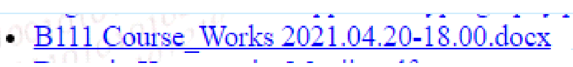
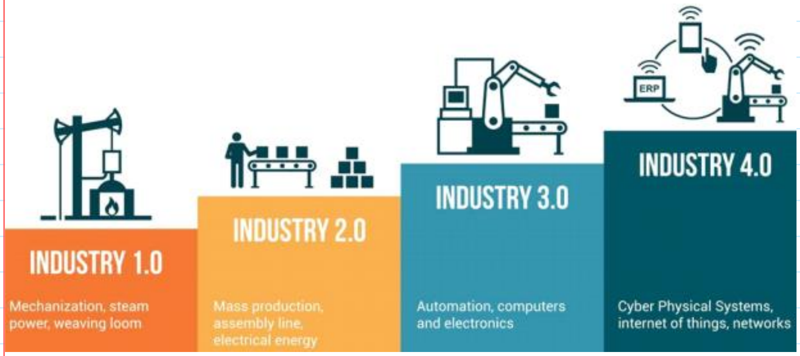
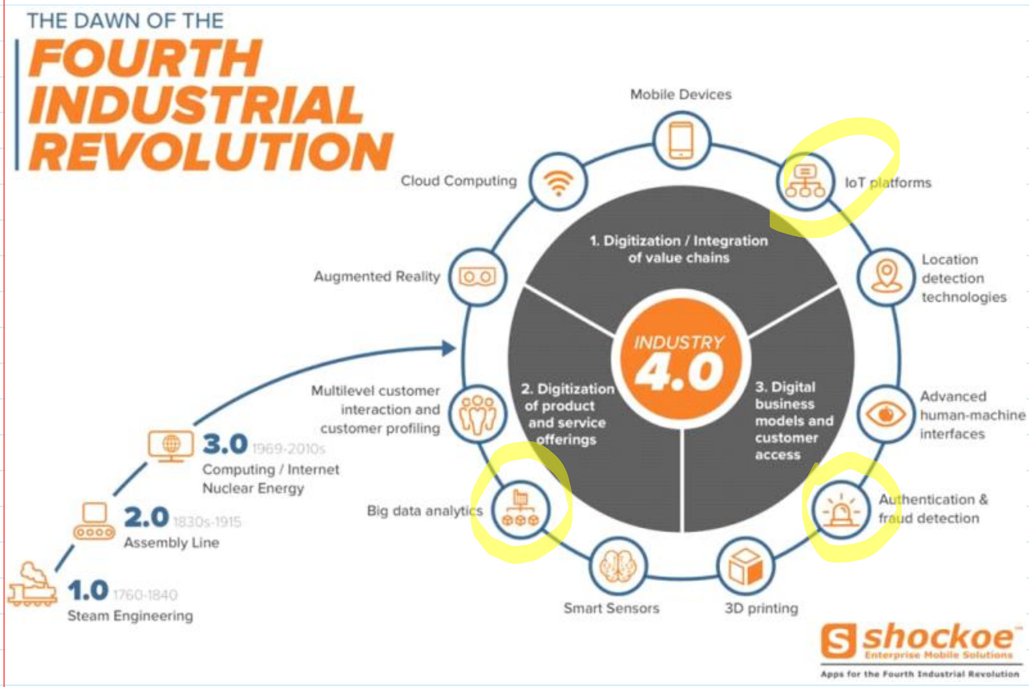
111_014 BlockChain_Overview

Topics an Example of course work
http://crypto.fmf.ktu.lt/xdownload/

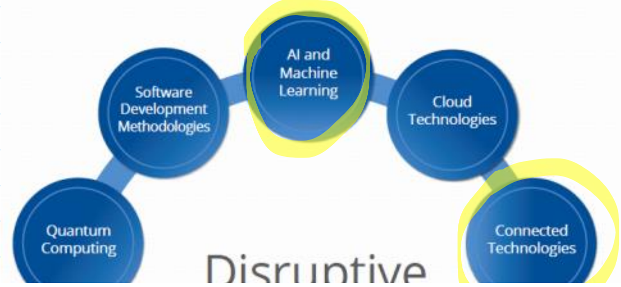

- B111 Course_Works 2021.04.20-18.00.docx

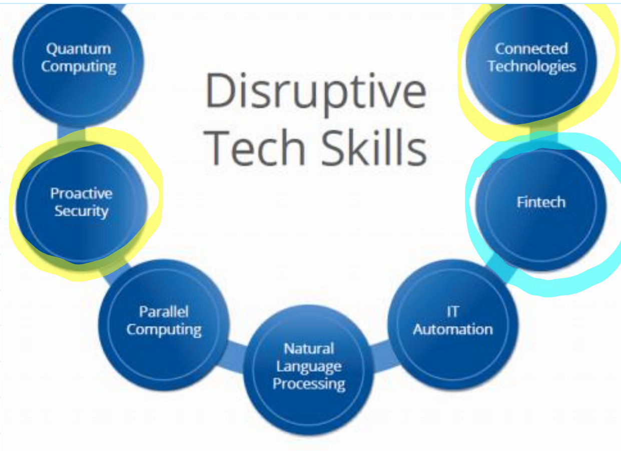
- Example of CourseWork.7z


INDUSTRY 1.0
Mechanization, steam power, weaving loom
INDUSTRY 2.0
Mass production, assembly line, electrical energy
INDUSTRY 3.0
Automation, computers and electronics
INDUSTRY 4.0
Cyber Physical Systems, internet of things, networks
ERP


