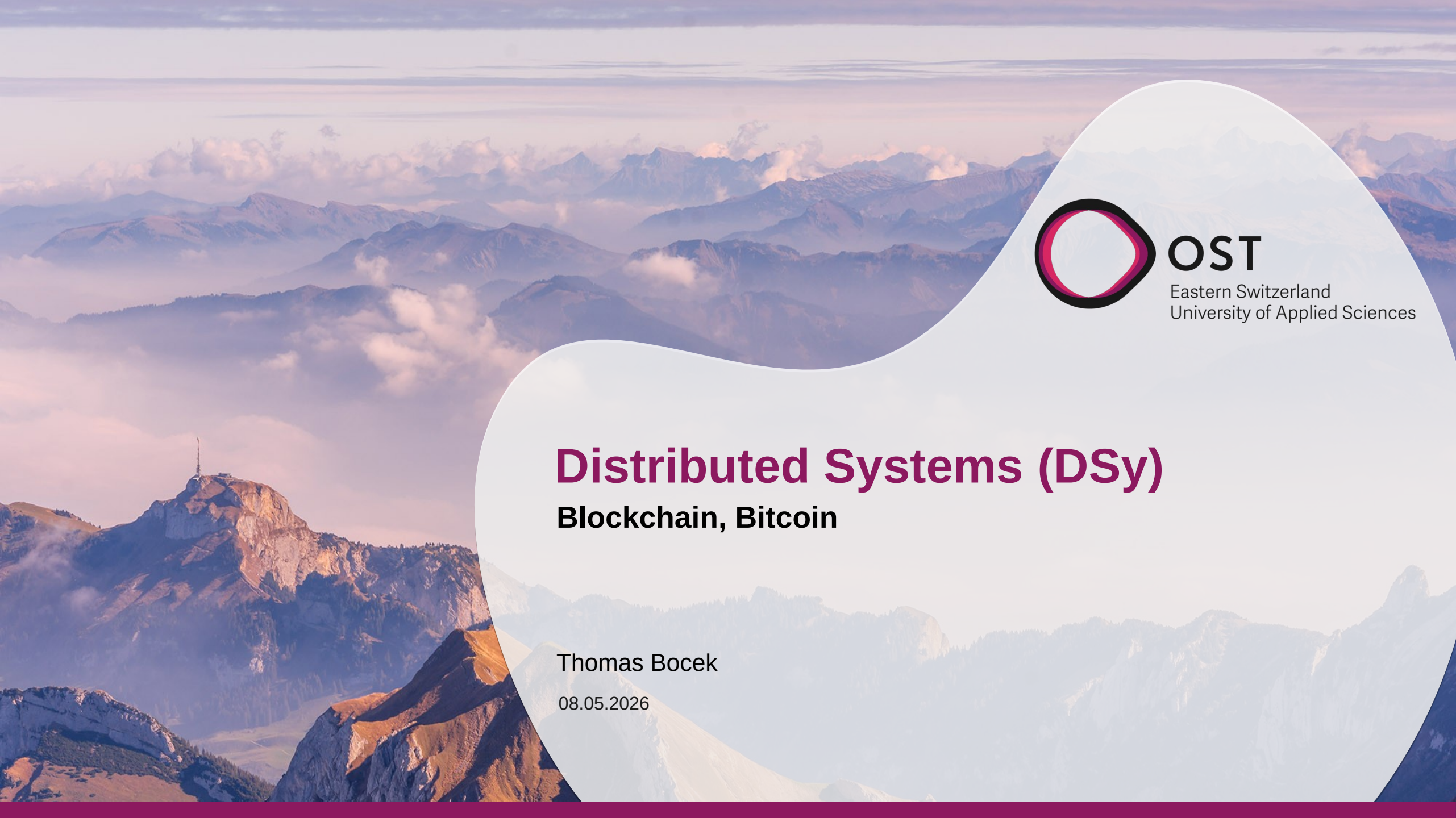


OST
Eastern Switzerland
University of Applied Sciences

Distributed Systems (DSy)

