



OST

Eastern Switzerland
University of Applied Sciences

Distributed Systems (DSy)

Blockchain, Bitcoin

Thomas Bocek

18.05.2025

Learning Goals

- Lecture 13 (Blockchain, Bitcoin, Ethereum, Smart Contracts)
 - Basic concepts (UTXO, account-based, mining, blockchain)
 - Advantages / disadvantages

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 (~660 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



```
draft@home: /scratch/bitcoin/blocks
File Edit View Search Terminal Help
blk000000.dat blk000002.dat blk000004.dat blk000006.dat blk000008.dat
blk000001.dat blk000003.dat blk000005.dat blk000007.dat blk000009.dat
draft@home:/scratch/bitcoin/blocks$ head -c 300 blk000000.dat | hexdump -C
00000000 f9 be b4 d9 1d 01 00 00 01 00 00 00 00 00 00 00 |.....|
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000020 00 00 00 00 00 00 00 00 00 00 00 00 3b a3 ed fd |.....;...|
00000030 7a 7b 12 b2 7a c7 2c 3e 67 76 8f 61 7f c8 1b c3 |z{..z.,>gv.a...|
00000040 88 8a 51 32 3a 9f b8 aa 4b 1e 5e 4a 29 ab 5f 49 |..Q2:..K.^J)..I|
00000050 ff ff 00 1d 1d ac 2b 7c 01 01 00 00 00 01 00 00 |.....+|.....|
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff |.....|
00000080 ff ff 4d 04 ff ff 00 1d 01 04 45 54 68 65 20 54 |..M.....EThe T|
00000090 69 6d 65 73 20 30 33 2f 4a 61 6e 2f 32 30 30 39 |imes 03/Jan/2009|
000000a0 20 43 68 61 6e 63 65 6c 6c 6f 72 20 6f 6e 20 62 | Chancellor on b|
000000b0 72 69 6e 6b 20 6f 66 20 73 65 63 6f 6e 64 20 62 |rink of second b|
000000c0 61 69 6c 6f 75 74 20 66 6f 72 20 62 61 6e 6b 73 |ailout for banks|
000000d0 ff ff ff ff 01 00 f2 05 2a 01 00 00 00 43 41 04 |.....*....CA.|
000000e0 67 8a fd b0 fe 55 48 27 19 67 f1 a6 71 30 b7 10 |g....UH'.g..q0..|
000000f0 5c d6 a8 28 e0 39 09 a6 79 62 e0 ea 1f 61 de b6 |\\..(.9..yb...a..|
00000100 49 f6 bc 3f 4c ef 38 c4 f3 55 04 e5 1e c1 12 de |I..?L.8..U.....|
00000110 5c 38 4d f7 ba 0b 8d 57 8a 4c 70 2b 6b f1 1d 5f |\\8M....W.Lp+k..._|
00000120 ac 00 00 00 00 f9 be b4 d9 d7 00 00 |.....|
0000012c
draft@home:/scratch/bitcoin/blocks$
```

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”

Bitcoin's Market Capitalization in USD

- Bitcoin boom, started in 2013 – current price



Bitcoin's Price USD 2025



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

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

759 348 123
Tweet +1 Share

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



Comment (45)

Print

E-mail

Permalink

Reprints & permissions

Previous

Next

Latest Babbage

Latest from all our blogs

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 die Schweiz

Registrieren

Login



Video TV Infografik Games E-Prospekte

Schweiz

Ausland

Panorama

Wirtschaft

Sport

Lokal

People

Entertainment

Digital

Mehr

News

SMI

Alle Indices

Ratgeber Geld

E-Marketing

Angebot

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

powered by X homegate.ch

Immobilien in Zürich

1.0 Zimmer Zi, Charmante
möblierte Zimmer im Herzen
von Zürich
Hornergasse 15 8001 Zürich



Immobilien finden

PLZ

8000

Preis

unlim.

bis

unlim.

