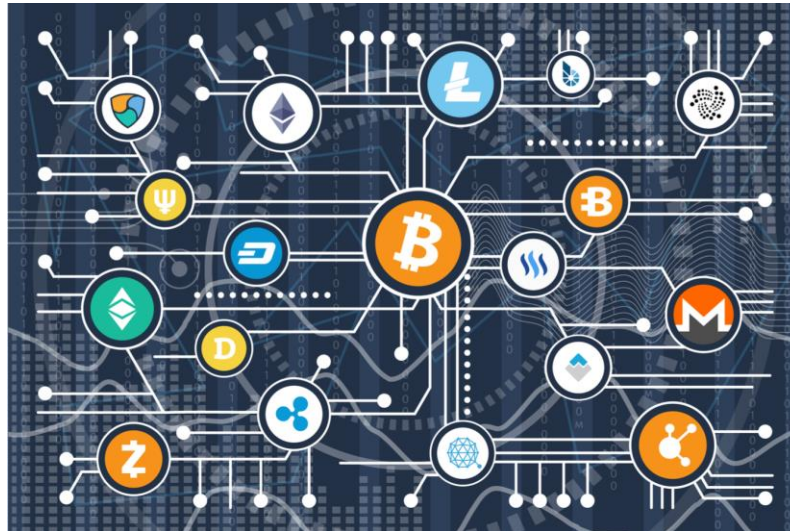


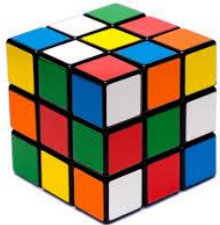
# How many of you:

- Have heard of bitcoins?
- Own cryptocurrency?
- Feel you understand the underlying blockchain technology?



# Block(chain) idea

1. Everyone tries to solve a puzzle
2. The first one to solve the puzzle gets 1 coin
3. The solution of puzzle  $i$  defines puzzle  $i+1$



3		2	4		6	
	4				5	3
1	8	9	6	3	5	4
			8		2	
	7	4	9	6	8	1
8	9	3	1	5	6	4
	1	9	2		5	
2		3			7	4
9	6	5			3	2

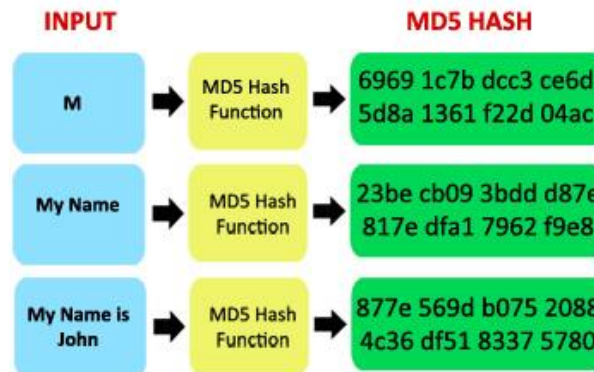
***It's EASY to VERIFY the solution, not to find it!***

# Hash functions

Hashing is a process which you turn anything (as long as you can represent it as a string) into a fixed length of bit string

A cryptographic hash function is a special class of hash functions which has various properties making it ideal for cryptography.

1. **Deterministic:** no matter how many times you hash a particular input, you will always get the same result
2. **Quick Computation:** The hash function should be capable of returning the hash of an input quickly
3. **Pre-Image Resistance:** given  $H(A)$  it is infeasible to determine  $A$ , where  $A$  is the input and  $H(A)$  is the output hash.
4. **Small Changes In The Input Changes the Hash.**
5. **Puzzle Friendly:** For every output “ $Y$ ”, if  $k$  is chosen from a distribution with high min-entropy it is infeasible to find an input  $x$  such that  $H(k|x) = Y$ .



# SHA256 hash functions

Here how you can try it in Python:

```
>>> import hashlib
```

```
>>> hashlib.sha256("hello world").hexdigest()  
'B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9'
```

```
>>> hashlib.sha256("helli world").hexdigest()  
'bd6952606ca18ccc9ff86bb8874ce0c61d7aa4fb72363e323f9eb2d3e783a487'
```

# The puzzle

I want to find a particular hash...

For example, **I want two ZEROs at the end of the hash** (“00”)...

