OST
Eastern Switzerland
University of Applied Sciences

Distributed Systems & Blockchain (DS1)

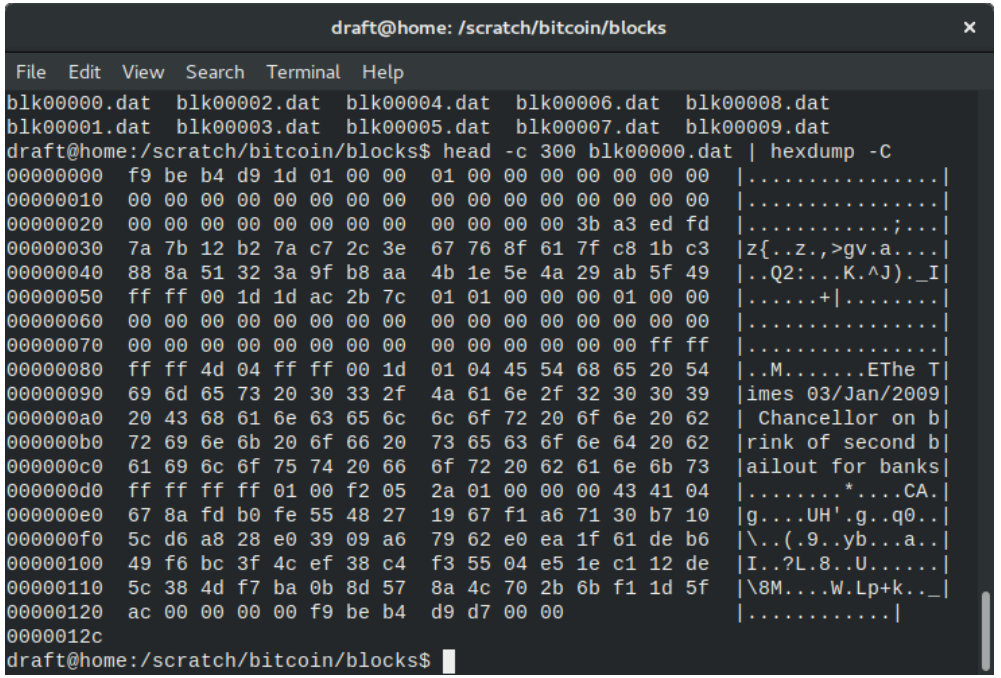
Bitcoin/Blockchain I

Thomas Bocek

19 April 2021

Introduction

- Bitcoin is an experimental digital currency
  - Bitcoin is fully peer-2-peer (no central entity)
  - 1st Bitcoin issued on January 3, 2009
  - Smallest unit: 0.00000001 BTC (1 satoshi)
- Key characteristics
  - Maximum of ~21 million BTC
  - Every transaction broadcast to all peers
    - Every peers knows all transactions (~340 GByte as of today)
  - Validation by proof-of-work (partial hash collision)
    - Difficult to fake proof-of-work
    - No double-spending
- The initiator is unknown so far



OST

Who is Satoshi Nakamoto?

- The New Yorker believes that Satoshi Nakamoto was Michael Clear.
  - Analyzed texts from Nakamoto and searching for linguistic clues
  - 2nd possible candidate Vili Lehdonvirta
- Fast Company argues its either Neal King, Vladimir Oksman, or Charles Bry.
- Other names suggested: Martii Malmi (involved in Bitcoins since the beginning), Jed McCaleb (founder of Ripple), Donal O'Mahony, Michael Peirce, Hitesh Tewari (authors of Electronic Payment Systems for E-Commerce 2nd edition), Shinichi Mochizuki (Math Prof. Kyoto University), Hal Finney, Michael Weber, Wei Dai, Nick Szabo, Craig Wright (wired article),
- Dorian S Nakamoto (a guy with the same name)

- Satoshi is probably rich, first miner, may have ~1mio BTC
- Craig Wright, May 2016: «I'm Satoshi Nakamoto», fails to deliver proof

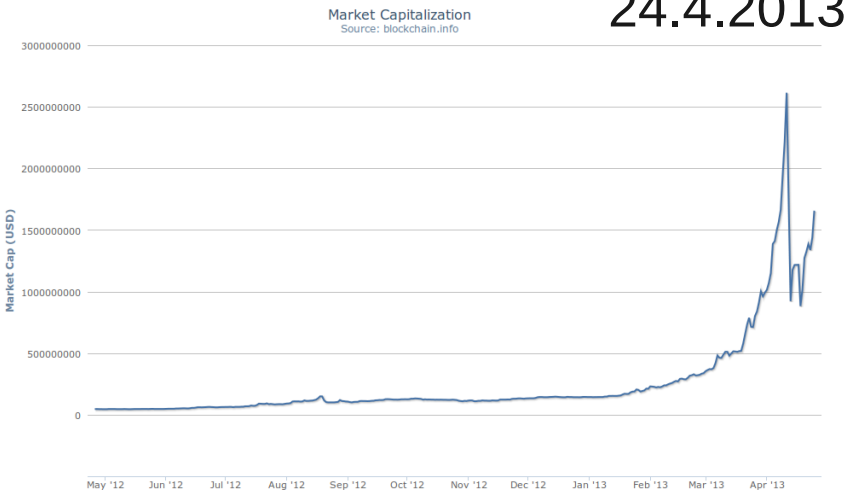
OST

Bitcoin‘s Market Capitalization in USD

- Bitcoin boom, started in 2013 – current price

10.4.2013

24.4.2013



26.4.2014

22.4.2015

OST

Bitcoin‘s Price USD 2021

FEATURES
For *John Carter*, Director Andrew Stanton Leaps From Animation to Live-Action Sci-Fi

START
MIT's Sebastian Seung Wants Computers to Map the Brain

PLAY
The Five-Year Engagement Takes Director Nick Stoller Off the Grid

/ MAGAZINE

FEATURES 19.12

The Rise and Fall of Bitcoin

759 348 123 Tweet +1 Share

By Benjamin Wallace | November 23, 2011 | 2:52 pm | Categories: Wired December 2011

Babbage
Science and technology

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON AND G… ME… OURN…

Like 8k Tweet 625

About Babbage

In this blog, our correspondents report on the inters… between science, technology, culture and policy. T… takes its name from Charles Babbage, a Victorian mathematician and engineer who designed a mec… computer.

