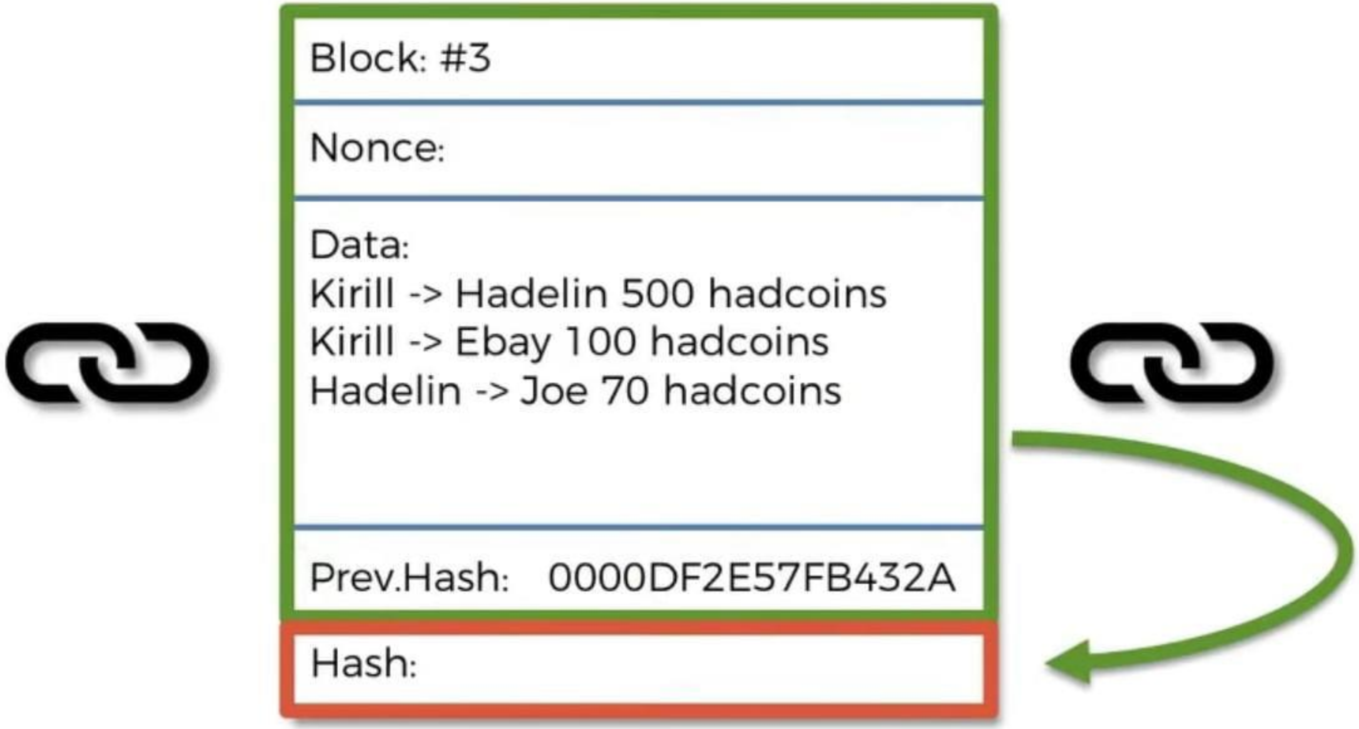
Blockchain and Cryptocurrency

By: Syeda Tayyaba Bukhari

Nonce Range

What we know about nonce till now:



Block: #3

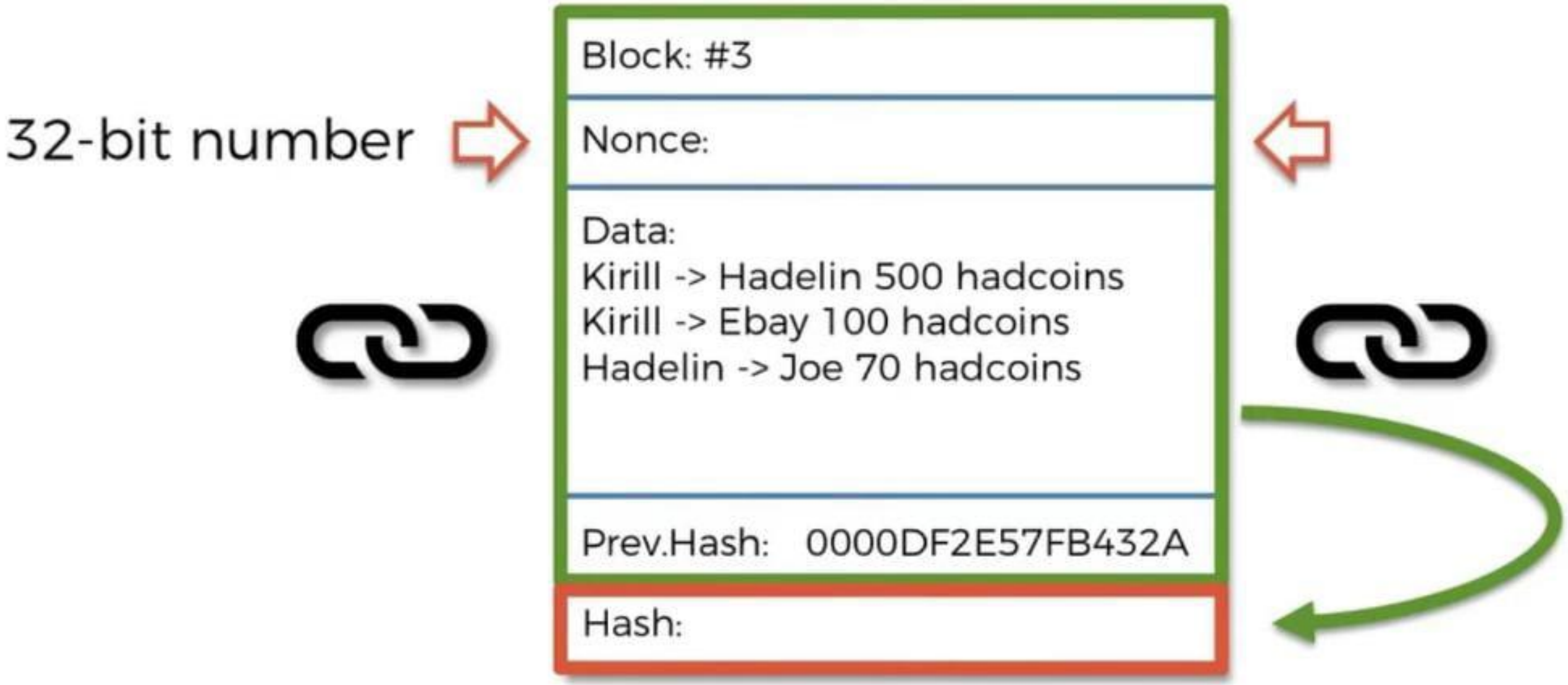
Nonce:

Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins

Prev.Hash: 0000DF2E57FB432A

Hash:

Length of Nonce:



32-bit number

Block: #3

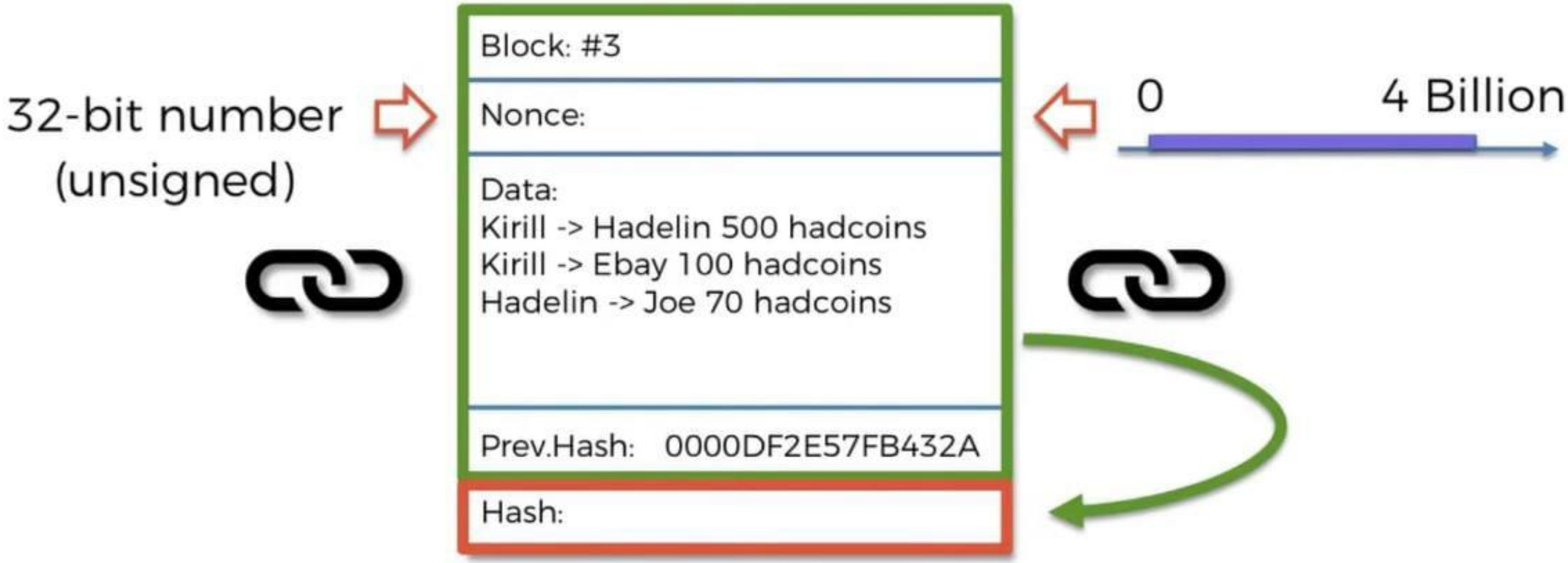
Nonce:

Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins

Prev.Hash: 0000DF2E57FB432A

Hash:

Range:



32-bit number (unsigned)

Block: #3

Nonce:

Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins

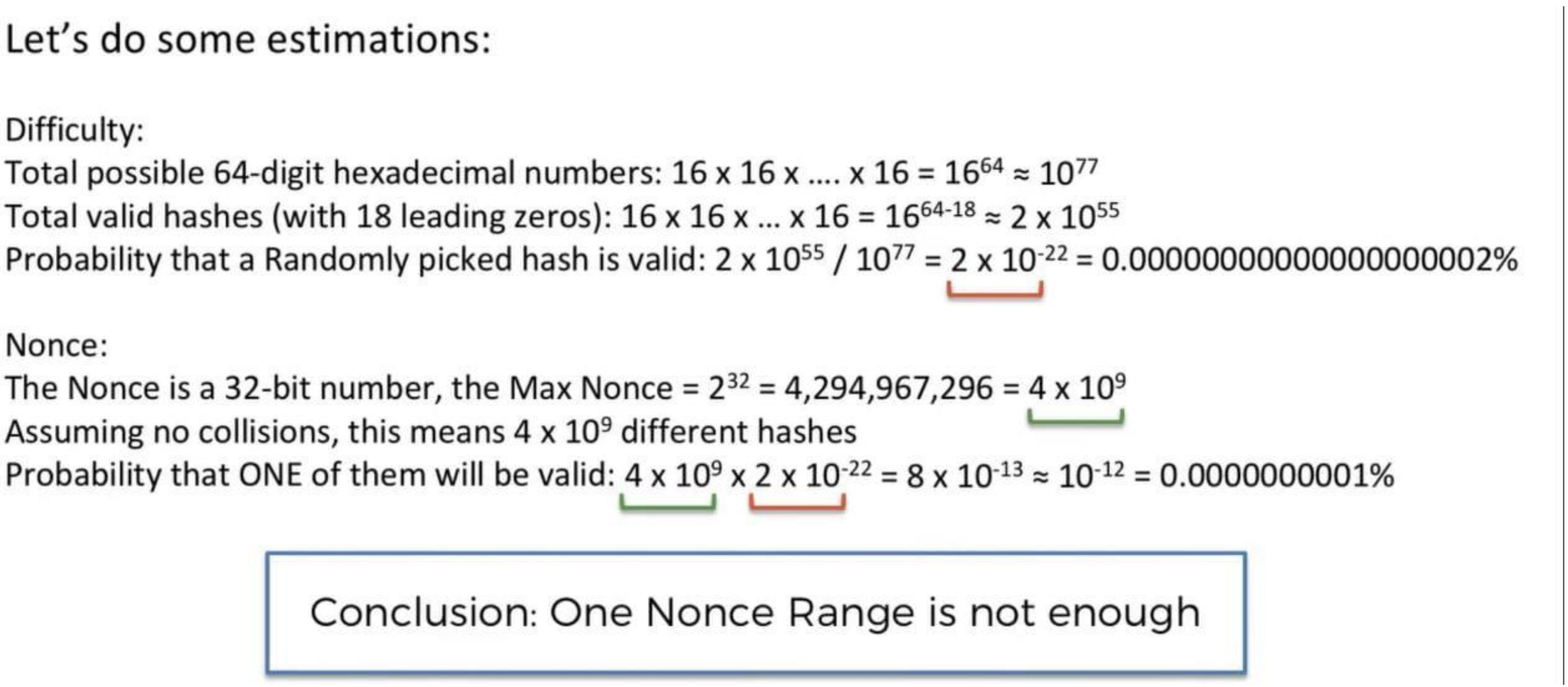
Prev.Hash: 0000DF2E57FB432A

Hash:

0

4 Billion

Some Calculations regarding percentage of finding golden nonce



Let’s do some estimations:

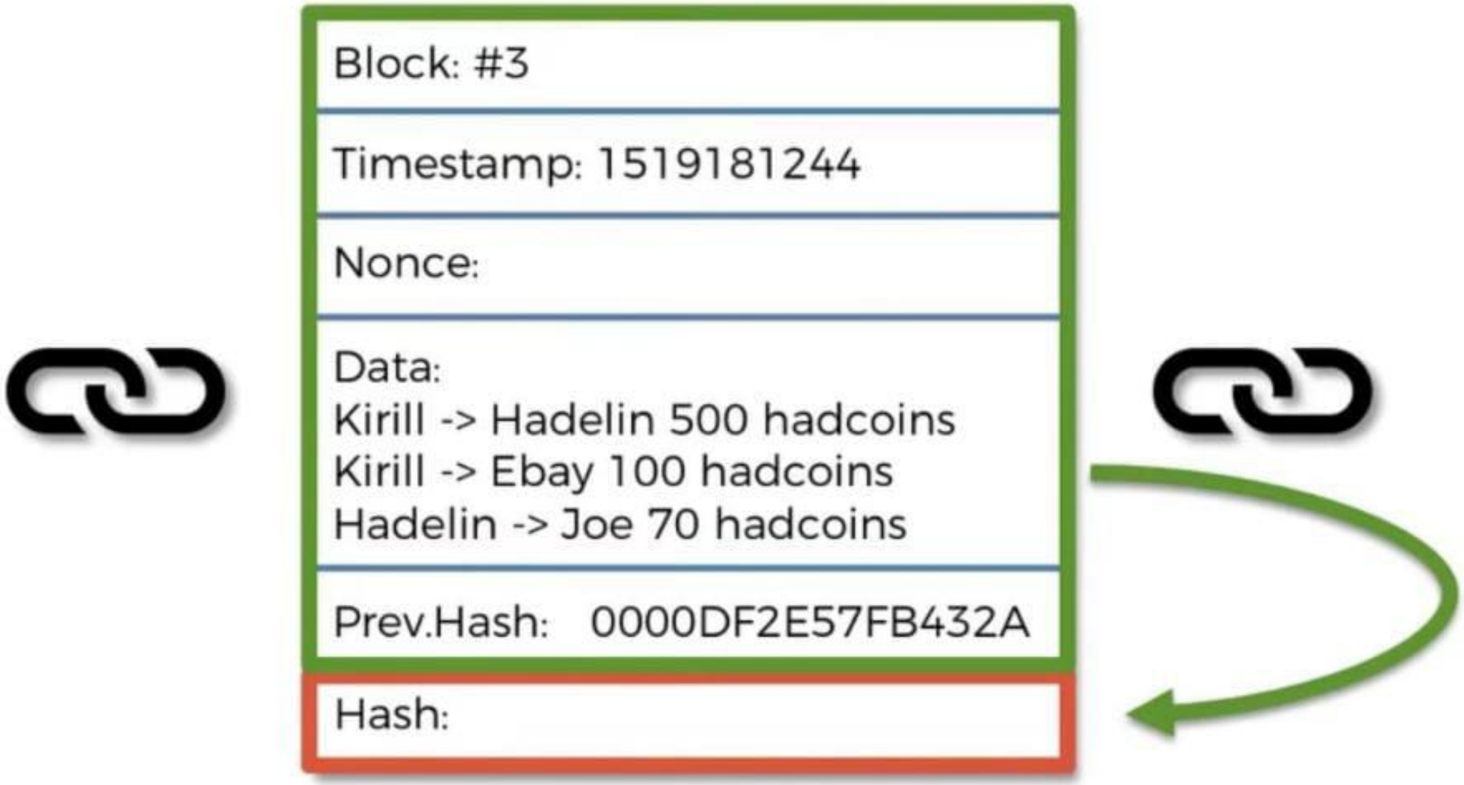
Difficulty:
Total possible 64-digit hexadecimal numbers: $16 \times 16 \times .... \times 16 = 16^{64} \approx 10^{77}$
Total valid hashes (with 18 leading zeros): $16 \times 16 \times ... \times 16 = 16^{64-18} \approx 2 \times 10^{55}$
Probability that a Randomly picked hash is valid: $2 \times 10^{55}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

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

Conclusion: One Nonce Range is not enough isn’t it too easy to find the golden nonce for miners having modest Hashing/Computing power??

