

# **Blockchain Introduction**

# Plan of Attack

- What is a Blockchain?
- Understanding SHA256 Hash
- Immutable Ledger
- Distributed P2P Network
- How Mining Works (Part 1: The Nonce)
- How Mining Works (Part 2: The cryptographic puzzle)
- Byzantine Fault Tolerance
- Consensus Protocol (Part 1: Defense against attackers)
- Consensus Protocol (Part 2: Competing chains)
- Blockchain Demo

# What is a blockchain

A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography.

– *Wikipedia*

# A block



1. Data: "Hello World!"
2. Prev.Hash: 034DFA357
3. Hash: 4D56E1F05

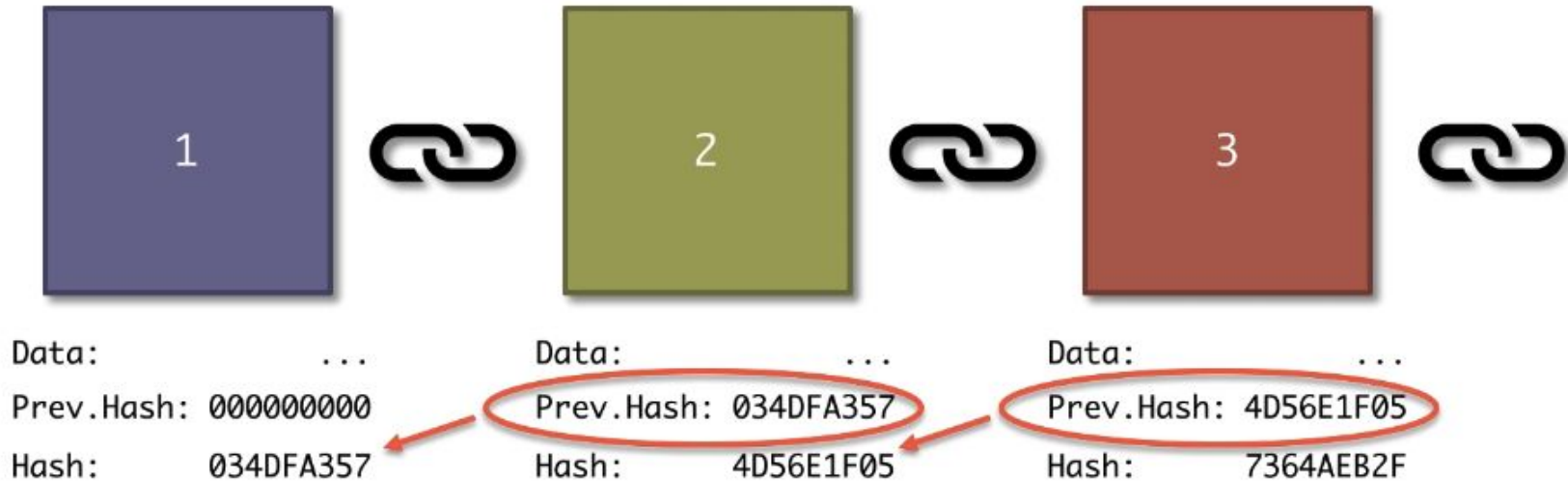


Block: #3
Data: Kirill -> Hadelin 500 hadcoins Kirill -> Ebay 100 hadcoins Hadelin -> Joe 70 hadcoins
Prev.Hash: 0000DF2E57FB432A
Hash:

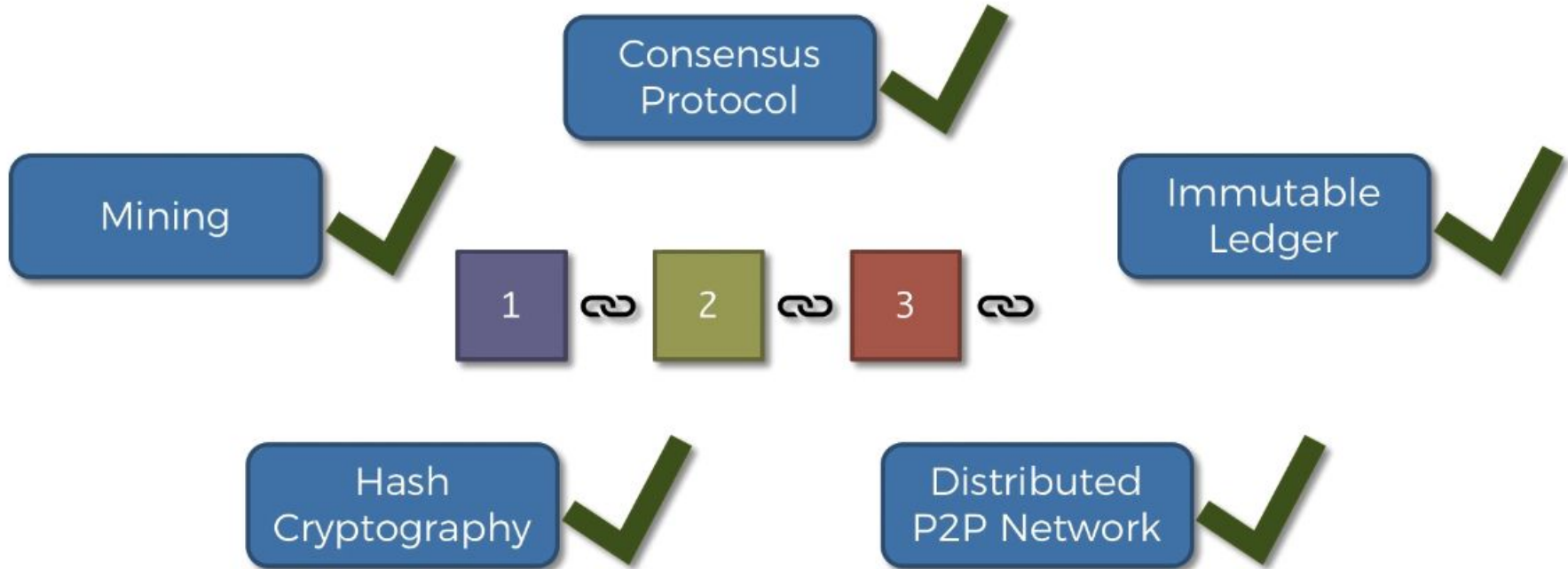


# A chain of blocks

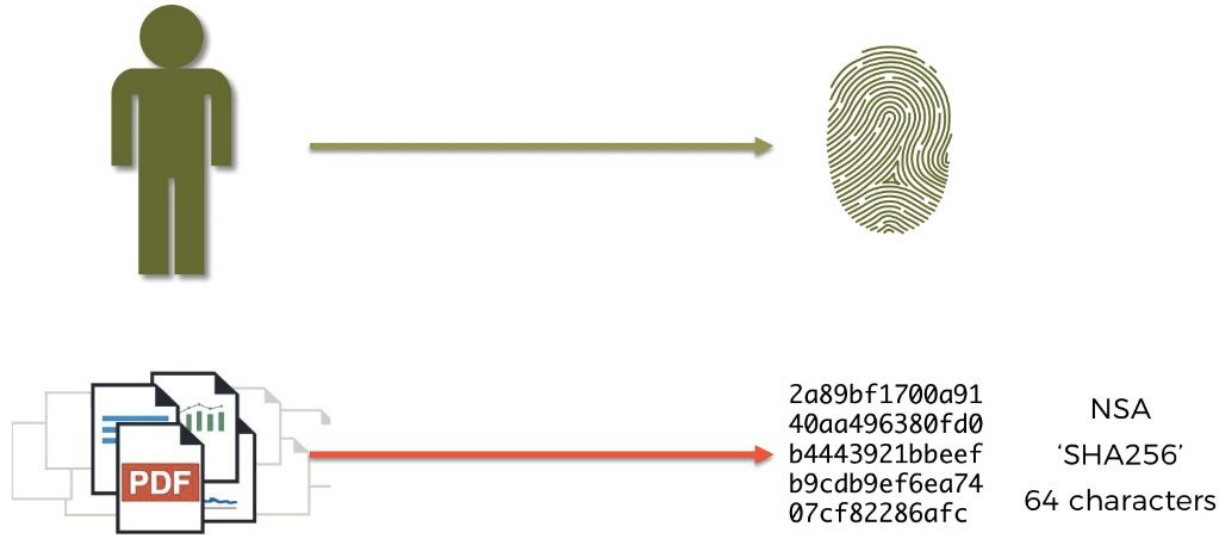
## GENESIS BLOCK



# Introductory plan

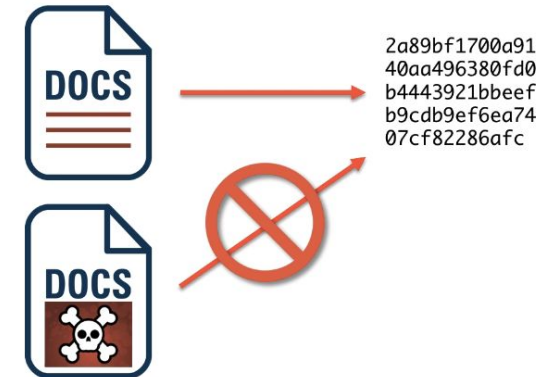
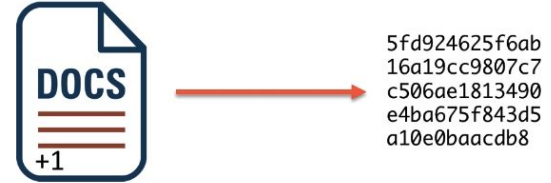
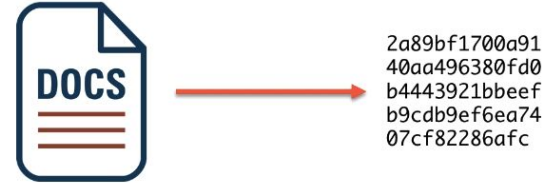


# Understanding SHA256 Hash



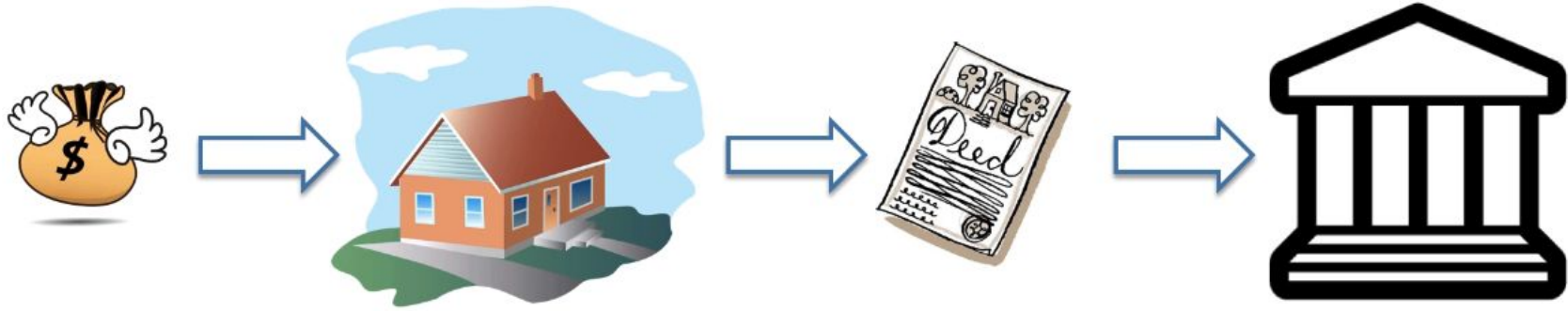
# The 5 requirements for Hash algorithms

