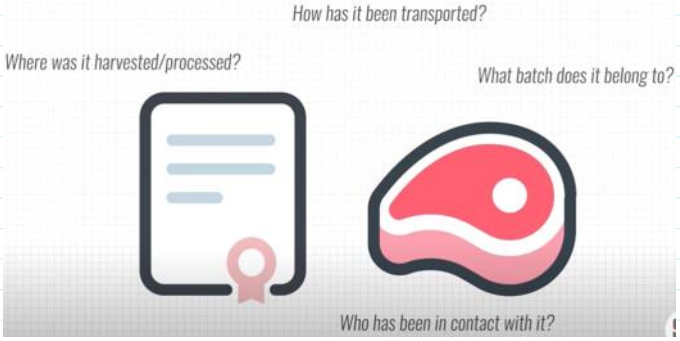
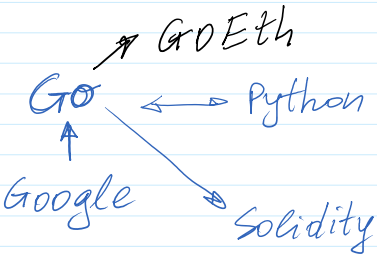
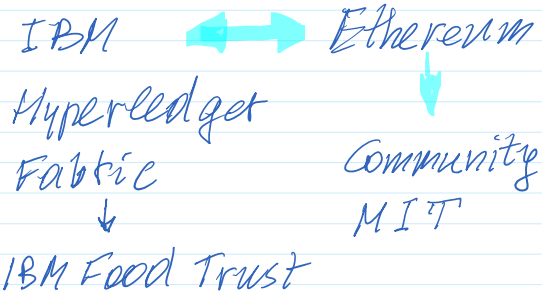
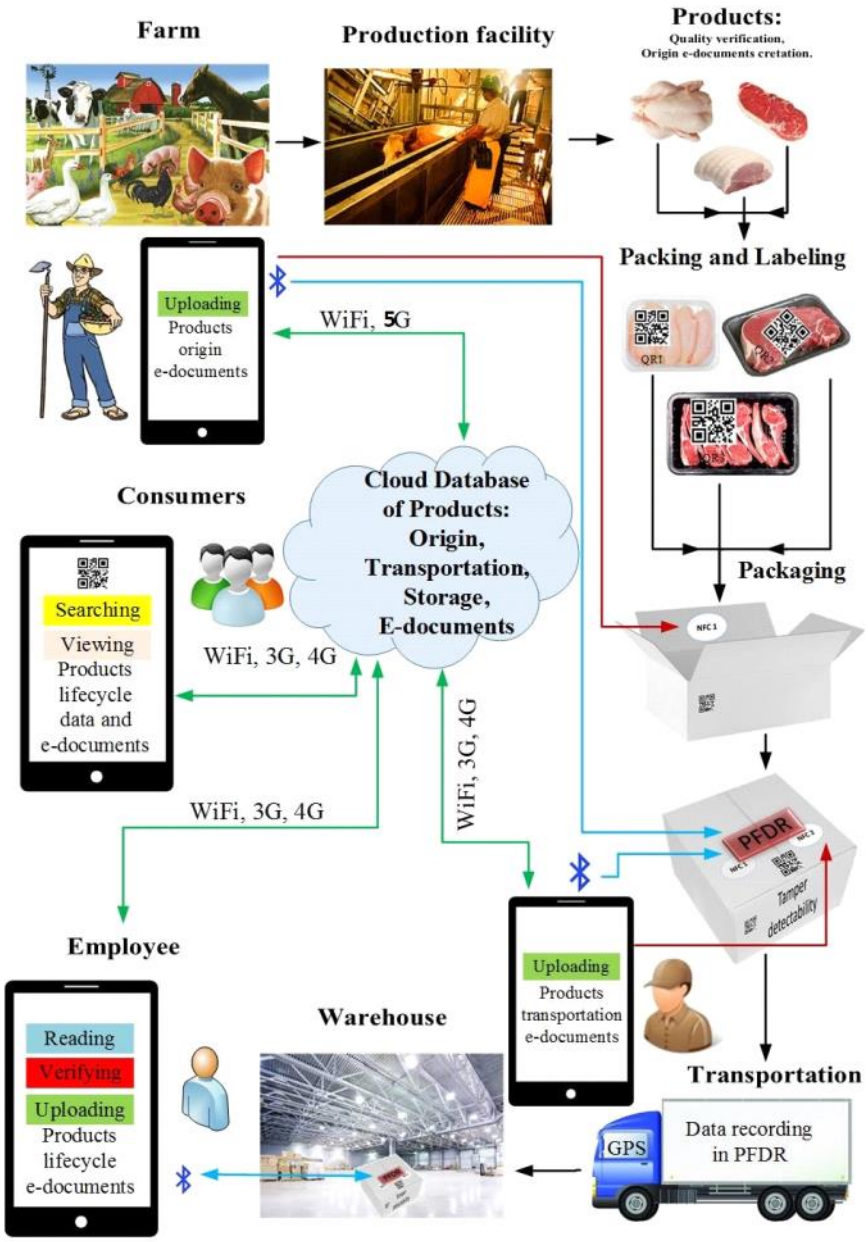