What string I have to use?

```
>>> import hashlib
```

```
>>> hashlib.sha256("hello world").hexdigest()  
'B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9'
```

```
>>> hashlib.sha256("hello world 1").hexdigest()  
'063dbf1d36387944a5f0ace625b4d3ee36b2daefd8bdaee5ede723637efb1cf4'
```

...

```
>>> hashlib.sha256("hello world 238").hexdigest()  
'd622375f29c4b358674794610404bdd1f4e060a7244568b5549eed9754dfa400'
```

# The puzzle

...and 3 ZEROs at the end of the hash (“ooo”)...?

```
>>> import hashlib
```

```
>>> hashlib.sha256("hello world 3198").hexdigest()  
'838ee925a5eff45a3337363e9a2e993e02eddcc2edd90cdd4fec14b0c6e59000'
```

...and 6?

```
>>> hashlib.sha256("hello world 28114982").hexdigest()  
3d28877e8af972f6732de4591245a87545b0221c26e446f09e98665a6d000000
```

**It's getting harder to find a solution, but easy to verify it!**

# The puzzle – python code

```
import hashlib

i=0
while True:
    res = hashlib.sha256("hello world "+str(i)).hexdigest()
    if res.endswith("000000"):
        print i
        print res
        break
    i += 1
```

# The puzzle – create a chain

How can the puzzle “depends” on the previous one?

```
>>> hashlib.sha256("hello world 3198").hexdigest()  
'838ee925a5eff45a3337363e9a2e993e02eddcc2edd90cdd4fec14b0c6e59000'
```



# The puzzle – create a chain

How can the puzzle “depends” on the previous one?

```
>>> hashlib.sha256("hello world 3198").hexdigest()  
'838ee925a5eff45a3337363e9a2e993e02eddcc2edd90cdd4fec14b0c6e59000'
```

A new string!

```
>>> hashlib.sha256("  
SECOND hello world + 838ee925a5eff45a3337363e9a2e993e02eddcc2edd90cdd4fec14b0c6e59000  
").hexdigest()  
'9b582a1b5fd41f36cc0a396d4747507148f3bdde58a4bfff18891406a9158a72e'
```

But this hash doesn't end with “000”...

# The puzzle – create a chain

How can the puzzle “depends” on the previous one?

```
>>> hashlib.sha256("hello world 3198").hexdigest()  
'838ee925a5eff45a3337363e9a2e993e02eddcc2edd90cdd4fec14b0c6e59000'
```

A new string!

```
>>> hashlib.sha256("  
SECOND hello world + 838ee925a5eff45a3337363e9a2e993e02eddcc2edd90cdd4fec14b0c6e59000  
").hexdigest()  
'9b582a1b5fd41f36cc0a396d4747507148f3bdde58a4bffa18891406a9158a72e'
```

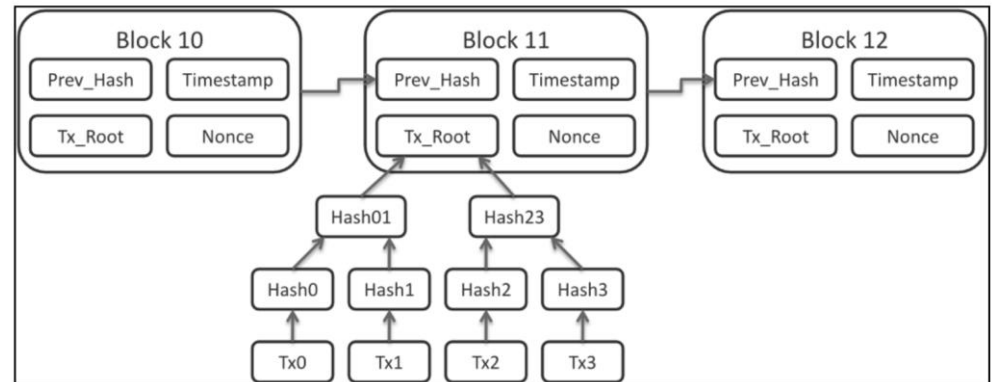
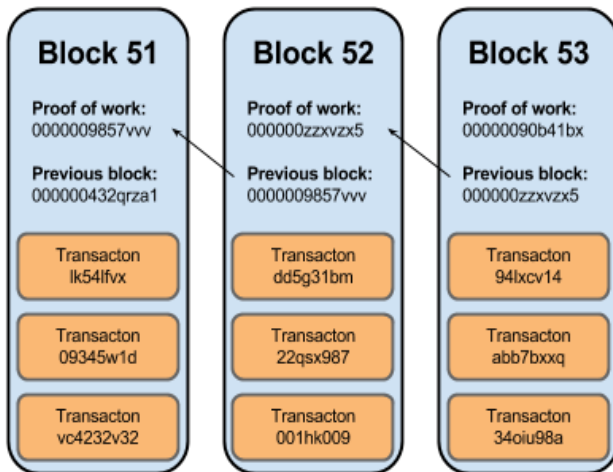
But this hash doesn't end with “000”... let's do the puzzle again:

```
SECOND hello world +  
838ee925a5eff45a3337363e9a2e993e02eddcc2edd90cdd4fec14b0c6e59000 + 1659  
'46eb8a72e26d849f9b755c39focaa08013b61b4592f02ab446c4fa1b498d4000'
```

