

Peer-to-Peer Systems and Applications



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Lecture 11: Peer-to-Peer Economics II

* Original slides provided by Arvid Norberg (Umea University), Thomas Bocek (University of Zurich), Matthäus Wander (University of Duisburg-Essen), Matthias Wichtlhuber (TU Darmstadt)

0. Motivation

- ❖ Accounting in Peer-to-Peer systems can have many flavors
 - No one-fits-all solution exists
 - Simple mechanisms are often file sharing specific, whereas complex solutions can be applied more widely, but do not have high performance
- ❖ Design space
 - Private history vs. shared history
 - Bilateral bartering vs. virtual currency
 - Centralized vs. decentralized accounting
- ❖ This lecture is about two extreme manifestations of accounting, that are deployed in the wild

0. Lecture Overview

1. BitTorrent: Concepts and Incentive
 1. Background
 2. Torrent Metadata
 3. Swarming/Tracking
 4. Unchoking Algorithm
 5. Piece Overlap vs. Distributed Copies
 6. Piece Picking Strategies
 7. Known Attacks
 8. Summary and Conclusions
2. BitCoin: A Peer-to-Peer Currency
 1. Background
 2. Protocol
 3. Transactions
 4. Proof-of-Work
 5. Block-Chain Split
 6. Mining
 7. Economic Aspects
 8. Summary and Conclusions
3. References



1. BitTorrent: Concepts and Incentive

Background, Metadata, Swarming, Tracker, Unchoking Algorithm, Piece Overlap vs. Distributed Copies, Piece Picking Strategies, Security of Incentive Scheme

1.1. Background

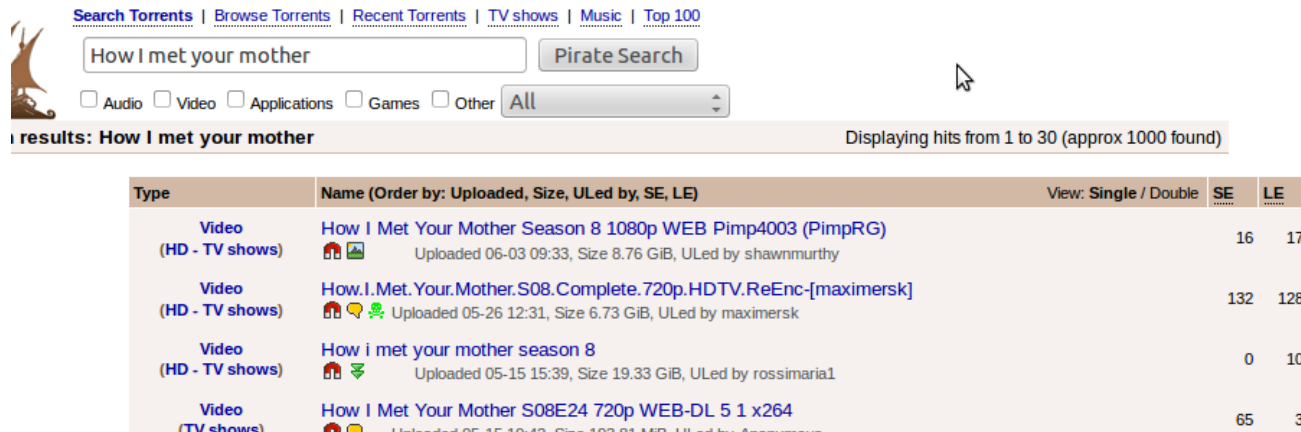
- ❖ BitTorrent is a system for efficient and scalable replication of large amounts of **static** data
 - Scalability: Overall throughput increases with the number of downloaders
 - Efficiency: The protocol uses a large amount of network bandwidth
- ❖ Introduced several new concepts [2][3]
 - Swarming, reciprocal incentives, ...
 - Design principle: „Distribute mechanisms only, if it is beneficial. If not, keep them centralised.“
 - No distributed search, use of central tracker server to coordinate peers

	Aggregate	
Rank	Application	Share
1	Netflix	29.03%
2	HTTP	16.59%
3	BitTorrent	13.47%
4	YouTube	9.90%
5	Flash Video	3.04%
6	RTMP	2.81%
7	iTunes	2.69%
8	SSL	1.96%
9	Facebook	1.84%
10	MPEG	1.49%
	Top 10	82.83%

SOURCE: SANDVINE NETWORK DEMOGRAPHICS 2012 [1]

1.2. Torrent Metadata

- ❖ A metadata file (.torrent) is distributed to all peers
 - Usually via HTTP
 - Can be found via (specialized) search engines
 - Google, The Pirate Bay, ...



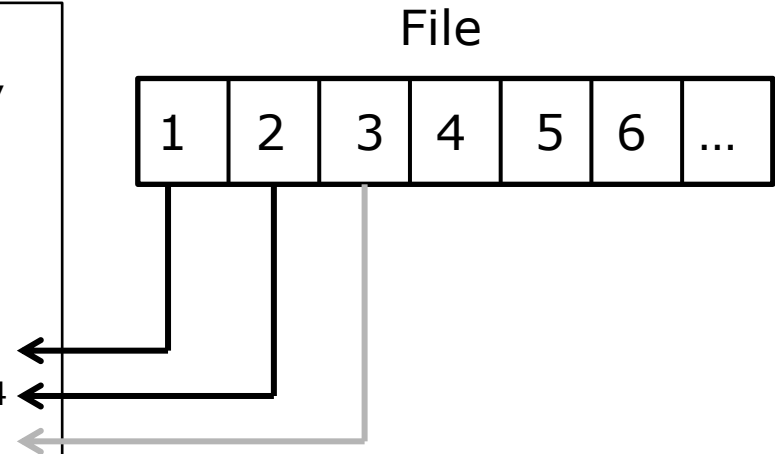
The screenshot shows the Pirate Search interface. At the top, there are navigation links: Search Torrents, Browse Torrents, Recent Torrents, TV shows, Music, and Top 100. Below these is a search bar containing the text 'How I met your mother' and a 'Pirate Search' button. Under the search bar, there are checkboxes for Audio, Video, Applications, Games, and Other, with a dropdown menu set to 'All'. Below the search bar, it says 'results: How I met your mother' and 'Displaying hits from 1 to 30 (approx 1000 found)'. The results are displayed in a table with columns: Type, Name (Order by: Uploaded, Size, ULed by, SE, LE), View: Single / Double, SE, and LE.