Timestamp: another attribute of a block

In cryptocurrency, a timestamp shows the “Unix” time, or the time and date when a block was mined and validated by a blockchain network



Block: #3

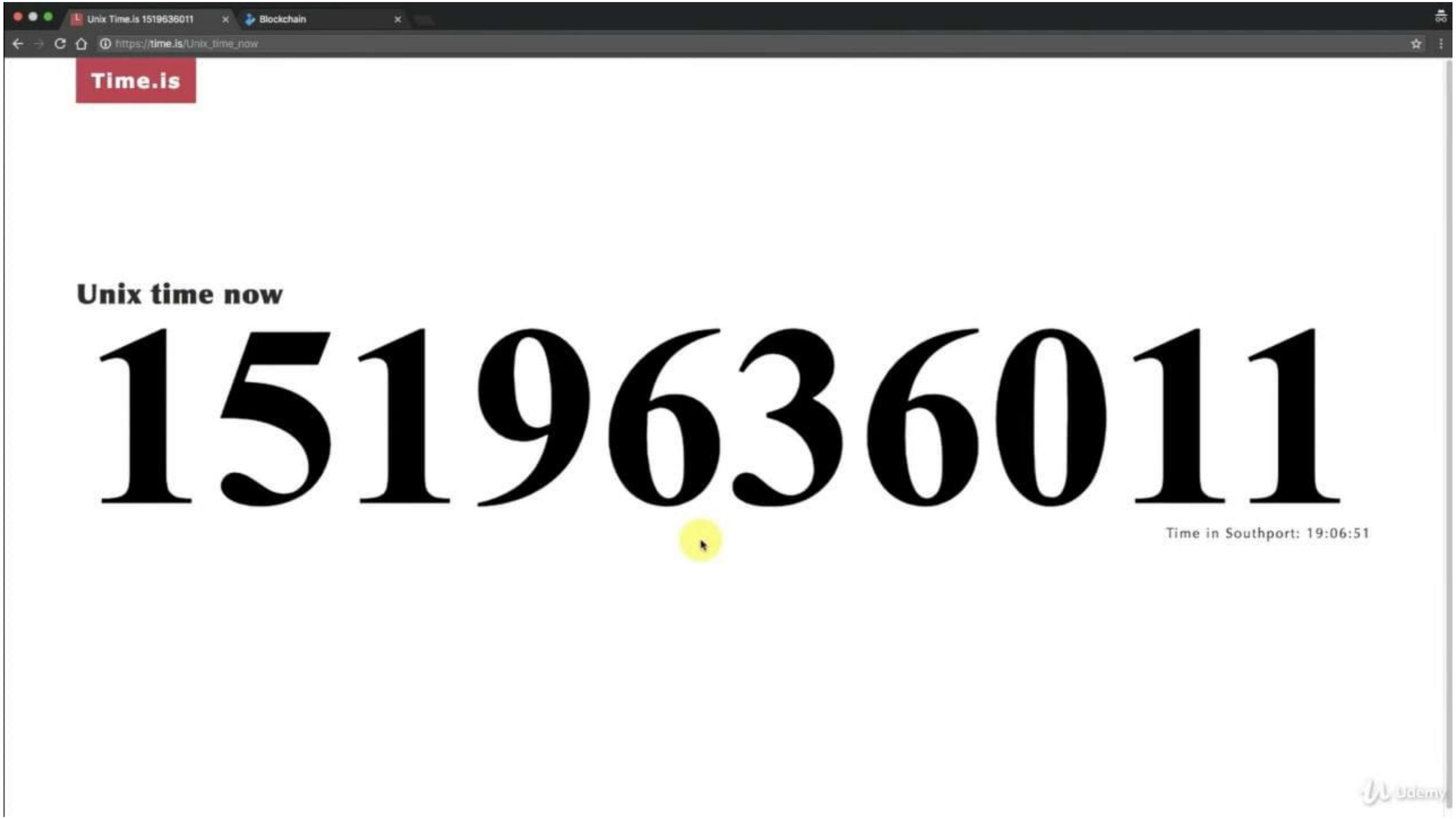
Timestamp: 1519181244

Nonce:

Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins

Prev.Hash: 0000DF2E57FB432A

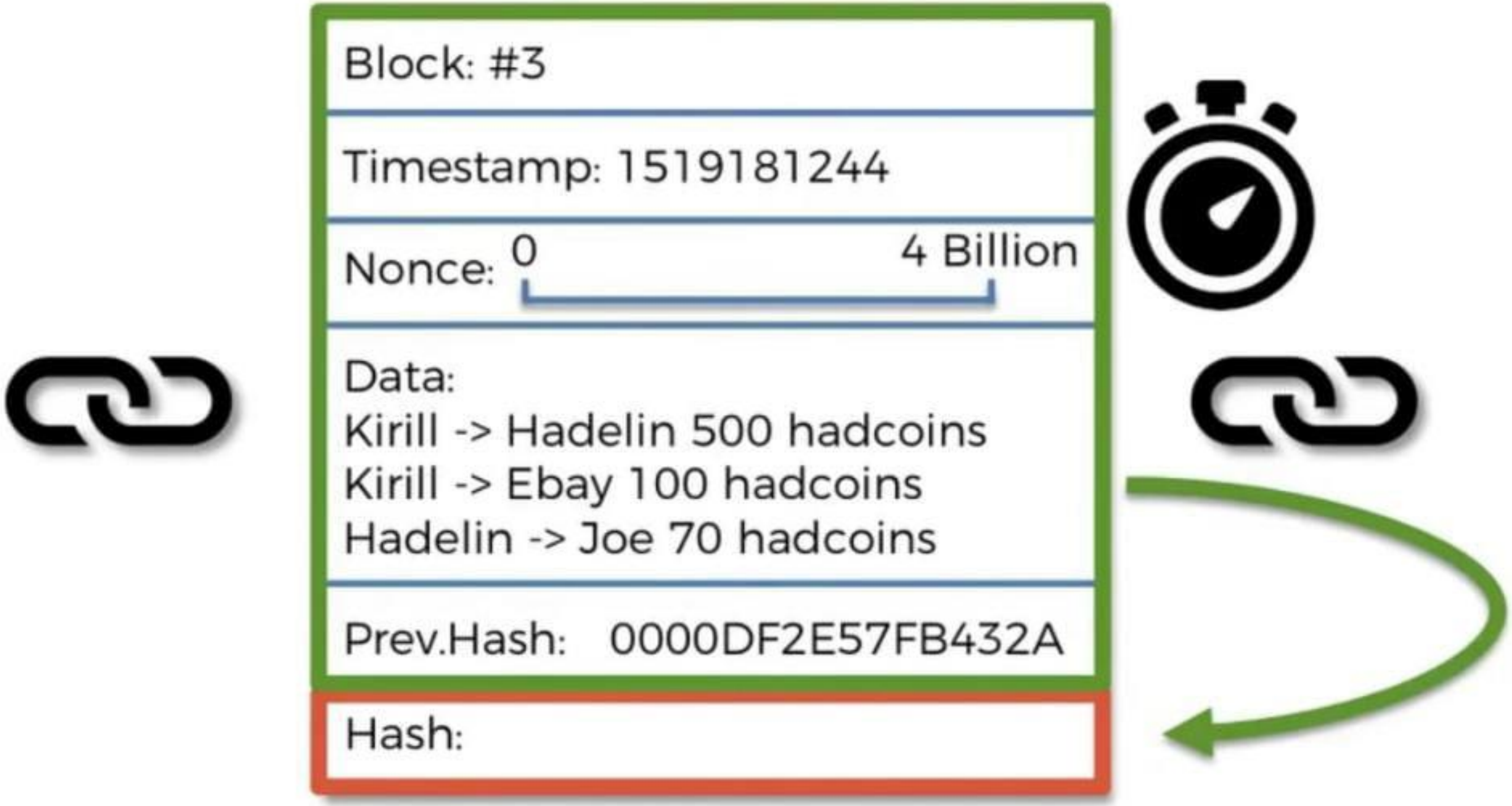
Hash:



Unix time now

1519636011

Time in Southport: 19:06:51



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

(Mining in Process)

Block: #500,112

Timestamp: 1519181244

Nonce:

Data:

Prev.Hash: 0000DF2E57FB432A

Hash:

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

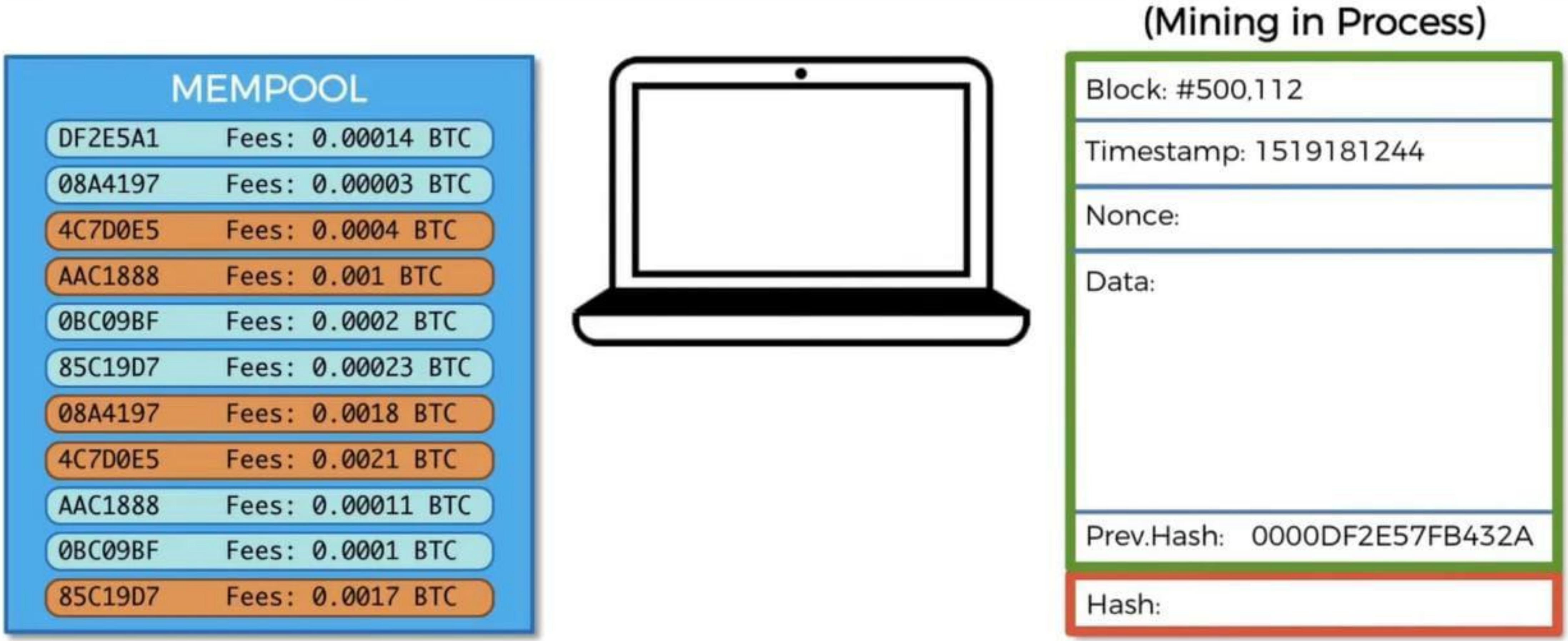
Timestamp: 1519181244

Nonce:

Data:

Prev.Hash: 0000DF2E57FB432A

Hash:



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

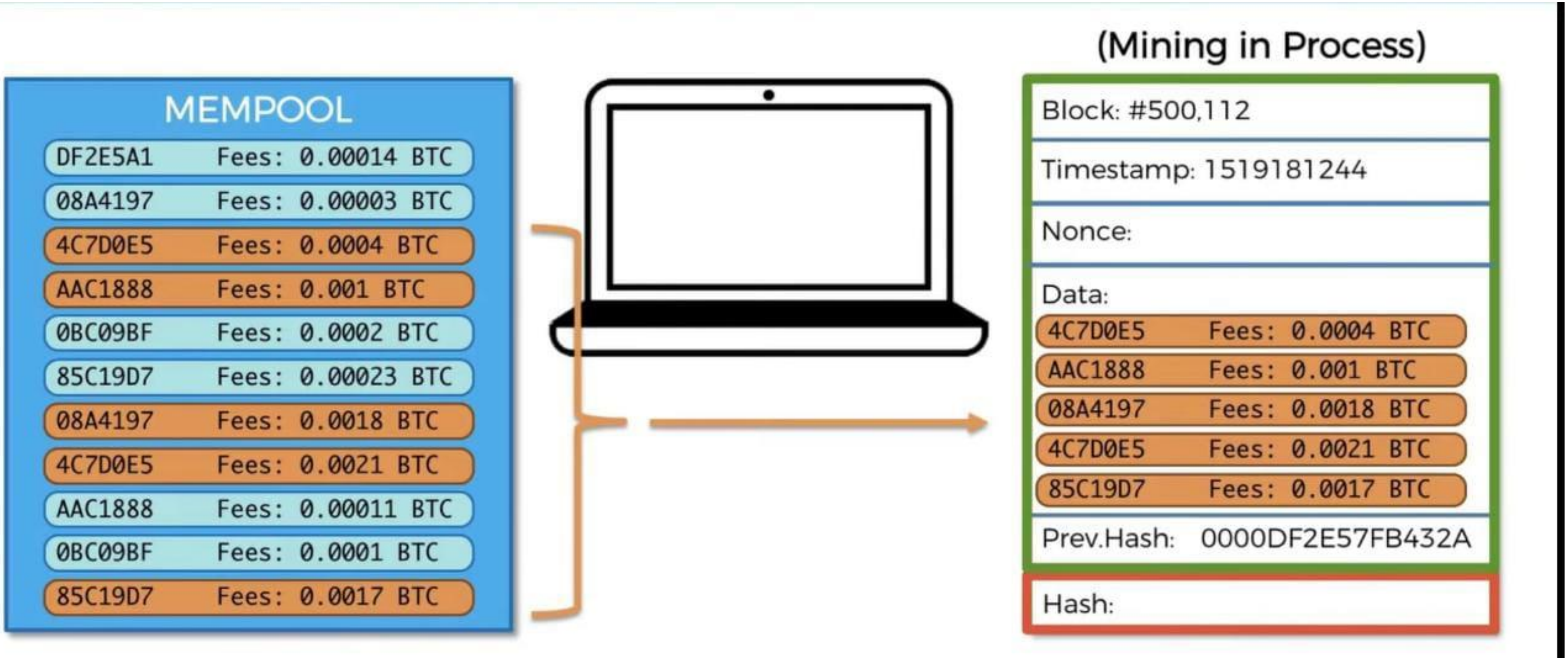
Timestamp: 1519181244

Nonce:

Data:

Prev.Hash: 0000DF2E57FB432A

Hash:



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

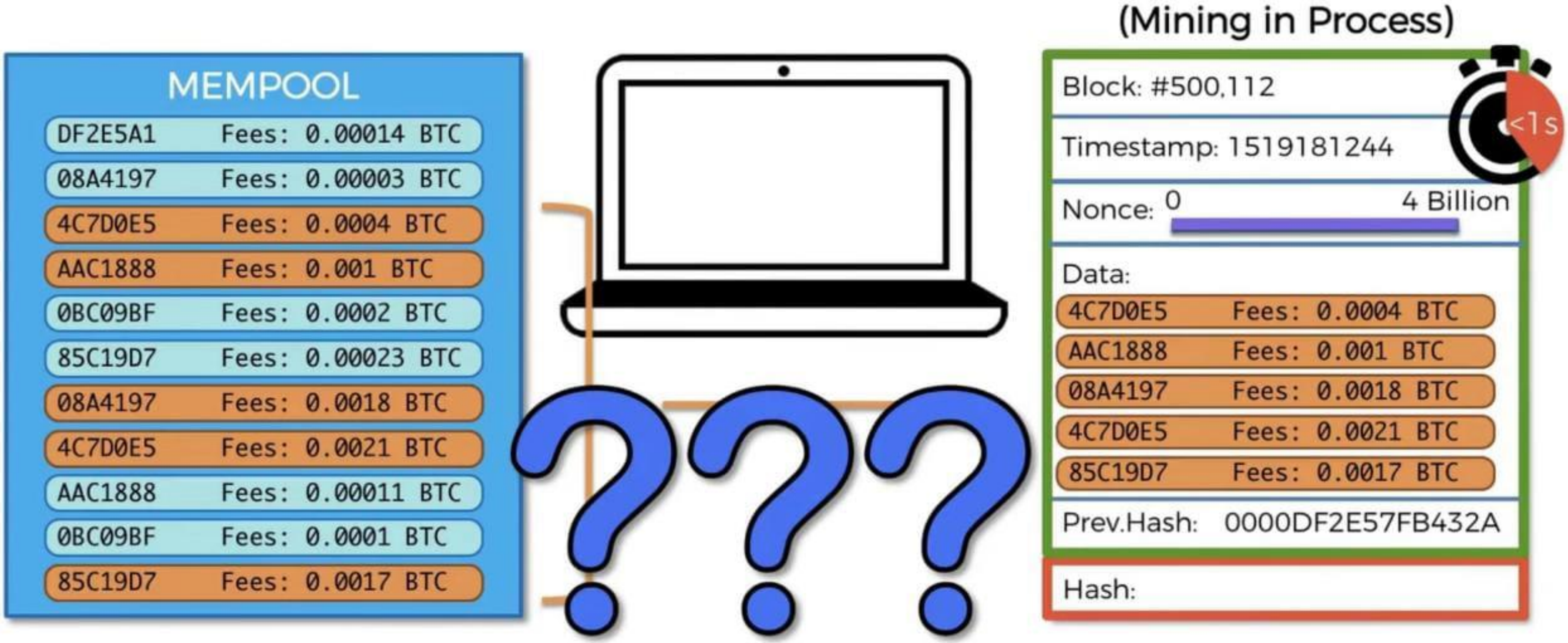
Nonce:

Data:

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:



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

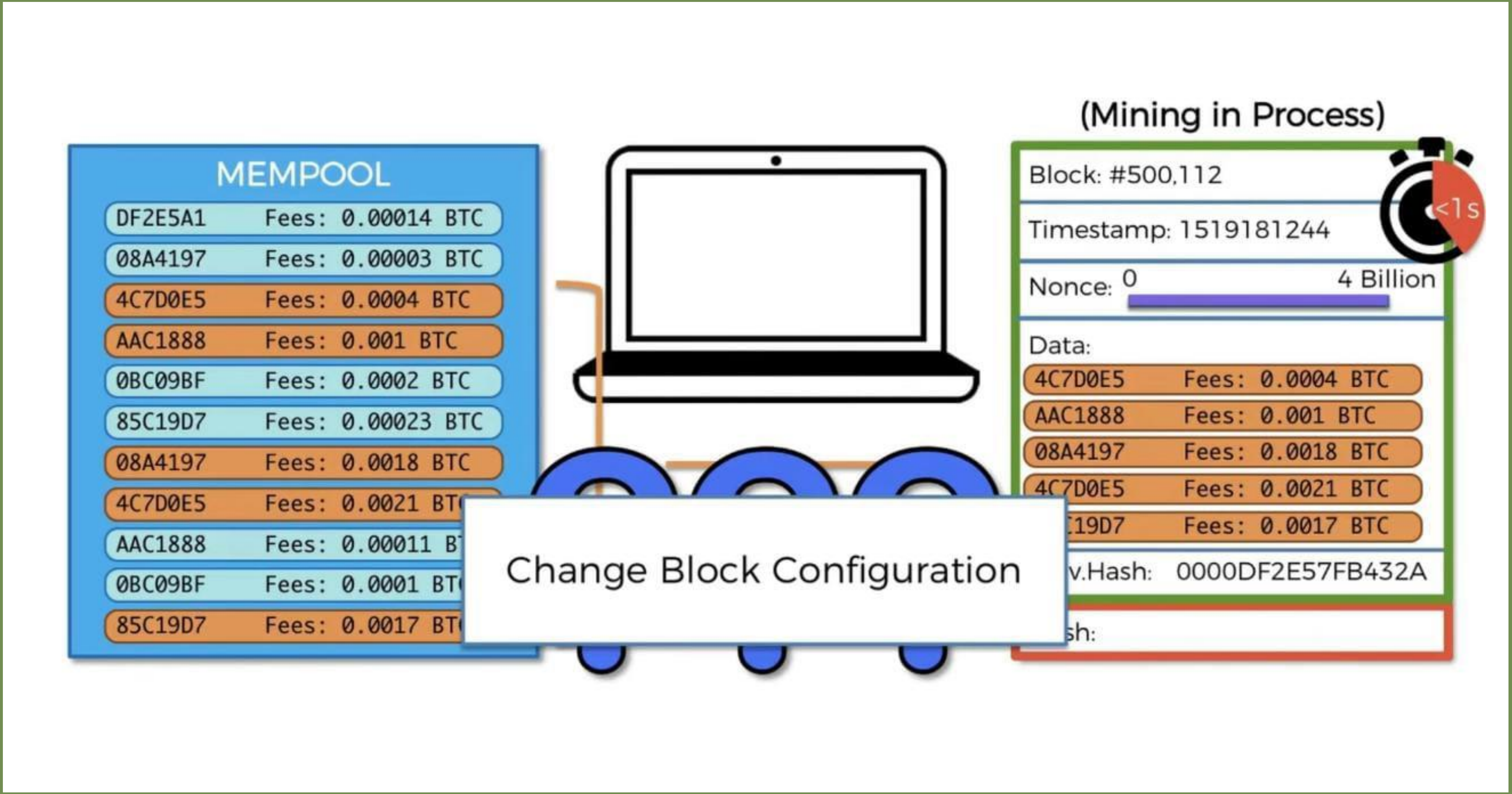
Nonce: 0 4 Billion

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:



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 BT
AAC1888	Fees: 0.00011 B
0BC09BF	Fees: 0.0001 BT
85C19D7	Fees: 0.0017 BT

(Mining in Process)

Block: #500,112

Timestamp: 1519181244

Nonce: 0 4 Billion

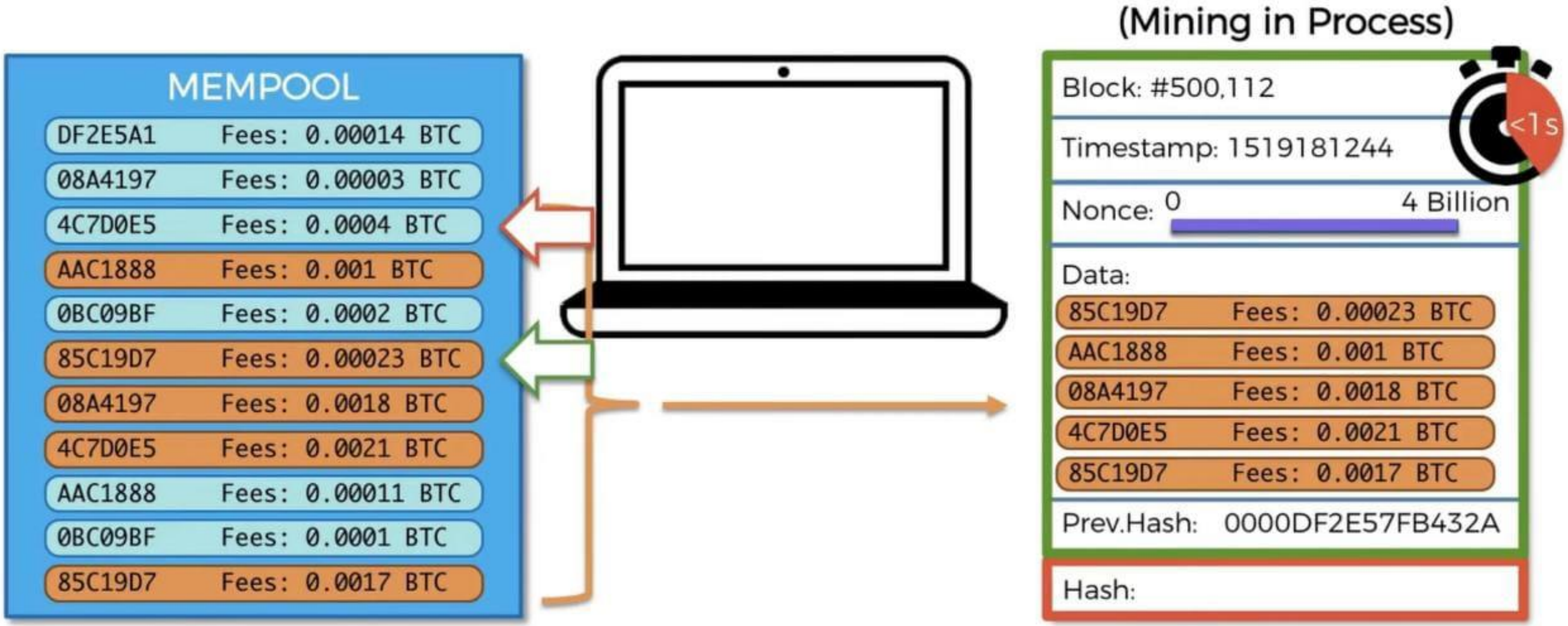
Data:

4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
C19D7	Fees: 0.0017 BTC

v.Hash: 0000DF2E57FB432A

sh:

Change Block Configuration



(Mining in Process)

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

Block: #500,112

Timestamp: 1519181244

Nonce: 0 4 Billion

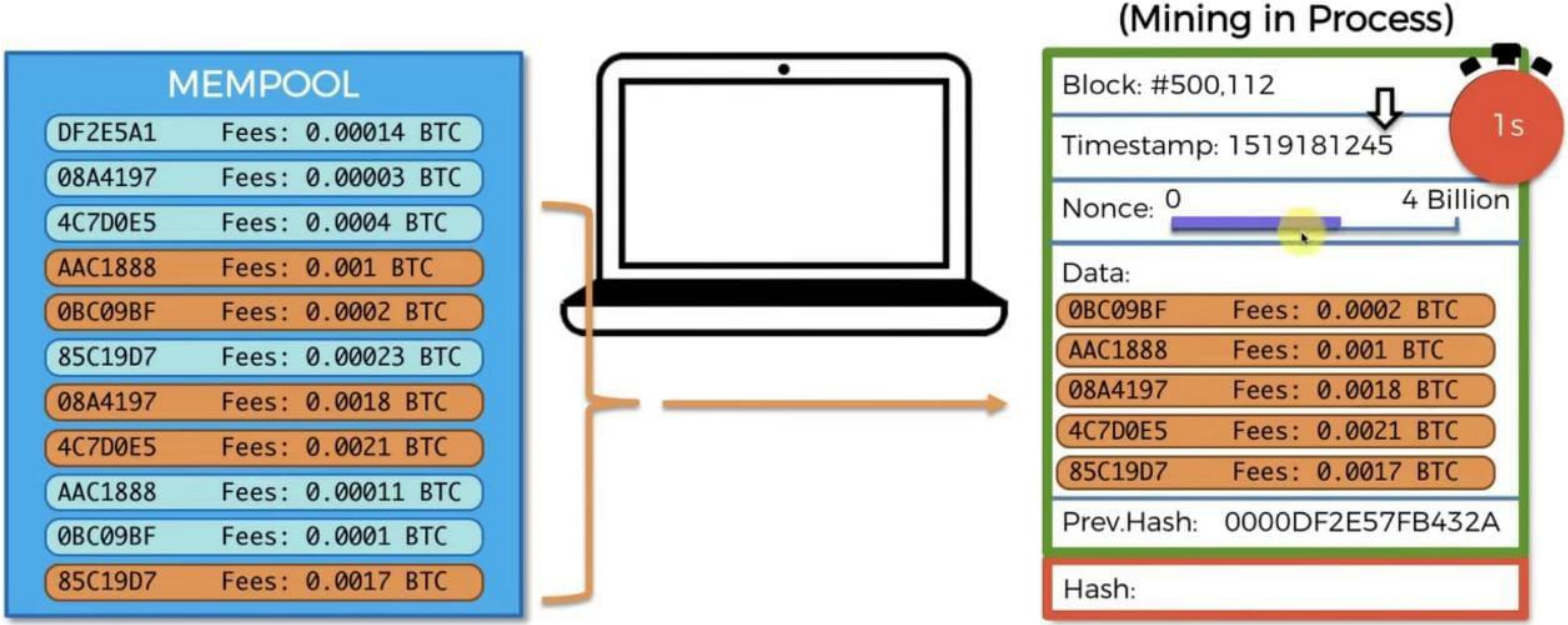
Data:

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:

Time updated:



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

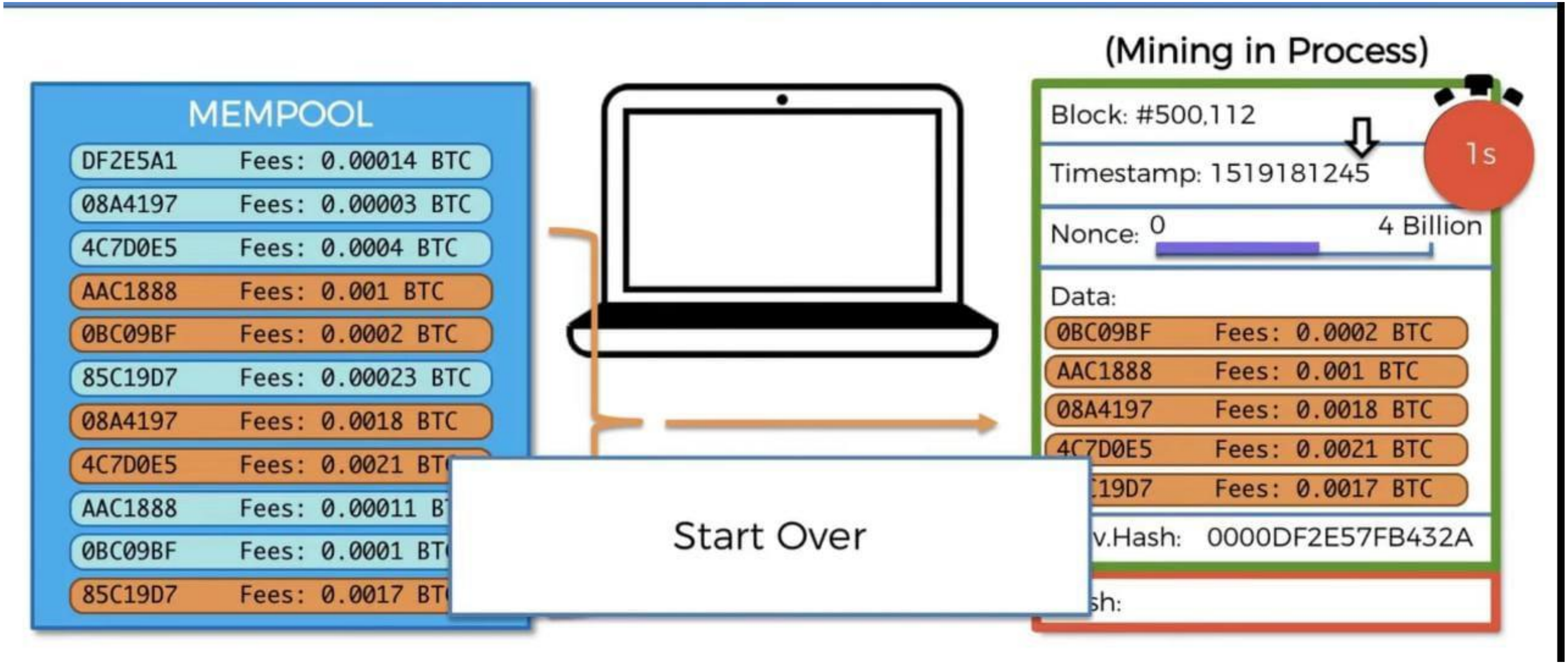
Nonce: 0 4 Billion

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:



(Mining in Process)

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 BT
AAC1888	Fees: 0.00011 B
0BC09BF	Fees: 0.0001 BT
85C19D7	Fees: 0.0017 BT

Start Over

Block: #500,112

Timestamp: 1519181245

Nonce: 0 4 Billion

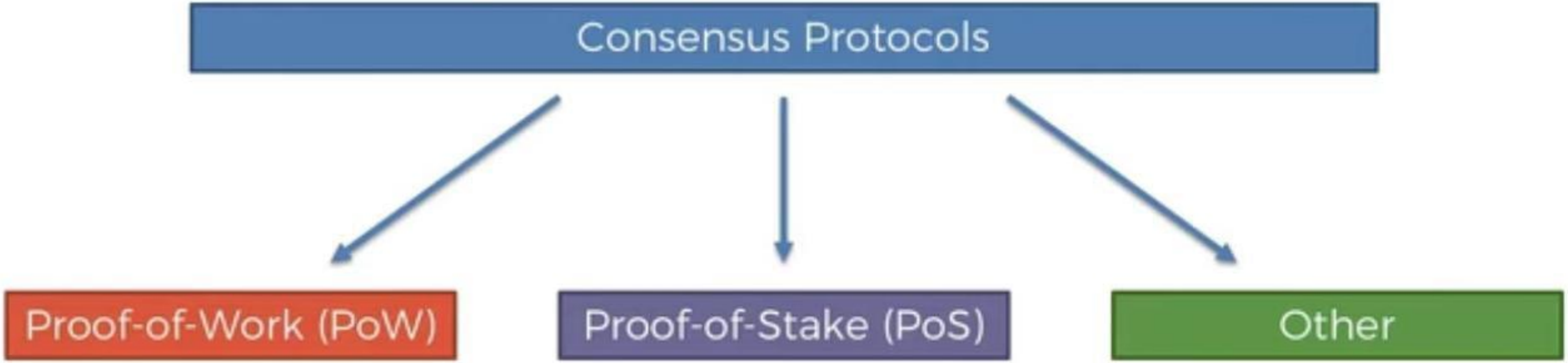
Data:

0BC09BF	Fees: 0.0002 BTC
AAC1888	Fees: 0.001 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
C19D7	Fees: 0.0017 BTC

v.Hash: 0000DF2E57FB432A

sh:

Consensus Protocol



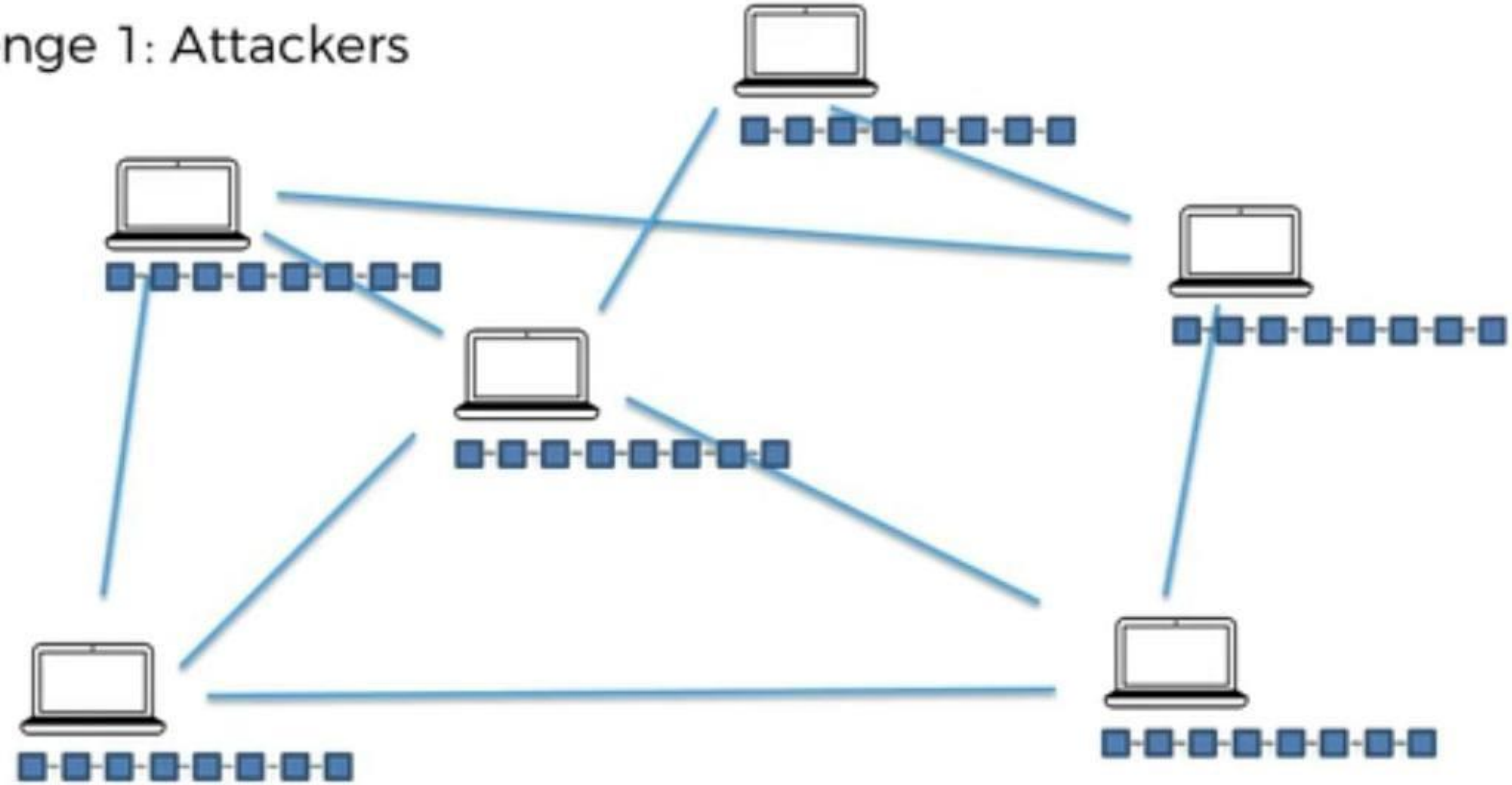
Consensus Protocols

Proof-of-Work (PoW)