Follow @EconSciTech 22.8K followers

RSS feed

Trending topics

Read comments on the site's most popular topics

Period: 1 day | 1 week | 2 weeks | 30 days

Ihre Story, Ihre Informationen, Ihr Hinweis? feedback@20minuten.ch

BITCOIN, DIE DEVISE IM WEB

07. Juni 2011 07:15; *Akt: 07.06.2011 09:11*

Der gefährliche Cyber-Dollar

von Gérard Moinat - Die Online-Währung Bitcoin wirft hohe Wellen. Es sei das «gefährlichste Open-Source-Projekt aller Zeiten» und «gefährde

Bitcoins in the News

As of 2021

- 15.04.2021, Handelsblatt
  «Coinbase-IPO beflügelt Bitcoin – Rekordmarke bleibt in Sicht»
- 17.04.2021, TagesAnzeiger
  «Geldblog: Immobilien, Aktien, BitcoinWie schütze ich mein Vermögen vor Inflation?»
- 13.04.2021, NZZ
  «Bitcoin: Die Kritik wächst, der Wert aber auch»
- 16.04.2021, 20min
  «Darum geht der Dogecoin durch die Decke»
- 16.04.2021, finews
  «Bitcoin: Exakt soviel gehört in ein ausgewogenes Portfolio»

OST

Bitcoin - Introduction

- Not relying on trust, but on strong cryptography
- Weak anonymity (pseudonimity)
  - All peers know all transactions
  - Clustering: e.g. if a transaction has multiple input addresses, assume those addresses belong to the same wallet. (example)
- Not controlled by a single entity
  - Development community, no central bank – forks – Bitcoin Cash, SV
- BIP: Bitcoin Improvement Proposals
- Bitcoins can be exchange for real currencies
  - Several companies allow to exchange BTC for Dollar, Euro, …
- US, CH considered Bitcoin friendly, China (energy), Turkey not that much

Bitcoin in Numbers / Fake Volume

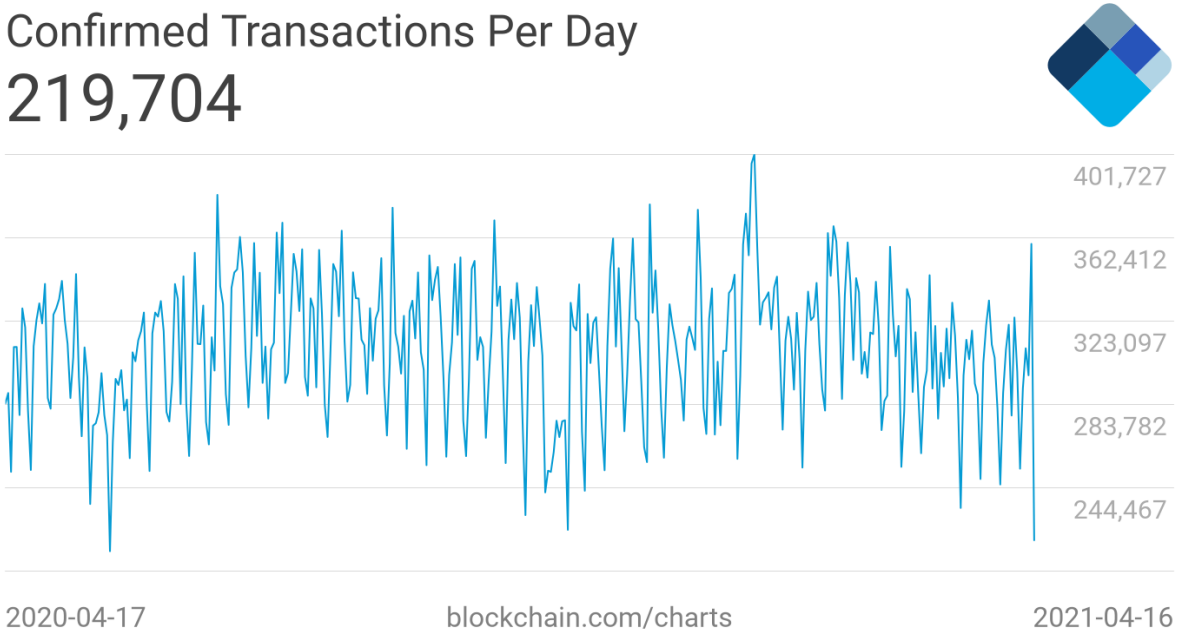
- 1 BTC ≈ 56422 US$ (19.04.2021)
- Total of 18.6 Million BTC mined
  - Market capitalization of 1.1 Trillion US$
  - Volume fake? E.g., CoinBene, RightBTC
- Spread, e.g. ETH
- High spread, should be around 0.01USD

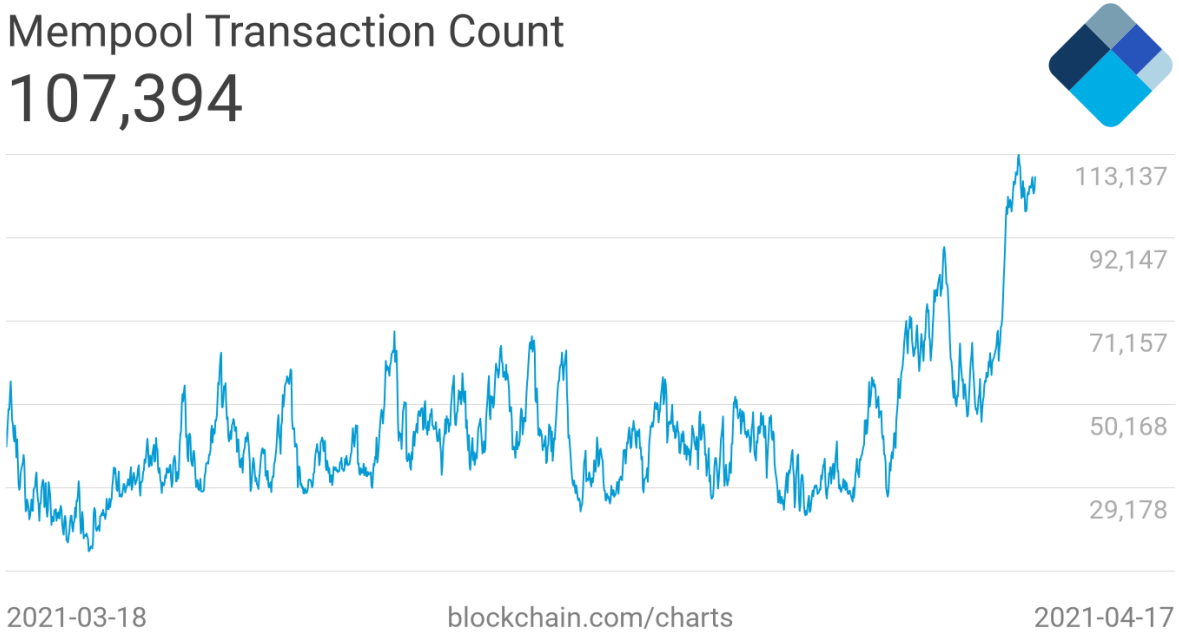
9	Bitfinex	ETH/USD	$2,405.70	$22,429,625	$8,879,712	$149,025,250	0.47%	High	645	Recently
10	Bitstamp	ETH/USD	$2,409.14	$2,117,937	$2,415,352	$120,185,425	0.38%	High	396	Recently
11	Binance	ETH/EUR	$2,423.08	$731,224	$1,017,017	$114,211,638	0.36%	High	727	Recently

