The Environmental Cost of Bitcoin

Jörn Loviscach

FH Bielefeld
University of
Applied Sciences

Agenda

- Money and the environment
- Computational resources required for Bitcoin
- Impact per Bitcoin and per transaction
- Mining and economic behavior
- Conclusion

All URLs checked last on 2012-09-18.

Money and the Environment

Isn't that a Crazy Question?

Isn't that a Crazy Question?

How to Measure Environmental Impact

- kWh for computing
- kWh for networking
- kWh for cooling
- tons of e-waste (also indicates impact of hardware production)
- plus minor factors
- compare to known quantities

Cowry Shells: Sustainable Money

- Ancient Chinese currency 貝
- Used in Africa even today

Gold Mining:
Harm for Humans and Nature

- Developing countries: intolerable working conditions, child labor www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/documents/publication/wcms_bk_pb_123_en.pdf
- Open pit mines: deforestation
- Waste rock removal
- Chemicals: cyanides, mercury
  Baia Mare, Romania, 2000: dam break; estimated 100 tons of cyanides released into rivers http://news.bbc.co.uk/2/hi/science/nature/4083331.stm#romania
- Smeltering: air pollution

Bank Notes: Lifecycle Assessment

- Approx. 4 MJ *total* energy usage
  per bank note for a livespan of three years
  http://www.bankofcanada.ca/banknotes/bank-note-series/polymer/life-cycle-assessment-lca/
- Euro: 14 billions of banknotes
  http://www.ecb.int/euro/banknotes/circulation/html/index.de.html
- Rough estimate: approx. 5 TWh per year
- For comparison:
  total use of electric energy in Germany
  approx. 600 TWh in the year 2010

Electronic Transactions: Just Flipping some Bits?

- Example: 5.3 MW (IT: 3.3 MW) for 66 million accounts http://pamina-business.karlsruhe.de/upload/mediapool/FiduciaBatzler.pdf
- That's a major part of all German accounts www.bankenverband.de/downloads/102009/ta0910-rb-girokonten.pdf
- Compare with 70 GW average consumption of electric power in Germany

High-Speed Trading: Expensive Millisecs

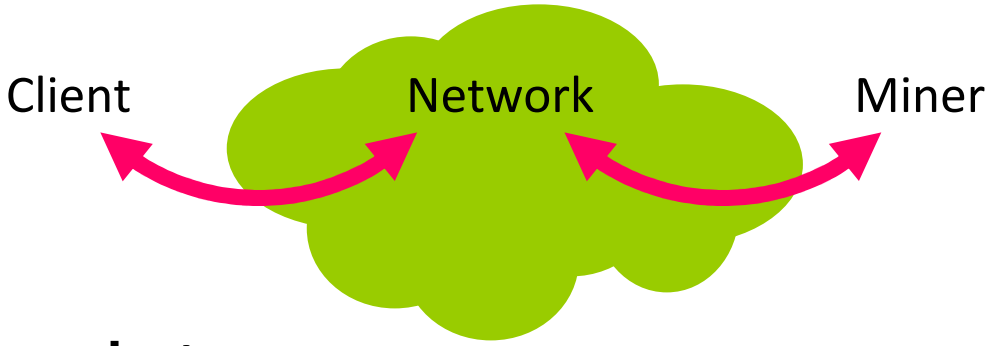
- NYSE Mahwah datacenter:
  $70 billion transactions per day
  http://spectrum.ieee.org/computing/networks/the-microsecond-market/0
  power consumption of 28 MW
  www.wallstreetandtech.com/data-management/226300061?pgno=1
- Three trans-arctic optic cables to link Japan and the UK, $300 million to $1.5 billion each, reducing the latency from 230 to 170 ms
  www.extremetech.com/extreme/
  122989-1-5-billion-the-cost-of-cutting-london-toyko-latency-by-60ms

What about Bitcoin?

Try to get some ballpark estimates!

Computational Resources Required for Bitcoin

Contributions to Examine



- Moore's law
- Clients and network: dwindling costs
- Clients and network: only additional use of existing resources; little specific e-waste
- Difficulty is increasing:
  mining remains expensive

