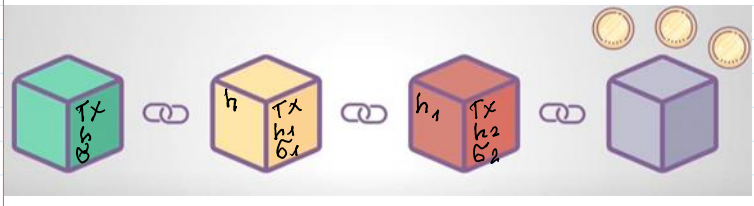
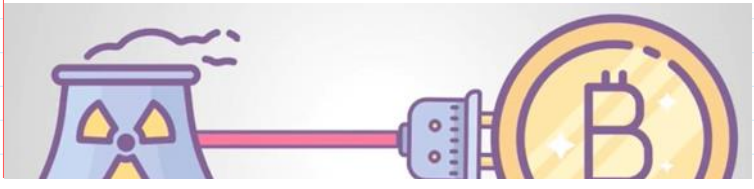
Federal Reserve Board is the **central bank of the United** States, provides the nation with a safe, flexible, and stable currency.



ICO - initial coin offer

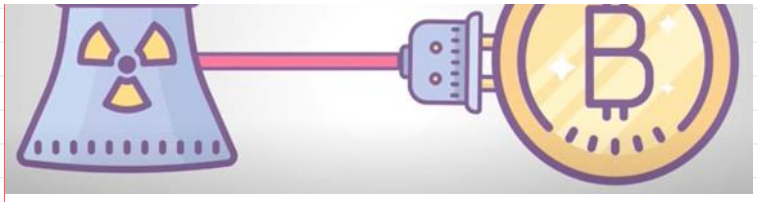
STO - secure token offer ERC 20, ERC 1410

NFT - non-fungible token offer



PoW - Proof of Work

1 BTC ~> 30 000 $

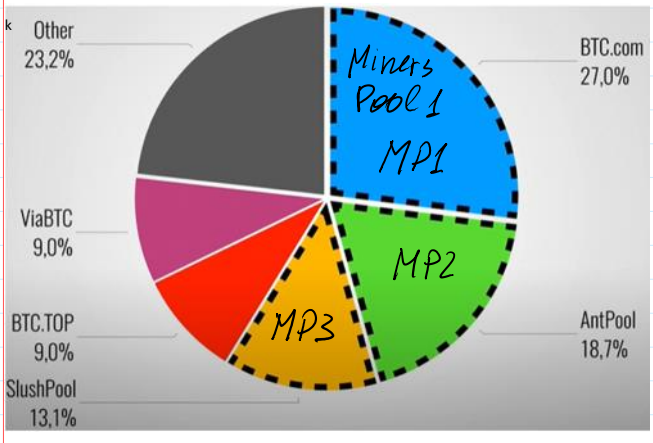


1 BTC ~ > 30 000 $
64 000 $

Electric energy consumption kWh
1 kWh ~ 0.193 Eur
54 TWh = $54 \cdot 10^9$ kWh
1 TWh = 10^{12} Wh

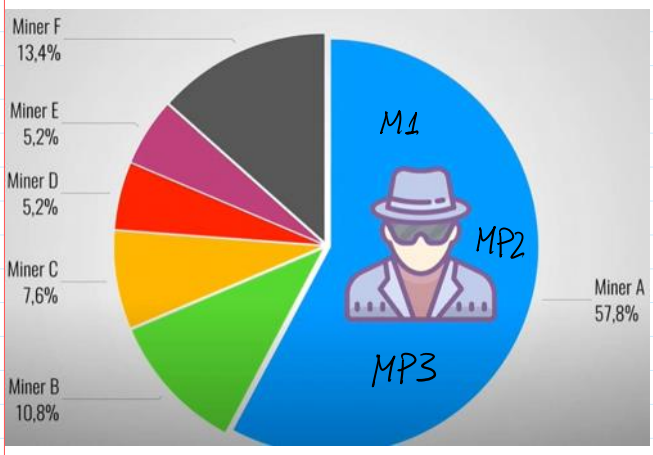
Application Specific Intrgrated Circuits - ASIC --> mining
Farm is using a huge el. power (FP)
[W] - watt
In 1 hoschold EP ~ 5 kW
During 1 hour Energy = 5 kWh
↓
~ 1 Eur