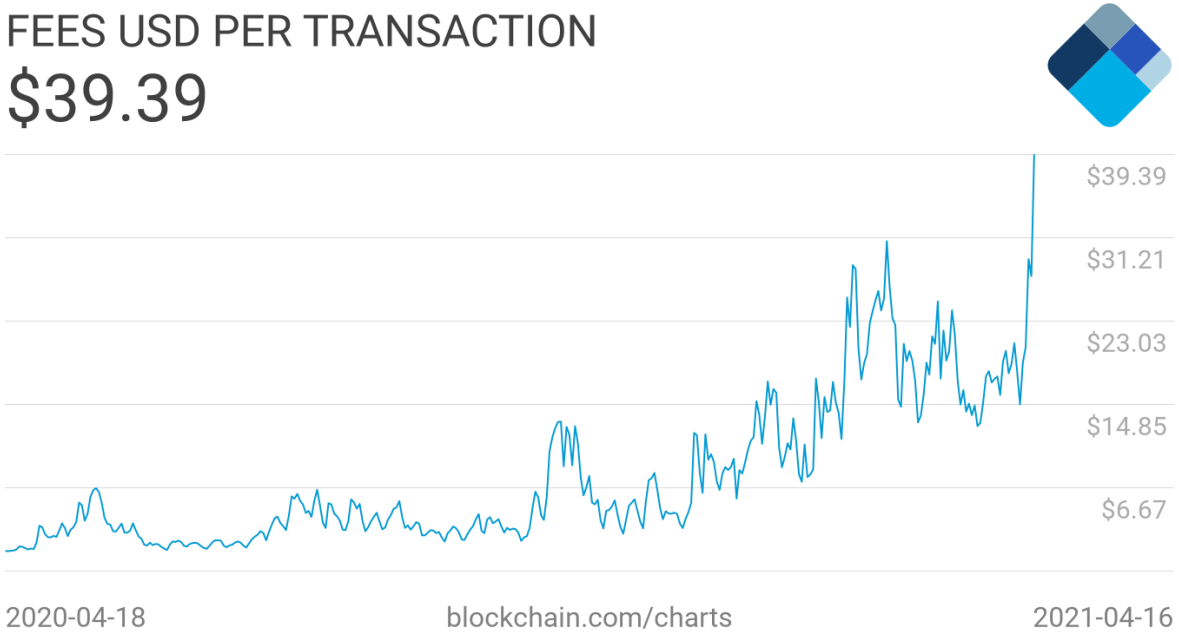
OST

Bitcoin Transactions

- 450,000 transactions per day (highest)
  - ~2-5 transactions per second
- 150,000 BTC traded per day
- Transaction fees per day ~ 140 BTC