Blockchain, Bitcoin

Thomas Bocek

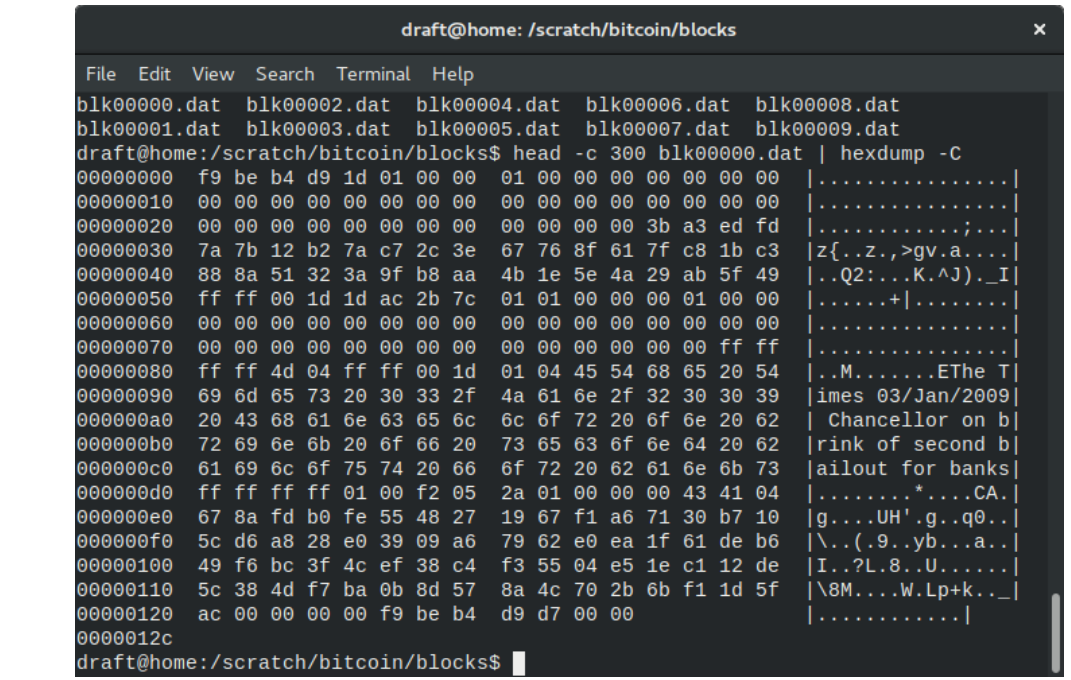
08.05.2026

Learning Goals

- Lecture 12 (Blockchain, Bitcoin)
  - Understand how Bitcoin works as a peer-to-peer system
  - Get familiar with UTXO, mining, and proof-of-work
  - Be aware of risks like the 51% attack
  - Reflect on advantages and disadvantages of Bitcoin

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 (~736 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



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 → 2024: "Judge rules computer scientist not Bitcoin inventor"
- Current: Satoshi Nakamoto Identity: 2026 Suspects and the $85B Question [link]

Bitcoin‘s Market Capitalization in USD

- Bitcoin boom, started in 2013 – current price

OST

Bitcoin‘s Price USD 2026

WIRED SUBSCRIBE » SECTIONS » BLOGS » REVIEWS » VIDEO » HOW

Sign In | RSS Feeds

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

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

Tweet +1 Share

The Economist

Log in | Register | Subscribe

Digital & mobile | Events | Topics A-Z | Newsletters | Jobs

Tuesday May 8th 2012

Search

World politics | Business & finance | Economics | Science & technology | Culture | Blogs | Debate | The World in 2012 | Multimedia | Print edition

Babbage

Science and technology

Previous | Next | Latest Babbage | Latest from all our blogs

Comment (45) | Print | E-mail | Permalink | Reprints & permissions

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

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON

Like Tweet 625

de fr it

Ihr Ort: Zürich 19° Mi 20° Do 26° Über Schweiz Registrieren Login

20 minuten ONLINE

Video TV Infografik Games E-Prospekte RSS Inhalt A-Z Suchen

Schweiz Ausland Panorama Wirtschaft Sport Blockbuster-Wi People Entertainment Digital Mehr

News SMI Alle Indices Ratgeber Geld Trading Anlageprodukte Finanzrechner Dossiers

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

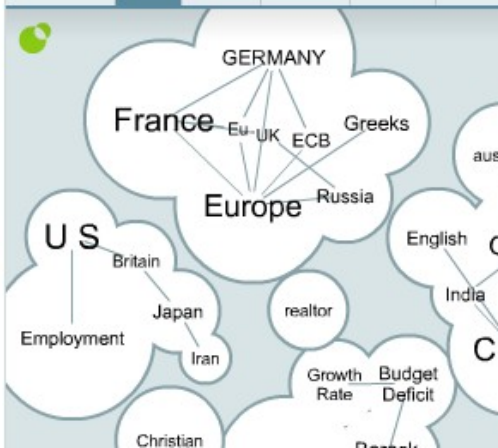
von Gérard Moinat - Die Online-Währung Bitcoin wirft hohe Wellen. Es sei das «gefährlichste Open-Source-Projekt aller Zeiten» und «gefährde

ought ought
ly,
stment
y a

Trending topics

Read comments on the site's most popular topics

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



From 2011

Bitcoins in the News

As of 2026

- 29.04.2026, 20min
  ”Wetten auf den Atomkrieg: So funktionieren Prediction Markets” [link]
- 15.04.2026, Faz
  ”Ist das Geheimnis um Satoshi Nakamoto gelüftet?” [link]
- 21.02.2026, swissinfo.ch
  ”Bitcoin causes 114 million tonnes of CO2 per year” [link]
- 02.05.2026, Forbes
  ”‘Go Time’—White House Quietly Confirms ‘Imminent’ May Bitcoin Price Game-Changer” [link]

