Elder-Head of this module for communications: send me e-mail.

Lectures are translated throuh the **Zoom**:
https://liedm.zoom.us/j/9999112448
Passcode: **12345678**

Practice are translated through the **Adobe Connect**:
https://ac.ktu.edu/p120m101
Enter as a **Guest** --> **Name** --> [**Enter Room**]

http://crypto.fmf.ktu.lt/
http://crypto.fmf.ktu.lt/telekonf/archyvas/B111%20Kriptologija/B111%202022/

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

- octave-6.3.0-w64-installer.exe
- 11-Octave_Stud_2021.11-Updated.7z

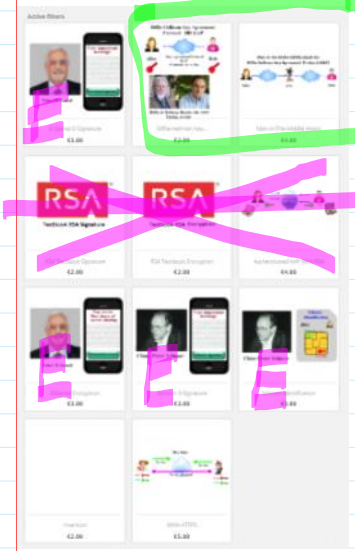
Course Works

B111 Course_Works 2021.docx

https://imimsociety.net/en/
https://imimsociety.net/en/16-intellect

https://imimsociety.net/en/14-cryptography
You must purchase **only one** problem at a time

Registration: S. Name for ex. S. Eligijus



Problems must be solved during Midterm exam

E - Problems must be solved during the Exam.

You must solve this problem and [Get reward] --> Your account --> OTDER 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		Details Reorder

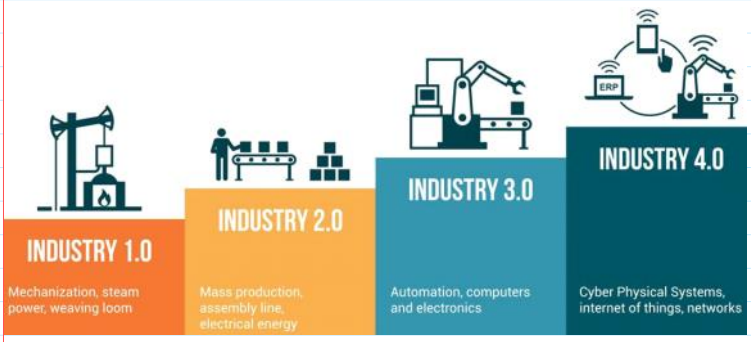
Moodle:

E-mails.

Sakalauskas Eligijus | Sakalauskas Eligijus

~~B111 Exam.~~ M123 Subject

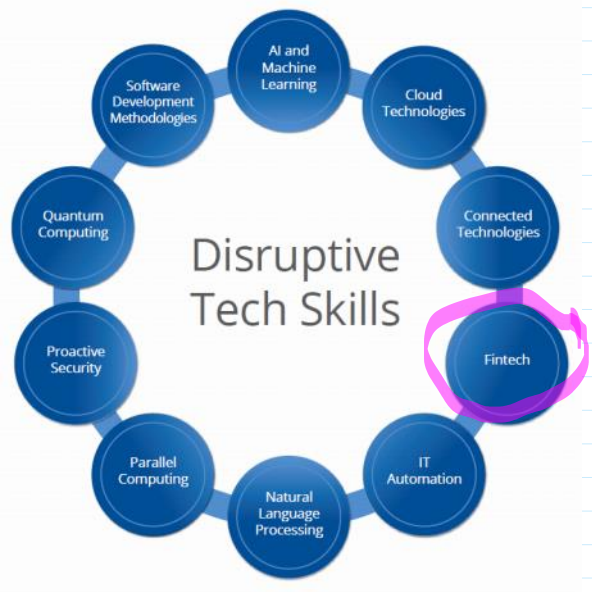
Text.
Name. Surname,
Group.



https://www.burning-glass.com/
https://www.burning-glass.com/wp-content/uploads/2020/12/Skills-of-Mass-Disruption-Report.pdf
Skills-of-Mass-Disruption-Report.pdf

Skills of Mass Disruption Tecnologies
Įgūdžiai Masinio Virsmo Technologijose

burningglass TECHNOLOGIES Solutions



Fintech: Skills related to technologies such as **blockchain** and others aimed at making **financial transactions more efficient and secure**.

