FS18

BLOCKCHAIN, BITCOIN, ETHEREUM

Introduction

T. Bocek

thomas.bocek@hsr.ch

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

Agenda

- **Distributed Systems in the News**
- **Bitcoin**
- **Transactions / Blocks**
- **Mining**

Distributed Systems - In the *News*

- **27.04.2018: A Thorough Introduction to Distributed Systems**
  - What is a Distributed System and why is it so complicated?
    - What is a distributed system?
    - Why distribute a system?
    - Database scaling example
  - Distributed System Categories
    - Distributed Data Stores
    - Distributed Computing
    - Distributed File Systems
    - Distributed Messaging
    - Distributed Applications
    - Distributed Ledgers
  - Summary: “Distributed Systems are complex”, … “They are harder to work with”, …
- **24.04.2018: Bitcoin Obituaries**
  - Bitcoin has died 288 times (slide 44, from lecture 5 :)

Kafka Exercises

- **From the exercises**
  - Recommended to use Windows
  - Kafka does not run with Win 32bit
  - Clean start: remove c:/tmp/zookeeper
- **private static final String APPLICATION_ID_DOC (Streaming – GroupID question)**
  - "An identifier for the stream processing application. Must be unique within the Kafka cluster. It is used as 1) the default client-id prefix, 2) the group-id for membership management, 3) the changelog topic prefix.“
- https://issues.apache.org/jira/browse/KAFKA-1194
  - Many run into this bug

```
 at
scala.collection.mutable.HashMap$$anonfun$foreach$1.apply(HashMap.scala:130)
        at
scala.collection.mutable.HashTable$class.foreachEntry(HashTable.scala:236)
        at scala.collection.mutable.HashMap.foreachEntry(HashMap.scala:40)
        at scala.collection.mutable.HashMap.foreach(HashMap.scala:130)
        at kafka.server.ReplicaManager.makeLeaders(ReplicaManager.scala:1163)
        at
kafka.server.ReplicaManager.becomeLeaderOrFollower(ReplicaManager.scala:1083)
        at
kafka.server.KafkaApis.handleLeaderAndIsrRequest(KafkaApis.scala:183)
        at kafka.server.KafkaApis.handle(KafkaApis.scala:108)
        at kafka.server.KafkaRequestHandler.run(KafkaRequestHandler.scala:69)
        at java.lang.Thread.run(Unknown Source)
Caused by: java.lang.OutOfMemoryError: Map failed
        at sun.nio.ch.FileChannelImpl.map0(Native Method)
        ... 43 more
```

```
Suppressed: java.nio.file.FileSystemException: F:\ELK\kafka-logs\beats-dev-
3\00000000000000457963.log -> F:\ELK\kafka-logs\beats-dev-
3\00000000000000457963.log.deleted: The process cannot access the file
because it is being used byanother process.
at
sun.nio.fs.WindowsException.translateToIOException(WindowsException.java:86)
at sun.nio.fs.WindowsException.rethrowAsIOException(WindowsException.java:97)
at sun.nio.fs.WindowsFileCopy.move(WindowsFileCopy.java:301)
at
sun.nio.fs.WindowsFileSystemProvider.move(WindowsFileSystemProvider.java:287)
at java.nio.file.Files.move(Files.java:1395)
at org.apache.kafka.common.utils.Utils.atomicMoveWithFallback(Utils.java:667)
... 28 more
```

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
- **Key characteristics**
  - Maximum of 21 million BTC
  - Every transaction broadcast to all peers
    - Every peers knows all transactions (~170 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 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  |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$
```

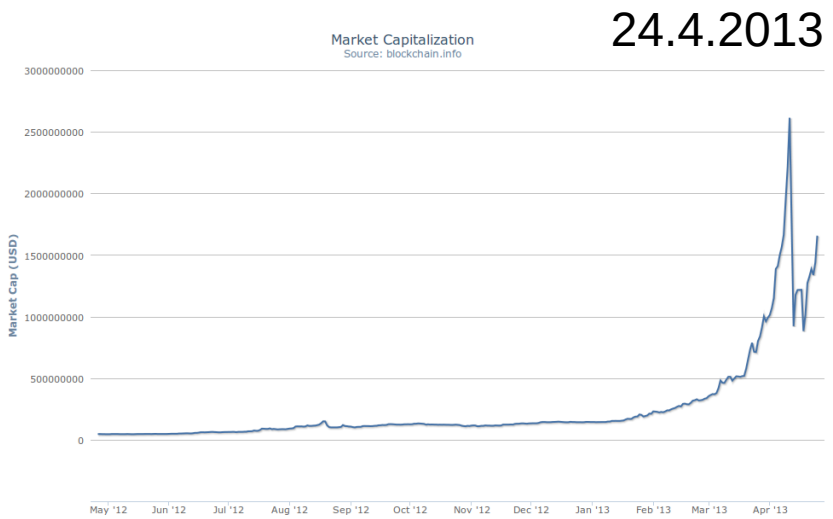
Who is Satoshi Nakamoto?

- 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)

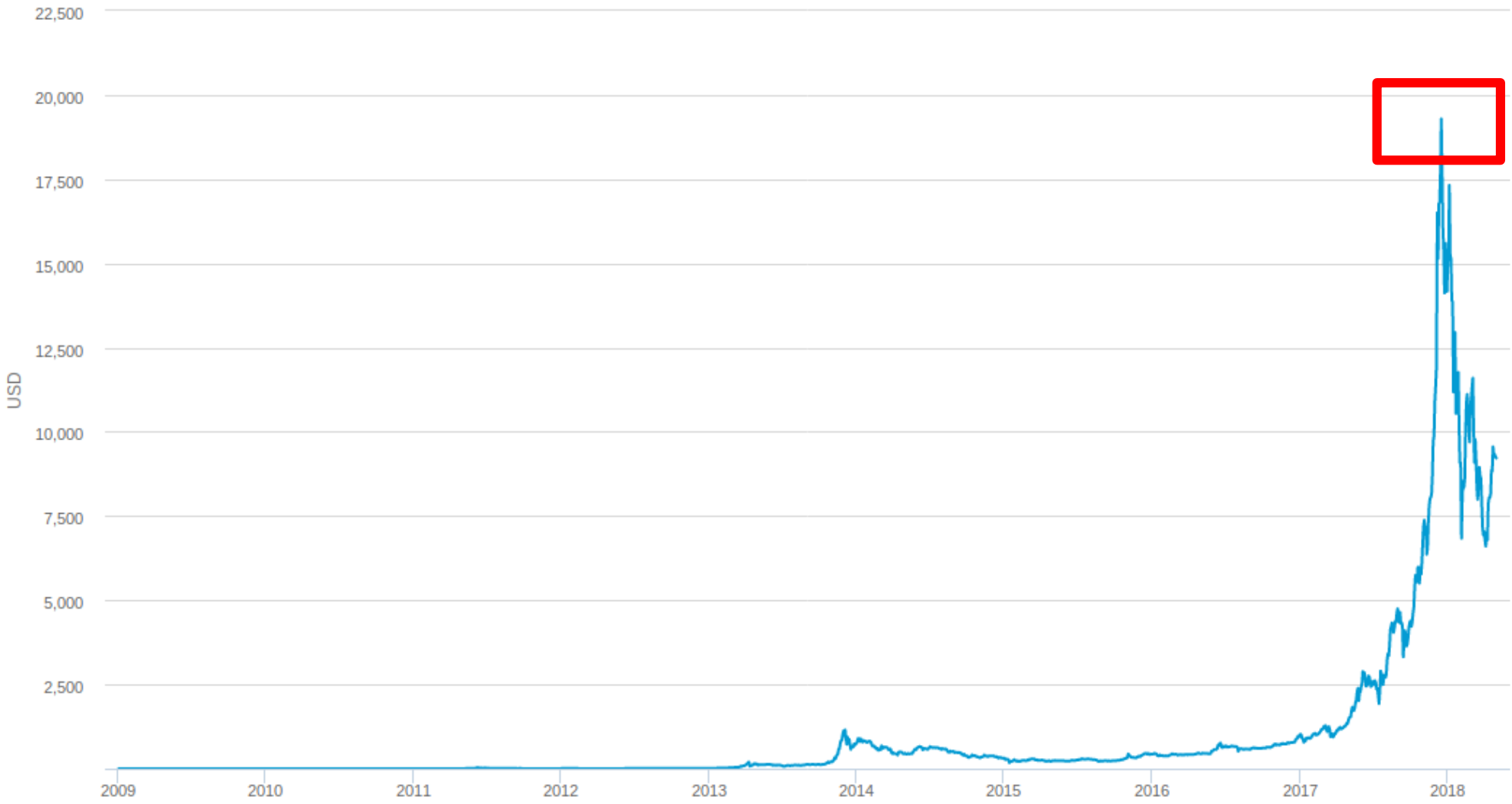
- **Satoshi is probably rich, first miner, may have ~1mio BTC**

Bitcoin‘s Market Capitalization in USD

- **Bitcoin boom, started in 2013 – current price**



Bitcoin‘s Market Capitalization in USD



2009 ***2011*** ***2014*** ***2016*** ***2018***

Bitcoi

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 | Topic

Tuesday May

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

Babbage
Science and technology

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

Comment (45)

E-mail

Reprints & permi

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by ... LONDON ... G.T. | MEL... IRNE

Like 1.8k Tweet 625

About Babba

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

Follow @Eco

RSS feed

de fr it

Ihr Ort: Zürich 19° Mi 20° Do 26° ... Schweiz

Registrieren Login

Video TV Infografik Games E-Prospekte Apps ... Inhalt A-Z Suchen

20 minuten ONLINE

Schweiz Ausland Panorama ... Sport Eishockey-WM People Entertainment Digital Mehr

News SMI Alle ... Ratg... Gelo... PROMOTION E-T...ung PROMOTION Anlageprodukte PROMOTION Finanzrechner Dossiers

Ihre Story, Ihre Inform...tionen, 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.