Type	Name (Order by: Uploaded, Size, ULed by, SE, LE)	View: Single / Double	SE	LE
Video (HD - TV shows)	How I Met Your Mother Season 8 1080p WEB Pimp4003 (PimpRG) Uploaded 06-03 09:33, Size 8.76 GiB, ULed by shawnmurthy		16	17
Video (HD - TV shows)	How.I.Met.Your.Mother.S08.Complete.720p.HDTV.ReEnc-[maximersk] Uploaded 05-26 12:31, Size 6.73 GiB, ULed by maximersk		132	128
Video (HD - TV shows)	How i met your mother season 8 Uploaded 05-15 15:39, Size 19.33 GiB, ULed by rossimaria1		0	10
Video (TV shows)	How I Met Your Mother S08E24 720p WEB-DL 5 1 x264 Uploaded 05-15 10:43, Size 102.81 MB, ULed by Anonymous		65	3

- ❖ Metadata can also be stored in a DHT
 - Magnet links for lookup

1.2. Metadata Content

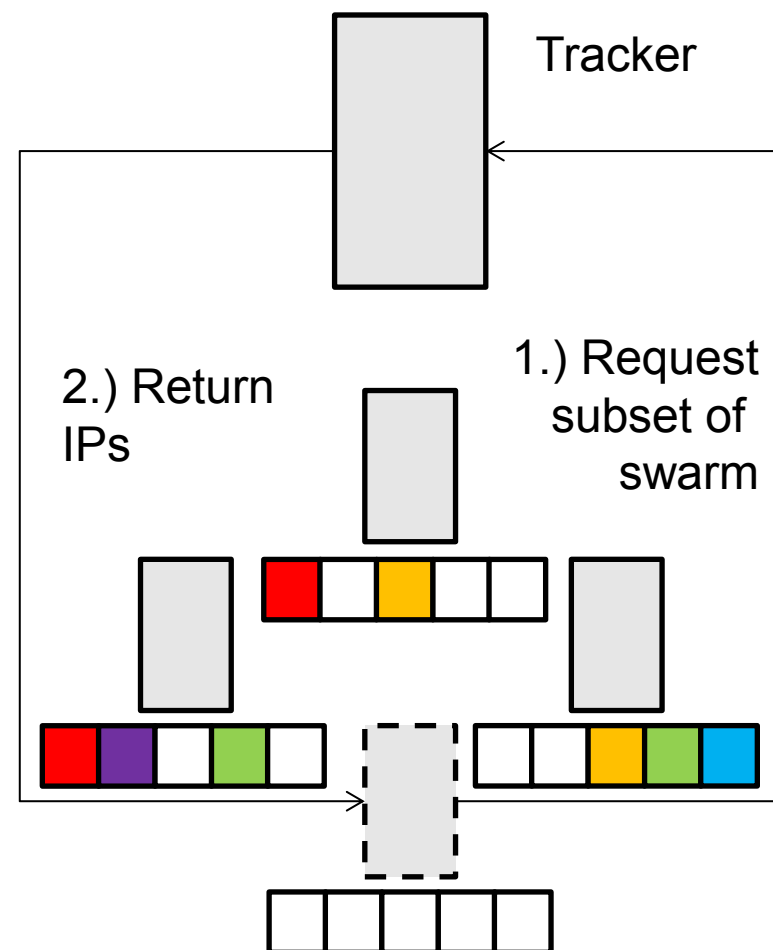
```
{
  'announce': 'http://bttracker.debian.org:6969/announce',
  'info':
  {
    'name': 'debian-503-amd64-CD-1.iso',
    'piece length': 262144,
    'length': 678301696,
    'pieces': 841ae846bc5b6d7bd6e9aa3dd9e551559c82a
              d14f1631d776008f83772ee170c42411618190a4
              ...
  }
}
```



- ❖ announce → tracker server reference (peering point)
- ❖ name → name of file to be downloaded
- ❖ piece length → length of piece (usually 256 KiB)
- ❖ length → overall length of file
- ❖ pieces → SHA-1 hash of all pieces (chunks)

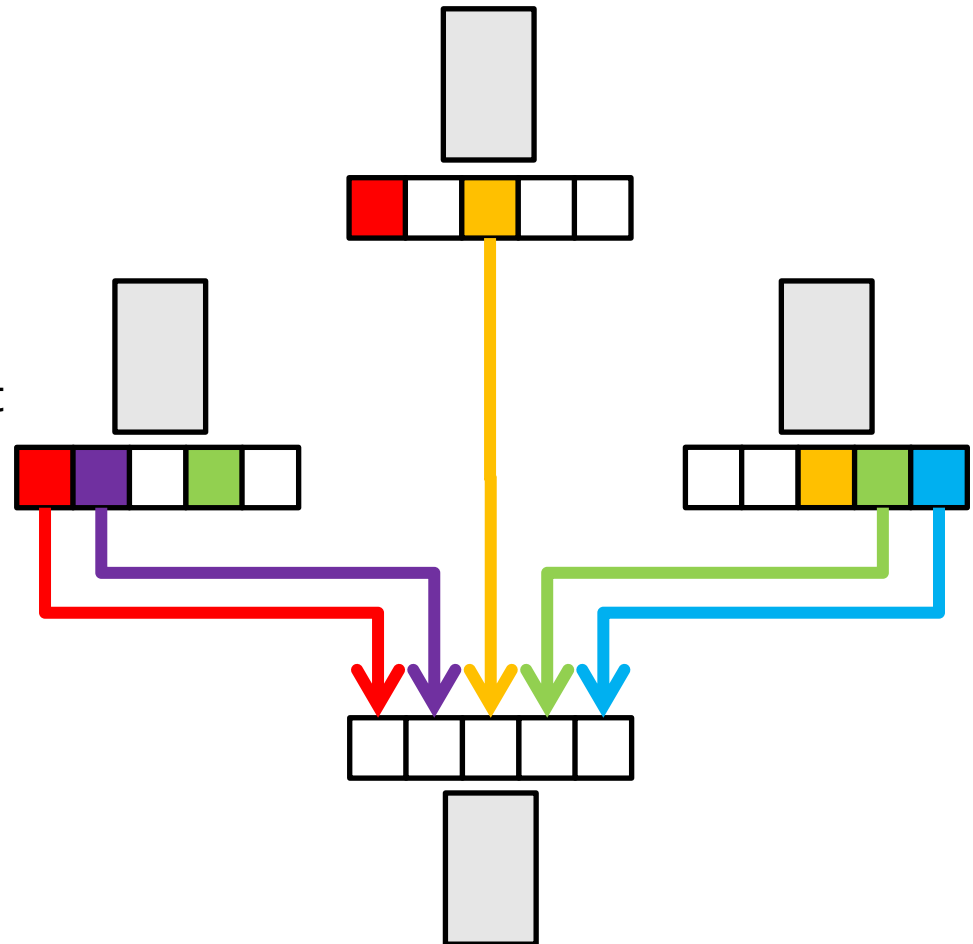
1.3. Swarming/Tracker

- ❖ The *tracker* is a central server keeping a list of all peers participating in the *swarm*
- ❖ The *swarm* is the set of peers participating in distributing the same file
- ❖ Join procedure:
 - New peer asks the tracker server for a subset of peers in the swarm
 - Tracker server returns random subset of IPs
 - New peer connects to IPs



1.3. Swarming/Tracker

- ❖ Efficiency
 - Fast multi-source download
- ❖ Reliability
 - Tolerant to dropping peers
 - Failover procedure: request chunk from other peer
 - Integrity of chunks can be proven
 - SHA-1 hash per chunk
- ❖ **However:** No incentive to share



1.4. The Unchoking Algorithm

- ❖ Connections with other peers are choked or unchoked
 - A *choke* message from peer A to peer B signals, that A will not upload to B, until the connection is unchoked
 - An *unchoke* message from peer A to peer B signals, that A will upload to B, until the connection is choked

