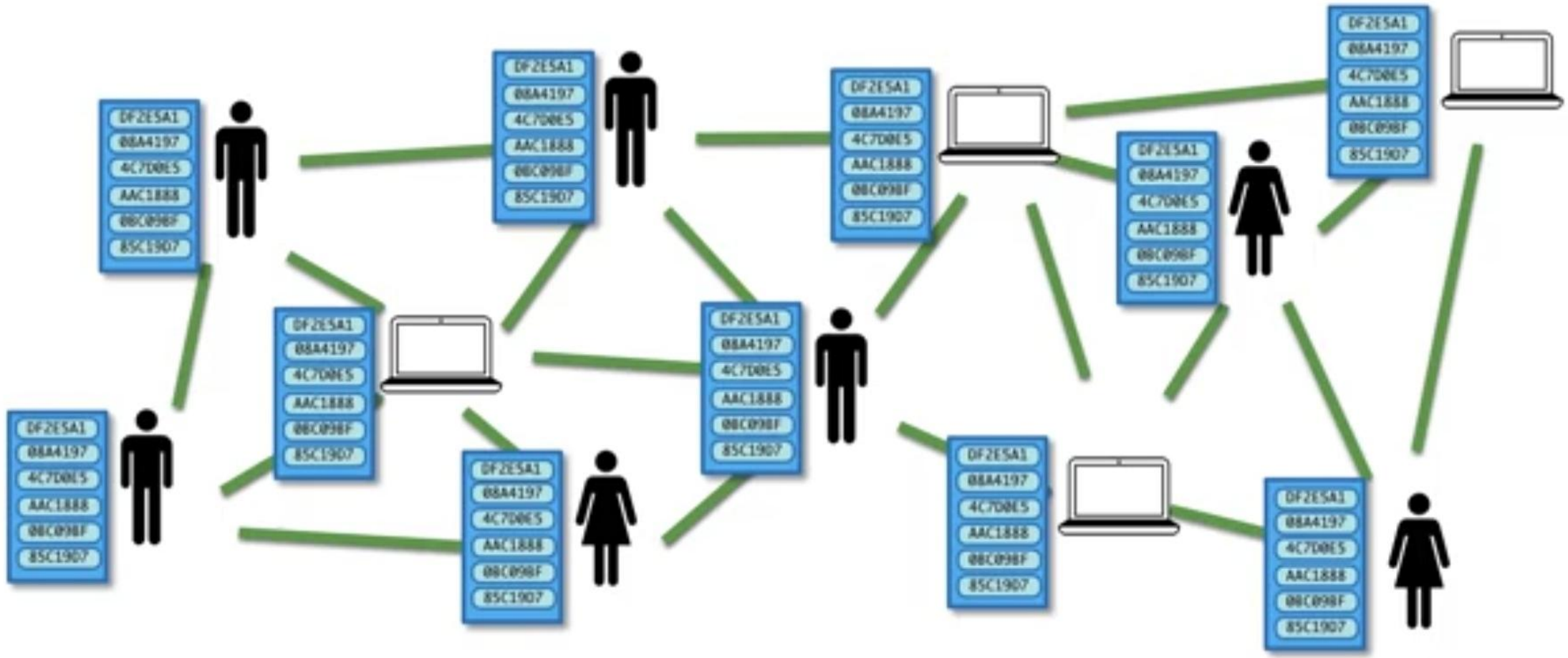


CPUs vs GPUs vs ASICs

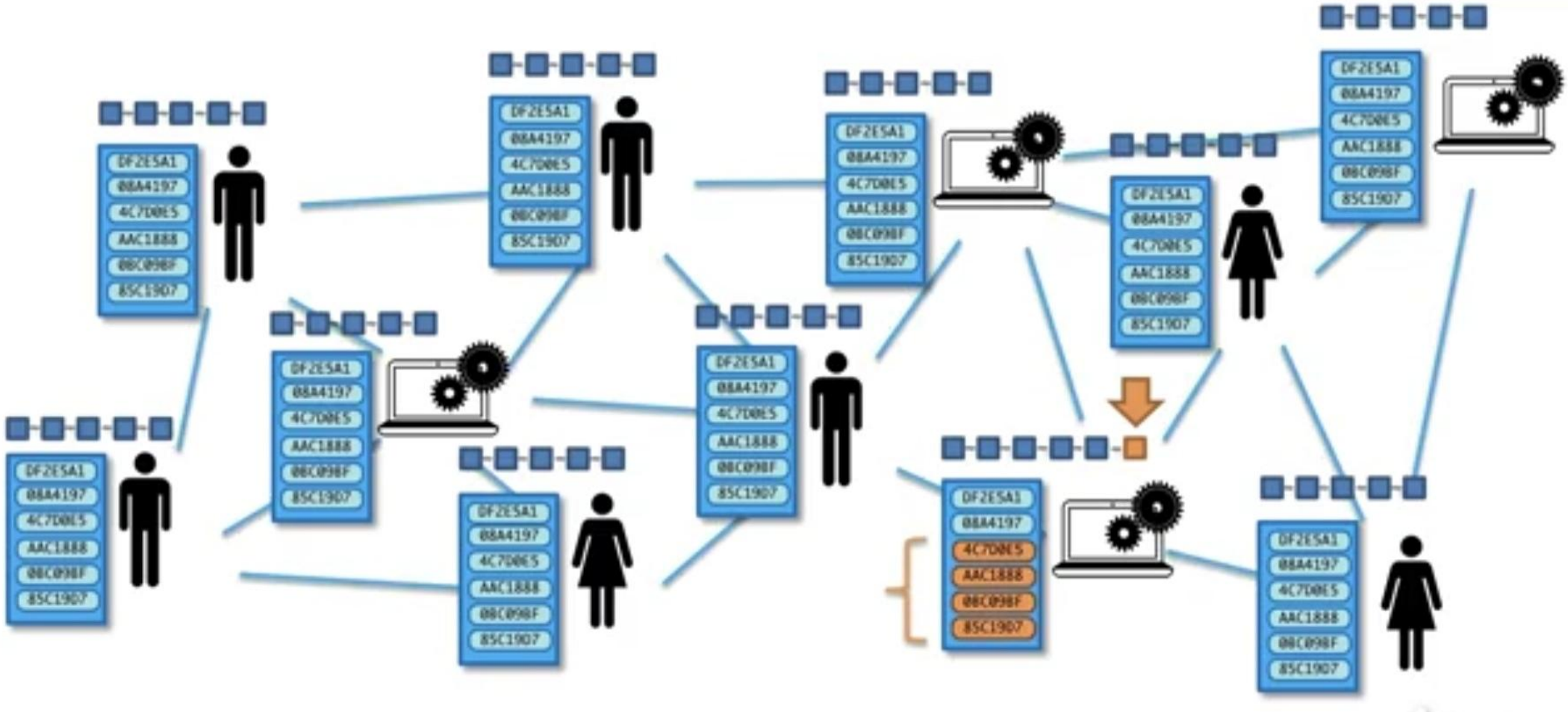
CPU = Central Processing Unit	General	< 10 MH/s
GPU = Graphics Processing Unit	Specialized	< 1 GH/s
ASIC = Application-Specific Integrated Circuit	Totally Specialized	> 1,000 GH/s