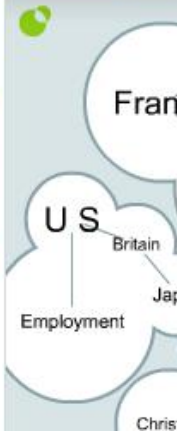
...ww.bitcoin.org

...ught ought ...ly, ...stment ...y a

Trending topi

Read comments o...

Period: 1 day



From 2011

HSR HOCHSCHULE FÜR TE... RAPPERSWIL

FHO Fachhochschule Ost...

Bitcoins in the News

- **3.5.2018, Handelsblatt**
  «UBS-Präsident Weber warnt „Krypto-Nation“ Schweiz vor Bitcoins»
- **2.5.2018, Finews**
  « SNB: Propaganda für den Bitcoin?»
- **3.5.2018, der Standard**
  «Warum es Bitcoin besser geht als je zuvor»
- **4.5.2018, focus.de**
  «Es gibt mehr als nur Bitcoin: Eine Stimmungsanalyse für die wichtigsten Kryptos IOTA, NEO, Cardano»
- **17.4.2018, cash.ch**
  «Der Bitcoin-Boom geht in die nächste Runde»
- **3.5.2018, coincierge**
  «Investment Bank prognostiziert düsteres Krypto-Ereignis»

As of 2018

URL: b.socrative.com/student/

Room: HSR

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.
- **Not controlled by a single entity**
  - Development community, no central bank – forks – Bitcoin Cash
- **Creation of Bitcoins: reward for validation (partial hash collision SHA-256) of payments**
