

## Notes Content:

- 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)
- CPU vs GPU vs ASICs
- How do Mempools work?
- Orphaned Blocks
- 51% attack
- Extra: Bit to Target conversion

What is Bitcoin?

There are three main layers in the crypto world

1. Technology
  - a. Blockchain
2. Protocol / Coin
  - a. Bitcoin
3. Token

Protocol: Is a set of rules that guides how participants over network communicate with each other

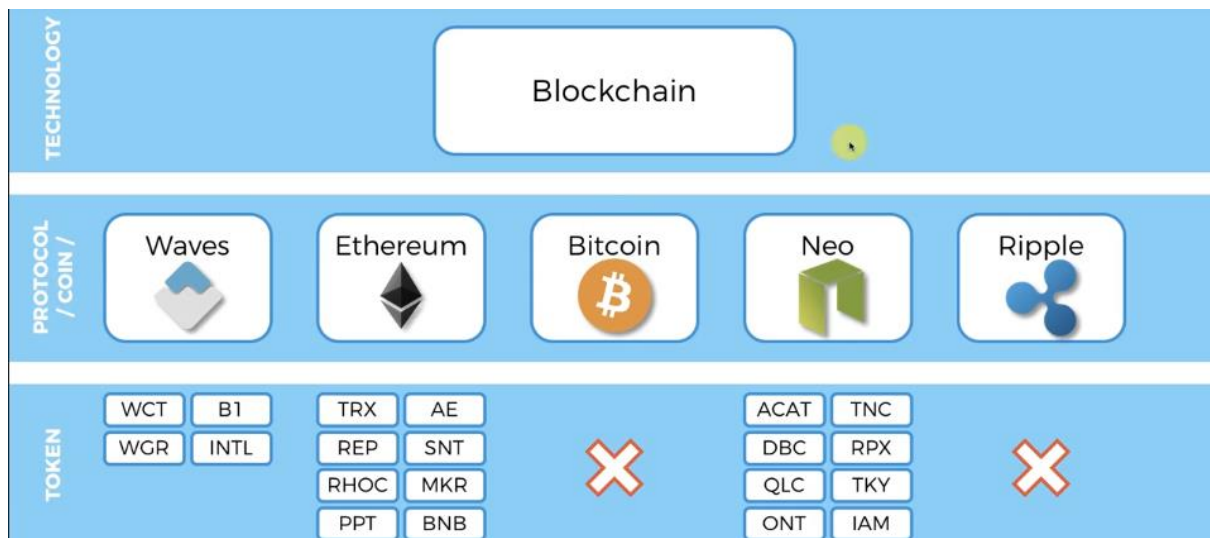
Ex. TCP, IP, SMTP, POP3, Bitcoin

The Bitcoin Protocol is

- how participant come to consensus, how public keys and signatures is used for authentication.
- Other Protocol: Ethereum, Ripple, Neo, Waves
- All protocol relies of blockchain technology
  
- The protocol contains within them an important feature i.e. coins
- The coin is an init asset which facilitates the interaction of players which is used to reward people, add blocks and purchase things from each other.

Token:

- Will be discussed later...

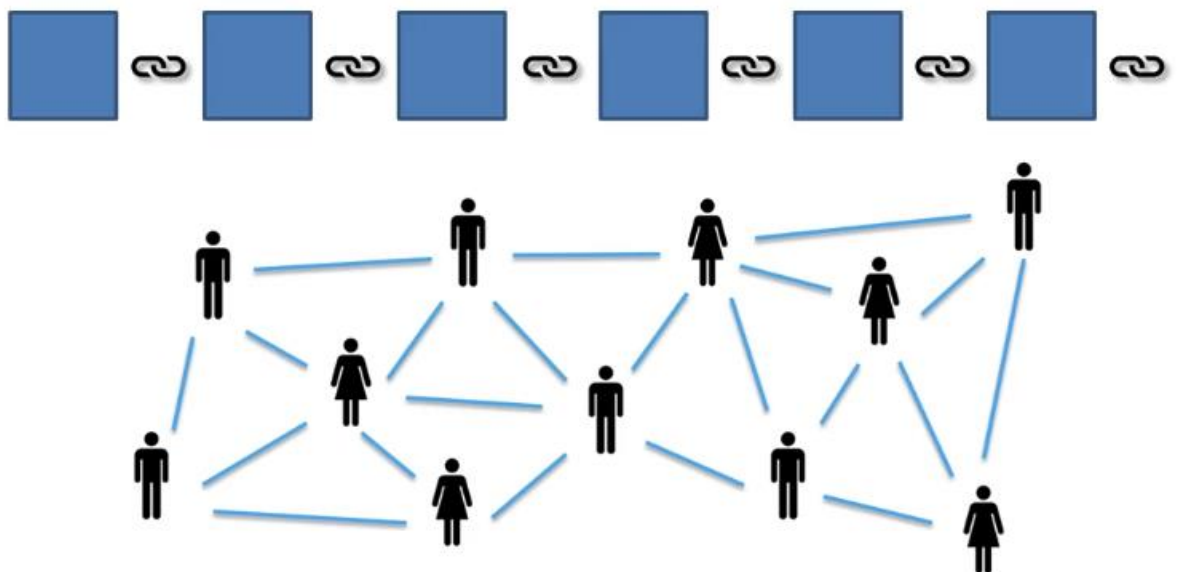


<http://coinmarketcap.com>

## Bitcoin

Bitcoin was invented by a person Satoshi Nakamoto.

Taking the blockchain technology and making it to practice. From this technology there will be no intermediaries between people transacting. The layer 2 is about creating a Protocol of how people transact. There will be no banking system.



## Bitcoin Ecosystem

- Nodes



- Large Mines



- Miners



- Mining Pools



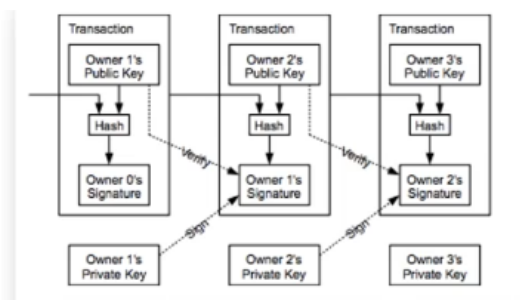
## Additional Reading

*Bitcoin: A Peer-to-Peer Electronic Cash System*

By Satoshi Nakamoto (2008)