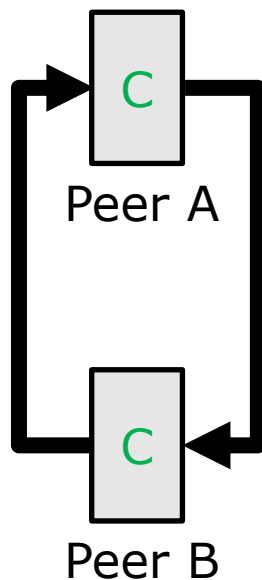
- ❖ Peers are *choked/unchoked* for several reasons
 - For ensuring reciprocal behavior
 - To allow new peers to enter the system

1.4. The Unchoking Algorithm

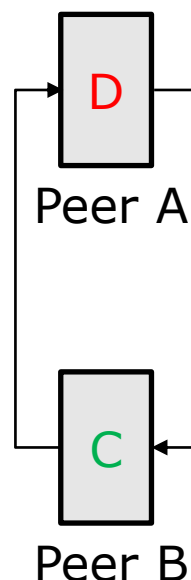
- ❖ Ensuring reciprocal behavior
 - Serve cooperating peers with higher probability
 - Every 10 seconds, the interested peers are ordered according to their download rate and the 3 fastest peers are unchoked
 - **Precondition:** Asymmetric interest → Peer A needs to have a chunk peer B is interested in and vice versa

- ❖ To allow new peers to enter the system (optimistic unchoking)
 - New peers do not have chunks to share
 - Every 30 seconds, unchoke one random peer

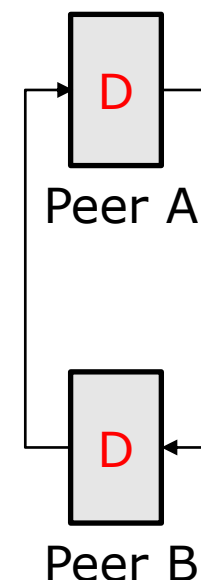
1.4. The Unchoking Algorithm



A cooperates &&
B cooperates
→ Data rate increases
until bandwidth limit is
reached by A || B



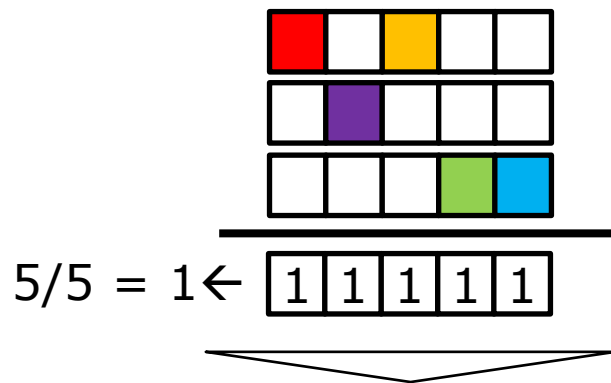
(A defects &&
B cooperates) || (A
cooperates && B defects)
→ Quick breakdown of
data rate, no use for
both sides



A defects &&
B defects
→ Quick breakdown of
data rate, no use for
both sides

1.5. Piece Overlap vs. Distributed Copies

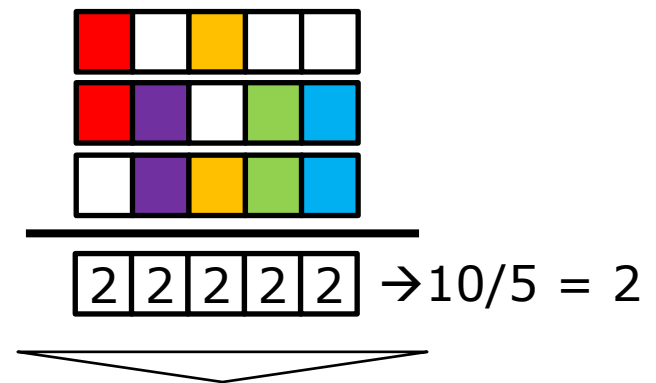
- ❖ Piece overlap is defined as the sum of overlapping pieces divided by the number of pieces
 - Determines efficiency of bilateral trading



Low Overlap
→ Any peer can trade
with any peer
→ Bandwidth is
utilized well

Peer A
Peer B
Peer C

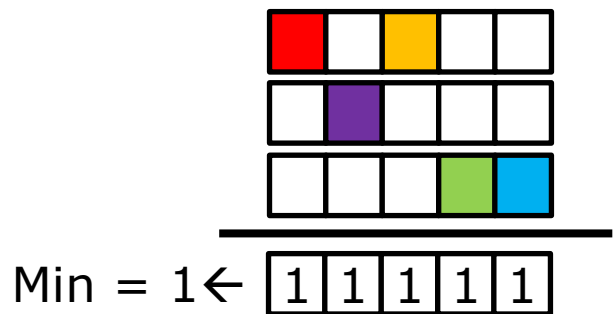
Overlaps



High Overlap
→ Only a few peers can
exchange pieces
→ Bandwidth is under
utilized

1.5. Piece Overlap vs. Distributed Copies

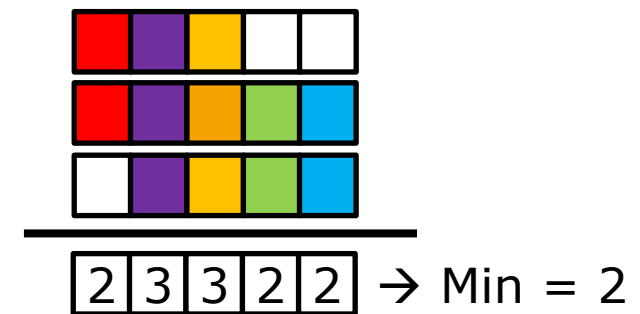
- ❖ The number of distributed copies is defined as the number of copies of the rarest piece
 - Determines loss of chunks



Low number of distributed copies
→ Danger of piece loss, as peers may quit the system

Peer A
Peer B
Peer C

Copies



High number of distributed copies
→ Low danger of losing pieces

1.5. Piece Overlap vs. Distributed Copies

- ❖ The system has to serve contradicting goals
 - Minimise piece overlap
 - minimises number of distributed copies
 - Ensure enough distributed copies to exist
 - maximises piece overlap
- ❖ BitTorrent solves this problem by applying a *rarest-first* piece picking strategy
 - Goal: ensure a certain number of distributed copies while ensuring to fill the buffer uniformly

1.6. Piece Picking Strategies

❖ **Default:** Rarest First

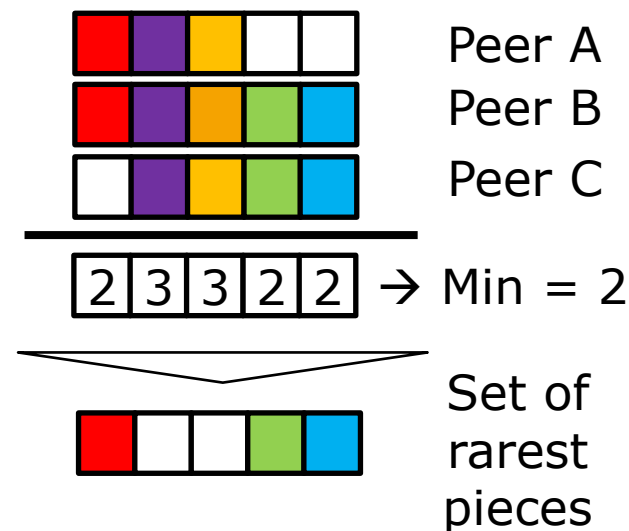
1.) Approximate number of copies of piece in neighbor set

- On handshake, peers exchange information on possessed pieces (bitfield)
- Client keeps this information, updates on answers to own requests

2.) Find pieces determining number of distributed copies

- Set of rarest pieces

3.) Select a random piece from the set of rarest pieces for next download



1.6. Piece Picking Strategies

❖ **On join:** Random First

1.) If number of downloaded pieces < 4 ...