- **Bitcoins can be exchange for real currencies**
  - Several companies allow to exchange BTC for Dollar, Euro, …
- **US, CH considered Bitcoin friendly, Russia not**

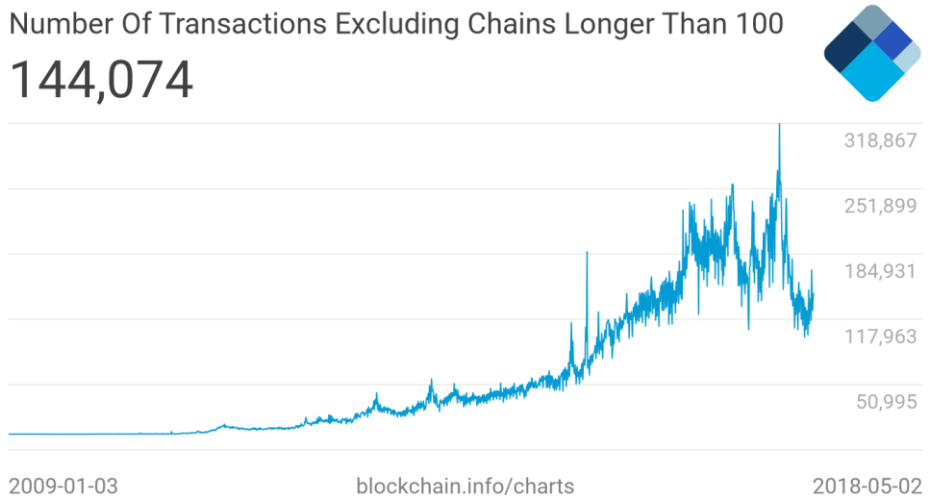
Bitcoin in Numbers

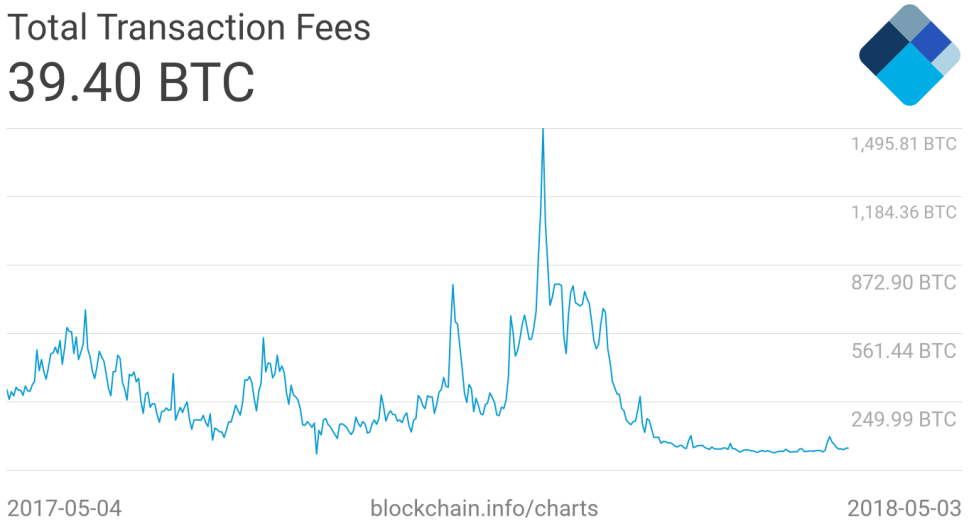
- **1 BTC ≈ 9731 US$ (4.5.2018)**
- **Total of 17.015 Million BTC mined**
  - Market capitalization of 165 Billion US$

#	Source	Pair	Volume (24h)	Price	Volume (%)
1	Bitfinex	BTC/USD	$399,089,000	$9,727.70	4.08%
2	Binance	BTC/USDT	$383,736,000	$9,699.38	3.92%
3	OKEx	BTC/USDT	$312,149,000	$9,713.49	3.19%
4	Huobi	BTC/USDT	$199,218,000	$9,698.41	2.04%
5	Binance	ETH/BTC	$193,109,000	$9,690.79	1.97%
6	Binance	TRX/BTC	$180,766,000	$9,882.97	1.85%
7	bitFlyer	BTC/JPY	$175,906,000	$9,675.15	1.80%
8	Upbit	BTC/KRW	$162,262,000	$9,926.20	1.66%
9	OKEx	TRUE/BTC	$158,638,000	$9,542.52	1.62%
10	GDAX	BTC/USD	$157,022,000	$9,691.80	1.60%
11	OKEx	EOS/BTC	$145,699,000	$9,743.80	1.49%
12	Binance	EOS/BTC	$144,533,000	$9,779.96	1.48%
13	OKEx	ETH/BTC	$136,844,000	$9,689.85	1.40%
14	Bithumb	BTC/KRW	$122,001,000	$9,912.26	1.25%

Bitcoin Transactions

