



**OST**

Eastern Switzerland  
University of Applied Sciences

# **Distributed Systems (DSy)**

## **Blockchain, Bitcoin**

Thomas Bocek

01.05.2023

# Learning Goals

- Lecture 10 (Blockchain, Bitcoin)
  - Basic concepts (UTXO, mining, chain)
  - 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 (~480 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
blk00000.dat blk00002.dat blk00004.dat blk00006.dat blk00008.dat
blk00001.dat blk00003.dat blk00005.dat blk00007.dat blk00009.dat
draft@home:/scratch/bitcoin/blocks$ head -c 300 blk00000.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 | .....|
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 | .....|
00000070 00 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](#)

# Bitcoin's Market Capitalization in USD

- Bitcoin boom, started in 2013 – current price



# Bitcoin's Price USD 2022





**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

## 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



## 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 | Schweiz | Registrieren | Login

20 Minuten ONLINE

Video TV Infografik Games E-Prospekte

Schweiz Ausland Panorama Wirtschaft Sport Shock-Welt People Entertainment Digital Mehr

News SMI Alle Indices Ratgeber Geld ...

# From 2011

Ihre Story, Ihre Informationen, Ihr Hinweis? [feedback@20minuten.ch](mailto: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 **homegate.ch**

### Immobilien in Zürich

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



### Immobilien finden

PLZ:

Preis:  bis

### Trending topics

Read comments on the site's most popular topics

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



As of 2023

## Bitcoins in the News

- 24.04.2023, CNBC  
"Crypto winter is over — and bitcoin could hit \$100,000 by the end of 2024, Standard Chartered says" [[link](#)]
- 24.04.2023, CNBC  
"'Crypto is dead in America,' says longtime bitcoin bull Chamath Palihapitiya" [[link](#)]
- 25.04.2023, DailyFX  
"Bitcoin & Ethereum Price Action: How Much More Downside?" [[link](#)]
- 24.04.2023, Decrypt  
"Satoshi-Era Bitcoin Whale Moves \$11 Million After Sleeping for 12 Years" [[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

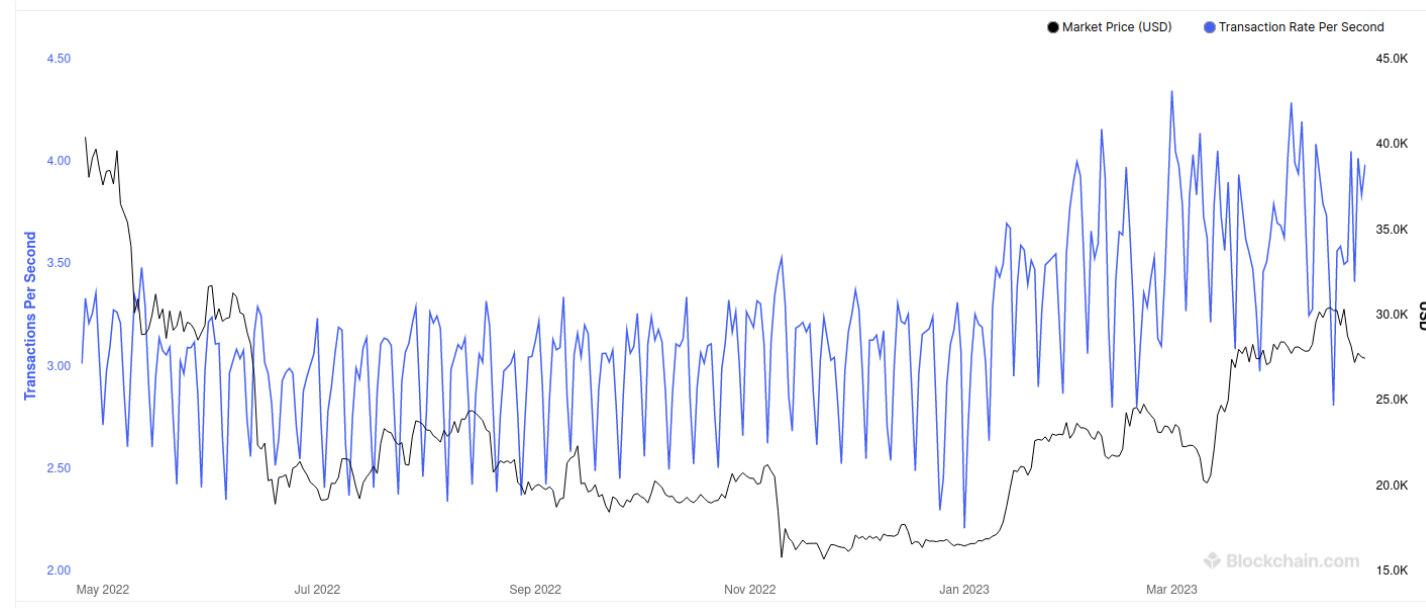
# Bitcoin in Numbers / Fake Volume

- Spread, e.g. ETH
- High spread, should be around 0.01USD
- 1 BTC  $\approx$  28'583 US\$ (01.05.2023)
- Total of 19 Million BTC mined
  - Market capitalization of 0.5 Trillion US\$
  - Volume fake? E.g., CoinBene, RightBTC