Creating a blockchain with Javascript
(Blockchain, part 1)
Create a blockchain
with JavaScript
14:52

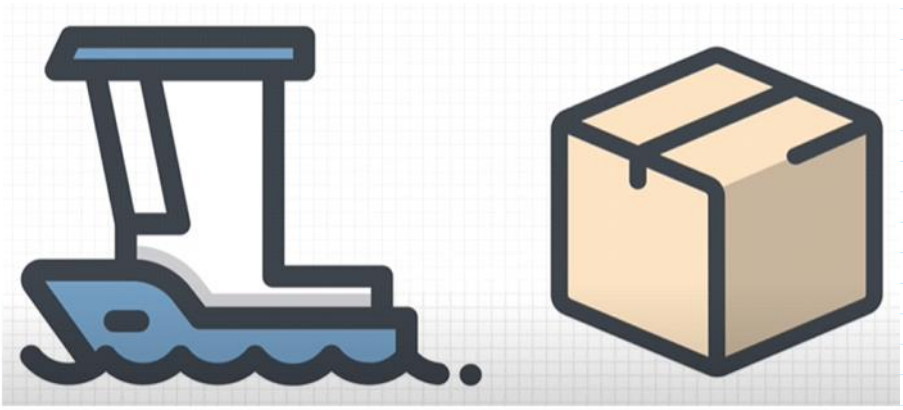

Food industry


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


GO
GO Eth
Python
Google
Solidity
Business processes
monitoring & control


IBM
Ethereum
Hyperledger
Fabric
IBM Food Trust
Community
MIT





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

A

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

B

IBM Hyperledger

Fabric

Distributed Ledger

Technology

Permissioned blockchain

Food Trust.

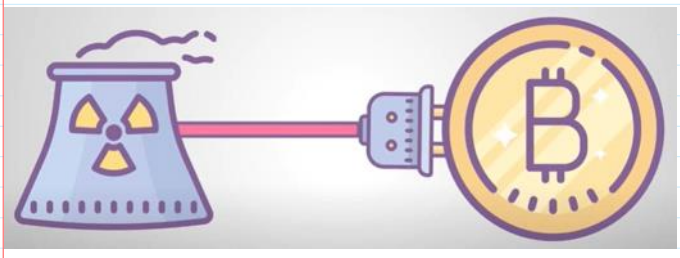
Ethereum blockchain

Permissionless Permissioned

Open Ethereum

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

Federal Burou of Reserve
Fed



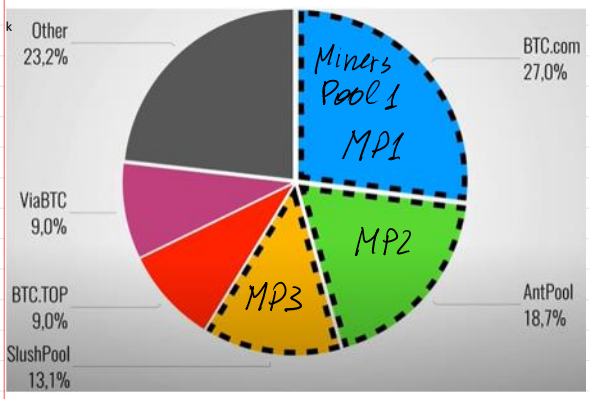
PoW - Proof of Work

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 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 €