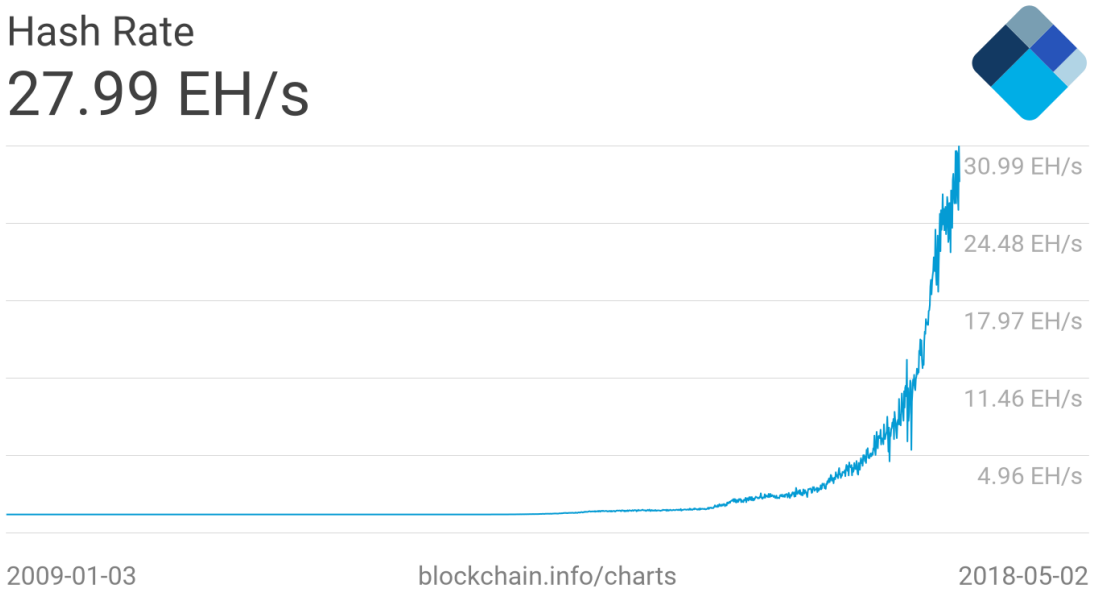
- **318,867 transactions per day (highest)**
  - 3.7 transactions per second
  - Maximum of 7 transaction per second
- **1,354,770 BTC traded per day**
  - Per hour
    ~56,448 BTC
  - Per second
    ~15.6 BTC
- **Transaction fees per day ~ 39 BTC**

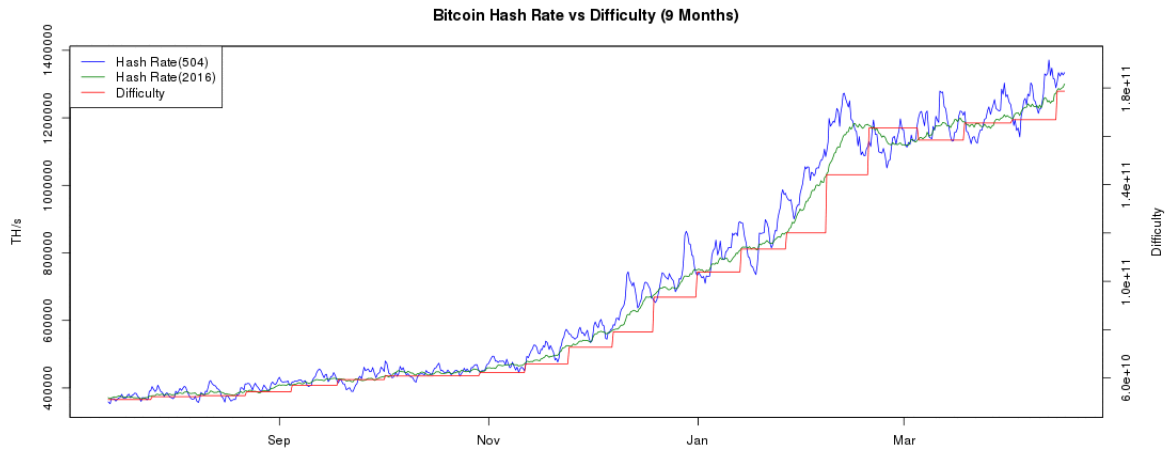




Bitcoin Numbers

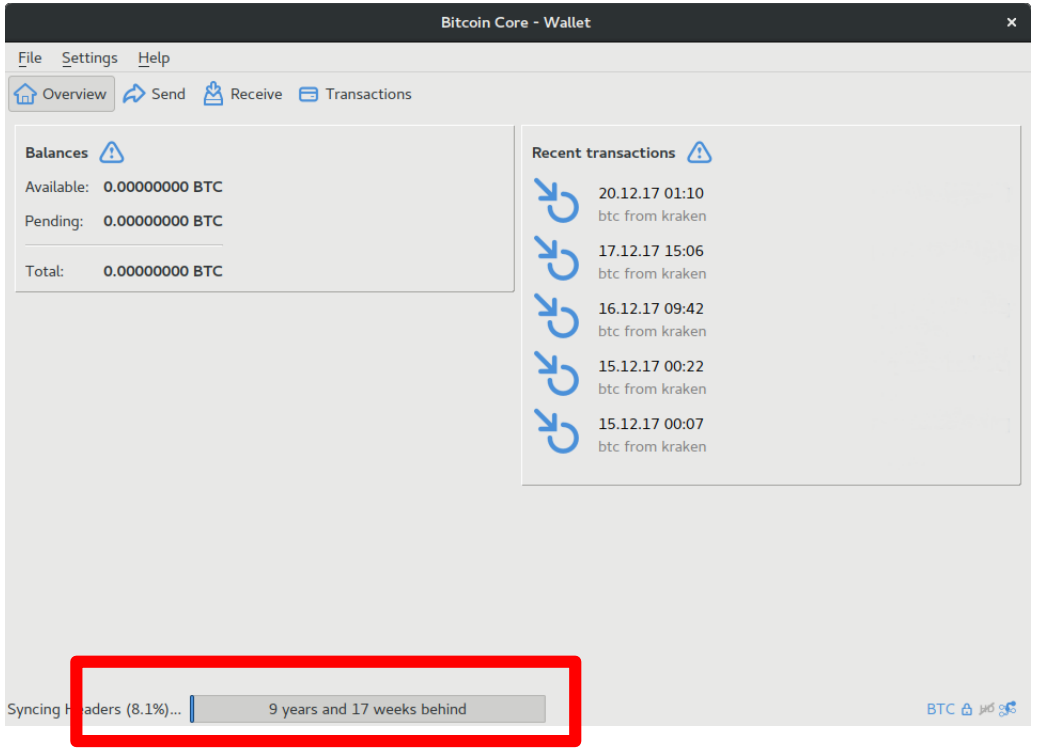
- **Network Hashrate (http://bitcoincharts.com)**
  - ~380 ZettaFLOPS
  - ~4 ZettaFLOPS in 2015
  - ~714 ExaFLOPS in 2014
  - ~900 PetaFLOPS in 2013
  - ~155 PetaFLOPS in 2012
- **Adjust time: 6.4 days**
- **Fastest supercomputer (top500.org) TaihuLight 93 PetaFLOPS (max), all 500 ~515 PetaFLOPS**

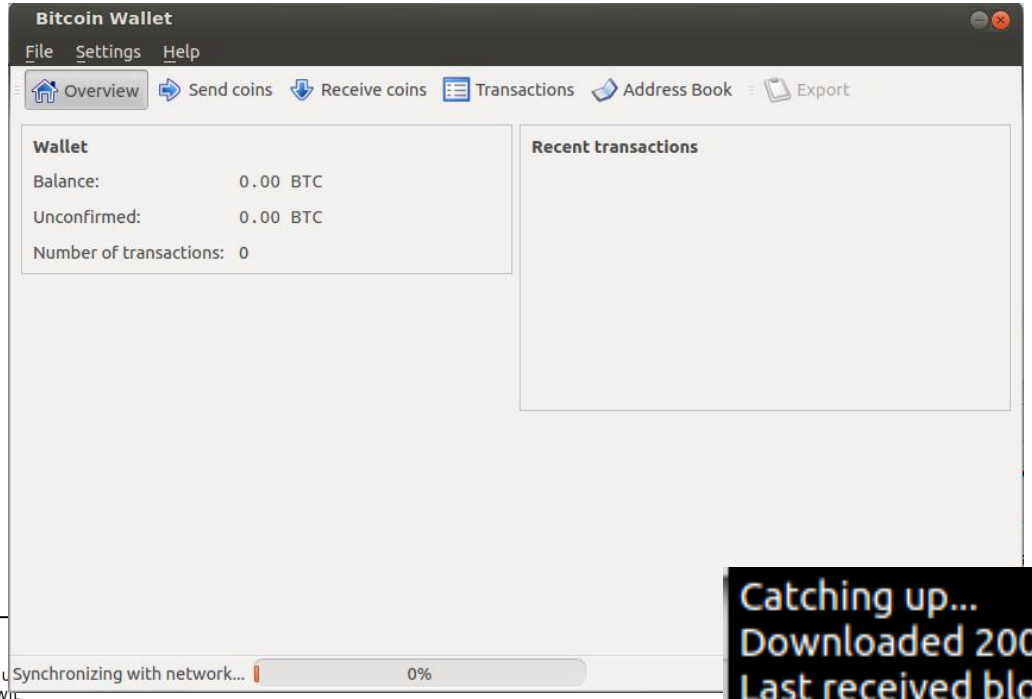




Bitcoin Example

- **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, 2018: 170GB



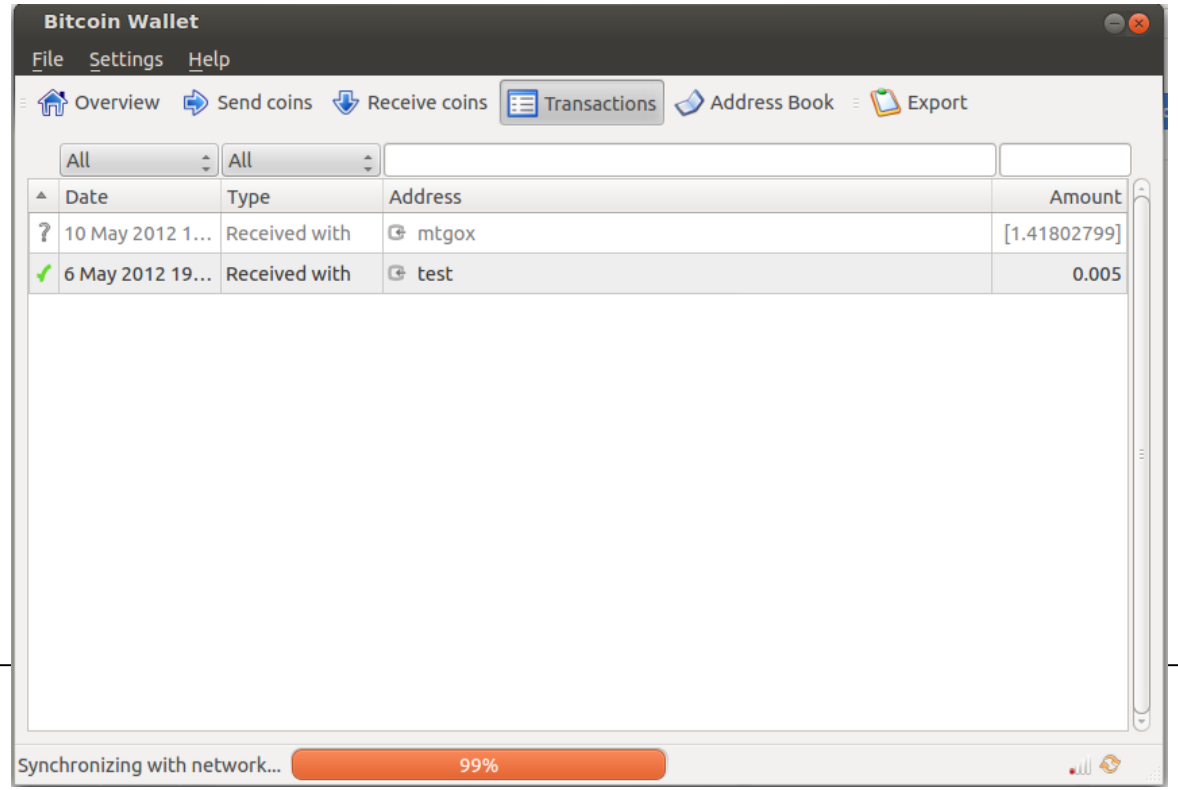


Bitcoin Example

- **Not easy to add funds…**
  - 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**

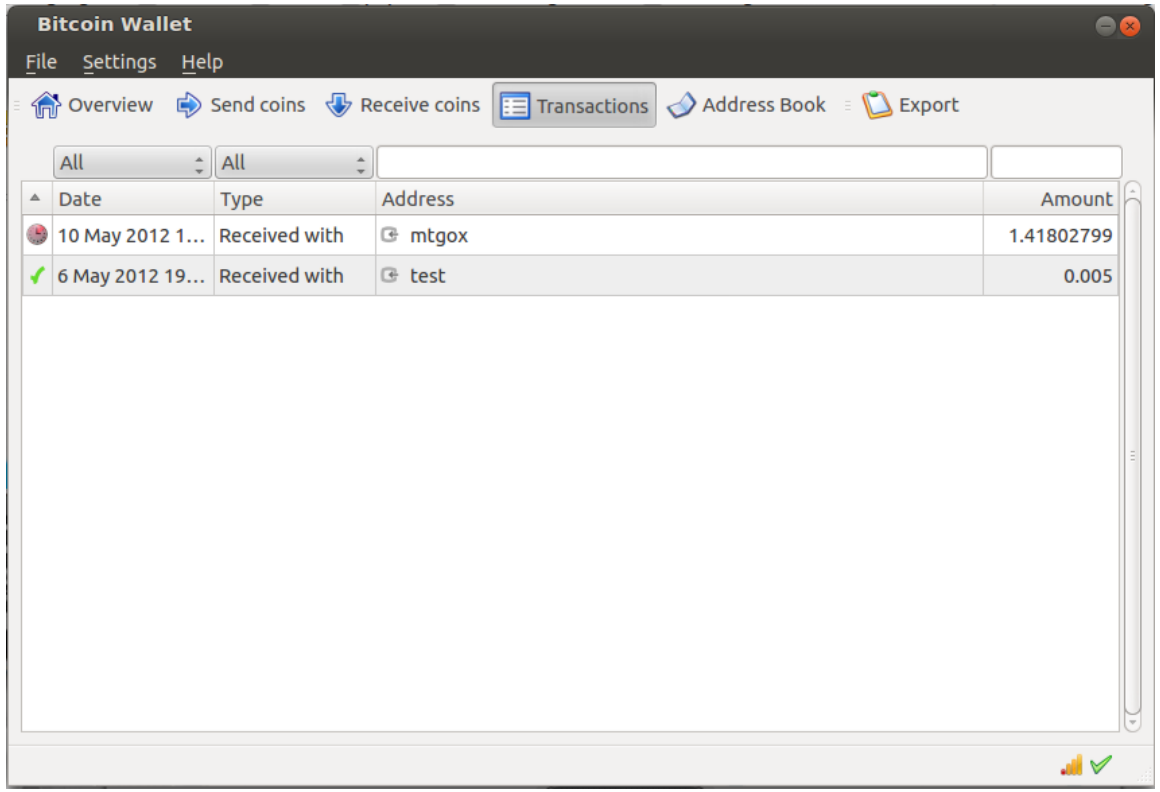
Bitcoin Client

- **2012: not easy to add funds… (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