About Babbage

In this blog, our correspondents report on the inter-
between science, technology, culture and policy. The
takes its name from Charles Babbage, a Victorian
mathematician and engineer who designed a meca-
nical 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



Bitcoins in the News

As of 2025

- 10.05.2025, 20min
"Krypto-Reserve: Kaufen die USA jetzt wirklich Bitcoin?" [[link](#)]
- 08.05.2025, Faz
"Bitcoin steigt über 100.000 US-Dollar" [[link](#)]
- 01.03.2025, swissinfo.ch
"Swiss central bank chief rejects holding bitcoin in reserves" [[link](#)]
- 12.05.2025, CoinDesk
"Bitcoin Eyes Record High Above \$109K as U.S. Cuts Tariffs on Chinese Goods to 30% From 145%" [[link](#)]

Bitcoin - Introduction

- Not relying on trust, but on strong cryptography
- Weak anonymity (pseudonymity)
 - 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

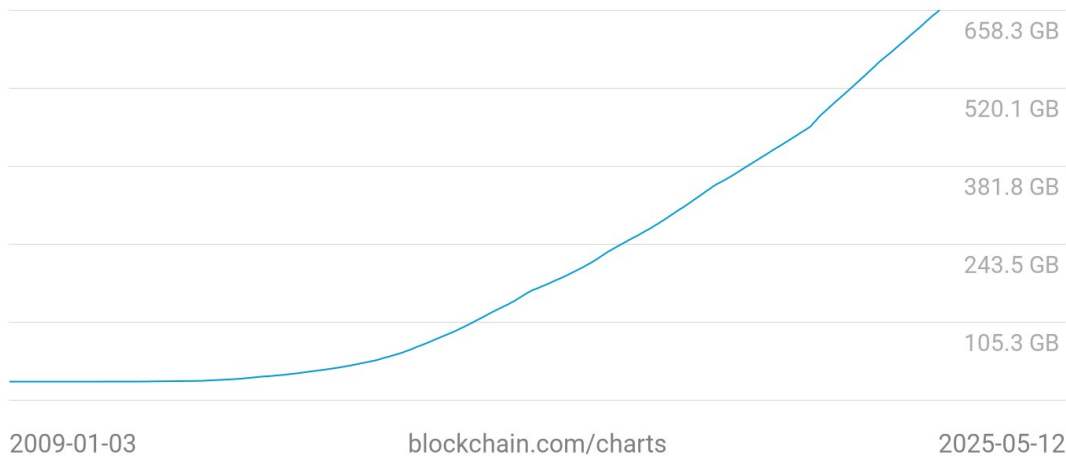
- Spread, e.g. ETH
- High spread, should be around 0.01USD
- 1 BTC $\approx$ 103'000 US\$ (19.05.2025)
- Total of 20 Million BTC mined
 - Market capitalization of 2 Trillion US\$
 - Volume fake? e.g., CoinBene, RightBTC

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

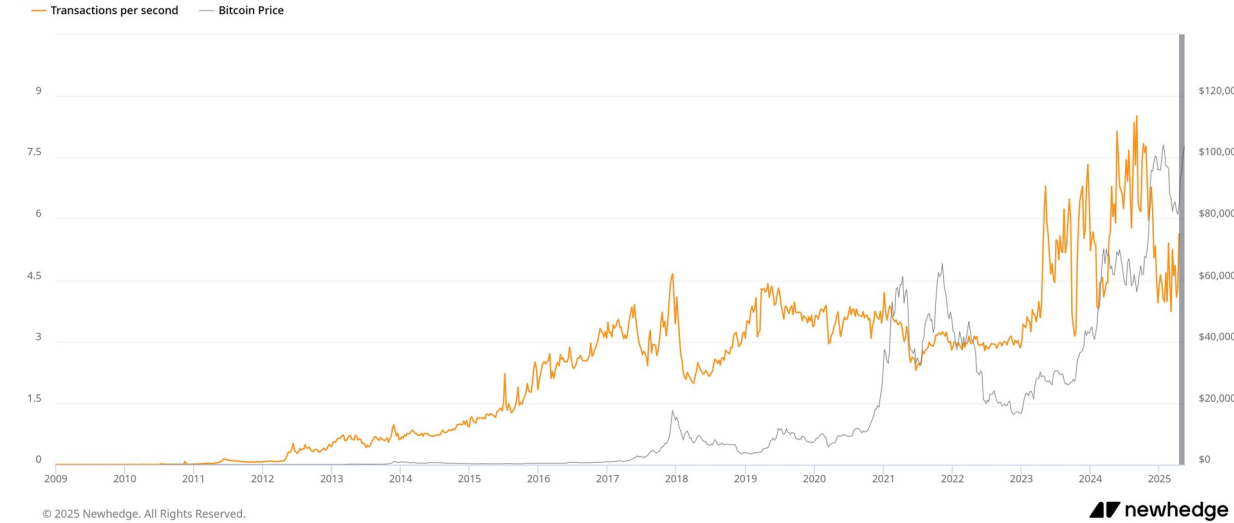
Bitcoin Transactions

- 920000 transactions per day (highest)
 - ~3-11 transactions per second
- Transaction fees / day USD: 80m USD
~ max. 20.04 – Bitcoin NFT
- Blocksize