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) not that much

Bitcoin in Numbers / Fake Volume

- Spread, e.g. ETH
- High spread, should be around 0.01USD

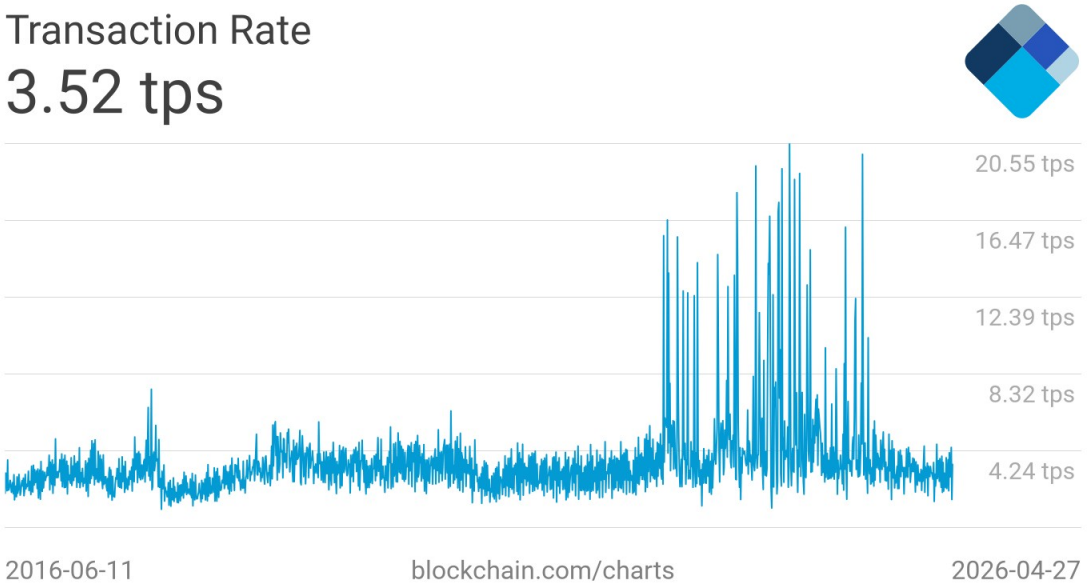
- Total of 20 Million BTC mined
  - Market capitalization of 1.5 Trillion US$
  - Volume fake? e.g., CoinBene, RightBTC

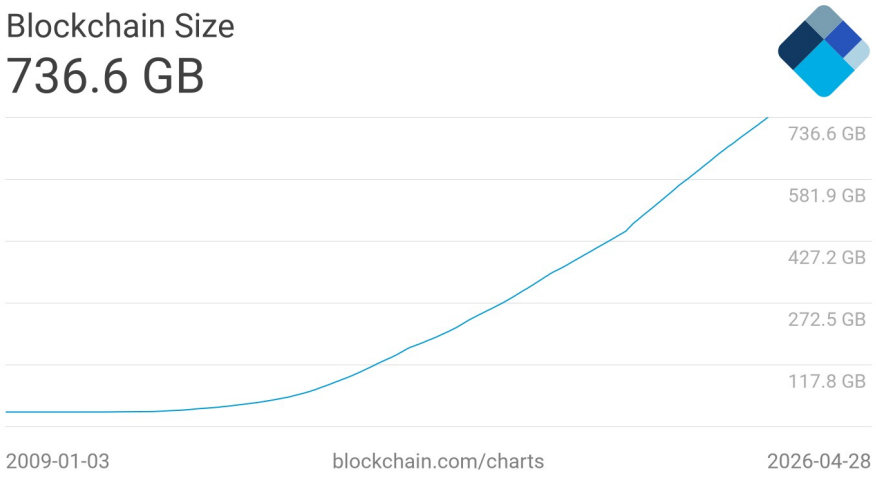
9	Bitfinex	ETH/USD	$2,405.70	$22,429,625	$8,879,712	$149,025,250	0.47%	High	645	Recently
10	Bitstamp	ETH/USD	$2,409.14	$2,117,937	$2,415,352	$120,185,425	0.38%	High	396	Recently
11	Binance	ETH/EUR	$2,423.08	$731,224	$1,017,017	$114,211,638	0.36%	High	727	Recently