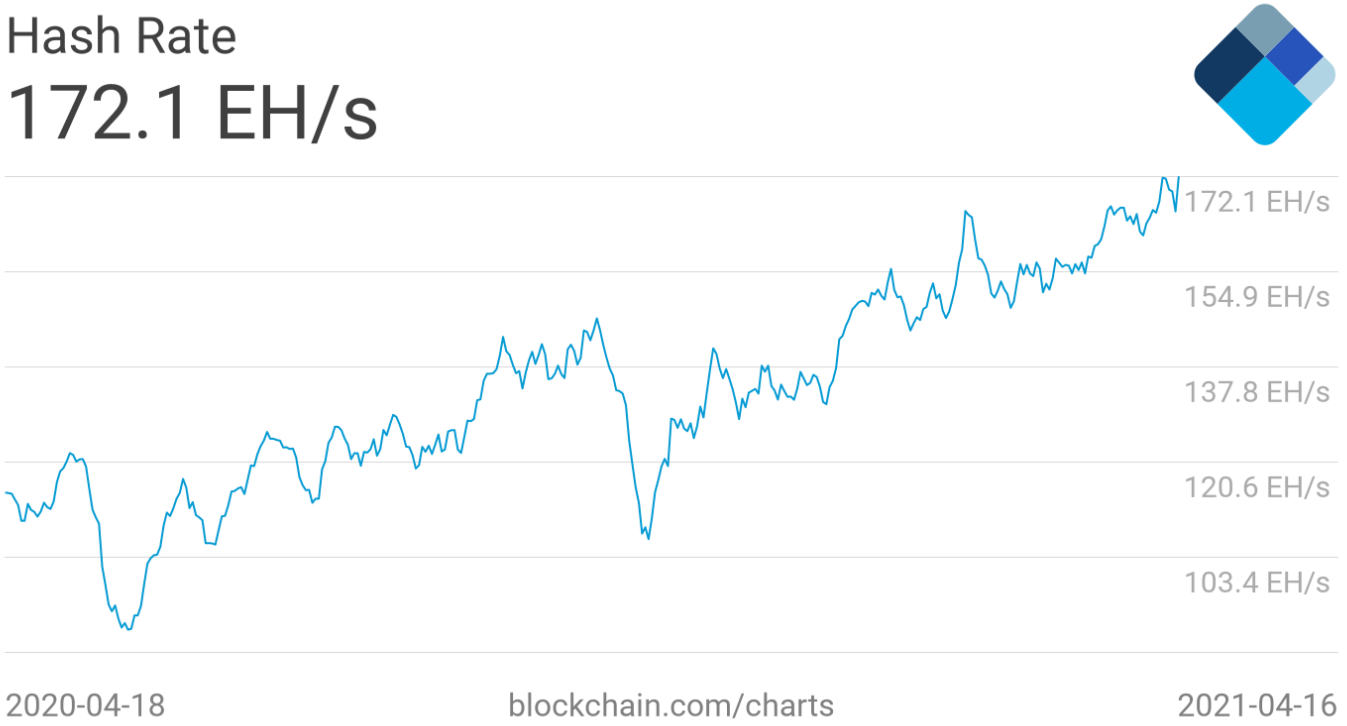


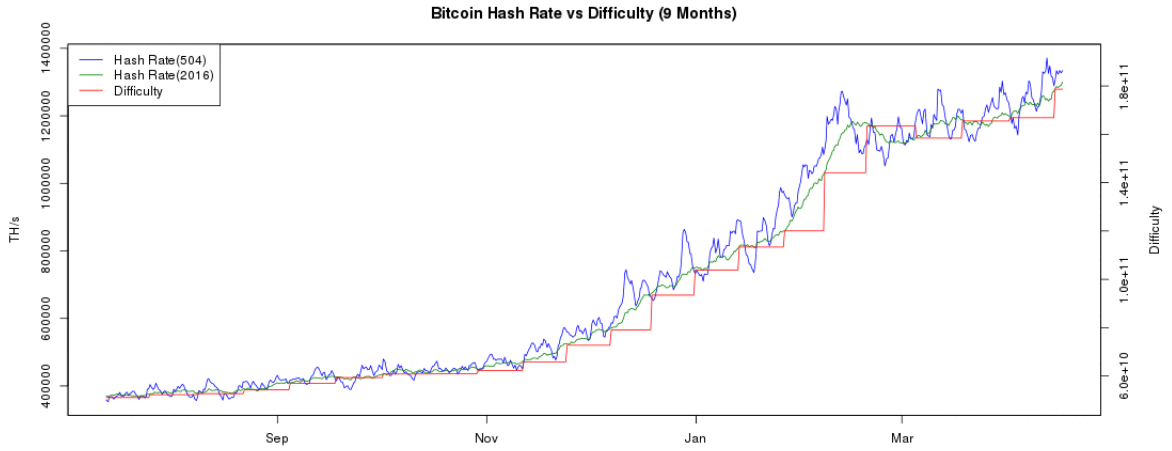




Bitcoin Numbers

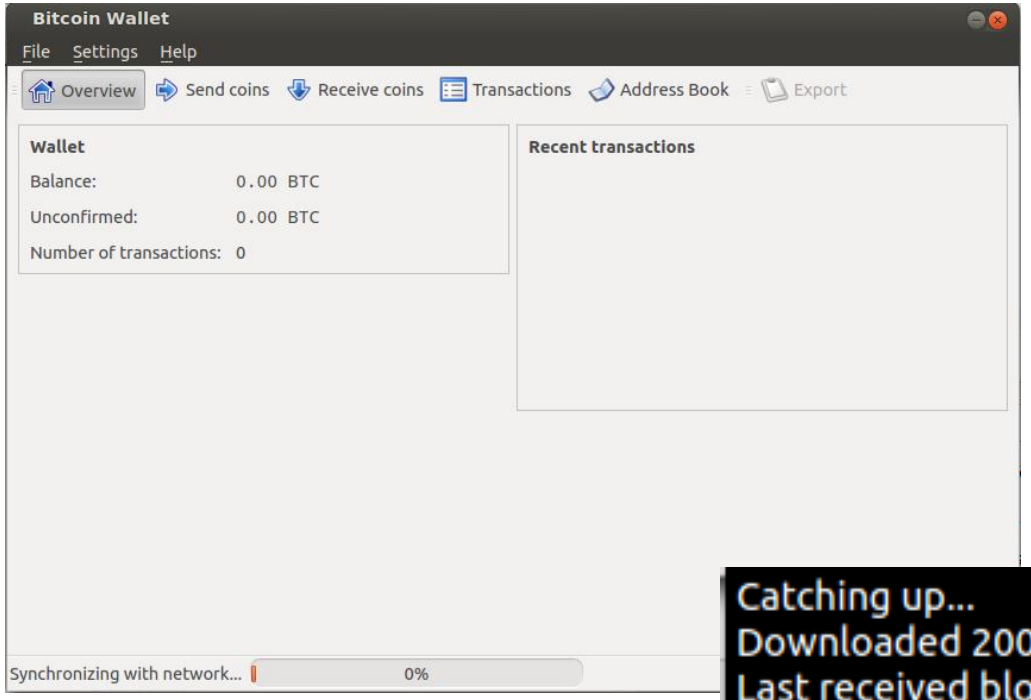
- Network Hashrate
  - ~2.1 YottaFLOPS in 2021
  - ~1.4 YottaFLOPS in 2020
  - ~635 ZettaFLOPS in 2019
  - ~4 ZettaFLOPS in 2015
  - ~714 ExaFLOPS in 2014
  - ~900 PetaFLOPS in 2013
  - ~155 PetaFLOPS in 2012
- Adjust time: ~14 days
- Fastest supercomputer (top500.org) Summit
  148 PetaFLOPS (max), all
  500 ~6 ExaFLOPS
- Fugaku with 442 PetaFLOPS
  - exascale-level processing