Choice of Hardware

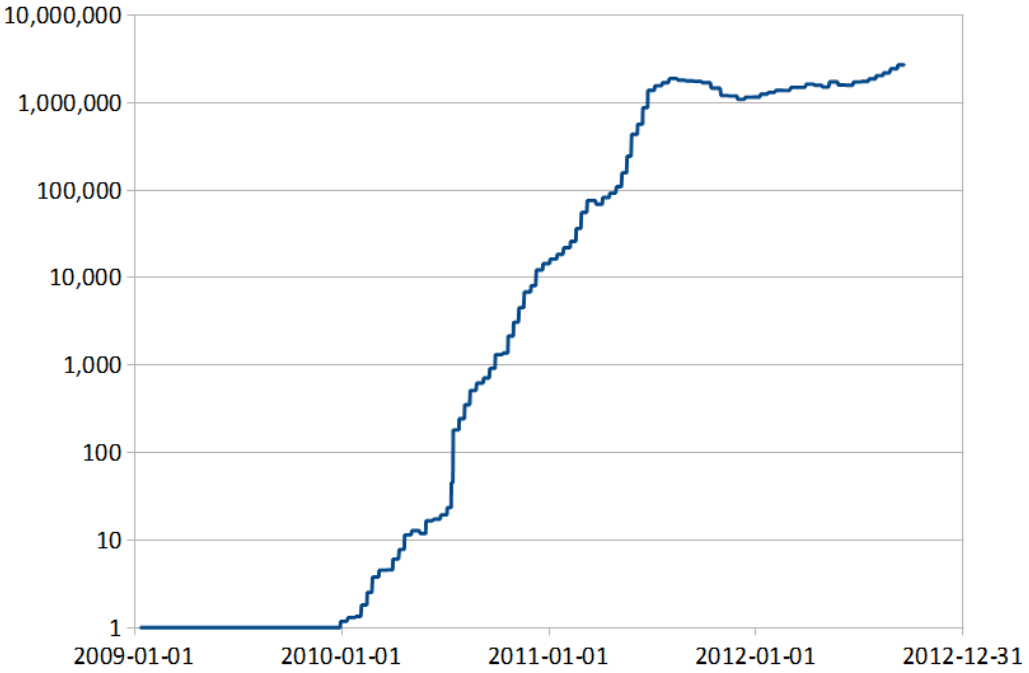
	Intel Core i7	Triple AMD Radeon HD 7970	BitForce MiniRig
GHash/s	0.008…0.02	2	25
Watts	100…150	850	1,250
Hash/kWh	$2…7 \cdot 10^{11}$	$8 \cdot 10^{12}$	$7 \cdot 10^{13}$
E-Waste	None additional if mining in background	10 kg/a for staying up to date	20 kg/a for staying up to date

https://en.bitcoin.it/wiki/Mining_hardware_comparison
http://www.butterflylabs.com/products/

Impact per Bitcoin and per Transaction

Hashes per Block

- Difficulty adapts to performance
  data from http://blockexplorer.com/q/nethash
- Difficulty = 1: 2^{224} out of 2^{256}
- September 2012:
  - Difficulty = approx. 2,700,000
  - Average number of hashes required to solve a block: $1.2 \cdot 10^{16}$



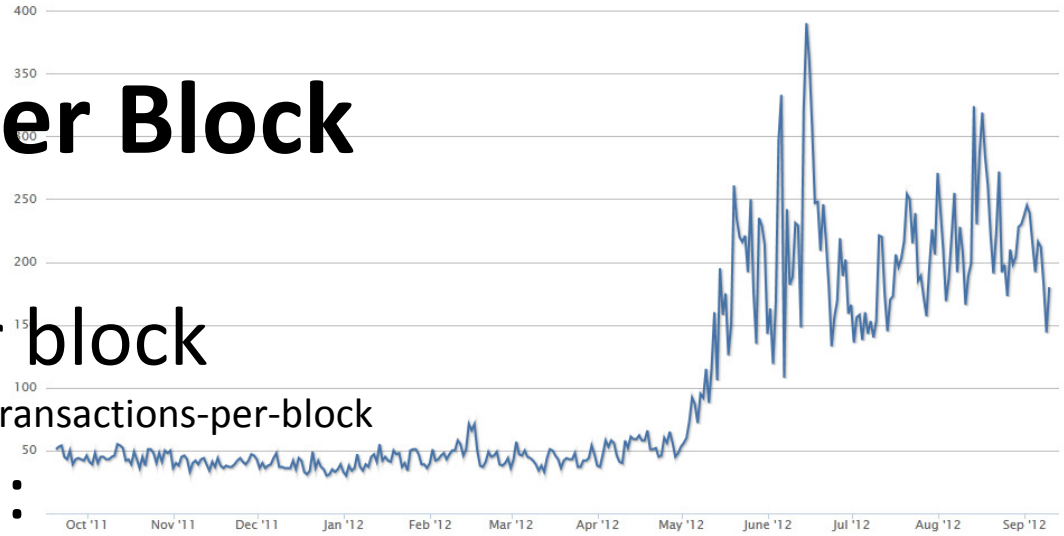
Energy Content of one Bitcoin

- BTC 50 per solved block,
  down to BTC 25 this December
- 2.3 or $4.6 \cdot 10^{14}$ hash/BTC
- 29 or 57 kWh/BTC for GPU ($8 \cdot 10^{12}$ Hash/kWh),
  up to 10x more for PC,
  up to 10x less for dedicated hardware
- **BTC 1 million** on GPUs = 29 or 57 GWh
  = **25 or 50 minutes of electric power for Germany**

