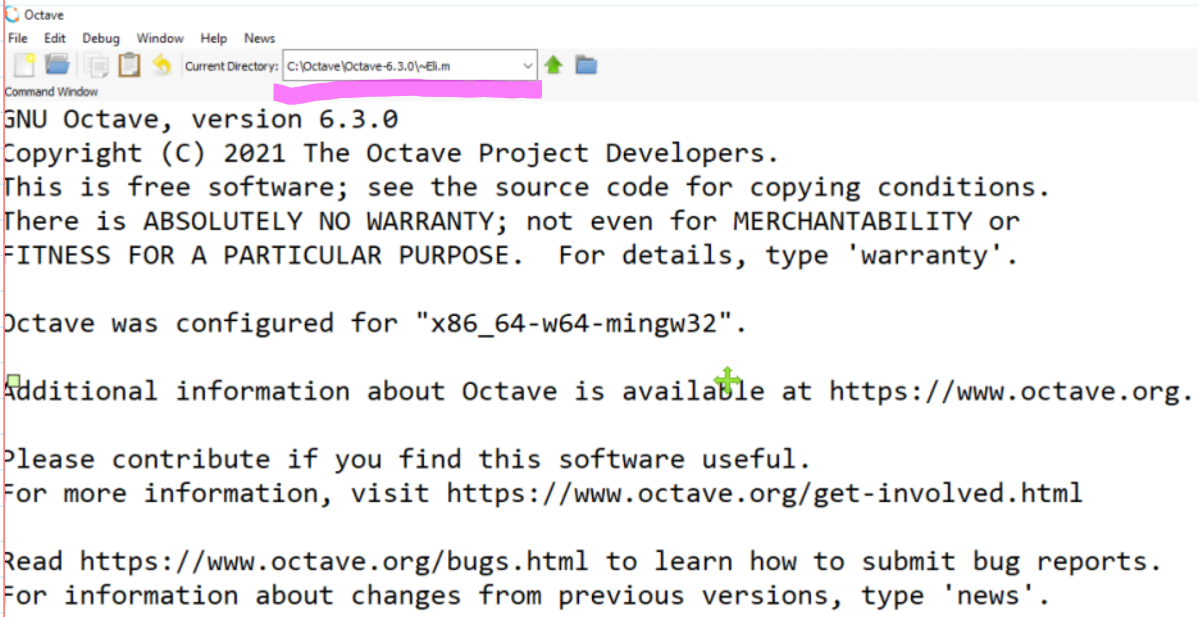
http://crypto.fmf.ktu.lt/
http://crypto.fmf.ktu.lt/telekonf/archyvas/M100%20KriptoSistemos/KS%202022/

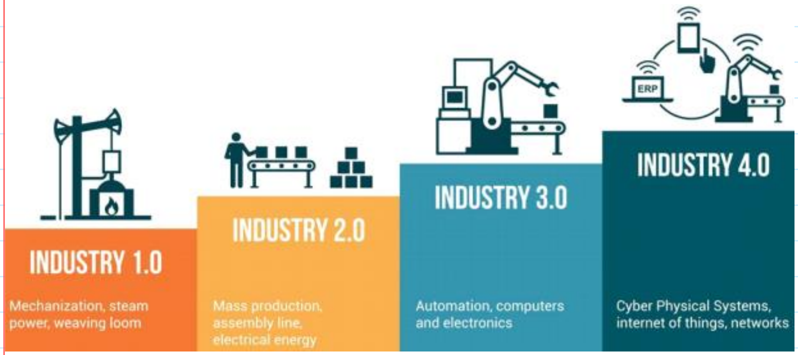
http://crypto.fmf.ktu.lt/xdownload/

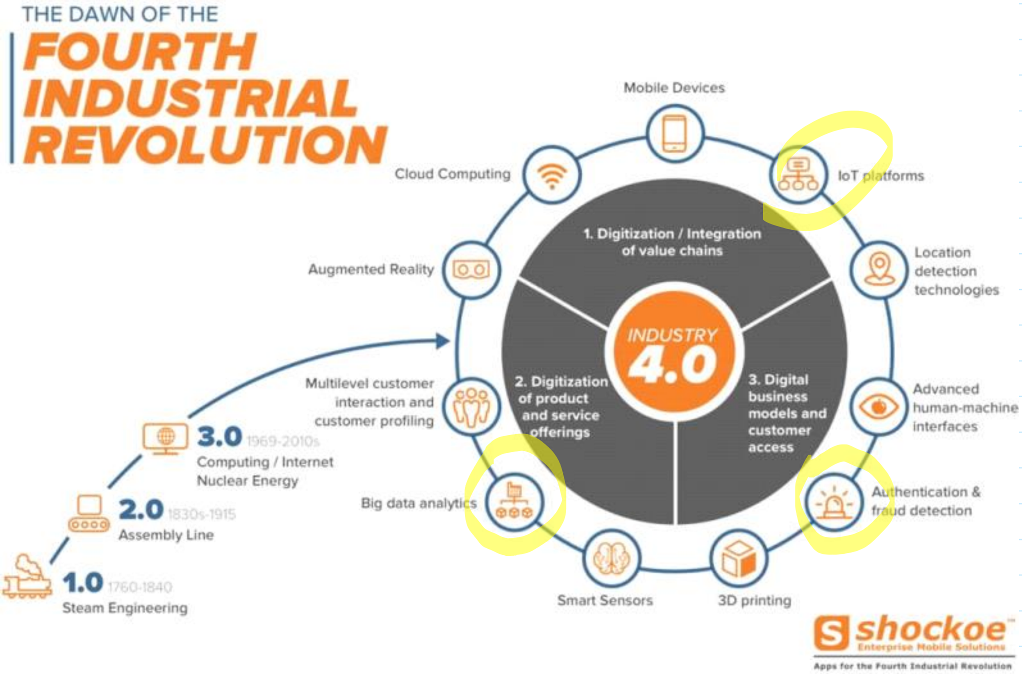
- octave-6.3.0-w64-installer.exe ✓
- octave.m.7z