- **2018: still not easy to add funds**
  - Credit cards often not working
  - KYC, delays



Bitcoin Client

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



URL: b.socrative.com/student/

Room: HSR

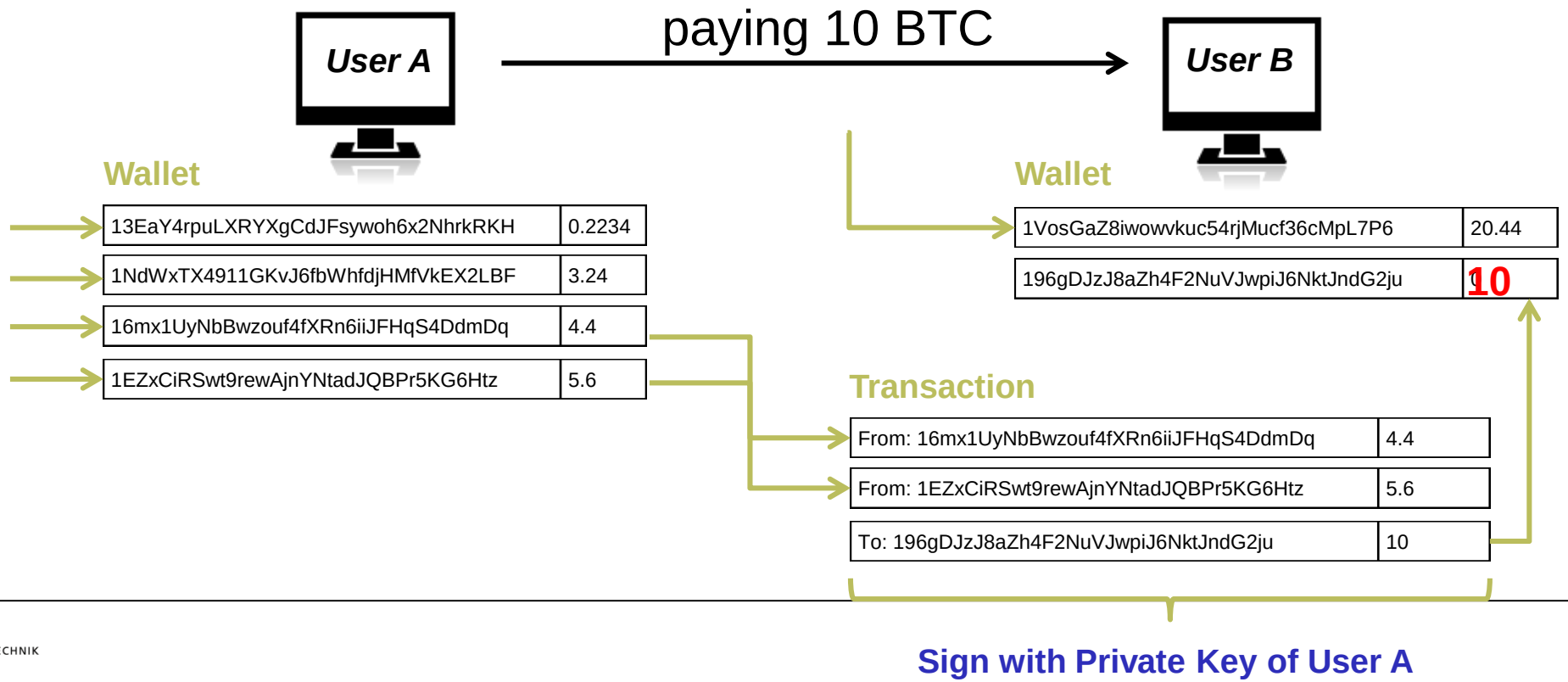
Mechanism

- **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

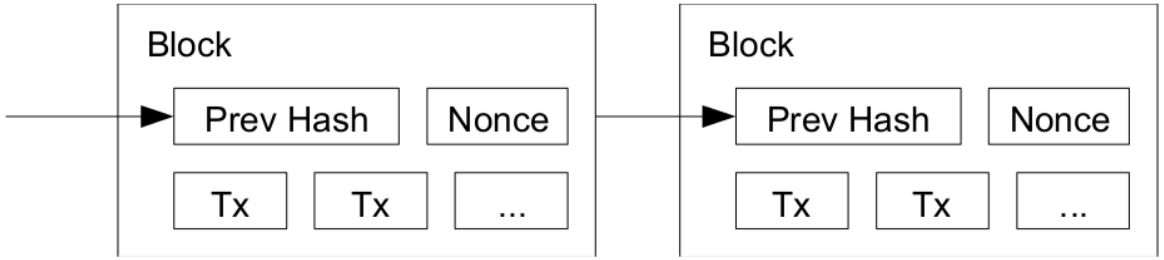
Key Bitcoin Operations (2)

- **Private key authorizes the transaction (“access“)**
  - If keys are stolen, thief may use “your” coins
  - If keys are lost, coins are lost



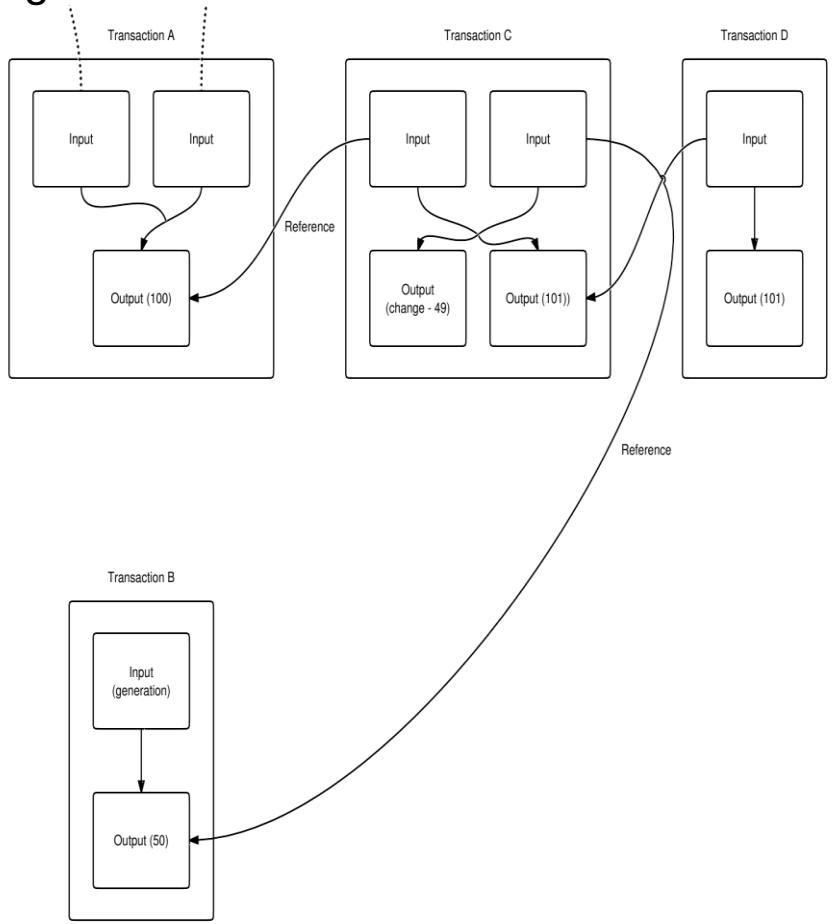
Mechanism

- **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 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



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

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

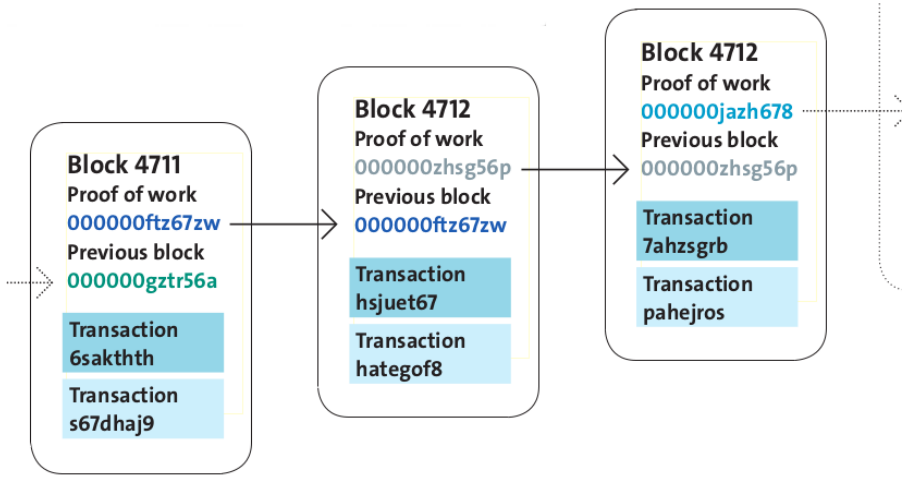
- **Non-turing complete (e.g. No loops)**
- **With scripts**
  - Multisig, n-of-m, escrow and dispute mediation
  - Micropayment channel, refund tx in future
- **Opcodes – all codes**
  - Data operations
    - OP_PUSHDATA1, OP_PUSHDATA4,...