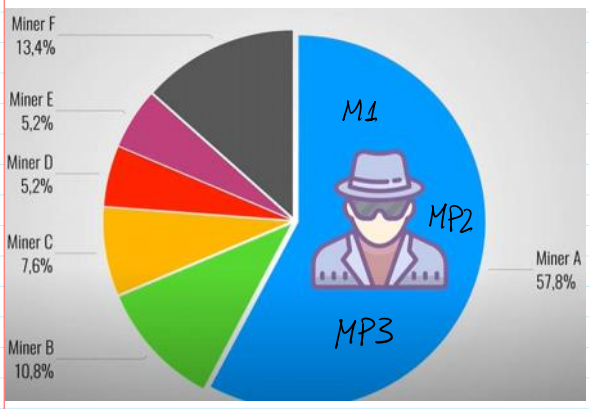


51% Attack

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

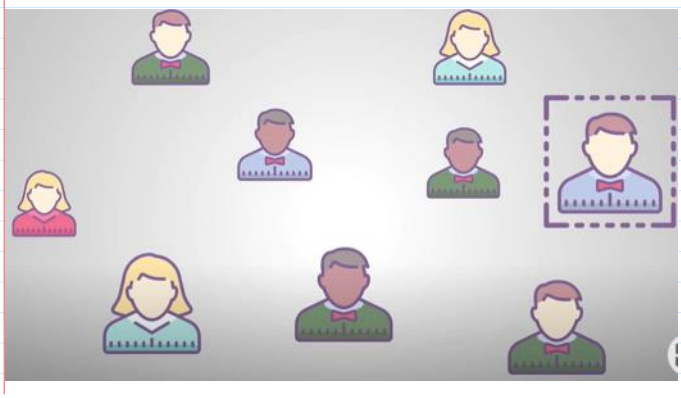
↓

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

1) Cryptocurrency Ether penetration to busines
2) Potential investors attraction

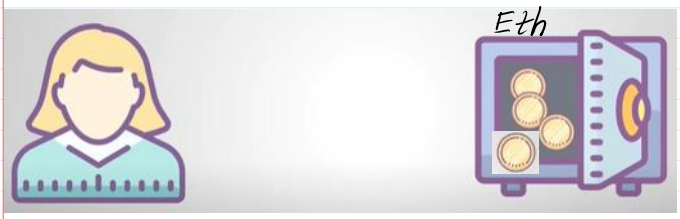
↓

Can buy Tokens related to Ether.



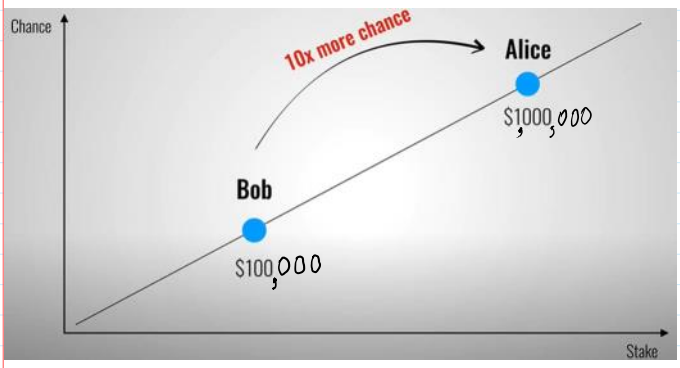
Vitalik Buterin

Vitalik Buterin



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

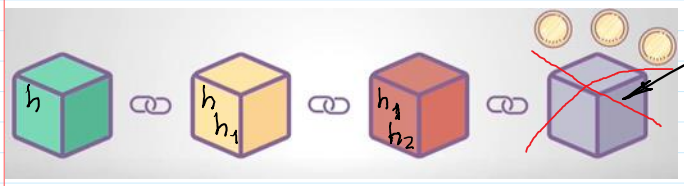
The difficulty of validat. is low → → the speed of validation is increased.



