



Oxford Blockchain Strategy Programme

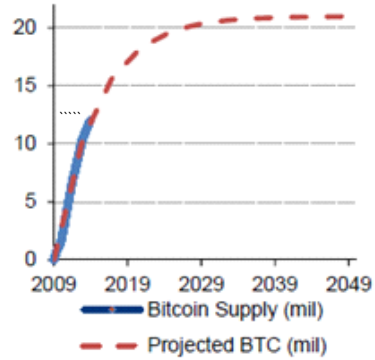
Discover how blockchain is changing business and how you can harness disruption

<https://coinmarketcap.com/>

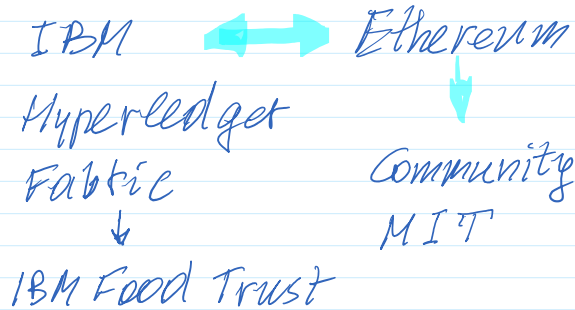
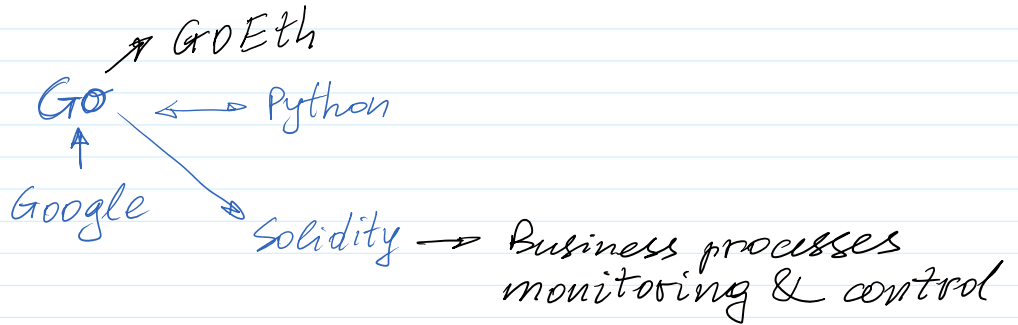
Bitcoin - BTC <https://bitcoin.org/en/>