  - Flow control
    - OP_IF, OP_ELSE, ...
  - Stack
    - OP_DUP, OP_SWAP, ...
  - Arithmetic
    - OP_ADD, OP_ABS, ...
  - Crypto
    - OP_SHA256, OP_CHECKSIGVERIFY

URL: b.socrative.com/student/

Room: HSR

Blockchain

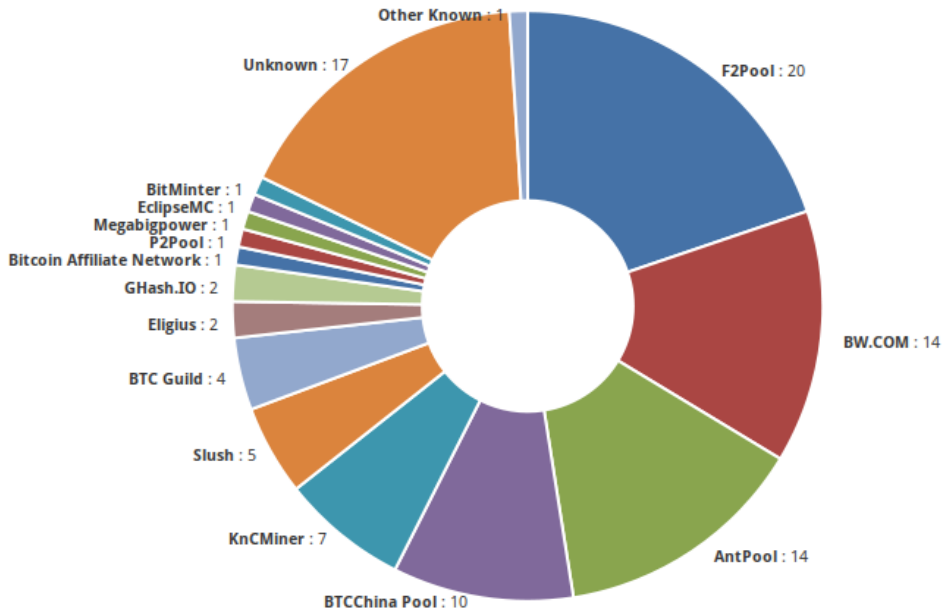
- **Transactions are collected in blocks**
  - New block created approximately every 10 min
- **Blocks contain solved crypto puzzles**
  - In the form of partial hash collisions (SHA256)
- **A block has a pointer to previous block → Blockchain**



- **Creation of blocks is called mining (reward)**
  - Miners use highly specialized hardware!

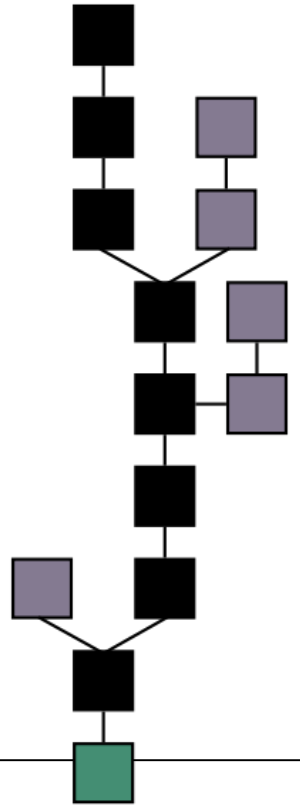
Mechanism - Mining

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



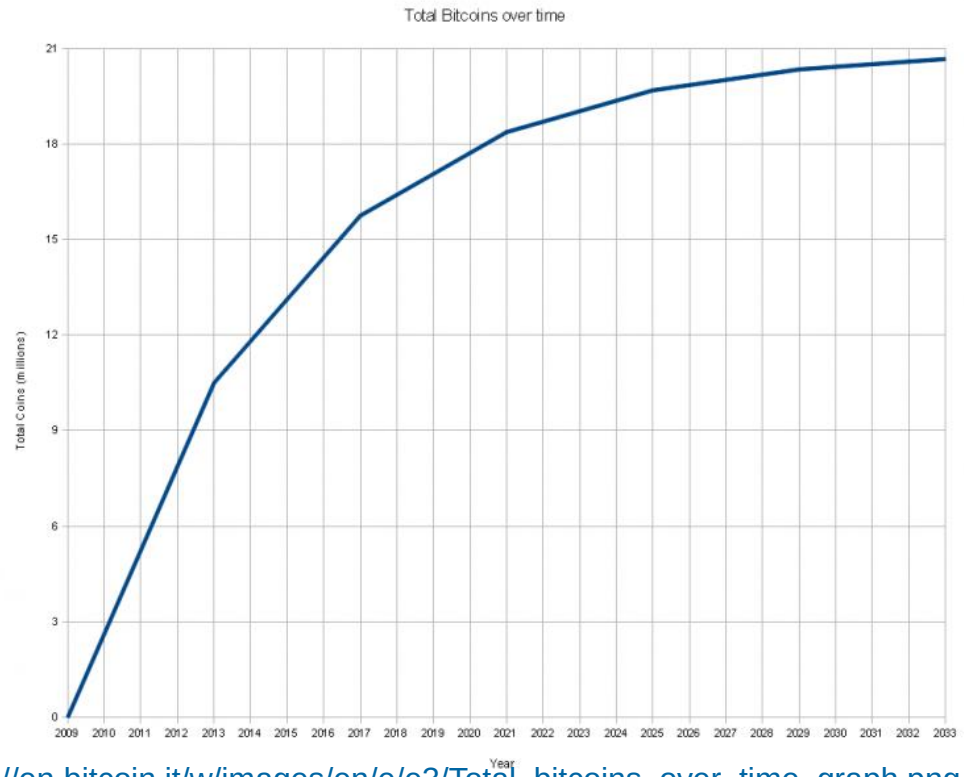
http://blockchain.info/pools

- **Mining = creating valid blocks**
- **Blocks are linked to previous blocks**
  - Longest block survive (most difficult)
- **Different level of confirmations**
  - 6 block conf. is considered secure



Mechanism

- **Mining**
  - Halves every 210000 blocks → max. 21m BTC
  - 12.5 BTC per block creation
  - Competition for creating valid block
- **Miner gets also transaction fees**
  - Required since BTC are limited
- **Dangerous if someone has more than 50% computing power**
  - Can exclude and modify the ordering of transactions

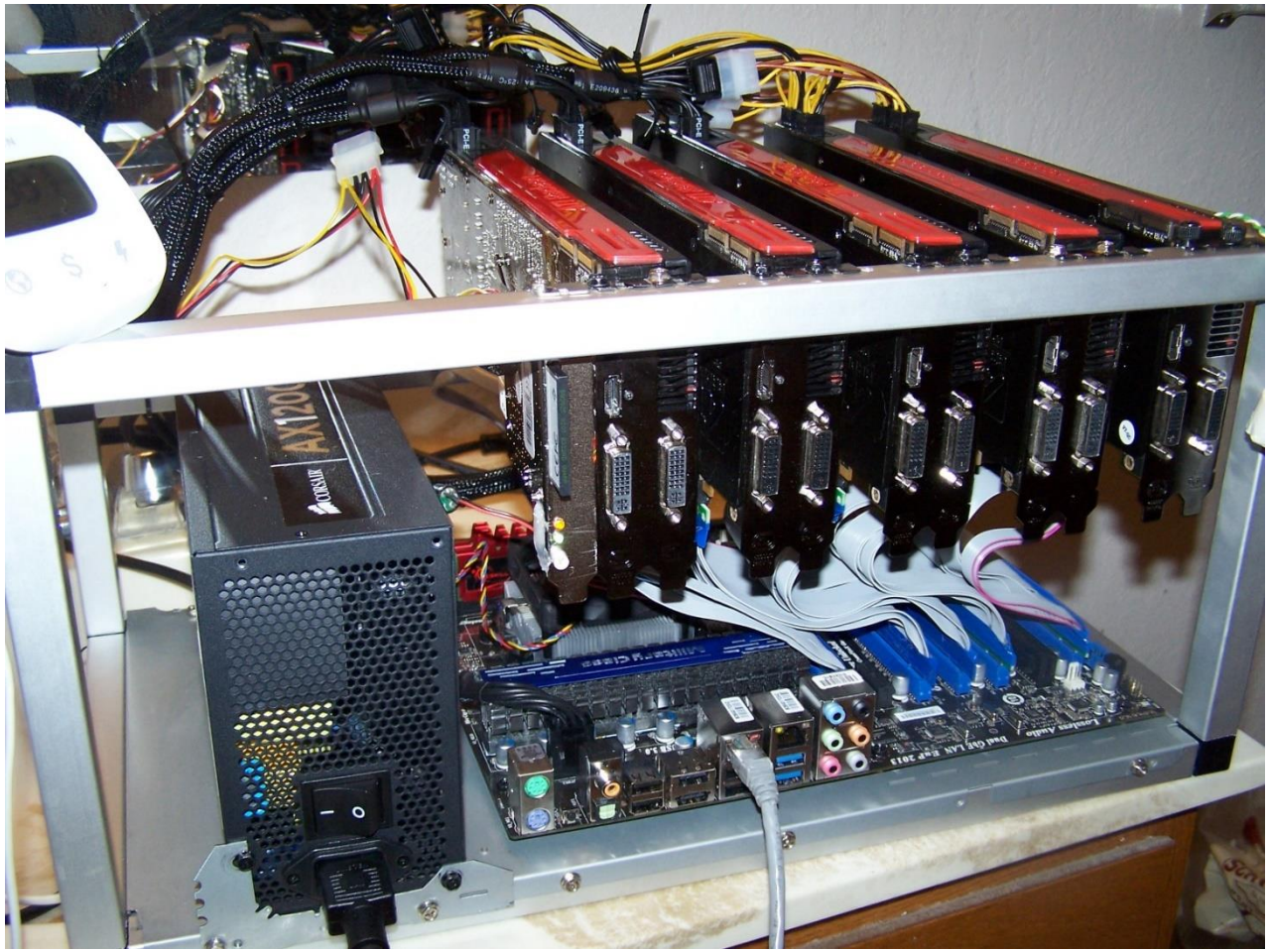


https://en.bitcoin.it/w/images/en/e/e3/Total_bitcoins_over_time_graph.png

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

- **KnCMiner**
  - Operator of the giant mining facility in Boden, Sweden
  - Maker of mining computers

Mining: Evolution ASIC

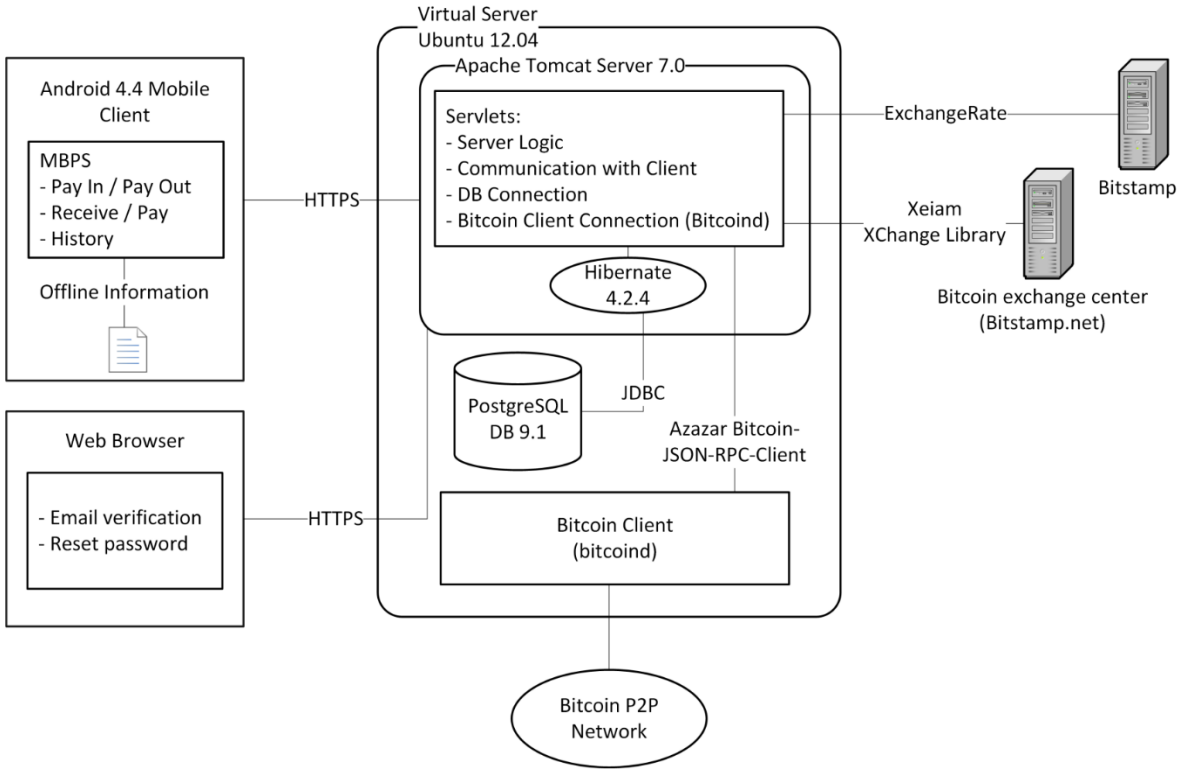
- **Scenario: old ASIC miner**
  - Example: Avalon Batch #2
  - 70GHash/s
- **Generates ~~2.11CHF per day~~**
- **Generates ~~~0.17CHF per day~~**
- **Generates ~0.08CHF per day**