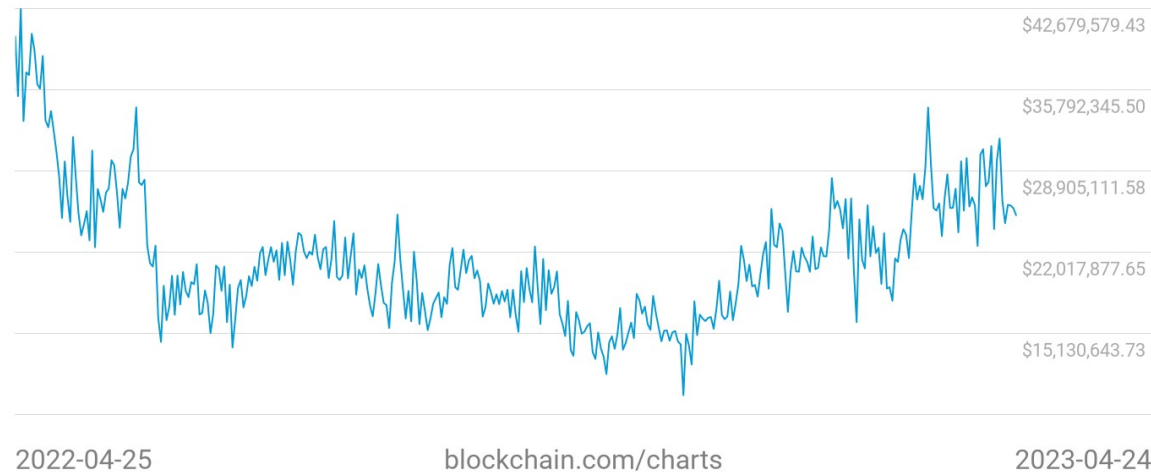
9	 Bitfinex	ETH/USD	\$2,405.70	\$22,429,625	\$8,879,712	\$149,025,250	0.47%	High	645	Recently
10	 Bitstamp	ETH/USD	\$2,409.14	\$2,117,937	\$2,415,352	\$120,185,425	0.38%	High	396	Recently
11	 Binance	ETH/EUR	\$2,423.08	\$731,224	\$1,017,017	\$114,211,638	0.36%	High	727	Recently

# Bitcoin Transactions

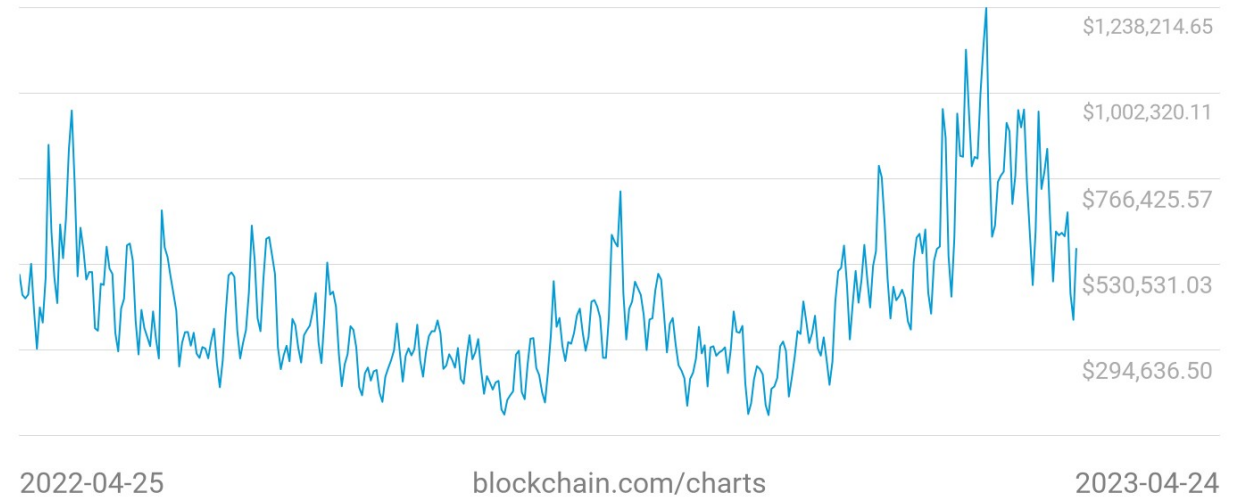
- 450,000 transactions per day (highest)
- ~2-5 transactions per second
- Transaction fees per day ~ 5-45 BTC