# What is the Blockchain

The blockchain is basically a linked list which contains data and a hash pointer to the previous block, hence creating a persistent, ever-growing, "blockchain" that constantly updates to represent the latest state of the ledger.

What is a hash pointer? A hash pointer is similar to a pointer, but instead of just containing the address of the previous block it contains the hash of the data inside the previous block.

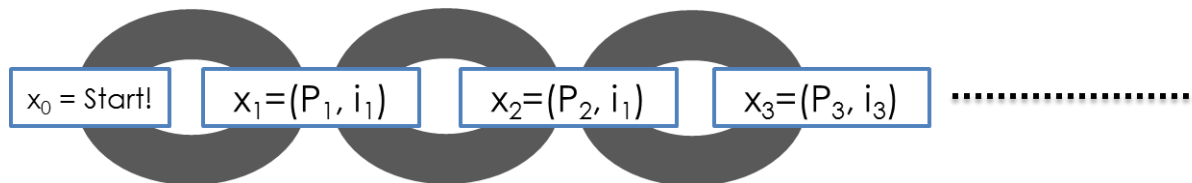


# What is the Blockchain

The blockchain is a decentralized, distributed and public digital ledger that is used to record information across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks.

Key concepts are:

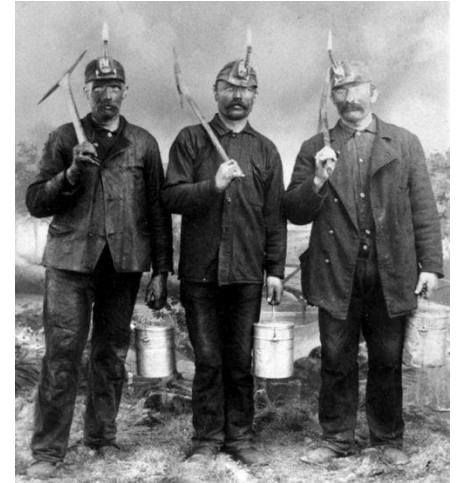
- **Decentralization:** the information is not stored in a privileged central server but in all the individual computers of each participant
- **Immutability:** no participant can modified a transaction after it has been recorded on the ledger
- **Cryptography:** integrity and security of the information on the blockchain are ensured with cryptographic functions
- **Transparency:** participants know where the assets came from and how its ownership has changed over time



# Proof of work (mining)

When you want to set a transaction this is what happens behind the scenes:

- Transactions are bundled together into what we call a block;
- Miners verify that transactions within each block are legitimate;
- miners solve a mathematical puzzle known as proof-of-work problem;
- A reward is given to the first miner who solves each blocks problem;
- Verified transactions are stored in the public blockchain



This “mathematical puzzle” has a key feature: **asymmetry**: hard on the requester side but easy to check for the network.



All the network miners compete to be the first to find a solution for the mathematical problem that concerns the candidate block, **a problem that cannot be solved in other ways than through brute force** so that essentially requires a huge number of attempts.

When a miner finally finds the right solution, he/she announces it to the whole network at the same time, receiving a cryptocurrency prize (the reward) provided by the protocol.

# Reward

mining process is an operation of inverse hashing: it determines a number (nonce), so the cryptographic hash algorithm of block data results in less than a given threshold.

This threshold, called difficulty, is what determines the competitive nature of mining: more computing power is added to the network, the higher this parameter increases, increasing also the average number of calculations needed to create a new block.

