



Blockchain and Cryptocurrency

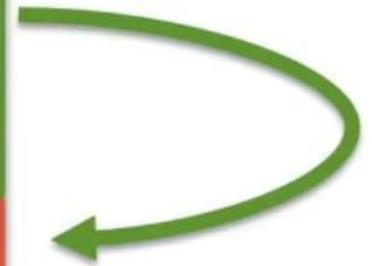
By: Syeda Tayyaba Bukhari

Nonce Range

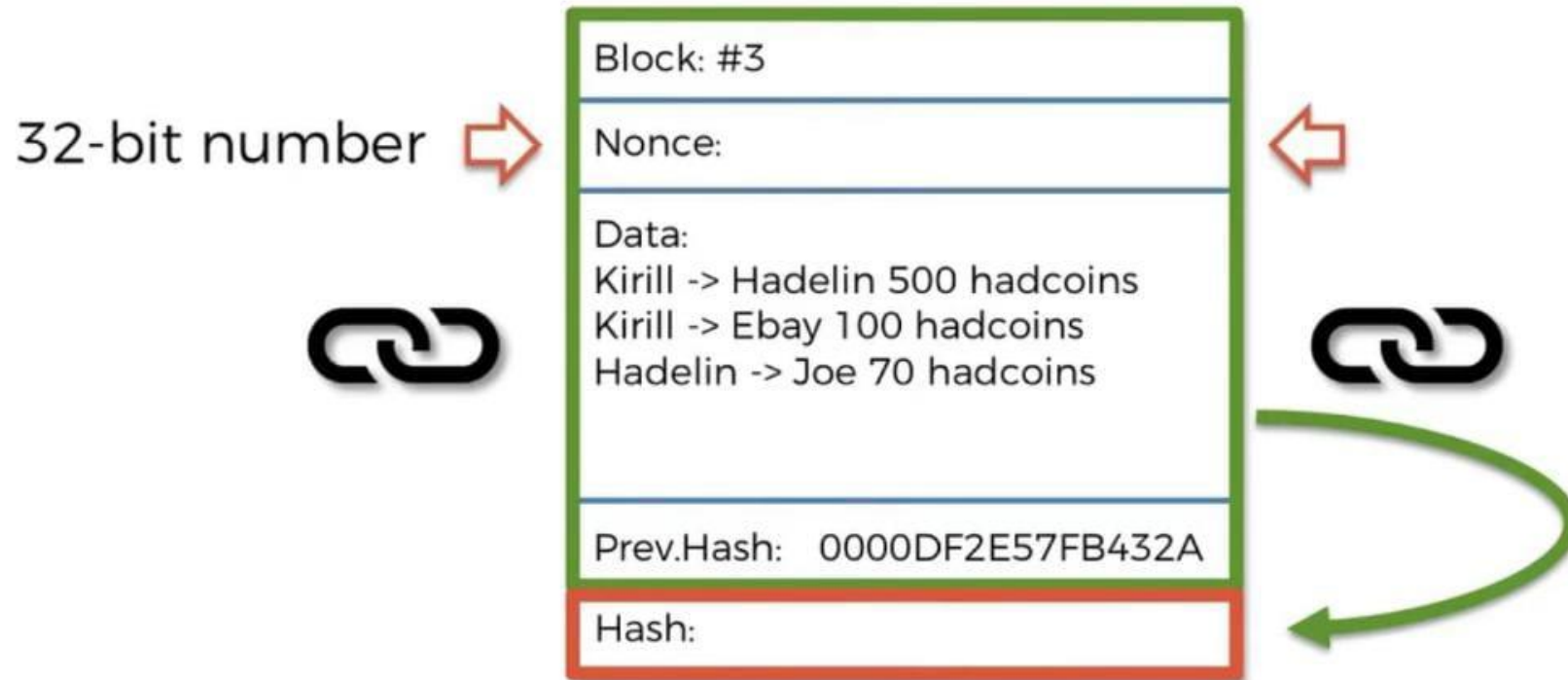
What we
know about
nonce till
now:



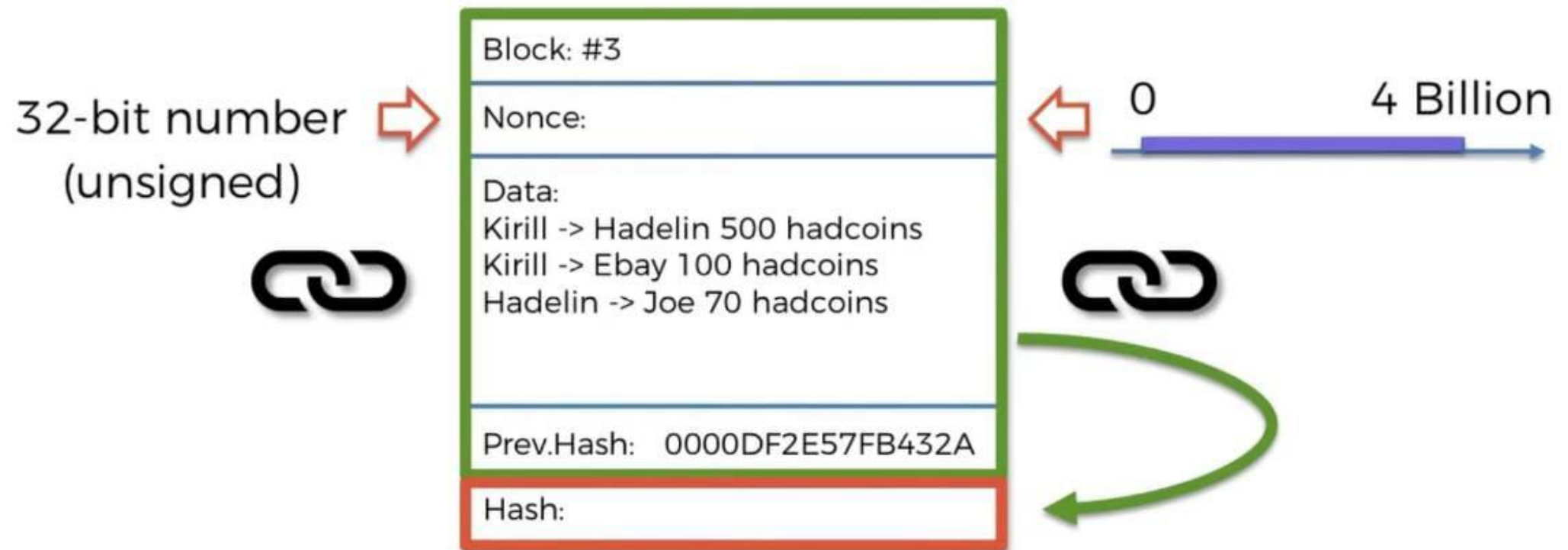
Block: #3
Nonce:
Data: Kirill -> Hadelin 500 hadcoins Kirill -> Ebay 100 hadcoins Hadelin -> Joe 70 hadcoins
Prev.Hash: 0000DF2E57FB432A
Hash:



Length of Nonce:



Range:



Some Calculations regarding percentage of finding golden nonce

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:

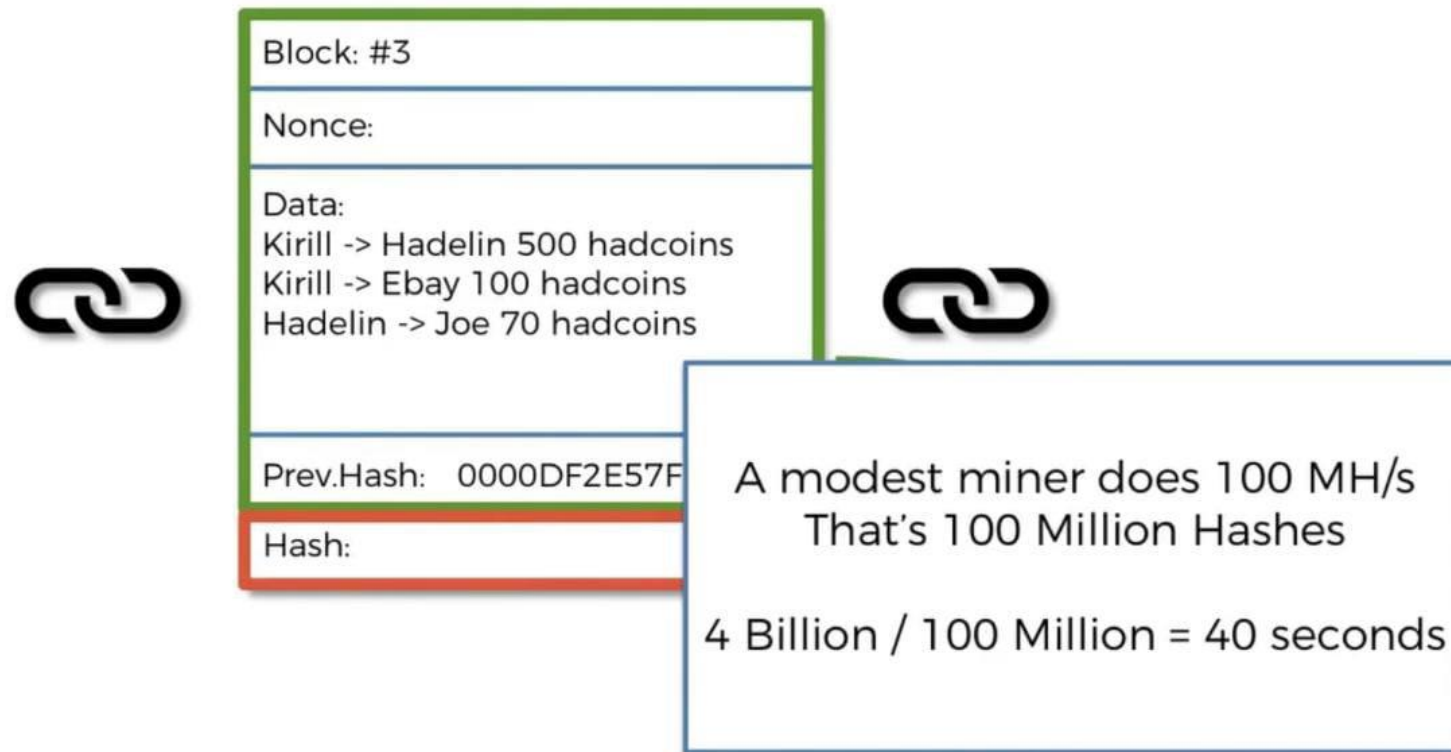
The Nonce is a 32-bit number, the Max Nonce = $2^{32} = 4,294,967,296 = 4 \times 10^9$

Assuming no collisions, this means 4×10^9 different hashes

Probability that ONE of them will be valid: $4 \times 10^9 \times 2 \times 10^{-22} = 8 \times 10^{-13} \approx 10^{-12} = 0.000000000001\%$

Conclusion: One Nonce Range is not enough

isn't it too easy to find the golden nonce??



Timestamp: another attribute of a block



Unix Time.is 1519636011 Blockchain

← → ↻ ⌂ ⓘ https://time.is/Unix_time_now ☆ ⋮

Time.is

Unix time now

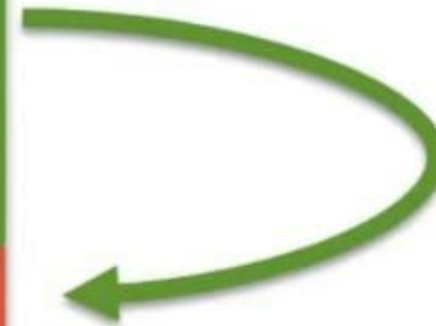
1519636011

Time in Southport: 19:06:51

Udemy



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:

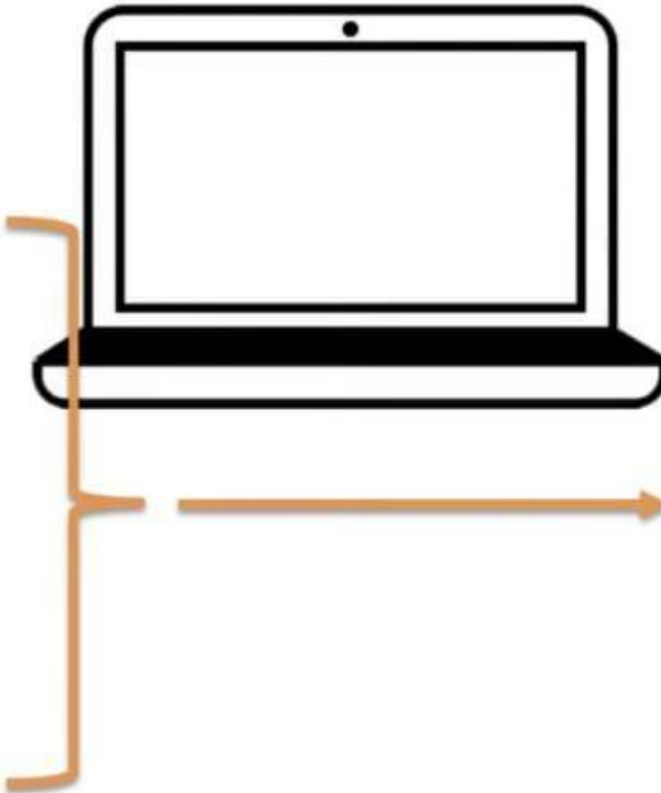
Data:

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:

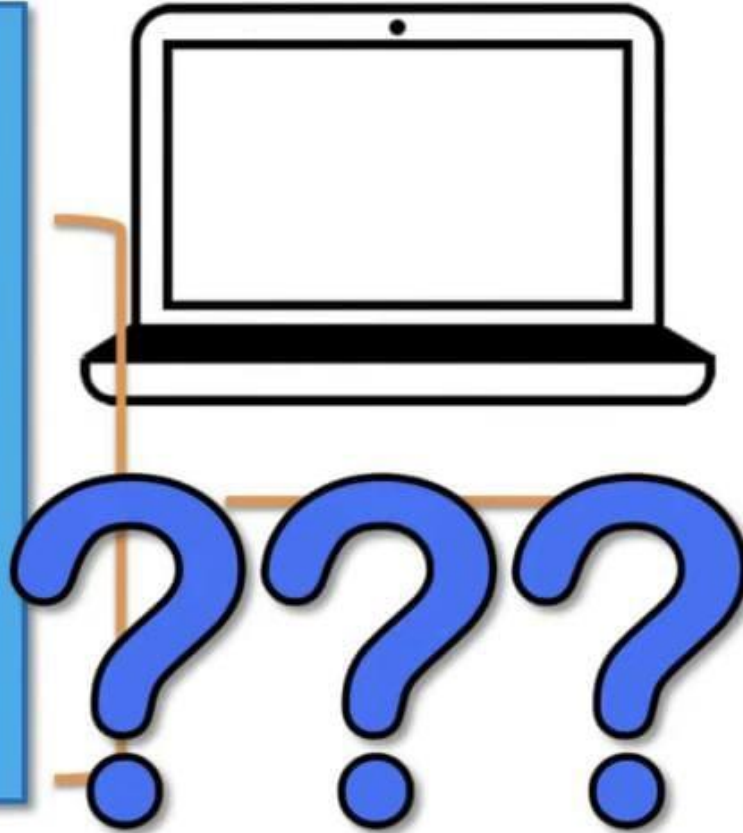
Data:

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

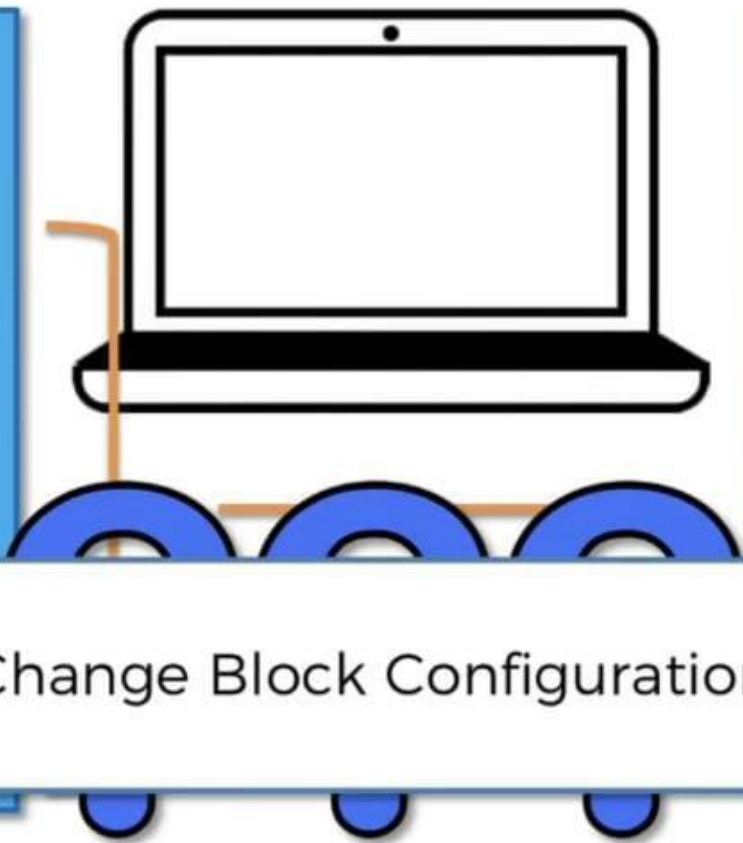
85C19D7 Fees: 0.0017 BTC

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 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

Timestamp: 1519181244

Nonce: 0

4 Billion

Data:

4C7D0E5 Fees: 0.0004 BTC

AAC1888 Fees: 0.001 BTC

08A4197 Fees: 0.0018 BTC

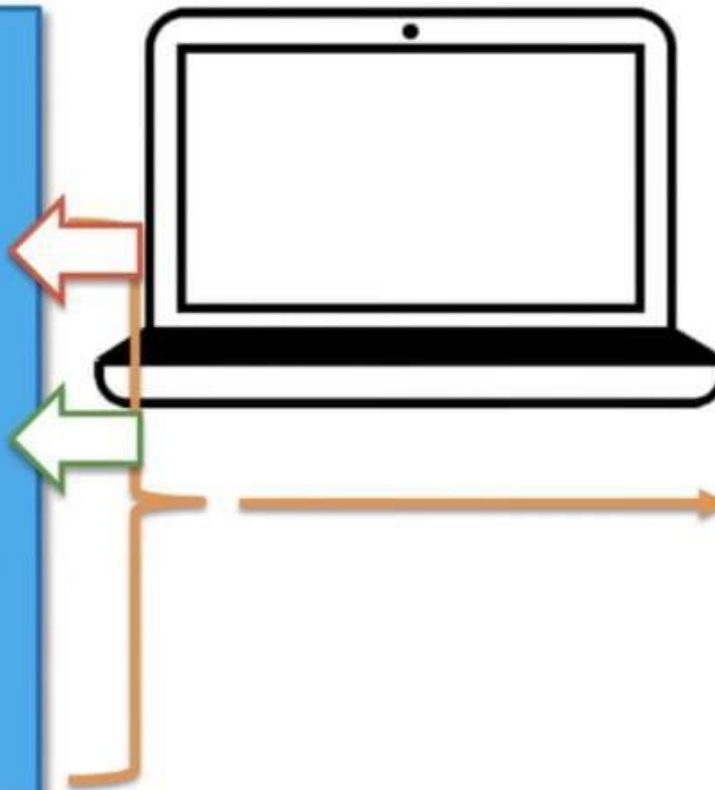
4C7D0E5 Fees: 0.0021 BTC

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 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC

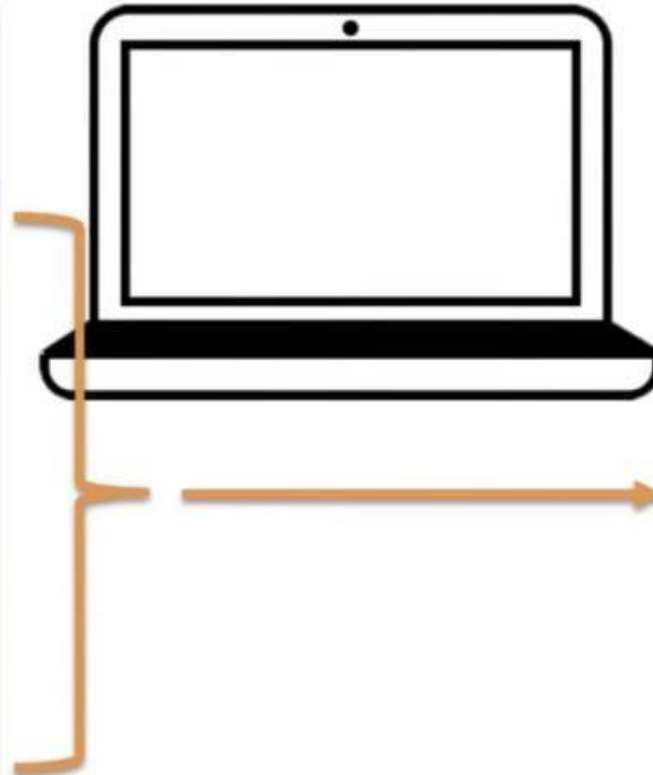


(Mining in Process)

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:	

Time updated:

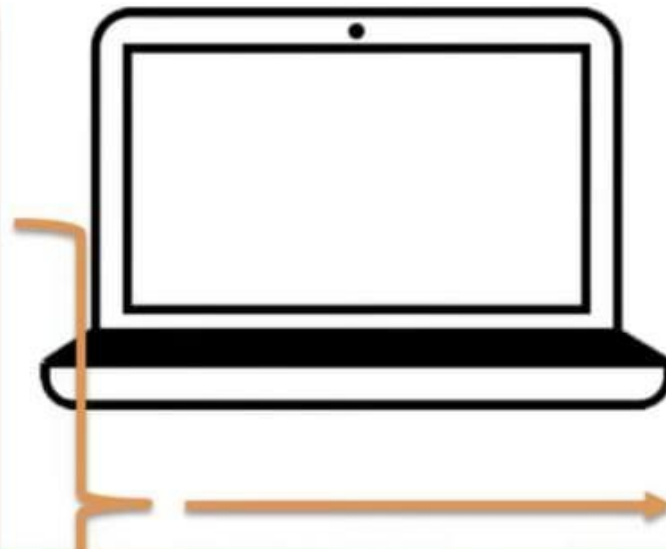
MEMPOOL	
DF2E5A1	Fees: 0.00014 BTC
08A4197	Fees: 0.00003 BTC
4C7D0E5	Fees: 0.0004 BTC
AAC1888	Fees: 0.001 BTC
0BC09BF	Fees: 0.0002 BTC
85C19D7	Fees: 0.00023 BTC
08A4197	Fees: 0.0018 BTC
4C7D0E5	Fees: 0.0021 BTC
AAC1888	Fees: 0.00011 BTC
0BC09BF	Fees: 0.0001 BTC
85C19D7	Fees: 0.0017 BTC



(Mining in Process)

Block: #500,112	↓	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		
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



Start Over

(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:

1s

Acknowledgement and Source:

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