Miners Revenue  
**\$25,151,563.92**



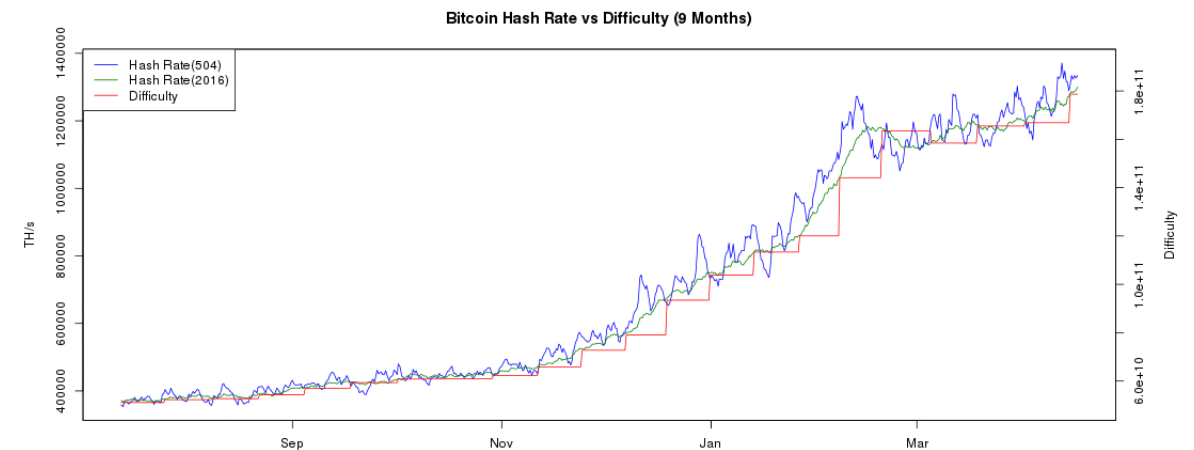
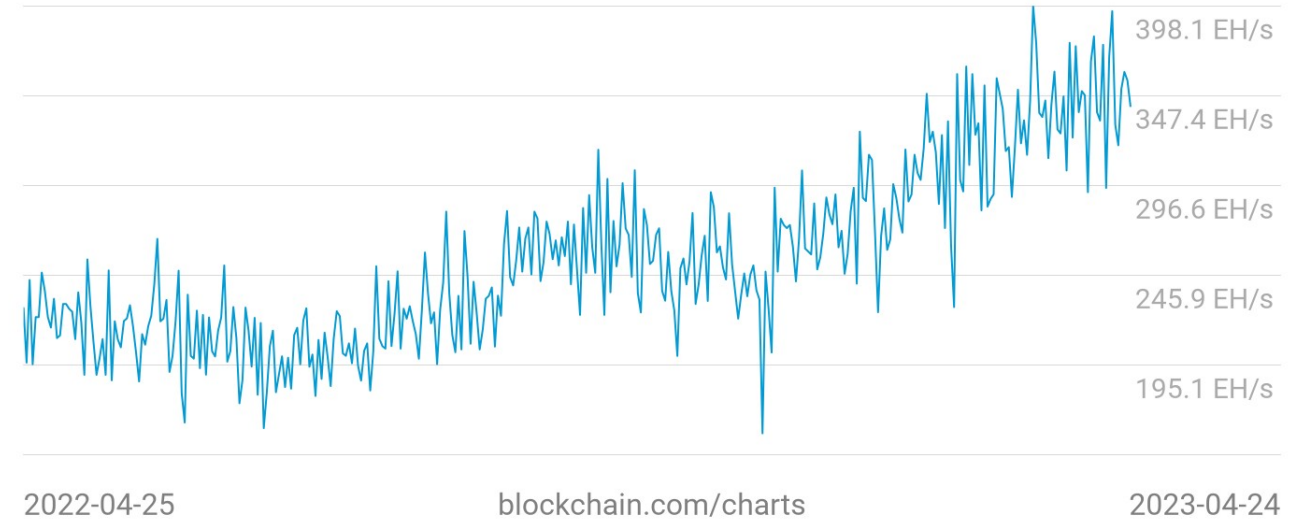
Total Transaction Fees in USD  
**\$573,245.17**