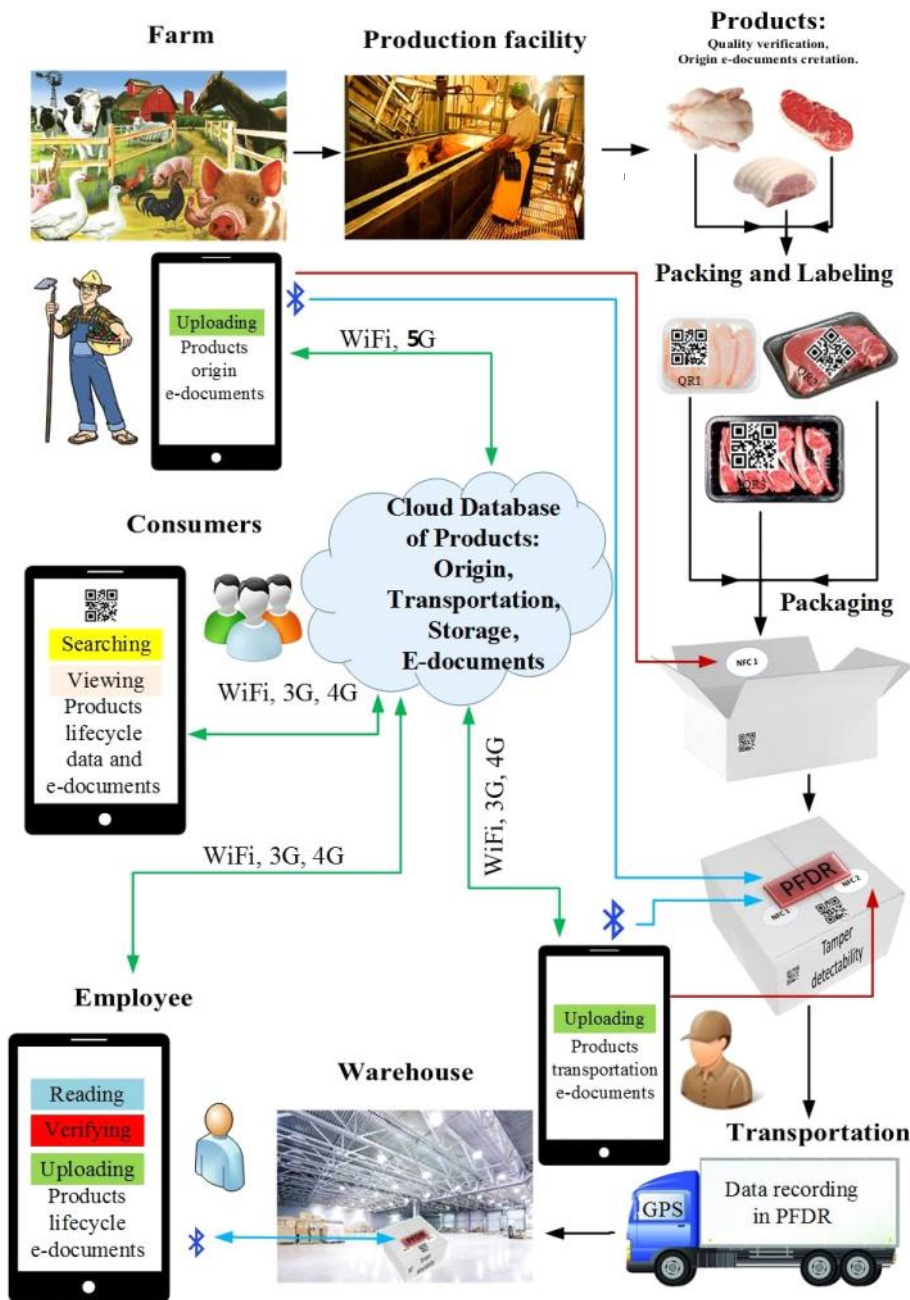
Ethereum - ETH <https://ethereum.org/>

Monero <https://www.getmonero.org/>

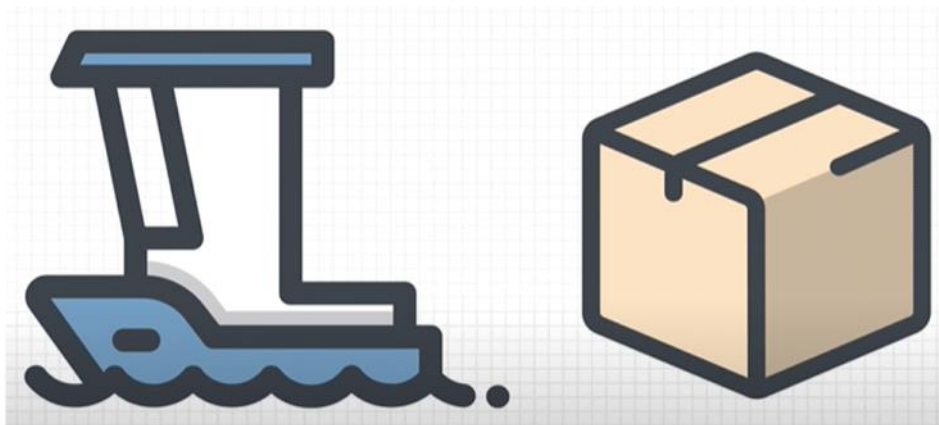


Total number of Bitcoins over time.