1. One-Way
2. Deterministic
3. Fast Computation
4. The Avalanche Effect
5. Must withstand collisions





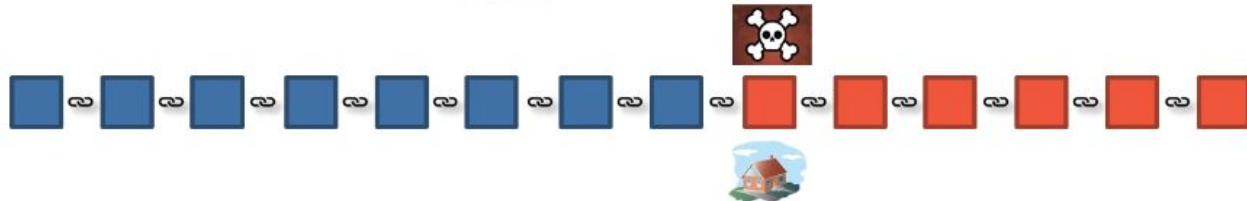
# Immutable Ledger



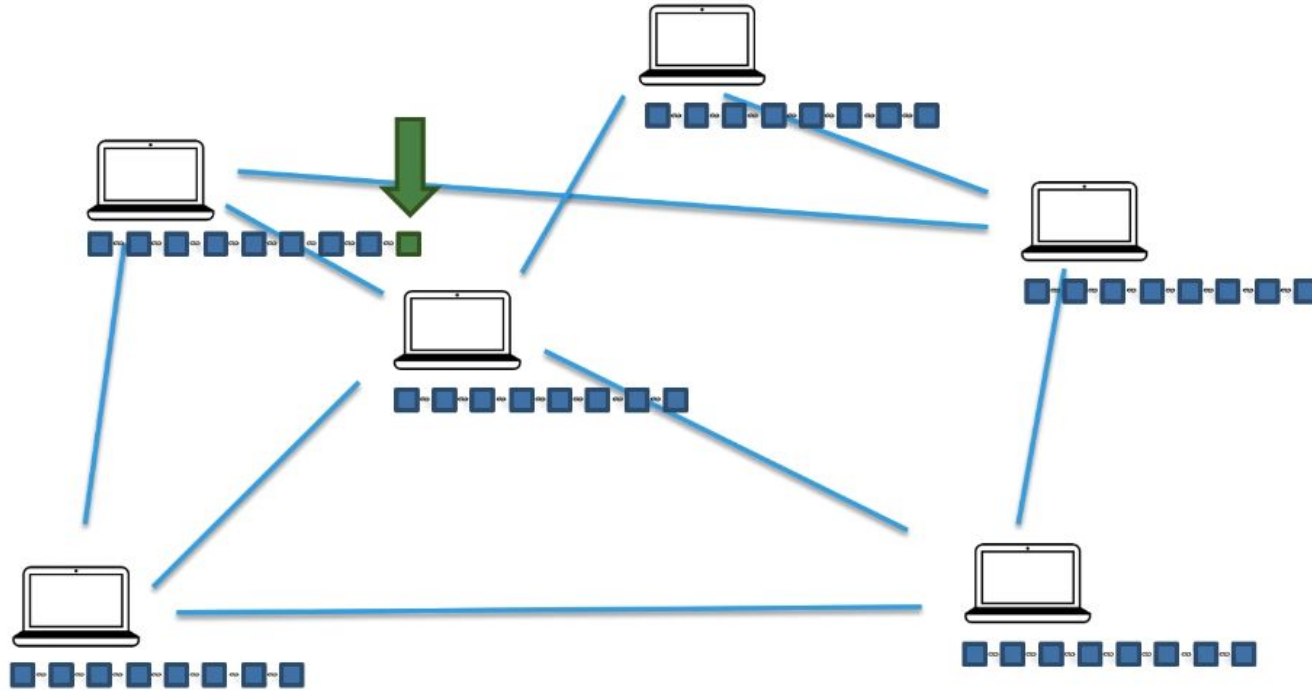
Traditional Ledger



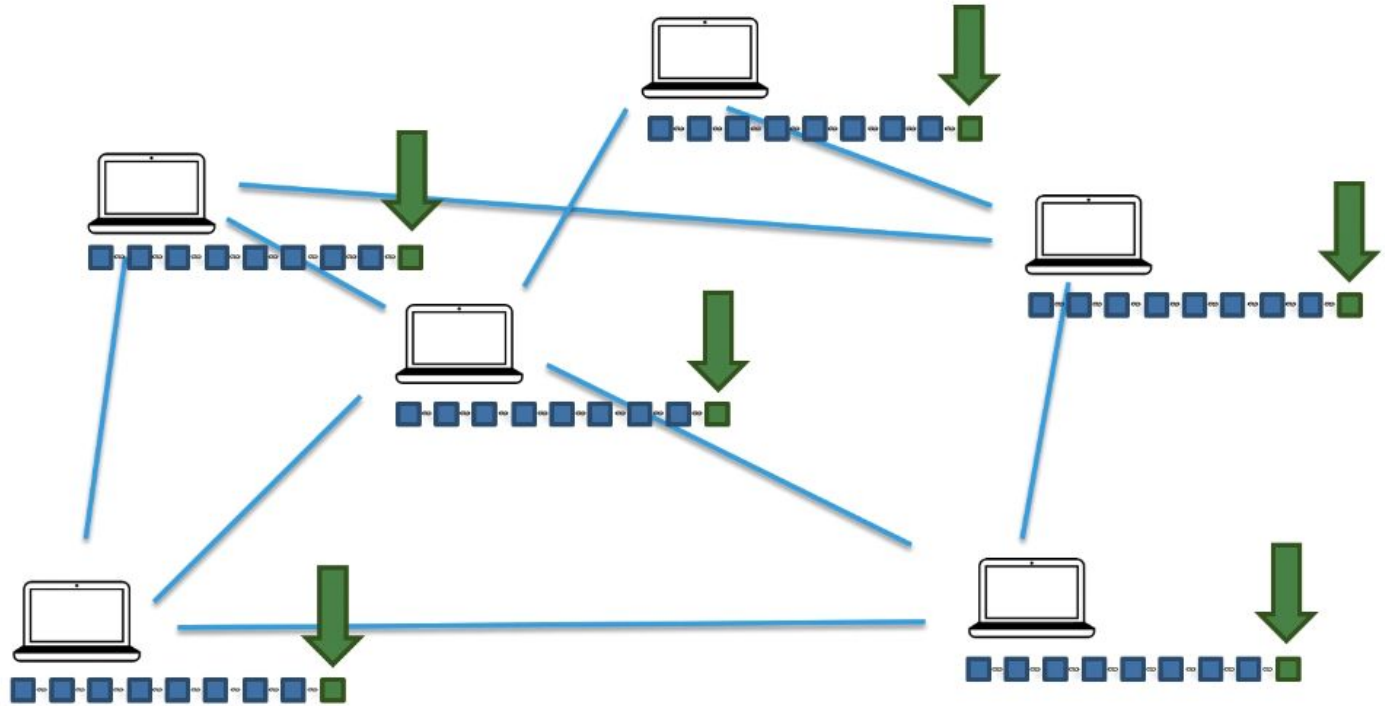
Blockchain



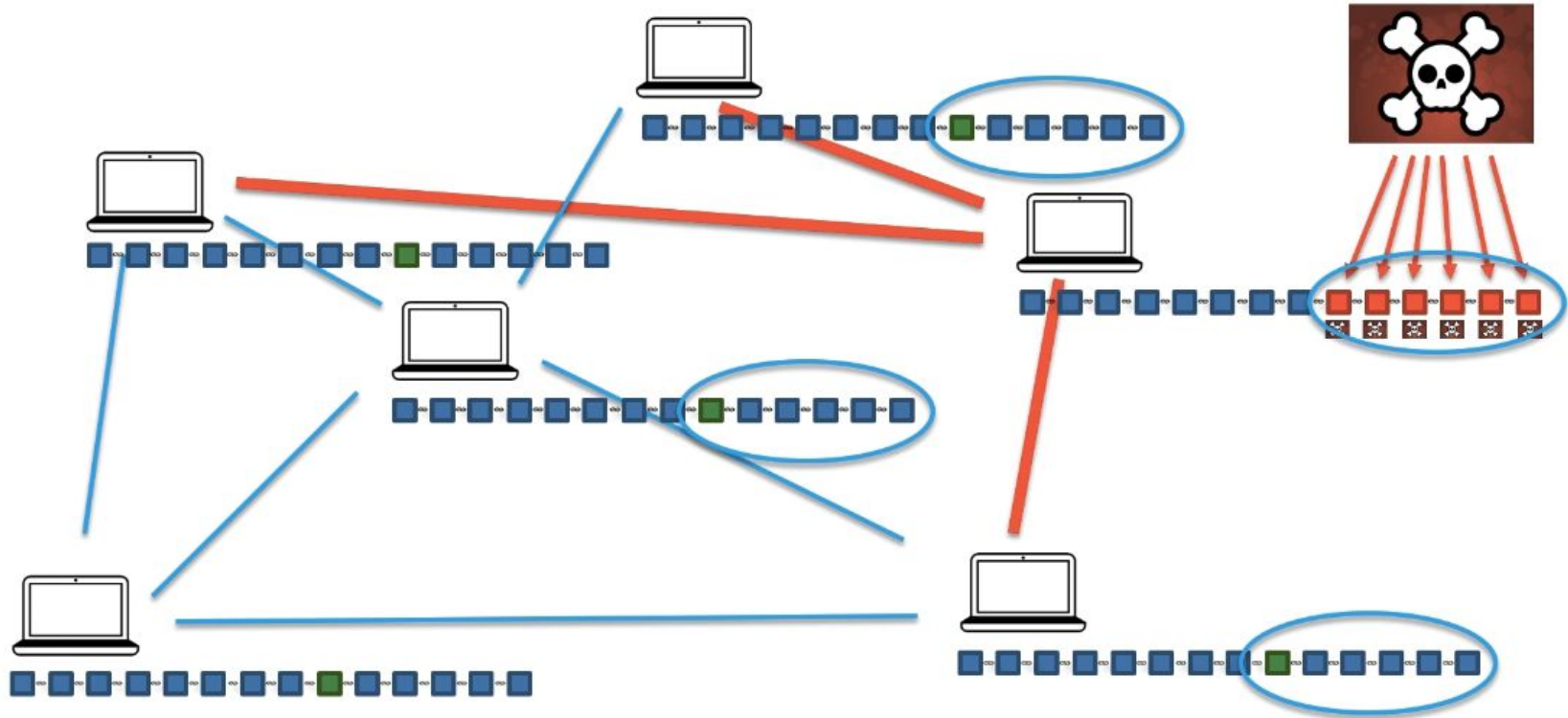
# Distributed P2P Network



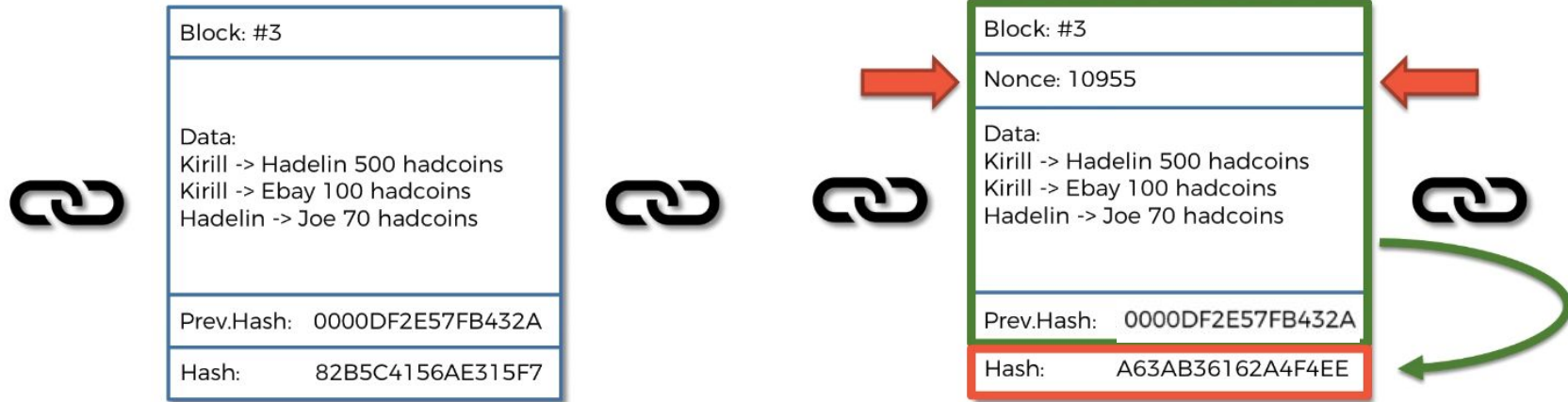
# Broadcasting



# Trust in a trustless environment



# How Mining Works



# Cryptographic puzzle

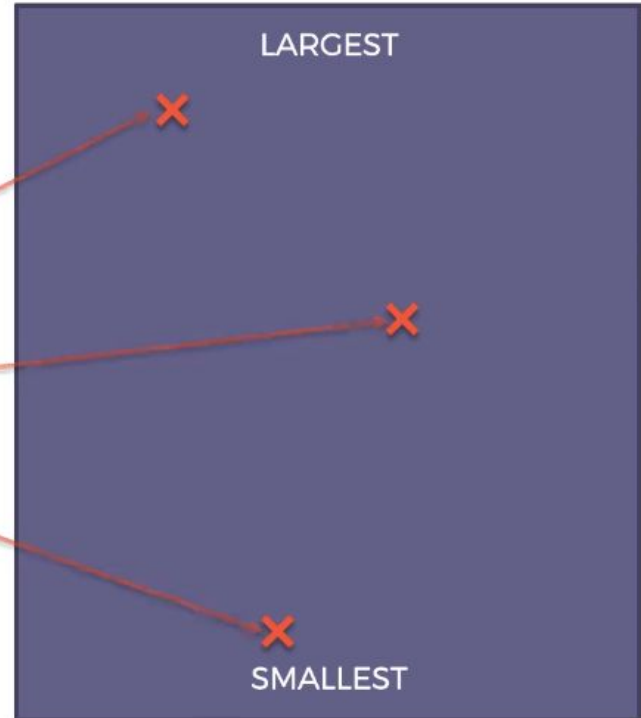
## A Hash is a Number

18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68  
=11232962686236154915841062771303455665105266333  
445130312258268457057784990824