# Bitcoin Numbers

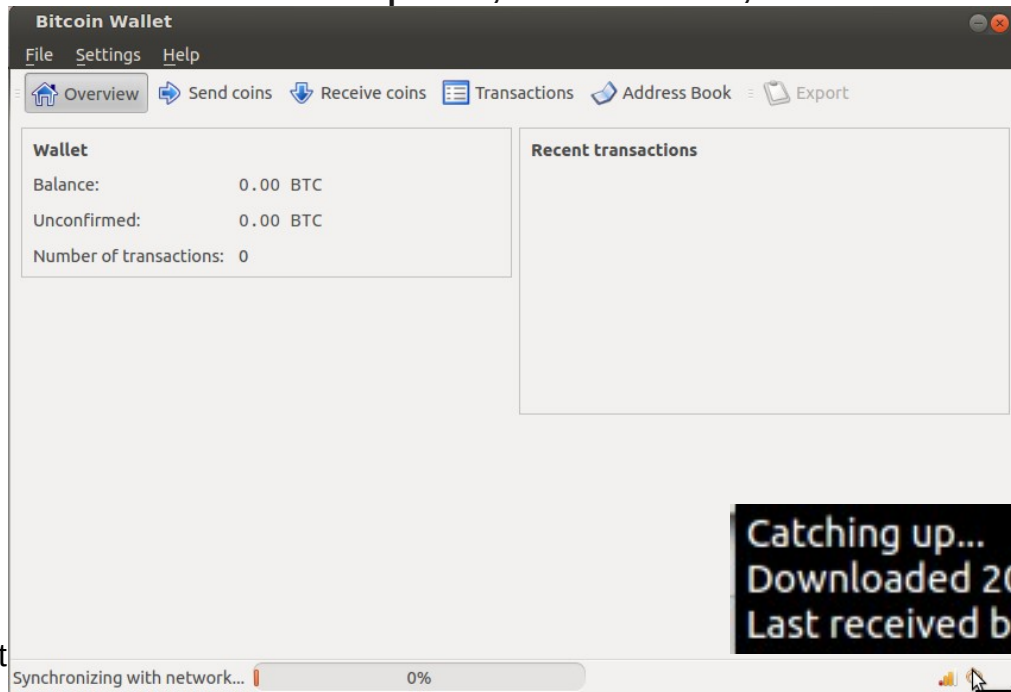
- Network Hashrate
  - ~4.3 YottaFLOPS in 2023
  - ~3 YottaFLOPS in 2022
  - ~2.1 YottaFLOPS in 2021
  - ~1.4 YottaFLOPS in 2020
  - ~635 ZettaFLOPS in 2019
  - ~4 ZettaFLOPS in 2015
  - ~714 ExaFLOPS in 2014
  - ~900 PetaFLOPS in 2013
  - ~155 PetaFLOPS in 2012
- Adjust time: ~14 days
- Fastest supercomputer ([top500.org](https://www.top500.org/)) Frontier  
1600 PetaFLOPS (max), all  
500 ~7.5 ExaFLOPS

Hash Rate  
341.4 EH/s

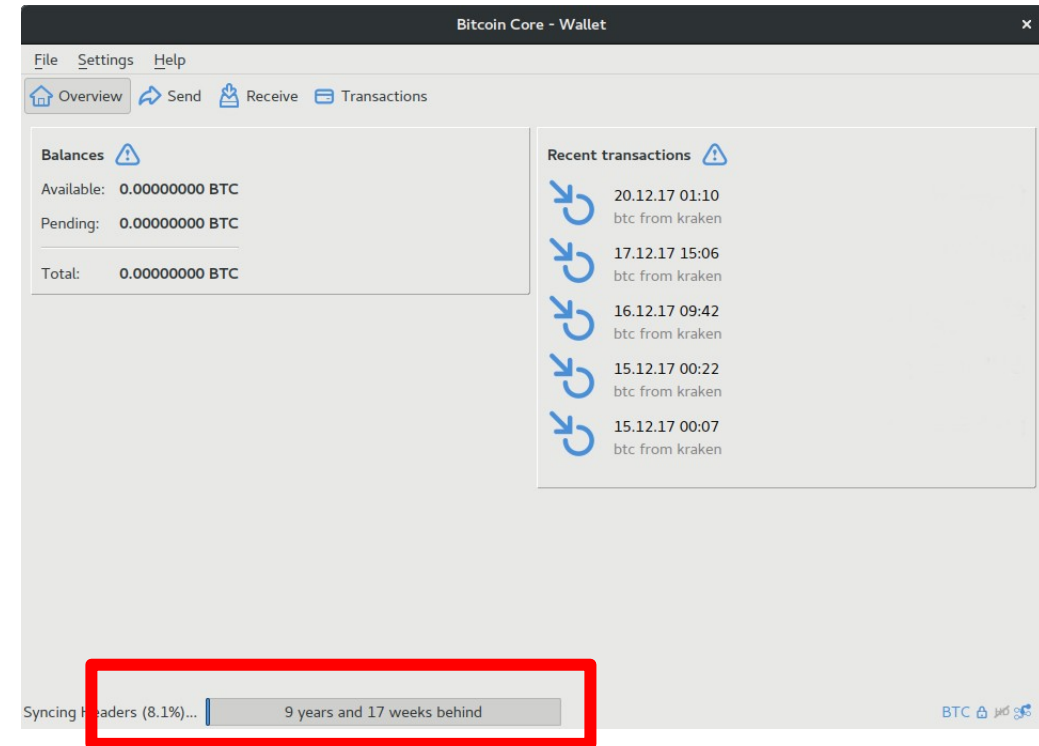


# Bitcoin Example

- 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



Catching up...  
Downloaded 2000 of 178717 blocks of transaction history.  
Last received block was generated 1194 days ago.