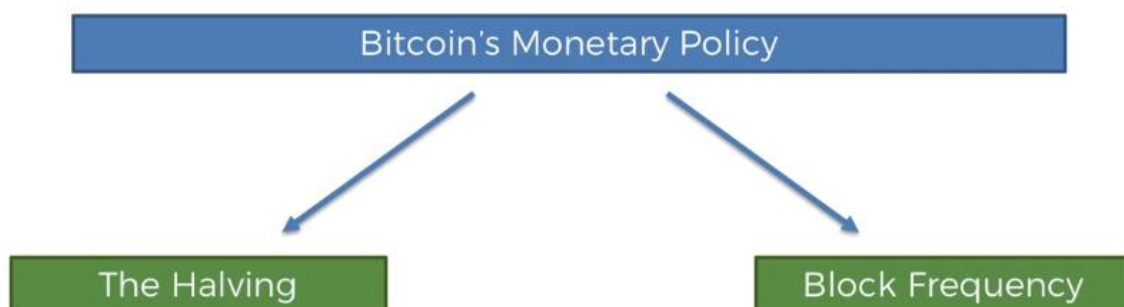
Link:

<https://bitcoin.org/bitcoin.pdf>



## Video 2

### Bitcoin Monetary Policy



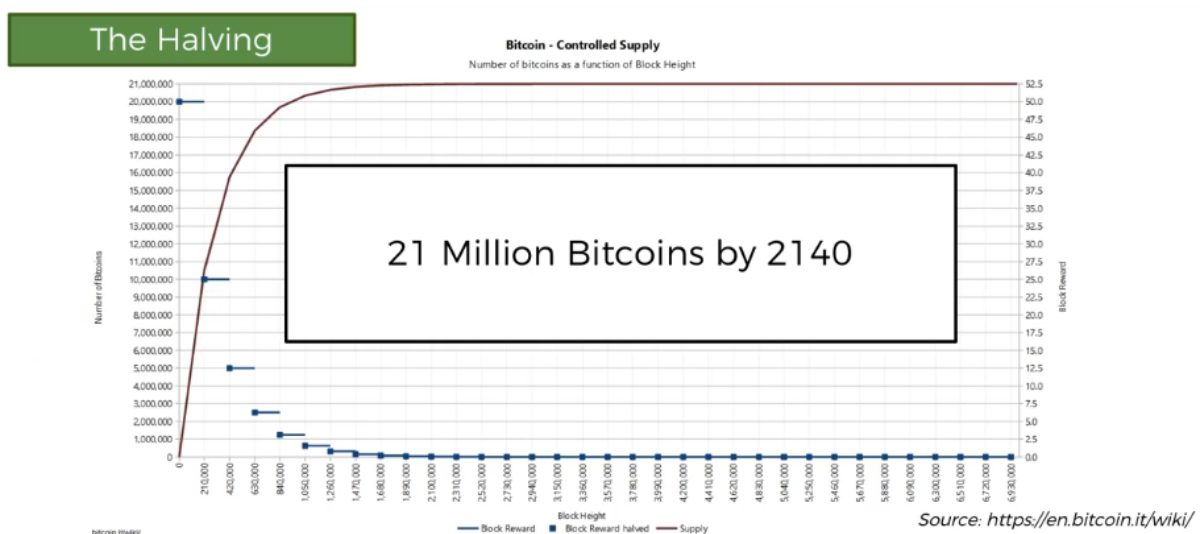
## The Halving

With every block mined, bitcoins are released as a reward to the miner. The halving principle says that the number of bitcoin released into the system will be halved every 210k (4 years) blocks mined.

For Example: First 210k blocks mined released a total of 50 Bitcoins, then from there to 420k blocks mined the number of bitcoins released will be 25 bitcoins.

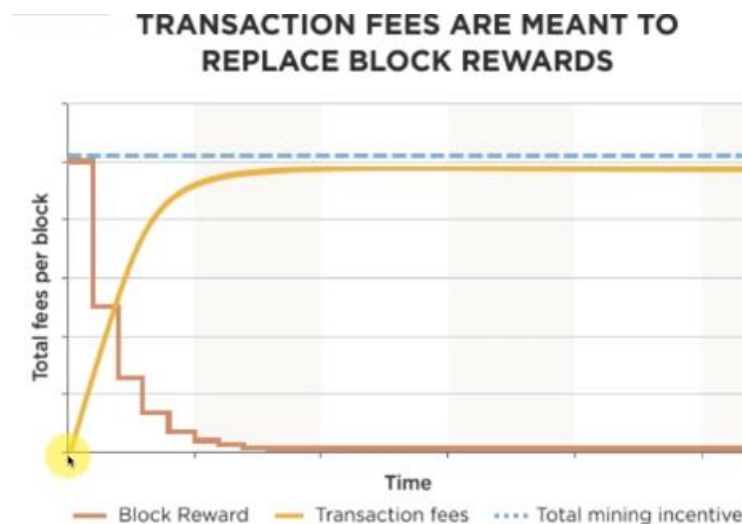
Date reached	Block	Reward Era	BTC/block
2009-01-03	0	1	50.00
2010-04-22	52500	1	50.00
2011-01-28	105000	1	50.00
2011-12-14	157500	1	50.00
2012-11-28	210000	2	25.00
2013-10-09	262500	2	25.00
2014-08-11	315000	2	25.00
2015-07-29	367500	2	25.00
2016-07-09	420000	3	12.50
2017-06-23	472500	3	12.50

This system is not controlled by any organization and is programmed in the bitcoin system



The total number of bitcoins released will be 21 million Bitcoin by 2140





If miners will get less and less reward each time after some time, they will not be able to mine blocks. But as the number of bitcoin to be released in the market is going down, **the transaction fees** which the Nodes pay to miners to mine their transaction is going high. So the system balances in this way.



Bitcoin is a deflationary type of currency.

## Block Frequency

How often new blocks are mined or how much time it takes to mine one block is the block frequency. The frequency given below and varies according to the type of coin

Cryptocurrency	Average block time
 <b>bitcoin</b>	10 min
 <b>ethereum</b>	15 sec
 <b>ripple</b>	3.5 sec
 <b>litecoin</b>	2.5 min

Transaction time of transaction:

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

### Additional Reading:

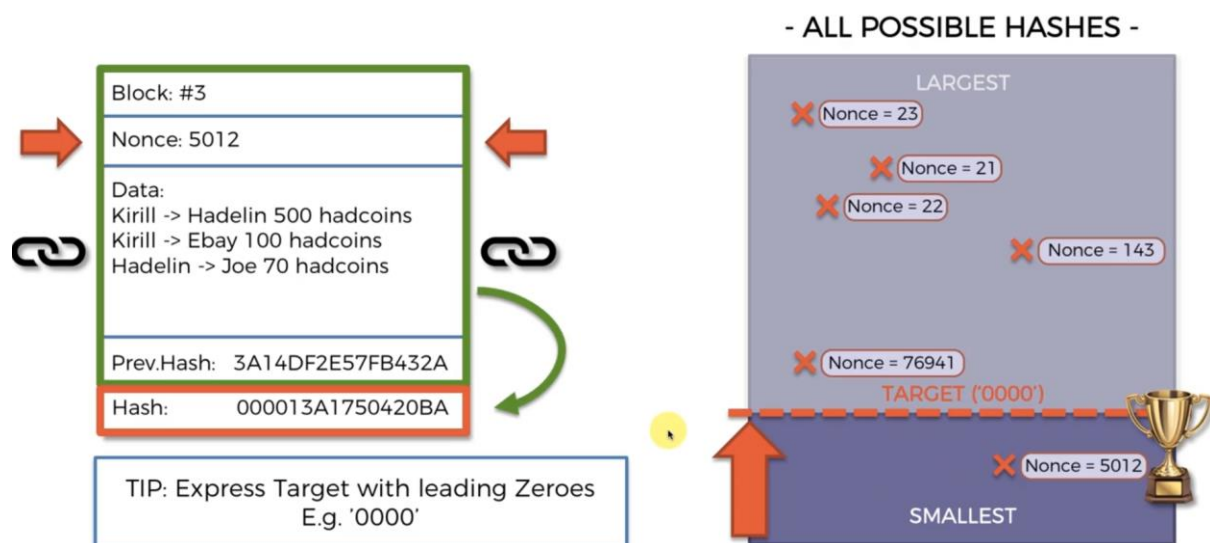
<https://hackernoon.com/this-time-is-different-part-2-what-bitcoin-really-is-ae58c69b3bf0>

### Video 3

### Understanding Mining Difficulty

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

### Current Target Intuition



We used the above diagram in module 1 notes to show what is the target that miners have to achieve to mine the block. But on a practical note, the target shown in the diagram is very disproportionate when compared to its value.

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



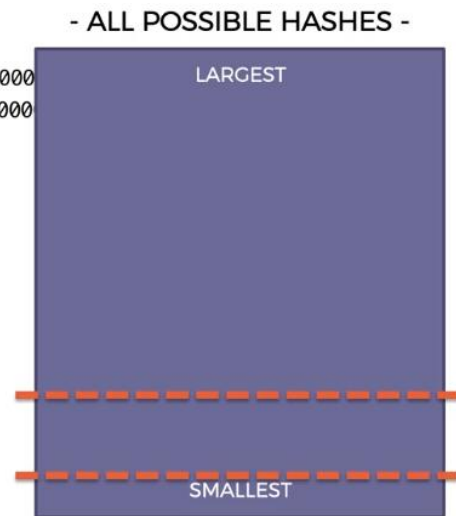
## How is Mining difficulty calculated?

Difficulty = current target / max target

Curr target = 00000000000000000005d97dc000000000000000000000000

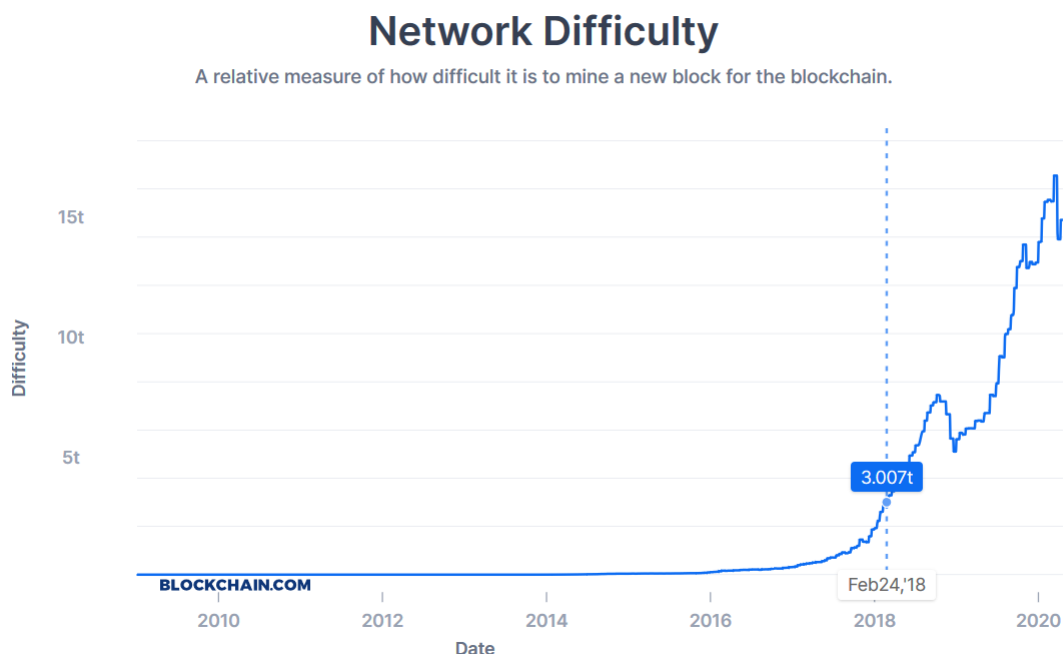
Max target = 00000000FFFF000000000000000000000000000000000000

Difficulty is adjusted every 2016 blocks (2 weeks)



The max target starts with 00000...FFF...000000 because if it would have started from FFFF...FFF... then each hash will be a golden hash. So this number is predefined from the beginning to keep the mining a challenge.

## Mining difficulty chart



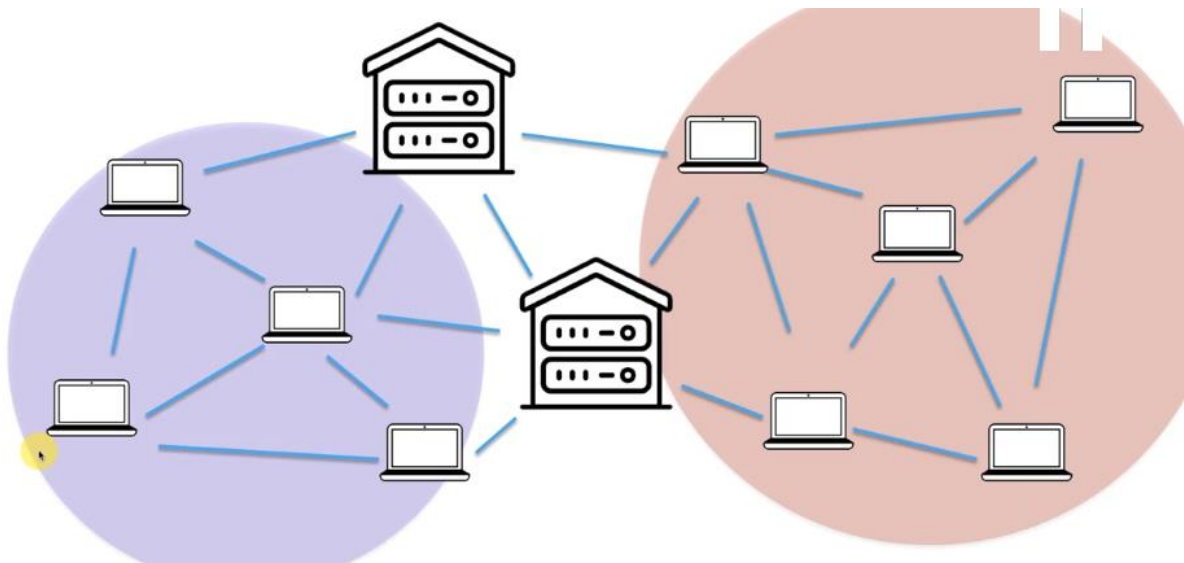
Right now the value is 14 trillion times difficult compared to when it was in the start.