- The peer has just joined the network and has no pieces for trading

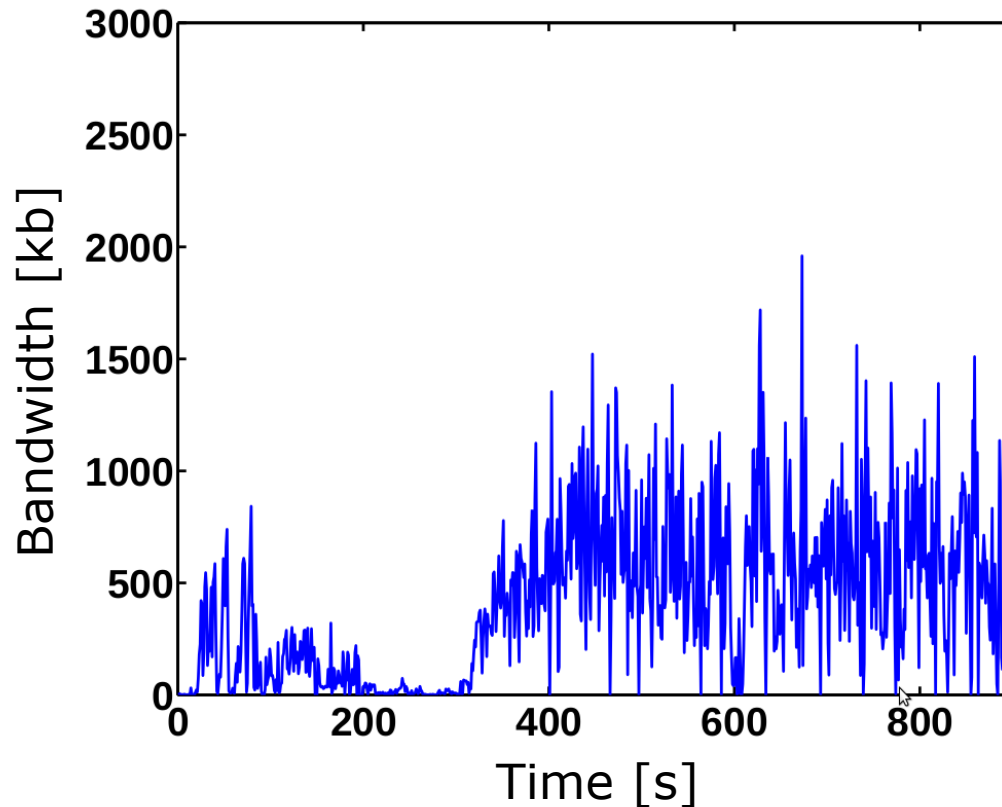
1.1) Request a random piece from neighbor peers

- Random piece is likely to be wider replicated
- Increases the probability to hit optimistic unchoke

2.) ... else switch to rarest first strategy

- ❖ Nevertheless, the bandwidth is under utilized in the beginning (see next slide)

1.6. Piece Picking Strategies



BitTorrent client downloading Ubuntu,
Random First causes ~300 s startup delay

1.6. Piece Picking Strategies

❖ **Before completion:** Endgame Mode

1.) If all blocks were requested once ...

- All blocks are either downloaded or pending

1.1) Request all pieces from all peers in neighborhood

- This increases the probability to receive last missing pieces

❖ This is an instance of the Coupon Collector's Problem

- Assume a merchant offering 50 different coupon cards
- The probability to receive a card not already possessed decreases sharply with every card
- Can only be circumvented by increasing requests
- <http://www-stat.stanford.edu/~susan/surprise/Collector.html>

1.7. Known Attacks

❖ In theory, BitTorrent is prone to ...

➤ Collusion

- Cooperation of peers to receive resources



➤ Whitewashing

- Frequent rejoining of peers with new identities



➤ Sibyl attacks

- Joining with several identities at the same time



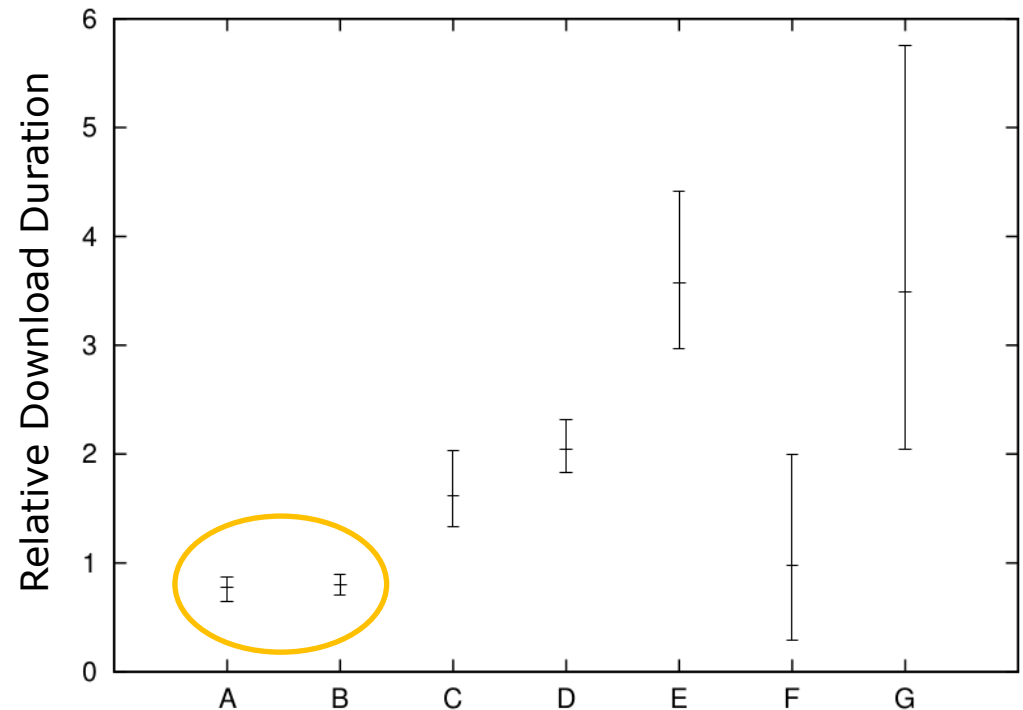
➤ Byzantine attacks

- Varying behavior towards different peers
- Cooperate with peer A, defect with peer B, ...



1.7. Known Attacks

- ❖ In practice, there are several ways to allow free-riding with high data rates
- ❖ BitThief [4]
 - Frequently contact tracker to grasp all peers in the swarm
 - Connect to all peers and benefit from optimistic unchoking
 - No rarest-first, always download what you can get



Free riding with BitThief in 7 different swarms. The downloading time of the reference client is normalized to 1.0.