Cloud Mining

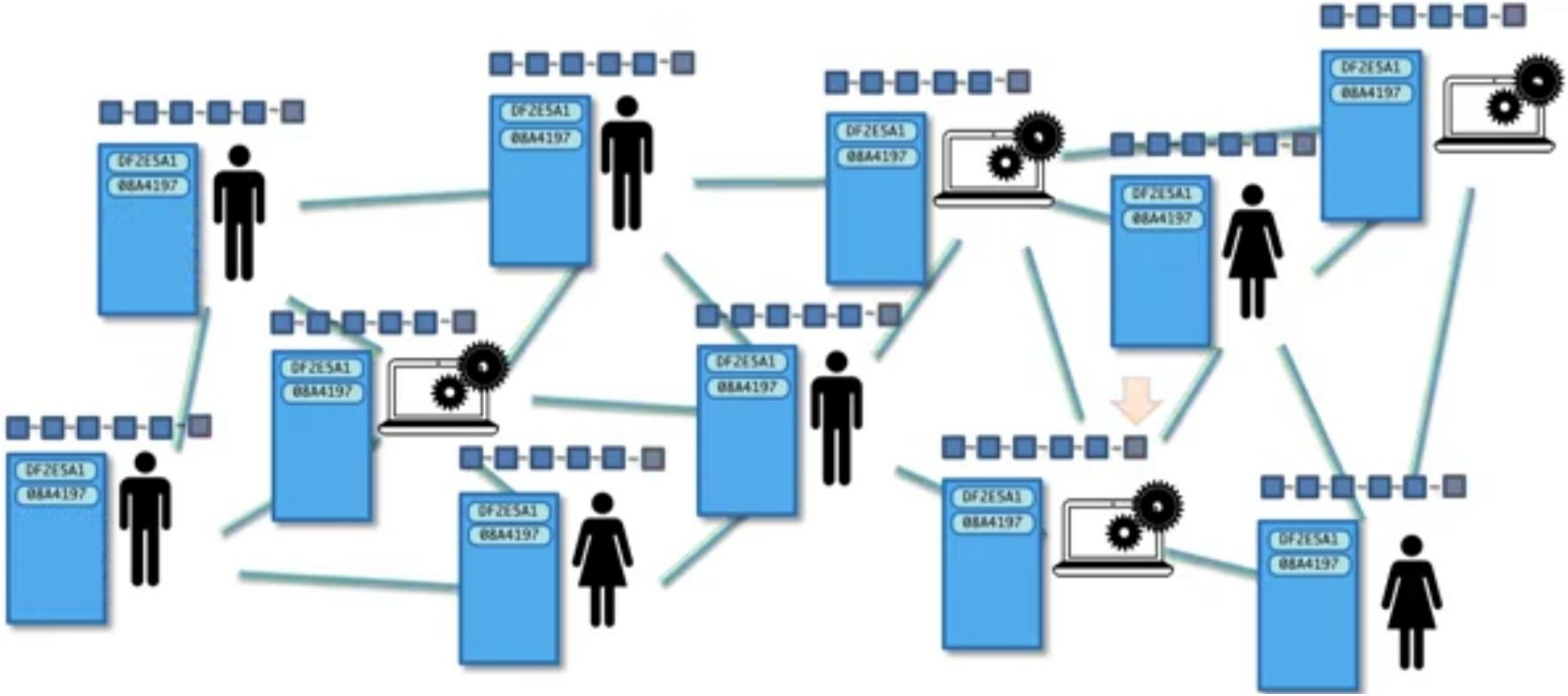
How do Mempools work?



How do Mempools work?



How do Mempools work?