## Virtual Tour of a Bitcoin Mine

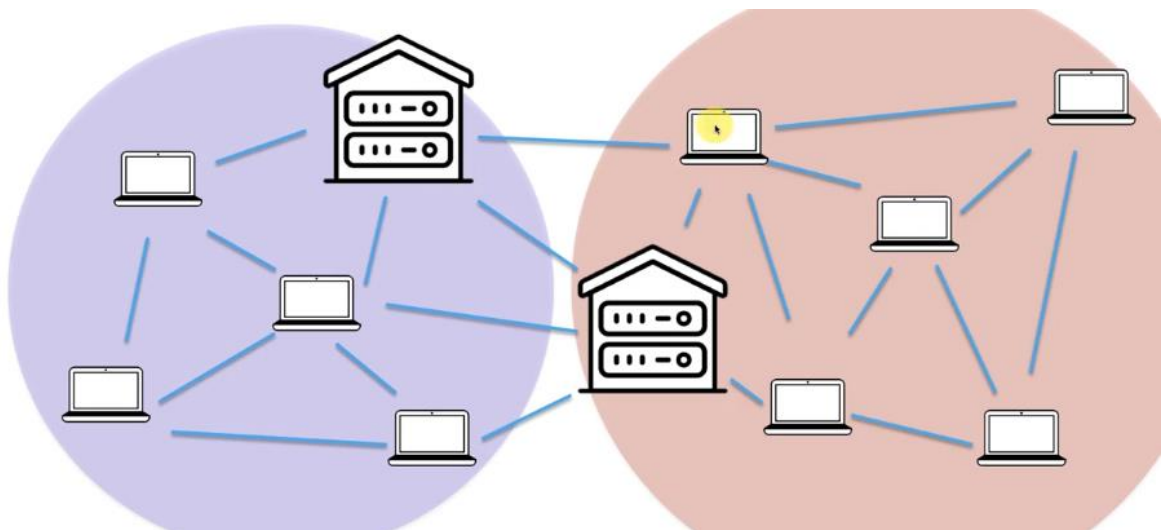
<https://qz.com/1055126/photos-china-has-one-of-worlds-largest-bitcoin-mines/>

### Video 5

#### Mining Pools



- Individual miners make groups and form mining pool.
- The cryptographic puzzle is solved by everybody by avoiding the problem of double work
- If the block is mined, the money is distributed among them according to hashing power



# Mining Rig

Hi! Sign in or register

Daily Deals

Gift Cards

Help & Contact

Turn Your Tax Refund Into Fun

Sell | My 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

★★★★★ 2 product ratings | About this product

9 viewed per hour



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

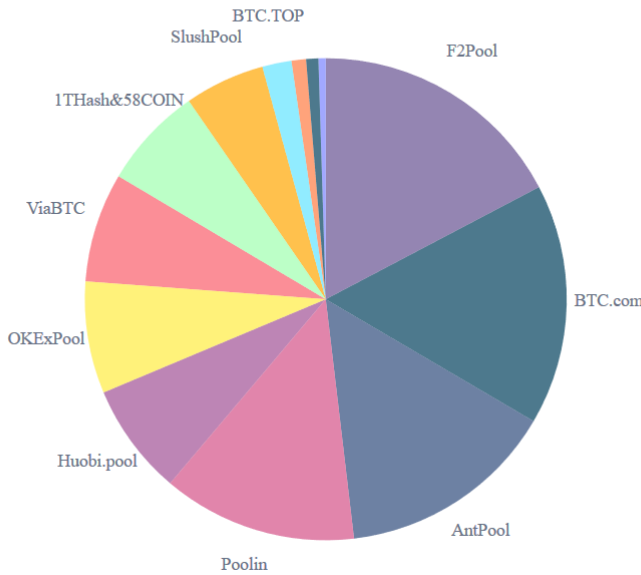
Sold by partdiscounter (42407) 99.8% Positive feedback

## Mining Pool Information:

<https://www.blockchain.com/pools>

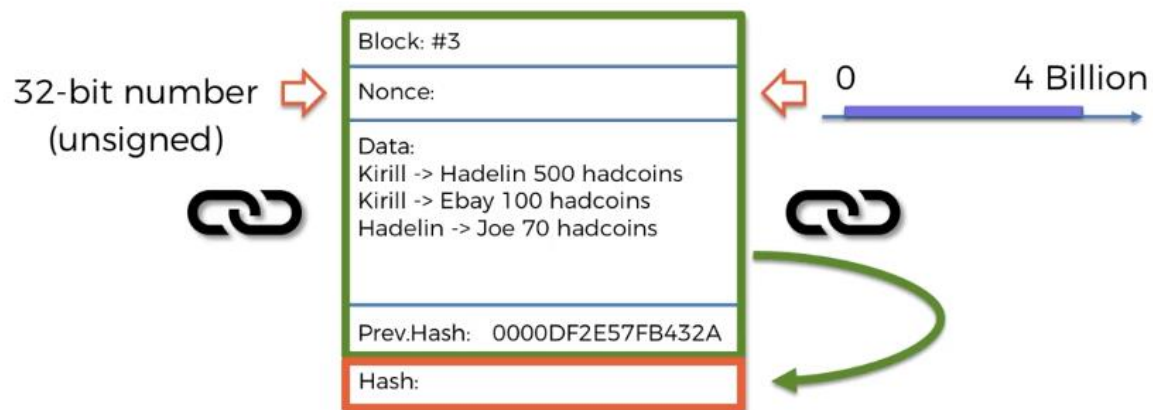
## Hashrate Distribution

An estimation of hashrate distribution amongst the largest mining pools.



## The Nonce and its range

Nonce is a field in a block which allows miners to participate in the cryptographic puzzle challenge. Miners cannot change any of the other fields and change only the nonce to generate a new hash.



As they keep changing the nonce to get the golden hash. Once a golden hash is encountered the block is mined and the miner gets a reward.

The Nonce field is a 32-bit in size i.e. 4 billion 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:  $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.00000000000000000002\%$

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

For Example:

A modest miner has a hashing power of 100 MH/s i.e. 100 Million Hashes. The nonce range is 4 billion.

