OST
Eastern Switzerland
University of Applied Sciences

Distributed Systems & Blockchain (DS1)

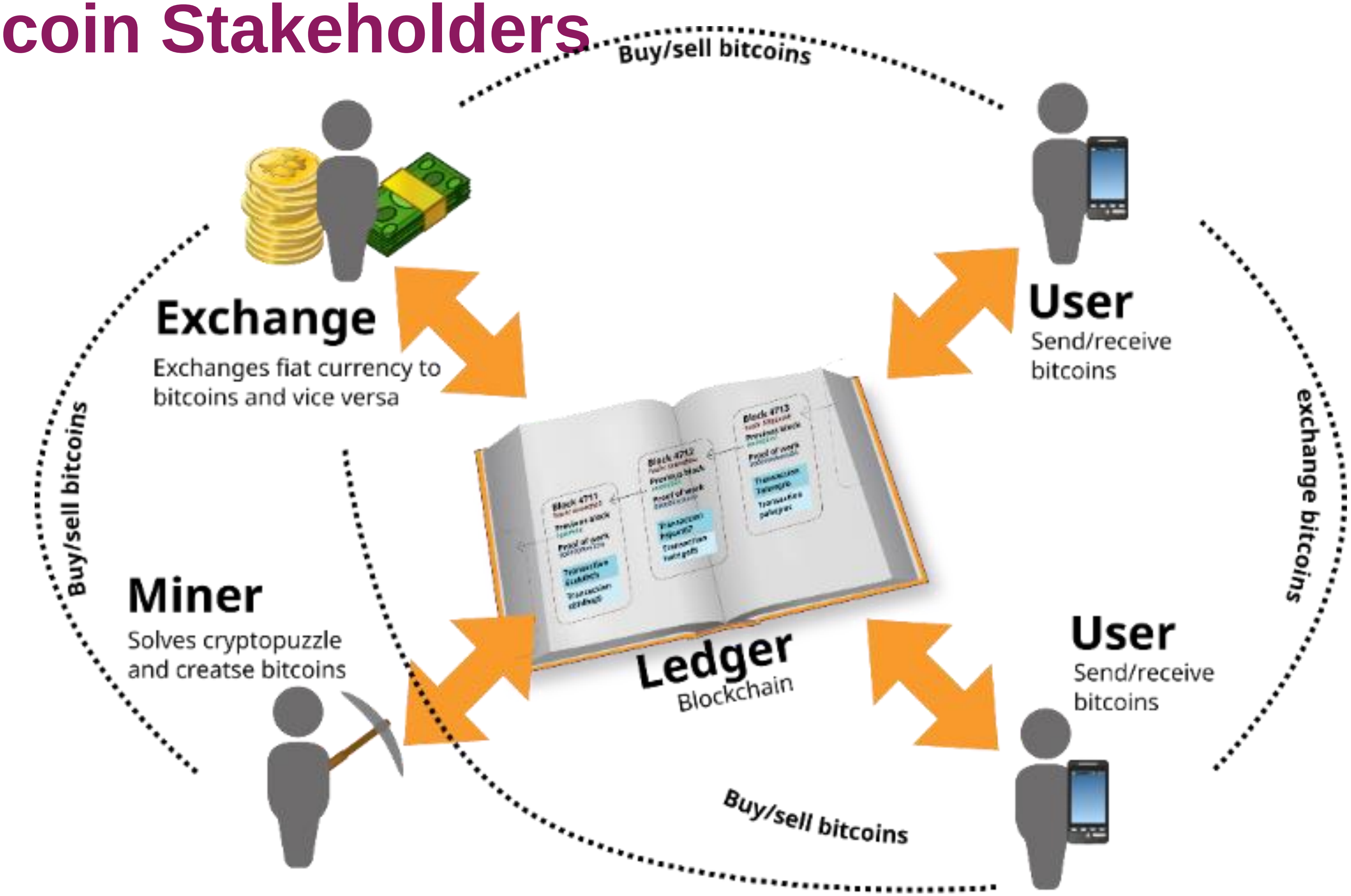
Bitcoin/Blockchain II

Thomas Bocek

25 April 2021

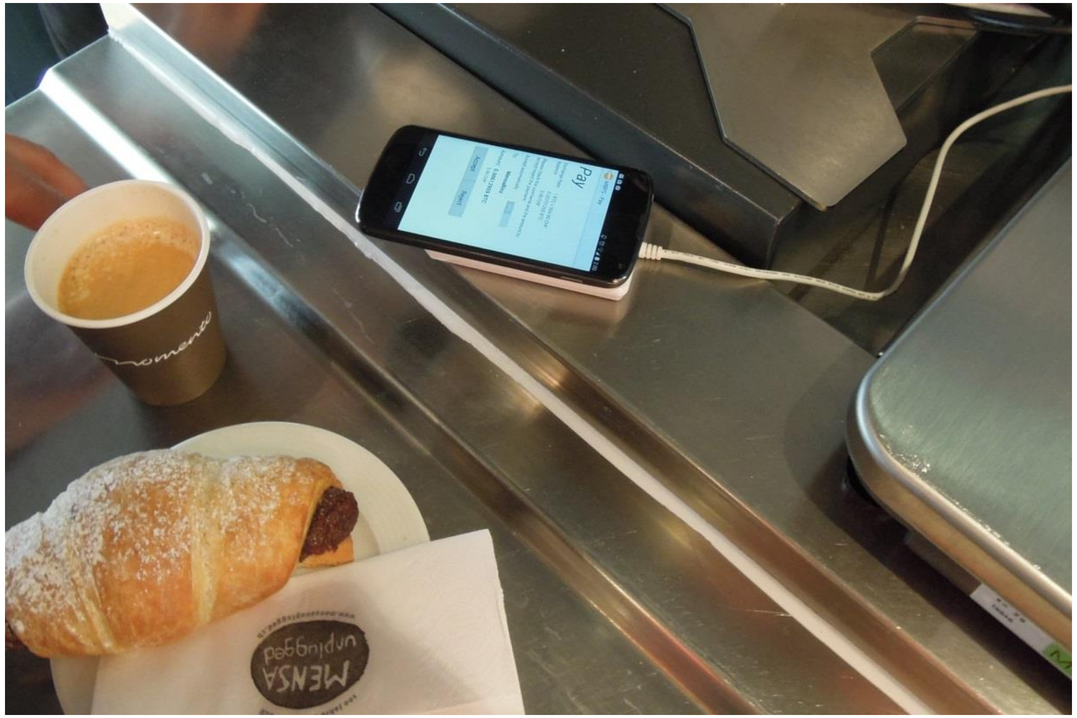
Summary: Bitcoin Stakeholders

- [Building blocks](#)
  - https://andersbrownworth.com/blockchain/



Bitcoins Payment in 2014: Evaluation: Mensa Test Run

- Designed and implemented a Bitcoin payment system
- One week test run from 10th to 14th of February 2014
- In collaboration with the Mensa Binzmühle
- Pay all consumptions in Mensa with Bitcoins
- Lessons learned: reduce Bitcoin volatility risk by immediate trades on Bitstamp.net
    - After selling Bitcoins at the exchange point → Buy the same amount of Bitcoins
        - Keep the balance of the exchange point constant
    - After the Mensa receives Bitcoins → Sell these Bitcoins
        - Since the Mensa wants to receive CHF at the end, the equivalent amount is assured in this way