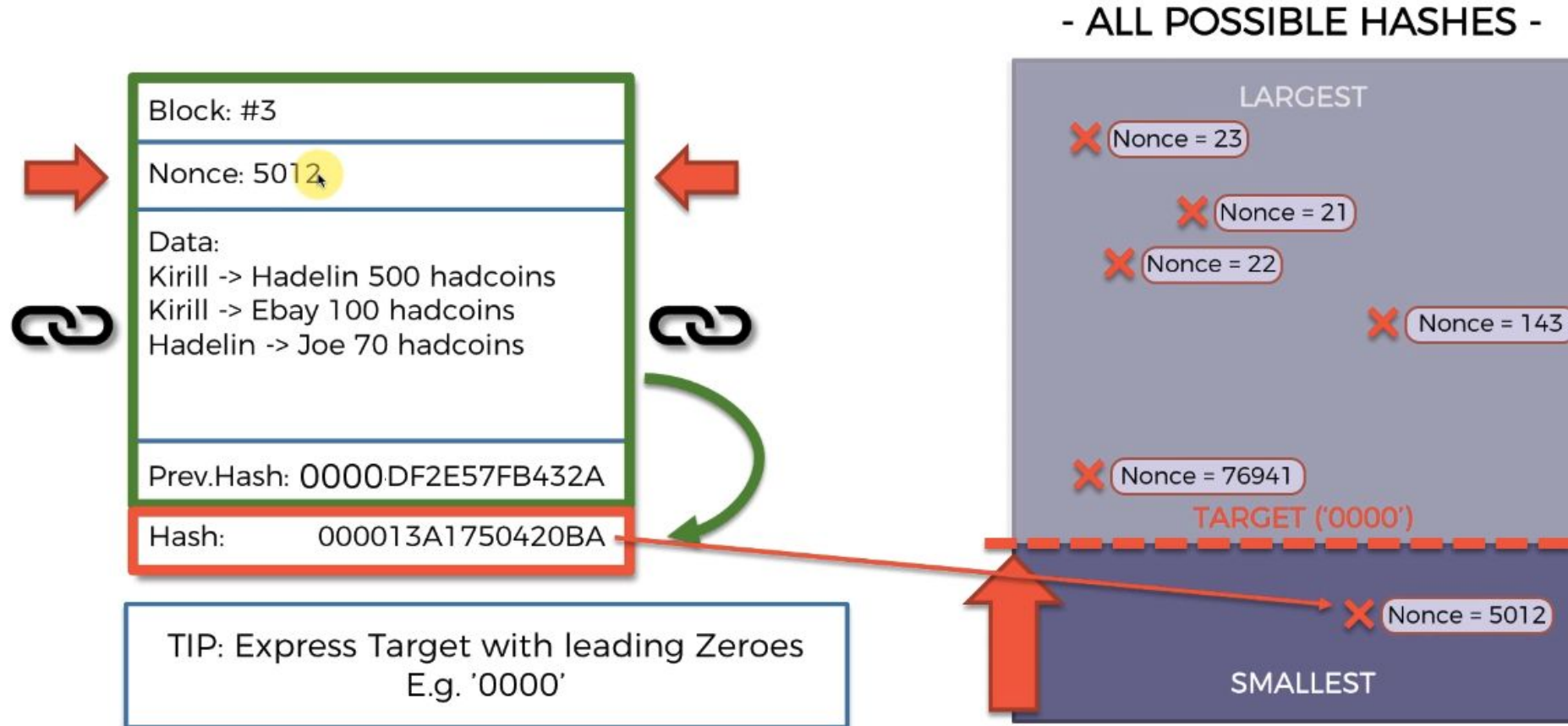
```
00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923
      =000000000000000218420711603109937116824492054445
      852323869008912526075378993443
```

[illegible]

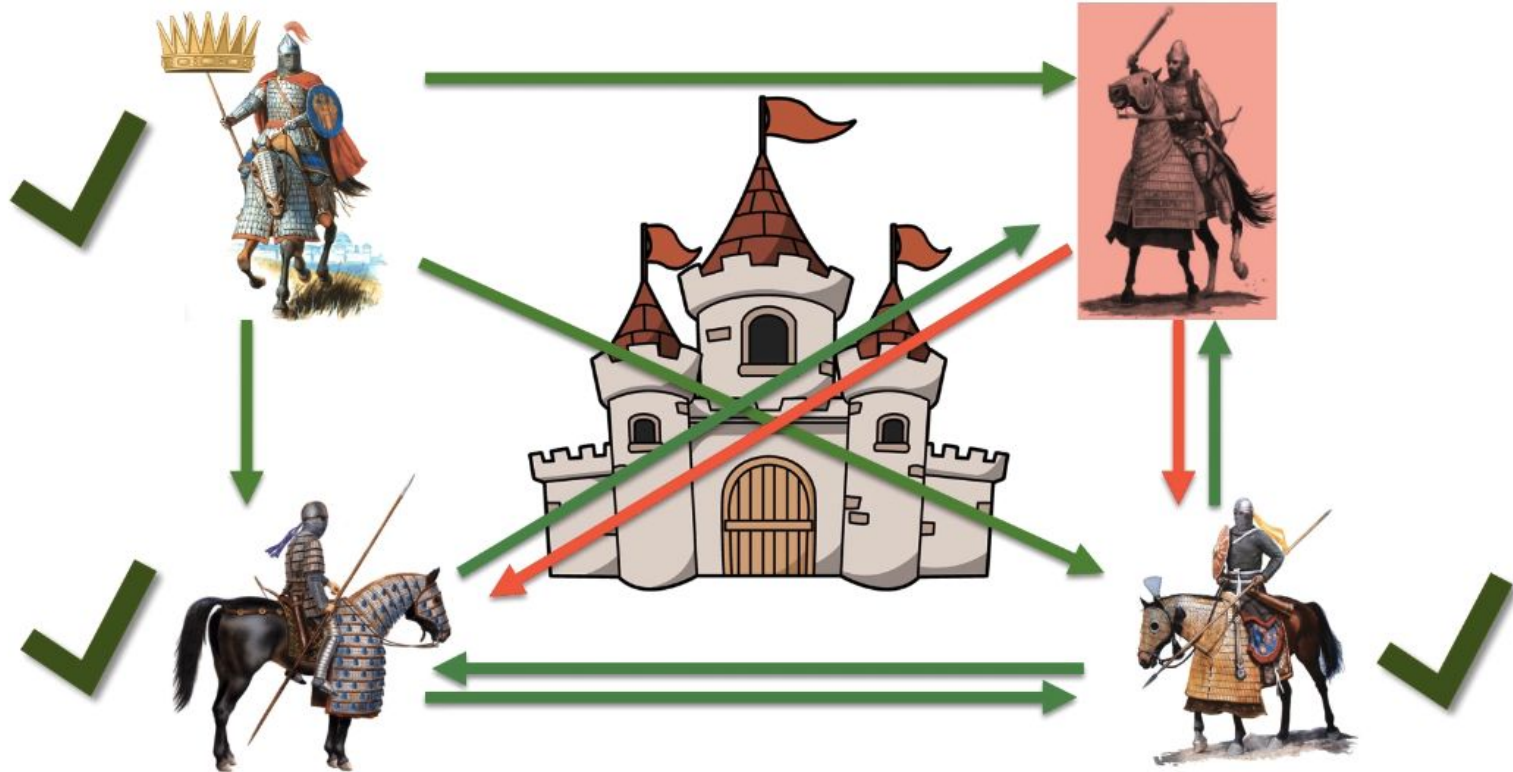
- ALL POSSIBLE HASHES -



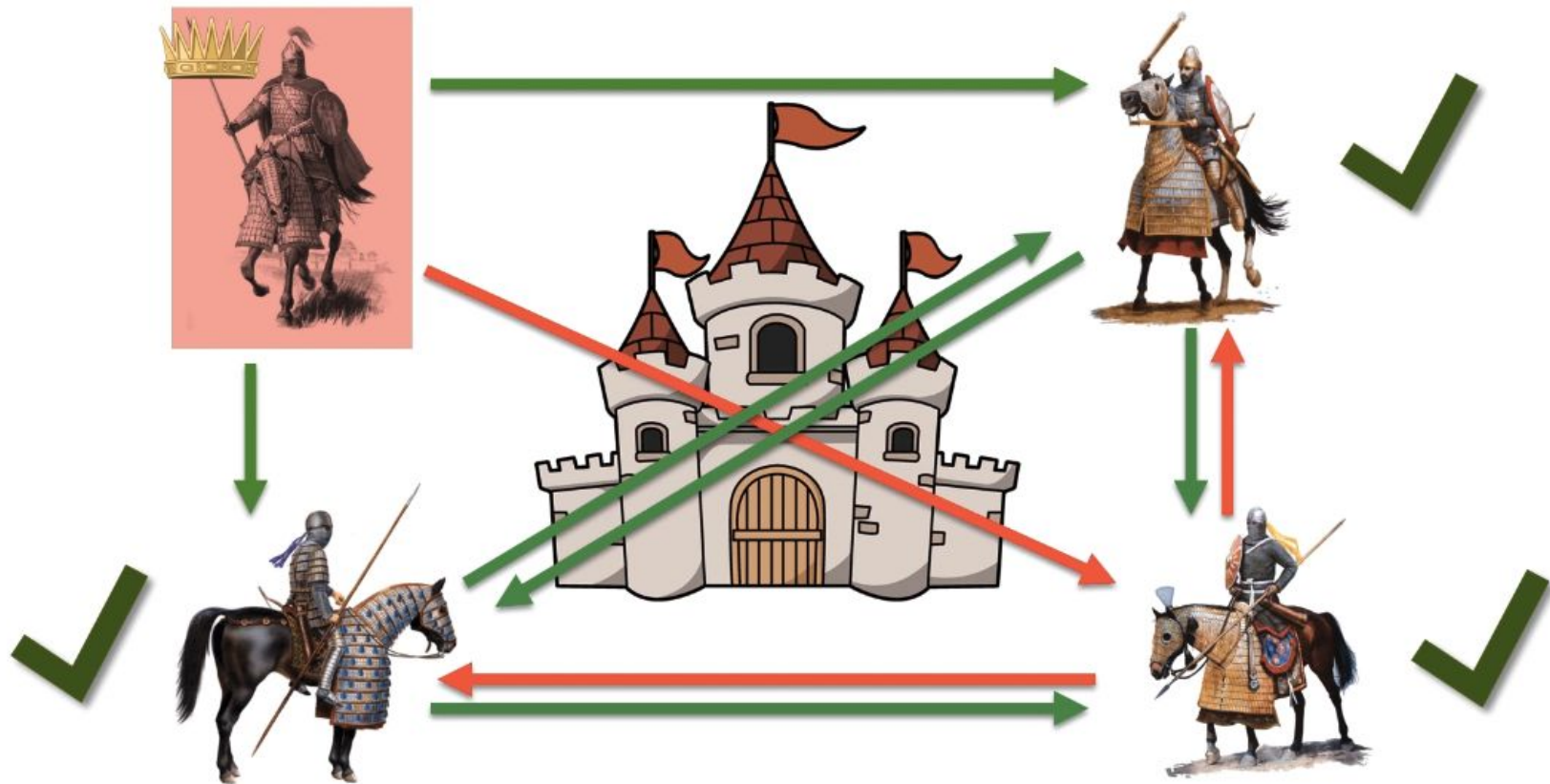
# PoW : only exhaustive brute force works



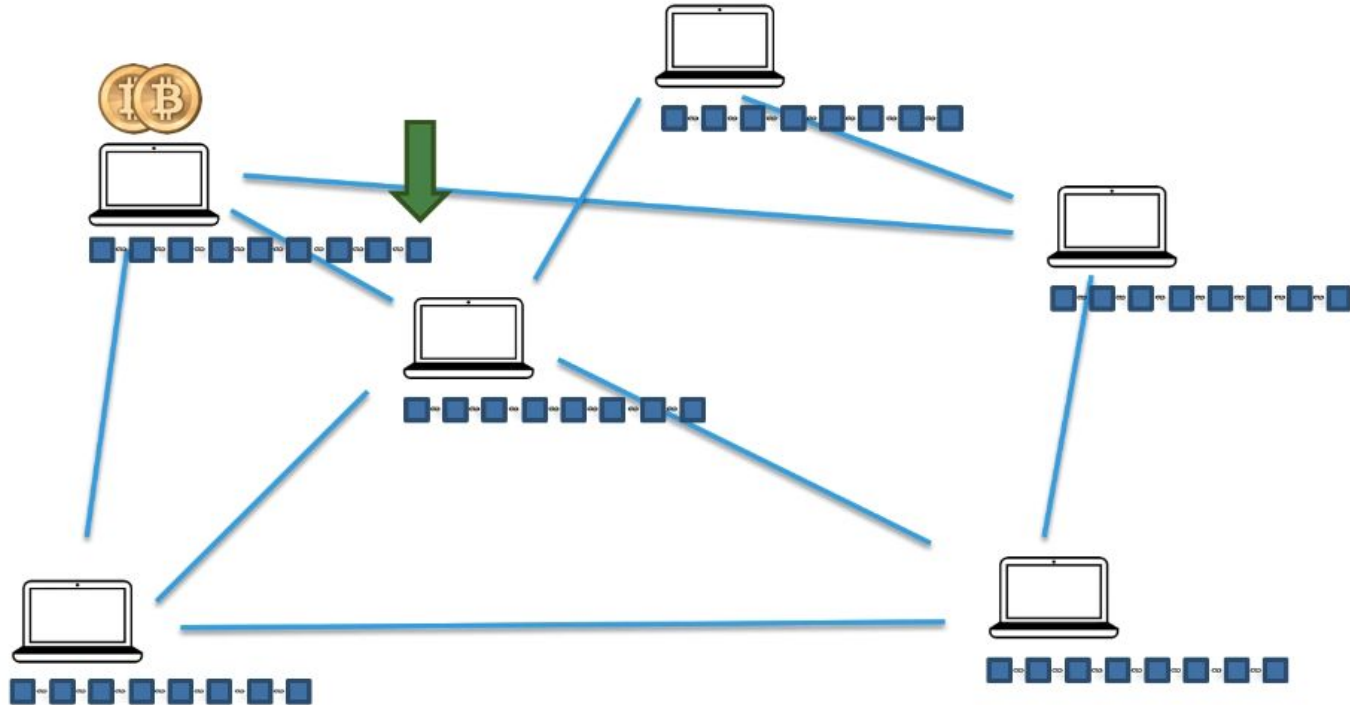
# Byzantine Fault Tolerance : achieving consensus with traitors