So,  $4 \text{ billion} / 100 \text{ million} = 40 \text{ seconds}$

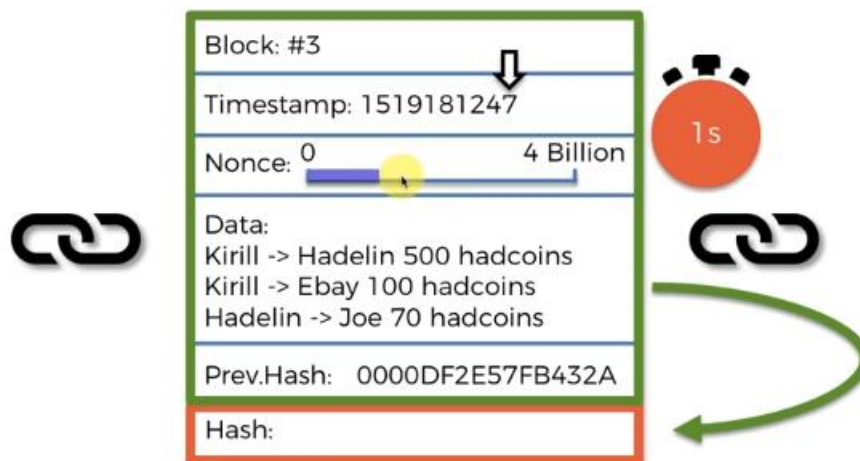
A miner with modest hashing power can mine a block in 40 seconds. Then why it takes 10 mins each time to solve the hashing algorithm in practical.

In reality there is an extra field in the block called **Timestamp**.

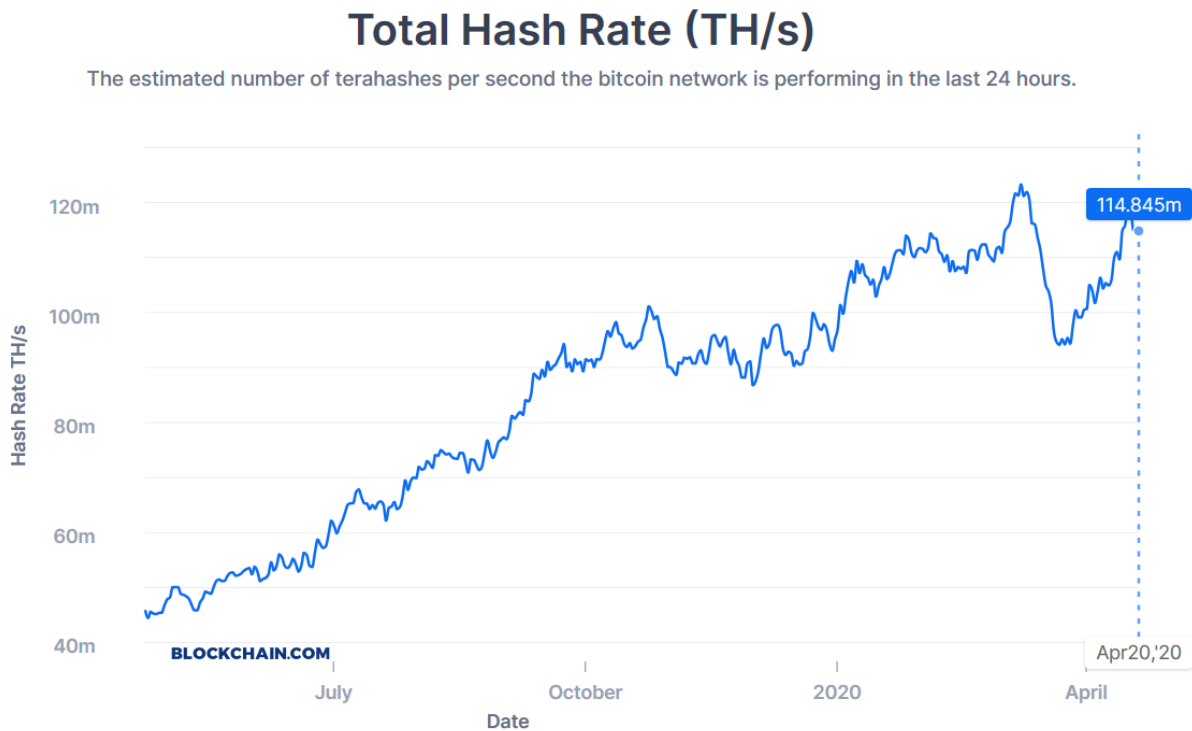
Unix time used in the timestamp field.

Now every second the information in the block is going to be updated due to the timestamp field.

So we have only one second to go through the complete nonce range. Because from the next second the timestamp field changes and there will be a different hash on each nonce.

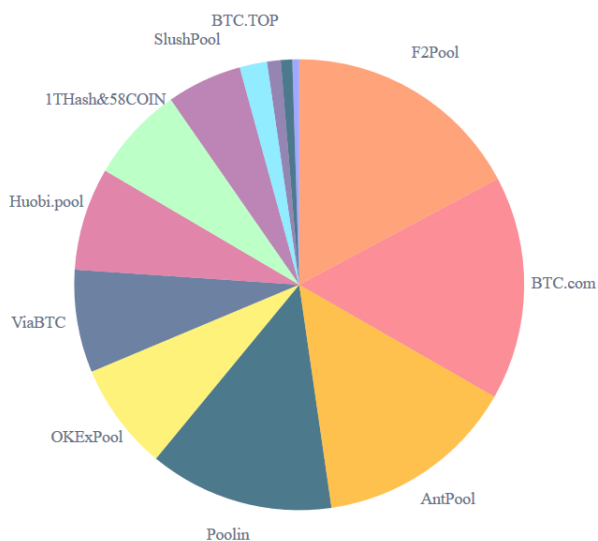


Below is the chart of miners hashing power



Current total hash rate is 114.8 million trillion hashes / second

The hash rate distribution chart below conveys that some miners like BTC.com covers at least 10% of the total hash rate (rough approx)



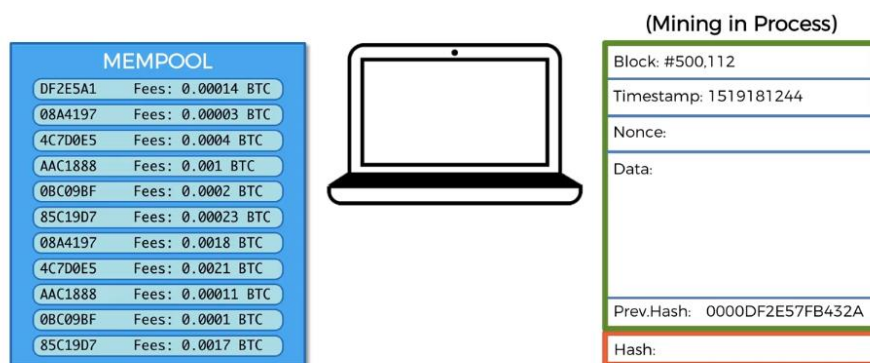
10% of 114 million trillion is 11.4 million trillion hashes per second.  
This number is so huge that these miners will check the complete

nonce range in fraction of seconds. This generates a difficulty for the miner as they have to wait for the next second to come and they start checking again with a different timestamp. The concept is solved later in the notes.