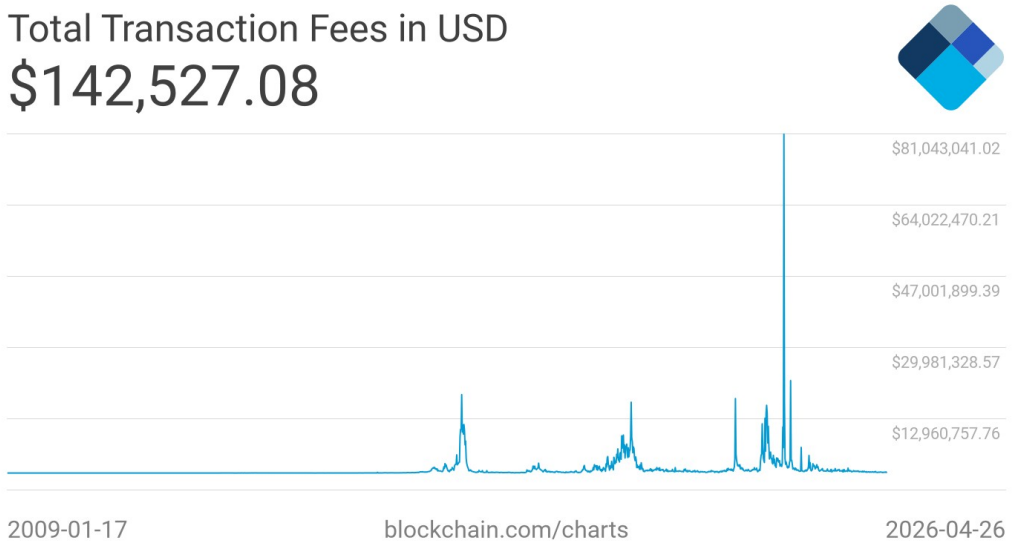
OST

Bitcoin Transactions

- 920000 transactions per day (highest)
  - ~3-11 transactions per second
- Transaction fees / day: $150k, $78m max
  ~ max. (20.04.2024)
- Blocksize

