

FS20

BLOCKCHAIN, BITCOIN, ETHEREUM

Introduction

T. Bocek

thomas.bocek@hsr.ch

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 (~270 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 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 | rnk 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..?L8..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 Market Capitalization in USD

■ COVID impact



Highcharts.com

Bitcoin

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

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

759 348 123
Tweet +1 Share



The Economist

Log in Register Subscribe

Digital & mobile Events Topics

Tuesday May

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

Babbage

Science and technology



Comment (45)

E-mail

Reprints & permissions

Previous Next Latest Babbage

Latest from all our blogs

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by TONY LONDON G.T. WELSH

Like 1.8k Tweet 625

About Babbage

In this blog, our
between scienc
takes its name fr
mathematician a
computer.

Follow @Eco

RSS feed

Trending topics

Read comments o

Period: 1 day

www.bitcoin.org

France

US

Britain

Japan

Employment

Chris

de fr it

Ihr Ort: Zürich 19° Mi 20° Do 26°

Registrieren Login



Video TV Infografik Games E-Prospekte Apps
Schweiz Ausland Panorama Welt Sport E-Sport People Entertainment Digital Mehr
News SMI Alle Images Ratgeber Geld E-Trading Anlageprodukte PROMOTION 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 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.

- 15.04.2020, NZZ
«[Bitcoin: Steigt bald ein Phönix aus der Asche?](#)»
- 20.03.2020, Cash
«[Bitcoin-Kurs zieht im Einklang mit Aktienmärkten deutlich an](#)»
- 26.03.2020, ARD
«[Dank Corona: Bitcoin vor neuem Hype?](#)»
- 04.04.2020, cryptomonday.de
«[Bitcoin Halving 2020: Knappheit in Zeiten von unbegrenzter Liquidität](#)»
 - Halving: ~ [12.05.2020](#), now 12.5BTC, after halving 6.25BTC
- 21.03.2020, Handelsblatt
«[Abschied vom „digitalen Gold“: Die Coronakrise stellt die Bitcoin-Welt auf den Kopf](#)»

As of 2020

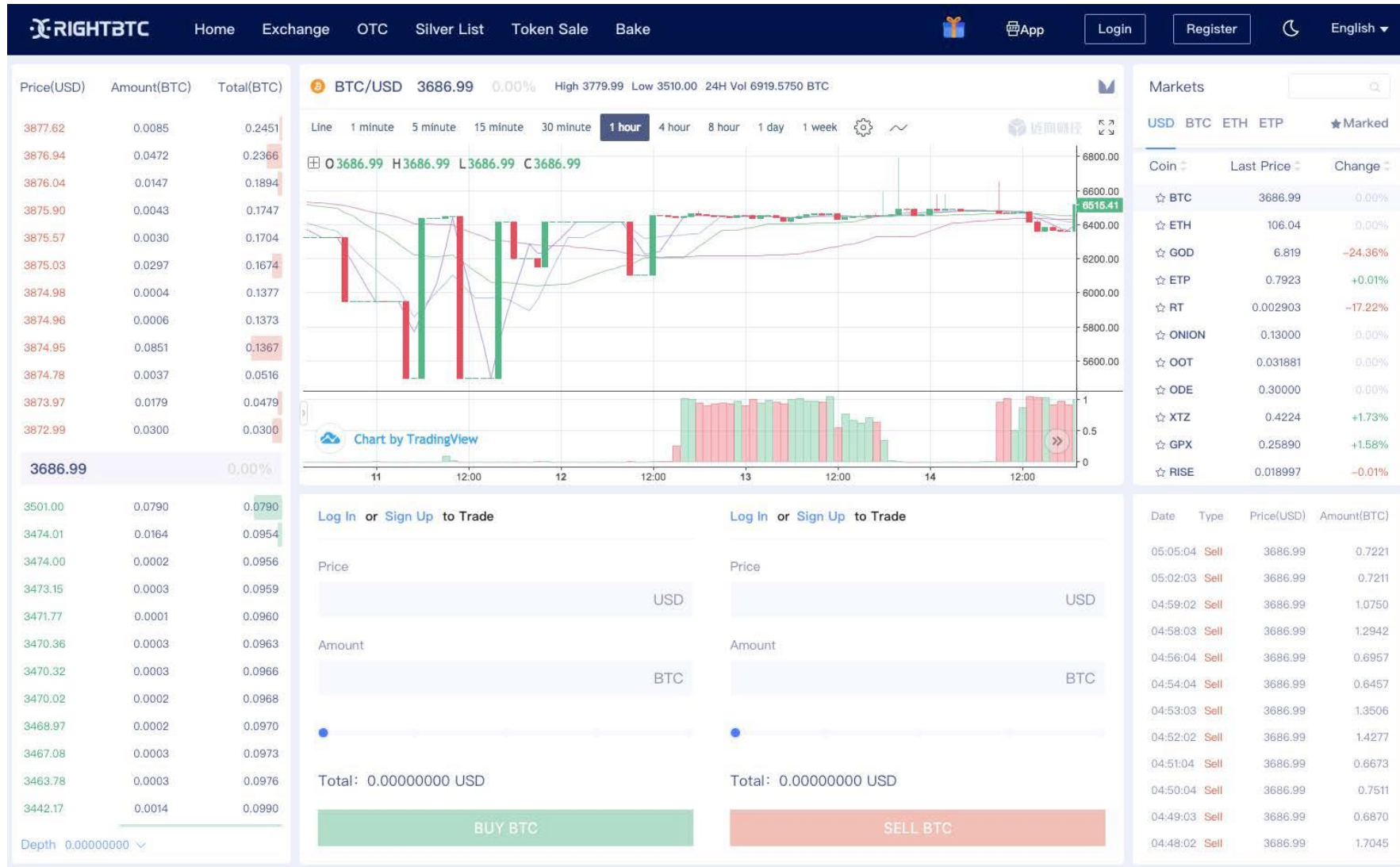
- **Not relying on trust, but on strong cryptography**
- **Weak anonymity (pseudonymity)**
 - All peers know all transactions
 - [Clustering](#): e.g. if a transaction has multiple input addresses, assume those addresses belong to the same wallet. ([example](#))
- **Not controlled by a single entity**
 - 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](#) not ([trading BTC in a P2P fashion](#)),**