## How Miners Pick Transactions

Every miner has a Mempool attached to it from which miner pick up transaction and fill them in the block and start mining

### Mempool



Fees are added by the one who is doing the transaction.

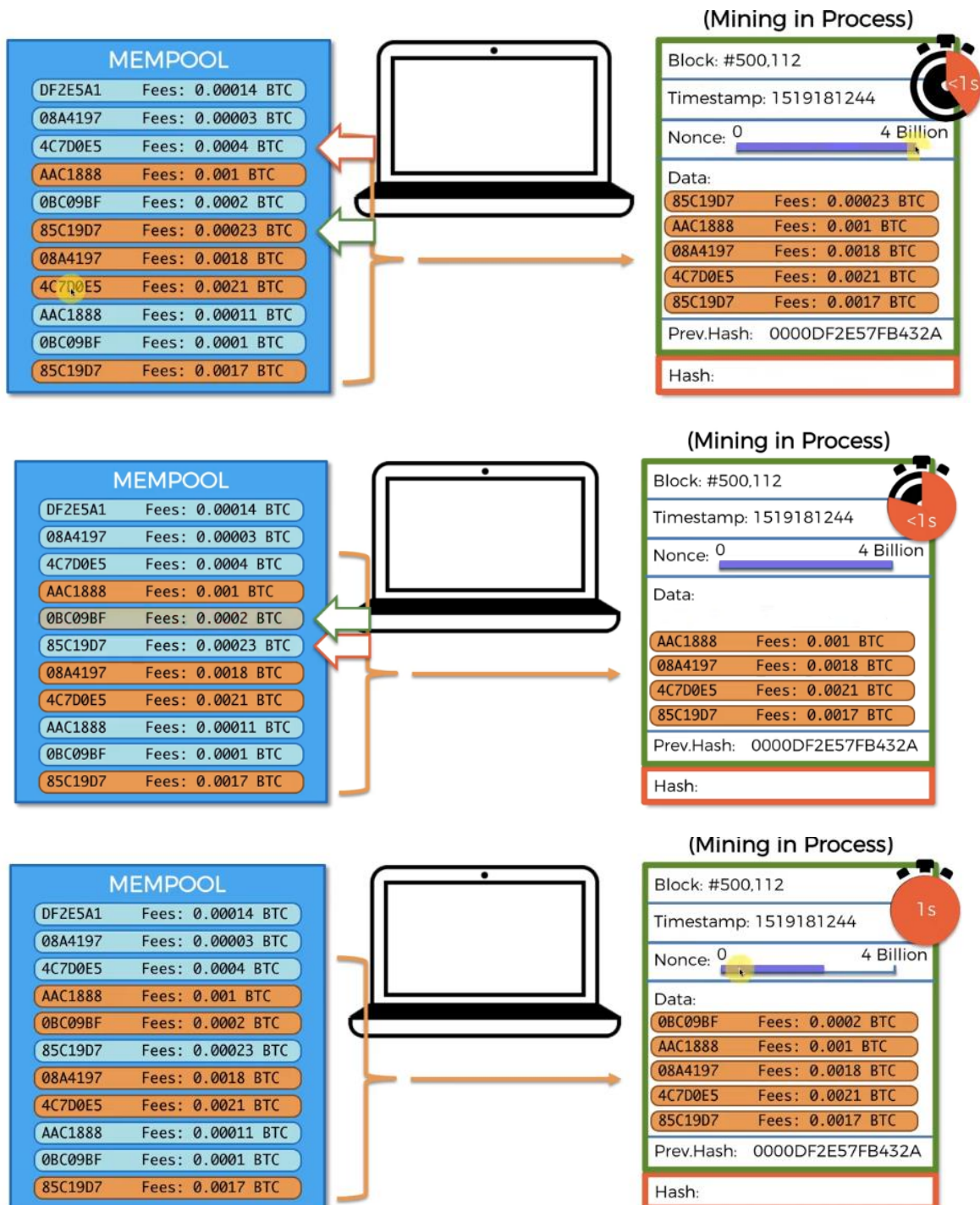
Miners pick the transaction with highest fees sort them out and put them inside the block.

The solution to the problem of miners who have so much hashing power is below.





The solution is to change the block configuration. Miners change the transactions in the block. Removes the transaction with the lowest fees from their block and add the transaction with the highest fees in the mempool and again go through the complete nonce range.



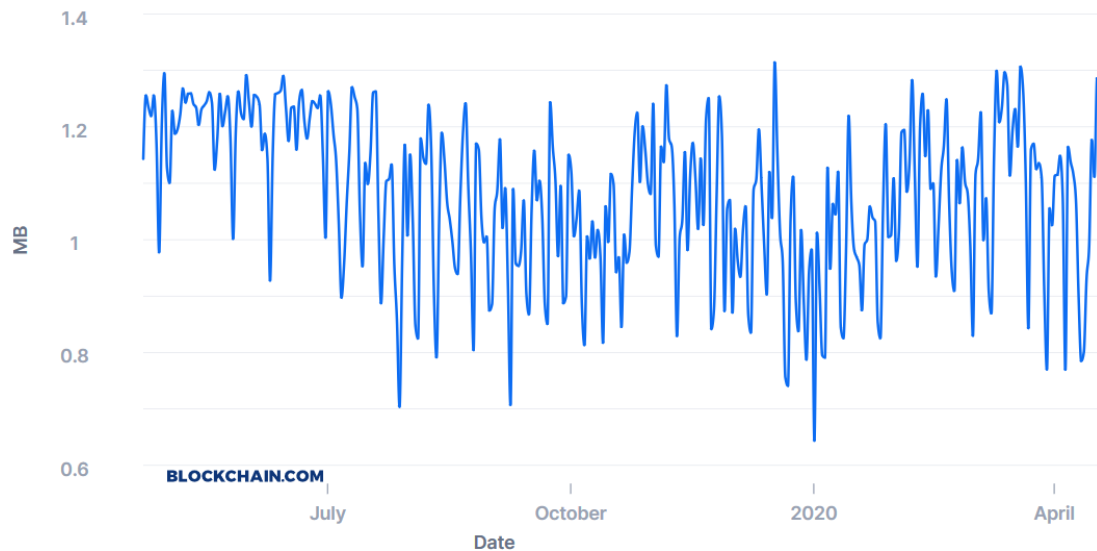
If the don't get the golden nonce we start over again with the highest transaction fees