Blockchain Size
658.4 GB

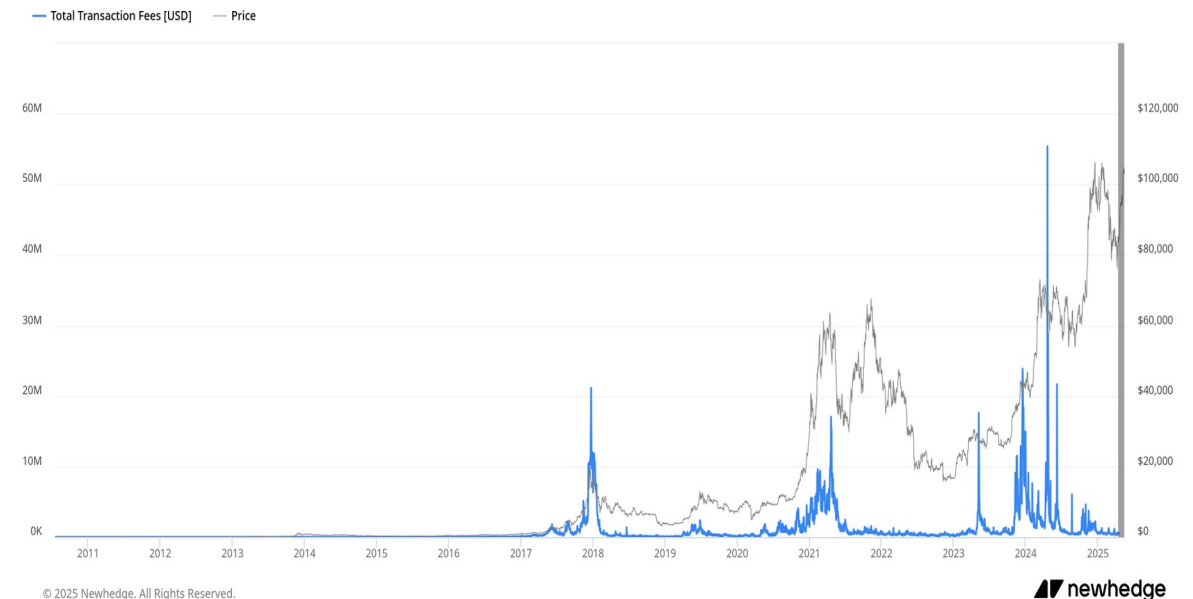


Bitcoin Transactions per Second



newhedge

Total Bitcoin Transaction Fees per Day (USD)

