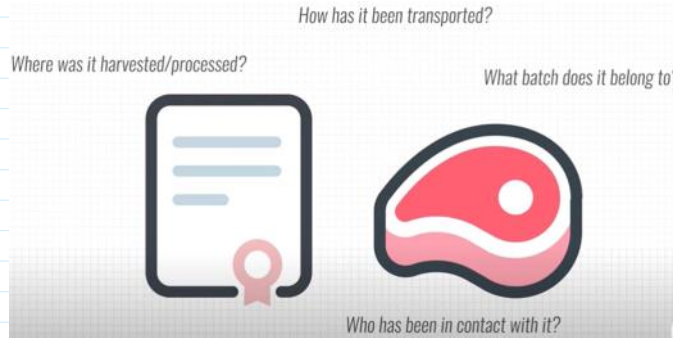
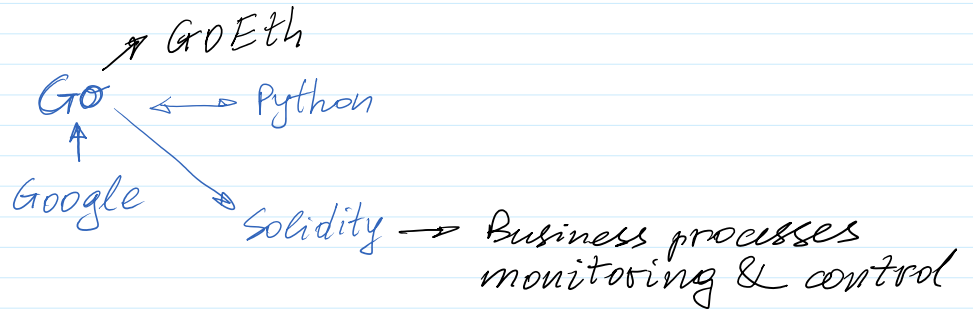
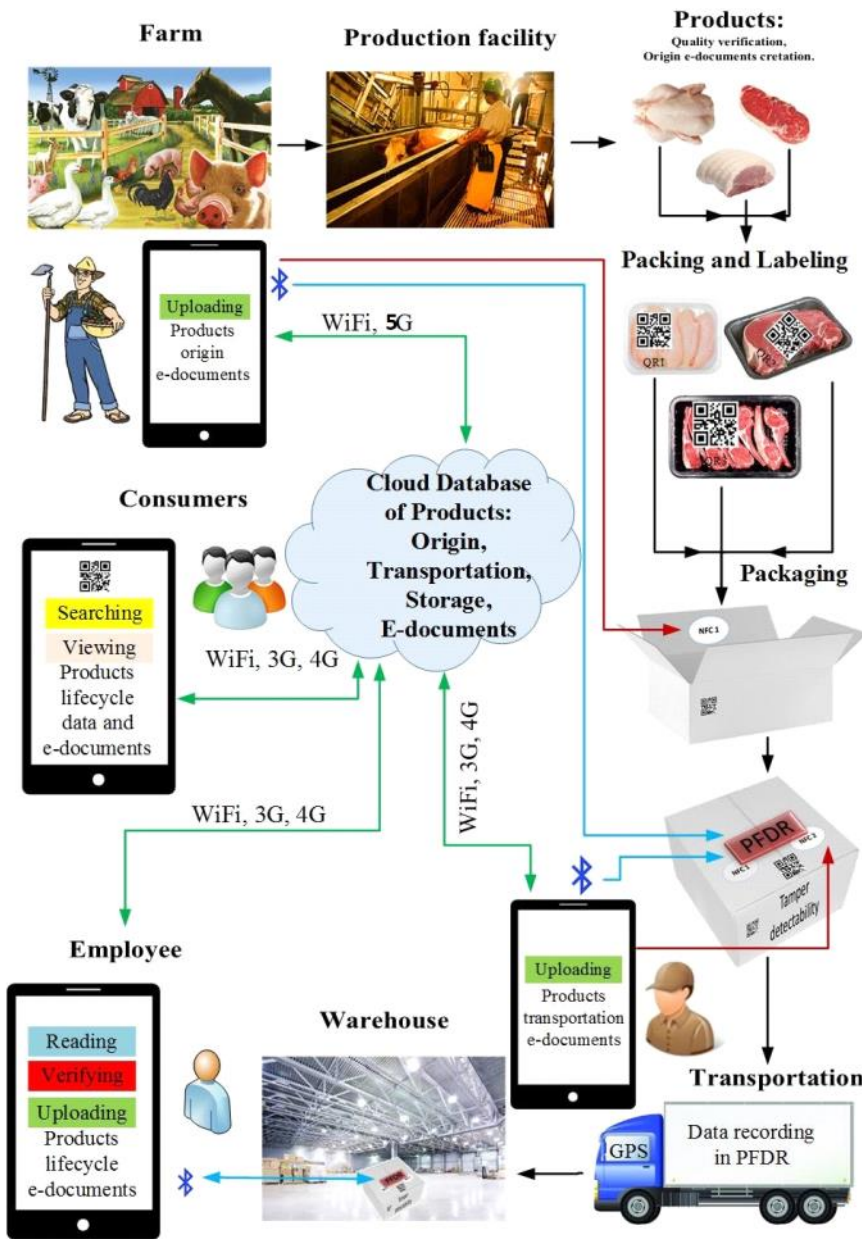
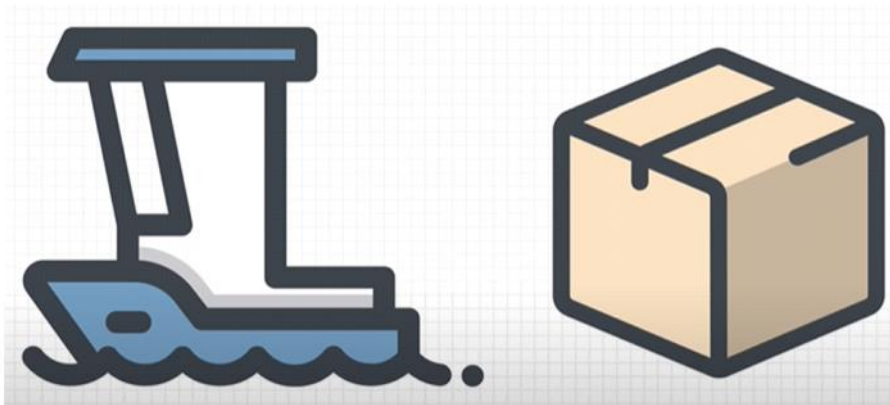