THE DAWN OF THE
FOURTH INDUSTRIAL REVOLUTION
Mobile Devices
IoT platforms
Location detection technologies
Advanced human-machine interfaces
Authentication & fraud detection
3D printing
Smart Sensors
Big data analytics
Multilevel customer interaction and customer profiling
Augmented Reality
Cloud Computing
1. Digitization / Integration of value chains
2. Digitization of product and service offerings
3. Digital business models and customer access
INDUSTRY 4.0
3.0 1969-2010s
Computing / Internet
Nuclear Energy
2.0 1830s-1915
Assembly Line
1.0 1760-1840
Steam Engineering
shockoe
Enterprise Mobile Solutions
Apps for the Fourth Industrial Revolution

Skills of Mass Disruption Tecnologies
Įgūdžiai Masinio Proveržio Technologijose





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

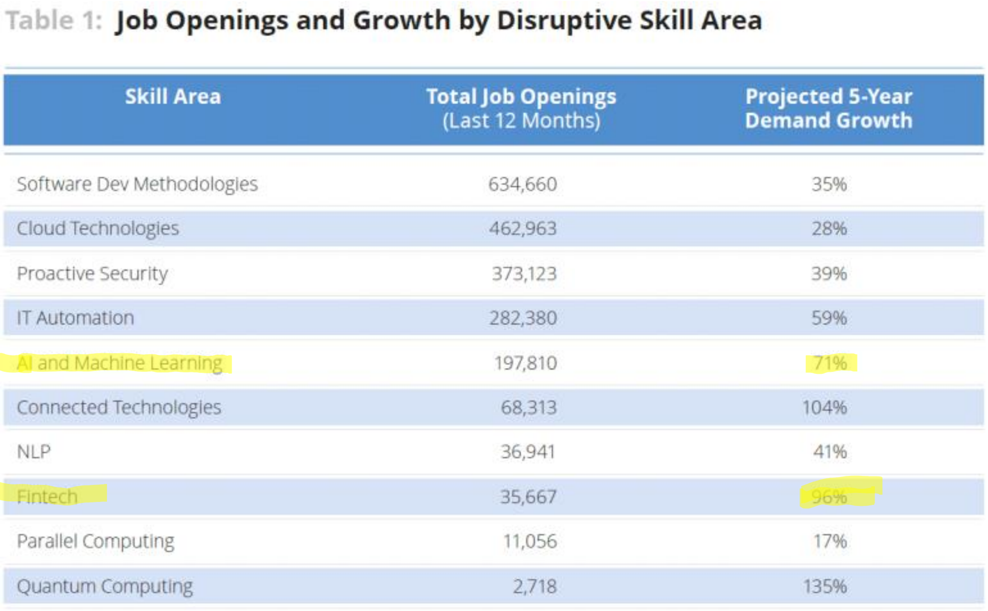


Table 1: **Job Openings and Growth by Disruptive Skill Area**

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%

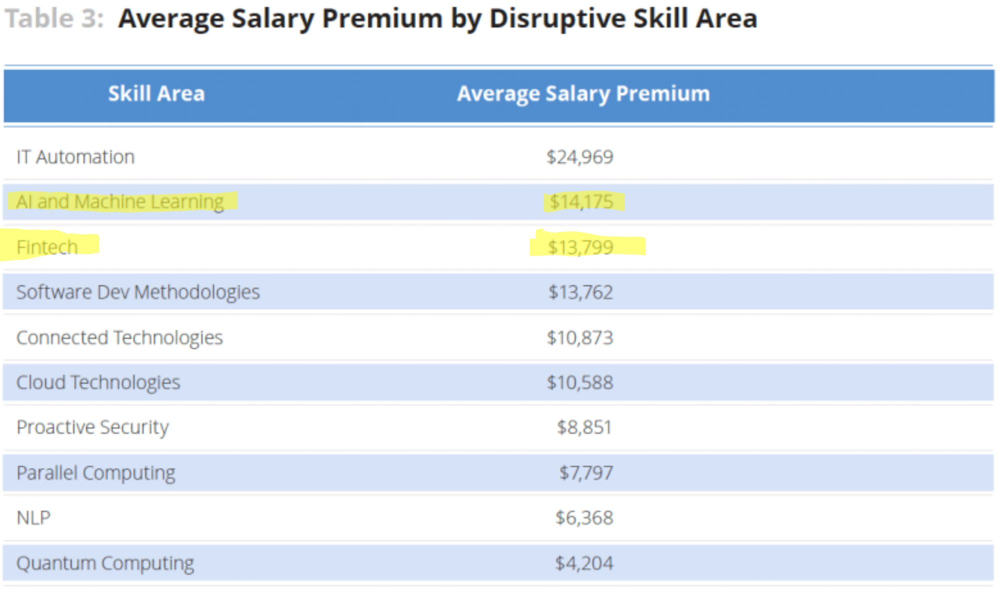
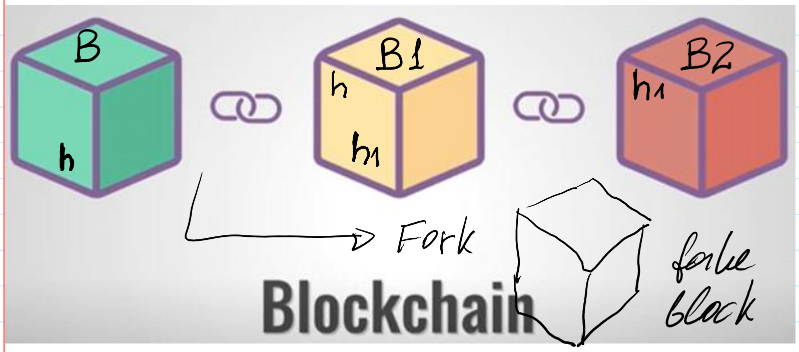


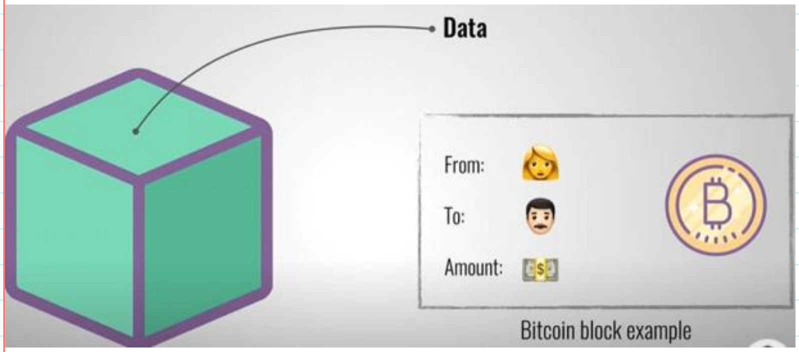
Table 3: **Average Salary Premium by Disruptive Skill Area**

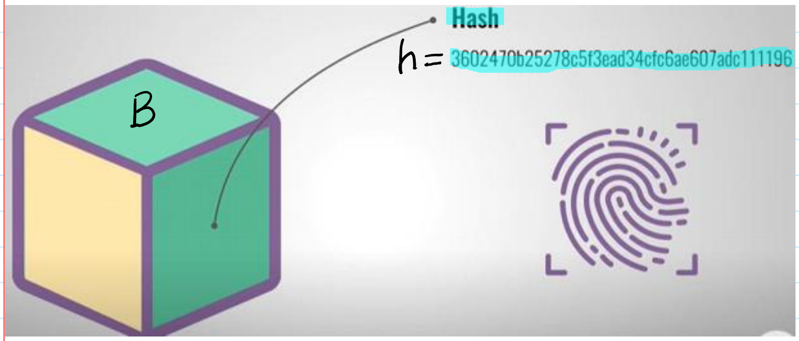
Skill Area	Average Salary Premium
IT Automation	$24,969
AI and Machine Learning	$14,175
Fintech	$13,799
Software Dev Methodologies	$13,762
Connected Technologies	$10,873
Cloud Technologies	$10,588
Proactive Security	$8,851
Parallel Computing	$7,797
NLP	$6,368
Quantum Computing	$4,204

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.