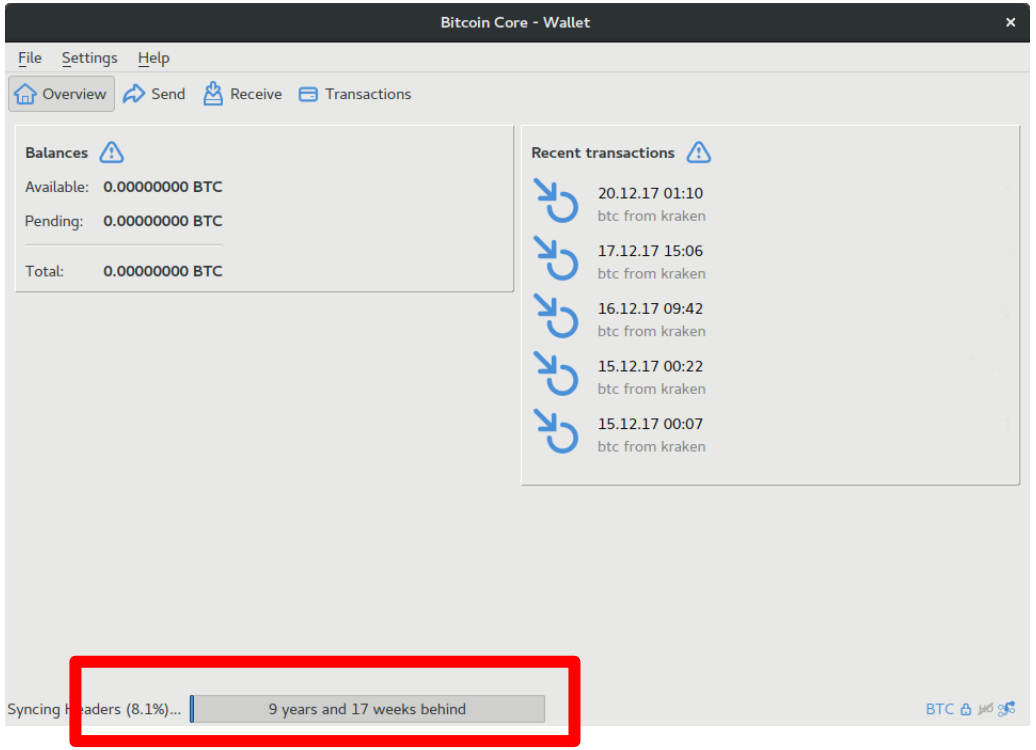




Bitcoin Example

- Bitcoin is also the name of the software
  - 2012: ~2 hours and 1.8G less disk space later…
  - 2013: 8G disk space
  - 2014: 19G disk space
  - 2015: 36G disk space, 2016: 71G, 2019: 220 GB





OST

Bitcoin Example

- Not easy to buy BTC…
  - Especially with credit cards / paypal / okpay

- Decided to transfer via bank
  - SWIFT (financial messaging network) fee 25CHF, send 20USD
  - Exchange rate 0.94000 → fee of 1,000 Yen → ~7.2USD

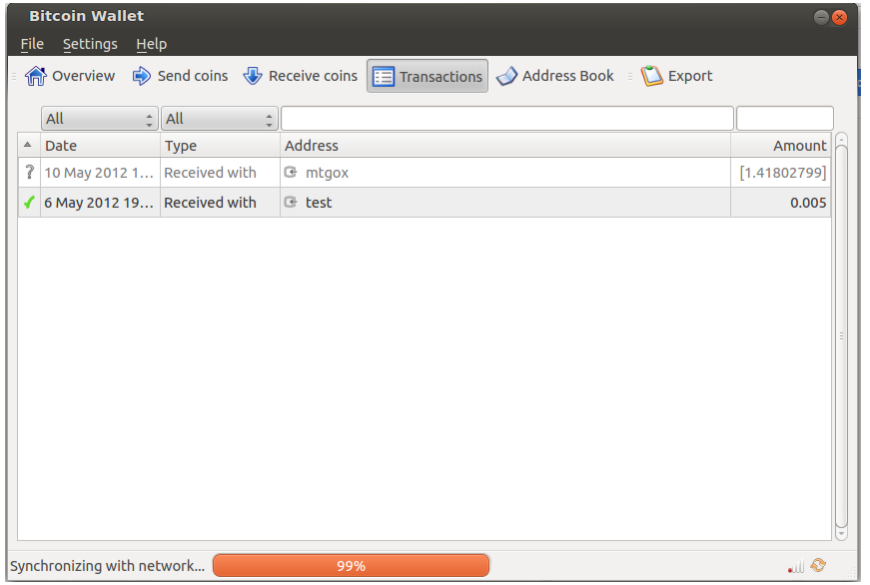
- Spend 43.80 CHF for ~1.42 lousy BTC (2012) on Mt.Gox

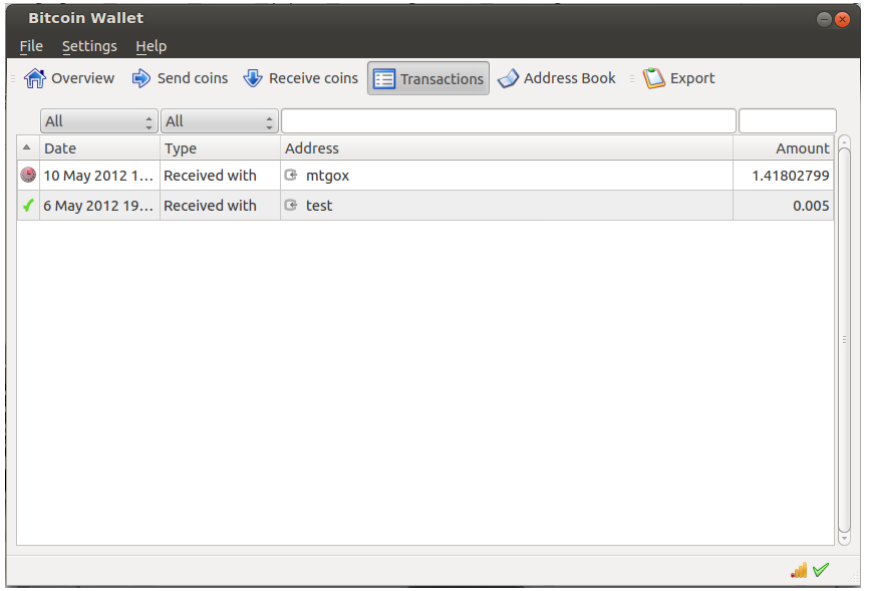
- Now, transfer with bitstamp, kraken: register, proof of residency, SEPA bank transfer → easier

OST

Bitcoin Client

- 2012: Not easy to buy BTC… (credit cards / paypal)
- 2016: more market places
  - http://coinbase.com, http://bitstamp.net, https://www.kraken.com/
  - Not operating: http://mtgox.com, http://bitcoin-24.com, http://bitfloor.com, http://bitcoin-central.net
- 2021: it's getting better
  - SBB
  - Exchanges: KYC, delays
- Good idea: don't leave coins in an online wallet