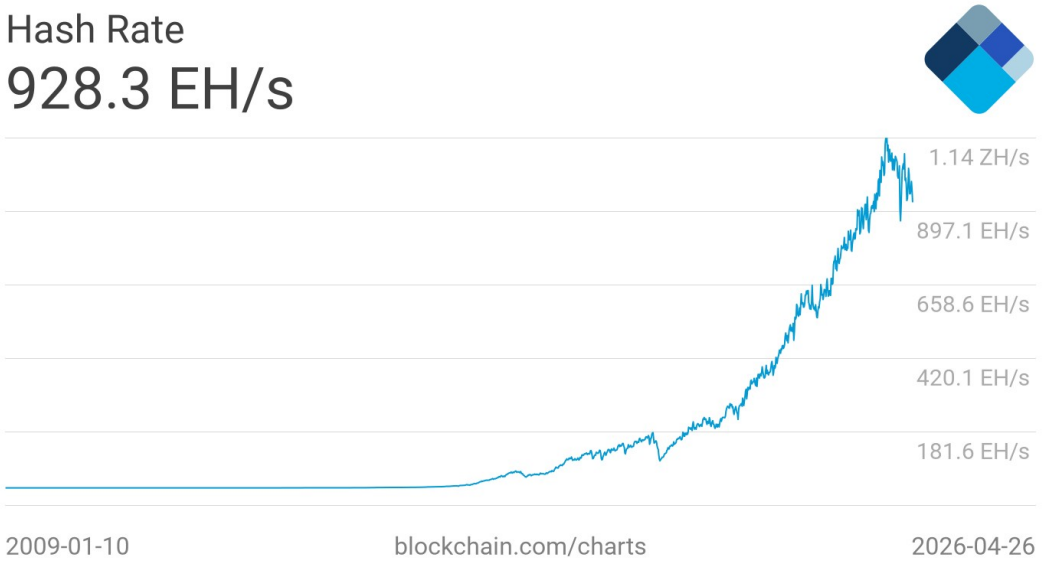


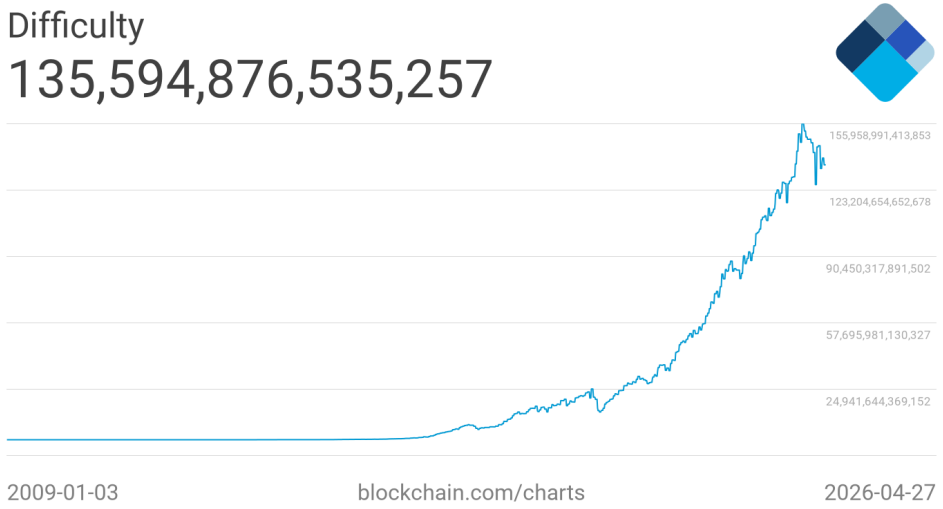




Bitcoin Numbers

- Network Hashrate (1 hash = 12.7 KFLOPs), 1000Eh/s
  - ~12.7 YottaFLOPS in 2025/2026
  - ~9.1 YottaFLOPS in 2024
  - ~4.3 YottaFLOPS in 2023
  - ~3 YottaFLOPS in 2022
  - ~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) El Capitan 2700 PetaFLOPS (max), all 500 ~22.1 ExaFLOPS