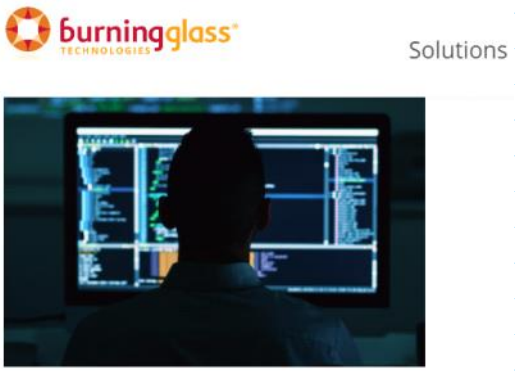
Current Directory: C:\Octave\Octave-6.3.0\~Eli.m

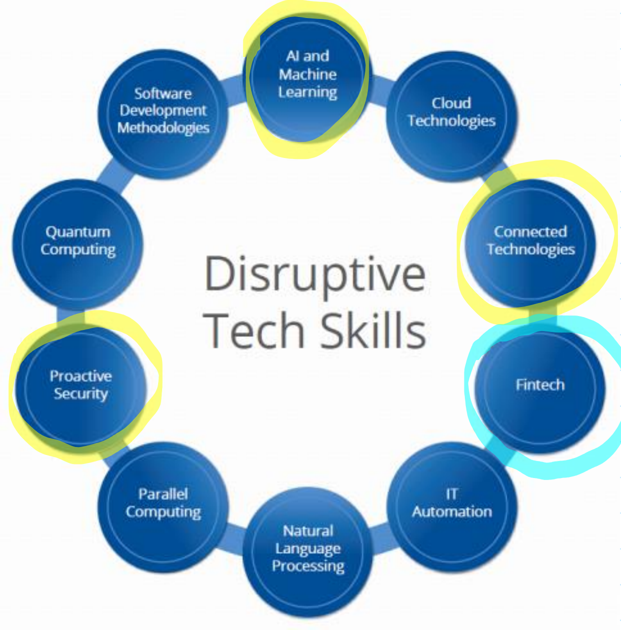
```
GNU Octave, version 6.3.0
Copyright (C) 2021 The Octave Project Developers.
This is free software; see the source code for copying conditions.
There is ABSOLUTELY NO WARRANTY; not even for MERCHANTABILITY or
FITNESS FOR A PARTICULAR PURPOSE.  For details, type 'warranty'.

Octave was configured for "x86_64-w64-mingw32".

Additional information about Octave is available at https://www.octave.org.

Please contribute if you find this software useful.
For more information, visit https://www.octave.org/get-involved.html

Read https://www.octave.org/bugs.html to learn how to submit bug reports.
For information about changes from previous versions, type 'news'.
```


ERP
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


THE DAWN OF THE
FOURTH INDUSTRIAL REVOLUTION
Mobile Devices
IoT platforms
Cloud Computing
Location detection technologies
Augmented Reality
1. Digitization / Integration of value chains
INDUSTRY 4.0
2. Digitization of product and service offerings
3. Digital business models and customer access
Advanced human-machine interfaces
Multilevel customer interaction and customer profiling
Big data analytics
Authentication & fraud detection
Smart Sensors
3D printing
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**.