51% of network computing power ⇒ fake chain



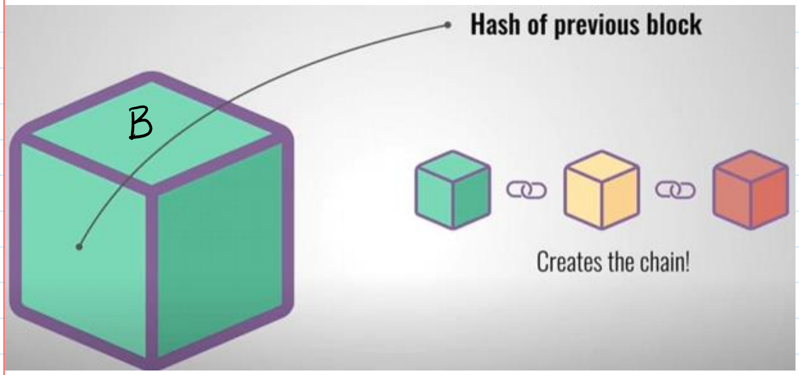


$H(B) = h$; $|h| = 256$ bit

$|B| \sim 1GB$ SHA-256

Finger print

H-function; Message digest



$h \sim 2^{256}$

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

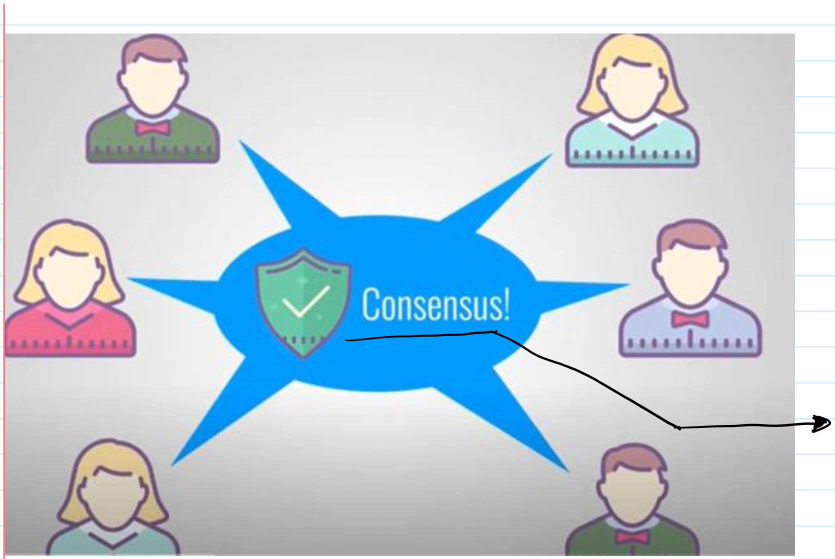
$1M = 2^{20}$

$1G = 2^{30}$

$1T = 2^{40}$

NEMovement

$P \sim 2^{2048}$



PoW - Proof-of-Work → Mining

Insenting (reward)

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

Block mining. To mine a B1 miner must compute its h- value consisting of certain number of leading hexadecimal zeroes in this h-value.

$B1 = ' h \,||\, List\ of\ Transactions \,||\, \dots \,||\, complexity \,||\, nonce '$

Complexity defines the number of leading hexadecimal zeroes in h-value of the block.

Currently complexity $= 18$ hex num. $\Rightarrow 72$ bits.

If $h = SHA\text{-}256(B1) \Rightarrow |h| = 256$ bits $\Rightarrow 64$ hex numb.

$$Pr(\text{of mining}) = \frac{\text{Number of suitable } h\text{-values}}{\text{Number of all } h\text{-values}} = \frac{NSh}{NAh}$$

NSh : $256 - 72 = 184$ bits $\Rightarrow NSh = 2^{184}$

NAh : represented by the number with 256 bits. $\Rightarrow NAh = 2^{256}$

$$Pr(\text{of mining}) = \frac{2^{184}}{2^{256}} = 2^{-72}.$$

Mining requiet a lot of Terra hashes per second - Ths

These trials are performed by changing nonce value

$nonce := nonce_0 \rightarrow h_1 = SHA\text{-}256(B1)$

$nonce := nonce + 1 \rightarrow h_2 = \dots$

Declaration of mined block : miner presents B1 and nonce Value to the net ⇒ Net verifies if SHA-256(B1) has 18 leading hex numbers ⇒ If Yes block is accepted by the net.

Bitcoin

By “Satoshi Nakamoto”

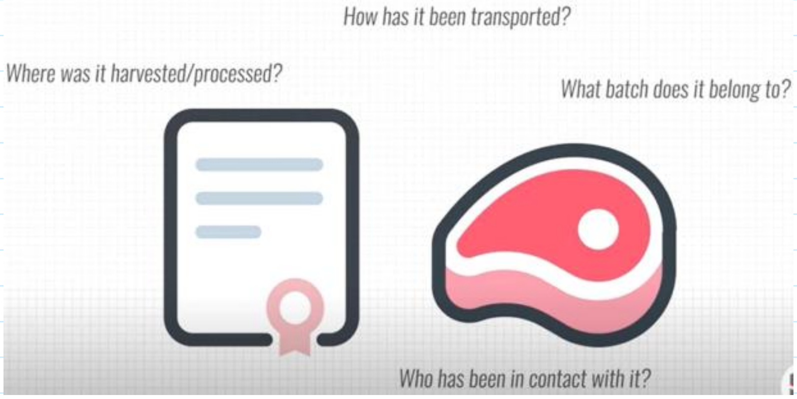
1 Sat = 10^{-8} BTC

1 BTC = 100 000 000 Sat

Creating a blockchain with Javascript (Blockchain, part 1)