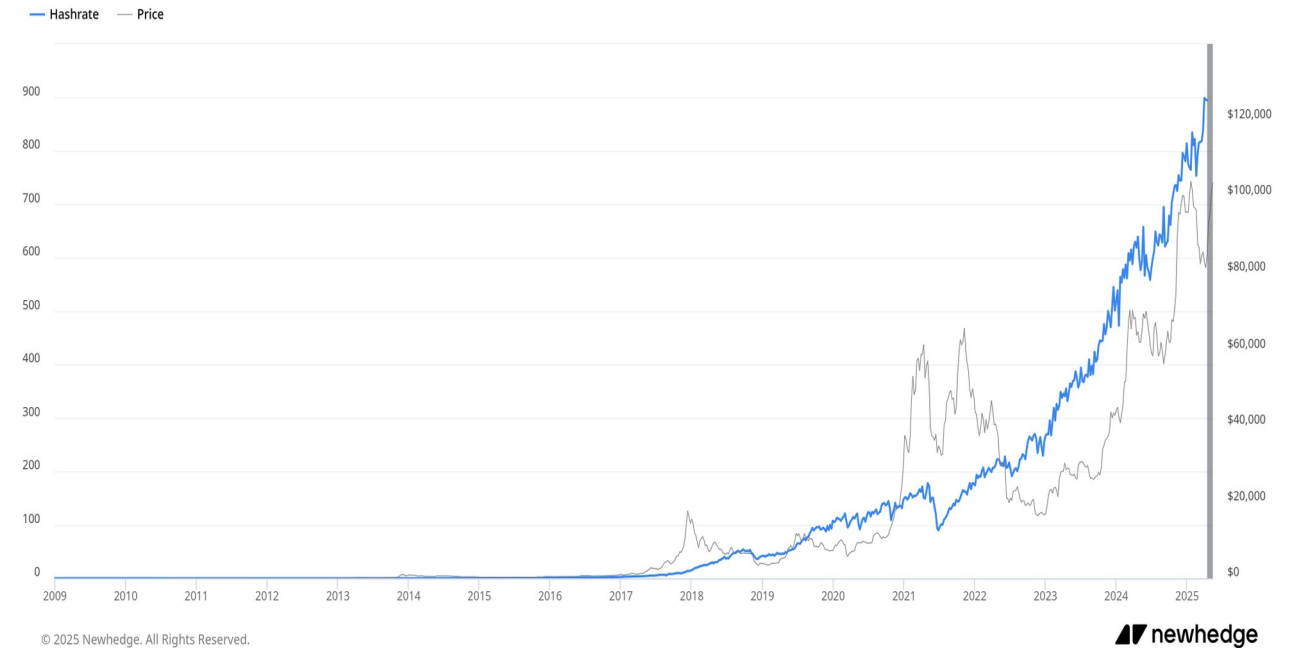


newhedge

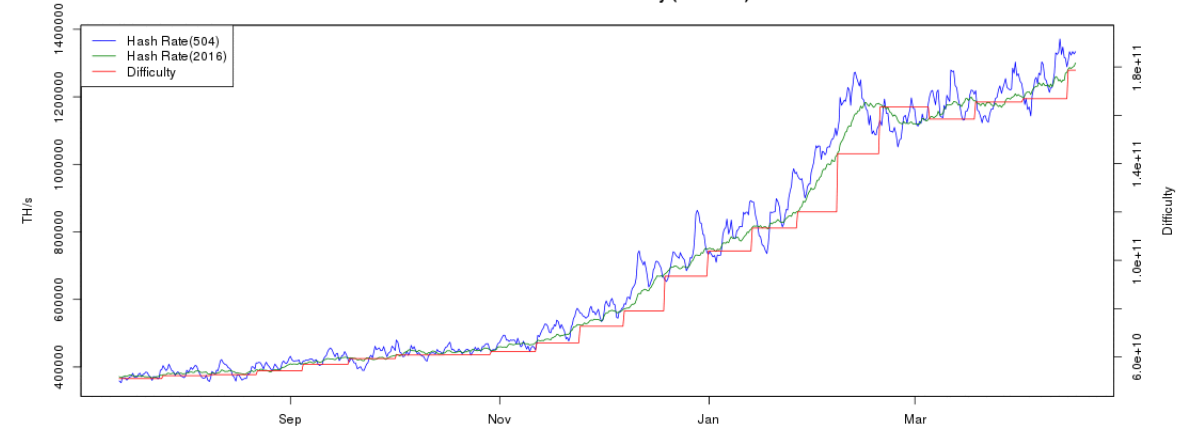
Bitcoin Numbers

- Network Hashrate (1 hash = 12.7 KFLOPs), 1000Eh/s
 - ~12.7 YottaFLOPS in 2025
 - ~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 ~17.7 ExaFLOPS

Bitcoin Hashrate vs Price



Bitcoin Hash Rate vs Difficulty (9 Months)