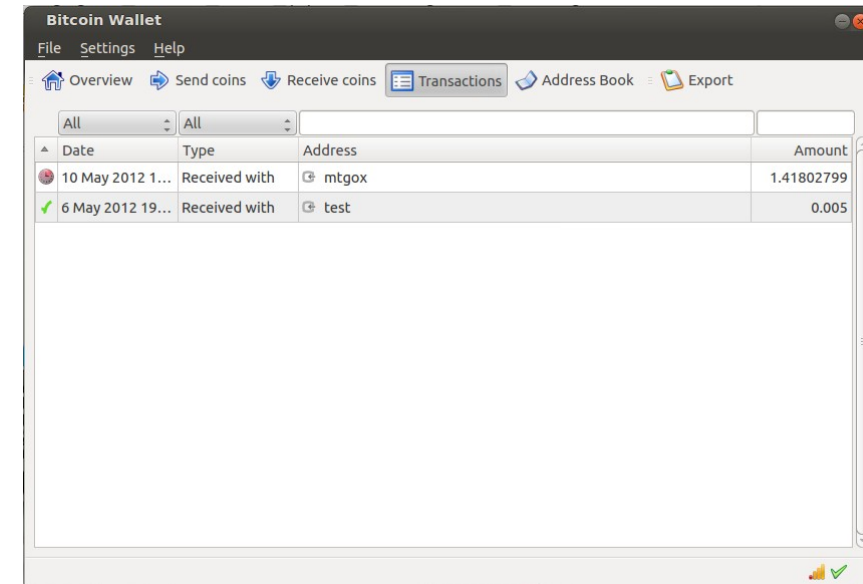
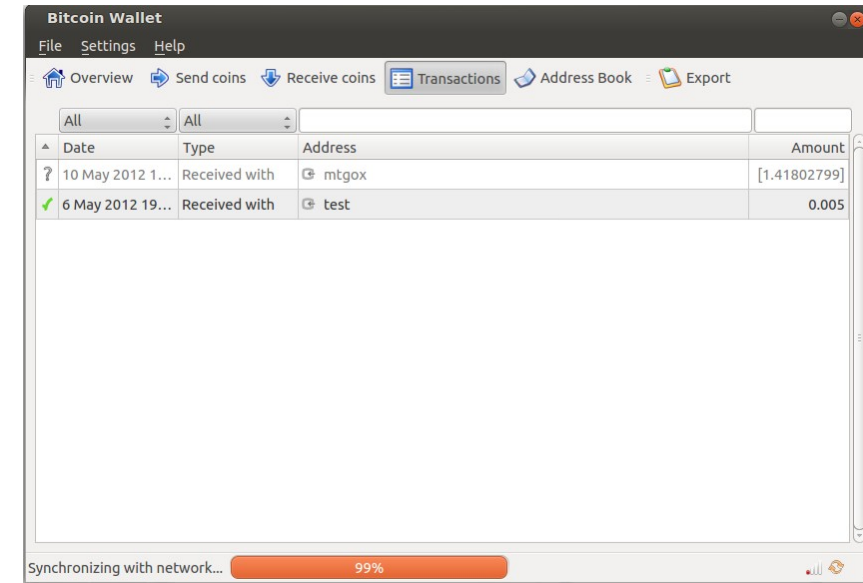


# Bitcoin Example

- 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

# 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>
- 2023: it's getting better
  - SBB
  - Exchanges: KYC, delays
- Good idea: don't leave coins in an online wallet