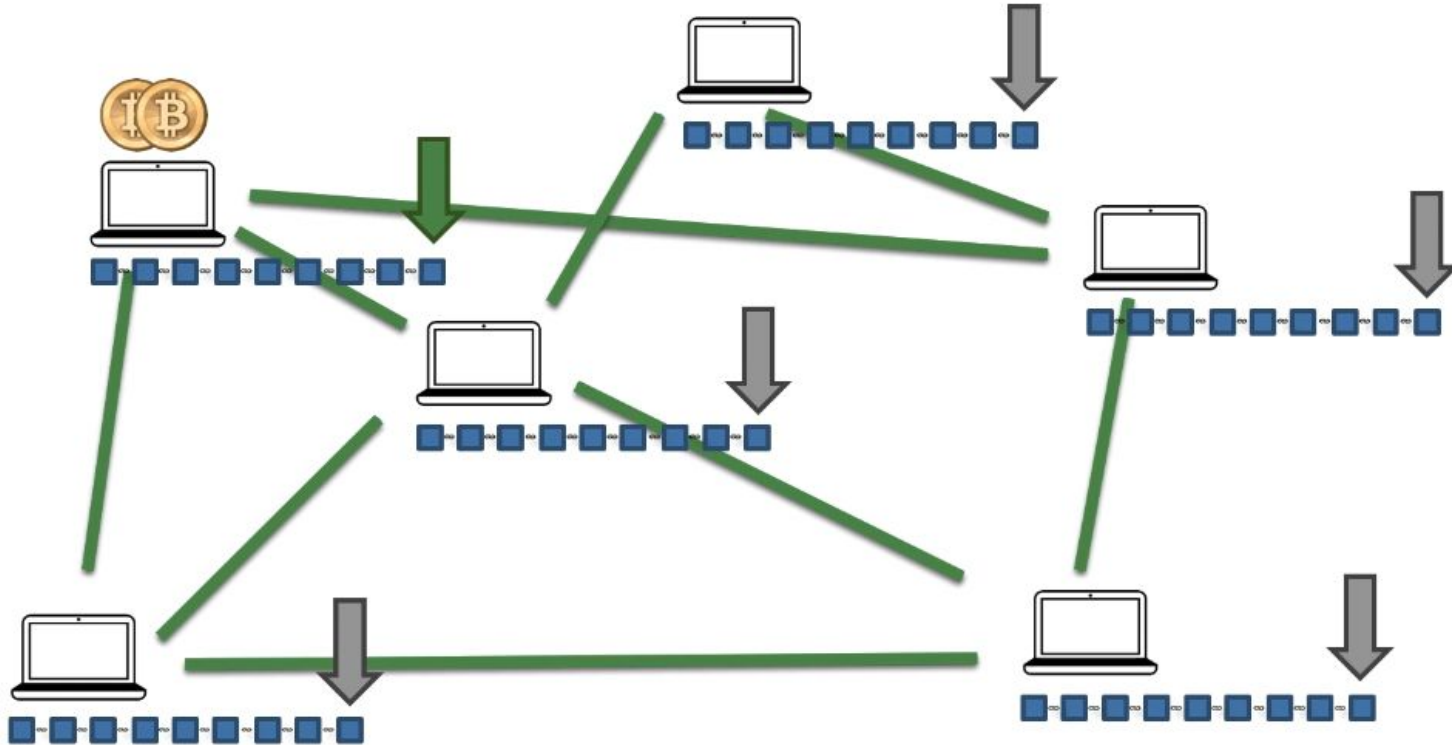




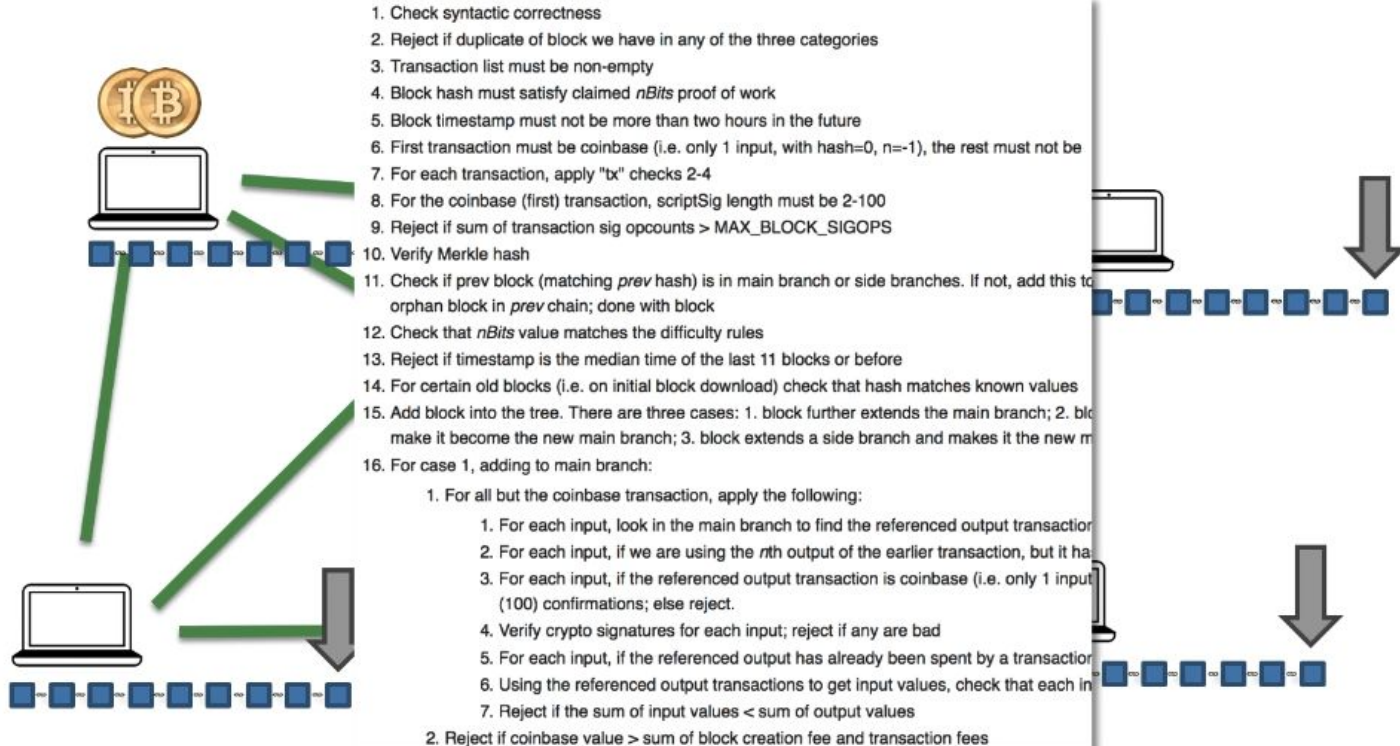
# Consensus Protocol



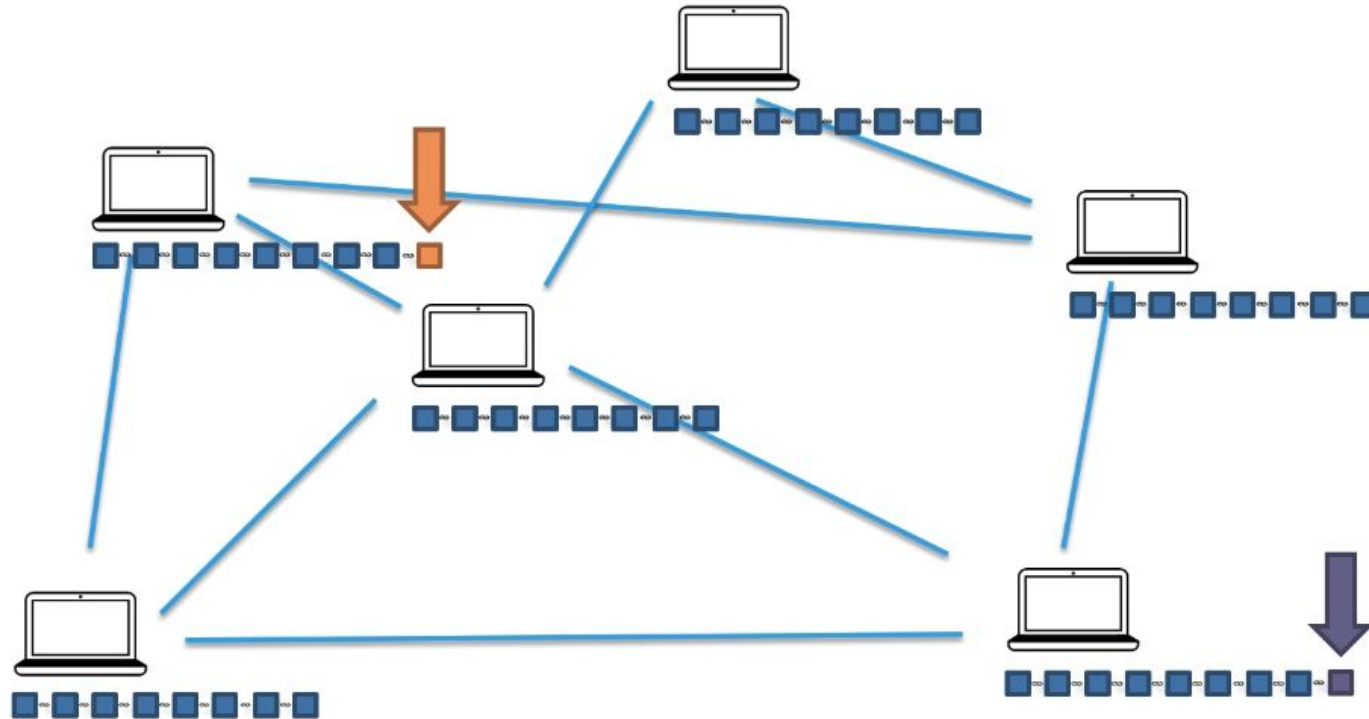
# Consensus protocol



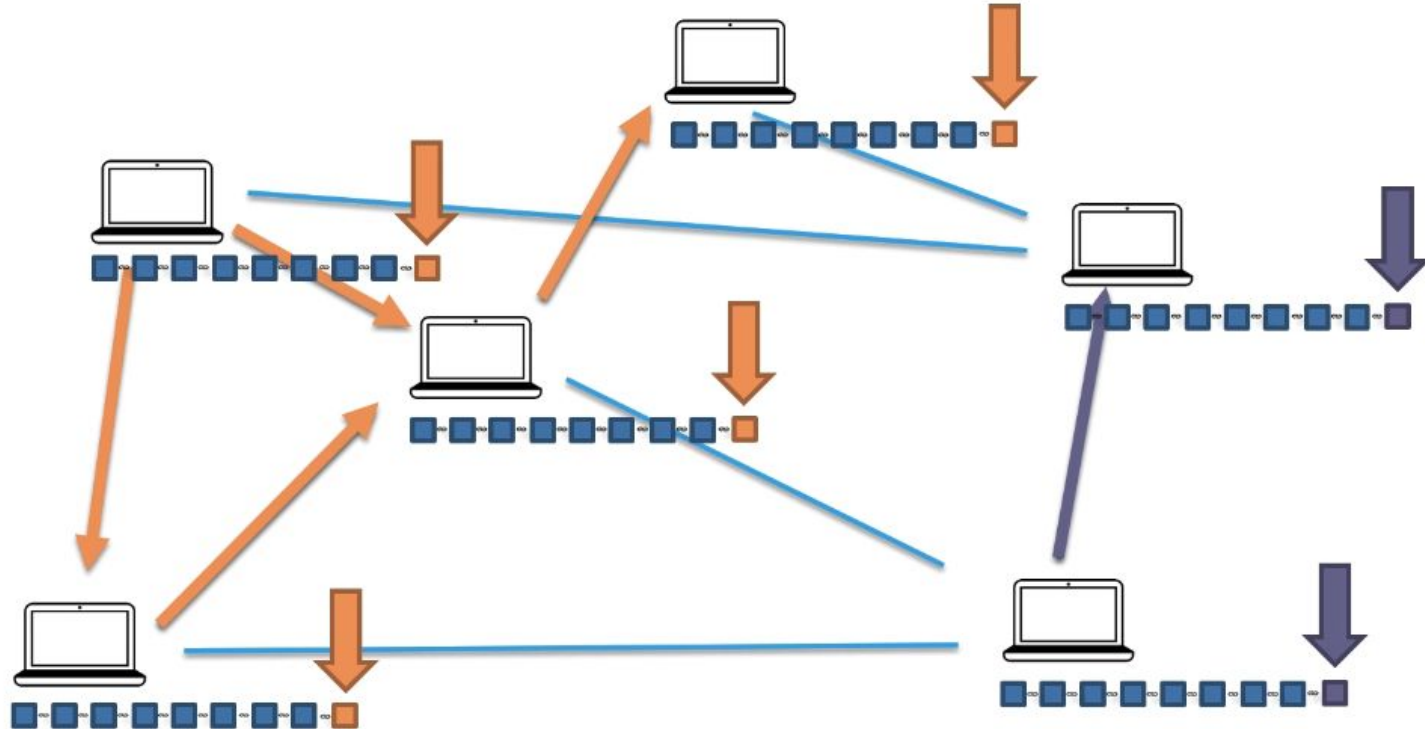
# Series of check



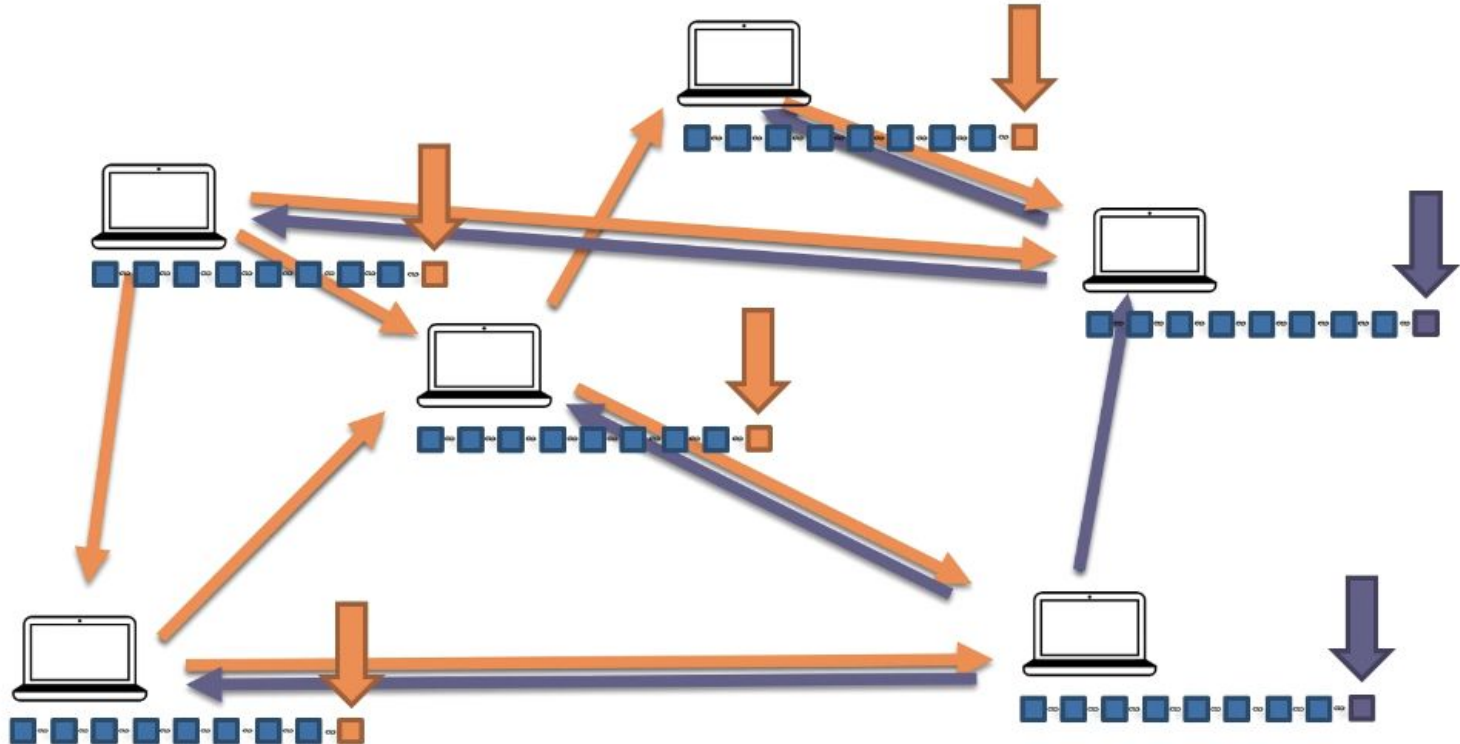
# PoW to avoid fraud



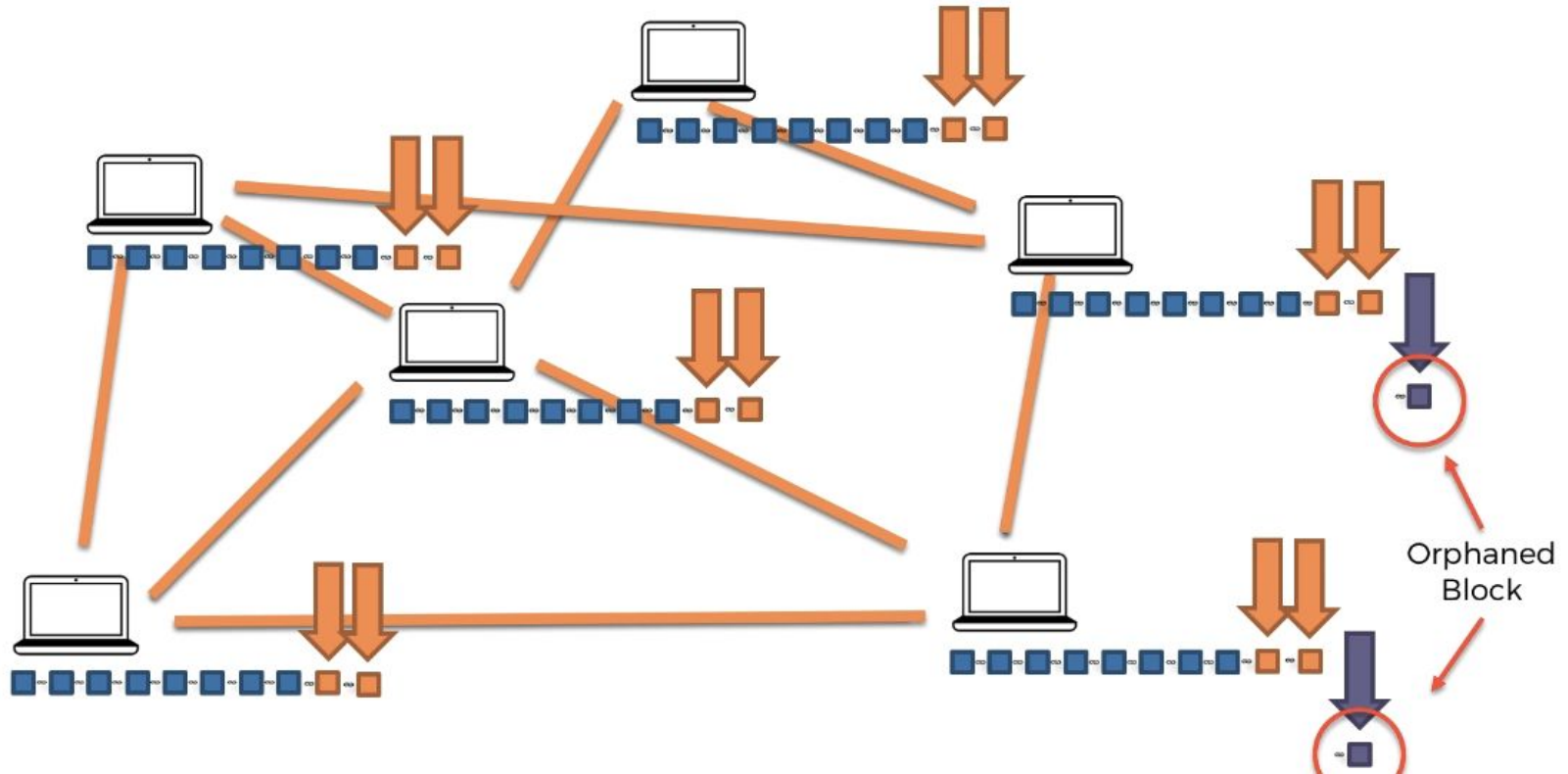
# PoW to avoid fraud



Byzantine Fault Tolerance : Wait to see which chain will be longer



Hashing power will define the longest chain hence the truth





# Blockchain demo !

<https://github.com/anders94/blockchain-demo/>

[https://github.com/sduprey/blockchain\\_introduction/blob/main/blockchain.py](https://github.com/sduprey/blockchain_introduction/blob/main/blockchain.py)

<https://tools.superdatascience.com/blockchain/hash/>

# Technological stack

TECHNOLOGY

Blockchain

PROTOCOL  
/ COIN /

Ethereum

Bitcoin

TOKEN

# Bitcoin Monetary Policy

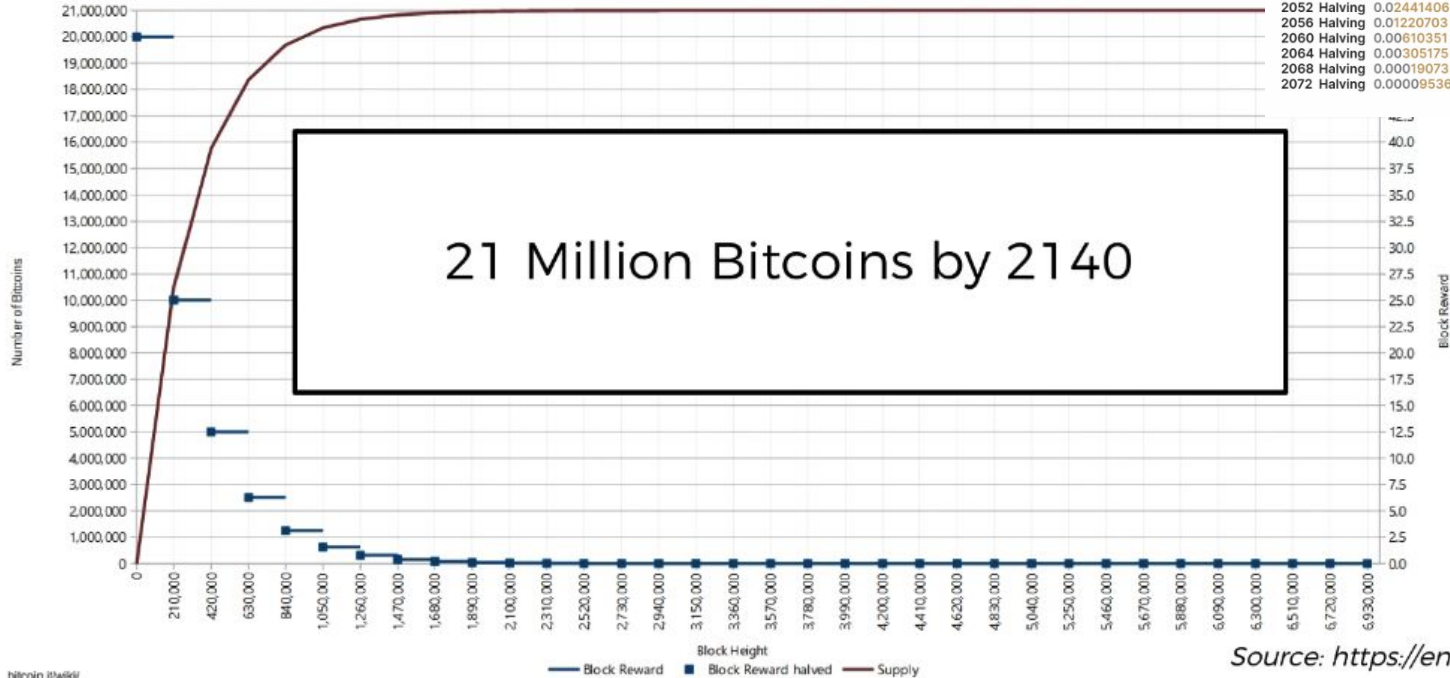
Bitcoin Halving Schedule  
(From Start To 1 Satoshi)

Genesis Block - 2009 - 50 BTC