A

$T, t, c(x, y)$

B



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

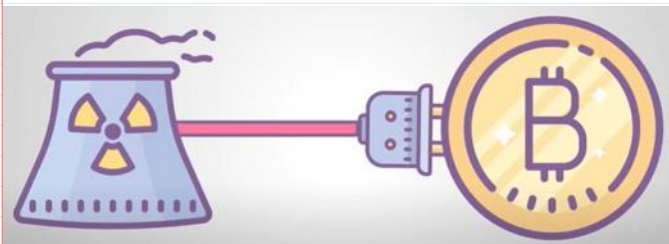
IBM Hyperledger
Fabric
Distributed Ledger
Technology
Permissioned Blockchain
Food Trust.

Ethereum Blockchain
Permissionless Permissioned
Open Ethereum

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

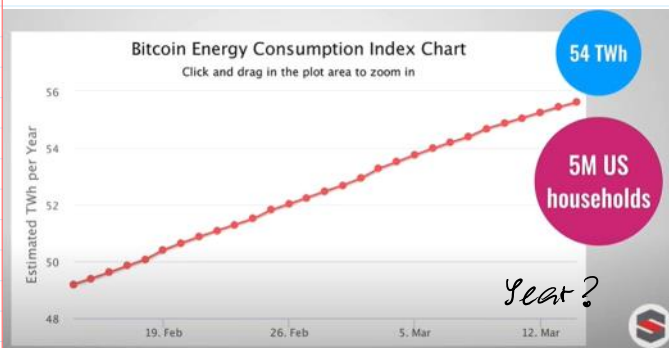


Federal Bureau of Reserve
 Fed



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^(EP)