- **Uses 500-600W**
  - 0.6KWh with 0.08 / 0.04CHF
  - Cost per day 2.59 CHF (Hochtarif, Mo-Sa 06:00-22:00)
  - Cost per day 1.30 CHF (Niedertarif, rest)

URL: b.socrative.com/student/

Room: HSR

Bitcoins at UZH

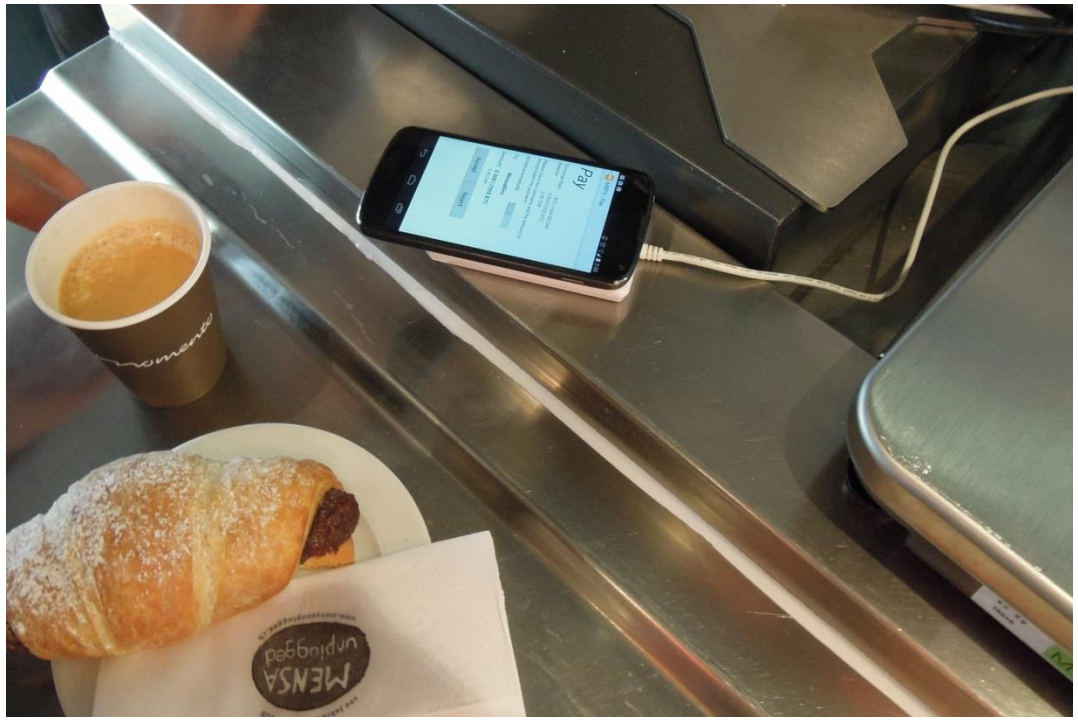
- **Bitcoin Mensa Project (MBPS/CoinBlesk)**
- **4 Testruns**
- **Why - transactions should be considered as verified after 3-6 block confirmations**
  - **Currently ~10-60 minutes**
  - **Not applicable for everyday transactions**
- **Goal - instant exchange of bitcoins (below 1sec)**
  - **By means of mobile devices (Android)**
  - **Use two-way Near Field Communication (NFC)**
- **Introduce a “clearing center” to reduce the number of Bitcoin core transactions**
  - **Reduce transaction fees**



System Architecture

Bitcoins at UZH: Evaluation: Mensa Test Run

- One week test run from 10th to 14th of February 2014
- In collaboration with the Mensa Binzmühle
- Pay all consumptions in Mensa with Bitcoins
- Reduce Bitcoin volatility risk by immediate trades on Bitstamp.net
  - After selling Bitcoins at the exchange point → Buy the same amount of Bitcoins
    - Keep the balance of the exchange point constant
  - After the Mensa receives Bitcoins → Sell these Bitcoins
    - Since the Mensa wants to receive CHF at the end, the equivalent amount is assured in this way



Example payment at Mensa Binzmühle

Bitcoins at UZH: Evaluation: Conclusions

- **NFC handling caused many problems because users are inexperienced with NFC**
- **Android 4.4 restriction → too big entry barrier at the moment / below 4.4 no two-way NFC possible**
- **Slide 39, lecture 5**
  - Bitcoins can currently hardly be used as means of payment because of the high volatility
    - Slide 39, lecture 5

USD/mBTC Exchange Rate Drop – February 10, 2014

URL: b.socrative.com/student/

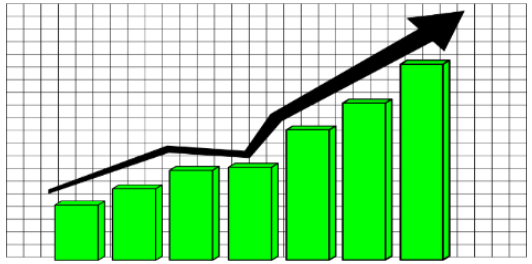