To charge e-vechile 20 - 50 kW
Farm can consume ~ 500 kW - 1 MW
During 1 hour you'll consume Energy = 1 MWh = 1000 kWh
1000 kWh * 0,2 € = 2000 €



51% Attack

Computation power of mining is related to the speed of h-values computation V_h ~ THash/sec
E.g. V_h = 1000 THash/sec
Total network has V_h = 1900 TH/s



> 51% Network power

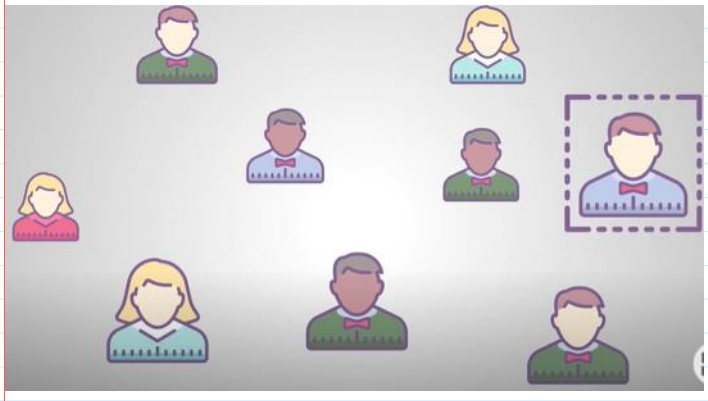
1000 TH/s is more then 51%
1900 TH/s

51% Attack

Forking

Ethereum 1 Eth ~ 2300 $

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



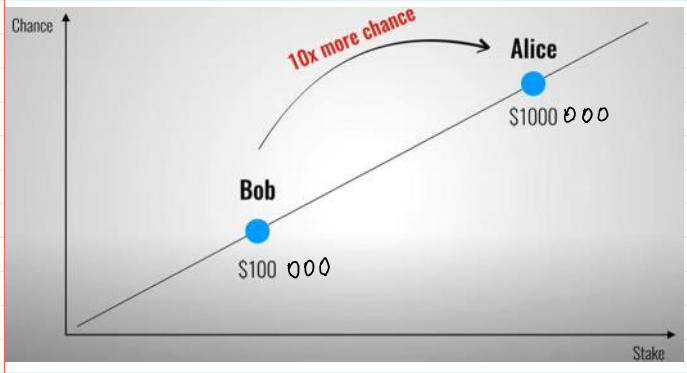
1) Cryptocurrency Ether penetration to busines
2) Potential investors attraction
   Can buy Tokens related to Ether.

Vitalik Buterin

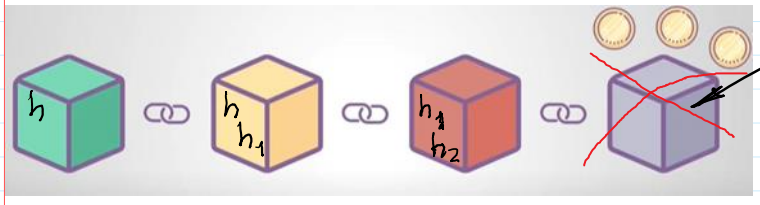
Eth → 32 Eth put into the "shell" to make a right to mine a block

" stake to make a right to mine a block
the difficulty of validat. is low →

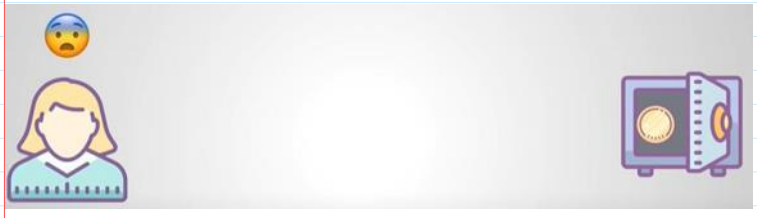
→ the speed of validation is increased.