[W] - watt

In 1 household EP $\sim$ 5 kW

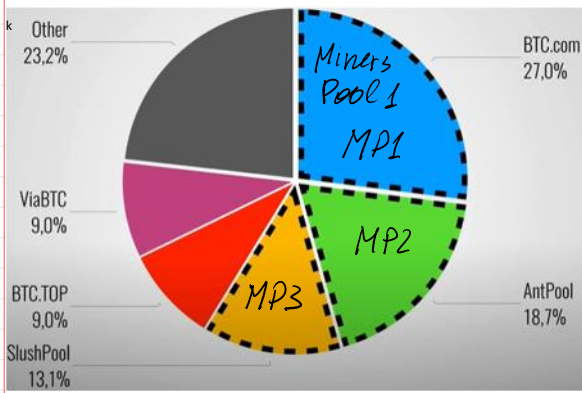
During 1 hour Energy = 5 kWh
 $\downarrow$
 $\sim$ 1 Eur

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 € = 200 €



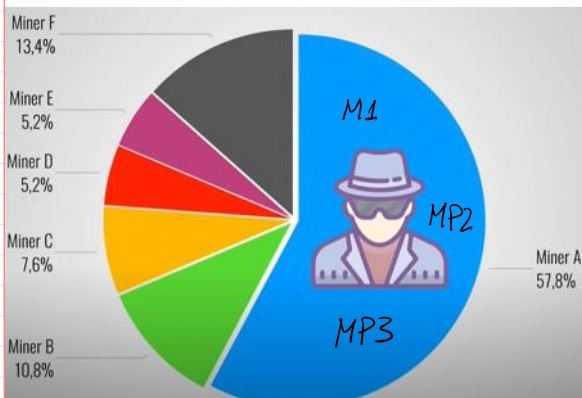
51% Attack

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

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

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

Total network has $V_h = 1900 TH/s$



> 51% Network power

1000 TH/s is more than 51%

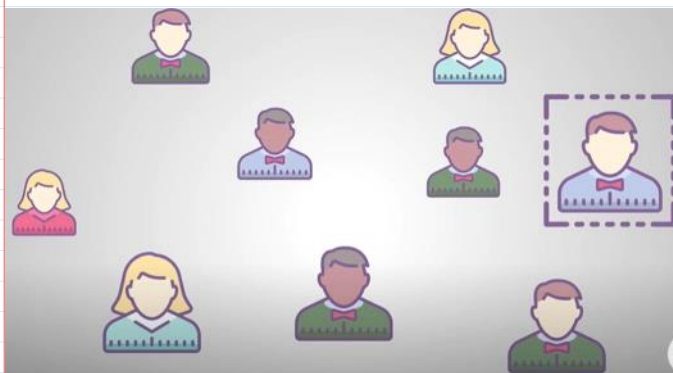
1900 TH/s

51% Attack



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

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



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

114_016 D. J. J. J.

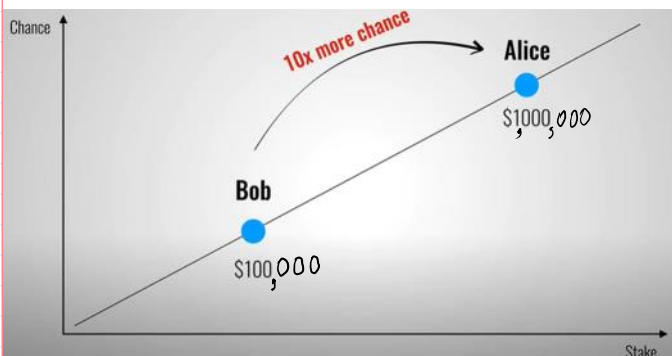


Vitalik Buterin

Eth $\rightarrow$ 32 Eth put into the "shell" to make a right to mine a block

The difficulty of validat. is low $\rightarrow$

$\rightarrow$ the speed of validation is increased.

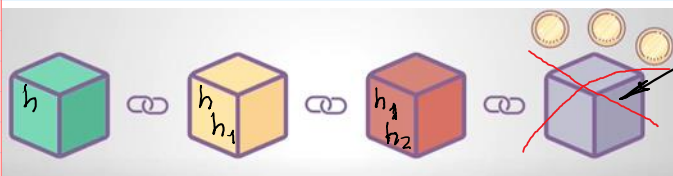


$$1 \text{ Wei} = 10^{-18} \text{ Eth}$$

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

To mine a block consisting of a lot of transactions $\rightarrow$

$\rightarrow$ every transaction has declared a reward in Gas for its validat.