1.8. Summary and Conclusions

- ❖ BitTorrent highly efficient for sharing static data
 - Metadata is stored in .torrent files, which can be distributed using the web
 - A tracking server coordinates the swarm
 - Multi-source download enables high data rates

- ❖ The unchoking algorithm sets incentives for sharing
 - In theory, only two cooperating peers can benefit from sharing
 - However, in practice, the scheme cannot prevent free riding

- ❖ Rarest-first strategy ensures balance of distributed copies vs. piece overlap

2. Bit Coin: A Peer-to-Peer Currency

Background, Protocol, Transactions, Proof-of-Work, Block-Chain Split, Mining, Economic Aspects, Summary and Conclusions

2.1. Background

❖ BitCoin [5] is a digital Peer-to-Peer currency

May 12, 2013 4:45 am

Bitcoin buzz shakes US bond market

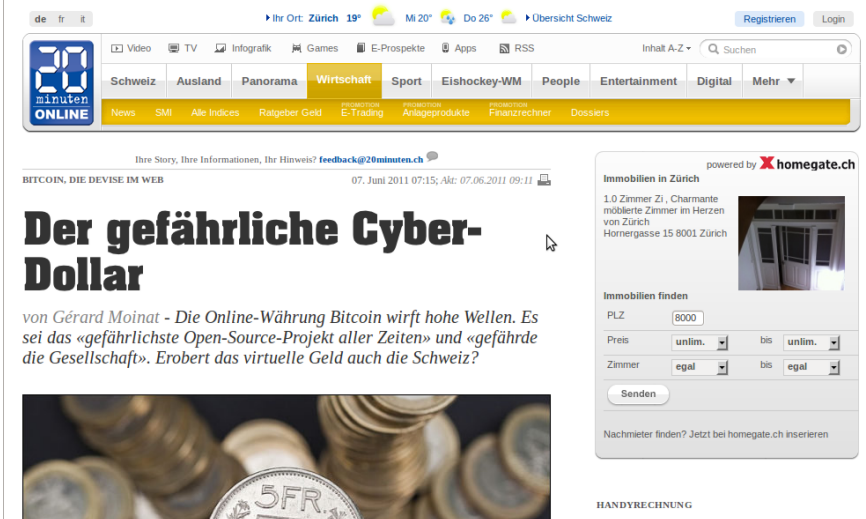
By Tom Stabile



Bitcoinista on the flip side of an exchange.

The buzz over **Bitcoin** is partly about its gall: an odd bunch of plotters aiming to build a vast community willing to trade in a digital currency free of central bank meddling. (Never mind that the favoured way to gauge its value is in good old Fed-tainted US greenbacks).

Folly or not, the new currency is an experiment in sowing trust across a yawning financial space without a supreme authority at its hub. The leap of faith is simply that, when needed, there will be another



de fr it

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

20 Minuten ONLINE

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


News SMI Alle Indices Rager Geld E-Trading Anlagensprodukte 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 die Gesellschaft». Erobert das virtuelle Geld auch die Schweiz?



Immobilien in Zürich powered by homegate.ch

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

Immobilien finden

PLZ

Preis bis

Zimmer bis

Nachmieter finden? Jetzt bei homegate.ch inserieren

HANDYRECHNUNG
EU verbilligt Roaminotarife

❖ BitCoin has seen a lot of attention in the press recently

2.1. Background

❖ BitCoin offers

- Secure accounting
 - Not relying on trust, but on strong cryptography
 - Based on an unstructured P2P network
- Weak anonymity (pseudonymity)
 - Transactions are visible to anyone
 - Identities in system are pseudonyms (public keys)
- BitCoins can be exchange for real currencies
 - Several companies allow to exchange BTC for Dollar, Euro, ...
- Currency Unit: BTC



2.1. Background

- ❖ Clients invest computing power to create coins
 - By solving cryptographic puzzles
 - Difficulty of the puzzle adapts
 - Number of coins is limited to 21 M BTC

- ❖ Public transactions for coin transfer
 - Senders and receivers have addresses
 - Authorized by private key signatures

- ❖ Honest majority prevents double spending
 - Public transaction database

2.2. Protocol

❖ Process for issuing new transactions

- 1.) New **transactions** are broadcast to all nodes
- 2.) Each node collects new transactions into a block
- 3.) Each node works on finding a difficult proof-of-work for its block
- 4.) When a node finds a proof-of-work, it broadcasts the block to all nodes
- 5.) Nodes accept the block only if all **transactions are valid** and not already spent
- 6.) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash

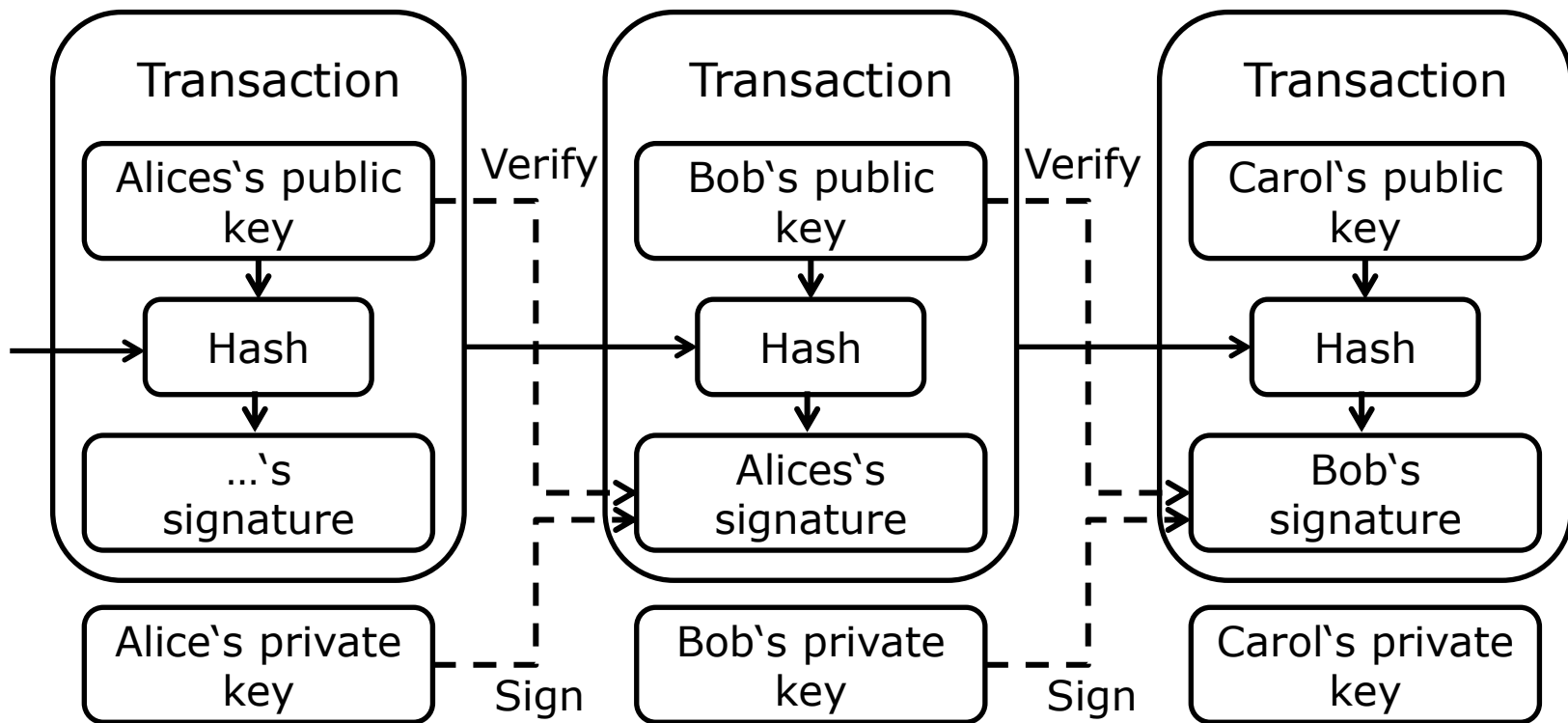
2.2. Protocol

- ❖ Client generates public/private key pairs
 - ECDSA 256 bit
 - Stores them in wallet file
- ❖ Wallet contains key pairs, not coins
 - Private key authorizes transactions
 - If keys are stolen, thief may use your coins
 - If keys are lost, coins are lost
- ❖ BitCoin address is fingerprint of public key



2.3. Transactions

- ❖ Public transfer between BitCoin addresses
 - Electronic coin is a chain of signed transactions



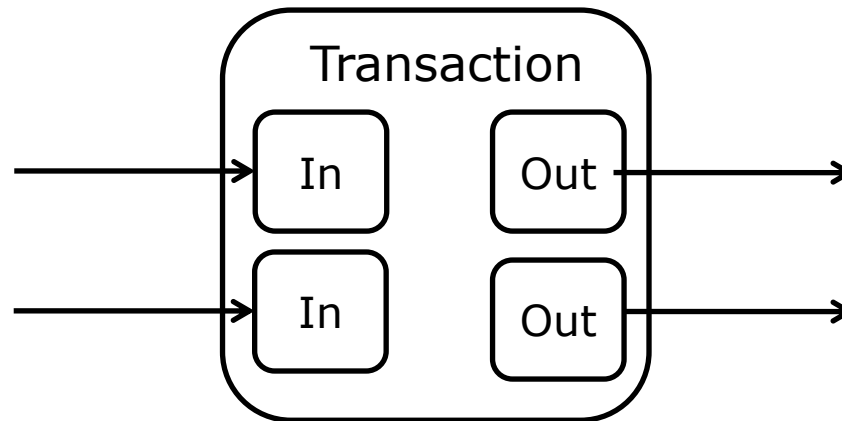
2.3. Transactions

❖ Value can be split and combined

➤ Smallest fraction: 10^{-8} BTC

➤ Usually:

- Either single input from larger previous transfer or multiple inputs combining smaller amounts
- Two outputs: one for payment, and one for returning „change“



2.3. Transactions

Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0...
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd...

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd78...
OP_EQUALVERIFY OP_CHECKSIG

Transaction of 50 BTC
with single input and
single output

- ❖ Input → marks first (and in this case only) input
- ❖ Previous tx → hash of the previous transaction
- ❖ Index → specific output of this transaction
- ❖ ScriptSig → operation codes for internal scripting engine (checks validity)
- ❖ Output → marks first (and in this case only) output
- ❖ Value → transaction value of 50 BTC
- ❖ scriptPubKey → operation codes for internal scripting engine (checks validity)

2.3. Transactions

❖ Scripting

- BitCoin clients include a Forth-Like scripting engine (stack machine)
- A transaction is valid, if and only if ...
 - scriptSig is executed
 - scriptPubKey is executed on the output of scriptSig
 - scriptPubKey yields true

❖ Allows to construct complex payments (e.g., paying peer can enforce receiver to possess several private keys)

- Basically determines validity of transaction, where „validity“ is defined on behalf the peer issuing the transaction

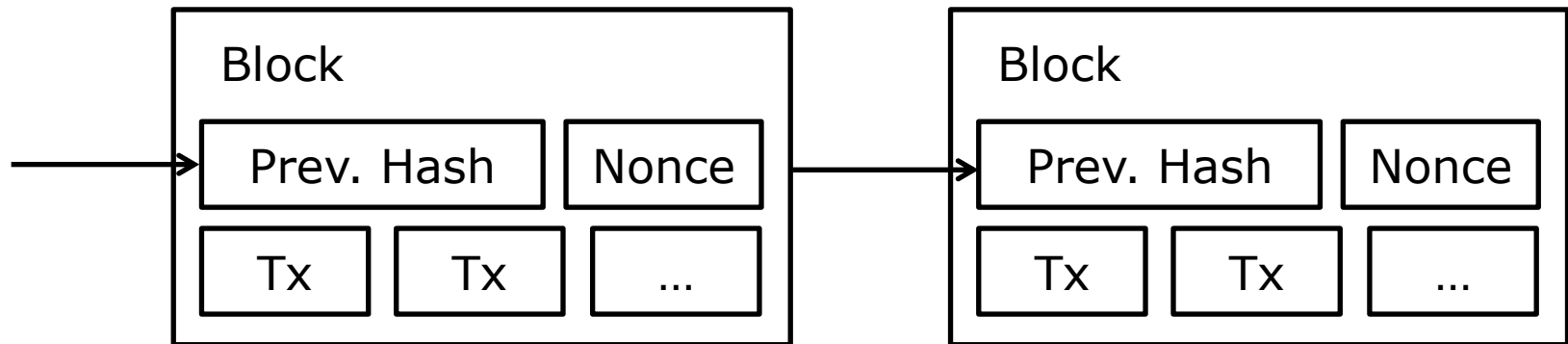
2.2. Protocol (Reprise)

❖ Process for issuing new transactions

- 1.) New transactions are broadcast to all nodes
- 2.) Each node collects new transactions into a block
- 3.) Each node works on finding a **difficult proof-of-work** for its block
- 4.) When a node finds a **proof-of-work**, it broadcasts the block to all nodes
- 5.) Nodes accept the block only if all transactions are valid and not already spent
- 6.) Nodes express their acceptance of the block by working on creating the **next block in the chain**, using the hash of the accepted block as the previous hash