E-Waste for one Bitcoin

- Run a GPU miner 24/7
- 2 GHash/s / 2.3…4.6·10^{14} Hash/BTC
  = 4…9 µBTC/s = 140…270 BTC/a
- E-waste: 10 kg/a / 140…270 BTC/a
  = **37…71 g/BTC**
- Gross comparison: bank note = 1 g

Transactions per Block



- Transactions per block
  http://blockchain.info/charts/n-transactions-per-block
  September 2012:
  150…300 transactions/block
- $1.2 \cdot 10^{16}$ Hash/block
  / 150…300 transactions/block
  = $4…8 \cdot 10^{13}$ Hash/transaction
- Some room for growth:
  Typical size of transaction: 300…500 bytes
  Fee increases steeply after a block size of 250 kB

Energy Consumption for Transactions

- GPU: $4…8 \cdot 10^{13}$ Hash/transaction
  / $8 \cdot 10^{12}$ Hash/kWh = 5…10 kWh/transaction,
  10x more for PC,
  10x less for dedicated hardware
- Germany: 17 billion transactions in 2010
  https://www.bankenverband.de/publikationen/ods/die-privaten-banken-fakten-und-zahlen/die-privaten-banken-fakten-und-zahlen/download
  which would be **85…170 TWh**
- One year of electric power for Germany:
  600 TWh

Mining and Economic Behavior

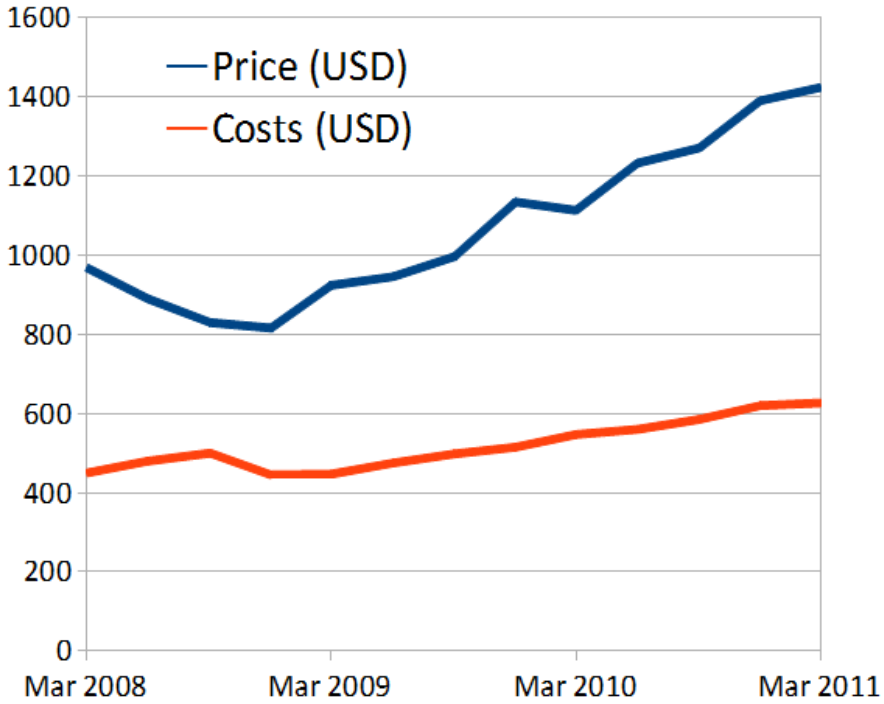
Similarity to Gold

- Decentralized anonymous proof of work?!
- Costs and price of 1 oz of gold

  data adapted from www.virtualmetals.co.uk/pdf/ABNGCQ111.pdf and www.indexmundi.com/commodities/?commodity=gold&months=60
- Naive economics:

  price > cost: mine!

  price < cost: don't!