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

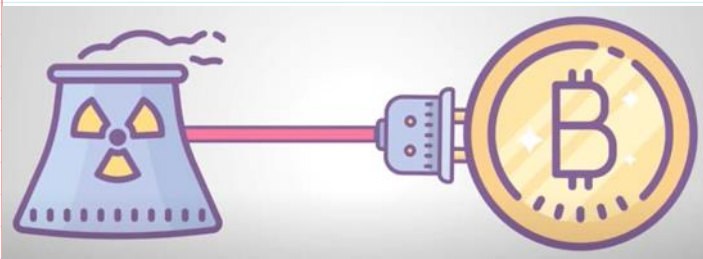
ICO - initial coin offer

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

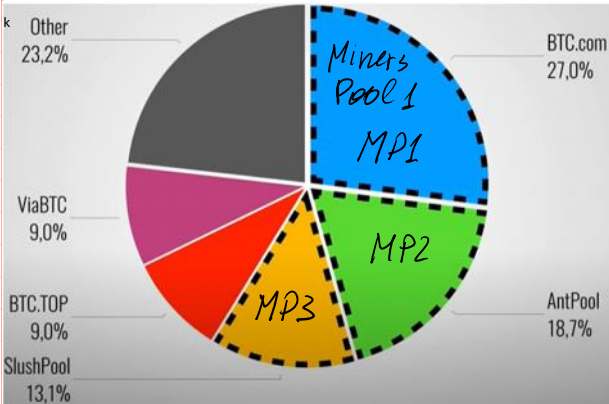
During 1 hour Energy = 5 kWh

\downarrow
 \sim 1 Eur

To charge e-vehicle 20-50 kWh

Farm can consume $\sim 500 \text{ kW} - (1 \text{ MW})$

During 1 hour you'll consume Energy = $1 \text{ MWh} = 1000 \text{ kWh}$
 $1000 \text{ kWh} * 0,2 \text{ €} = 200 \text{ €}$



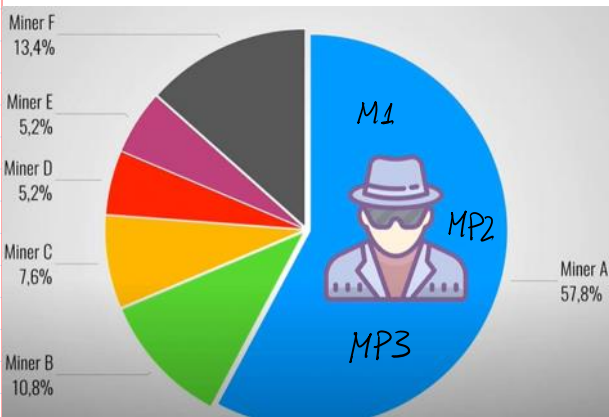
51% Attack

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

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

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

Total network has $V_h = 1900 \text{ TH/s}$



> 51% Network power

1000 TH/s is more than 51%

1900 TH/s

51% Attack

Forking



Energie usage 

Mining pools -> centralization 

-> We need new algorithm!




Proof-of-stake



~~Miners~~

~~Mining~~



Validators

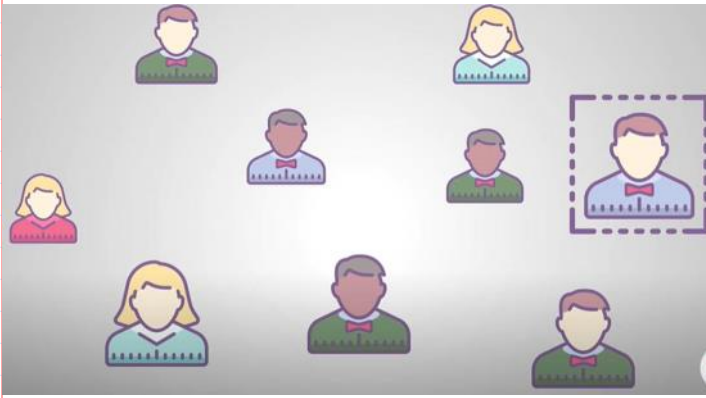
Minting / Forging

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

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

1) Cryptocurrency Ether

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

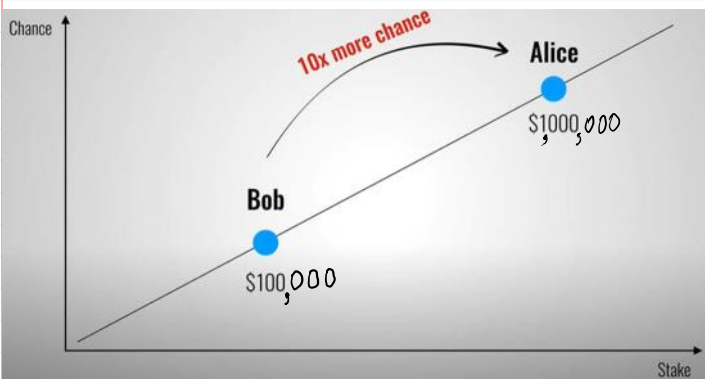


Vitalik Buterin

Eth → 32 Eth put into the "shell" to make a right to mine a block
 The difficulty of validation is low →



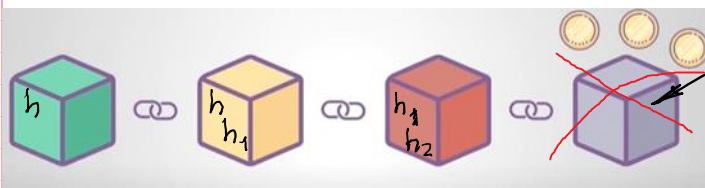
→ the speed of validation is increased.