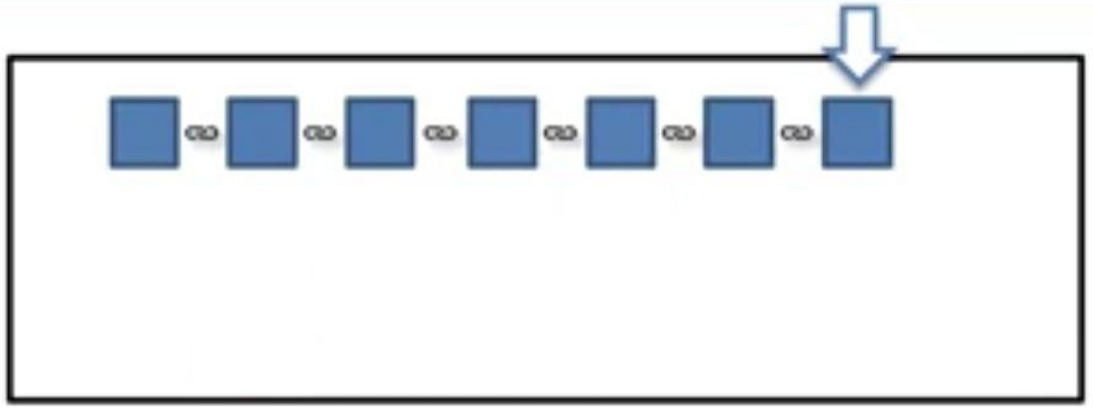


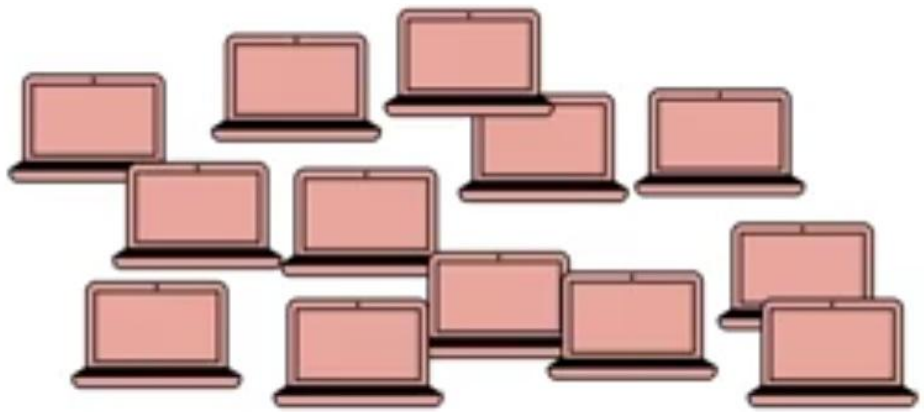
CPUs vs GPUs vs ASICs

CPU = Central Processing Unit	General	< 10 MH/s
GPU = Graphics Processing Unit	Specialized	< 1 GH/s
ASIC = Application-Specific Integrated Circuit	Totally Specialized	> 1,000 GH/s