Monitoring and control of business processes

H2020 projects

Table 1: **Job Openings and Growth by Disruptive Skill Area**

Skill Area	Total Job Openings (Last 12 Months)	Projected 5-Year Demand Growth

H2020 projects

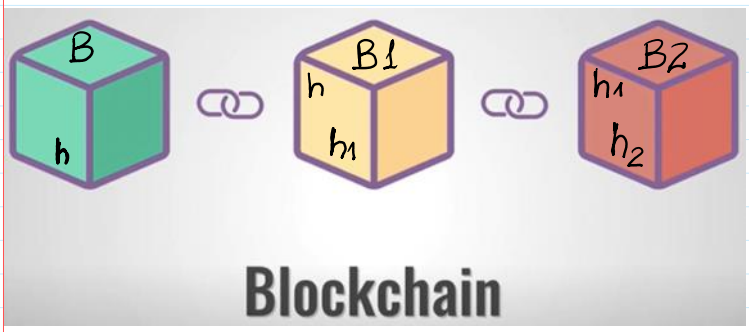
Table 1: Job Openings and Growth by Disruptive Skill Area

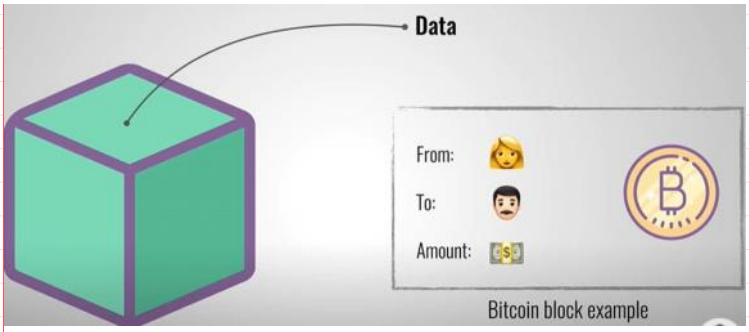
Skill Area	Total Job Openings (Last 12 Months)	Projected 5-Year Demand Growth
Software Dev Methodologies	634,660	35%
Cloud Technologies	462,963	28%
Proactive Security	373,123	39%
IT Automation	282,380	59%
AI and Machine Learning	197,810	71%
Connected Technologies	68,313	104%
NLP	36,941	41%
Fintech	35,667	96%
Parallel Computing	11,056	17%
Quantum Computing	2,718	135%

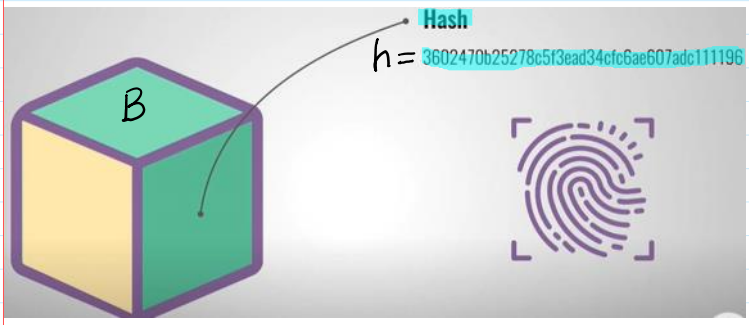
Table 3: Average Salary Premium by Disruptive Skill Area

Skill Area	Average Salary Premium
IT Automation	$24,969
AI and Machine Learning	$14,175
Fintech	$13,799
Software Dev Methodologies	$13,762
Connected Technologies	$10,873
Cloud Technologies	$10,588
Proactive Security	$8,851
Parallel Computing	$7,797
NLP	$6,368
Quantum Computing	$4,204

Students and Job Seekers.
Identify and Learn High-Value Disruptive Skills.
The disruptive tech skills are growing rapidly and can lead to significant salary boosts.
Individuals who identify and develop these future-ready skills – and continuously update their skill sets as new needs emerge – will be best-positioned to enhance their career prospects, both in tech and beyond.