## The Halving

### Bitcoin - Controlled Supply

Number of bitcoins as a function of Block Height



bitcoin.it/wiki/

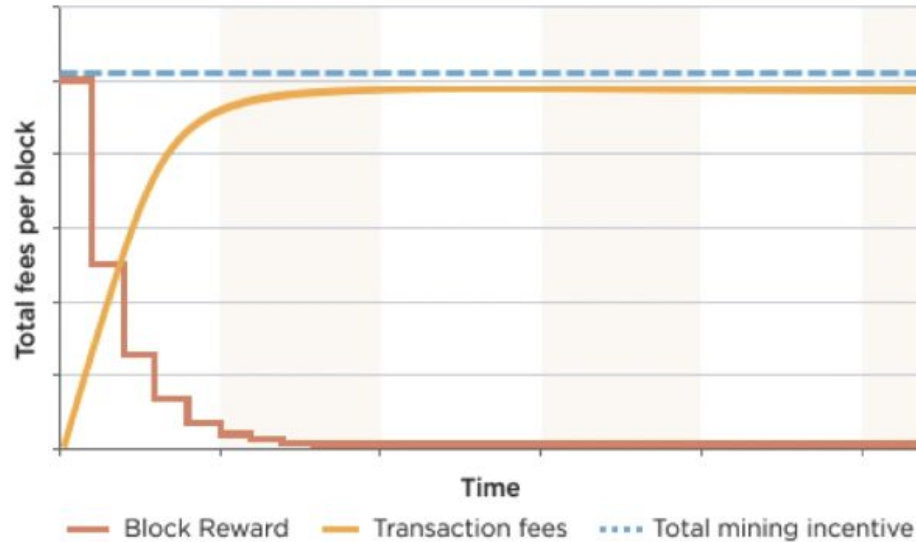
Year	Block Subsidy	Year	Block Subsidy
2012 Halving	25 BTC	2076 Halving	0.00038146 BTC
2016 Halving	12.5 BTC	2080 Halving	0.00019073 BTC
2020 Halving	6.25 BTC	2084 Halving	0.00009536 BTC
2024 Halving	3.125 BTC	2088 Halving	0.00004768 BTC
2028 Halving	1.5625 BTC	2092 Halving	0.00002384 BTC
2032 Halving	0.78125 BTC	2096 Halving	0.00001192 BTC
2036 Halving	0.390625 BTC	2100 Halving	0.00000596 BTC
2040 Halving	0.1953125 BTC	2104 Halving	0.00000298 BTC
2044 Halving	0.09765625 BTC	2108 Halving	0.00000149 BTC
2048 Halving	0.04882812 BTC	2112 Halving	0.00000074 BTC
2052 Halving	0.02441406 BTC	2116 Halving	0.00000037 BTC
2056 Halving	0.01220703 BTC	2120 Halving	0.00000018 BTC
2060 Halving	0.00610351 BTC	2124 Halving	0.00000009 BTC
2064 Halving	0.00305175 BTC	2128 Halving	0.00000004 BTC
2068 Halving	0.00152588 BTC	2132 Halving	0.00000002 BTC
2072 Halving	0.00076294 BTC	2136 Halving	0.00000001 BTC