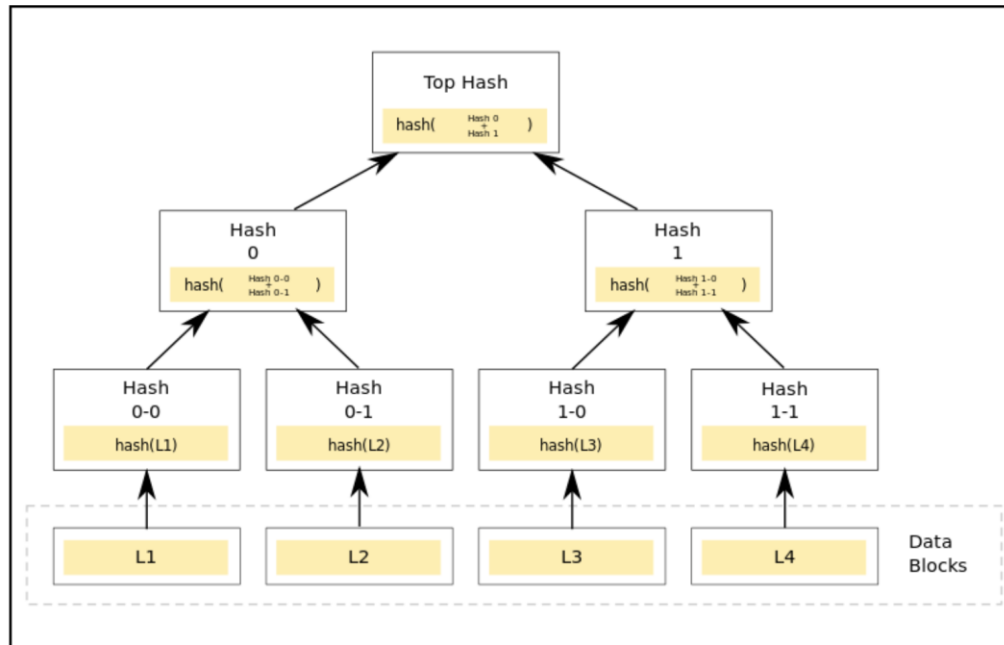
This method also increases the cost of the block creation, pushing miners to improve the efficiency of their mining systems to maintain a positive economic balance.



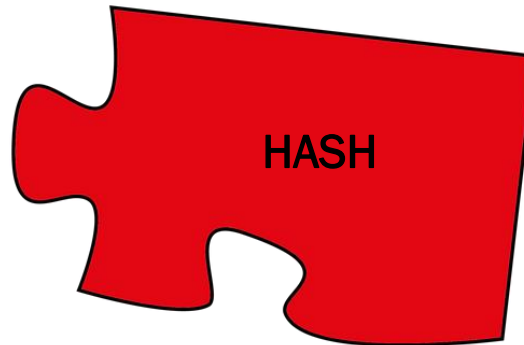
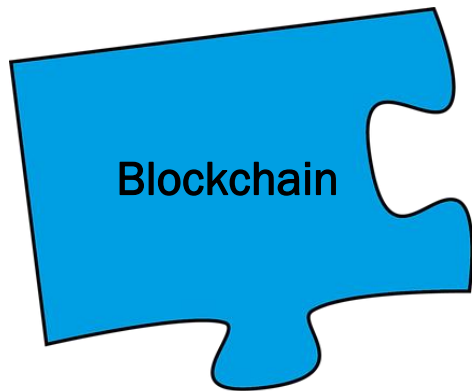
# Merkle Tree

A Merkle tree is a type of binary tree:

- each node is the hash of its two children
- a single root node, also formed from the hash of its two children, representing the "top" of the tree.



So much things... 😞



Be patient! Let's see a real case:  
BITCOIN



# Bitcoin

Blockchain technology was first introduced in a whitepaper entitled: “Bitcoin: A Peer-to-Peer Electronic Cash System,” by Satoshi Nakamoto in 2008.