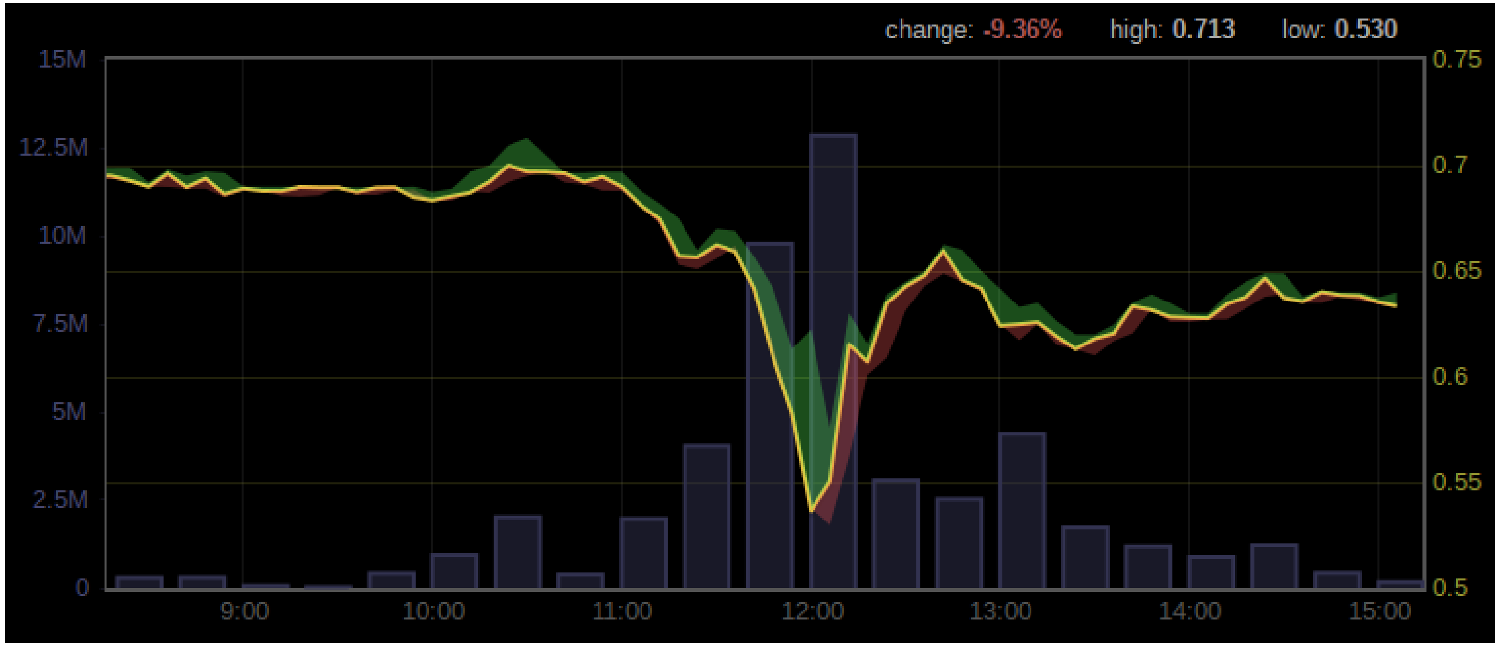


Example payment at Mensa Binzmühle

Bitcoins Payment in 2014: Evaluation: Conclusions

- NFC handling caused many problems