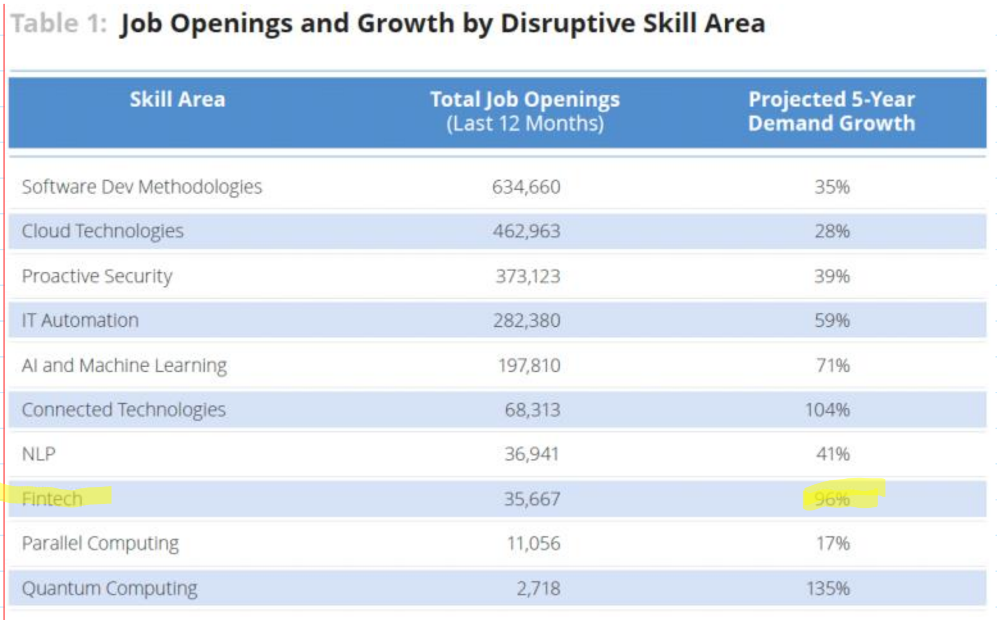


Table 1: **Job Openings and Growth by Disruptive Skill Area**

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%

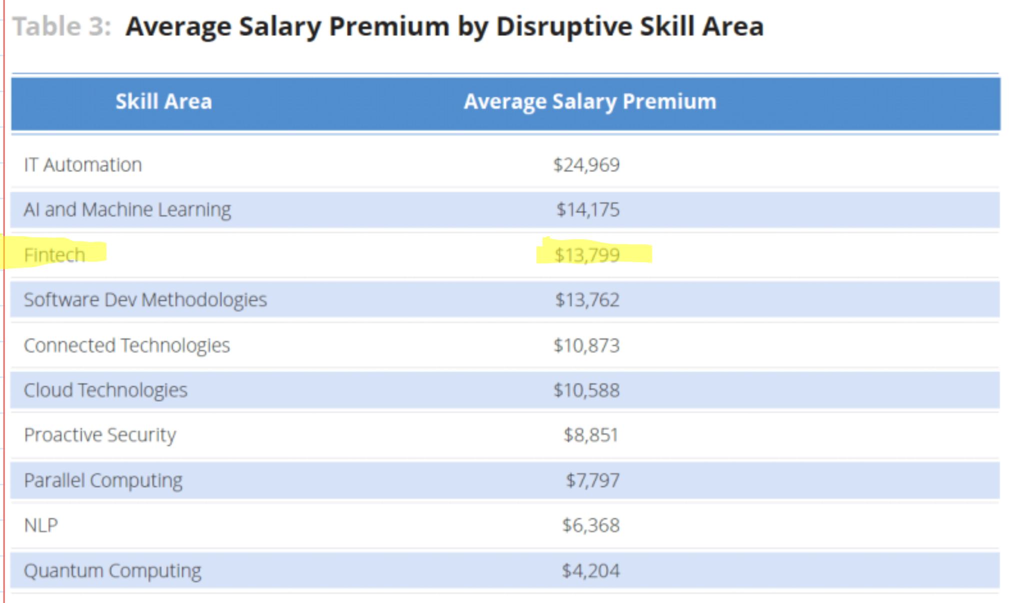


Table 3: **Average Salary Premium by Disruptive Skill Area**

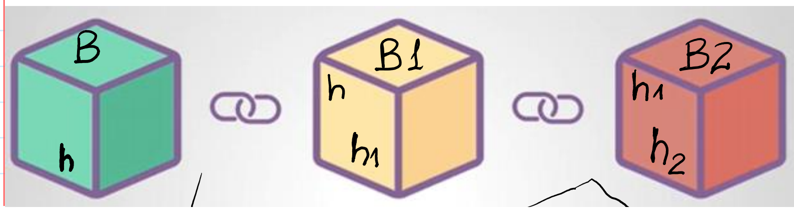
Skill Area	Average Salary Premium
IT Automation	$24,969
AI and Machine Learning	$14,175
Fintech	$13,799
Software Dev Methodologies	$13,762
Connected Technologies	$10,873
Cloud Technologies	$10,588
Proactive Security	$8,851
Parallel Computing	$7,797
NLP	$6,368
Quantum Computing	$4,204

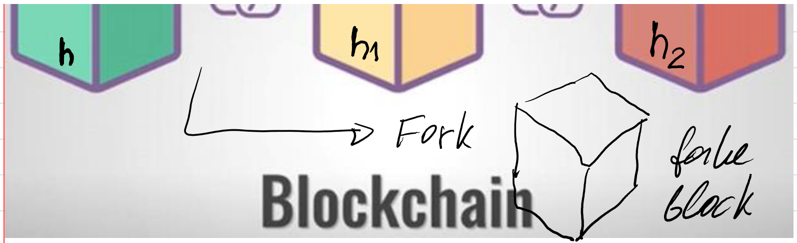
Students and Job Seekers.

Identify and Learn High-Value Disruptive Skills.

