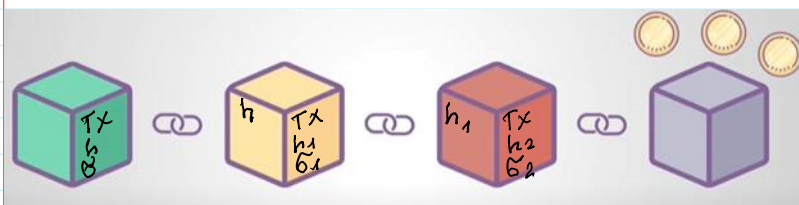


[Federal Reserve Board](#) is the **central bank of the United States**, provides the nation with a safe, flexible, and stable currency.



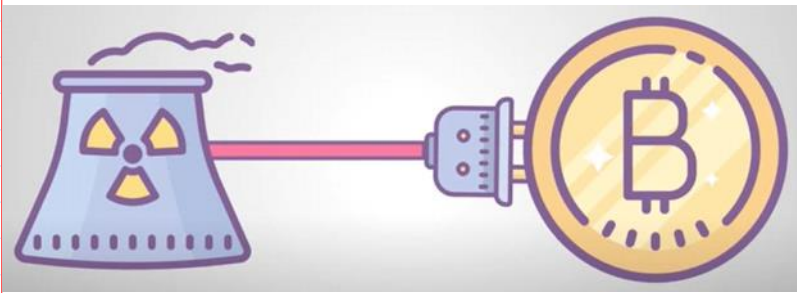
ICO - initial coin offer

STO - secure token offer

NFT - non-fungible token offer

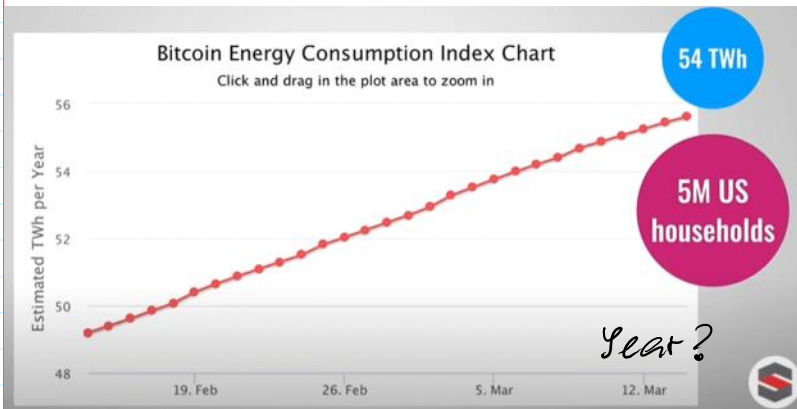


POW - Proof of Work



PoW - Proof of Work

1 BTC  $\sim$  > 30 000 \$  
 64 000 \$



Electric energy consumption kWh

1 kWh  $\sim$  0.193 Eur

54 TWh =  $54 \cdot 10^9$  kWh

1 TWh =  $10^{12}$  Wh



Application Specific Integrated Circuits - ASIC --> mining

Farm is using a huge el. power (FP)

[W] - watt

In 1 household EP  $\sim$  5 kW

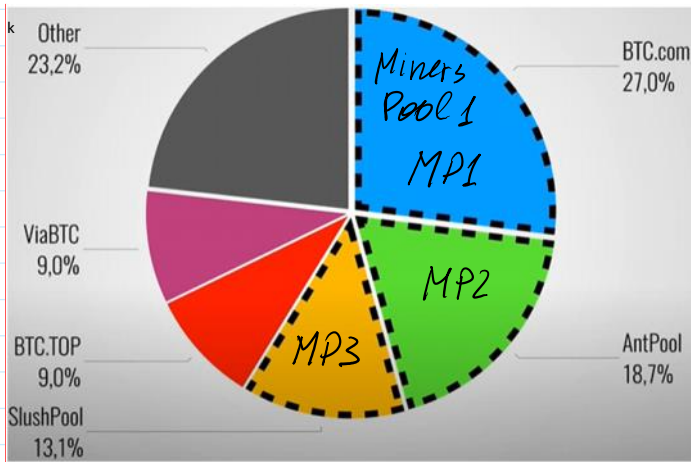
During 1 hour Energy = 5 kWh  
 $\downarrow$   
 $\sim$  1 Eur