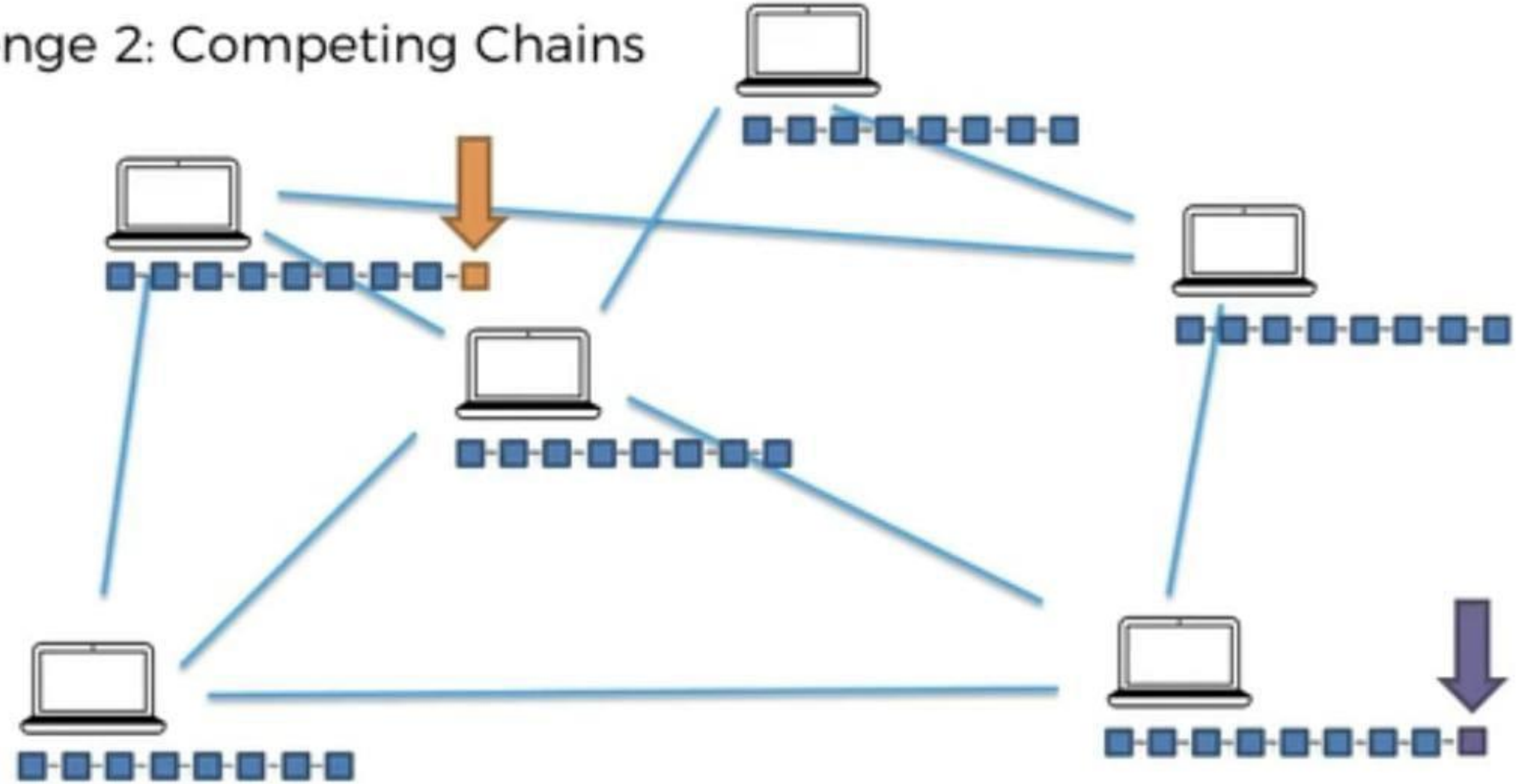
Proof-of-Stake (PoS)