$1 \text{ Wei} = 10^{-18} \text{ Eth}$
 $1 \text{ Eth} = 1000000000000000000 \text{ Wei}$
 To mine a block consisting of a lot of transactions →

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

Gas price: $1 \text{ Gas} = 2000 \text{ Wei}$



Mistaken validated block
 ↓
 Intentionally Non-Intentionally

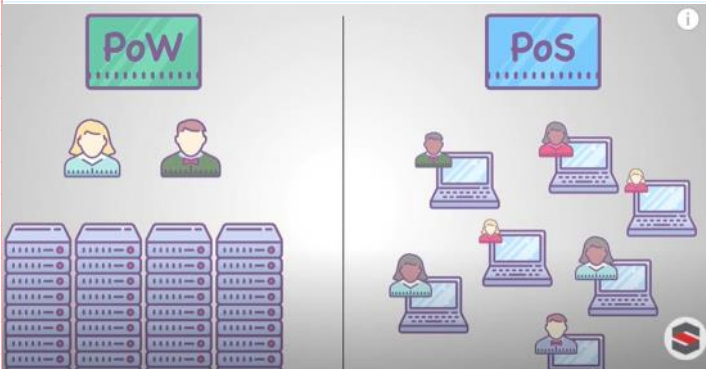


To empty your deposit after some time.



to empty your deposit after some time.

TSMC



Ethereum 2.0

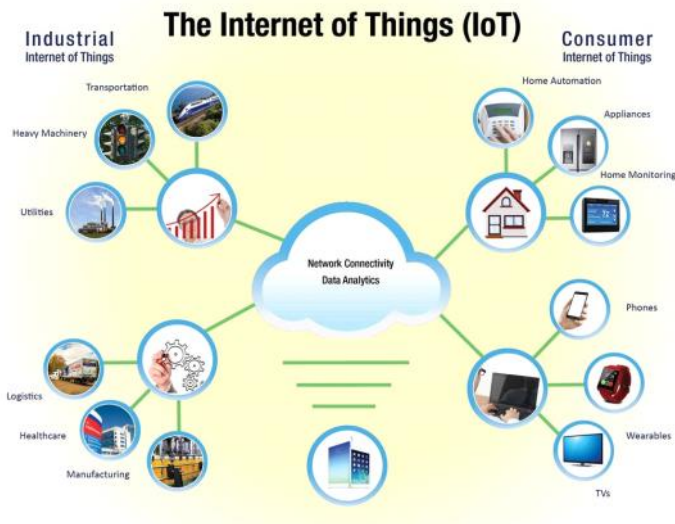
32 Eth; 1 Eth ~ 140 \$

Ethereum, Libra, ... etc.



Fiat currency → crypto curr. →

- Financial transact. →
- Smart contracts
- Investment mech. → tokens

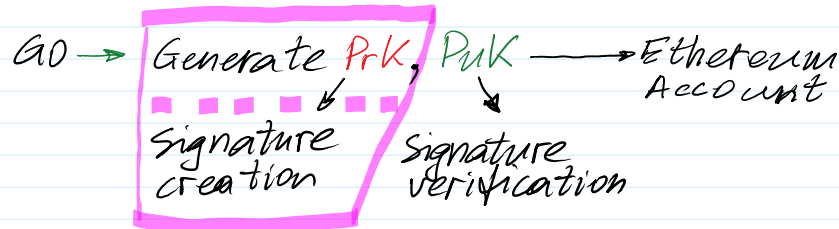


< 1000 Tx/s

→ 15000 Tx/s

ECDSA 512 bits

G5 → G6



PrK generation:

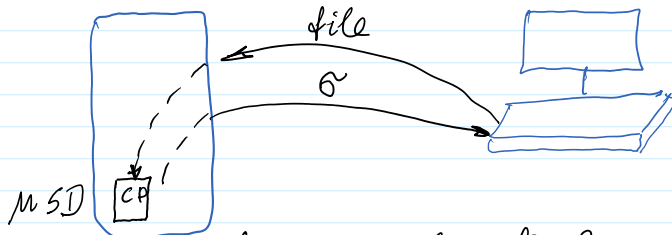
1. Generate with independent software and together with PuK save it in separate token. Device for PrK generation

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 , $PubK$, cryptographic functions

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

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

<https://www.ledger.com>

<https://trezor.io>

[Trezor Hardware Wallet \(Official\) | Bitcoin & Crypto Security](#)

The safest cold storage wallets for crypt security and financial independence. Easily use, store, and protect Bitcoins.
trezor.io



Book-keeping --> accounting --> balance --> state

Bookkeeping is the recording of financial transactions, and is part of the process of **accounting** in **business**.^[1] Transactions include purchases, sales, receipts and payments by an individual person or an organization/corporation. There are several standard methods of bookkeeping, including the **single-entry** and **double-entry** bookkeeping systems.