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

# Bitcoin Monetary Policy

## The Halving

**TRANSACTION FEES ARE MEANT TO  
REPLACE BLOCK REWARDS**



Source: <https://bitsonblocks.net>

# Understanding mining difficulty

[illegible]

Let's do some estimations:

### Probability:

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

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

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

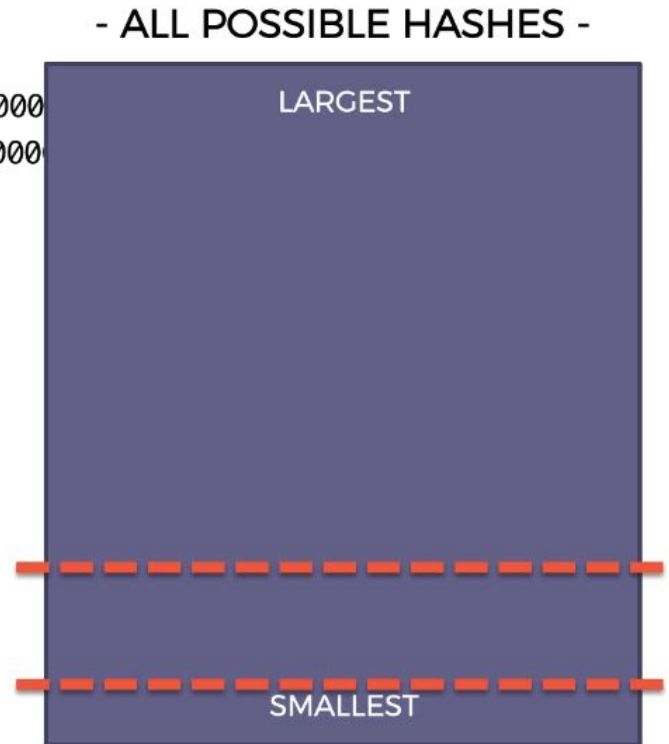
Difficulty is adjusted in regard to hash power to fit the block frequency

$$\text{Difficulty} = \text{current target} / \text{max target}$$

Curr target = 00000000000000000005d97dc00000000000000000000

[illegible]

Difficulty is adjusted every 2016 blocks (2 weeks)



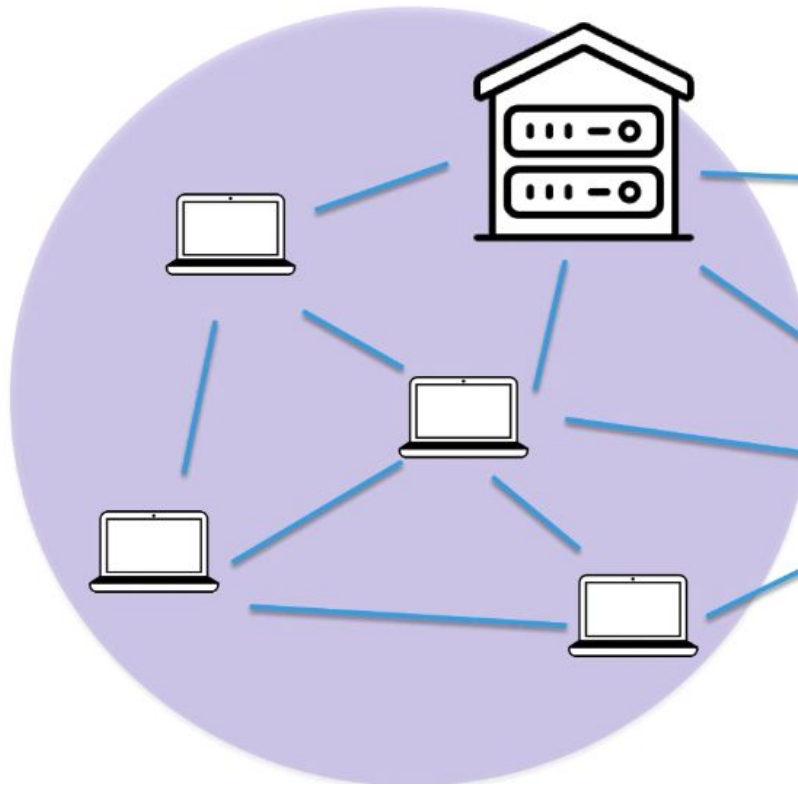
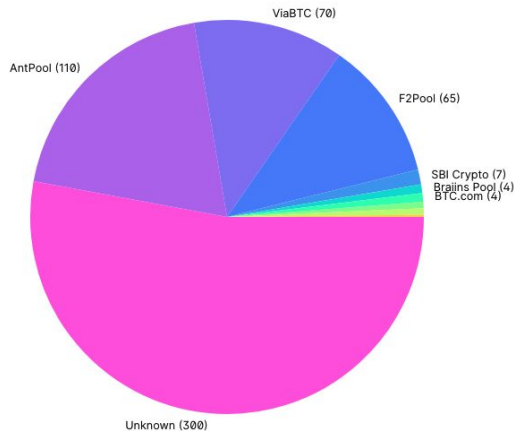
# Mining pool

- Splitting works (nonce range)
- Redistributing rewards pro-rata of hash power brought
- Remove hurdles for investing

## Hashrate Distribution

An estimation of hashrate distribution amongst the largest mining pools.

24H 2D 4D 7D 10D 6M 1Y 2Y 3Y



# Nonce range : is the nonce to brute force our puzzle ?

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:  $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.00000000000000000002\%$

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  $4 \times 10^9$  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



32 bits Nonce : around 4 billions trials

A modest miner does 100 MH/s  
That's 100 Million Hashes

$4 \text{ Billion} / 100 \text{ Million} = 40 \text{ seconds}$

Block: #3
Timestamp: 1519181246
Nonce: 0  4 Billion
Data: Kirill -> Hadelin 500 hadcoins Kirill -> Ebay 100 hadcoins Hadelin -> Joe 70 hadcoins
Prev.Hash: 0000DF2E57FB432A
Hash:



- good for a single miner
- What for a mining pool ?

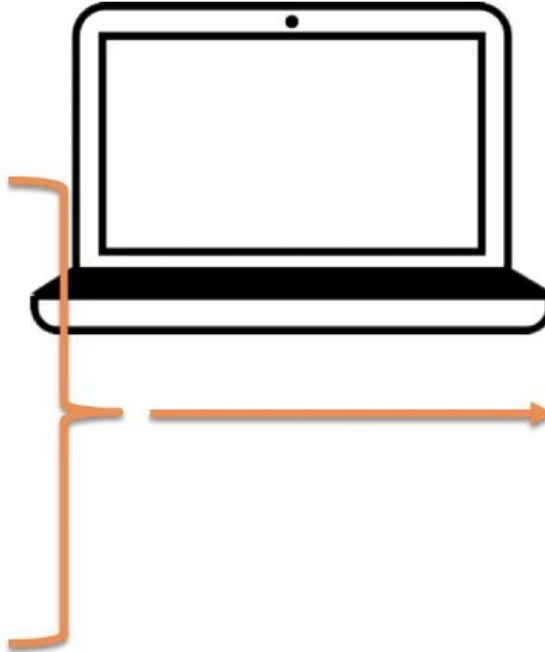
# Blockchain.com explorer

<https://www.blockchain.com/explorer/charts/hash-rate>

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

# Picking 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

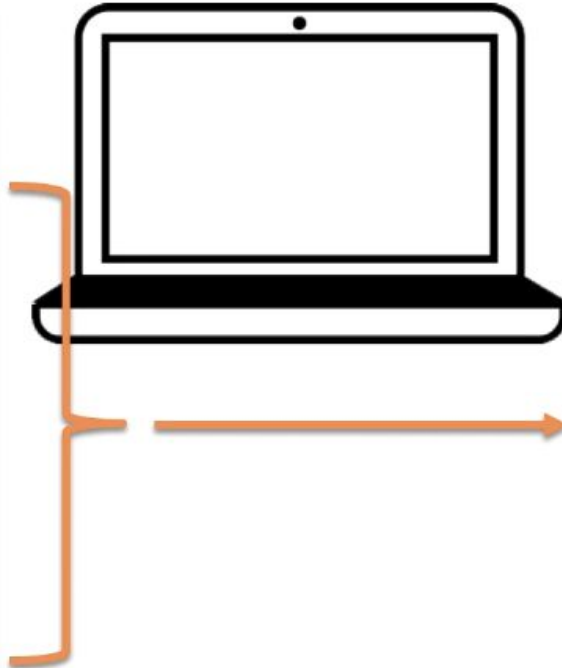


## (Mining in Process)

Block: #500,112
Timestamp: 1519181244
Nonce:
Data:
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:

# Reshuffling transactions to use most of hashing power

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

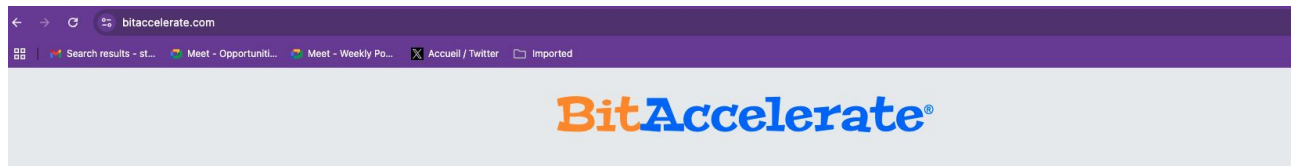


## (Mining in Process)

Block: #500,112
Timestamp: 1519181244
Nonce: 0 <span style="float: right;">4 Billion</span>
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:



# Accelerate your transaction



TXID (Transaction ID) ...

Accelerate

## Free Bitcoin Transaction Accelerator (FAQ)

### What is BitAccelerate, and how does it work?

**BitAccelerate** is a free Bitcoin transaction accelerator that enables faster confirmations for your unconfirmed transactions. It operates by rebroadcasting transactions to **22** popular and highly connected Bitcoin nodes.

Additionally, we provide a [premium acceleration service](#) for most transactions, available for a fee. With this service, transactions receive priority confirmation by the miners. We are partnering with some of the largest mining pools.

### Why is my transaction unconfirmed?

As more people start to use Bitcoin, the block size reaches its limit, leading to a crowded Bitcoin network. Consequently, low-fee transactions are delayed, and sometimes even dropped (purged) from the confirmation queue (mempool).

It often occurs that the network becomes congested immediately after you have sent your transaction, especially when the price of Bitcoin is rapidly rising. In such cases, even if your initial fee was sufficient, it may no longer be adequate due to changed market conditions.

In such situations, you need to take measures to expedite your transaction. You can use a transaction accelerator, [RBF](#) (if the transaction supports it), or [CPFP](#) (if you control any of the transaction's outputs). Otherwise, you may have to wait days, weeks, or even months for the transaction to be confirmed.

### How does transaction rebroadcasting help?

Transaction rebroadcasting aids in the following ways:

- **Rapid propagation of new transactions.** If the transaction carries a lower fee compared to the prevailing market rate, Bitcoin nodes prioritize distributing other transactions with higher fees.