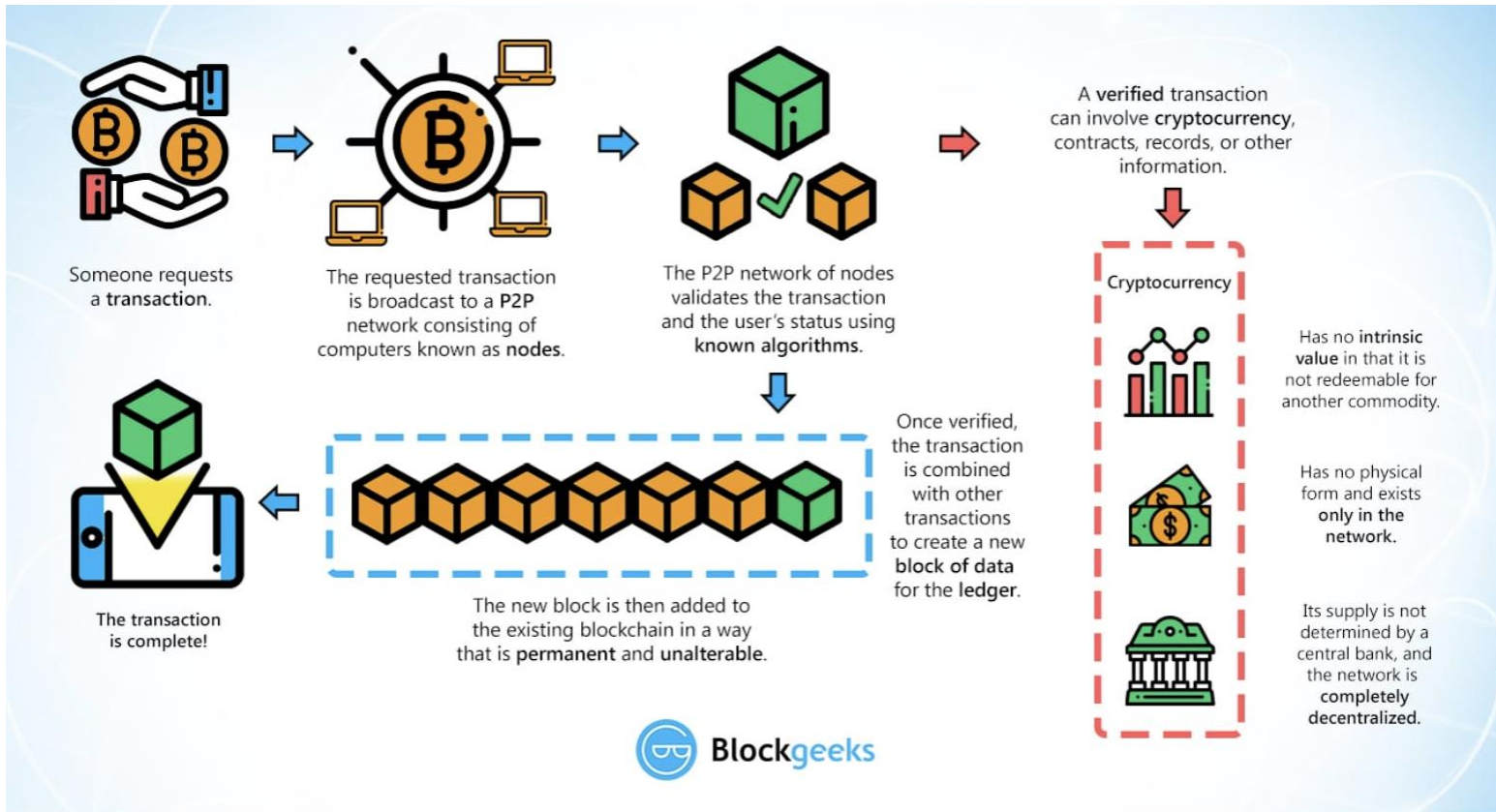
Bitcoin is a collection of concepts and technologies creating a digital money ecosystem



- A decentralized peer-to-peer network (the bitcoin protocol)
- A public transaction ledger (the blockchain) (roughly one block created every ten minutes)
- A decentralized mathematical and deterministic currency issuance (distributed mining)
- A decentralized transaction verification system (transaction script)

# Bitcoin

Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System



# Blockchain

A block header contains:

Version: The block version number.