OST

Mechanism

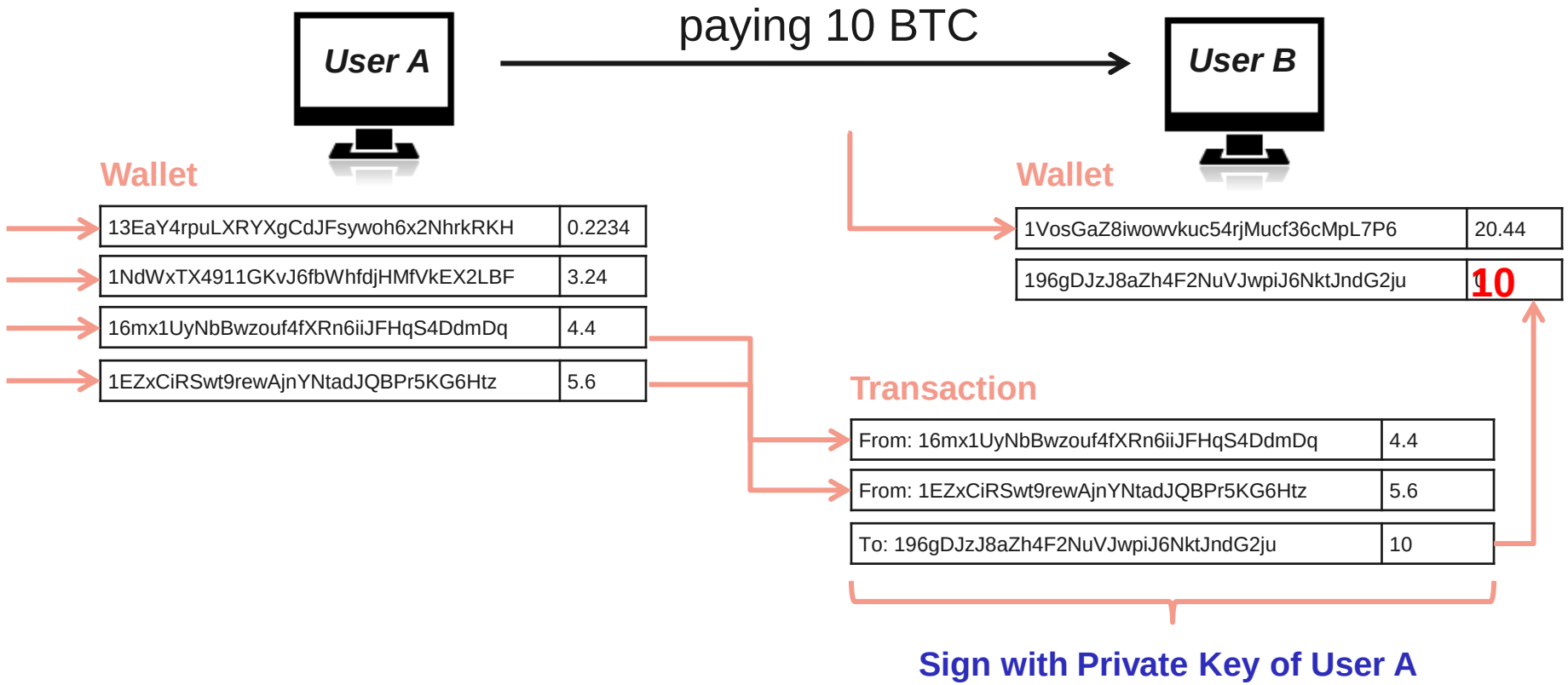
- A wallet has public-private keys (wallet.dat)
  - Public key, ECDSA 256 bit → Bitcoin address (can receive bitcoins)
  - Simple address ~ base58(RIPEM160(Sha256(ecdsa public key)))
    - E.g. 1GCeaKuhDYnNLNR6LGmBtKhPqEJD4KeEtF
  - Private key used for signing transactions

- Transaction
  - Peer A wants to send BTC to peer B → creates transaction message
  - Transaction contains input / output
    - where the BTC came from and where it goes
  - Peer A broadcasts the transaction to all the peers in the network
  - Transaction stored in blocks → block is created / verified ~10min

OST

Key Bitcoin Operations

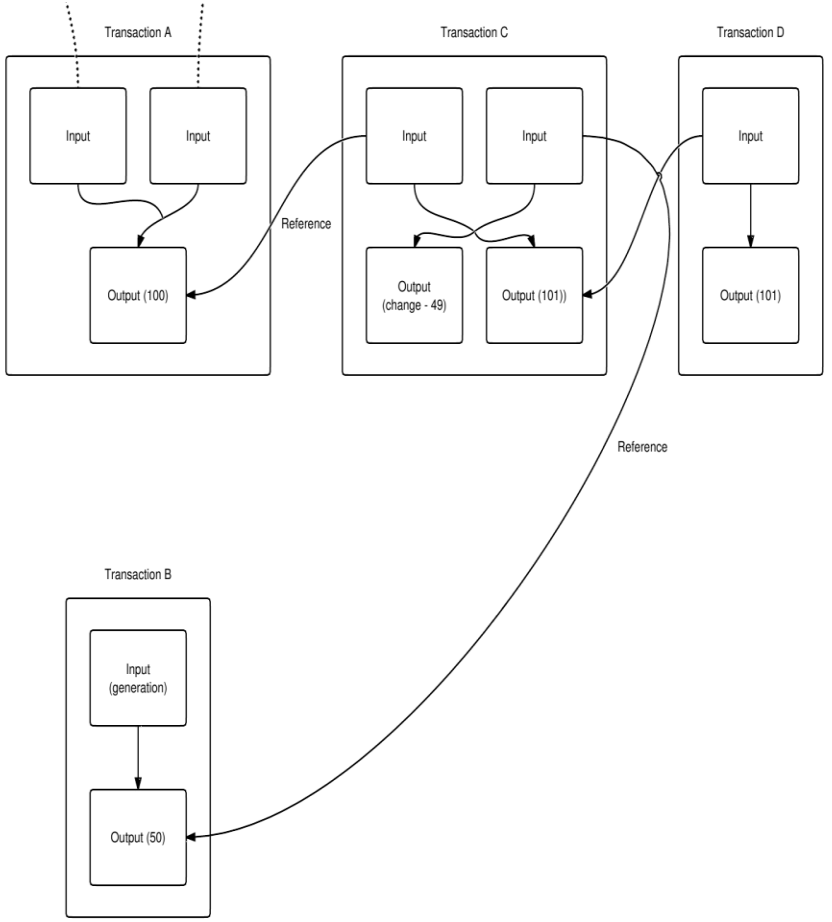
- Private key authorizes the transaction (“access“)
  - If keys are stolen, thief may use “your” coins
  - If keys are lost, coins are lost
  - In UTXO (unspent transaction output) systems, complete output is spent