because users are inexperienced with NFC

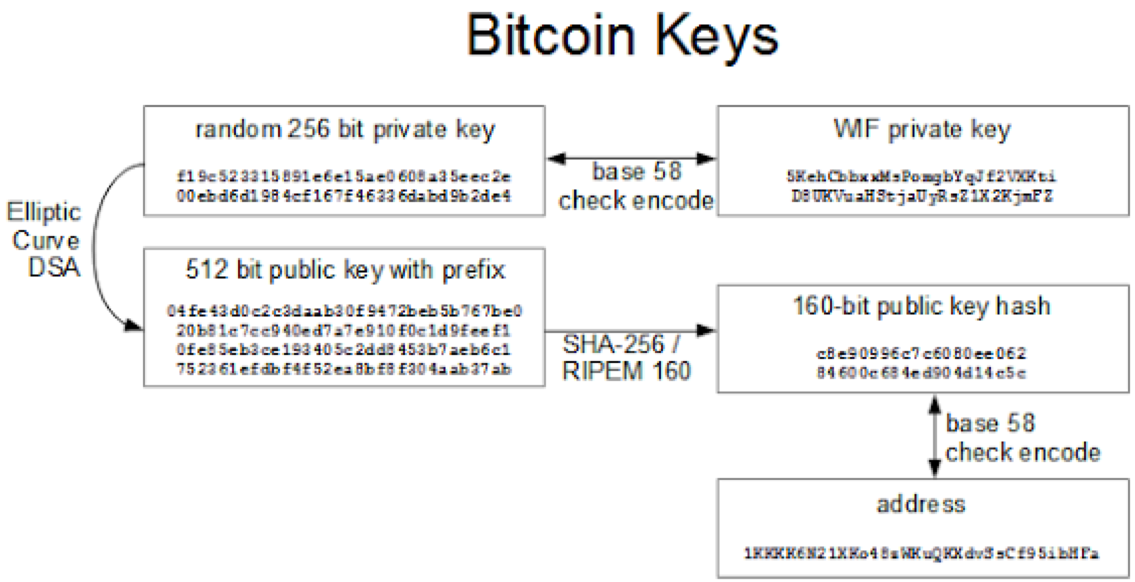
- Android 4.4 restriction → too big entry barrier, below 4.4 no two-way NFC possible