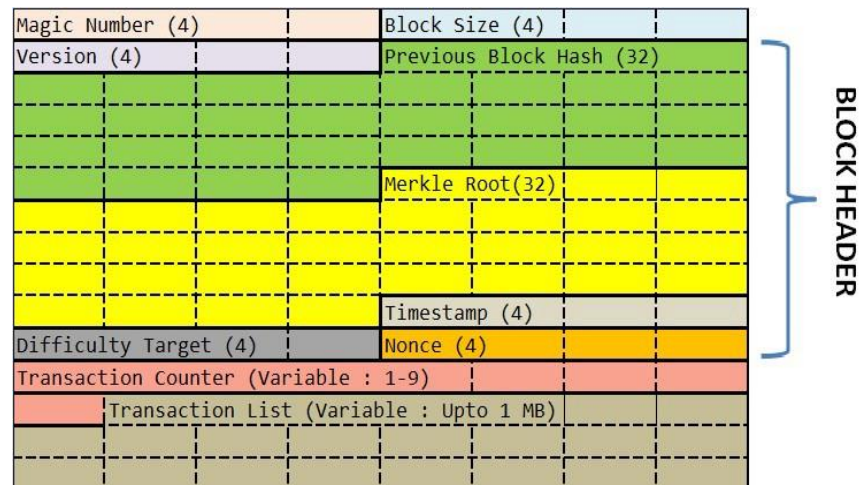
Time: the current timestamp.

The current difficult target.

Hash of the previous block.

Nonce.

The Merkle Root.



# difficulty

Mining is like a game, you solve the puzzle and you get rewards.

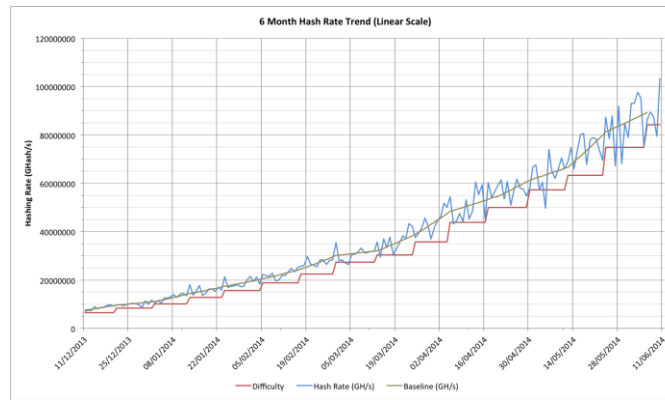
Setting difficulty makes that puzzle much harder to solve and hence more time-consuming.

the difficulty target is a 64-character string (which is the same as a SHA-256 output) which begins with a bunch of zeroes.

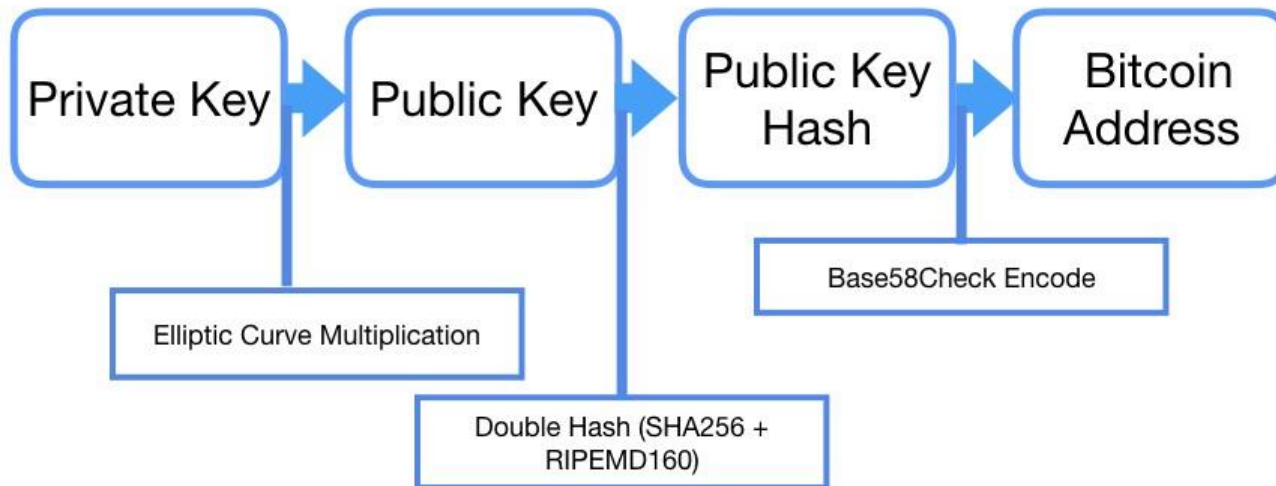
A number of zeroes increases as the difficulty level increases.