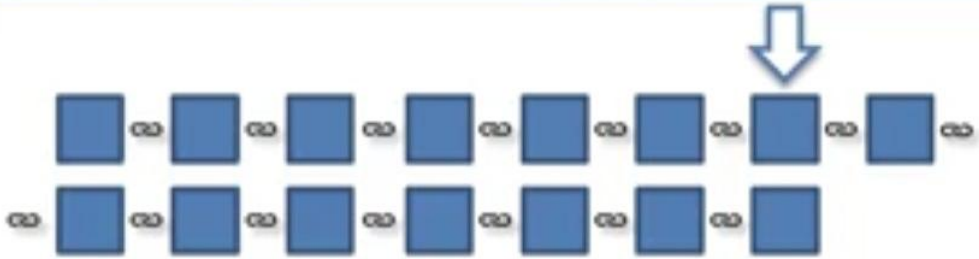
Cloud Mining

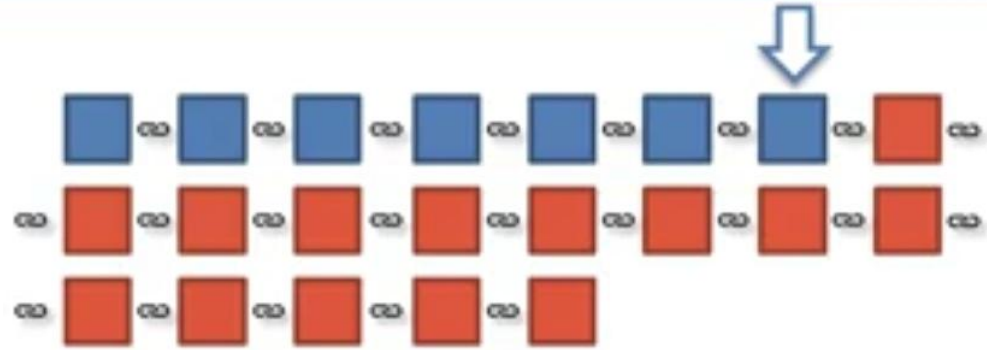
The 51% Attack

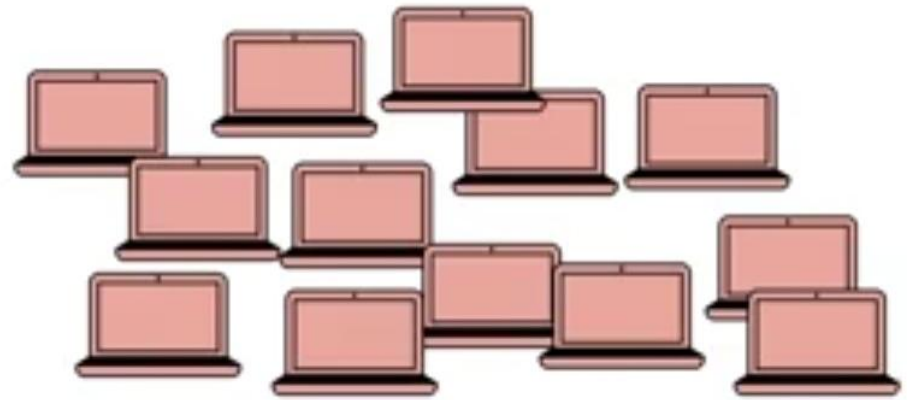




The 51% Attack







Deriving the current target

Difficulty = current target / max target
Curr target = 0000000000000000005d97dc0000000000000000000
Max target = 00000000FFFF0000000000000000000000000000000

Where is the current target stored?
Bits -> Hex -> Derive target

Block #510808

Summary	
Number Of Transactions	329
Output Total	2,093.19925201 BTC
Estimated Transaction Volume	138.61944625 BTC
Transaction Fees	0.06499689 BTC
Height	510808 (Main Chain)
Timestamp	2018-02-25 06:48:56
Received Time	2018-02-25 06:48:56
Relayed By	ViaBTC
Difficulty	3,007,383,866,429.73
Bits	392009692
Size	1006.782 kB
Weight	3978.903 kWU
Version	0x20000000
Nonce	1936277748
Block Reward	12.5 BTC

Deriving the current target

Difficulty = current target / max target
Curr target = 0000000000000000005d97dc0000000000000000000000000000000000000000
Max target = 00000000FFFF0000000000000000000000000000000000000000000000000000

Where is the current target stored?
Bits -> Hex -> Derive target
Bits: 392009692
Bits in Hex: 175D97DC

Deriving the current target

Difficulty = current target / max target

Curr target = 0000000000000005d97dc0000000000000000000000000000000000000000000

Max target = 00000000FFFF0000000000000000000000000000000000000000000000000000

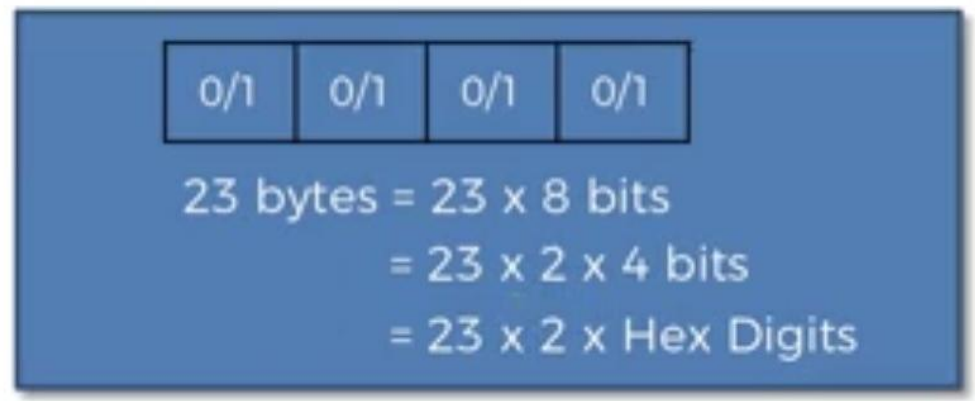
Where is the current target stored?

Bits -> Hex -> Derive target

Bits: 392009692

Bits in Hex: 175D97DC

16*1+7
= 23



23x2 = 46 Hex Digits

0000000000000000000000000000000000000000000000

Deriving the current target

Difficulty = current target / max target
Curr target = 0000000000000005d97dc0000000000000000000000000000000000000000000
Max target = 00000000FFFF0000000000000000000000000000000000000000000000000000

Where is the current target stored?
Bits -> Hex -> Derive target
Bits: 392009692
Bits in Hex: 175D97DC