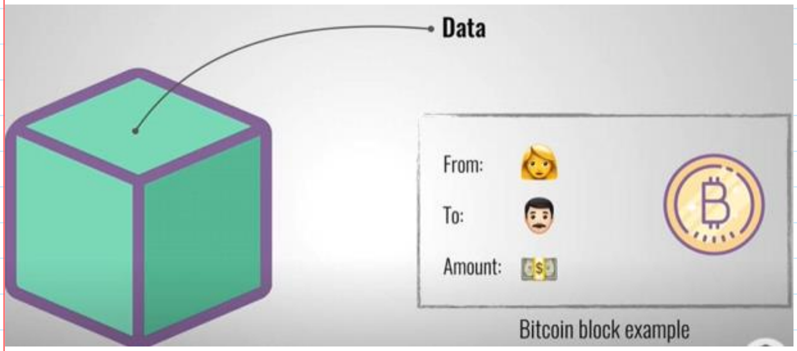
The disruptive tech skills are growing rapidly and can lead to significant salary boosts.

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.

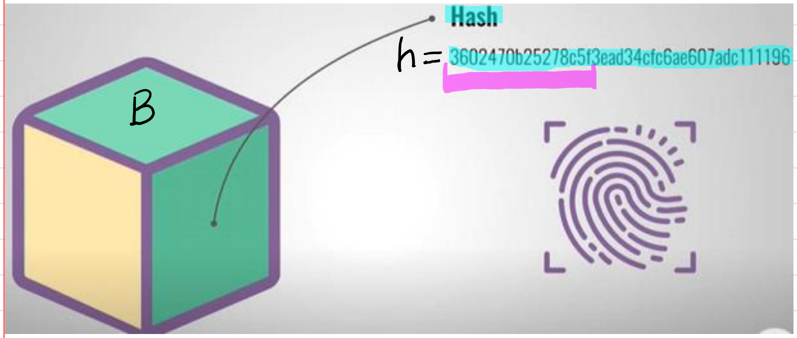




51% of network computing power ⇒ fake chain



From: 👩
To: 👨
Amount: 💵

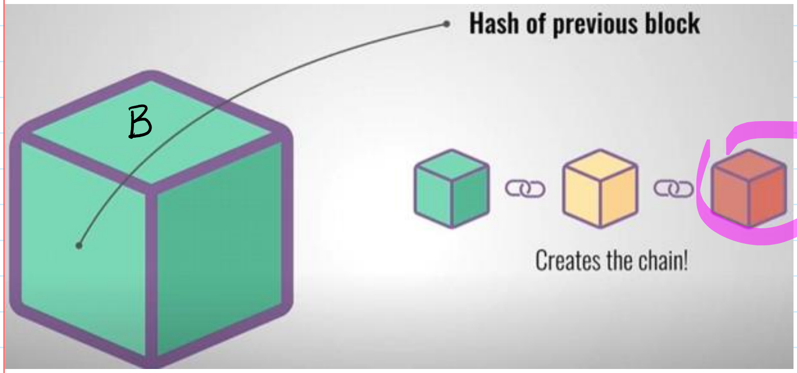


$H(B) = h$; $|h| = 256$ bit

$|B| \sim 1GB$

Finger print

H-function; Message digest



$h \sim 2^{256}$

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

$1M = 2^{20}$

$1G = 2^{30}$

$1T = 2^{40} - 1$

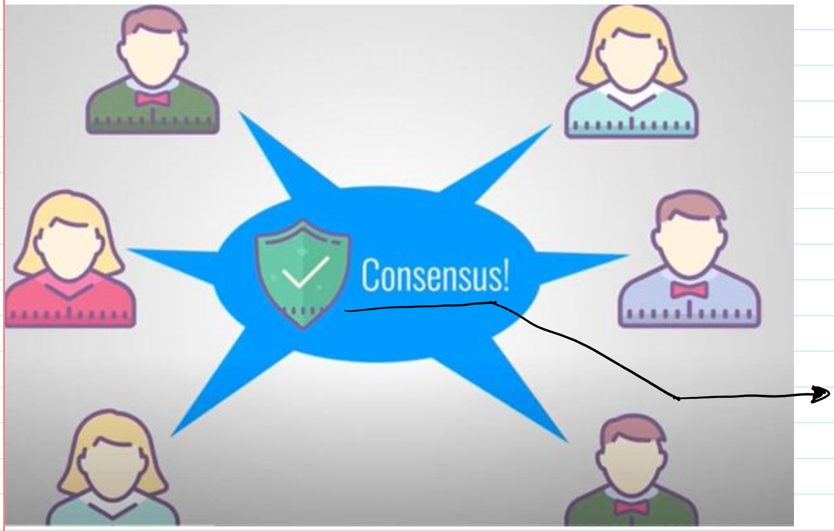
$P \sim 2^{2048}$

```
>> 2^28-1
ans = 2.6844e+08
>> int64(2^28-1)
ans = 268435455
>> dec2bin(ans)
ans = 1111111111111111111111111111
```

In our case we will use

$p \sim 2^{28}$; $|p| = 28$ bits arithm.

PoW - Proof-of-Work → Mining



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.