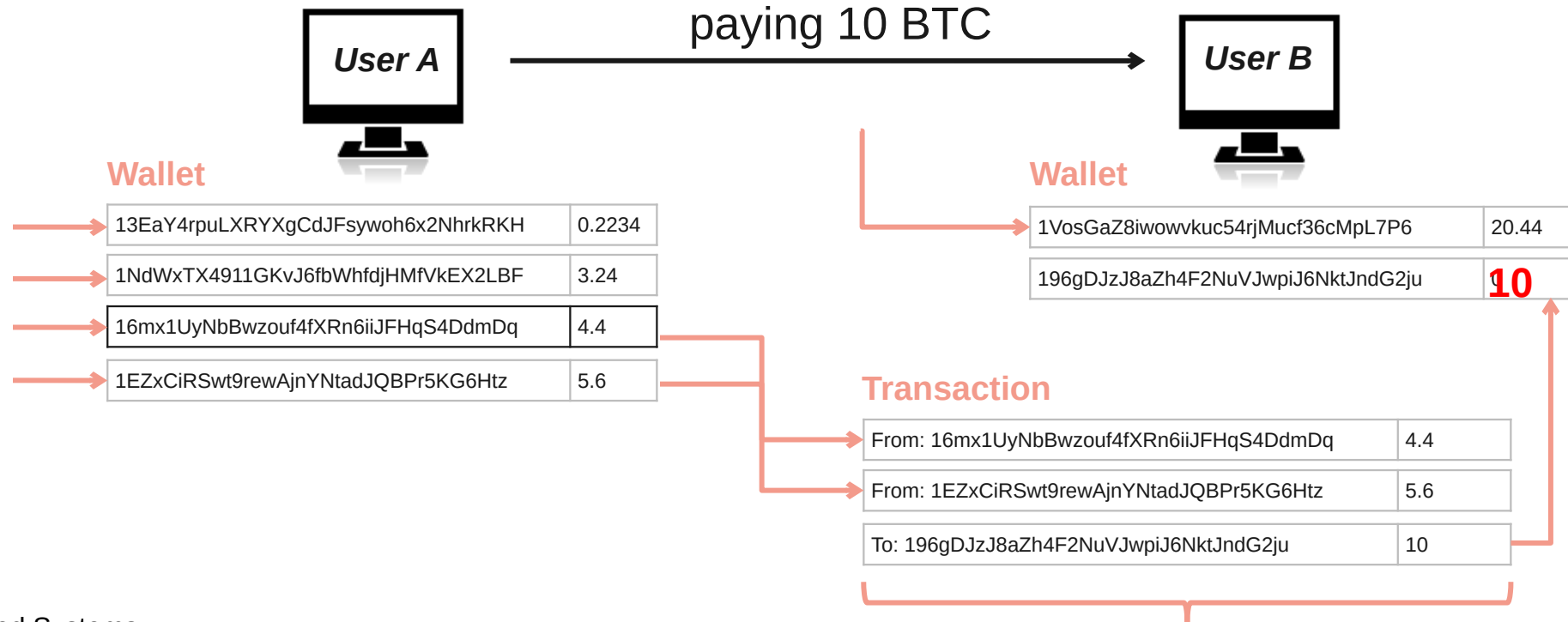
Mechanism

- 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



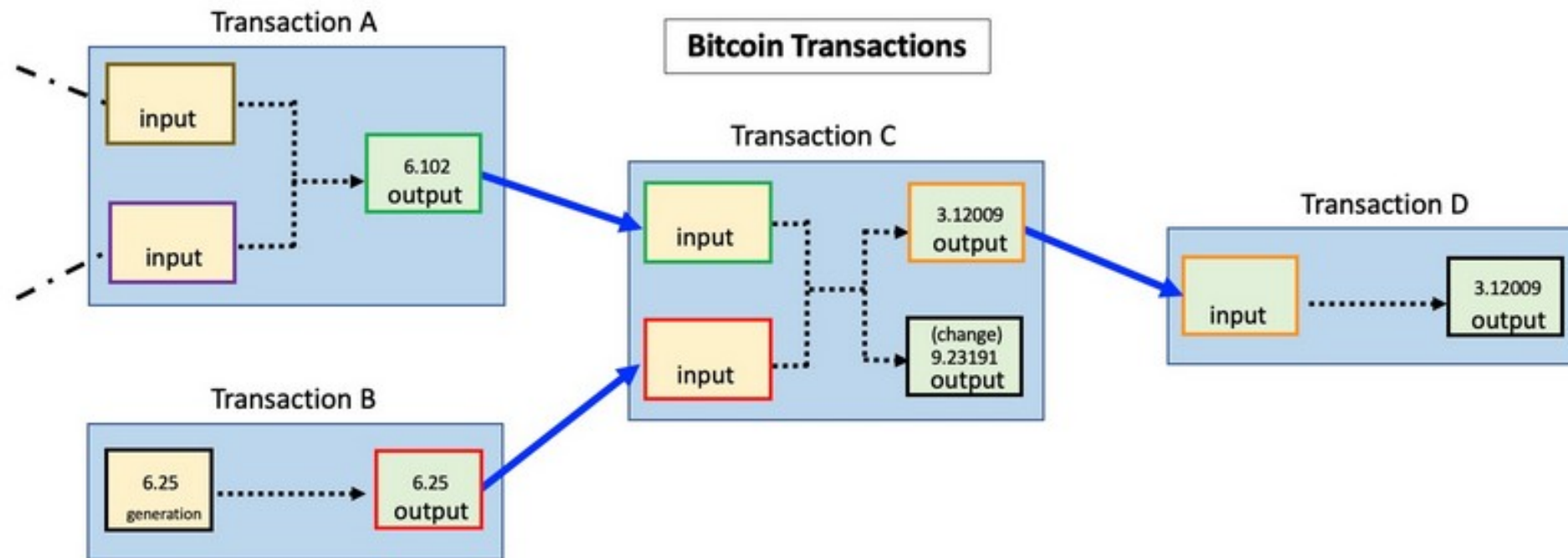
Key Bitcoin Operations

- 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



Sign with Private Key of User A

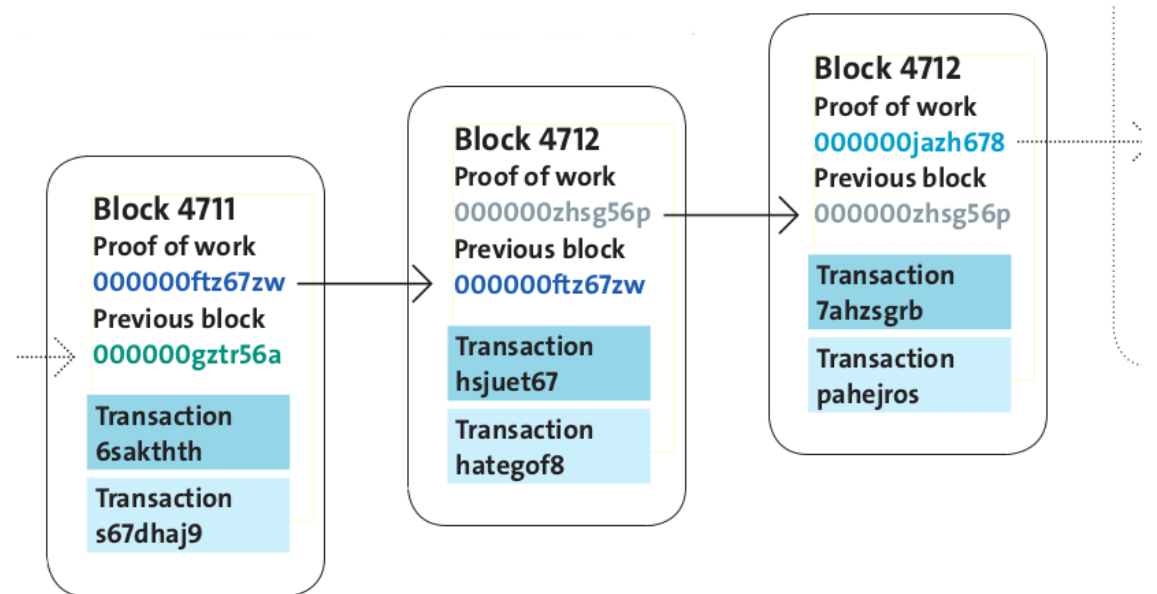
Transactions



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

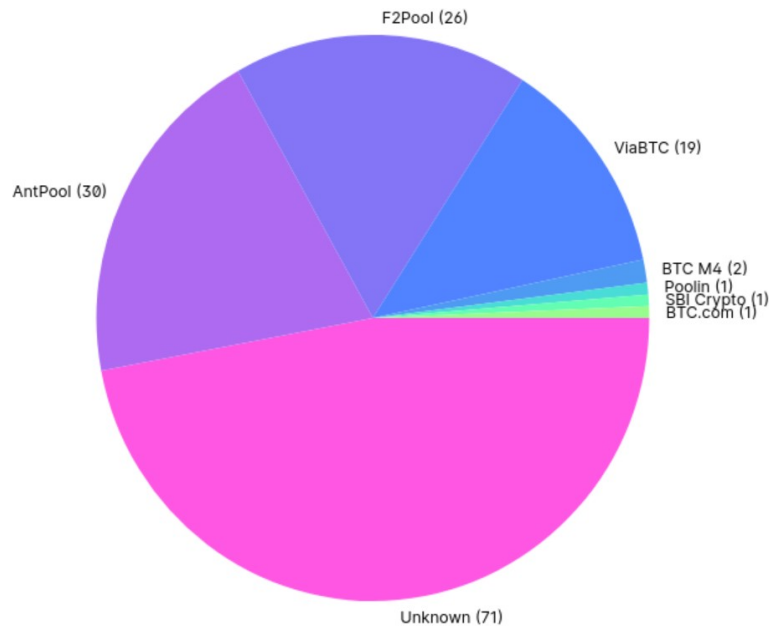
Blockchain

- 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)
 - Mining / creating blocks → Miner get currently 3.125 BTC per creation