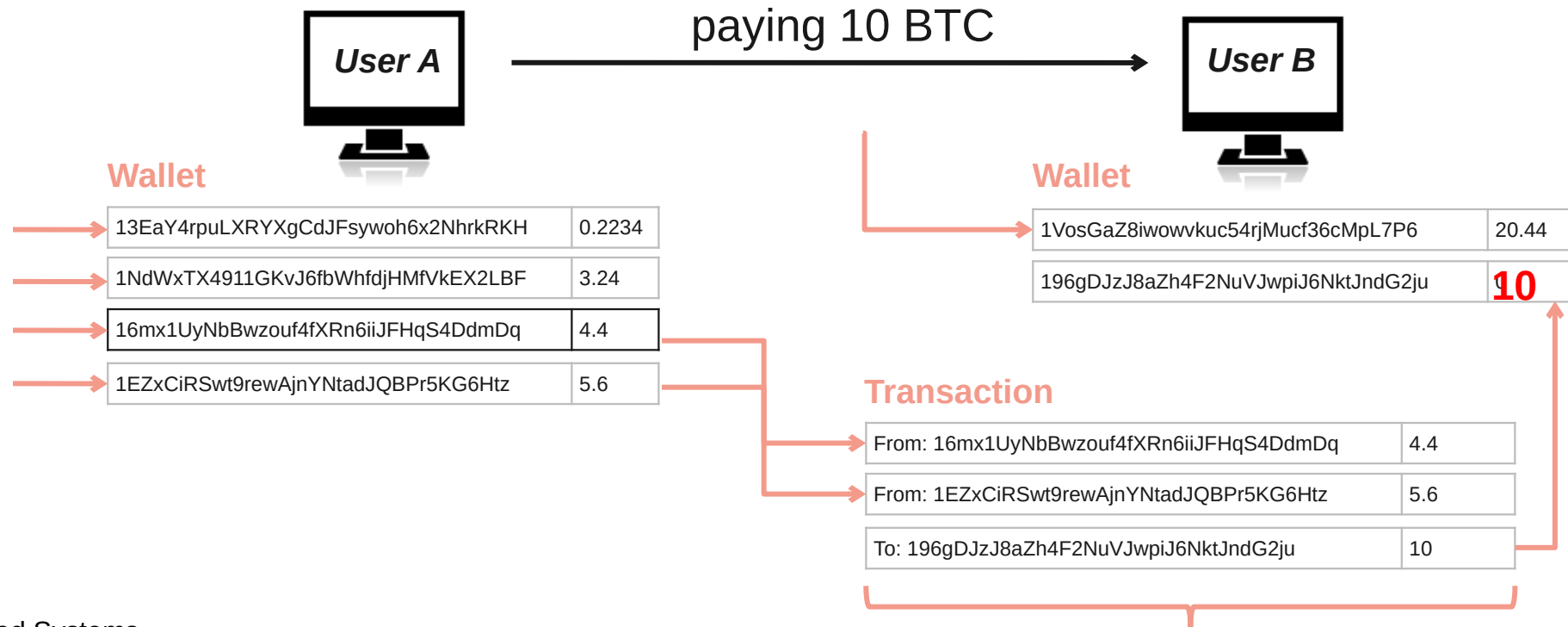
# Mechanism

- 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

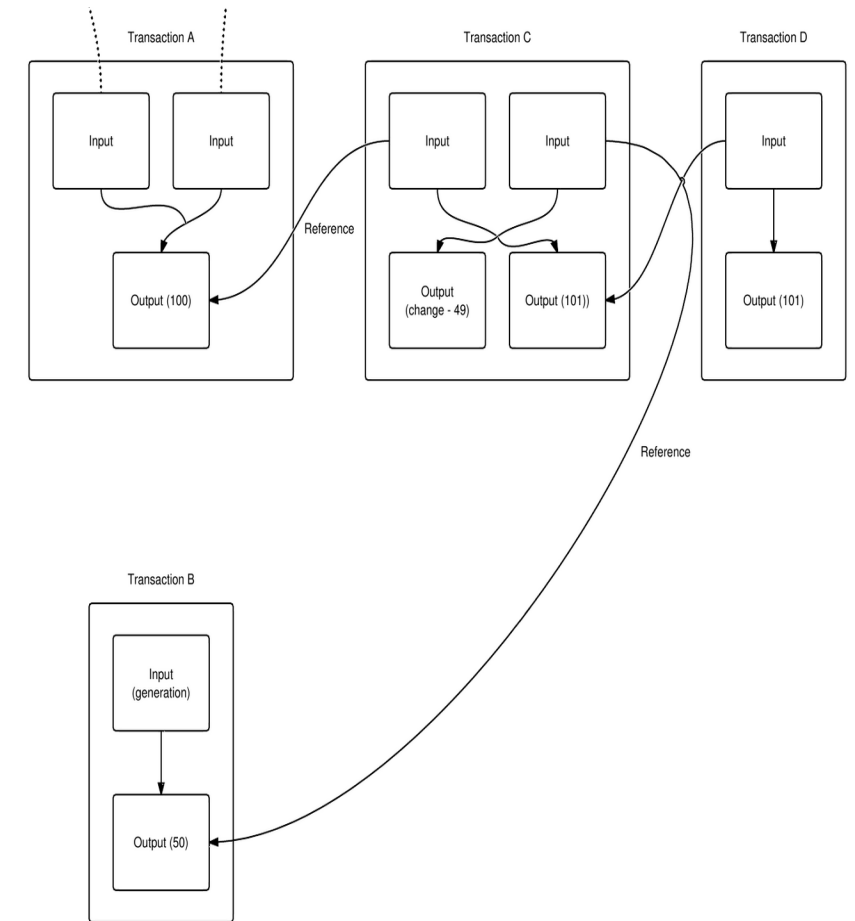


Sign with Private Key of User A

# Mechanism

- Avoiding double spending
  - Transactions in blocks are confirmed.
  - guessing value that results in zero bits (00000000000001805ff174586b6acf100f733aaf634e92f9580b4fac9272ed97)
  - 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





# Bitcoin - Protocol

- TX in details

version	01 00 00 00	
input count	01	
input	previous output hash (reversed)	48 4d 40 d4 5b 9e a0 d6 52 fc a8 25 8a b7 ca a4 25 41 eb 52 97 58 57 f9 6f b5 0c d7 32 c8 b4 81
	previous output index	00 00 00 00
	script length	8a
	scriptSig	47 30 44 02 20 2c b2 65 bf 10 70 7b f4 93 46 c3 51 5d d3 d1 6f c4 54 61 8c 58 ec 0a 0f f4 48 a6 76 c5 4f f7 13 02 20 6c 66 24 d7 62 a1 fc ef 46 18 28 4e ad 8f 08 67 8a c0 5b 13 c8 42 35 f1 65 4e 6a d1 68 23 3e 82 01 41 04 14 e3 01 b2 32 8f 17 44 2c 0b 83 10 d7 87 bf 3d 8a 40 4c fb d0 70 4f 13 5b 6a d4 b2 d3 ee 75 13 10 f9 81 92 6e 53 a6 e8 c3 9b d7 d3 fe fd 57 6c 54 3c ce 49 3c ba c0 63 88 f2 65 1d 1a ac bf cd
	sequence	ff ff ff ff
output count	01	
output	value	62 64 01 00 00 00 00 00
	script length	19
	scriptPubKey	76 a9 14 c8 e9 09 96 c7 c6 08 0e e0 62 84 60 0c 68 4e d9 04 d1 4c 5c 88 ac
block lock time	00 00 00 00	