Bitcoin in Numbers / Fake Volume

- 1 BTC $\approx$ 7050 US\$ (20.04.2020)
- Total of 18.3 Million BTC mined
 - Market capitalization of [130 Billion US\\$](#)
 - [Volume fake?](#)
- Spread, e.g. ETH
- High spread, should be around 0.01USD
- [Coinmarketcap](#): only few excluded

16	 CoinEgg	LTC/ETH	\$189,499,412	\$185.48	1.59%	Spot	Percentage	Recently
17	 Bit-Z	ETH/BTC	\$188,722,528	\$187.35	1.59%	Spot	Percentage	Recently
18	 Bit-Z	ETH/USDT	\$179,029,483	\$187.66	1.51%	Spot	Percentage	Recently
19	 TOPBTC	ETH/CNY	\$178,495,626	\$189.91	1.50%	Spot	Percentage	Recently



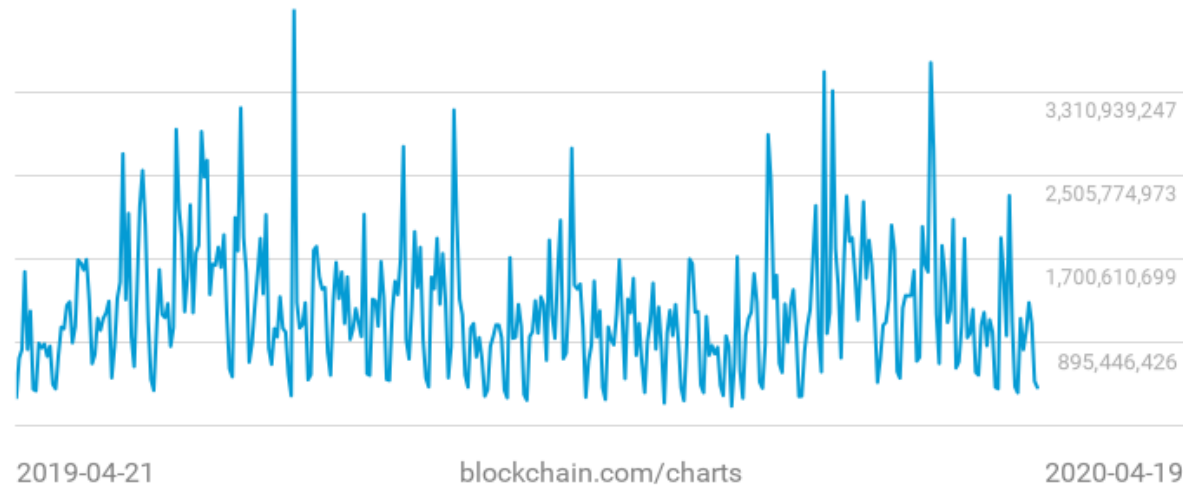




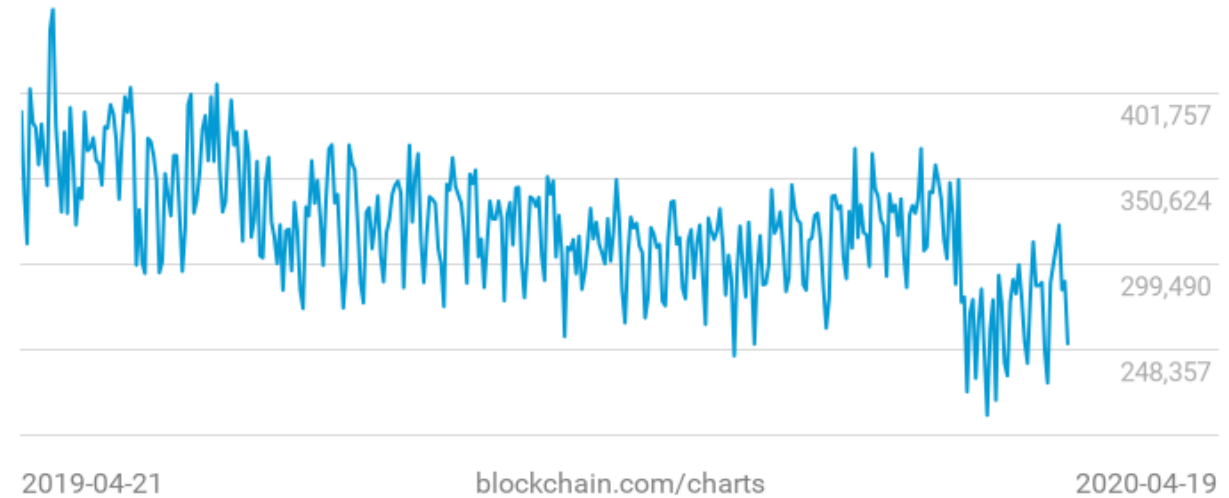
Bitcoin Transactions

- **450,000 transactions per day (highest)**
 - ~5 transactions per second
- **150,000 BTC traded per day**
- **Transaction fees per day ~ 27 BTC**