Mechanism

- Avoiding double spending
  - Transactions in blocks are confirmed.
  - guessing value that results in zero bits (000000000000001805ff174586 b6acf100f733aaf634e92f9580b4fac9272ed97)
  - Chained proofs of work
- Generation of coins
  - Mining / creating blocks → Miner get currently 6.25 BTC per creation
    - adjustable difficulty 6 blocks / h
    - Sometime in 2024 reward will be 3.125, now (6.25)

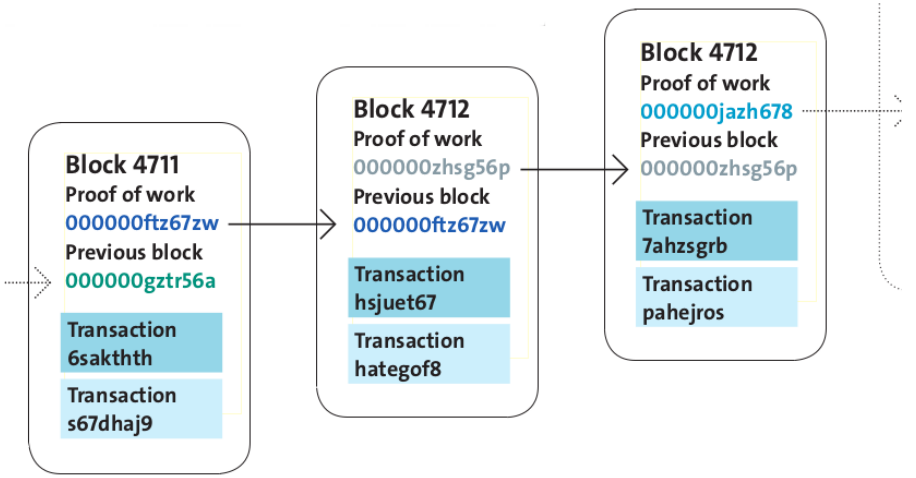
- Transactions have one or more inputs
  - A sends 100 BTC to C, C generates 50 BTC. C sends 101 BTC to D, and send himself some change. D sends the 101 BTC to someone



https://en.bitcoin.it/wiki/Transaction

Blockchain

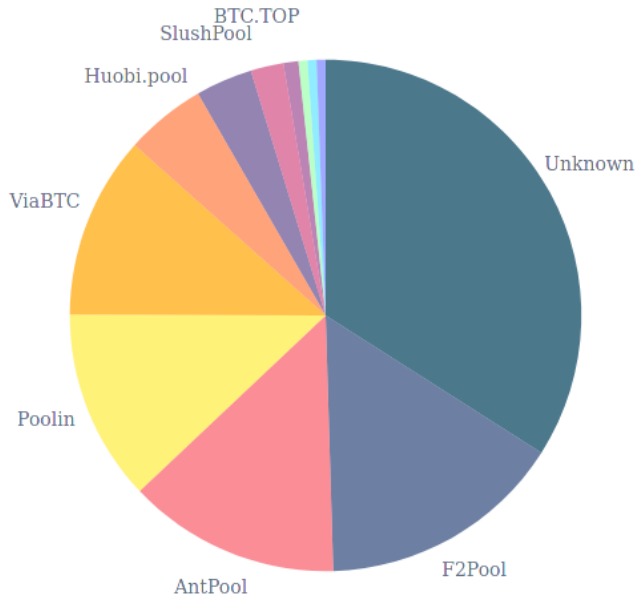
- Transactions are collected in blocks
  - New block created approximately every 10 min
- Blocks contain solved crypto puzzles
  - In the form of partial hash collisions (SHA256)
- A block has a pointer to previous block → **Blockchain**
- Creation of blocks is called mining (reward)
  - Miners use highly specialized hardware!



OST

Mechanism - Mining

- Couple of big miners
  - Miners specialized, AMD GPUs, FPGA, ASIC (application-specific integrated circuit) [1][2][3]



http://blockchain.info/pools

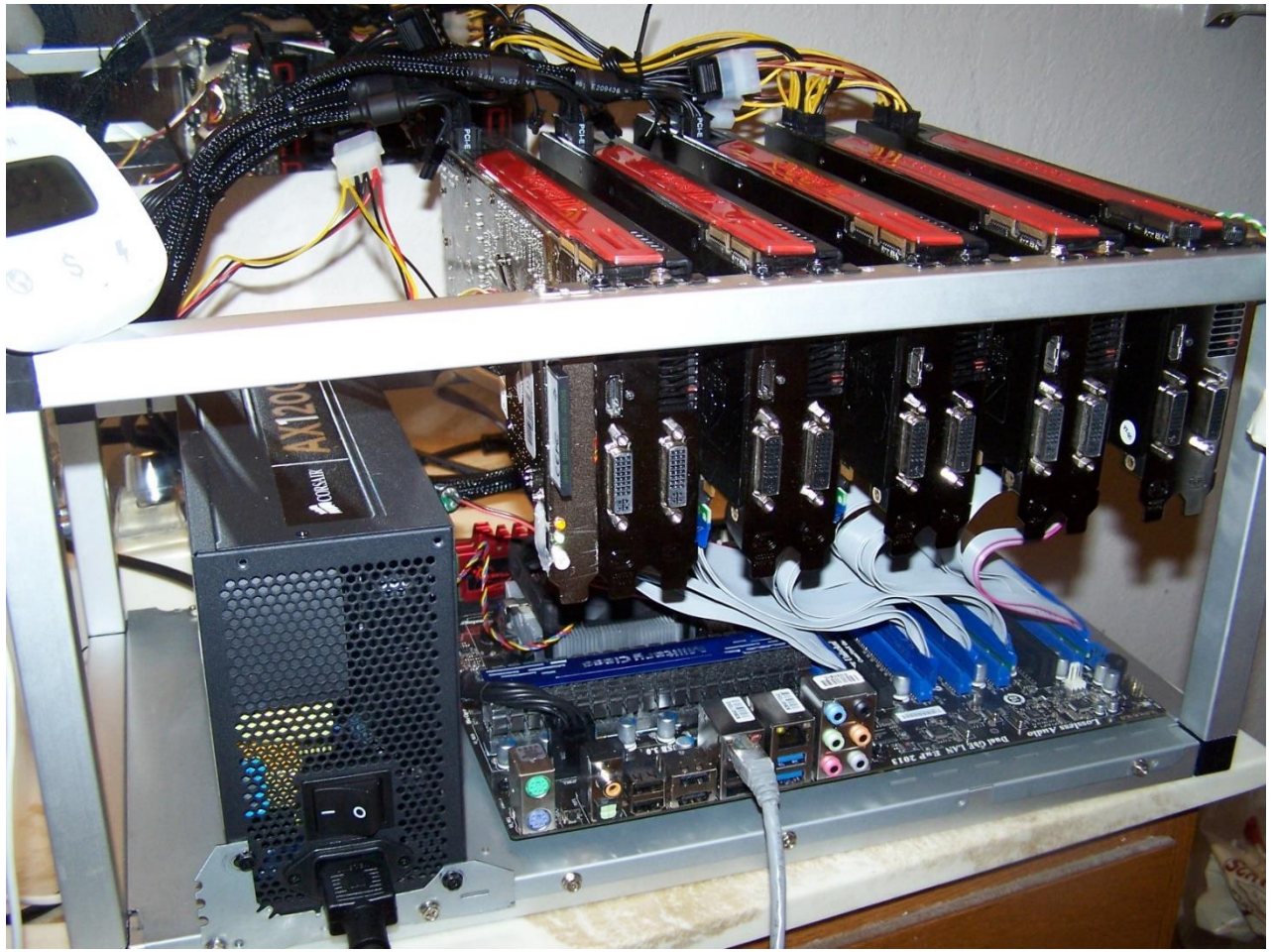
- Mining = creating valid blocks
- Blocks are linked to previous blocks
  - Longest block survive (most difficult)
- Different level of confirmations
  - 3-6 block conf. is considered secure
- Dangerous if someone has more than 50% computing power
  - Can exclude and modify the ordering of transactions