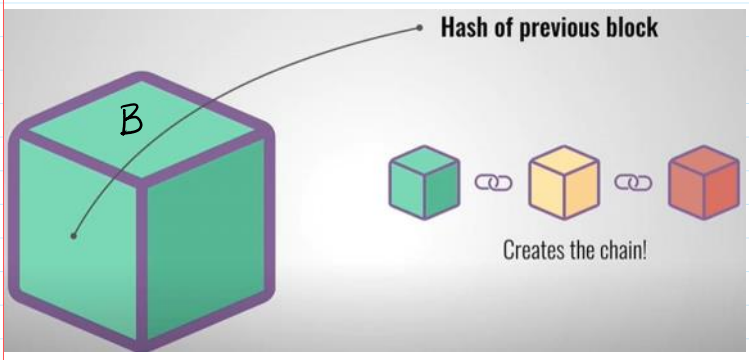


$H(B) = h$; $|h| = 256$ bit

$|B| \sim 1$ GB

Finger print

H-function; Message digest

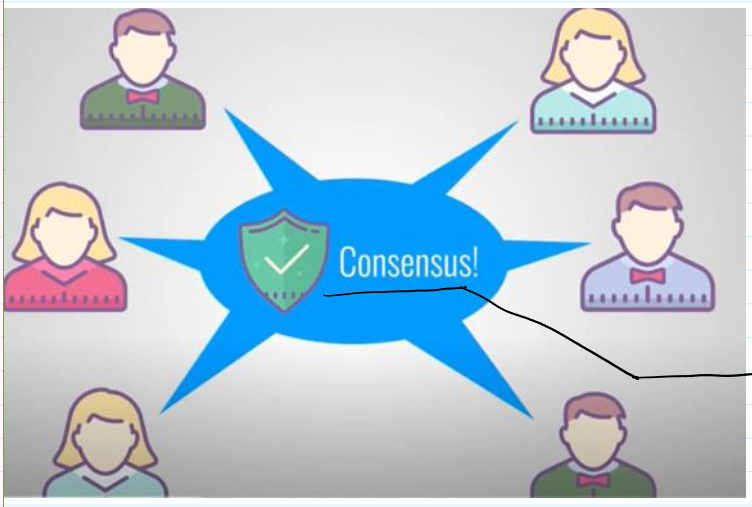


$1K = 2^{10} = 1024$

$1M = 2^{20}$

$1G = 2^{30}$

$1T = 2^{40}$



PoW - Proof-of-Work → Mining

Inventing (reward)

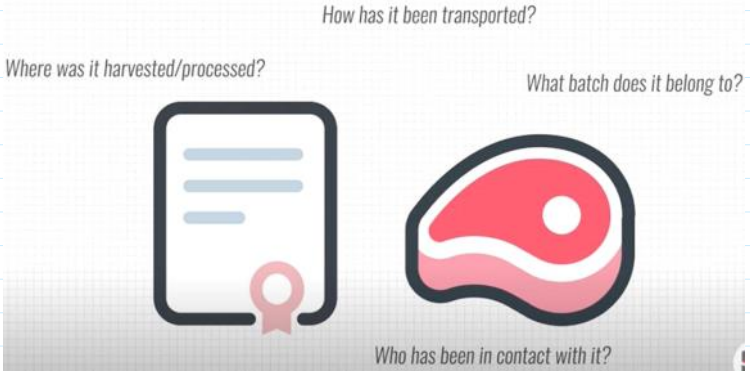
1. To define a rules of block acceptance.
2. To achieve the consensus of block validation in the net.