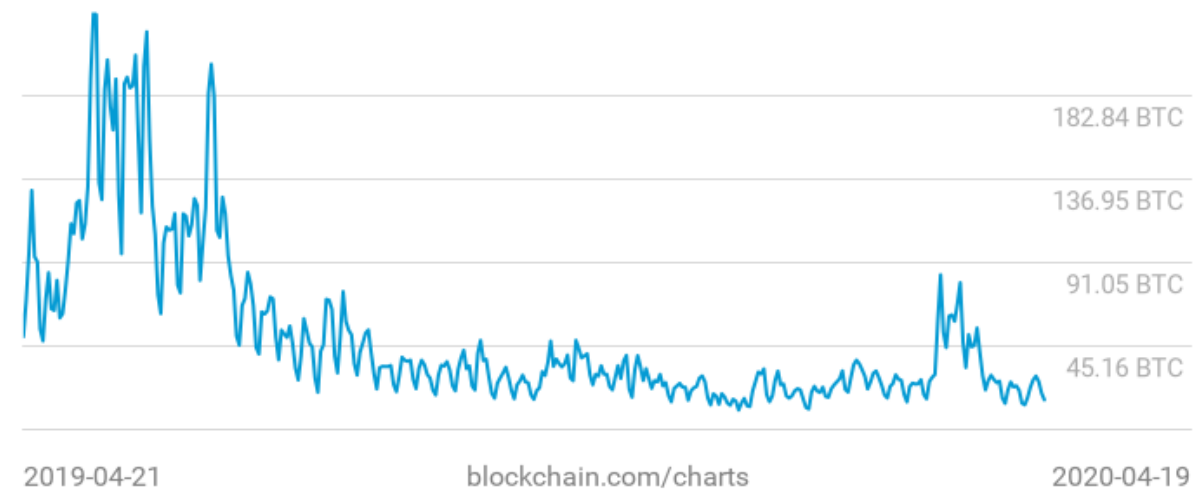
Estimated USD Transaction Value
458,165,164



Confirmed Transactions Per Day
251,984



Total Transaction Fees
15.57 BTC



Bitcoin Numbers

■ Network Hashrate

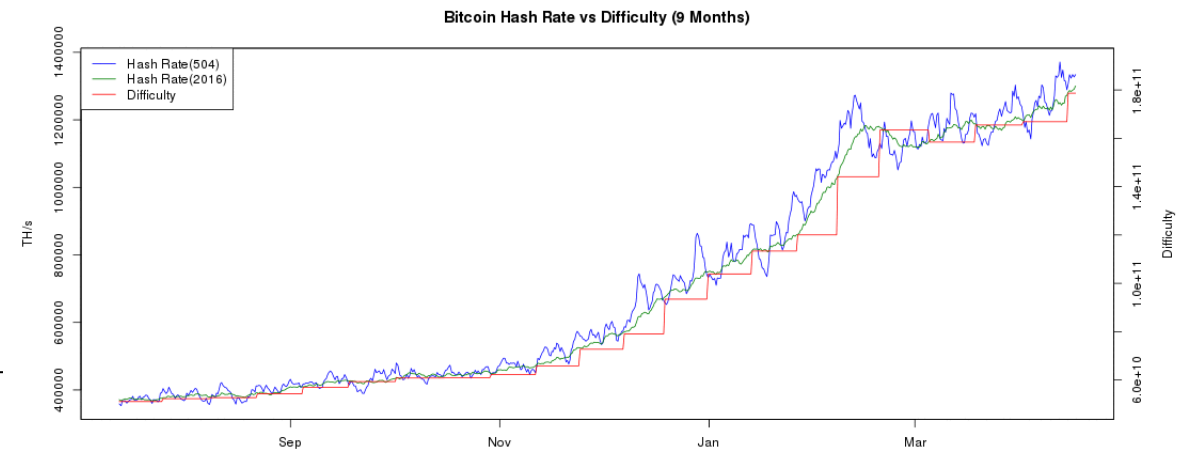
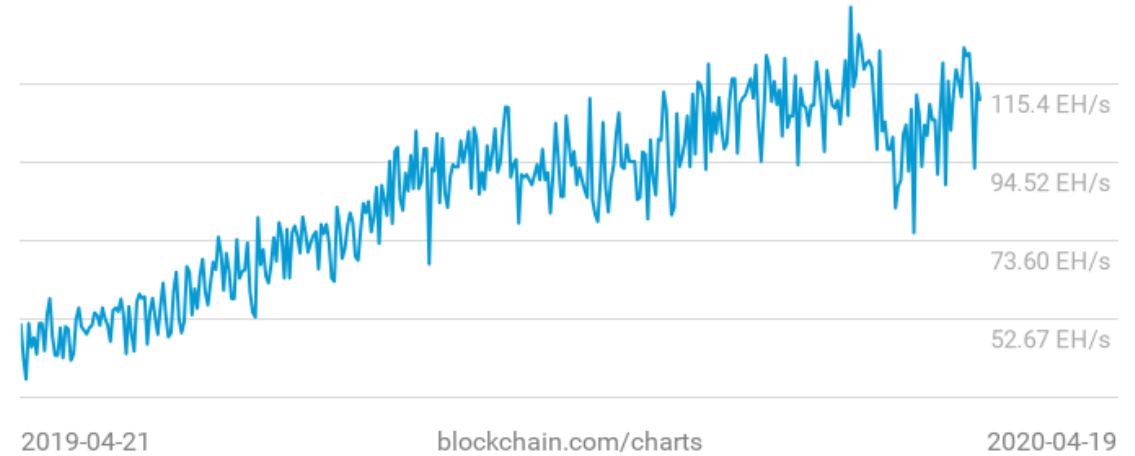
- ~1.4 YottaFLOPS in 2020
- ~635 [Zetta](#)FLOPS in 2019
- ~4 ZettaFLOPS in 2015
- ~714 ExaFLOPS in 2014
- ~900 PetaFLOPS in 2013
- ~155 PetaFLOPS in 2012

■ Adjust time: ~14 days

■ Fastest supercomputer ([top500.org](#)) Summit 148 PetaFLOPS (max), all 500 ~1.6 ExaFLOPS