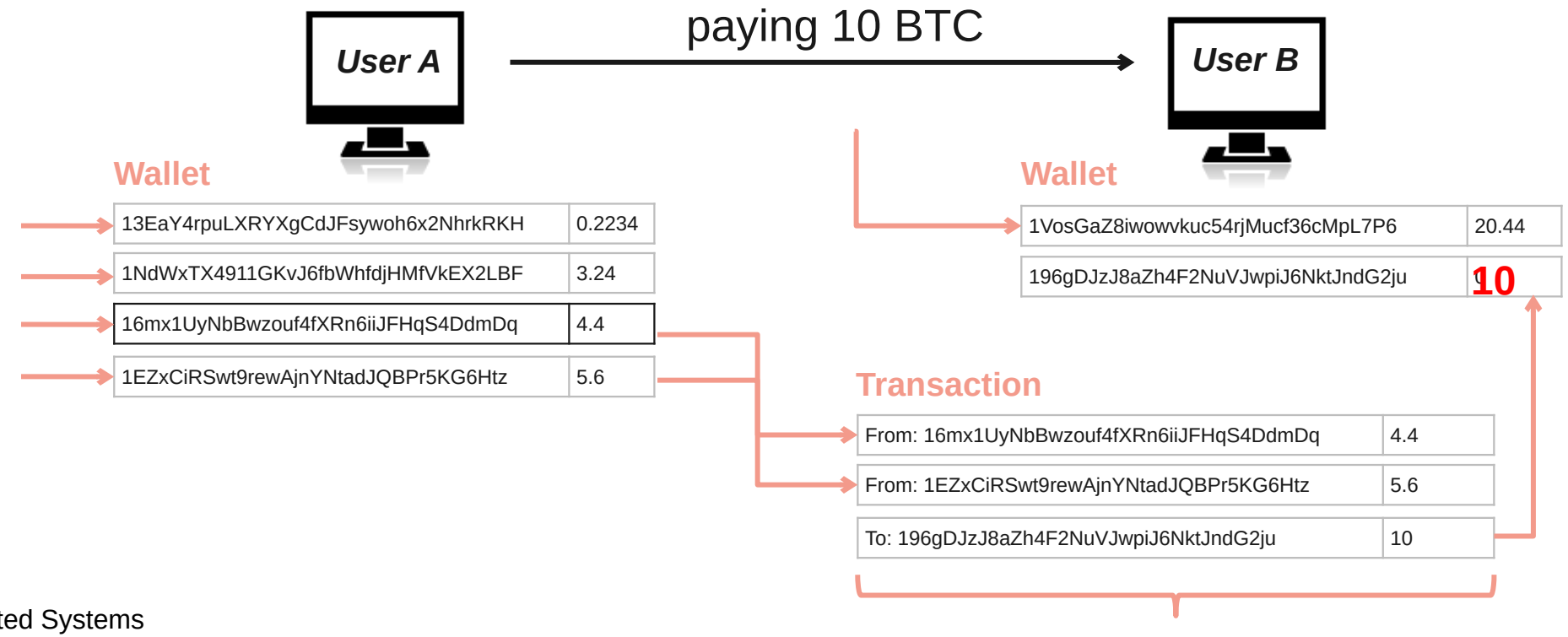
Mechanism

- 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

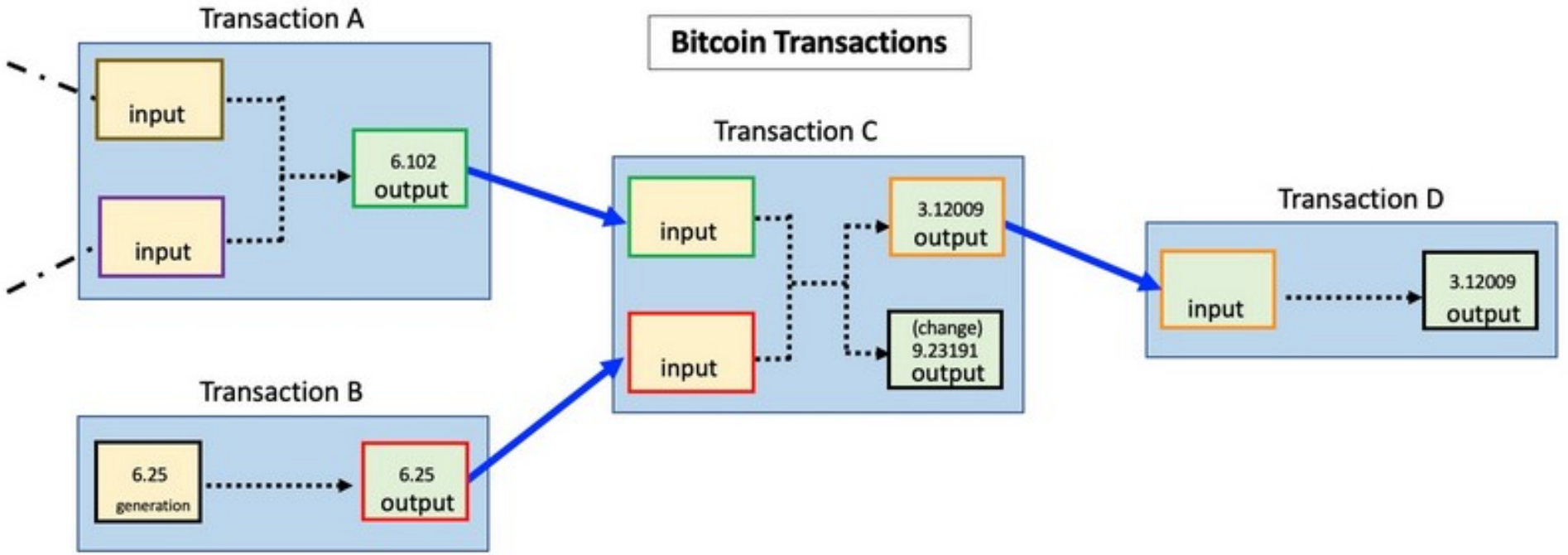
Key Bitcoin Operations

- 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



OST

Transactions

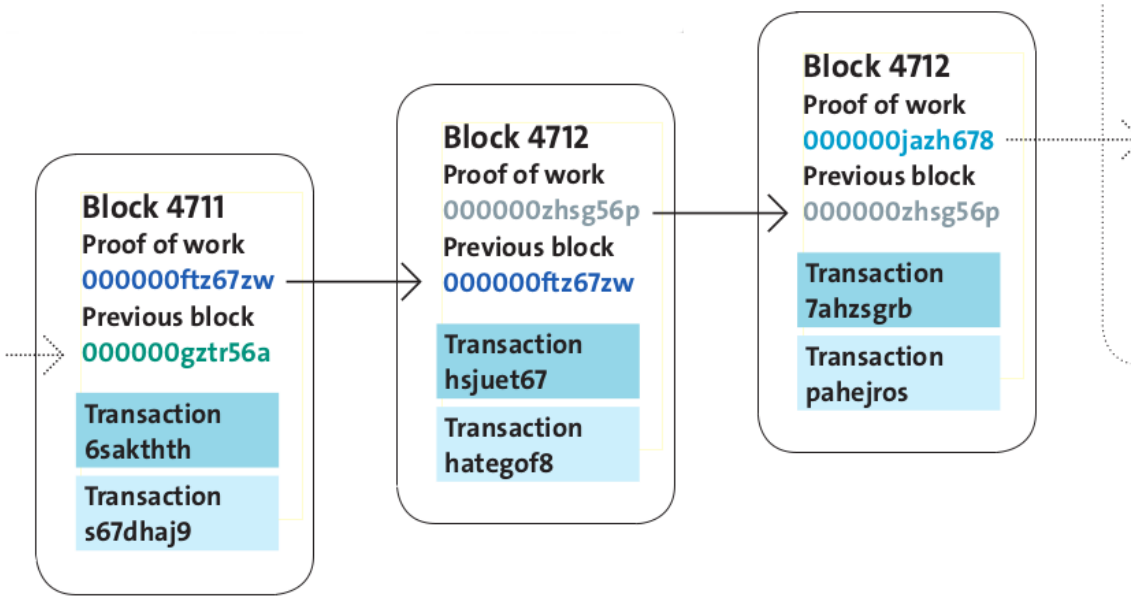


https://en.bitcoin.it/wiki/Transaction

OST

Blockchain

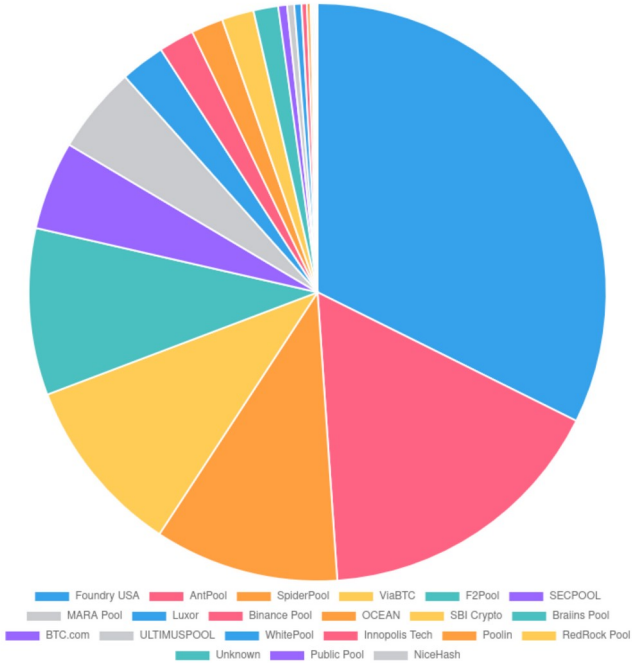
- Transactions are collected in blocks
  - New block created approximately every 10 min
- Blocks contain
  solved crypto puzzles
  - In the form of partial hash collisions (SHA256)
- A block has a pointer to previous block → Blockchain
- Creation of blocks is called mining (reward)
  - Mining / creating blocks → Miner get currently 3.125 BTC per creation
    - adjustable difficulty 6 blocks / h
    - Sometime in 2028 reward will be 1.5625