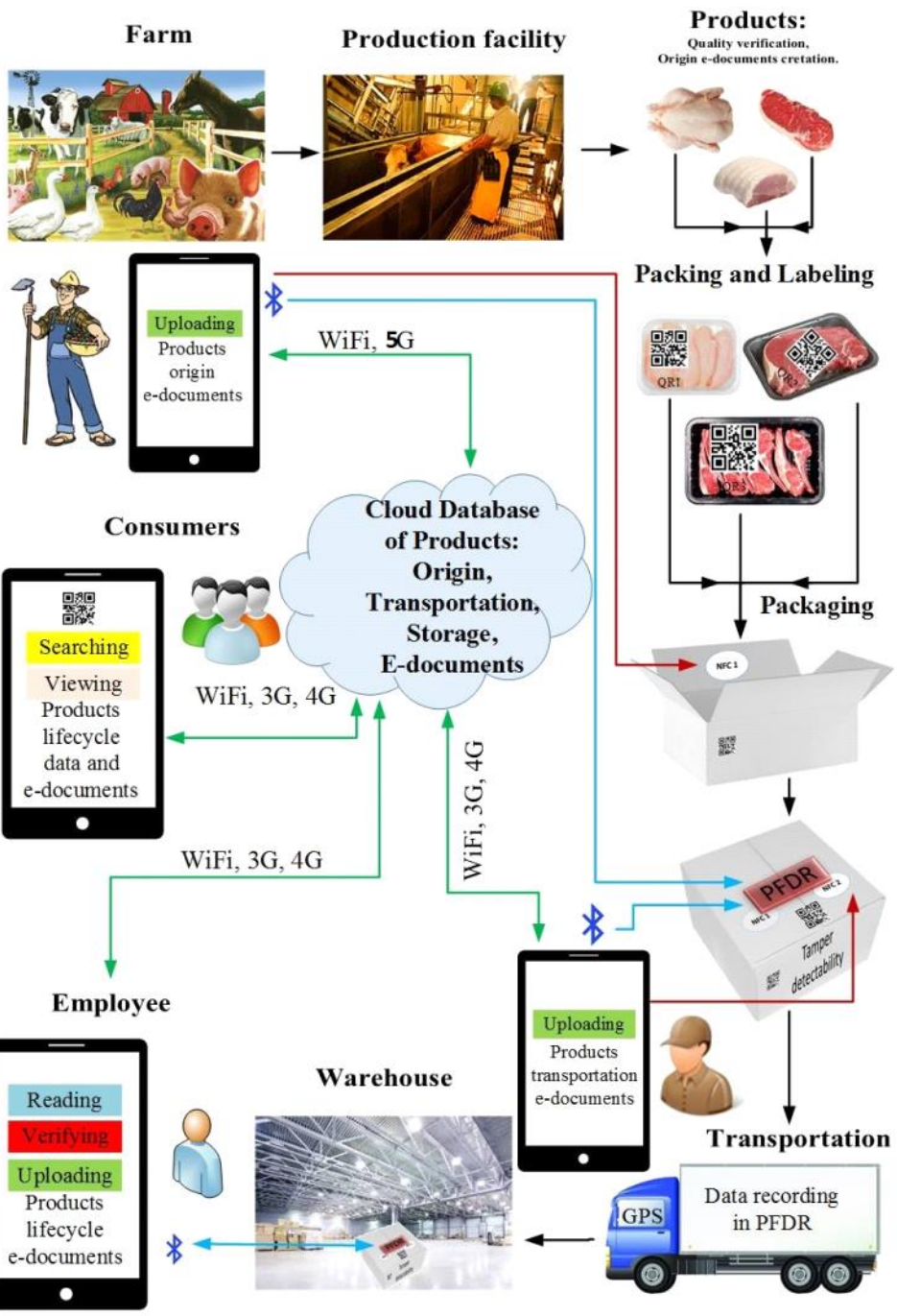
$1 Sat = 10^{-8}$ BTC

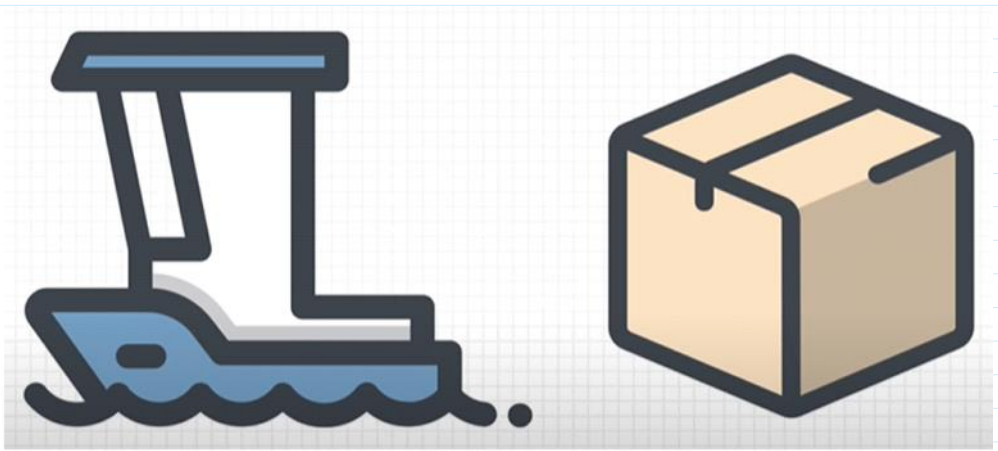
$1 BTC = 100\,000\,000$ Sat

$1\,Sat = 10^{-8}\,BTC$

$1\,BTC = 100\,000\,000\,Sat$







Containers: **IBM** and containers shipping giant **Maersk Group**

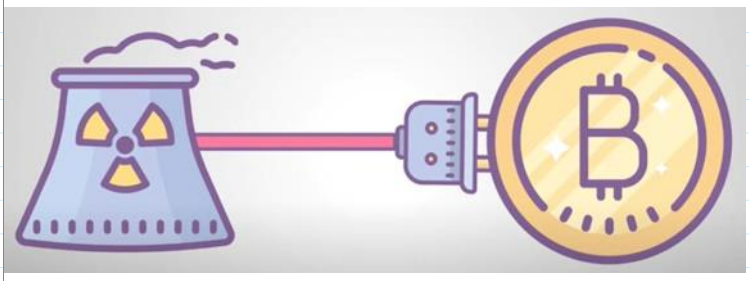
IBM Hyperledger Fabric

Distributed Ledger Technology

Ethereum blockchain

Containers: **IBM** and containers shipping giant **Maersk Group**.
Maersk Group is No 1 in the top 10 transport companies.