 - adjustable difficulty 6 blocks / h
 - Sometime in 2028 reward will be 1.5625



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

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/>

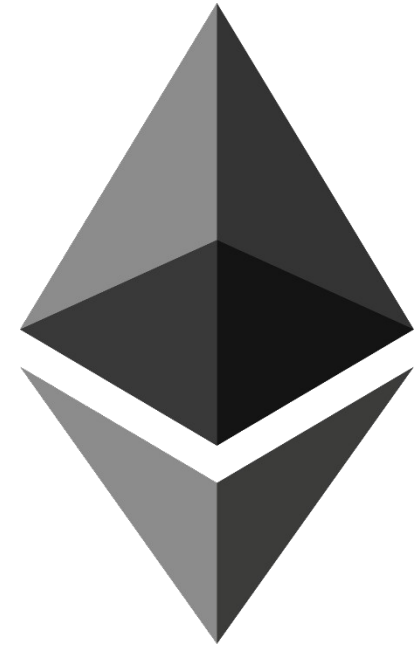
Mining: Evolution ASIC

- Scenario: old ASIC miner
 - Example: Avalon Batch #2
 - 70GHash/s
- Generates ~0.004CHF per day in 2025
- 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)



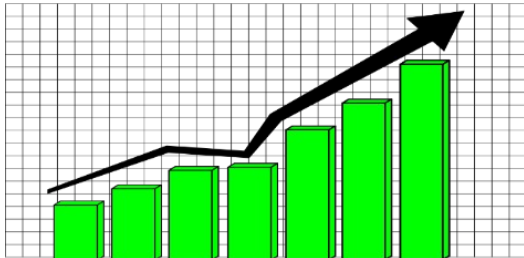
Many Coins – Similar Mechanism