To charge e-vehicle 20-50 kW

Farm can consume  $\sim$  500 kW - 1 MW

During 1 hour you'll consume Energy = 1 MWh = 1000 kWh

1000 kWh  $\times$  0.2 € = 2000 €



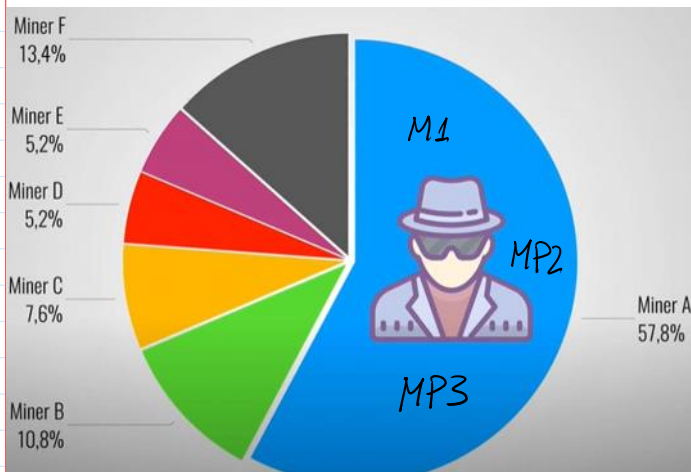
## 51% Attack

Computation power of mining is related to the speed of h-values

computation  $V_h \sim T\text{Hash/sec}$

E.g.  $V_h = 1000 T\text{Hash/sec}$

Total network has  $V_h = 1900 TH/s$



## > 51% Network power

1000 TH/s is more than 51%

1900 TH/s

## 51% Attack

## Forking



Energie usage 

Mining pools -> centralization 

-> We need new algorithm!




**Proof-of-stake**



~~Miners~~

~~Mining~~

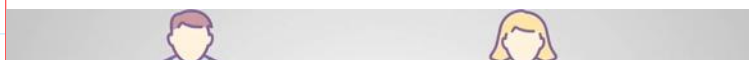


**Validators**

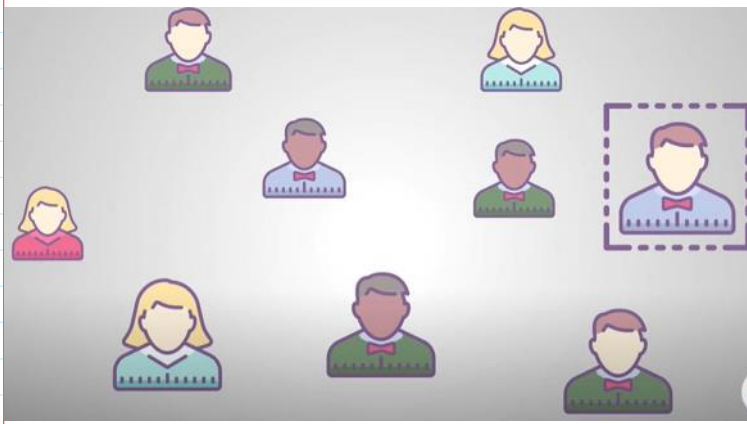
**Minting / Forging**

Ethereum  $1\text{Eth} \sim 2300 \$$

The name of cryptocurrency in Ethereum blockchain is named as Ether - Eth



1) Cryptocurrency Ether



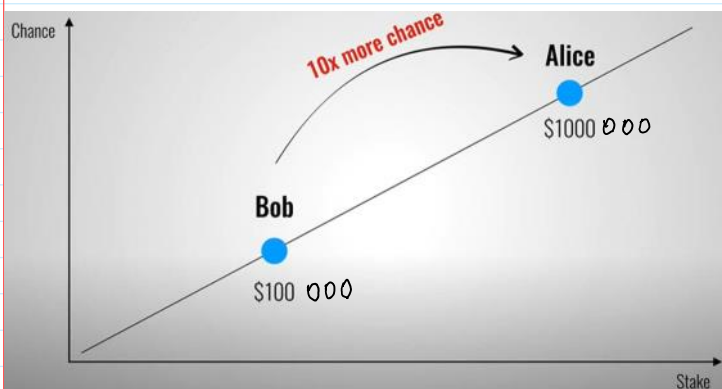
- 1) Cryptocurrency Ether penetration to business
- 2) Potential investors attraction  
↓  
Can buy Tokens related to Ether.