■ Frontier with [1.5 ExaFLOPS](#) ■ exascale-level processing

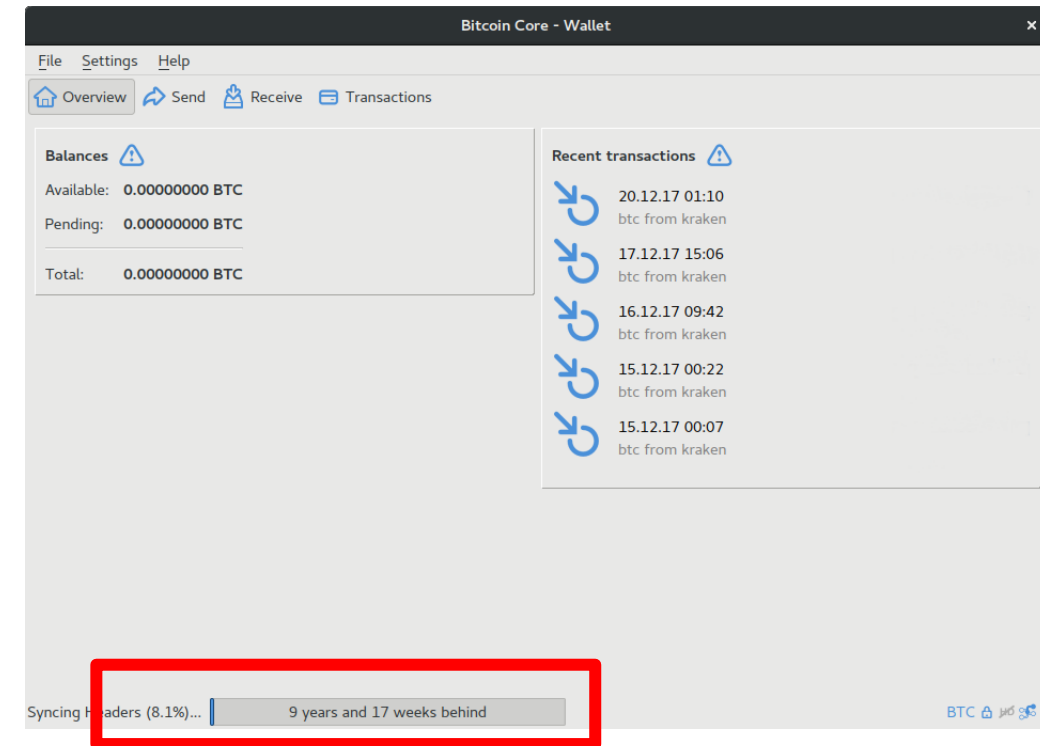
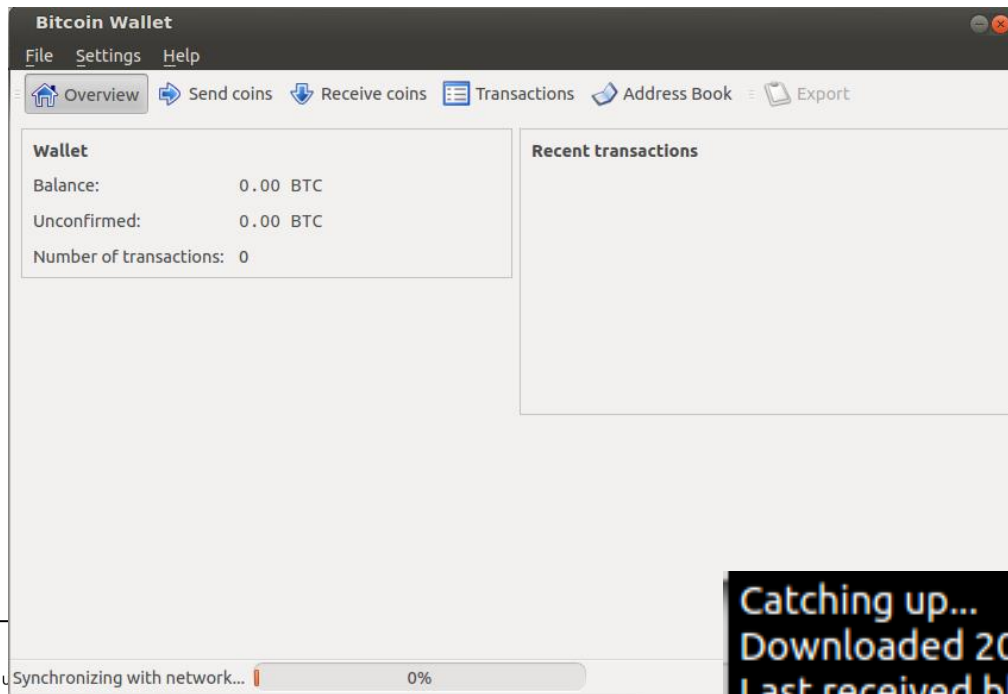
Hash Rate
111.2 EH/s