From <https://en.wikipedia.org/wiki/Bookkeeping>

<https://www.dreamstime.com/stock-image-d-life-cycle-accounting-process-illustration-circular-flow-chart-image30625511>



Authorized capital
Credit
Fixed Assets
Costs
Incomes

Op.No.	Input	Output	RemainingAmount
1	123	0	123
2	5	11	117

Compare with UTXO system



Compare with UTxO system

<https://medium.com/@olxc/ethereum-and-smart-contracts-basics-e5c84838b19>

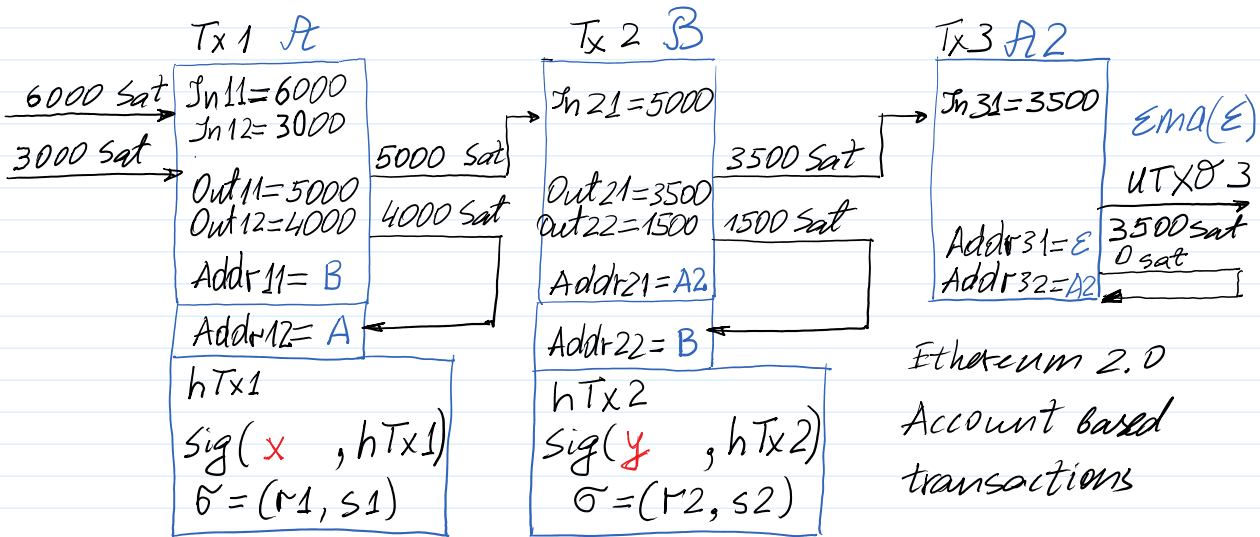
State 0	Authorized Capital	Credit	Fixed Asset				Balance 0
	12 000	9 000	-12 000				9 000

State 1	Authorized Capital	Credit		Electricity Cost 1	Mining 1	Percent for Credit	Balance 1
		9 000		-3 000	+31 000	-1 000	36 000

State 2	Authorized Capital	Credit		Electricity Cost 2	Mining 2	Percent for Credit	Balance 2
		8 000		-15 000	-	-1 000	20 000

Book-keeping --> Accounting --> Balance --> State

Block structure - Unspent Transaction Output (UTxO) model



$Tx1 = '1 : In11 = 6000 || In12 = 3000 || Out11 = 5000 || Out12 = 4000 || Rec1 = B || Rec2 = A'$
 $Tx2 = '2 : In21 = 5000 || Out21 = 3500 || Out22 = 1500 || Rec1 = A2 || Rec2 = B'$
 $Tx3 = '3 : In31 = 3500 || Out31 = 3500 || Out32 = 0 || Rec1 = E || Rec2 = A2'$

$h_1 = H(Tx1) = h_{28}(Tx1)$

$h_2 = H(Tx2) = h_{28}(Tx2)$

$h_3 = H(Tx3) = h_{28}(Tx3)$

[Redacted]

[Redacted]