OST

Mining Evolution – CPU

Source: https://99bitcoins.com/20-insane-bitcoin-mining-rigs/

Mining Evolution – GPU



https://bitcointalk.org/index.php?topic=7216.560

Mining Evolution – FPGA

http://www.openmobilefree.net/?p=1308

Mining Evolution – ASIC Farms

- Big mining facilities
  - https://www.youtube.com/watch?v=K8kua5B5K3I
    https://www.youtube.com/watch?v=-z4qbkQ3cK8,
    https://www.youtube.com/watch?v=XWPifXIWPwE,
    https://www.youtube.com/watch?v=OLddN0y2cS8 ,
    https://www.youtube.com/watch?v=4ekOcDG2D8E ,
    https://www.youtube.com/watch?v=-AJhJKSx_70
    https://www.youtube.com/watch?v=f0HC1Udk6-E

Source: https://www.datacenterdynamics.com/en/news/knc-miner-to-build-second-facility-in-the-node-pole/

Mining: Evolution ASIC

- Scenario: old ASIC miner
  - Example: Avalon Batch #2
  - 70GHash/s
- Generated ~0.005CHF per day in 2020
- Generates ~0.02CHF per day in 2021
- Uses 700W
  - 0.6KWh with 0.08 / 0.04CHF
  - Cost per day 2.59 CHF
    (Hochtarif, Mo-Sa 06:00-22:00)
  - Cost per day 1.30 CHF
    (Niedertarif, rest)

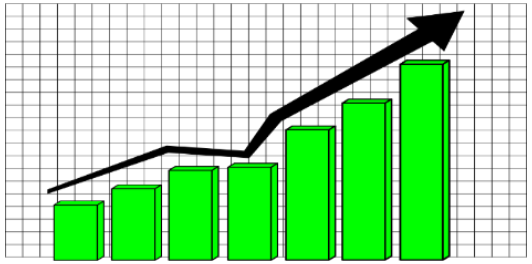
Many Coins – Similar Mechanism

- All electronic backed by scarce resource - avoid: double spending
  - Bitcoin: SHA256 partial hash collision: time, ASIC, electricity
  - Ethereum: variant of Dagger-Hashimoto, time, GPU, memory, electricity, miner store dataset: 1GB, verification only needs 16MB
  - Ethereum: Opcodes in Bitcoin, smart contracts in Ethereum
  - Litecoin: scrypt partial hash collision: time, GPU, memory, electricity
  - Ripple XRP: Unique node list (trusted validators, 1000): web of trust
  - Tezos, next Ethereum: proof of stake:
    - Holding/staking 1% will generate e.g., 1% of coins
    - Energy efficient / proof of stake
  - Cardano/EOS/…many more

OST

Discussion (1)

- Advantages
  - Low (fixed) tx fees
    - ~102 satoshi per byte / 14USD
  - Scalable
    - Hardware/storage gets faster



  - Anonymity
    - No privacy concerns/ datamining difficult

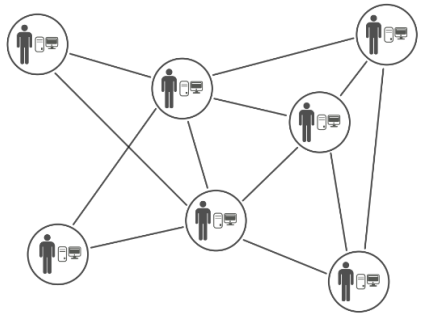
- Disadvantages
  - Power consumption
    - ~ as much as Netherlands
  - Not scalable
    - Bitcoin with 5 tps vs. VISA 57,000 tps (23.12)
      [tps: transactions per sec]

  - Anonymity
    - Can be used for illegal activities

OST

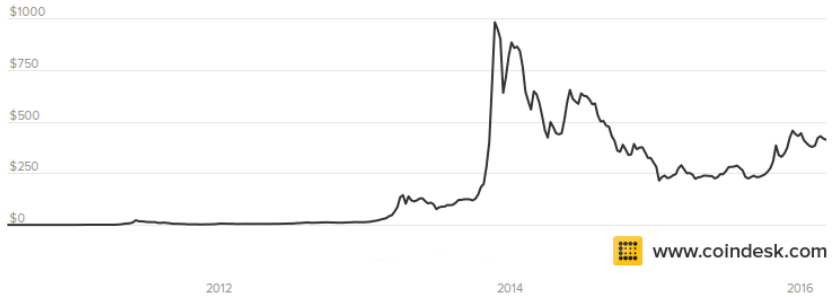
Discussion (2)

- Advantages
  - No major “crashes”
    - Mt.Gox was exchange site!
  - Decentralized
    - Open protocol
    - Forks



  - Many other blockchain use cases
    - Smart contracts

- Disadvantages



  - Central elemements
    - Core developers