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

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

Creating a blockchain with Javascript (Blockchain, part 1)

Create a blockchain with JavaScript

14:52

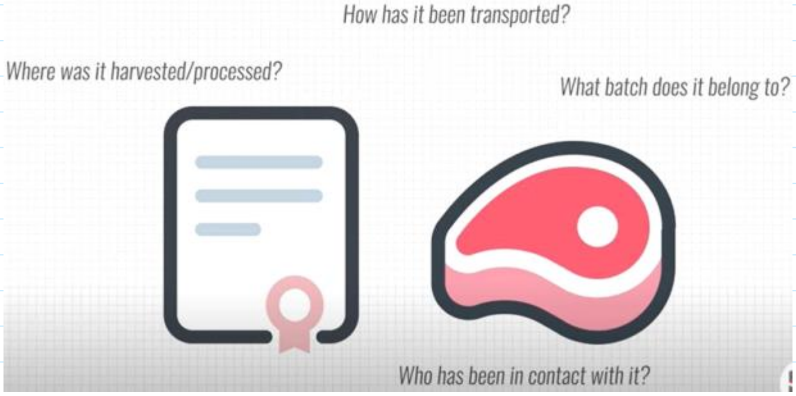
Go ← Moodle

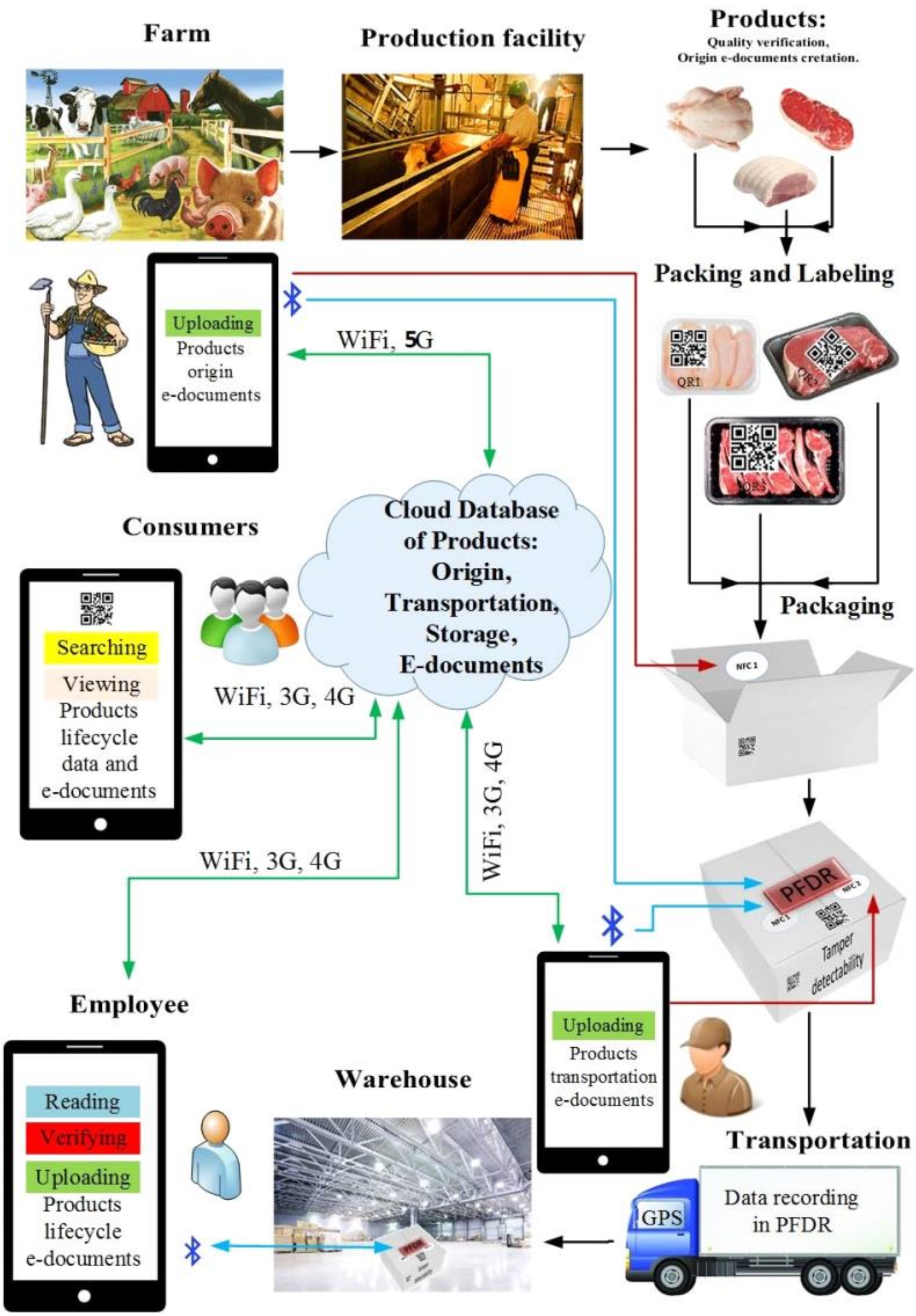
↕

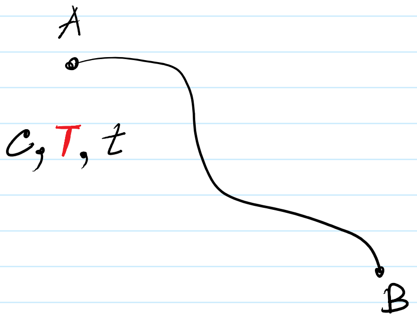
Python

Security programming

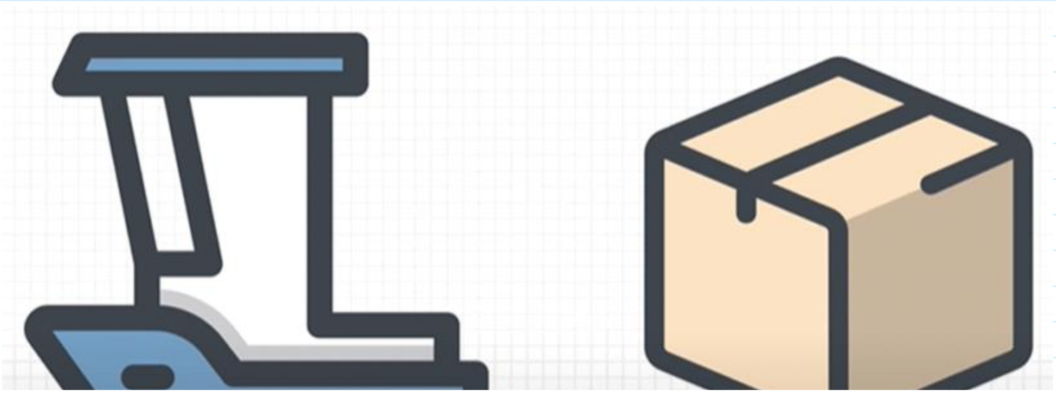
Blockchain → Solidity


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