ICO - initial coin offer
STO - secure token offer
NFT - non-fungible token offer



PoW - Proof of Work

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

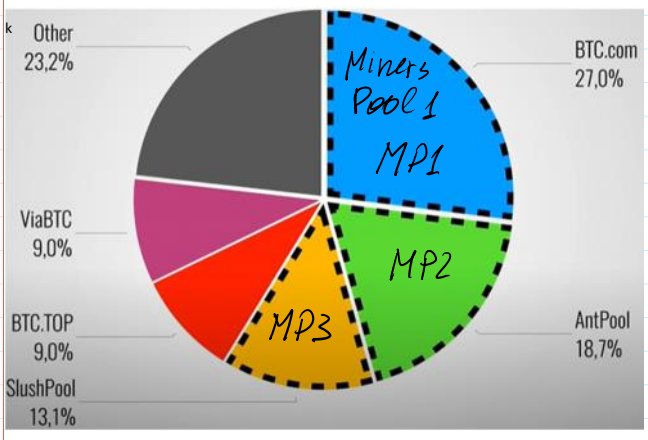
Application Specific Intrgrated Circuits - ASIC --> mining
Farm is using a huge el. (EP) power
[W] - watt
In 1 household EP ~ 5 kW
During 1 hour Energy = 5 kWh
↓
~ 1 Eur

To charge e-vechile 20 - 50 kW
Farm can consume ~ 500 kW - 1 MW
During 1 hour we'll consume Energy = 1 MWh = 1000 kWh