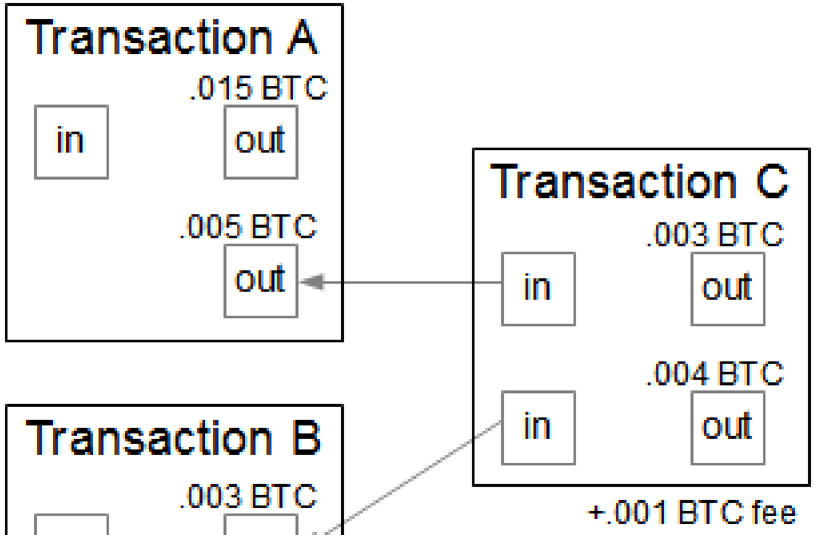


USD/mBTC Exchange Rate Drop – February 10, 2014

Bitcoin in Detail

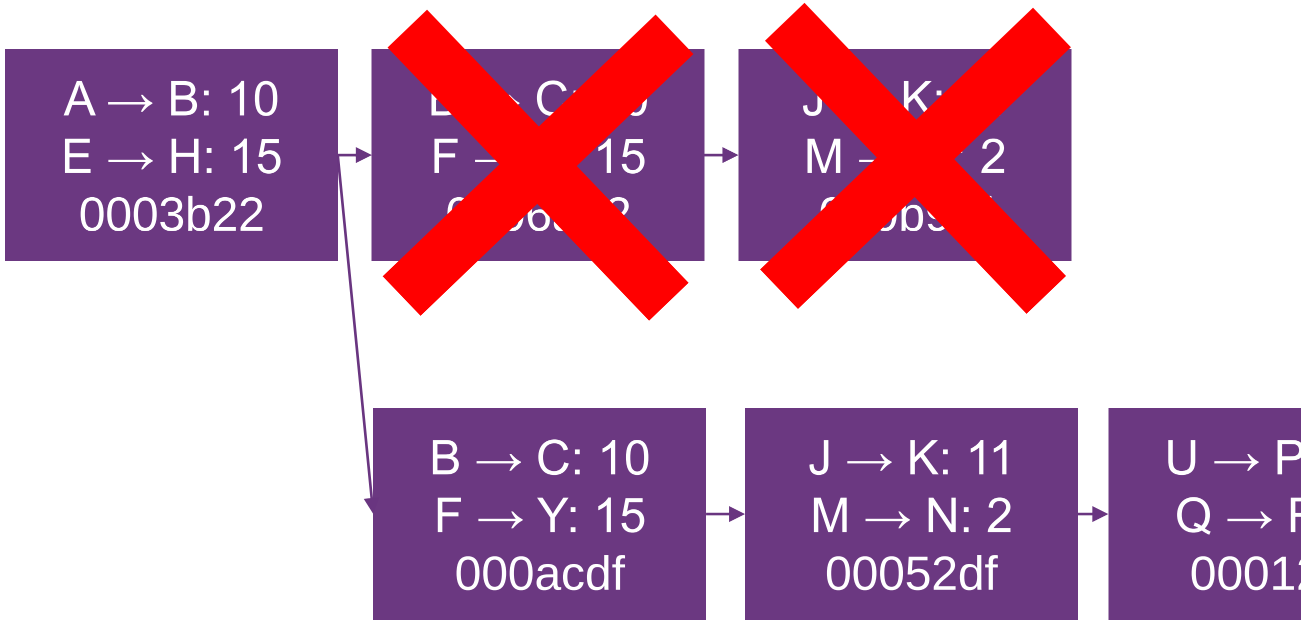
- Good information: http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html


Bitcoin Keys
random 256 bit private key
f19c523315891e6e15ae0608a35eec2e
00ebd6d1984cf167f46336dabd9b2de4
base 58
check encode
WIF private key
5KehCbbxxMsPomgbYqJf2VXKti
D8UKVuaHStjaUyRsZ1X2KjmFZ
Elliptic
Curve
DSA
512 bit public key with prefix
04fe43d0c2c3daab30f9472beb5b767be0
20b81c7cc940ed7a7e910f0c1d9feef1
0fe85eb3ce193405c2dd8453b7aeb6c1
752361efdbf4f52ea8bf8f304aab37ab
SHA-256 /
RIPEM 160
160-bit public key hash
c8e90996c7c6080ee062
84600c684ed904d14c5c
base 58
check encode
address
1KKKK6N21XKo48zWKuQKXdvSsCf95ibHFa



51% Attack

- “If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.”
  - https://bitcoin.org/bitcoin.pdf
- PoW: majority of hashing power, PoS: majority of coins
- How expensive is a 51% attack?
  - Buy an attack?
- Double spend, or rollback transactions
  - X is an exchange
  - Mine secretly, Y is your address
  - X arrived – payout (1 block conf.)
  - You mine faster, broadcast secret chain
  - Tx F→X: 15 never happened, goes to Y