## How Miners Pick Transaction Part 2

### Average Block Size (MB)

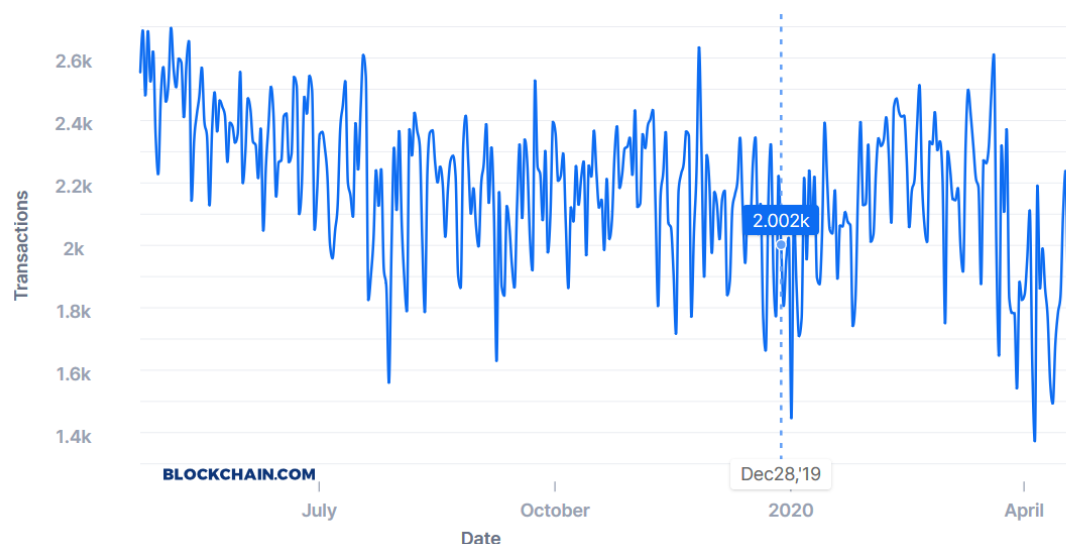
The average block size over the past 24 hours in megabytes.



Average block size right now is 1.08 MB. The size of the block depends upon the size of the transactions and the size vary around 1 MB.

### Average Transactions Per Block

The average number of transactions per block over the past 24 hours.



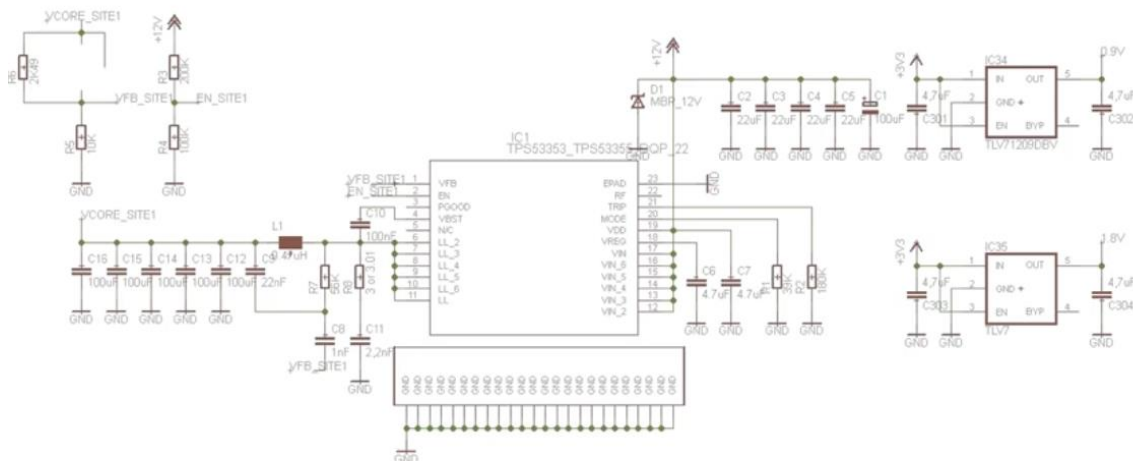
The average transaction per block also varies around 2000.

## CPU vs GPU 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

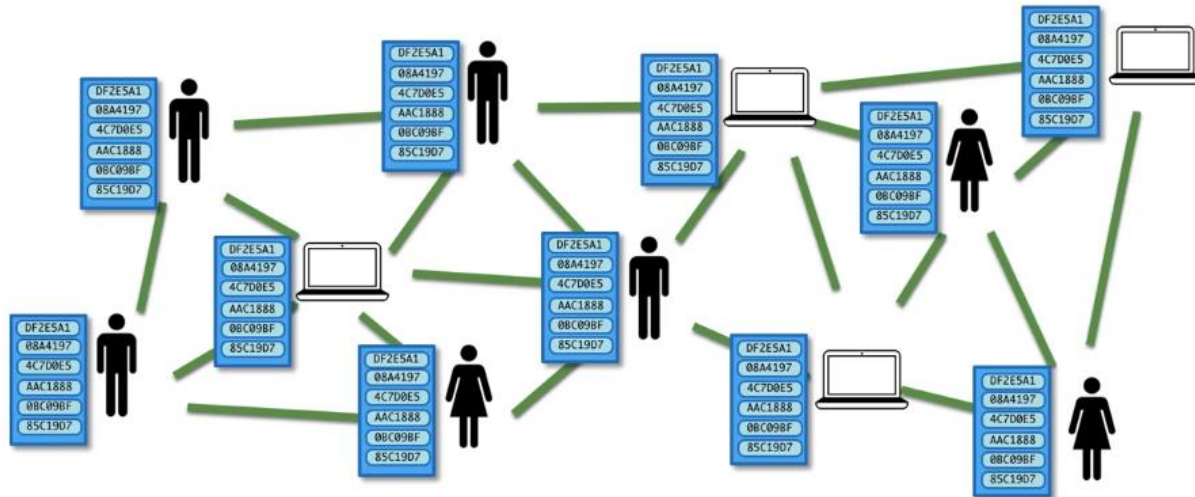
Cloud Mining

## Applications Specific Integrated Circuit

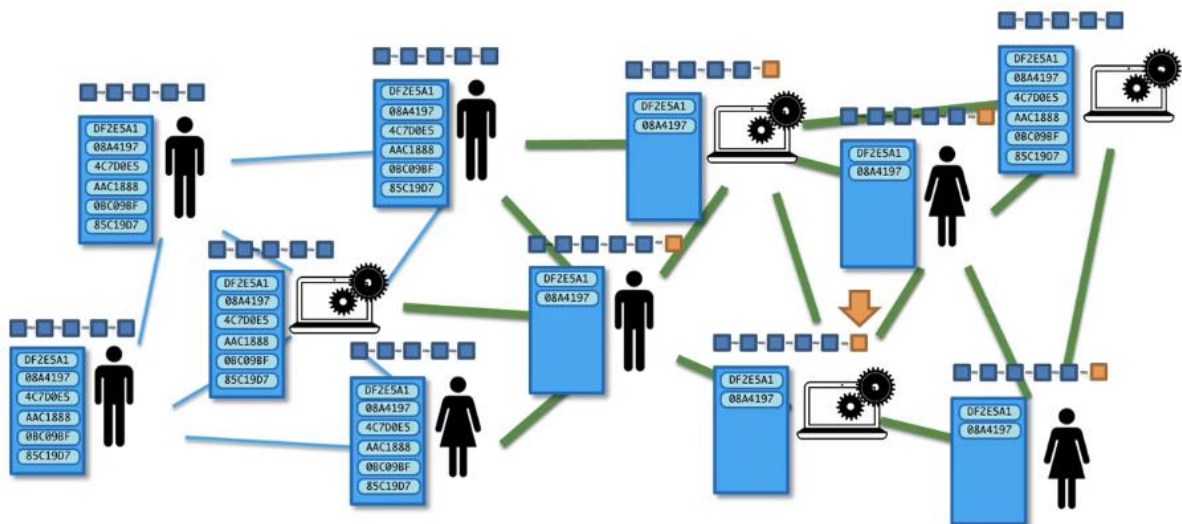


## How do Mempools work?

Mempools is a staging area of transactions before they are added to block.