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

1000 kWh * 0,2 € = 2000 €

Till this place

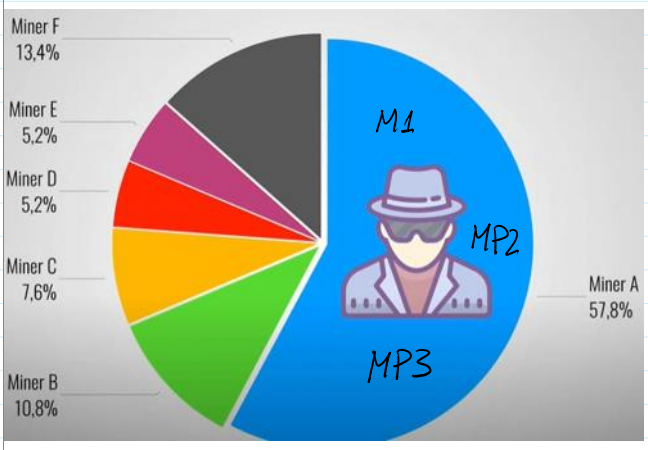


51% Attack

computation power of mining related to the speed of h-values computation $V_h \sim$ THash/sec

E.g. V_h = 1000 THash/sec

Total network has V_h = 1900 TH/s



> 51% Network power

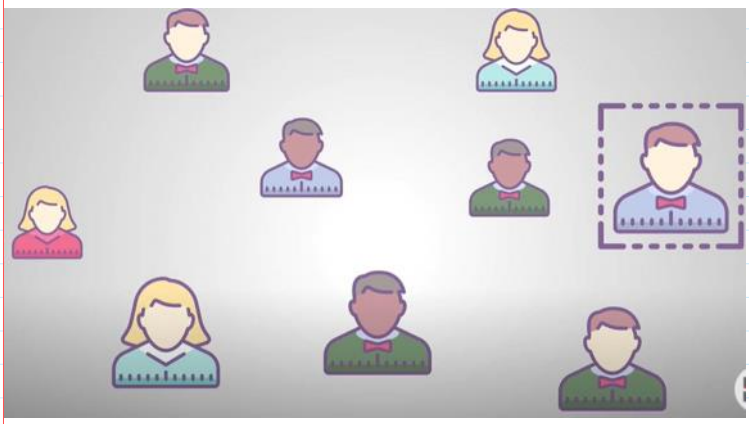
1000 TH/s is more then 51% 1900 TH/s

51% Attack

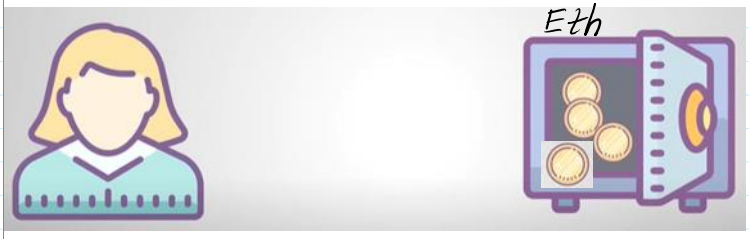
Ethereum 1 Eth ~ 2300 $

↓

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



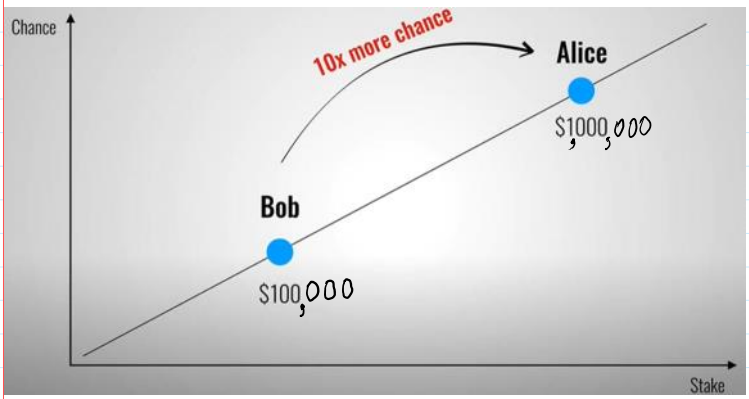
Vitalik Buterin



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

The difficulty of validat. is low →

→ the speed of validation is increased.