IBM Food Trust

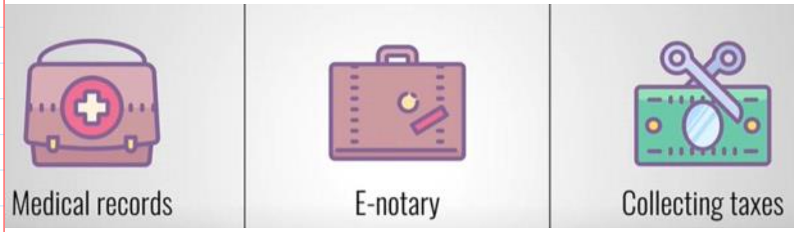


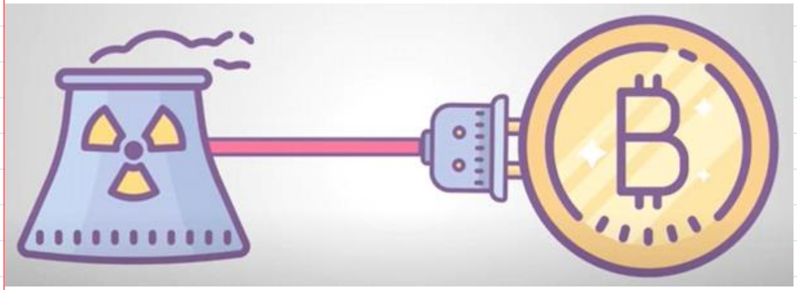
IBM Hyperledger
Fabric
Distributed Ledger
Technology
Permissioned

Permissioned Blockchain

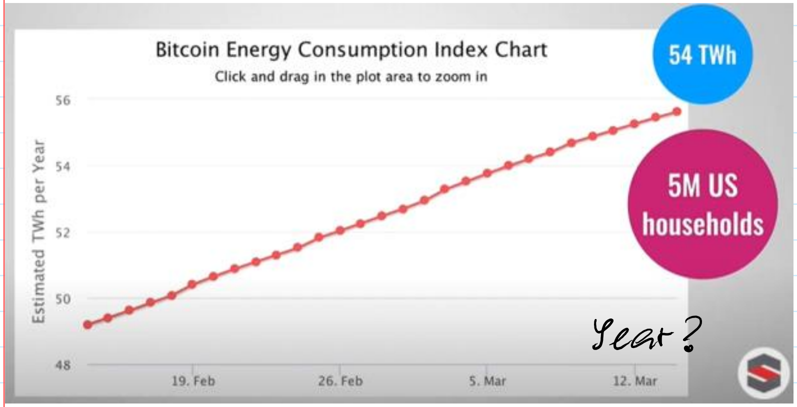
Containers: **IBM** and containers shipping giant **Maersk Group**.
Maersk Group is No 1 in the top 10 transport companies.

3 stud. : IBM DLT vs Ethereum Blockchain





PoW – Proof of Work



Electric energy consumption kWh

1 kWh ~ 0,13 Eur.