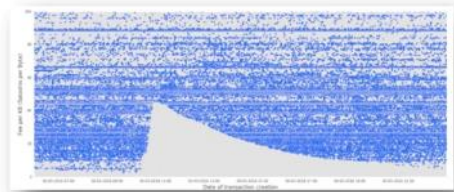
As a new block is mined, the transactions which we've added in the block are removed from the mempool and new mempool is copied to the whole network



## Additional Reading

*An in-depth guide into how the mempool works*

By Marion Deneuville (2016)



Link:

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

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

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

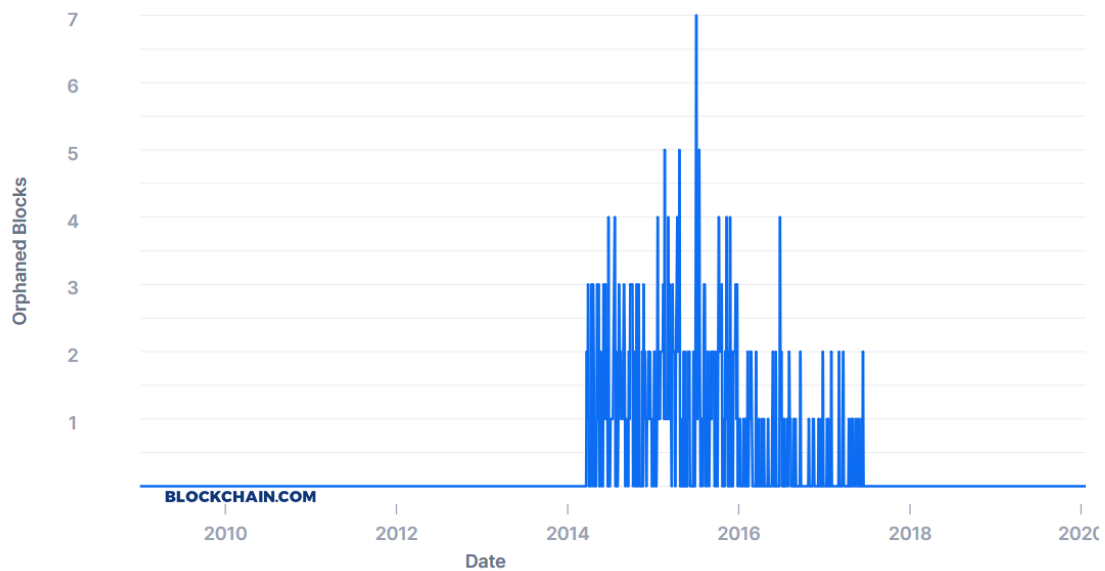
<https://www.blockchain.com/charts/mempool-growth>

<https://www.blockchain.com/btc/unconfirmed-transactions>

# Orphaned Blocks

## Number Of Orphaned Blocks

The total number of blocks mined but ultimately not attached to the main Bitcoin blockchain.



<https://www.blockchain.com/charts/n-orphaned-blocks>

## 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

Timestamp	2018-01-12 23:10:32
Number Of Transactions	1766
Relayed By	BTC.com

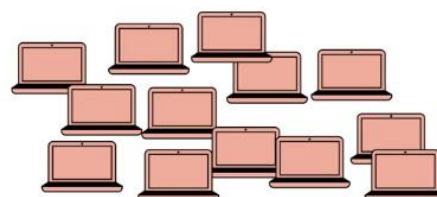
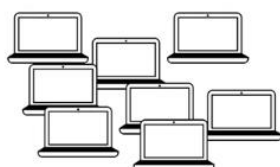
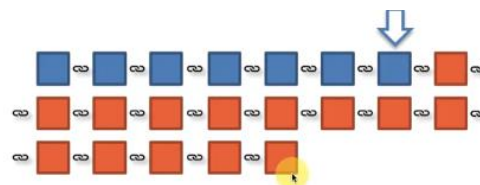
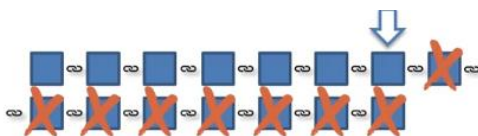
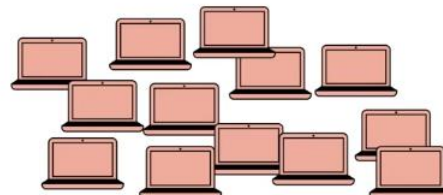
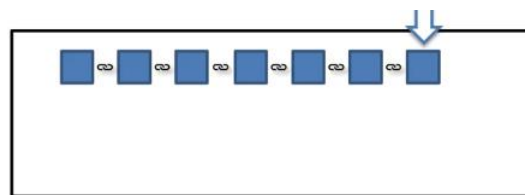
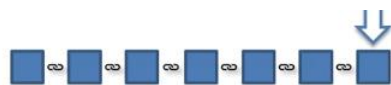
Timestamp	2017-12-06 06:45:56	Timestamp	2017-12-06 06:46:32
Number Of Transactions	2437	Number Of Transactions	2446

## The 51% Attack

A 51% attack refers to an attack on a blockchain—most commonly bitcoins, for which such an attack is still hypothetical—by a group of miners controlling more than 50% of the network's mining hash rate or computing power.

The attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins.

They would almost certainly not be able to create new coins or alter old blocks. A 51% attack would probably not destroy bitcoin or another blockchain-based currency outright, even if it proved highly damaging.



The cancelled blocks transaction goes to the mempool and the money miners got before on mining the blocks remains as it is with the miner.

See video here:

<https://drive.google.com/open?id=1phQRiN86XHeEwiy4ZsWlqzC4V390xLmp>

#### Additional Reading:

*Choosing ASICs for Sia [plus, we suggest reading the comments]*

By David Vorick (2017)

Link:

<https://blog.sia.tech/choosing-asics-for-sia-b318505b5b51>