## Vitalik Buterin

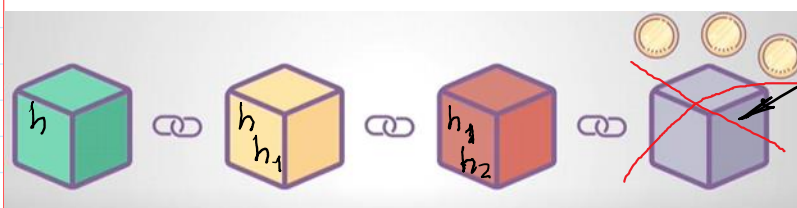


Eth → 32 Eth put into the "shell" to make a right to mine a block  
the difficulty of validation is low →

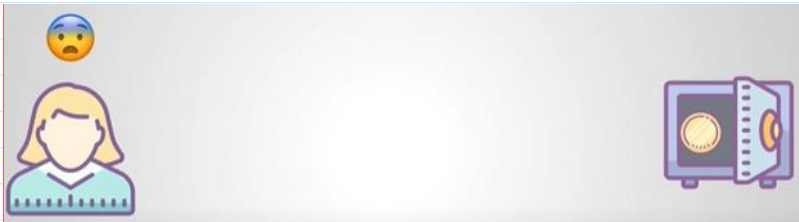
→ the speed of validation is increased.



$1 \text{ Wei} = 10^{-18} \text{ Eth}$   
 $1 \text{ Eth} = 1000\,000\,000\,000\,000\,000 \text{ Wei}$   
 to mine a block consisting of a lot of transactions →  
 → every transaction has declared a reward in Gas for its validation.  
 → Gas price:

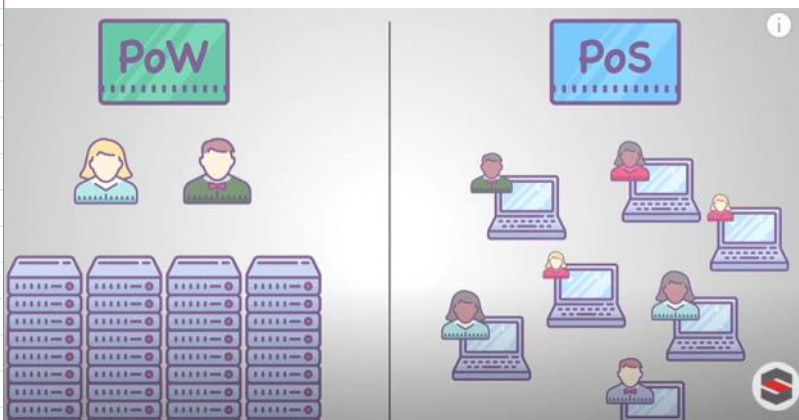


Mistaken validated block  
 ↓  
 Intentionally Non-Intentionally



To empty your deposit after some time.

TSMC



Ethereum 2.0

32 Eth; 1 Eth ~ 140 \$

Ethereum, Libra, ... etc.



Fiat currency → crypto curr. →

→ { Financial transact. →  
→ Smart contracts  
→ Investment mech. → tokens

Blockchain for business processes monitoring and control economic

NEM - New Economic Movement

Industry tokenization ← crowd funding

CBDC - Central Bank Digital Currency

Registration to [inimsociety.net](http://inimsociety.net) :

Name

Su\_inf

Su\_i

Su\_kk

Operations mod  $p$ :  $p$  - prime number - is a number which is not divisible except 1 and themselves. E.g.  $p = 11$

$$n = 123 \rightarrow 123 \bmod 11 = 2$$

$$\begin{array}{r} 123 \\ - 11 \\ \hline 13 \\ - 11 \\ \hline 2 \end{array}$$

>> 2\*2

ans = 4

>> p=11

p = 11

>> n=123

n = 123

>> mod(n,p)

ans = 2

In our simulation we will use integer numbers having 28 bit length.

The operations will be performed

mod  $p$ , when  $p$  has a 28 bit length and is prime.

>> p=genprime(28)

p = 174320929

>> isprime(p)

ans = 1

>> pb=dec2bin(p)

pb = 1010 0110 0011 1110 1101 0010 0001

ph = A 6 3 E ? 2 1

>> ph=bin2hex(pb)

ph = A 6 3 E D 2 1

Hexadecimal number are expressed by 4 bits and 1 digit of hex. number is represented by letters