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**

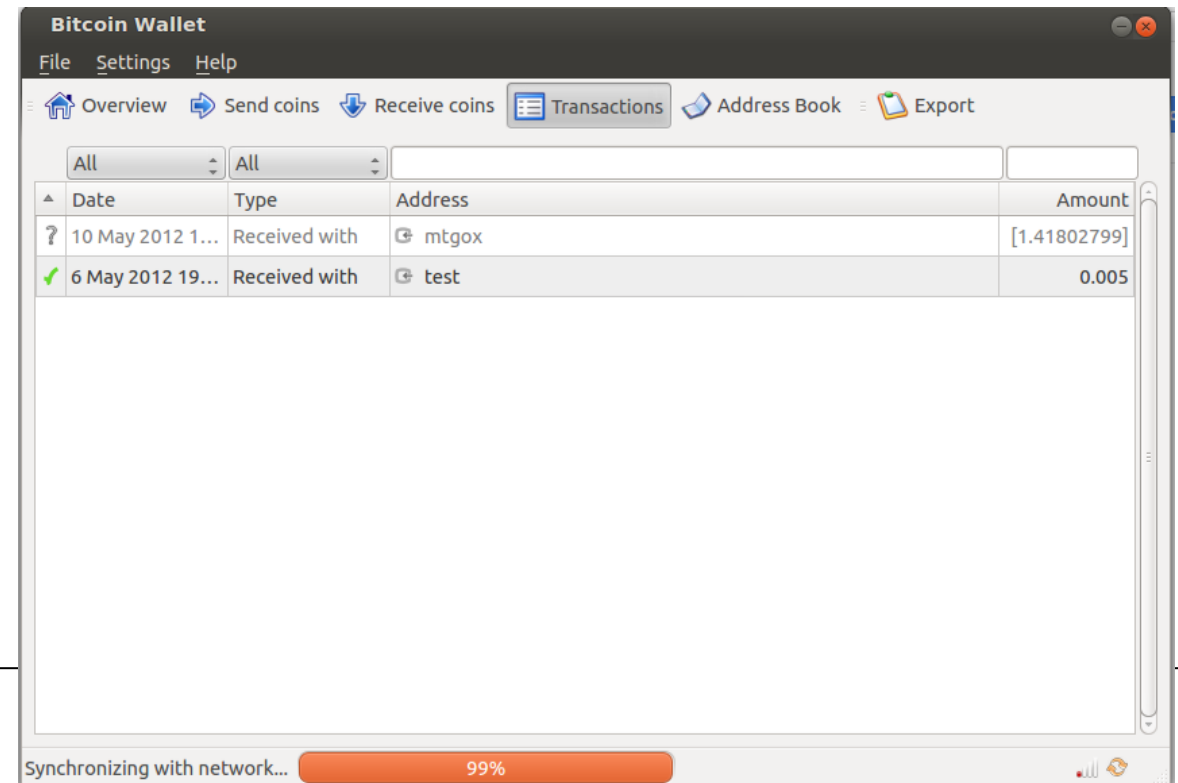
- SWIFT (financial messaging network) fee 25CHF, send 20USD
- Exchange rate 0.94000 → fee of 1,000 Yen → ~7.2USD

- **Spend 43.80 CHF for ~1.42 lousy BTC (2012)**

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

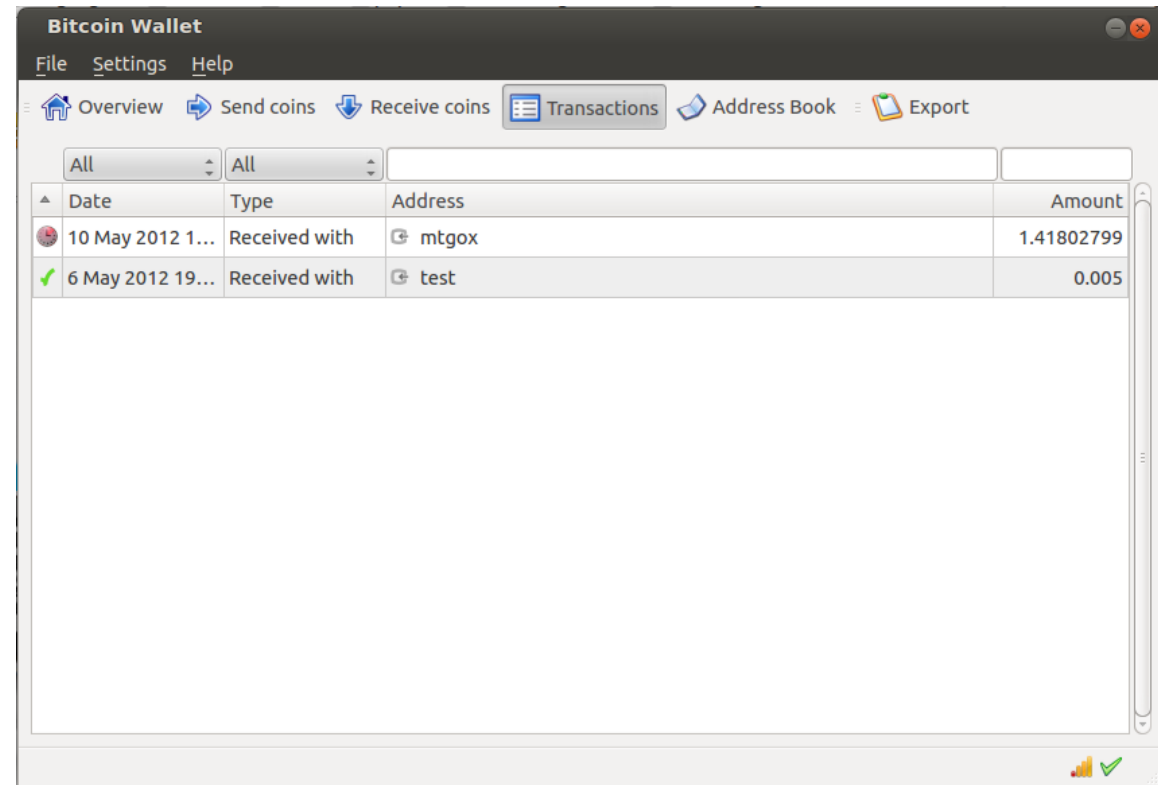
Bitcoin Client

- **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>
- **2020: its getting better**
 - SBB
 - However, credit cards often not working
 - Exchanges: KYC, delays



Bitcoin Client

- Transaction ongoing
 - Waiting for confirmations
- Good idea: don't leave coins in an online wallet