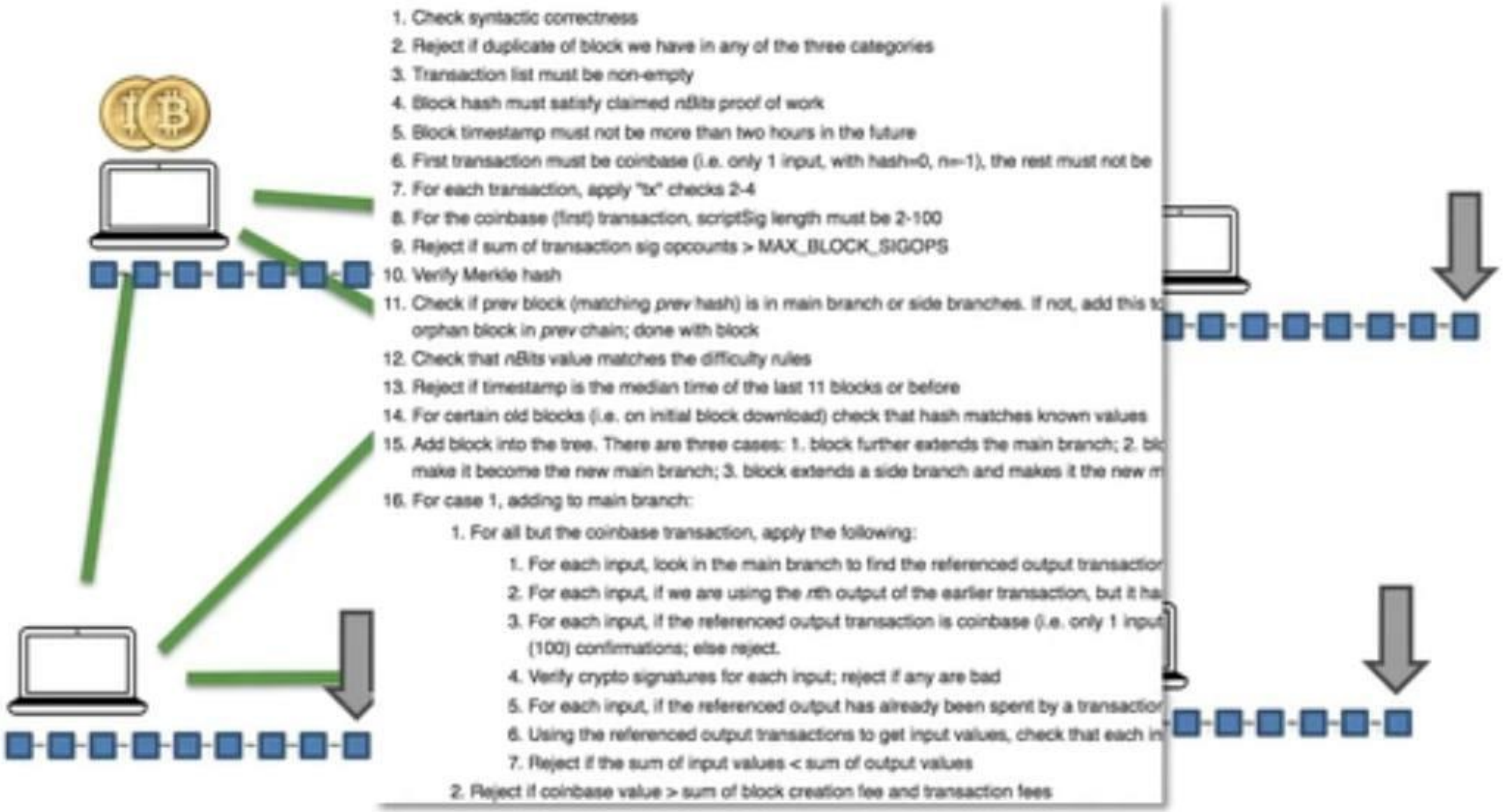
Other

Challenge 1: Attackers

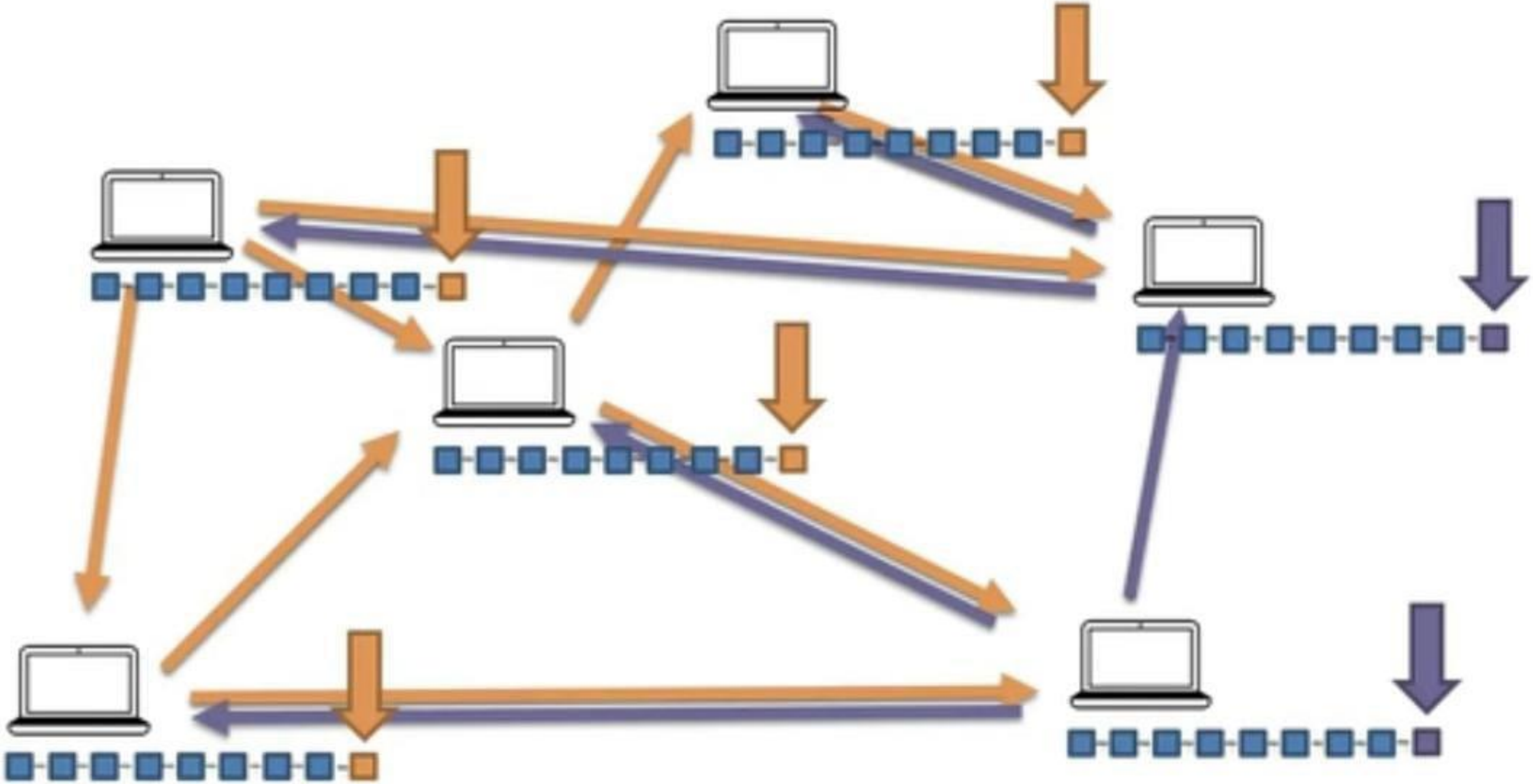


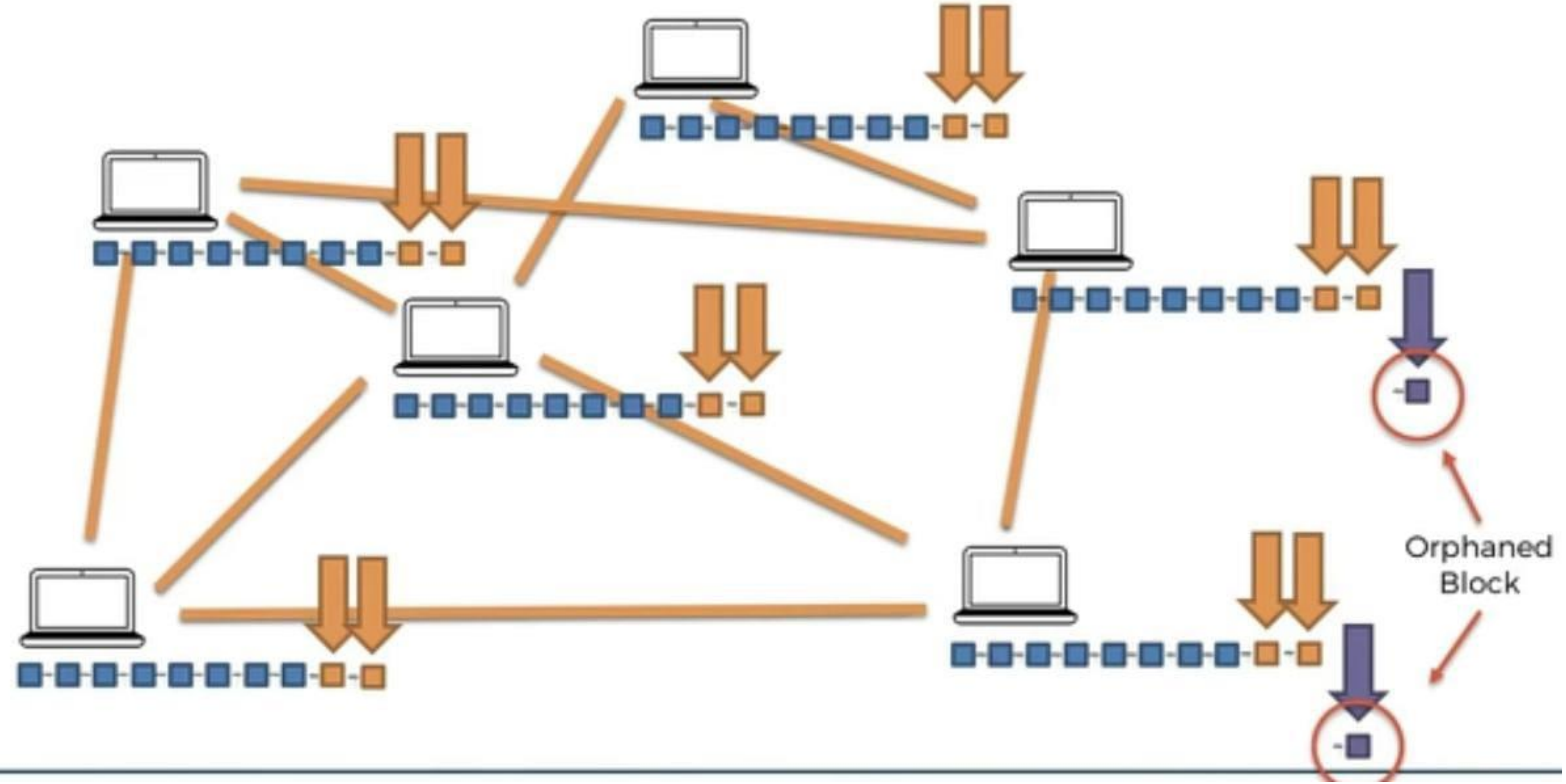
Challenge 2: Competing Chains

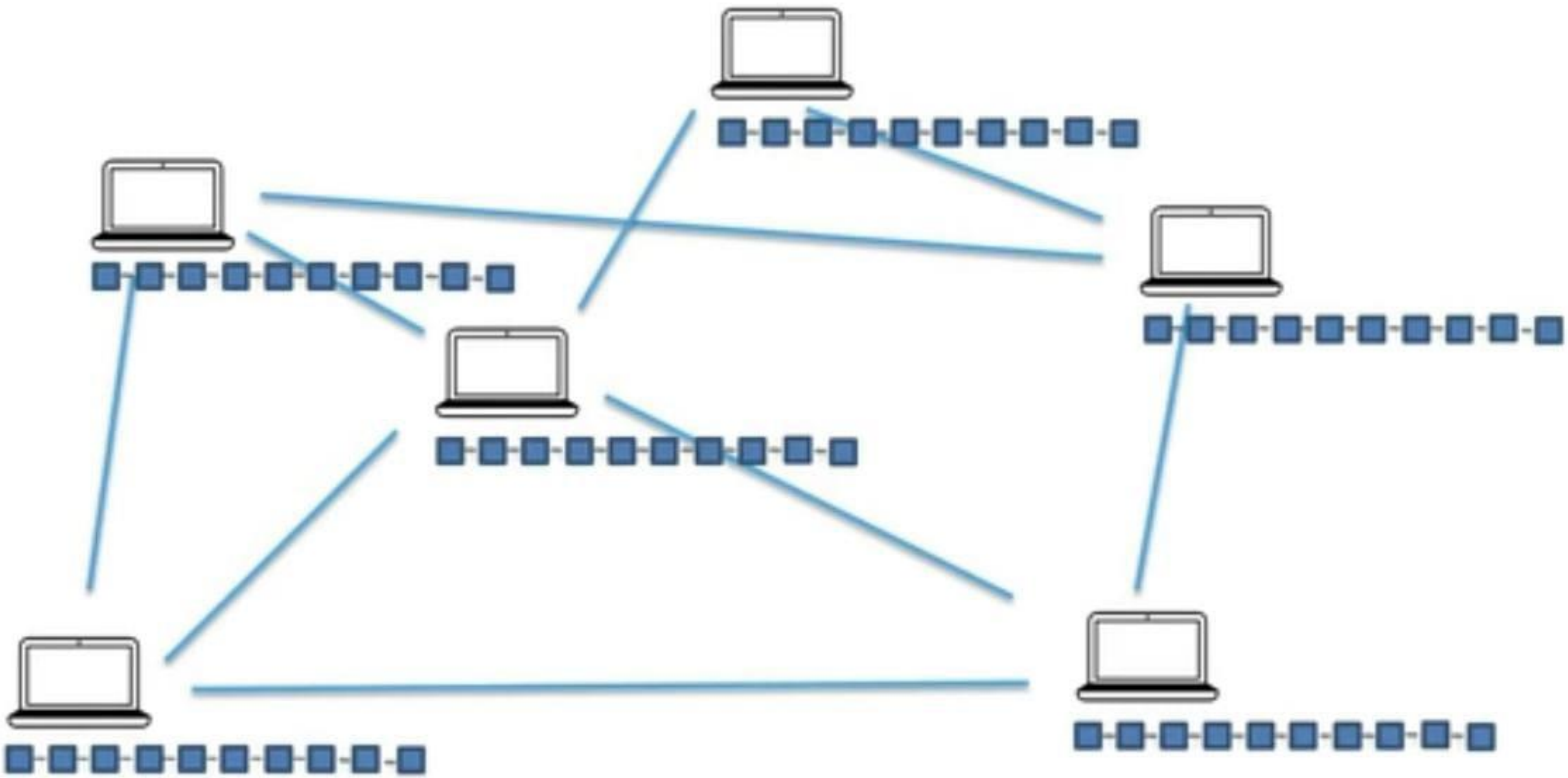




1. Check syntactic correctness
2. Reject if duplicate of block we have in any of the three categories
3. Transaction list must be non-empty
4. Block hash must satisfy claimed *nBits* proof of work
5. Block timestamp must not be more than two hours in the future
6. First transaction must be coinbase (i.e. 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. blo
    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 transactio
        2. For each input, if we are using the *n*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 transactio
        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




Orphaned
Block



CA-002

https://www.coinbase.com/en-gb/learn/crypto-basics/how-do-cryptocurrency-miners-work

Acknowledgement and Source:

- https://www.udemy.com/course/build-your-blockchain-az/