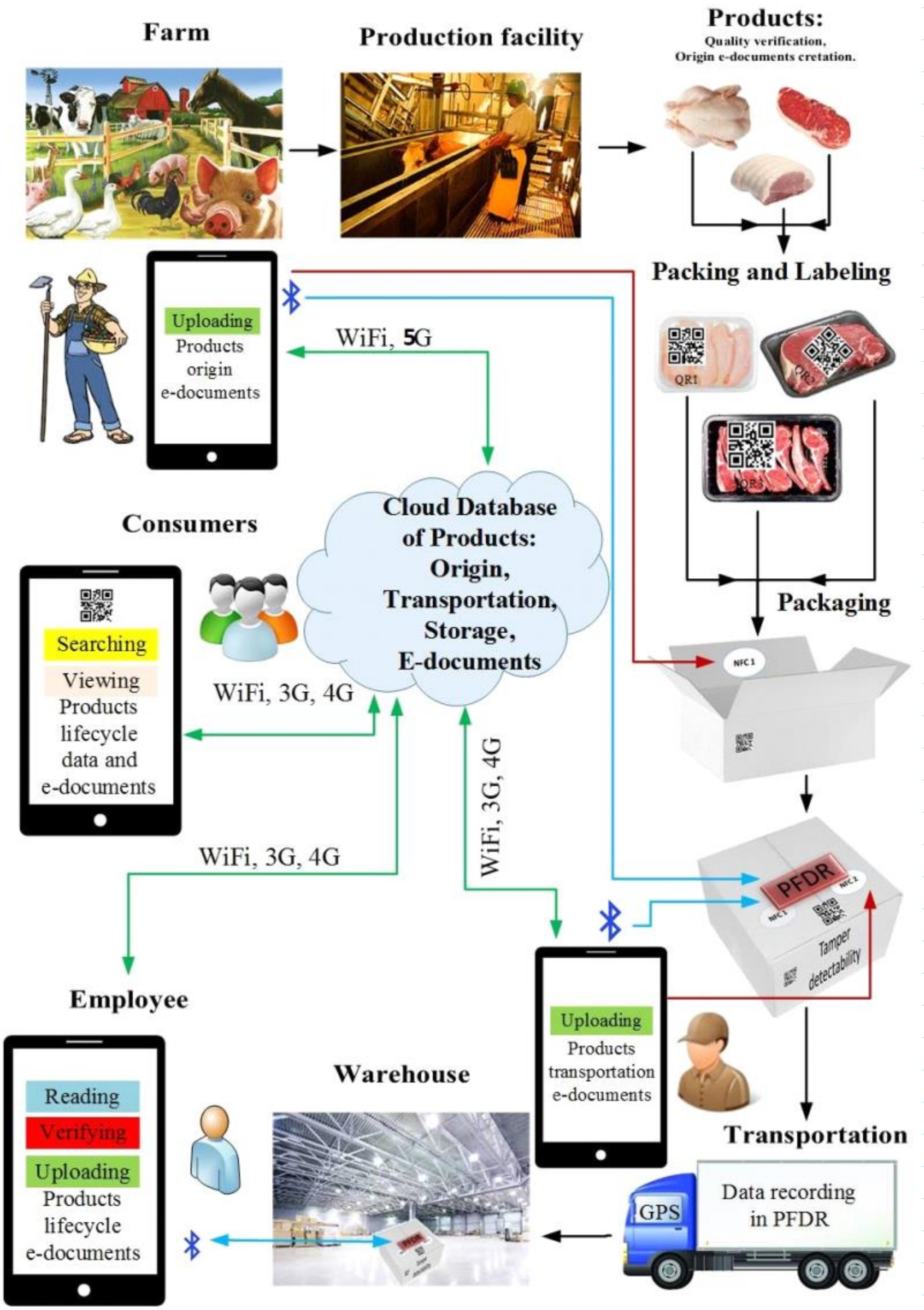
Create a blockchain with JavaScript

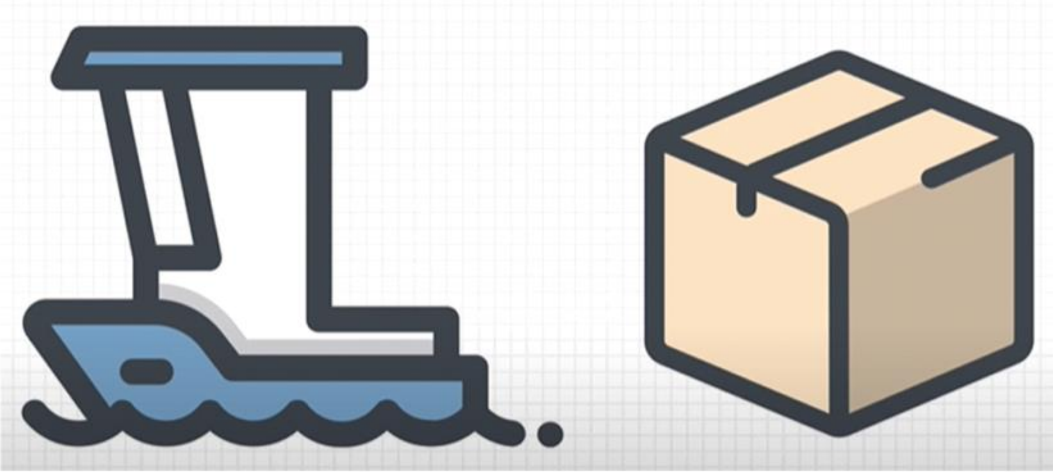
Food industry



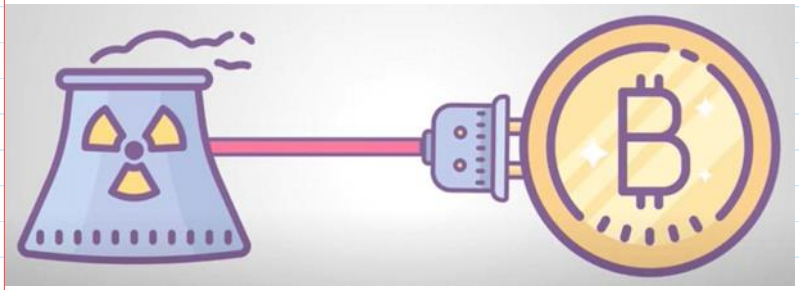
How has it been transported?
Where was it harvested/processed?
What batch does it belong to?
Who has been in contact with it?

H2020

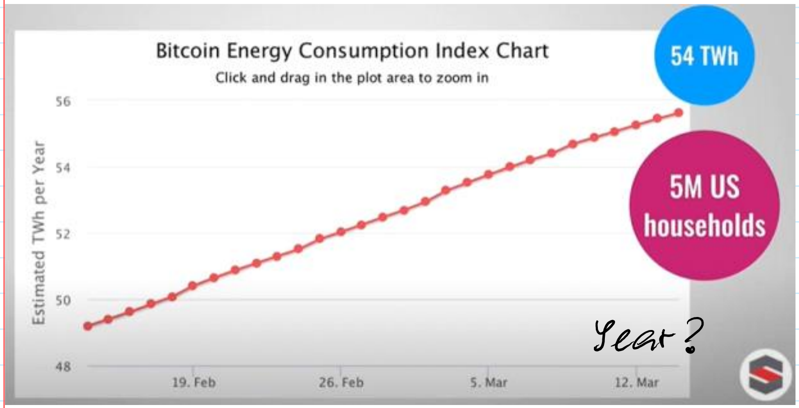

Farm
Production facility
Products:
Quality verification,
Origin e-documents cretation.
Packing and Labeling
QR1
QR2
QR3
Uploading
Products
origin
e-documents
WiFi, 5G
Cloud Database
of Products:
Origin,
Transportation,
Storage,
E-documents
Consumers
Searching
Viewing
Products
lifecycle
data and
e-documents
WiFi, 3G, 4G
Packaging
NFC 1
WiFi, 3G, 4G
WiFi, 3G, 4G
PFDR
NFC 1
NFC 2
Tamper
detectability
Employee
Uploading
Products
transportation
e-documents
Warehouse
Transportation
Reading
Verifying
Uploading
Products
lifecycle
e-documents
GPS
Data recording
in PFDR



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



PoW – Proof of Work



Electric energy consumption kWh

1 kWh ~ 0.13 Eur.

$54\,TWh = 54 \cdot 10^{9}\,kWh$

$1\,TWh = 10^{12}\,Wh$

Power: W, kW, GW

Application Specific Intrgrated Circuits - ASIC --> mining

Farm is using a huge el. power (EP)