■ 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



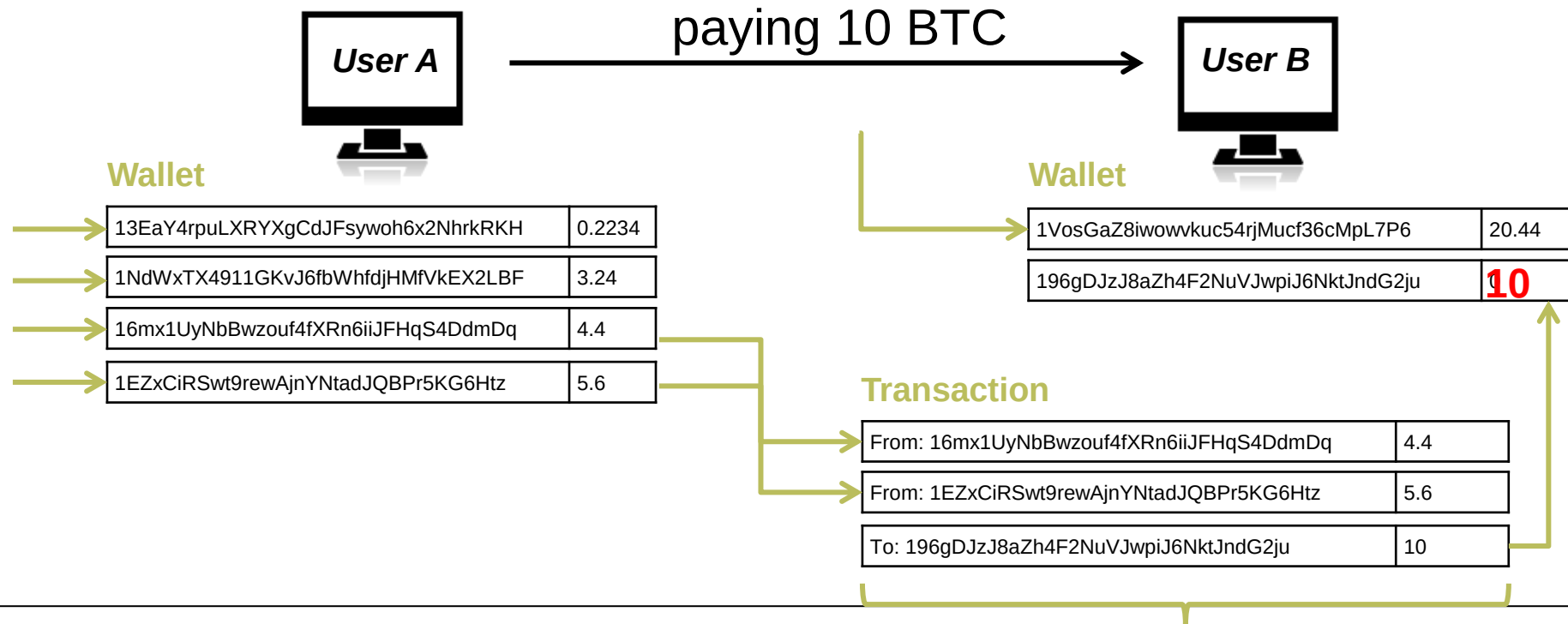
■ Transaction

- 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 (2)

■ 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

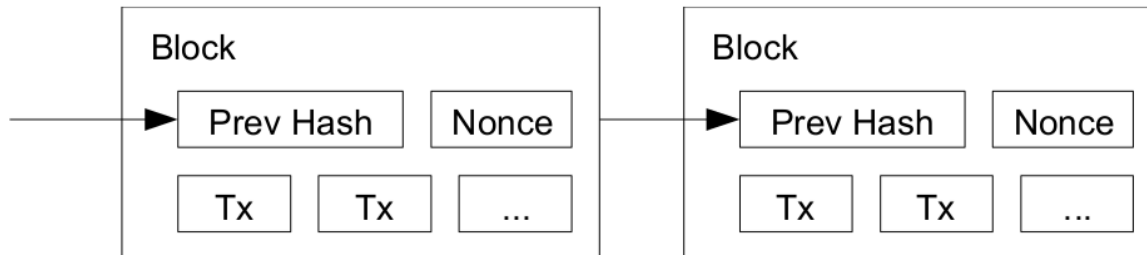


Sign with Private Key of User A

Mechanism

■ Avoiding double spending

- Transactions in blocks are confirmed.
- guessing value that results in zero bits
(00000000000001805ff174586
b6acf100f733aaf634e92f9580b4fac9272ed97)
- Chained proofs of work