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

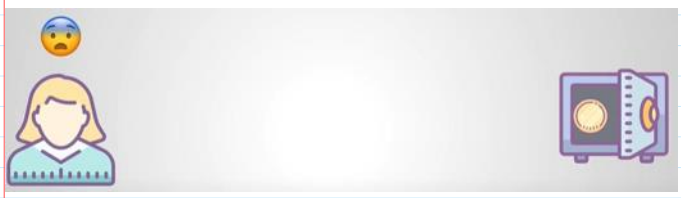
$1 \text{ Eth} = 1000000000000000000 \text{ Wei}$

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



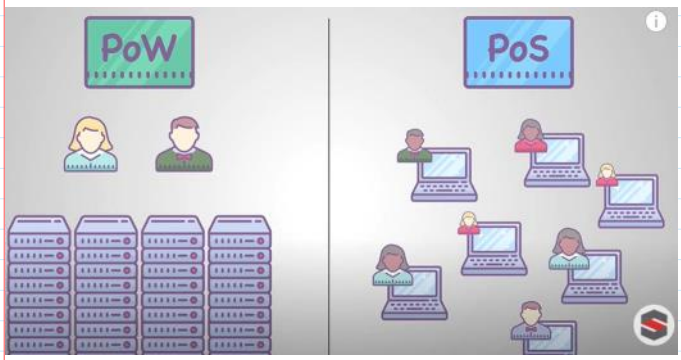
Mistaken validated block

Intentionally Non-Intentionally



To empty your deposit after some time.

TSMC

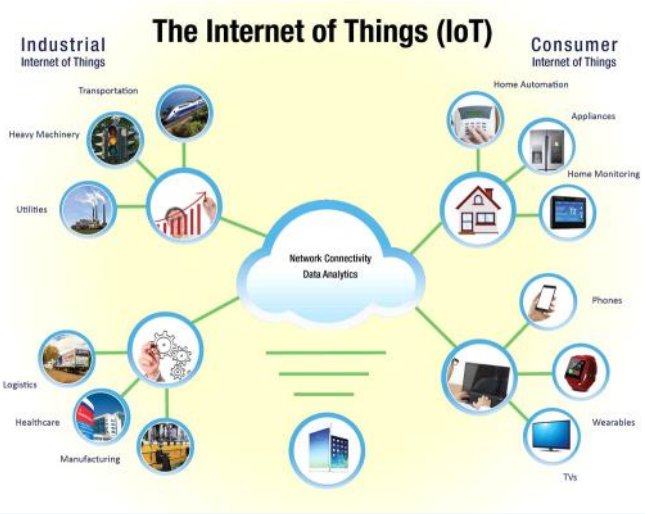


Ethereum 2.0

32 Eth ; 1 Eth ~ 140 $

Ethereum, Libra, ... etc.

Fiat currency → crypto curr. →
→ { Financial transact. → Smart contracts
→ { Investment mech. → tokens



< 1000 Tx/s
→ 15000 Tx/s
ECDSA 512 bits
G5 → G6

G0 → Generate PrK, PuK → Ethereum Account
Signature creation
Signature verification

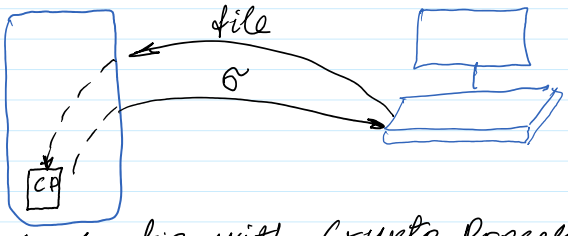
PrK generation:

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 separete token or mobile phone.



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

1) $h = H(file)$

2) $Sign(prk, h) = \sigma = (r, s)$