Price and Cost of Bitcoin

- GPU mining:
  10…20 ¢/kWh · 29…57 kWh/BTC
  = 2.9…11.4 US$/BTC
- Exchange rate (Sep 2012):
  BTC 1 = US$ 12
- Similar market effect as with gold?
- **Energy content and hence environmental impact remain substantial through economic behavior**

Conclusion

Bitcoin = Digital Gold

- We seemingly can't get the benefits:
  - Decentralization
  - Anonymization
- Without the issues:
  - Waste of resources, in particular energy
  - Pollution through energy production and hardware production/disposal

Research Questions

- Can there be a proof-of-work concept that is environmentally friendly?
- Or even meaningful? (Search queries? Folded proteins? Social work?)
- Reduce the number of transactions: Could Bitcoin back another, less costly digital currency?

Questions?

joern.loviscach@fh-bielefeld.de

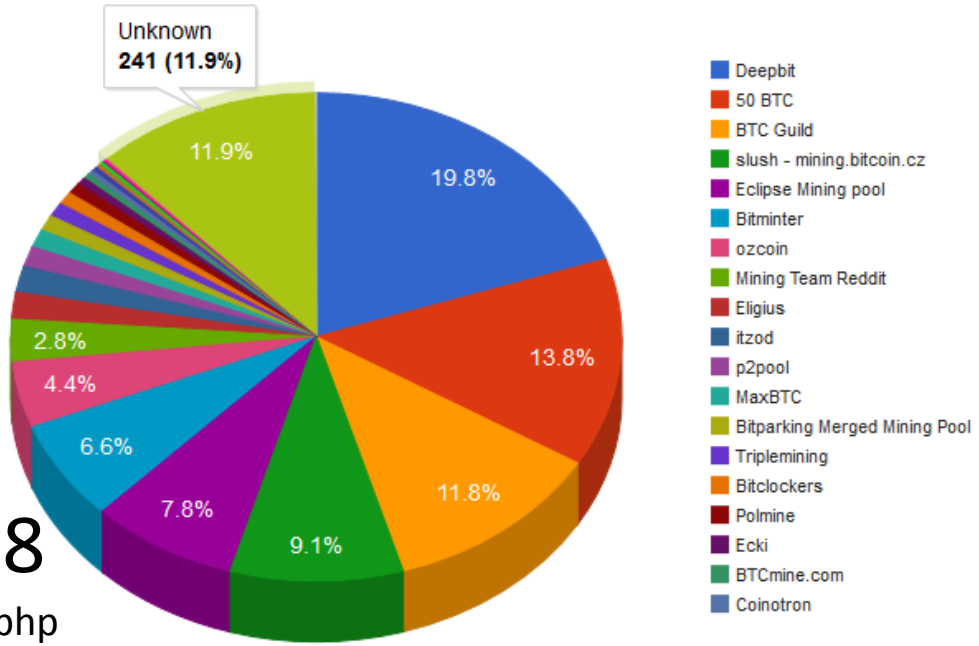
Mining Pools vs. Individuals

Jörn Loviscach

FH Bielefeld
University of
Applied Sciences

Why Pool?

- "Solo" mining with a standard PC:
  40 years to first solved block
- Pool the workforce, share the reward:
  smooth flow of income



- Hash rates
  2012-09-05 to -18
  http://blockorigin.pfoe.be/chart.php

Measuring the Effort

- Unit of measurement:
  one share
  = a solution for difficulty 1 (typically)
- Frequent proof of smaller work:
  2,700,000 times more likely than solution
- Hard to fake
- Good measure of contributed computational power

Proportional Reward

- Split the reward in proportion to the number of shares in the round
- Encourages pool hopping or switching to solo mining

http://bitcoin.atspace.com/poolcheating.pdf

A	B	C
0	1/2	1/3
1/4	2/5	2/6
2/7	3/8	3/9
3/10	4/11	4/12

A	B	C
0	1/2	1/3
1/4	2/5	2/6
2/7	Solo 1	2/8
2/9	Solo 1	2/10

Fraction earned by B

Pay per Share

- Immediately pay expected reward per share
- Pool hopping not encouraged
- Risk for pool operator:
  variance
- Higher fee

Further Reward Systems

- Pay per Last N Shares:
  - Split the reward in proportion to the effort in the preceding N shares (possibly including an earlier block)
  - Keeps everybody working, not hopping
  - No risk (like PPS) for pool operator
- Geometric Method:
  geometrically increasing score for each share
- And many more

https://bitcoil.co.il/pool_analysis.pdf

Further Issues with Pooling

- Fees (some percent)
- Pool can be target of DoS attacks
- Stale shares:
  Block is already solved elsewhere,
  but nobody told us so far
- Withhold a solution from the pool
  and submit it solo?
  Won’t work:
  50 BTC payment to pool is part of that block.

Questions?

joern.loviscach@fh-bielefeld.de