- 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



Discussion (1)

- Disadvantages
 - Power consumption
 - ~ as much as 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

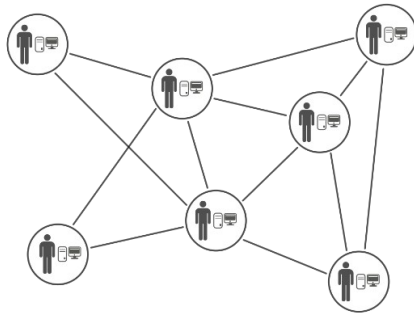
- Advantages
 - Low (fixed) tx fees
 - ~1.2 satoshi per byte / 0.25USD (~200bytes tx)
 - Scalable
 - Hardware/storage gets faster



- Anonymity
 - Preserving privacy

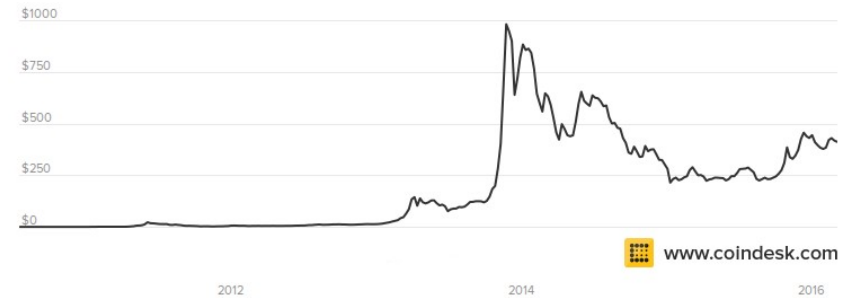
Discussion (2)

- 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 elements
 - Core developers