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

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

Application Specific Intrgrated Circuits - ASIC --> mining

Farm is using a huge el. power (EP)

[W] – watt

In 1 hosehold EP ~ 5 kW

During 1 hour Energy = 5 kWh

In 1 hosehold EP ~ 5 kW

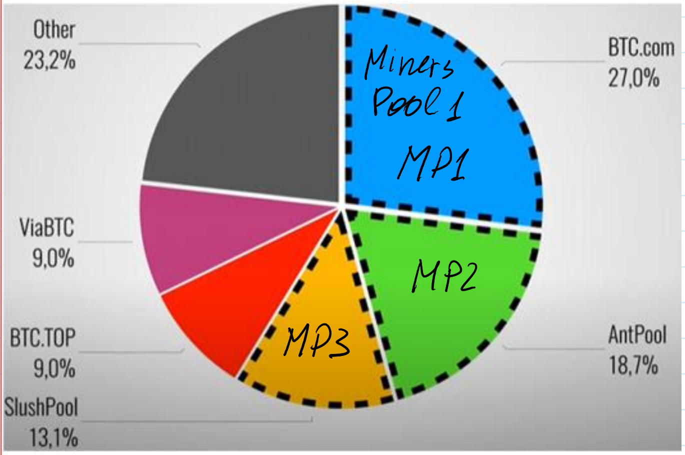
During 1 hour Energy = 5 kWh
↓
0,65 €

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 €

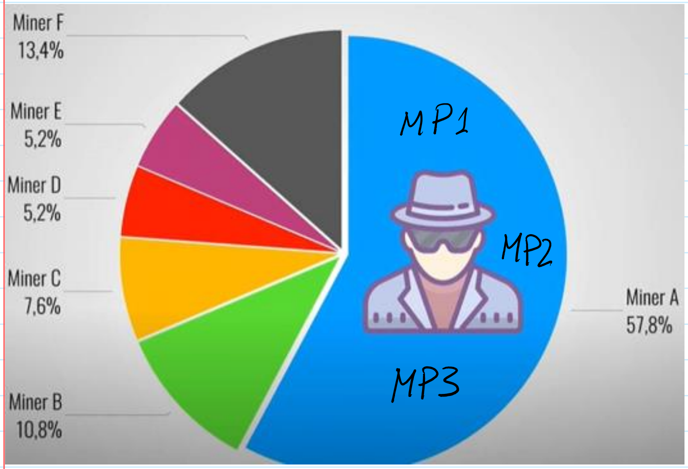


51% Attack

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

E.g. V_h = 1000 THash/sec

Total network has V_h = 1900 TH/s

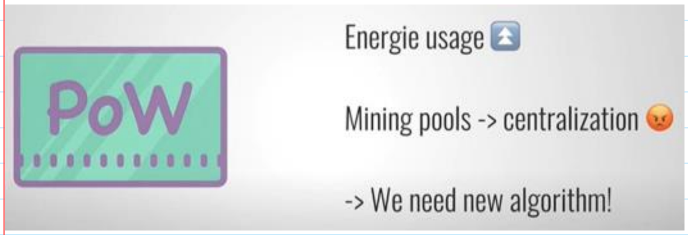


> 51% Network power

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

51% Attack

From Laurynas Veščiūnas to Everyone 06:20 PM
https://batcoinz.com/50-landfills-mining-bitcoin-a-zero-emission-bitcoin-network/
čia straipsnis, kur praeitą kartą minėjau dėl BTC kasimo



Energie usage

Mining pools -> centralization

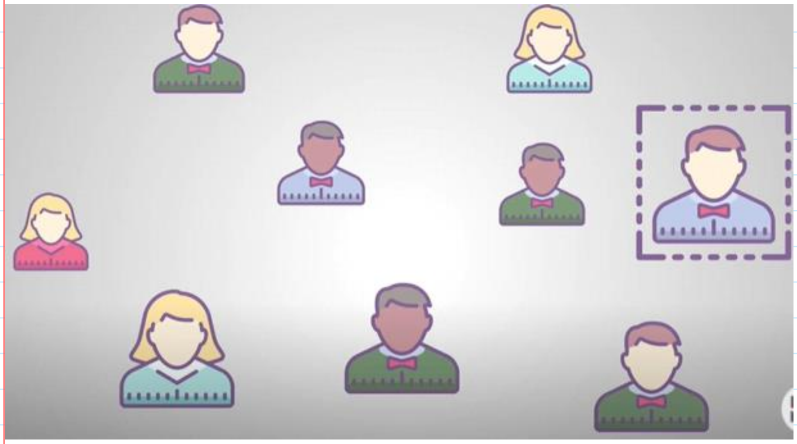
-> We need new algorithm!

Ethereum   1 Eth ~ 2300 $
↓

~~Miners~~
~~Mining~~
Validators
Minting / Forging

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

1 Eth ~ 2300 $

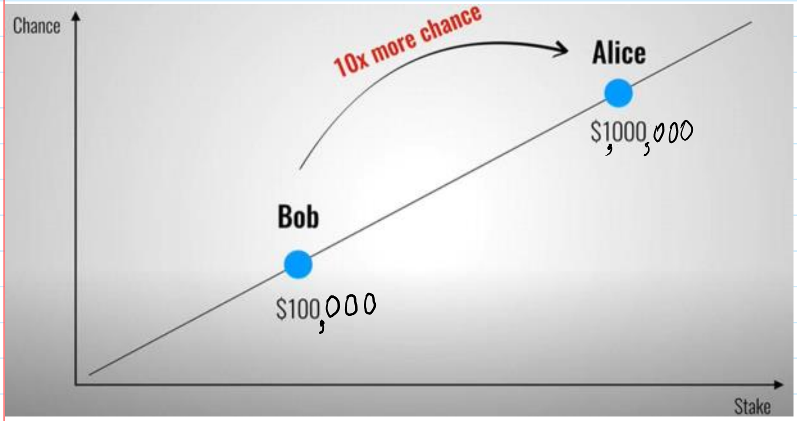


Vitalik Buterin

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.