Room: HSR

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
  - 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 1% will generate 1% of coins
    - 1% inflation per year
    - Energy efficient / proof of stake
  - Many more

Discussion (1)

- **Advantages**
  - Low (fixed) tx fees
    - 10-30 satoshi per byte
  - Scalable
    - Hardware/storage gets faster



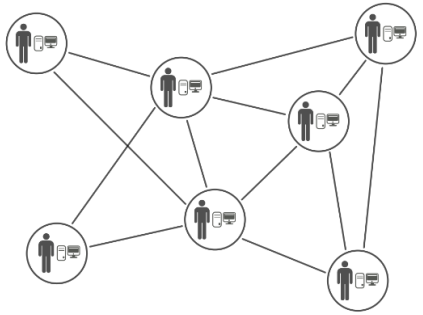
  - Anonymity
    - No privacy concerns/ datamining difficult

- **Disadvantages**
  - Power consumption
    - ~ 6 times AKW Leibstadt
  - Not scalable
    - Bitcoin with 7 tps vs. VISA 57,000 tps (23.12)
      [tps: transactions per sec]

  - Anonymity
    - Can be used for illegal activities

Discussion (2)

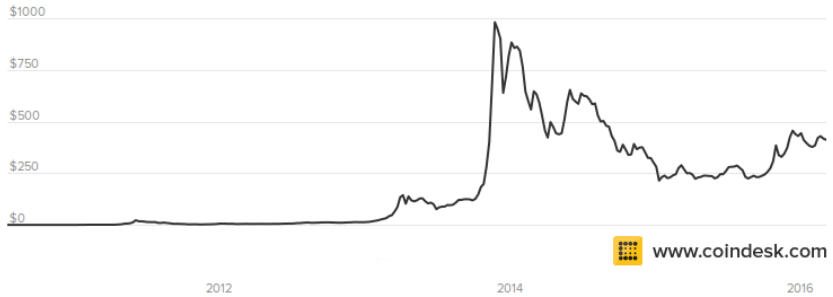
- **Advantages**
  - No major “crashes”
    - Mt.Gox was exchange site!
  - Decentralized
    - Open protocol



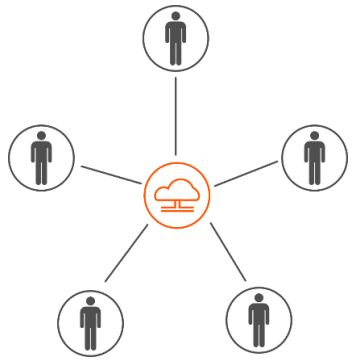
MT.GOX

  - Other blockchain usage
    - Smart contracts, Registry of Deeds

- **Disadvantages**
  - Volatile exchange rate



  - Core developers



Discussion

- **But! wrt ASIC – *"It shows that Bitcoin is considered stable enough for a company to invest a LOT of money on design and production on it, which is very good. ASICs were bound to happen if Bitcoin survived long enough."***
- **But! Bitcoin does not intend to replace VISA**
  - Still affordable by (some) individuals
  - Better comparable to wire transfers
- **But! Moore's, Nielson's law, and other laws**
  - Moore's law: number of transistors doubles every two years
  - Nielson's law: Bandwidth grows 50% per year
  - Kryder's Law: Space per unit cost has doubled roughly every 14 months
- **But! Lightning**
  - TX fees up to 30 USD → micro payments
  - Multisig, hashed timelock → fast and cheap transactions

Questions?

Prof. Dr. Thomas Bocek
thomas.bocek@hsr.ch