A → B: 10
E → H: 15
0003b22

B → C: 10
F → Y: 15
000acdf

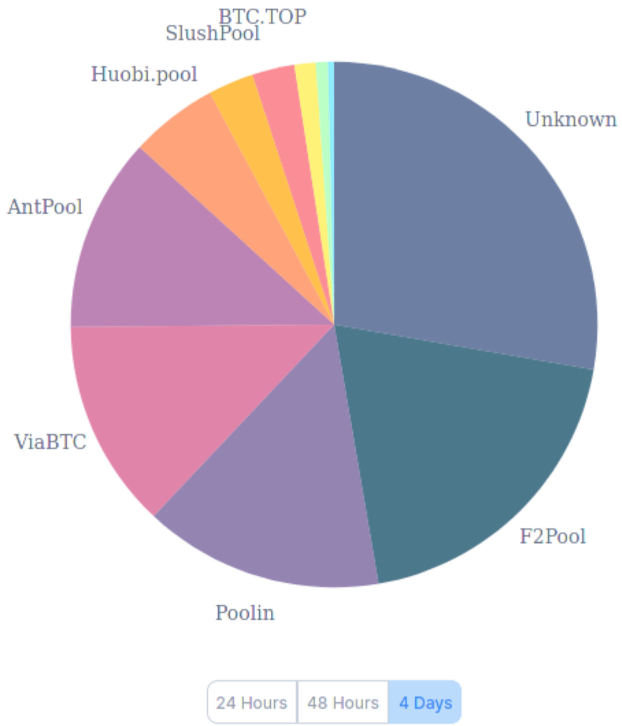
J → K: 11
M → N: 2
00052df

U → P
Q → F
0001

51% Attack

- Control over 50% of the scarce resources
  - Pools: cooperative puzzle solving
  - Solo: competitive puzzle solving

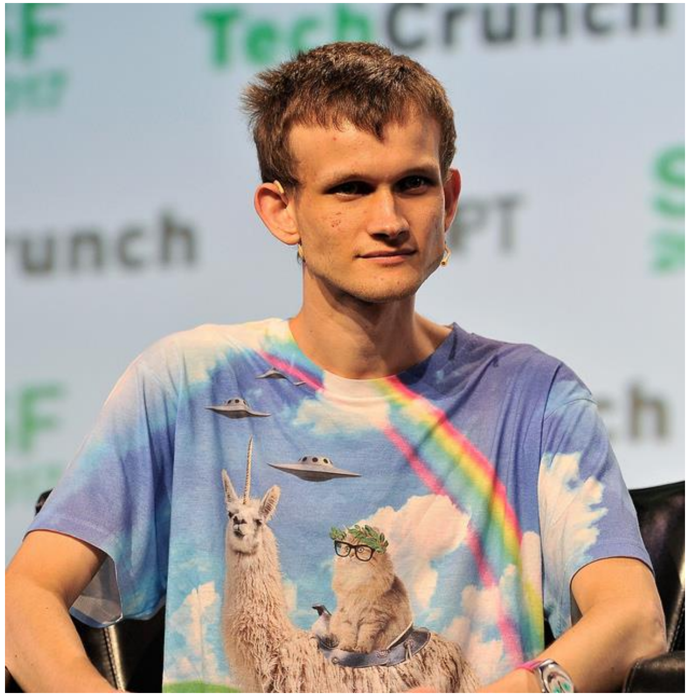
http://blockchain.info/pools



- 03.01.2019: BTC.TOP, Mining Pool, Controls Over 50% Of The BCH Hashrate
  - Bitcoin Cash
- 25.06.2018: Bitmain’s Mining Pools Now Control Nearly 51 Percent of the Bitcoin Hashrate
  - Was at ~42%, now ~30%
- 07.01.2019: Deep Chain Reorganization Detected on Ethereum Classic (ETC)
  - “The total value of the double spends that we have observed thus far is 219,500 ETC (~$1.1M).”
- 23.04.2020: DeFi Platform Suffers 51% Attack From Its Top Miners — or Does It?
  - “resulted in $6.7 million worth of the USD-pegged stablecoin pUSD”
- 08.11.2020: Grin network hit with 51% attack while GRIN token remains resilient

Bitcoin / Ethereum

- Bitcoin vs. Ethereum
  - Implementing new features slow
    - Many Bitcoin hardforks (segregated witness vs. increasing block size voting) Cash vs. SV
  - Bitcoin Script limited
    - Lightning network
  - Pros and Cons – no silver bullet
- Ethereum (1 ETH ~2220$)
  - Generalized blockchain (loops, arithemitcs, etc.)
  - White paper released in December 2013
  - Protocols designed from scratch (not like Litecoin, Peercoin)
  - Ethereum foundation located in Zug (initiator known) - non-profit foundation
  - Mining reward ~ block every ~14s – ~2 ETH (“always”, unlike Bitcoin)



Vitalik Buterin