ASIC --> mining

Farm is using a huge el. (EP) power

[W] - watt

In 1 hosehold EP ~ 5 kW

During 1 hour Energy = 5 kWh

↓

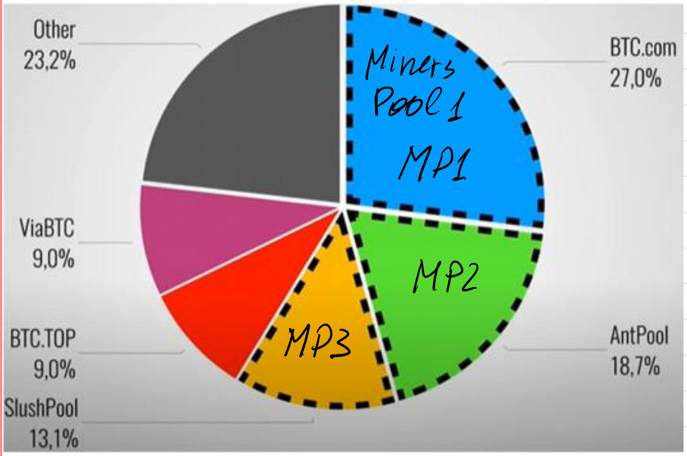
0,65 €

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 * 0,13 € = 130 €

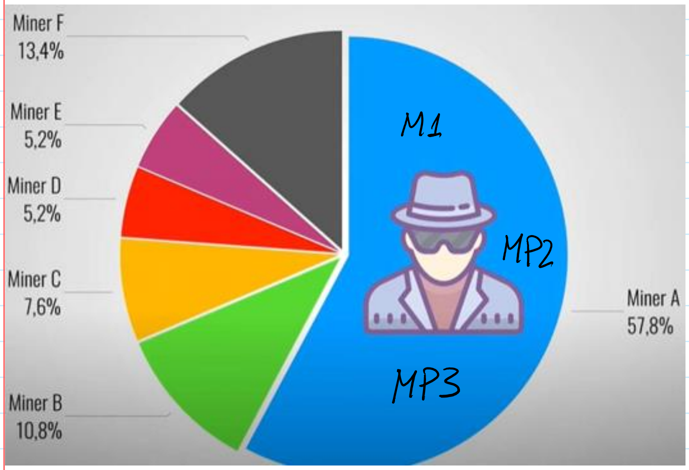


51% Attack

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

E.g. V_h = 1000 THash/sec

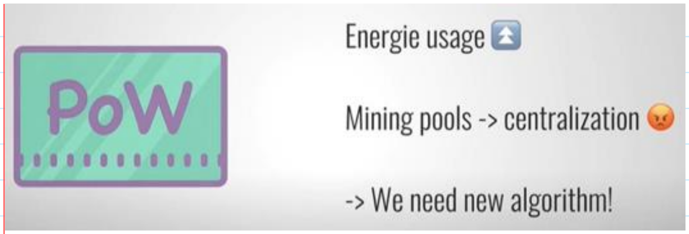
Total network is has V_h = 1900 TH/s



> 51% Network power

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

51% Attack

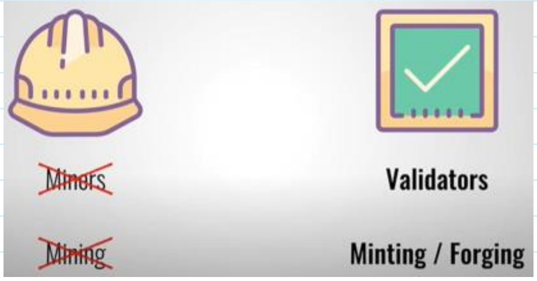


Energie usage ⏫

Mining pools -> centralization 😡

-> We need new algorithm!

Proof-of-stake

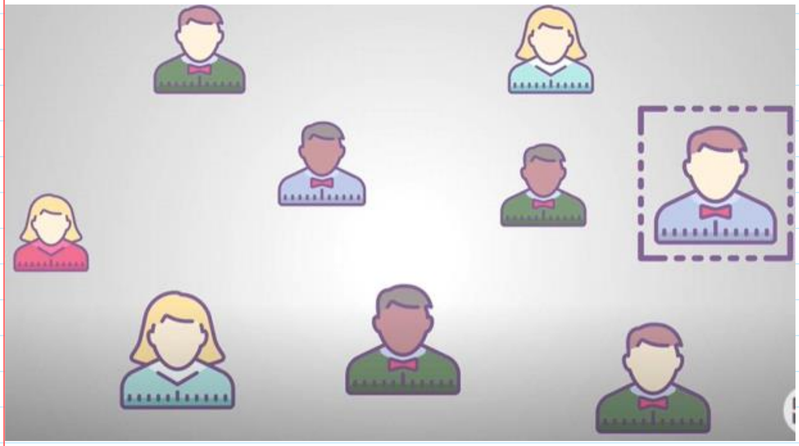


~~Miners~~ Validators

~~Mining~~ Minting / Forging

Ethereum ↓ 1 Eth ~ 2300 $

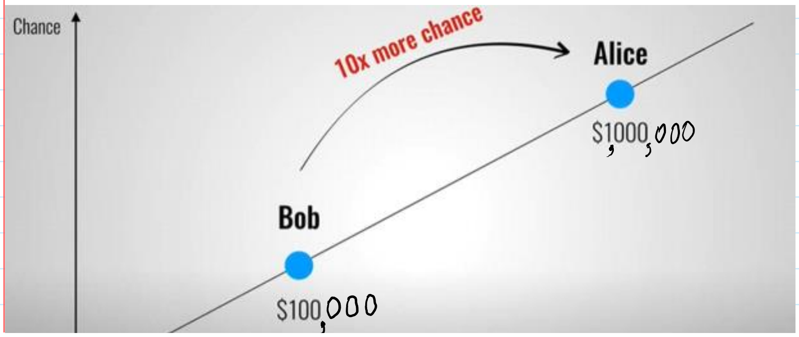
The name of cryptocurrency in Ethereum blockchain is named as Ether – Eth



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.