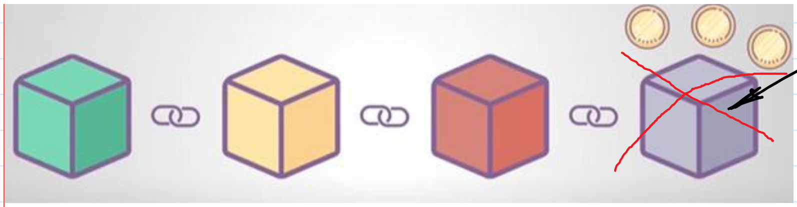


$1\ \text{Wei} = 10^{-18}\ \text{Eth}$

$1\ \text{Eth} = 1000000000000000000\ \text{Wei}$

To mine a block consisting of a lot of transactions →
→ every transaction has declared a reward in Gas for its validat.

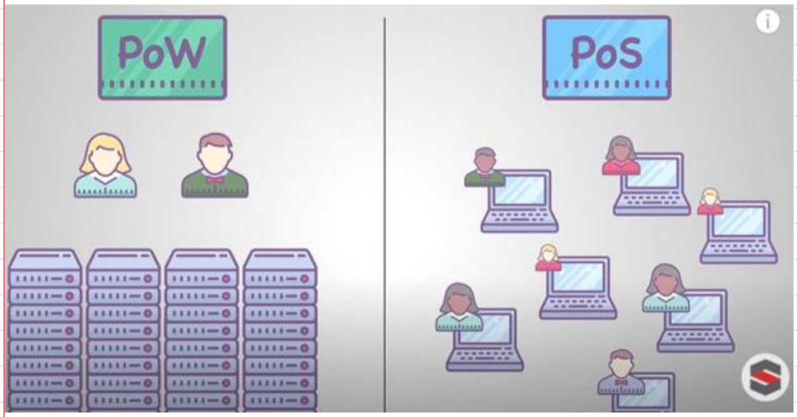
Mistaken validated block
↓ ↘
Intentionally



Mistaken validated block

Intentionally   Non-Intentionally

To empty your deposit after some time.



Ethereum 2.0

32 Eth ;   1 Eth ~ 140 $

Ethereum, Libra, ... etc.

Fiat currency

Validator generated Public Key Cryptosystem – PKCs

private Key $PrK = x$ and public key $PuK = a$: $a = g^x \bmod p$.

Block B validation by validator V : (PrK, PuK)

1. H(B) = h ; h-value computation

2. Validator signs a block B, placing a signature on h :

Sign(PrK, h) = S

Go : 1. PrK & PuK generation ? 2. Smart contract signing

malware)))))

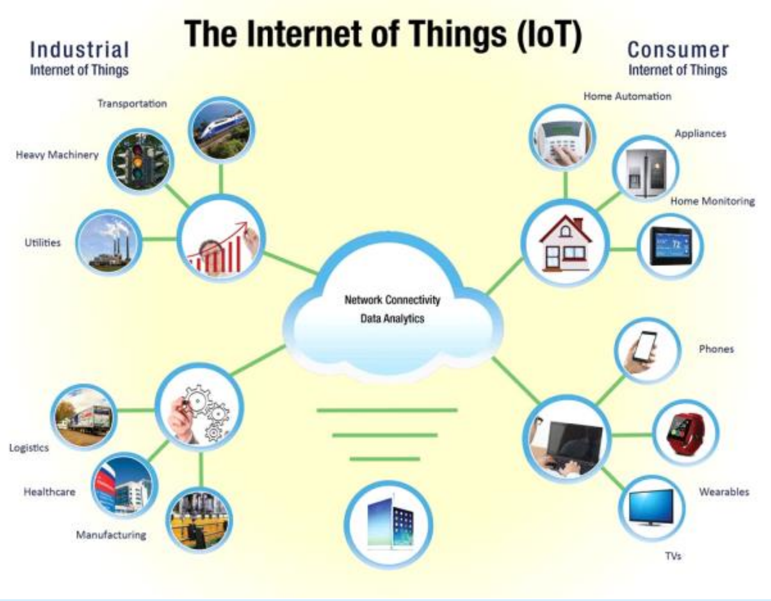
Net

Secure PrK, PuK generation & signing

computer ✗

(PrK, PuK) → Flash token

Go Trust (Taiwan)



< 1000 Tx/s

→ 15 000 Tx/s

ECDSA 512 bits

Max BTC ~ 20 000 000

$$\text{Max BTC} \sim 20\,000\,000$$

$$1\ \text{BTC} = 10^8\ \text{Sat}$$

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