# CPU versus GPU versus ASICs

CPU = Central Processing Unit

## General

 $< 10 \text{ MH/s}$ 

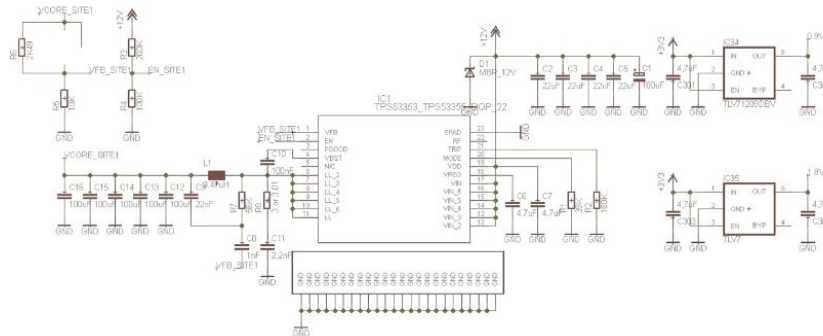
CPU = Central Processing Unit

Specialized

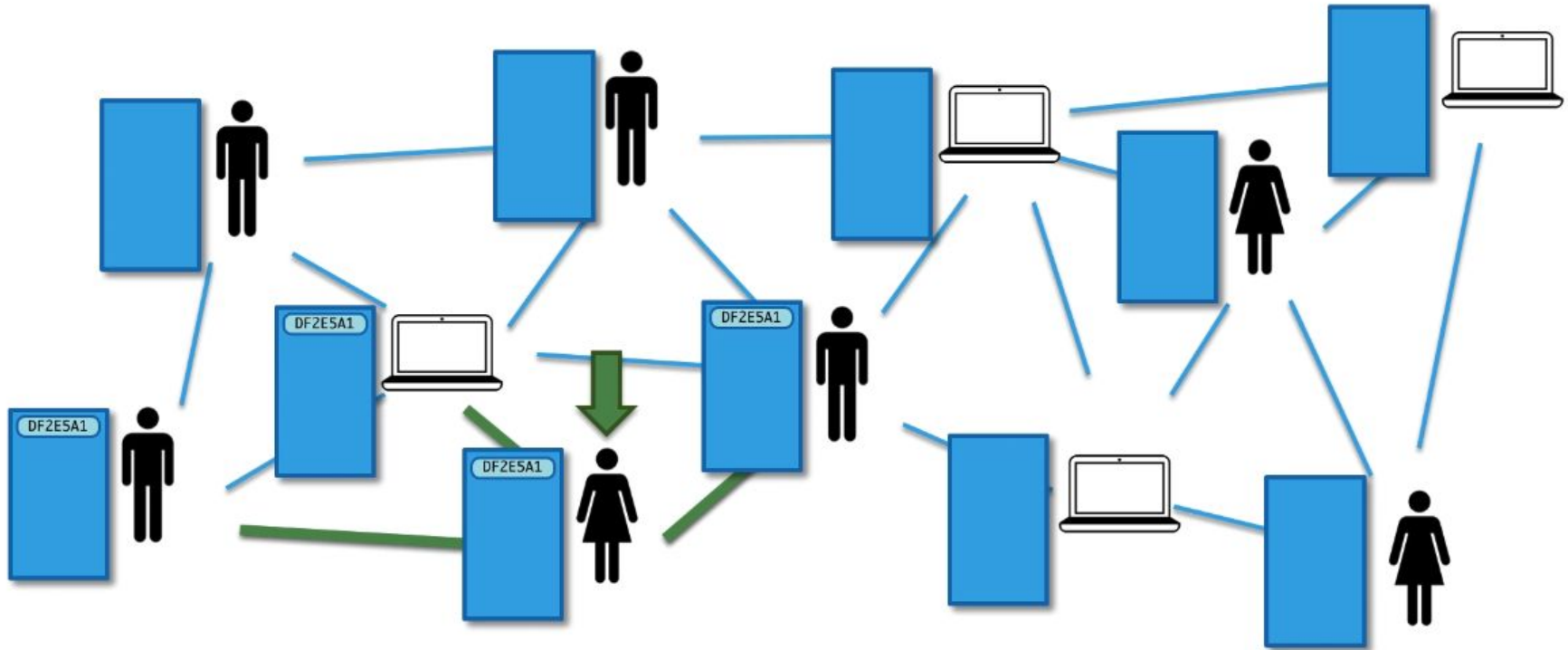
 $< 1 \text{ GHz/s}$ 

ASIC = Application-Specific Integrated Circuit

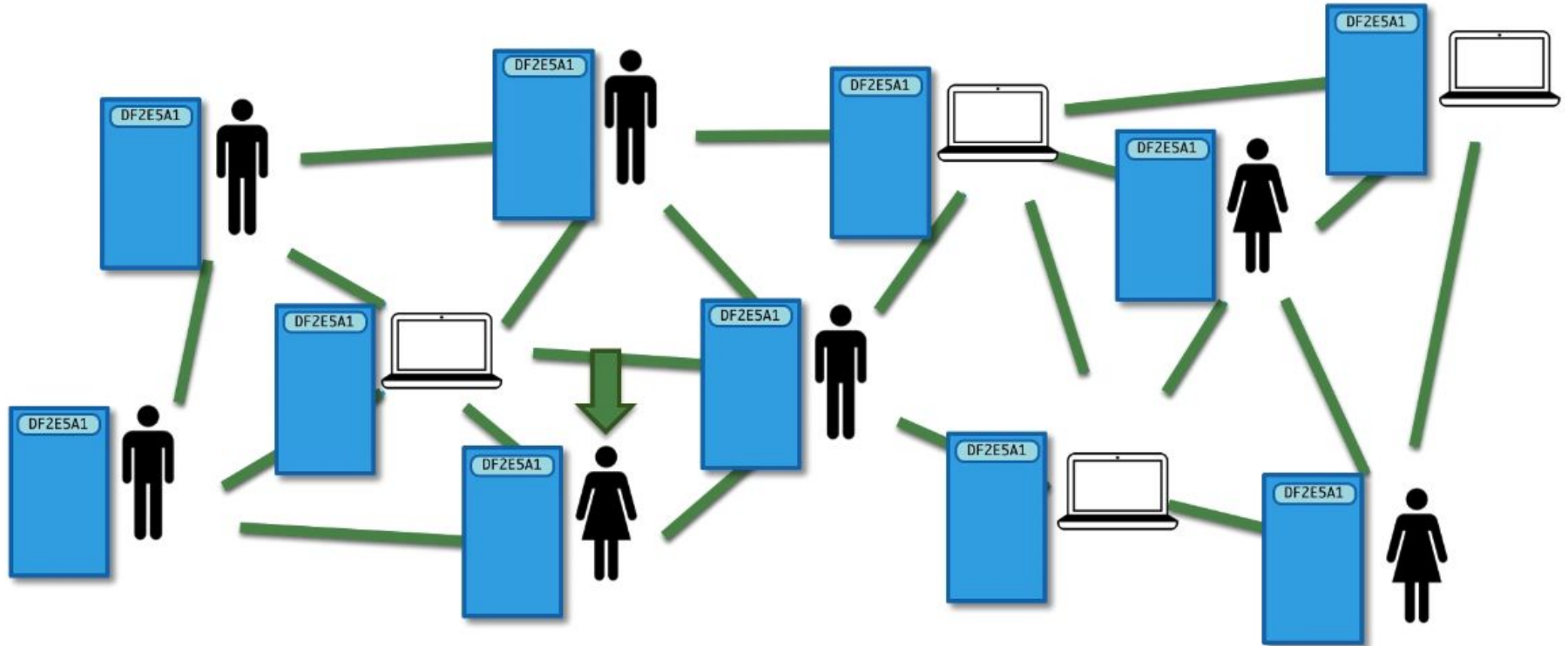
## Totally Specialized

 $> 1,000 \text{ GHz/s}$ 

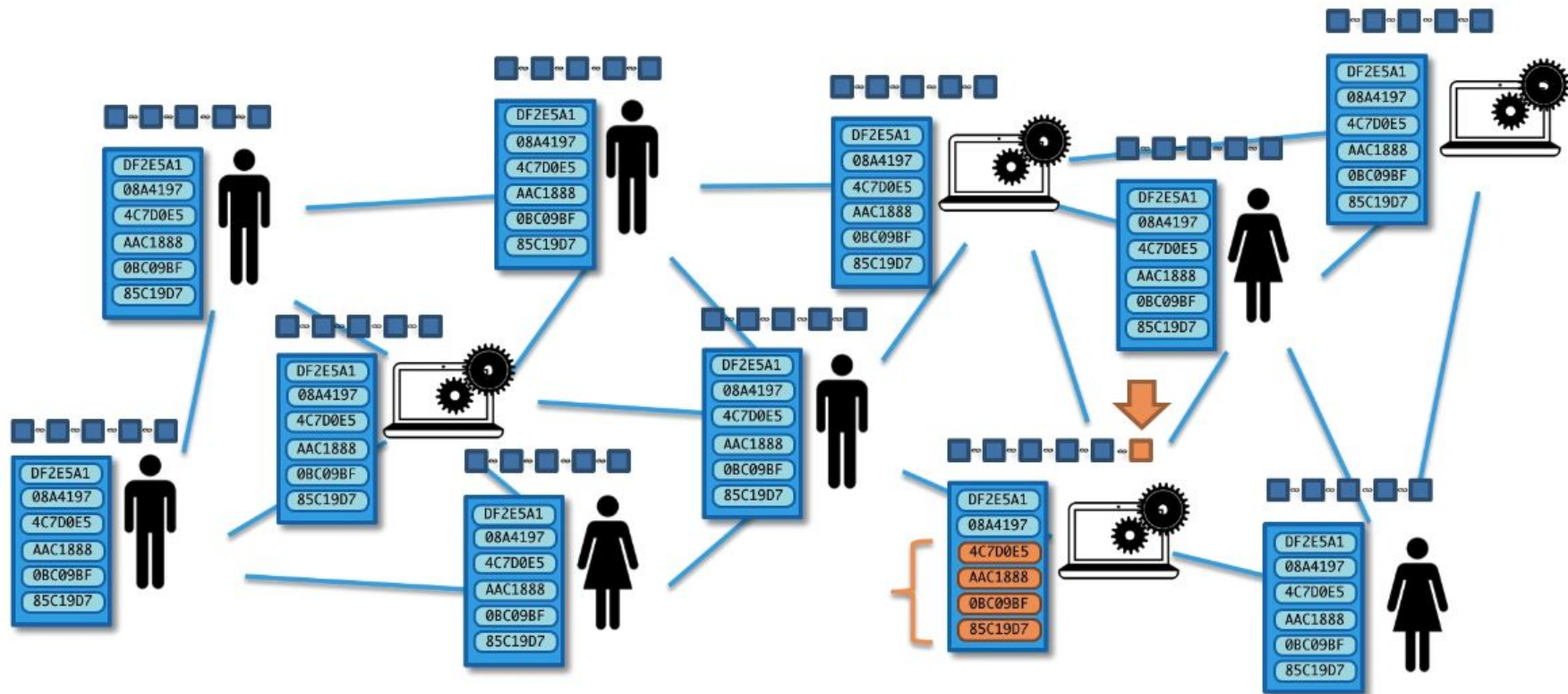
# How do MemPools work ?



# How do MemPools work ?



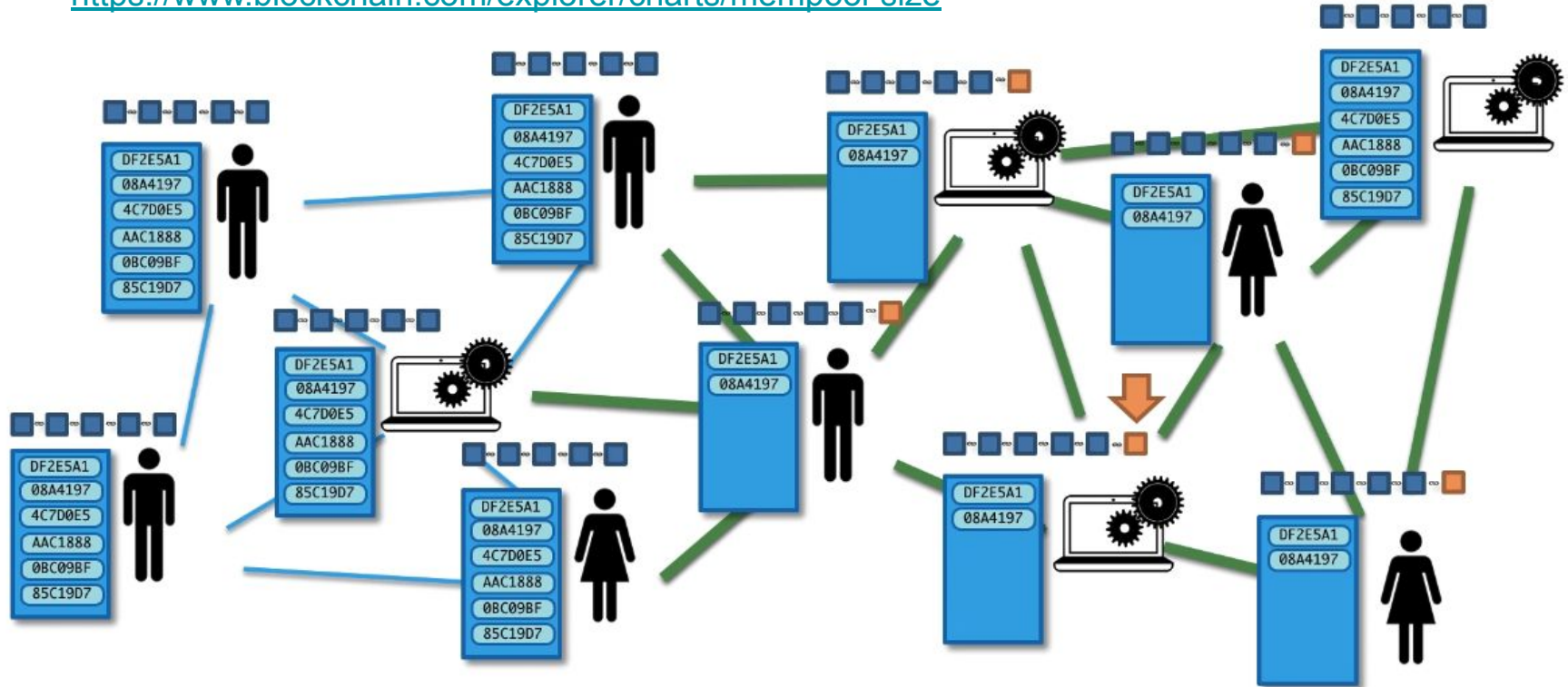




<https://blog.kaiko.com/an-in-depth-guide-into-how-the-mempool-works-c758b781c608>

<https://www.blockchain.com/explorer/charts/avg-block-size>

<https://www.blockchain.com/explorer/charts/mempool-size>



# Orphaned block: part of the experience

## transactions are rereleased into the mempool

Blockchain Luxembourg S.A.R.L [LU] | https://blockchain.info/orphaned-blocks?offset=0



BLOCKCHAINWALLETDATAAPIABOUT

Q BLOCK, HASH, TRANSACTION, ETC...