The difficulty level changes after every 2016th block to produce a block every 10 minutes.

The miner of every block is entitled to include a transaction giving themselves 12.5 BTC out of nowhere. Additionally, there are "transaction fee".




# BTC Address



# BTC transaction

## Transazione Ottieni informazioni su una transazione bitcoin

[ac60220be92a9ae91adfacc98594c34c4a3ea57112988fb86d6bcbdc6be7b82ca](#)

bc1qdnjnhv4h7drws852eq0caspmuzslccx48u38v  [38hm7FKkQDZgSFJCTc2xiqJT6fckEyt9m](#) 0.13765206 BTC  
bc1qdnjnhv4h7drws852eq0caspmuzslccx48u38v 0.00125492 BTC

**2 conferme** **0.13890698 BTC**

Sommar	
Dimensione	667 (byte)
Peso	1378
Orario di Ricezione	2019-05-22 20:59:16
Incluso nei Blocchi	<a href="#">577303</a> ( 2019-05-22 21:16:53 + 18 minuti )
conferme	2
Visualizza	<a href="#">Osserva il Grafico ad Albero</a>

Input e Output	
Totale Input	0.14048818 BTC
Totale Output	0.13890698 BTC
tasse	0.0015812 BTC
Tariffa per byte	237.061 sat/B
Tariffa per unità di peso	114.746 sat/WU
Stima dei BTC scambiati	0.13765206 BTC
Script	<a href="#">Mostra gli script e la coinbase</a>

Way more complex than this...

# Crypto Puzzles – mining bitcoin

When the Bitcoin mining software wants to add a new block to the blockchain, this is the procedure it follows.

Whenever a new block arrives, all the contents of the blocks are first hashed.

If the hash is lesser than the difficulty target, then it is added to the blockchain and everyone in the community acknowledges the new block.

However, it is not as simple as that. You will have to be extremely lucky to get a new block just like that. This is where the nonce comes in.

The nonce is an arbitrary string which is concatenated with the hash of the block.

After that this concatenated string is hashed again and compared to the difficulty level. If it is not less than the difficulty level, then the nonce is changed and this keeps on repeating a million times until finally, the requirements are met. When that happens the block is added to the block chain.

# Mining bitcoin 2009 - CPU

the first bitcoin miners used standard multi-core CPUs

If you had a couple computers lying around with decent specs you could have earned about five euro a day.

The difficulty of mining was so low then it was worth it for hobbyists and crypto nerds to participate.





# Mining bitcoin 2010 - GPU

in October 2010 the code for mining bitcoin with GPUs was released to the general public.



# Mining bitcoin 2011 - FPGA

mining difficulty continued to rise, and with it, the power requirements would soon become too steep for your average hobbyist to make any money.

By June 2011 field-programmable gate arrays (FPGAs) were becoming all the rage.

The biggest draw to this hardware was the fact that it used three times less power than simple GPU setups to effectively accomplish the same task.



# Mining bitcoin 2013 – cheap ASIC

Where FPGA requires tweaking after purchase (the field-programmable part of FPGA), an ASIC is created for a specific use, in this case mining cryptocurrency. This is why ASIC miners remain the standard.