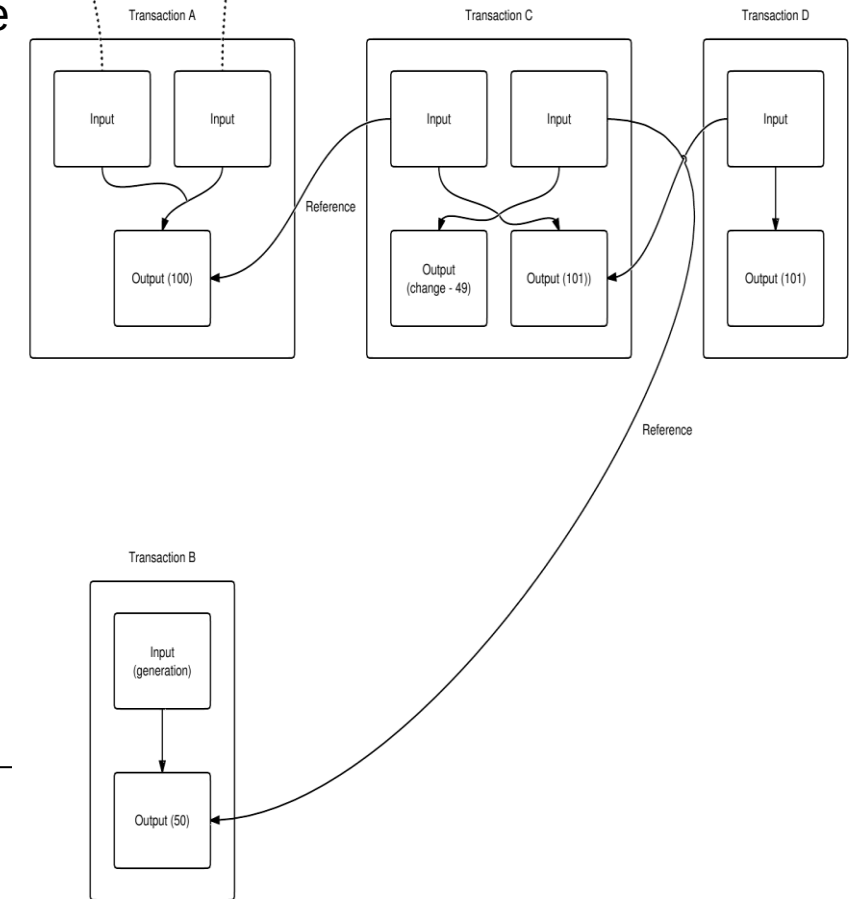


■ Generation of coins

- Mining / creating blocks → Miner get currently 12.5 BTC per creation
 - [adjustable difficulty](#) 6 blocks / h
 - Sometime in 2020 reward will be 6.25

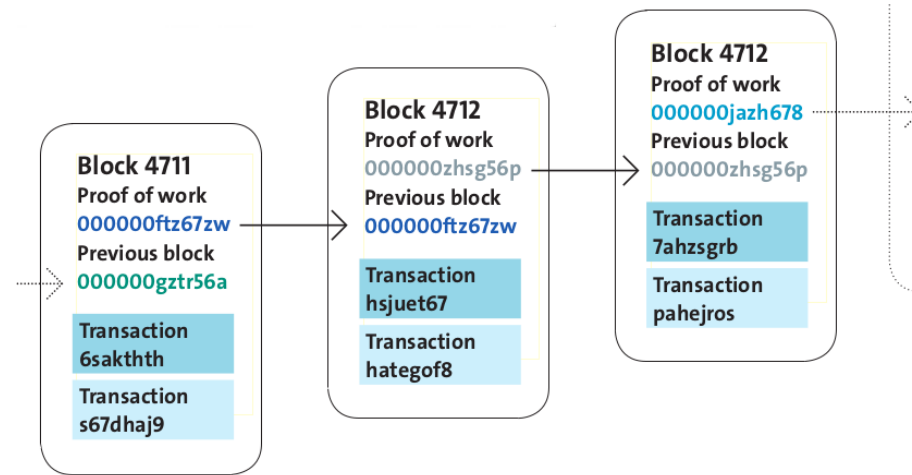
■ Transactions have one or more inputs

- 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



Blockchain (repetition)

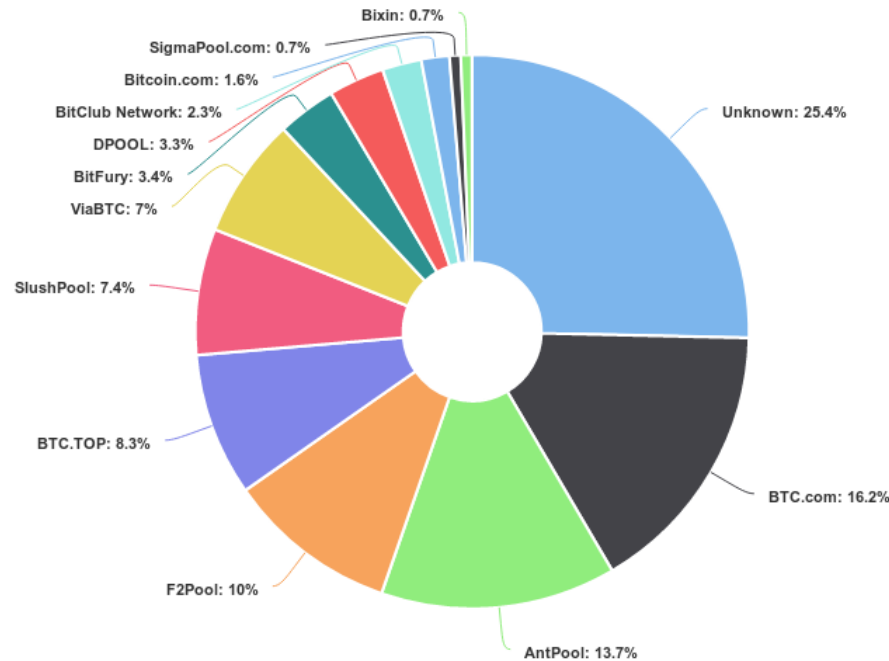
- **Transactions are collected in blocks**
 - New block created approximately every 10 min
- **Blocks contain solved crypto puzzles**
 - In the form of partial [hash collisions](#) (SHA256)
- **A block has a pointer to previous [block](#) → [Blockchain](#)**
- **Creation of blocks is called mining (reward)**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

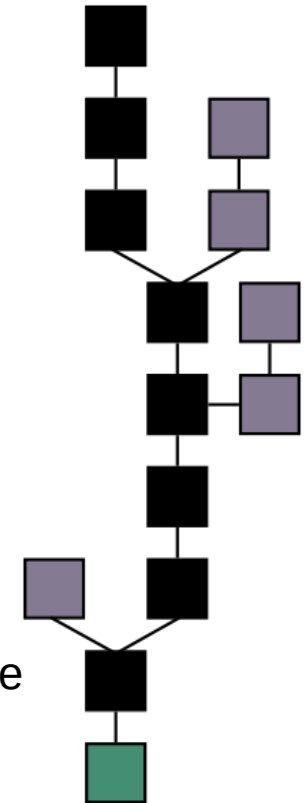
- Longest block survive (most difficult)