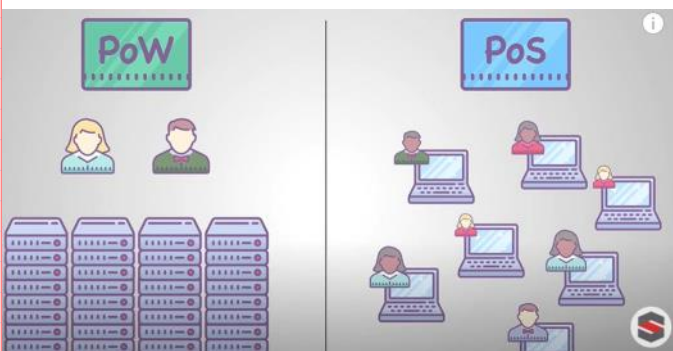


Intentionally Non-Intentionally



To empty your deposit after some time.

TSMC



Ethereum 2.0

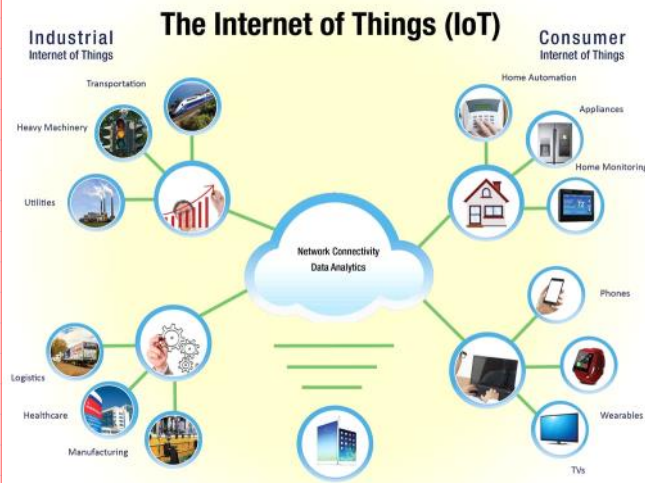
32 Eth; 1 Eth $\sim$ 140 \$

Ethereum, Libra, ... etc.



Fiat currency $\rightarrow$ crypto curr. $\rightarrow$

- $\rightarrow$ { Financial transact. $\rightarrow$
- $\rightarrow$ Smart contracts
- $\rightarrow$ Investment mech. $\rightarrow$ tokens

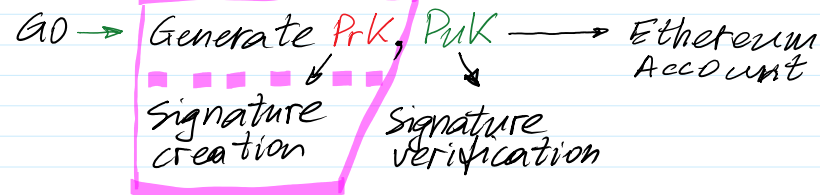


$< 1000 \text{ Tx/s}$

$\rightarrow 15000 \text{ Tx/s}$

ECDSE 512 bits

G5 $\rightarrow$ G6



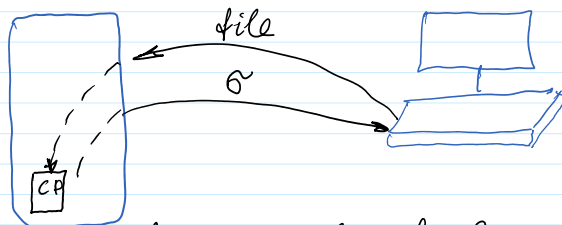
PrK generation :

1. Generate with independent software and together with PuK save it in separate token. Device for PrK generation must be disconnected from internet.

1.1. Flash stick (Go Trust, Taiwan)

1.2. In mobile phone :

2. Signing must be performed using separate token or mobile phone.



Flash stick with Crypto Processor : having PrK, PuK, cryptographic functions

$$1) h = H(\text{file})$$

$$2) \text{Sign}(\text{Prk}, h) = \tilde{b} = (r, s)$$