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

# Bitcoin Scripting Language

- ScriptSig

PUSHDATA

signature data and SIGHASH\_ALL

PUSHDATA

public key data

- ScriptPubKey

OP\_DUP

OP\_HASH160

PUSHDATA

Bitcoin address (public key hash)

OP\_EQUALVERIFY

OP\_CHECKSIG

- Non-turing complete (e.g. No loops)

- With scripts

- Multisig, n-of-m, escrow and dispute mediation
- Micropayment channel, refund tx in future

- Opcodes – [all codes](#)

- Data operations

- OP\_PUSHDATA1, OP\_PUSHDATA4,...

- Flow control

- OP\_IF, OP\_ELSE, ...

- Stack

- OP\_DUP, OP\_SWAP, ...

- Arithmetic

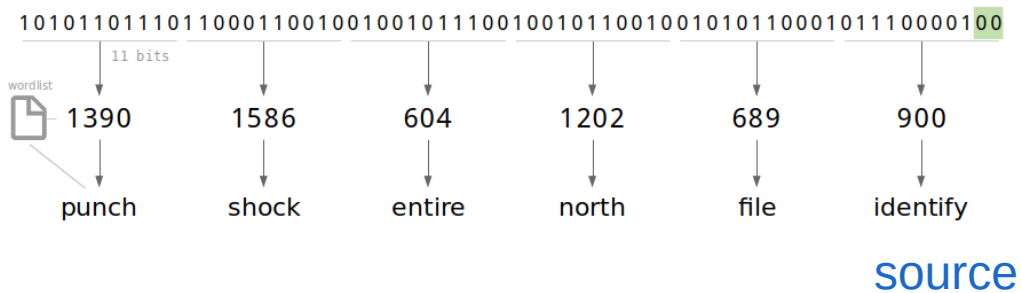
- OP\_ADD, OP\_ABS, ...

- Crypto

- OP\_SHA256, OP\_CHECKSIGVERIFY

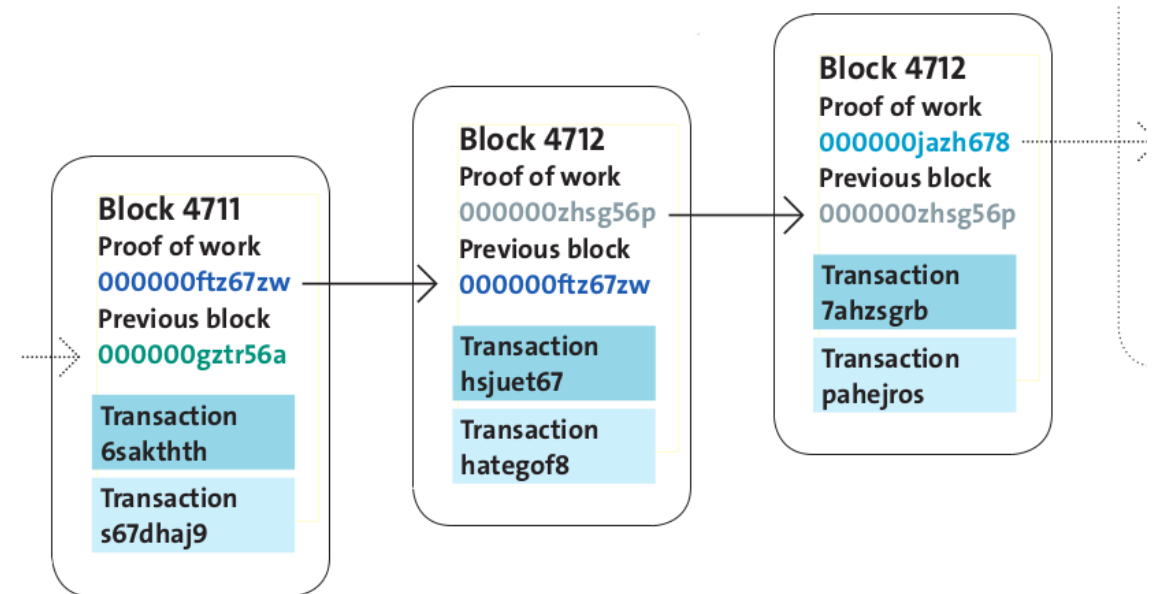
# BIP39

- **BIP39**: Bitcoin Improvement Proposal 39
- Purpose: Enhance security & simplify backup for cryptocurrency wallets
- Key component: Mnemonic phrase (human-readable seed)
  - Hierarchical deterministic (HD) wallets
  - Use mnemonic phrase to generate & recover wallets
- Step 1: Generate random entropy (128-256 bits)
- Step 2: Calculate SHA256 checksum (4, 8 bits)
- Step 3: Concatenate entropy & checksum
  - E.g., 128bit random + 4 bit (msb of SHA256)
- Step 4: Divide into groups of 11 bits
  - E.g.,  $132/11 = 12$  words
- Step 5: Match each group with a predefined word from the BIP39 [wordlist](#) (2048 words)