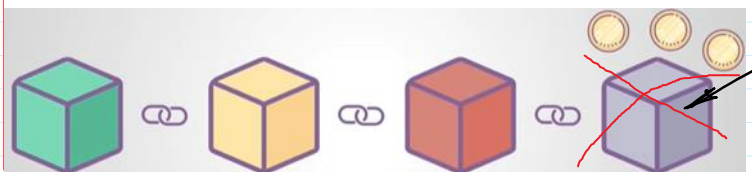


1 Wei = 10^{-18} Eth

1 Eth = 1000 000 000 000 000 000 Wei

To mine a block consisting of a lot of transactions →

→ every transaction has declared a reward in Gas for its validat.

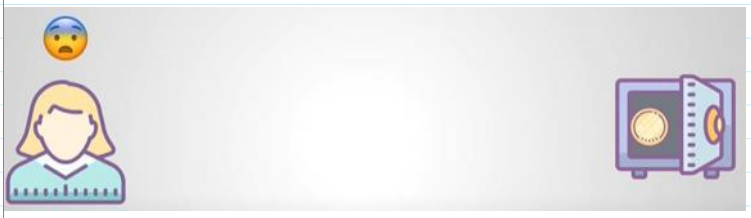


Mistaken validated block

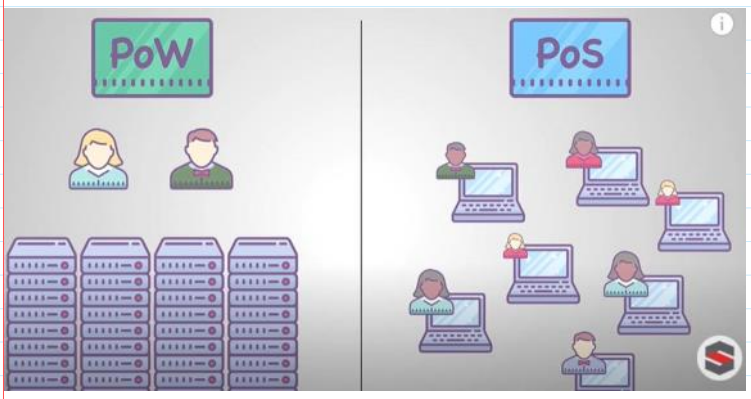
↓ ↓

Intentionally Non-Intentionally

Intentionally Non-Intentionally



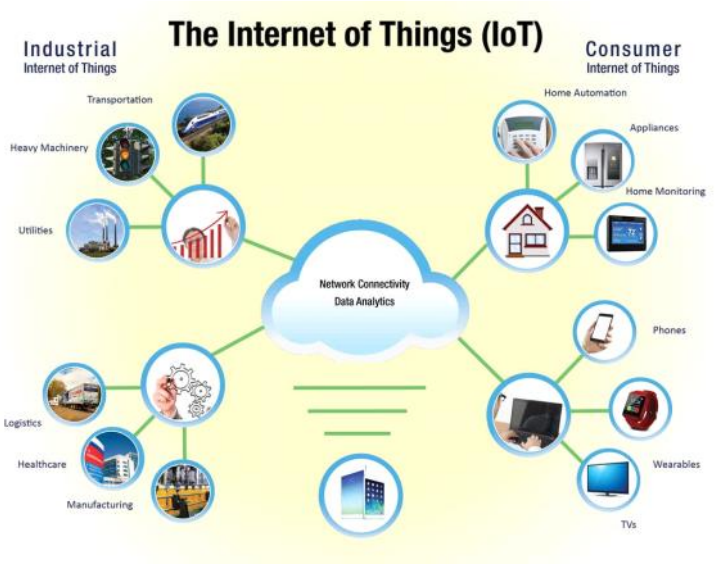
To empty your deposit after some time.



Ethereum 2.0
32 Eth; 1 Eth ~ 140 $

Ethereum, Libra, ... etc.

Fiat currency



< 1000 Tx/s

→ 15 000 Tx/s

ECDSA 512 bits

Max BTC ~ 20 000 000

1 BTC = 10^8 sat

$20 \cdot 10^6 \cdot 10^8 = 20 \cdot 10^{14} = 2000$ Tsat