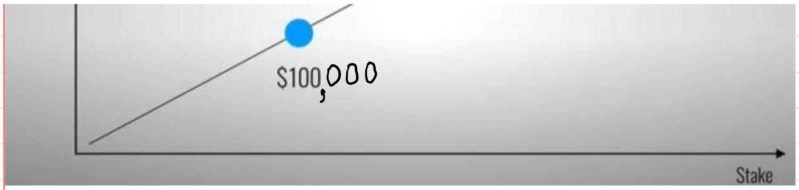


1 Wei = 10^{-18} Eth

1 Eth = 1000 000 000 000 000 000 Wei

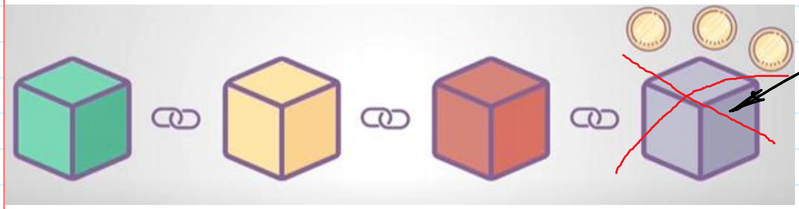
To mine a block consisting of a lot of transactions →

→ every transaction has declared



a lot of transactions →

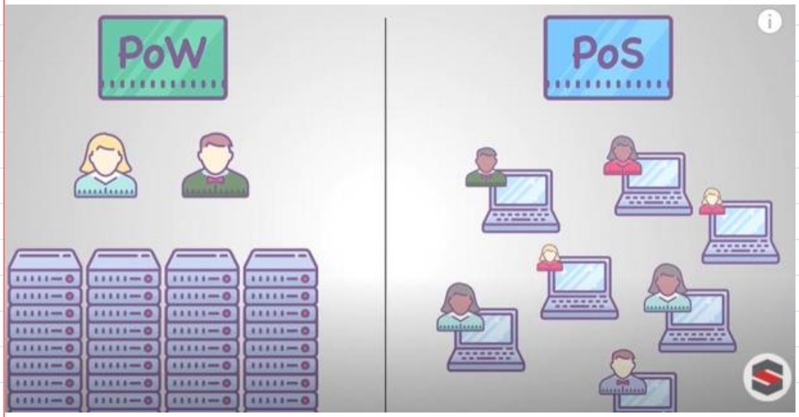
→ every transaction has declared a reward in Gas for its validat.



Mistaken validated Block

Intentionally   Non-Intentionally

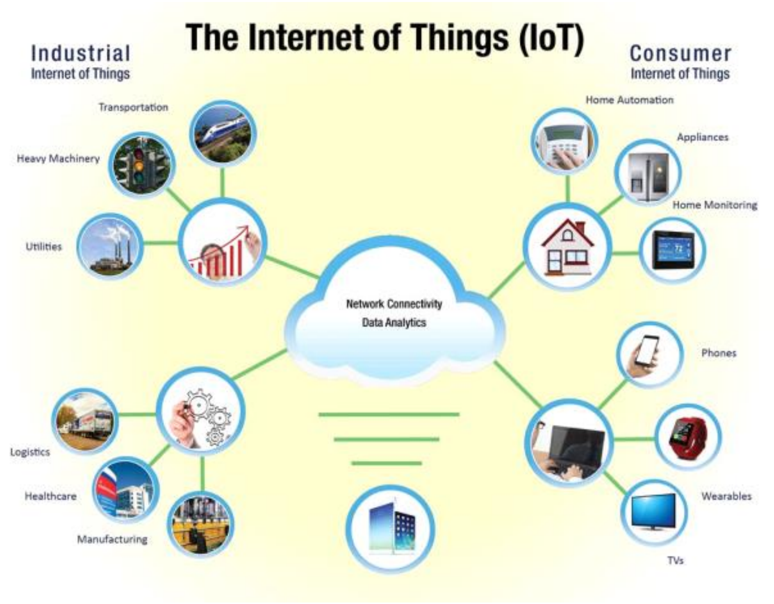
To empty your deposit after some time.



Ethereum 2.0

32 Eth ;   1 Eth ~ 140 $

Ethereum, Libra, ... etc.


The Internet of Things (IoT)
Industrial
Internet of Things
Consumer
Internet of Things
Transportation
Heavy Machinery
Utilities
Home Automation
Appliances
Home Monitoring
Network Connectivity
Data Analytics
Phones
Wearables
TVs
Logistics
Healthcare
Manufacturing