## Orphaned Blocks

Detached or Orphaned blocks are valid blocks which are not part of the main chain. They can occur naturally when two miners produce blocks at similar times or they can be caused by an attacker (with enough hashing power) attempting to reverse transactions.

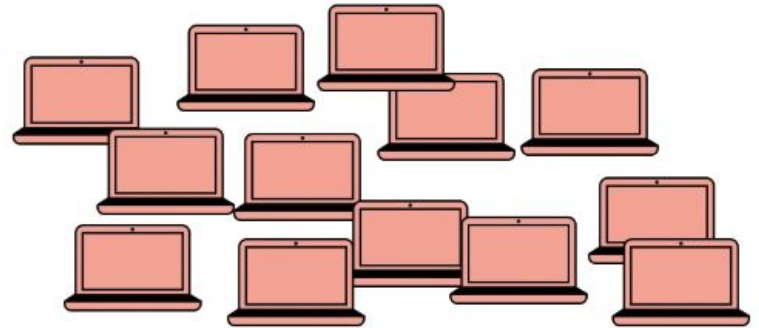
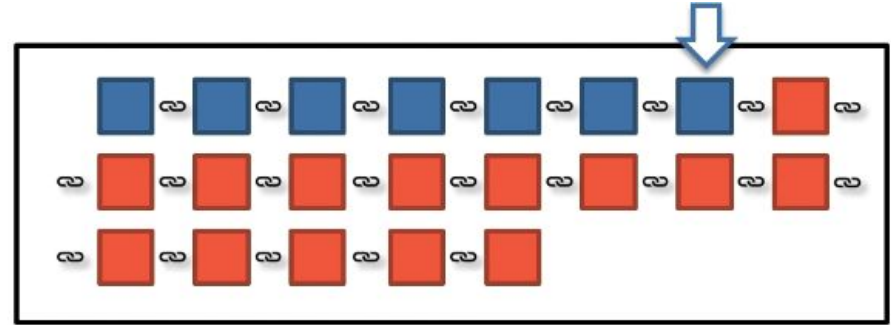
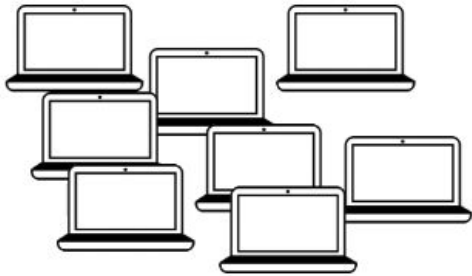
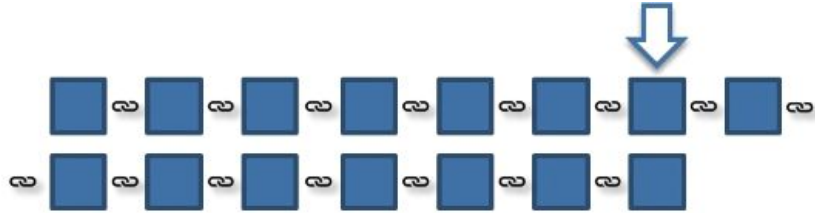
[Next Page >>](#)

		
Timestamp	2018-01-12 23:28:07	Timestamp 2018-01-12 23:28:33
Number Of Transactions	2991	Number Of Transactions 2874
Relayed By	GBMiners	Relayed By SlushPool

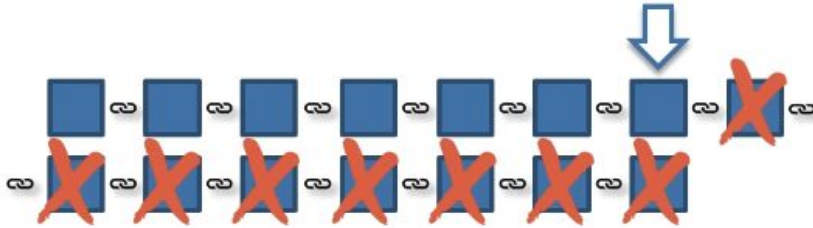
503949

That is why we wait a few blocks to be sure the transaction is confirmed !

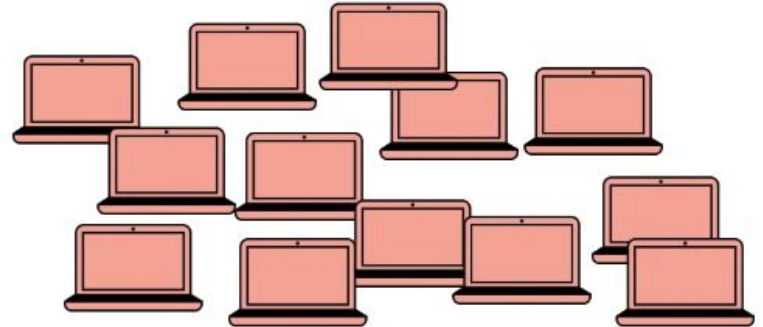
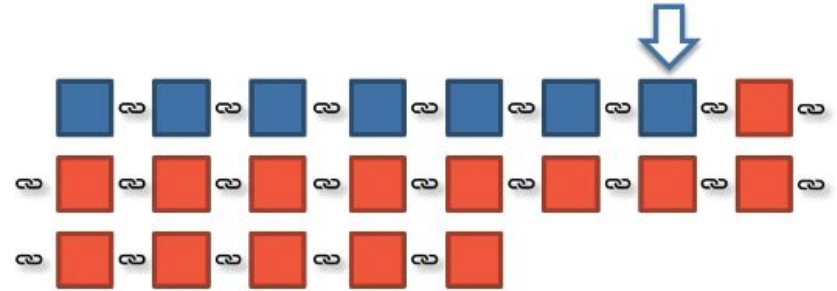
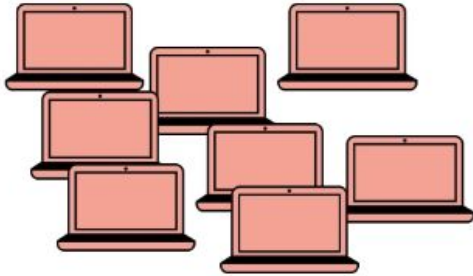
# The 51% attack



# The 51% attack



Double spent occurring!



# Deriving the current target

Difficulty = current target / max target

Curr target = 0000000000000000005d97dc000

Max target = 00000000FFFF000

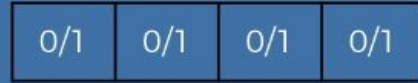
Where is the current target stored?

Bits -> Hex -> Derive target

Bits: 392009692

Bits in Hex: 175D97DC

$$16 \times 1 + 7 \\ = 23$$



23 bytes = 23 x 8 bits  
= 23 x 2 x 4 bits  
= 23 x 2 x Hex Digits

23x2 = 46 Hex Digits

000000000000000000005D97DC000

Add missing zeros  
(64-46 = 18)

# Transactions and UTXOs

Mark	->	Me	0.1 BTC	} UTXOs
Hadelin	->	Me	0.3 BTC	
<del>Helen</del>	<del>-&gt;</del>	<del>Me</del>	<del>0.6 BTC</del>	
Susan	->	Me	0.7 BTC	

I want to Buy a bicycle for 0.5 BTC

TRANSACTION:

Input:

0.6 BTC from Helen

Output:

0.5 BTC to the bike shop,  
0.1 BTC back to myself

UTXO  
For the bike shop

UTXO  
For me



UTXOs





# Multiple outputs & Fees

Mark	->	Me	0.1 BTC
Sarah	->	Me	0.1 BTC
<del>Hadelin</del>	<del>-&gt;</del>	<del>Me</del>	<del>0.4 BTC</del>
<del>Ebay</del>	<del>-&gt;</del>	<del>Me</del>	<del>0.3 BTC</del>
<del>Hadelin</del>	<del>-&gt;</del>	<del>Me</del>	<del>0.3 BTC</del>

} UTXOs

I want to Buy a 3<sup>rd</sup> bicycle for 0.9 BTC and an apple for 0.02 BTC

TRANSACTION:

Input:

0.4 BTC from Hadelin,  
0.3 BTC from Ebay  
0.3 BTC from Hadelin

Output:

0.9 BTC to the bike shop,  
0.02 BTC to the fruit shop,  
0.06 BTC to myself

Fees: 0.02 BTC

UTXO for the bike shop

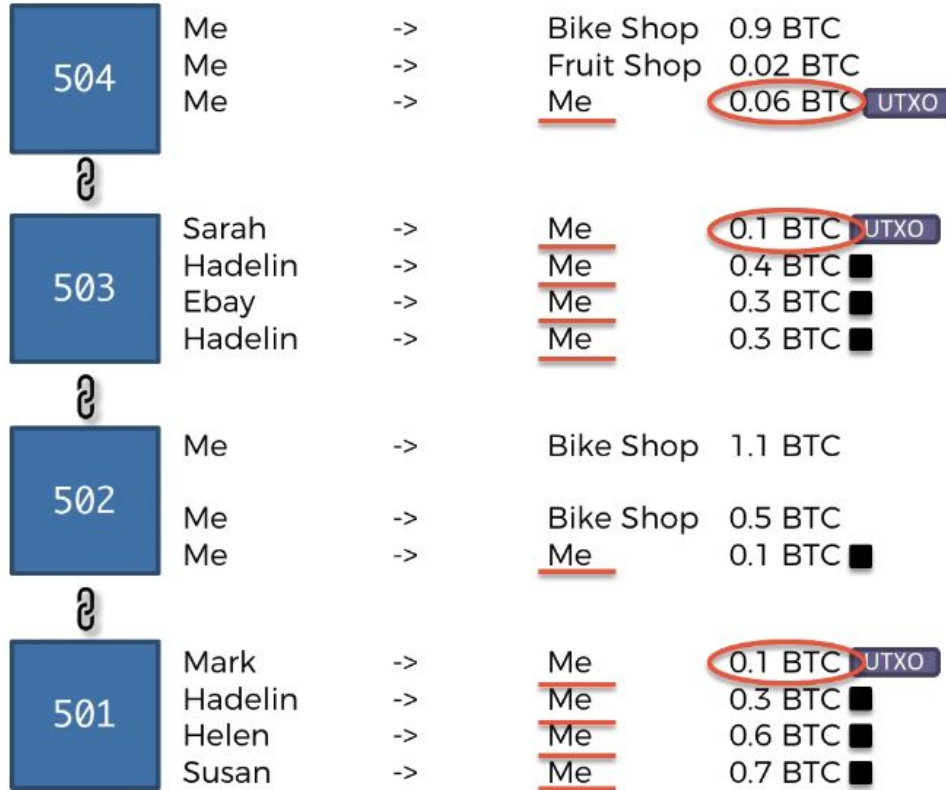
UTXO for the bike shop

UTXO for me

UTXO for the miner



# How wallets work ?



# Private & Public Keys

Privacy

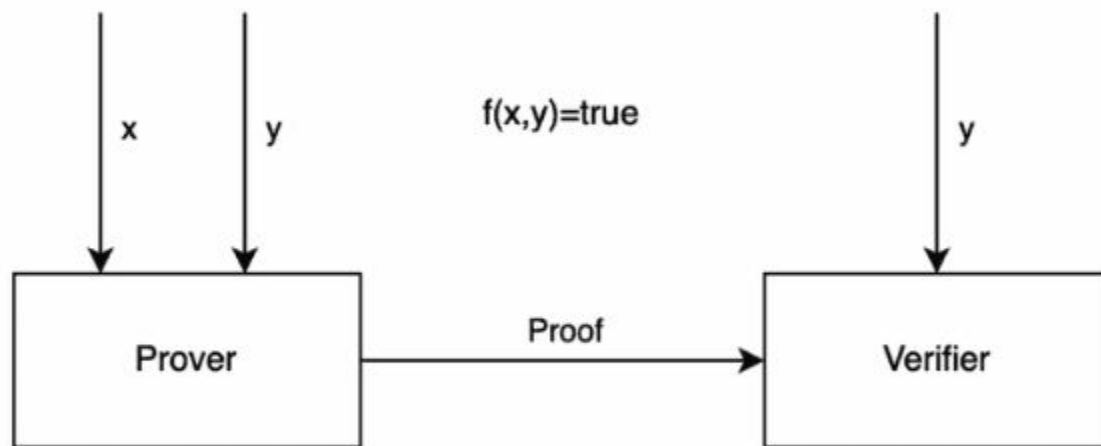
Ownership







# ZK SNARK explained



<https://github.com/Magnum35puc/VanityAddressGenerator>

Samouraïe wallet

Cash mixer : Tornado cash

Defi