2.4. Proof-of-Work

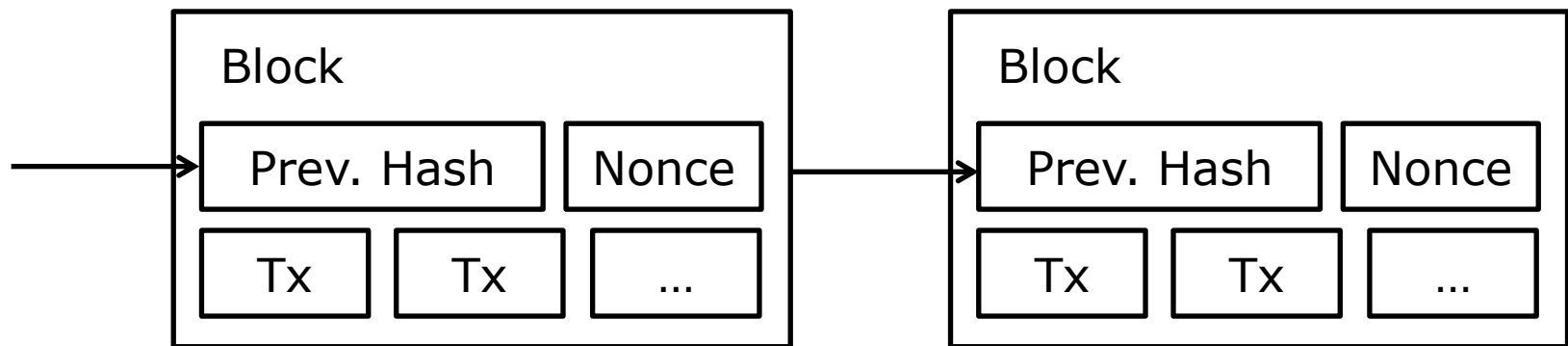
- ❖ Double spending has to be prevented
 - Transactions are verified solving a cryptographic puzzle over a number of transactions → mining
 - This is a proof that a transaction has been issued before a certain point in time
 - Double transactions are ignored in this process



2.4. Proof-of-Work

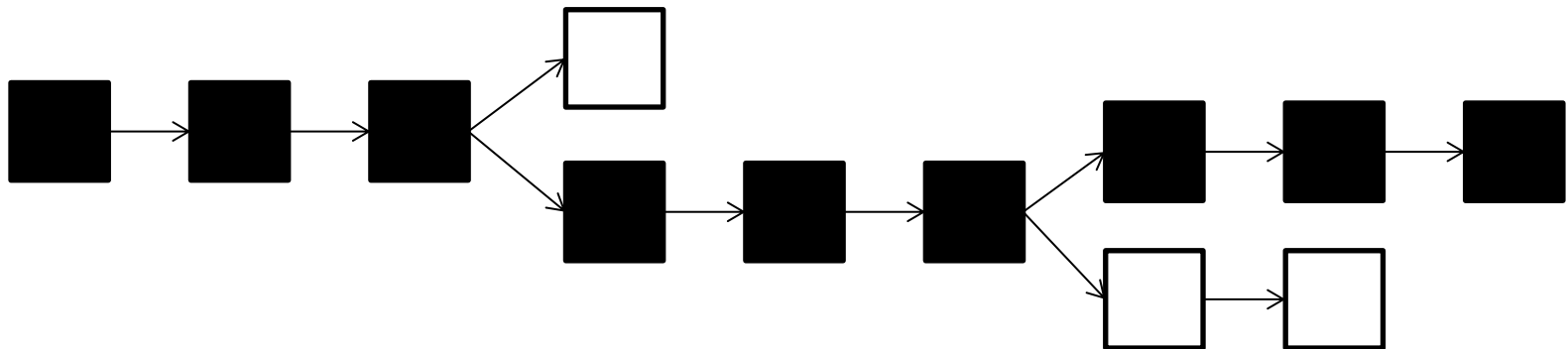
❖ Cryptographic puzzle

- Nonce is to be guessed by the peer confirming the transaction
- The puzzle is solved, if the blocks hash has a prefix of n zeros →
 $H(\text{data}, \text{nonce}) = 000000\text{bf}7834\text{ab}...$
- n determines difficulty and can be adapted



2.5. Block-Chain Split

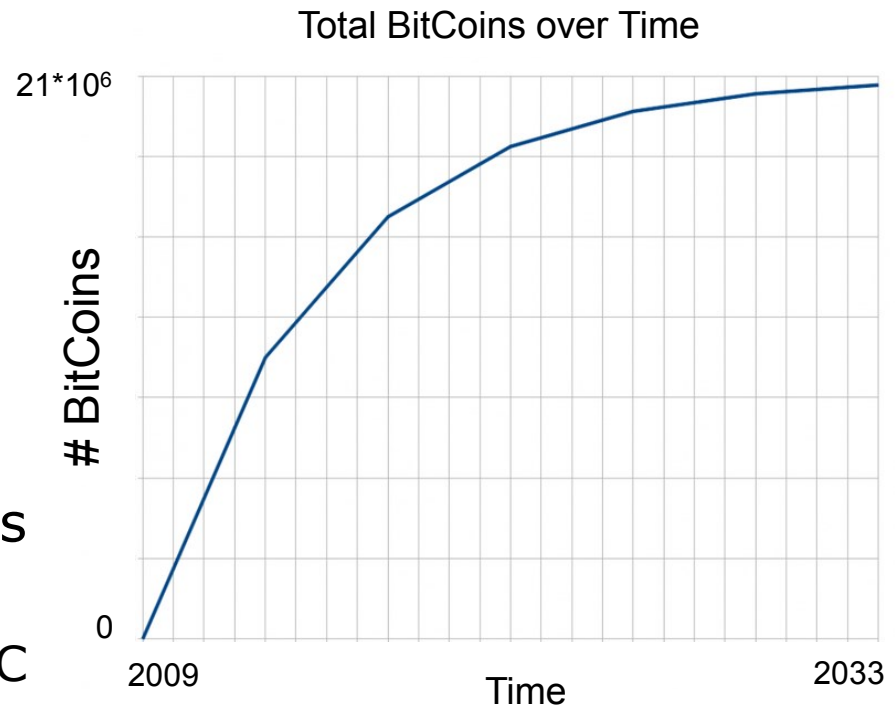
- ❖ The block chain can split up
 - Two blocks may be generated at the same time
 - The propagation delay of the two blocks may cause portions of the peers to start working on different blocks



- ❖ In this case, peers will stop working on one branch as soon as the other gets longer

2.6. Mining

- ❖ By convention, the first transaction in a block is a special transaction
 - The peer solving the block is allowed to grant himself 50 BTC
 - Halves every four years (< 1 BTC in 2033)
- ❖ The total number of Bitcoins is a geometric series
 - Upper bound: 20.7 million BTC
 - Miners also get transaction fees