■ 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

■ Life Inside a Secret Chinese Bitcoin Mine

- 4,000 BTC per month
- <https://www.youtube.com/watch?v=K8kua5B5K3I>
- Others: <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>



■ KnCMiner

- Operator of the giant mining facility in Boden, Sweden
- Former maker of mining computers
- [Bankruptcy](#)



Mining: Evolution ASIC

■ Scenario: old ASIC miner

- Example: Avalon Batch #2
- 70GHash/s

■ Generates ~~2.11CHF~~ per day

■ Generates ~~~0.17CHF~~ per day

■ Generates ~0.005CHF per day in 2020

■ Uses 500-600W

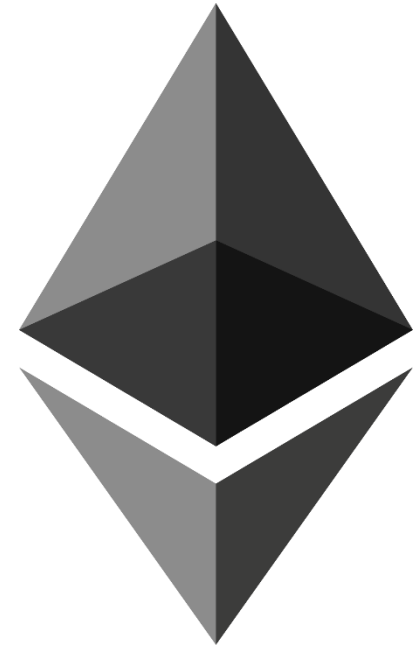
- 0.6KWh with 0.08 / 0.04CHF
- Cost per day 2.59 CHF
(Hochtarif, Mo-Sa 06:00-22:00)
- Cost per day 1.30 CHF
(Niedertarif, rest)



Many Coins – Similar Mechanism

■ All electronic backed by scarce resource - avoid: double spending

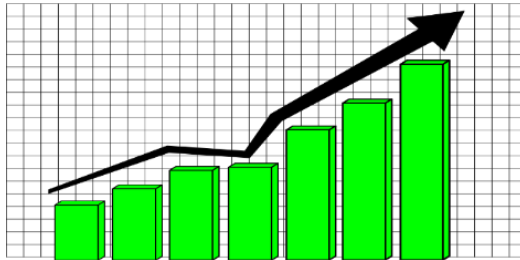
- Bitcoin: SHA256 partial hash collision: time, CPU, electricity
- Ethereum: variant of Dagger-Hashimoto, time, CPU, memory, electricity, miner store dataset: 1GB, verification only needs 16MB
- Ethereum: Opcodes in Bitcoin, smart contracts in Ethereum
- Litecoin: scrypt partial hash collision: time, CPU, memory, electricity
- Ripple XRP: Unique node list (trusted validators, 1000): web of trust
- [PPCoin](#)/Peercoin: proof of stake / (proof of work):
 - Holding/staking 1% will generate e.g., 1% of coins
 - Energy efficient / proof of stake
- [Cardano/EOS/...many more](#)



Discussion (1)

■ Advantages

- Low (fixed) tx fees
 - ~[18](#) satoshi per byte
- Scalable
 - Hardware/storage gets faster



- Anonymity
 - No privacy concerns/ datamining difficult

■ Disadvantages

- Power consumption
 - ~ 12 times AKW Beznau
- Not scalable
 - Bitcoin with 5 tps vs. VISA 57,000 tps (23.12)
[tps: transactions per sec]

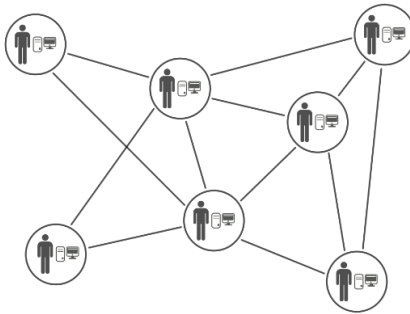


- Anonymity
 - Can be used for illegal activities

Discussion (2)

■ Advantages

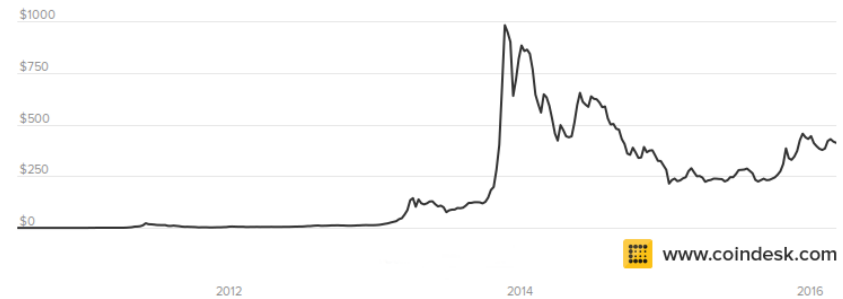
- No major “crashes”
 - [Mt.Gox](#) was exchange site!
- Decentralized
 - Open protocol
 - Forks



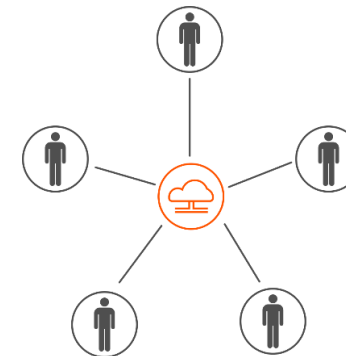
- Many other blockchain use cases
 - Smart contracts

■ Disadvantages

- Volatile exchange rate



- Core developers



Questions?



Dr. Thomas Bocek
thomas.bocek@hsr.ch