330 Mh/s



1.8 Gh/s

# Mining bitcoin 2013 – mining pool



# Mining bitcoin now – expensive ASIC



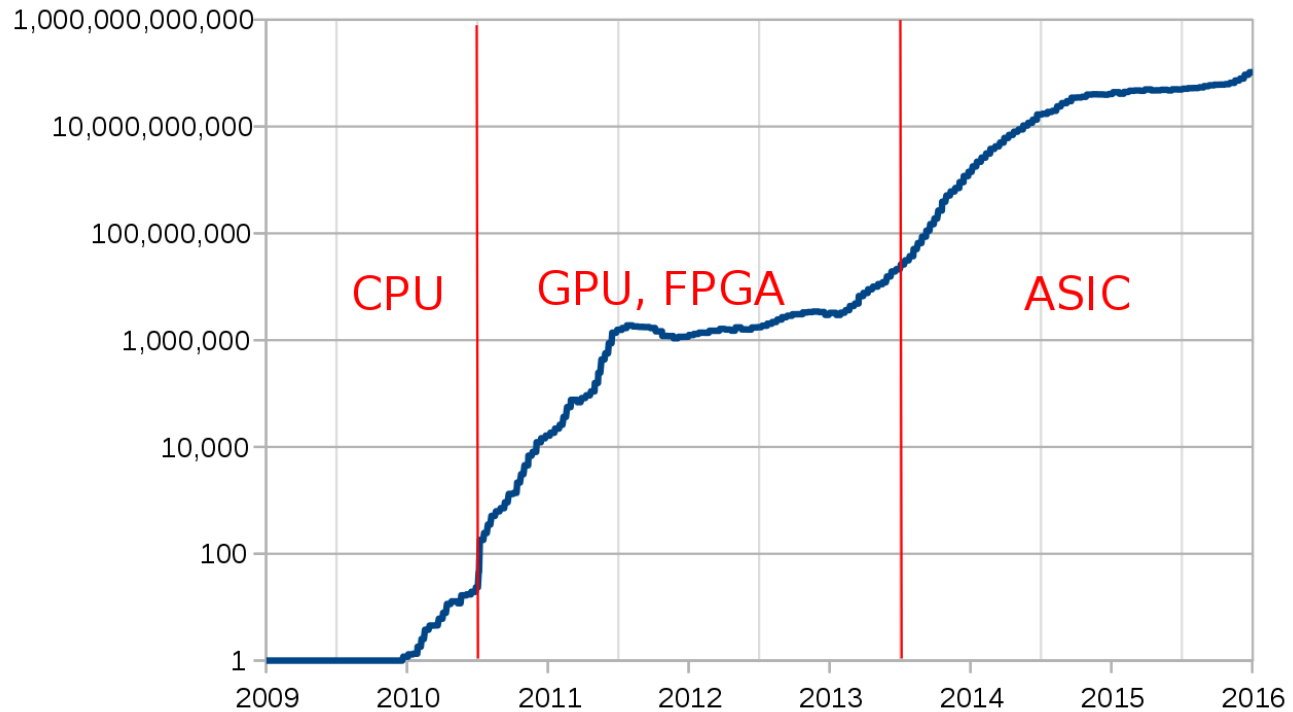
14 Th/s



# Mining bitcoin now



# Mining bitcoin - difficulty



# Bitcoin PIZZA

*I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place ...*

<https://bitcointalk.org/index.php?topic=137.0>

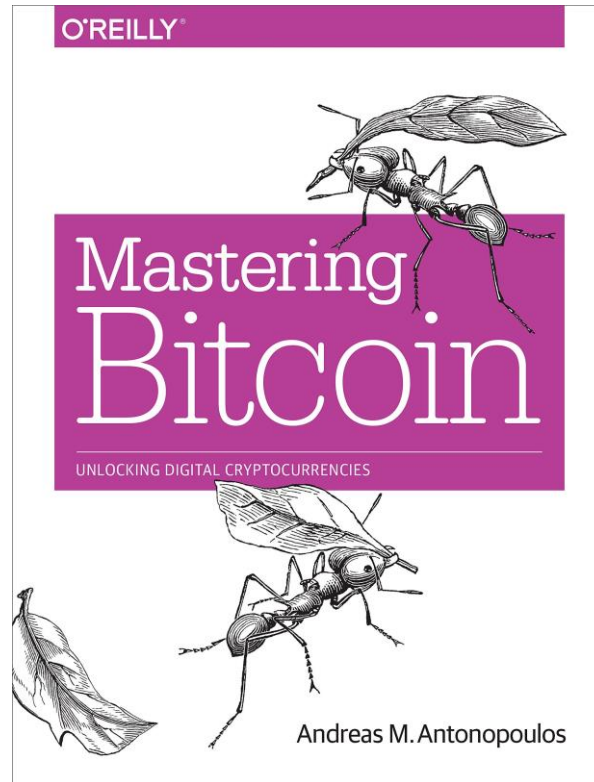
Eventually someone took him up on the offer and Hanyecz ended up eating a meal that, only some years later, would be worth \$71 million.



*Every year, the crypto community celebrates 'Bitcoin Pizza Day' on May 22.*



# For more infos...



<https://github.com/bitcoinbook/bitcoinbook>

*Internet of Things A.Y. 18-19*