2.6. Mining

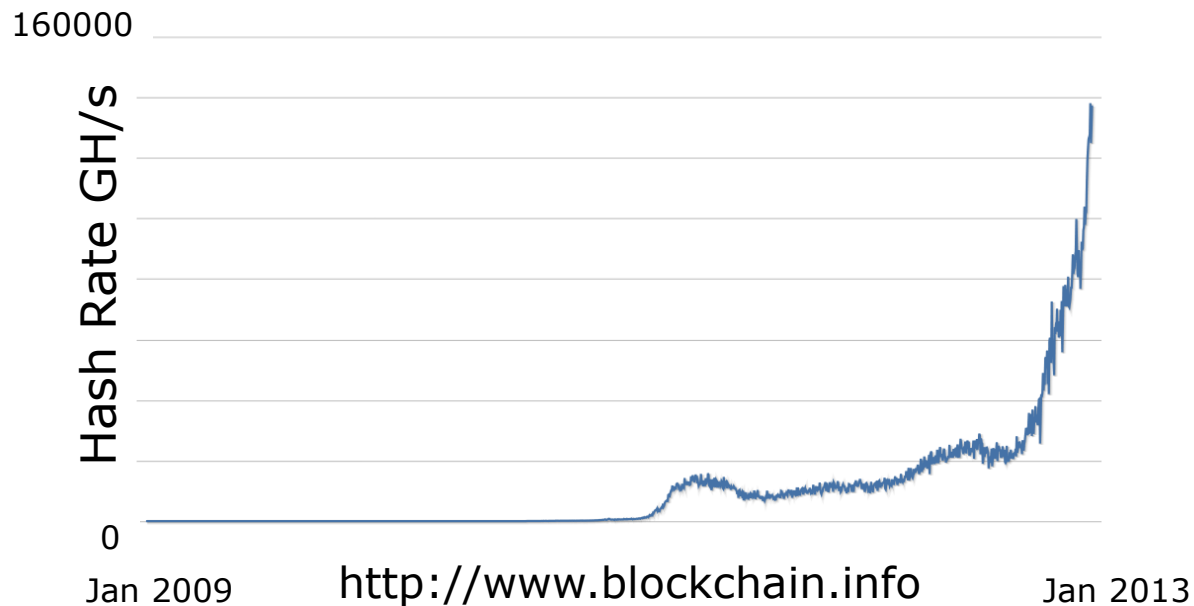
- ❖ Mining has started to get professional
 - Crucial trade-off: hash rate vs. power consumption
- ❖ GPU mining is common, CPU mining pointless
 - Expenditures for CPU mining exceed gained value
- ❖ Professional miners have started to switch to FPGAs and ASICs



Mining board with two Spartan 6 FPGAs
(<http://www.fpgamining.com/products/x6500-rev3>)

2.6. Mining

- ❖ Overall hash rate increases rapidly
 - Specialized miners using ASICs
 - E.g. Avalon and Butterflylabs

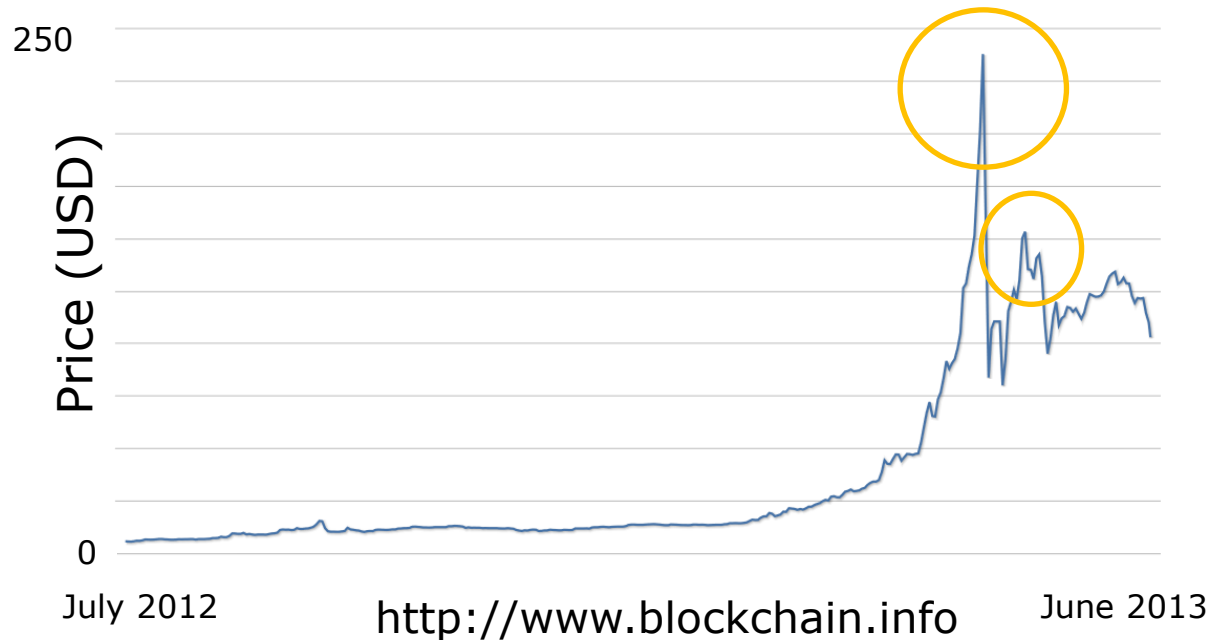


2.7. Economic Aspects

- ❖ Market capitalization $\sim 11\text{m BTC}$ / $\sim 1500\text{m USD}$
- ❖ ~ 1700 tph / $\sim 40'000$ per day
- ❖ $\sim 26'000\text{K BTC hour}$ / $\sim 0.6\text{m}$ per day
- ❖ Network Hashrate (<http://bitcoincharts.com>) ~ 900 PetaFLOPS
 - If a party can gain more than 50 % of the CPU capacity in the network, transaction can be forged
 - However, fastest supercomputer at the moment: ~ 27 PetaFLOPS

2.7. Economic Aspects

- ❖ BTC can be exchanged for physical currencies
 - The course is highly volatile (economic bubbles)
 - Security flaws have a big impact on trust in BTCs



2.8. Summary and Conclusions

❖ Advantages

- No control / fully decentralized (disadvantage?)
- Pseudonym / [Anonymity](#) (Zerocoin)
 - But exchange sites may be [regulated](#)
- 24/7 - no banking holidays
- Fully transparent
- Works for now

❖ Disadvantages

- Bitcoins not widely accepted
- Wallet can be lost
- Transaction cannot be reversed (fraud)
- Max. number of bitcoins is 21m → deflation if it becomes popular
- Transactions are broadcasted within seconds and verified within 10 to 60 minutes.

2.8. Summary and Conclusions

- ❖ Waste of processing power/electricity
 - 1.5 MHash/W (GPU!) → 105MW → ~14% of AKW Beznau
 - Energy as currency?

- ❖ Does BitCoin scale
 - Scale to VISA ~2000 transaction/s (currently ~0.5 tps)
 - Transaction size ~1kbytes -> 1.14 GB per block
 - Disk → every 21 days new 3TB harddrive

- ❖ Specialized miners ASIC
 - application-specific integrated circuit
 - [Avalon](#) 65 Ghash (1300\$)
 - [Butterflylabs](#) 60Ghash (\$2500)

2.8. Summary and Conclusions

- ❖ 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 checks, 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
 - [Storage](#): Space per unit cost has doubled roughly every 14 months

3. References

3.1. References

-
- [1] Sandvine: "Fall 2012 Global Internet Phenomena Report". Tech. Rep., 2012. <http://www.sandvine.com>, last accessed 02/11/2012.
- [2] B. Cohen: "Incentives Build Robustness in BitTorrent". Workshop on Economics of Peer-to-Peer systems, Berkeley, 2003.
- [3] A. Legout, G. Unoy-Keller, O. Michiardi: "Rarest First and Choke Algorithms are Enough". ACM SIGCOMM Conference on Internet Measurement (IMC), Rio de Janeiro, 2006.
- [4] T. Locher, P. Moor, S. Schmid, R. Wattenhofer: "Free Riding in BitTorrent is Cheap". Workshop on Hot Topics in Networks (HotNets), Irvine CA, 2006.
- [5] S. Nakamoto: "BitCoin: A Peer-to-Peer Electronic Cash System". Unpublished whitepaper, 2008. <http://bitcoin.org/bitcoin.pdf>, last accessed 09/06/2013.
-