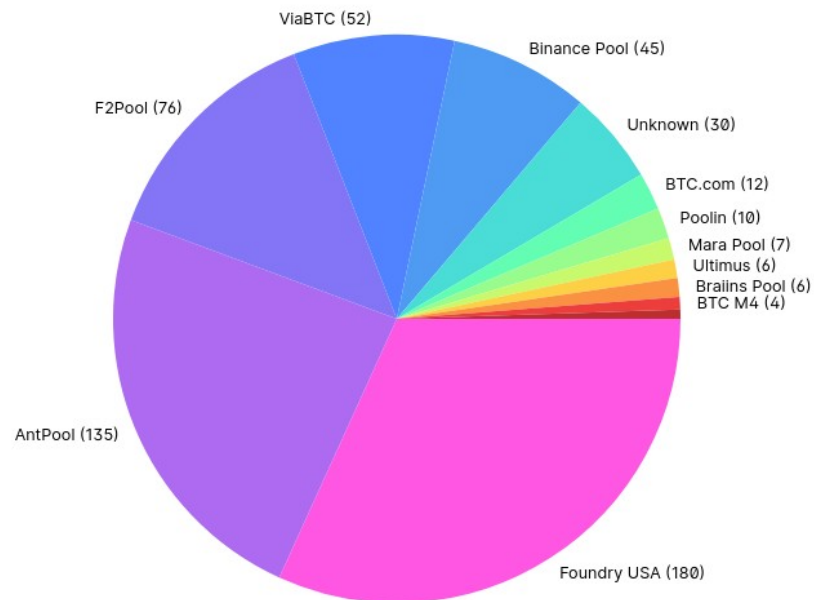
# Blockchain

- 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!



# 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=-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/>



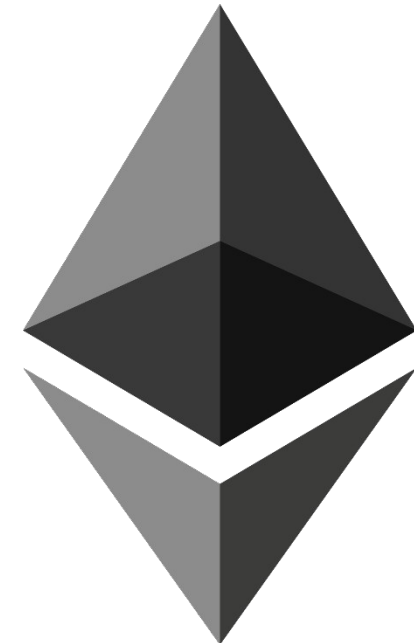
# Mining: Evolution ASIC

- 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)



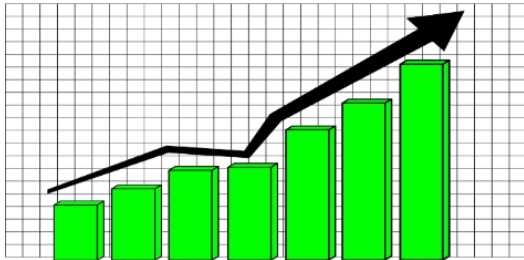
# Many Coins – Similar Mechanism

- 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](#)



# Discussion (1)

- 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

- Advantages
  - Low (fixed) tx fees
    - ~[102](#) satoshi per byte / 6USD
  - Scalable
    - Hardware/storage gets faster

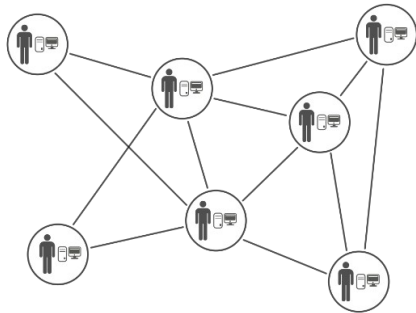


- Anonymity
  - No privacy concerns/ datamining difficult



# Discussion (2)

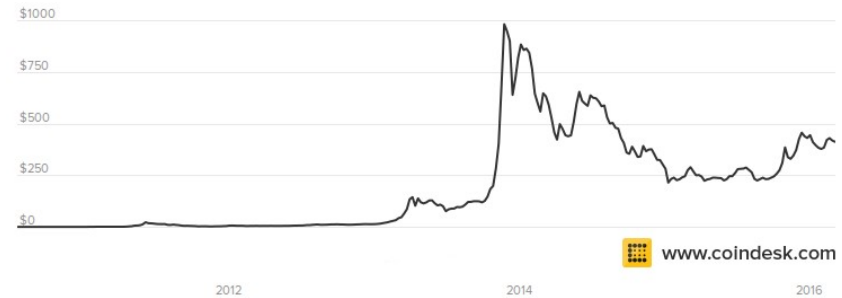
- Advantages
  - No major “crashes”
    - [Mt.Gox](#) was exchange site!
  - Decentralized
    - Open protocol
    - Forks



- Many other blockchain use cases
  - Smart contracts



- Disadvantages
  - Volatile exchange rate



- Central elements
  - Core developers