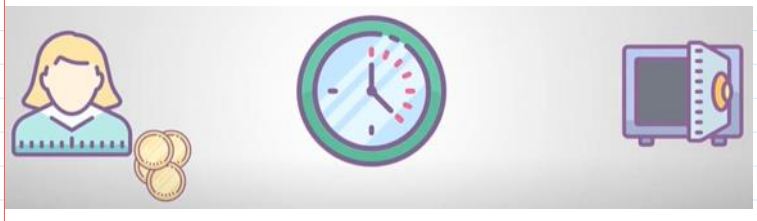


$1\ Wei = 10^{-18}\ Eth$
$1\ Eth = 1000000000000000000\ Wei$
to mine a block consisting of a lot of transactions →
→ every transaction has declared a reward in Gas for its validat.
→ Gas price :

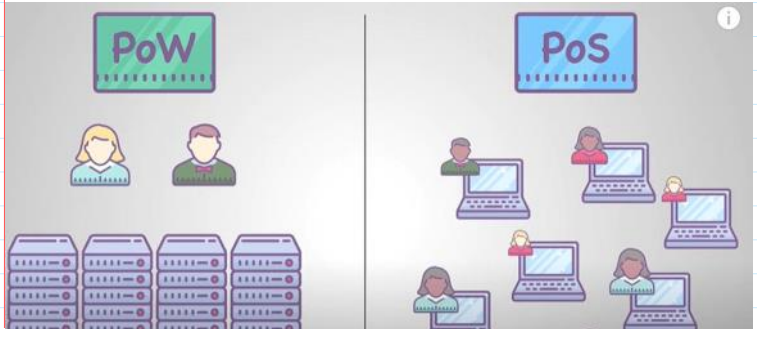


Mistaken validated block
Intentionally / Non-Intentionally



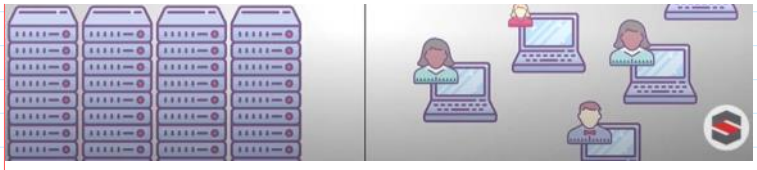


To empty your deposit after some time.
TSMC



Ethereum 2.0
32 Eth ; 1 Eth ~ 140 $

Ethereum, Libra, ... etc.



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 imimsociety.net : Name

Course Works
http://crypto.fmf.ktu.lt/xdownload/

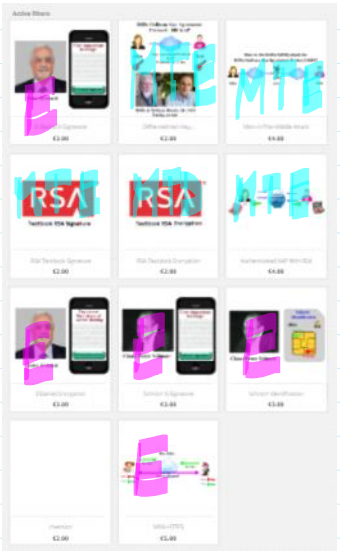
- Course_Work-Example.7z
- Course_Work-Requirements-2022.doc
- Course_Works-List.docx

Registracija bus pateikta mano Google drive.

Midterm Exam, Exam.

https://imimsociety.net/en/
https://imimsociety.net/en/16-intellect
Registration: **Jonas Petraitis** must register as [Surname: **Pe**] [Name: **Jonas**].
You must purchase only one problem at a time

https://imimsociety.net/en/14-cryptography



After successful problem You are invited to press a button [Get reward]
The result you can verify in Your account --> ORDER HISTORY AND DETAILS -->

Here are the orders you've placed since your account was created.