OST

Mechanism - Mining

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



https://bitref.com/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

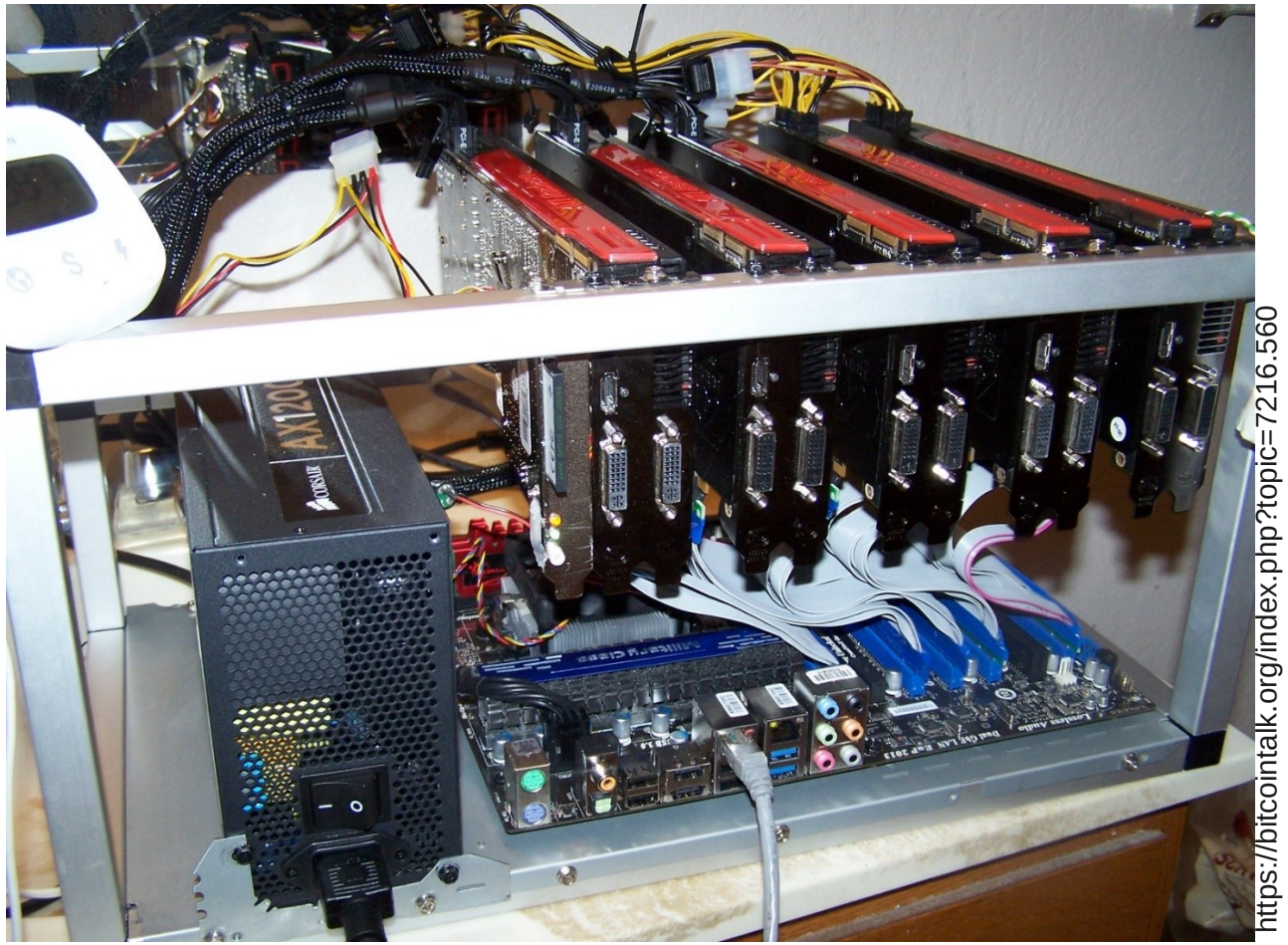
OST

Mining Evolution – CPU

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

OST

Mining Evolution – GPU



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

OST

Mining Evolution – FPGA

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

OST

Mining Evolution – ASIC Farms

- Big mining facilities
  - Inside a Billion Dollar Bitcoin Mining Farm!
    https://www.youtube.com/watch?v=82vMOVREXzM
  - Private Tour of Riot's MASSIVE Whinstone Bitcoin Mining Facility
    https://www.youtube.com/watch?v=La7vMl1txCU
  - Inside Iceland's Massive Bitcoin Mine
    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
- Generates ~0.004CHF per day in 2026
- Uses 700W
  - 16.8kWh
  - Cost per day 3.69 CHF
    (Hochtarif, 0.2CHF per kWh)
  - Cost per day 2.18 CHF
    (Niedertarif, 0.15CHF per kWh)

OST

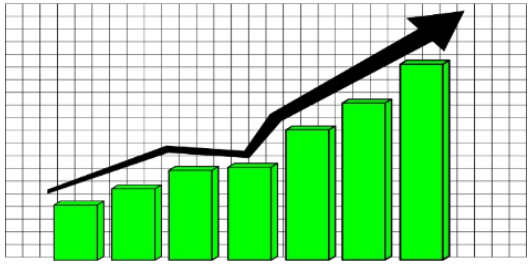
Many Coins – Similar Mechanism

- All electronic backed by scarce resource - avoid: double spending
  - Bitcoin: SHA256 partial hash collision: time, ASIC, electricity (proof of work)
  - Ethereum: Opcodes in Bitcoin, smart contracts in Ethereum (proof of stake)
    - Energy efficient / proof of stake
  - Litecoin: scrypt partial hash collision: time, GPU, memory, electricity
  - Ripple XRP: Unique node list (trusted validators, 1000): web of trust
  - …many more

OST

Discussion (1)

- Disadvantages
  - Power consumption
    - ~ more than Poland
  - Not scalable
    - Bitcoin with ~7 tps vs. VISA 57,000 tps (23.12)
      [tps: transactions per sec]



  - Anonymity
    - Can be used for illegal activities

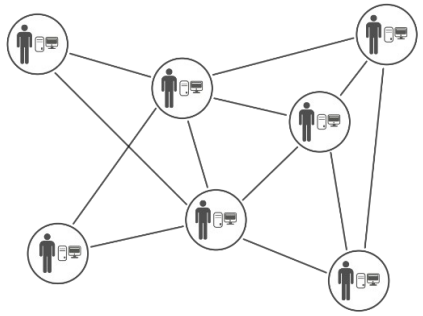
- Advantages
  - Low (fixed) tx fees
    - ~0.5 - 1 satoshi per byte / 0.25USD (~200bytes tx)
  - Scalable
    - Hardware/storage gets faster

  - Anonymity
    - Preserving privacy

OST

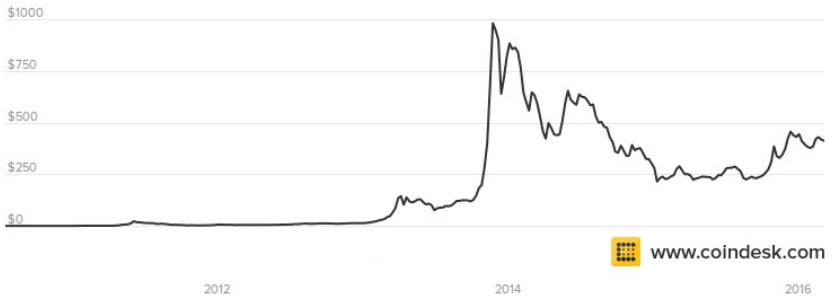
Discussion (2)

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



  - Many other blockchain use cases
    - Smart contracts

- Disadvantages
  - Volatile exchange rate



  - Central elemements
    - Core developers