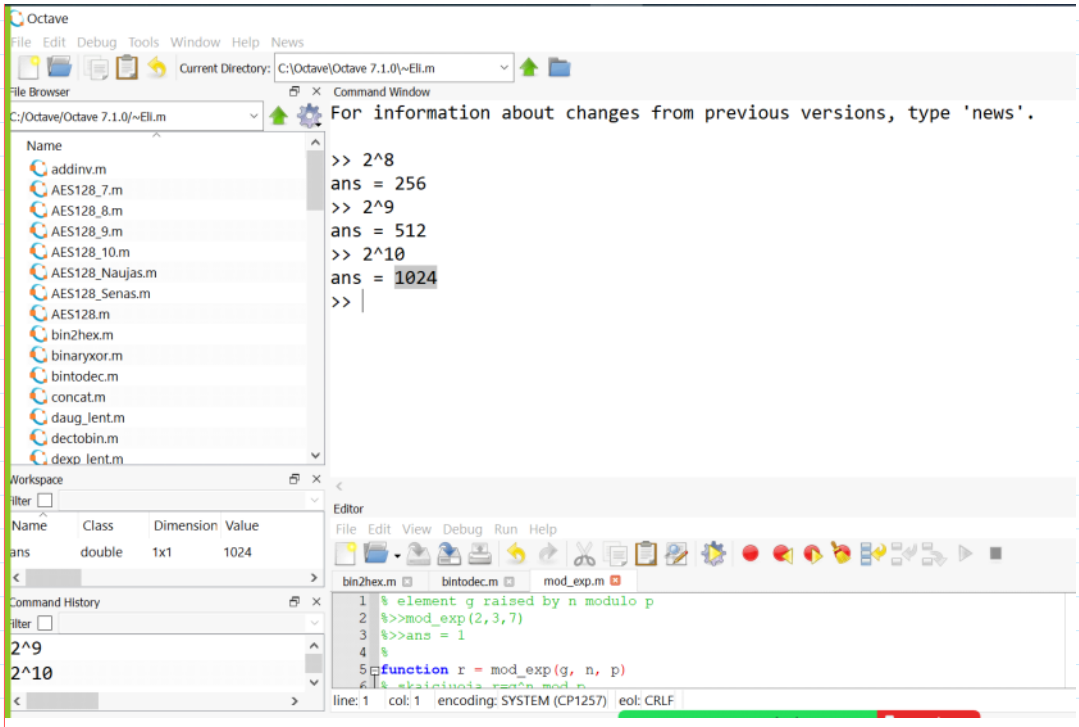
Order reference	Date	Total price	Payment	Status	Invoice	
KTVWXUNJO	01/24/2022	€0.00	Knowledge Bank	Payment accepted	PDF	Details Reorder

Moodle:

http://crypto.fmf.ktu.lt/

http://crypto.fmf.ktu.lt/xdownload/

- octave-7.3.0-w64-installer.exe
- octave.m.7z



For our simulation we will use integers of 28 bit length.
In cryptography we will use random generated integers, prime numbers, strong prime numbers.

```
>> r=randi(2^28-1)
r = 1.0235e+08
>> r=int64(randi(2^28-1))
r = 97878448
>> r=int64(randi(2^28-1))
r = 129372293
>> rb=dec2bin(r)
rb = 111101101100001000010000101
>> rh=bin2hex(rb)
rh = 7B61085

>> r=int64(152983475)
r = 152983475
>> rh=dec2hex(r)
rh = 91E57B3
>> rb=hex2bin(rh)
rb = 100100011110010101111110110011

>> p=genprime(28)
p = 265365371
>> isprime(p)
ans = 1

>> ph=dec2hex(p)
```

```
r = 129 372 293
rb = 111 1011 0110 0001 0000 1000 0101
rh =  7   B   6   1   0   8   5

r = 152983475
rb = 1001 0001 1110 0101 0111 1011 0011
rh =  9   1   E   5   7   B   3
```

$2^4\,2^3\,2^2\,2^1\,2^0$

$10000 = 1\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 0\cdot 2^0 = 2^4 = 16$

```
p = 265365371
>> isprime(p)
ans = 1
pb = 1111 1101 0001 0010 0111 0111 1011
ph =  F   D   1   2   7   7   B

>> max=int64(2^28-1)
max = 268435455
```

Dec	Bin	Hex
0	0000	0_h
1	0001	1_h
2	0010	2_h
3	0011	
4	0100	
5		
6		
7	0111	
8	1000	8
9		
10	1010	A_h
11	1011	B
12		C
13		D
14		E
15	1111	F
16	10000	10

ans = 1

```
>> ph=dec2hex(p)
ph = FD1277B
>> pb=hex2bin(ph)
pb = 11111101000100100111011111011

>> ps=genstrongprime(28)
ps = 210821363
```

```
>> max=int64(2^28-1)
max = 268435455
```

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

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

$123 : 11 = 11$, -11, 13, -11, 2

```
>> 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

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

16 number representind 1 digit of hex. number.

0000 0001 0010 0011 1010 1111