ERCIS
European
Research
Center for
Information
Systems

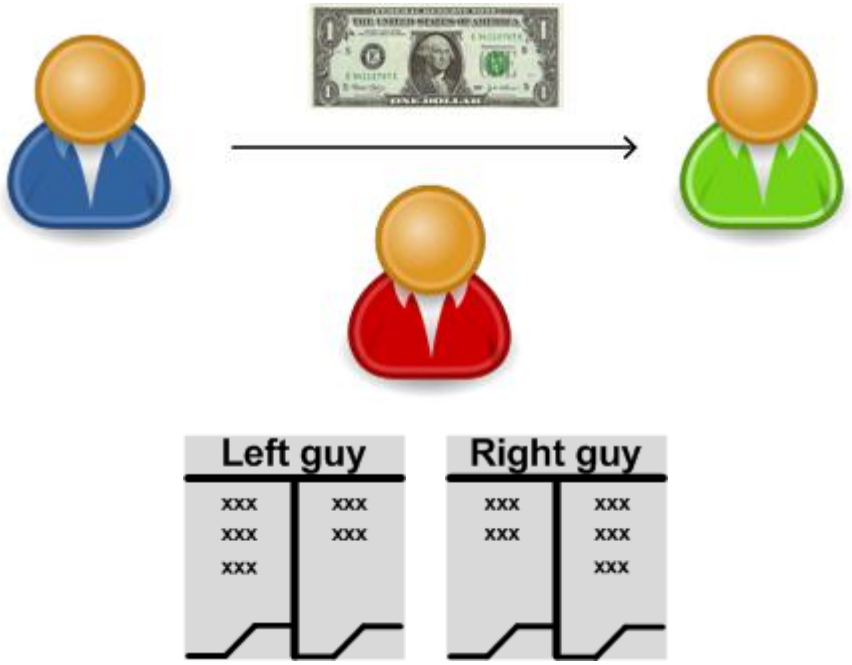
Can we Afford Integrity by Proof-of-Work?

Scenarios Inspired by the Bitcoin Currency

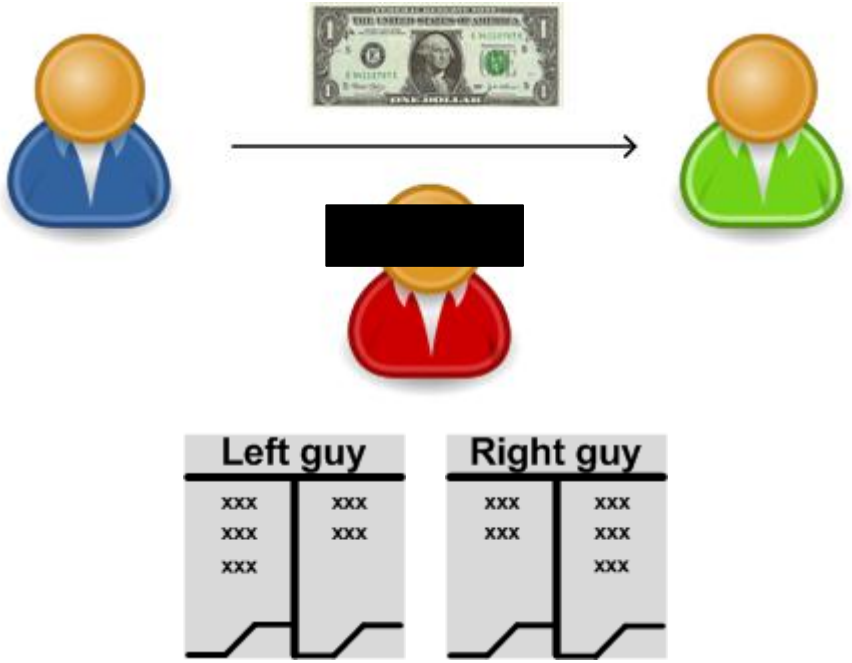
Jörg Becker, Dominic Breuker, Tobias Heide, Justus Holler, Hans Peter Rauer, Rainer Böhme

Westfälische Wilhelms-Universität Münster

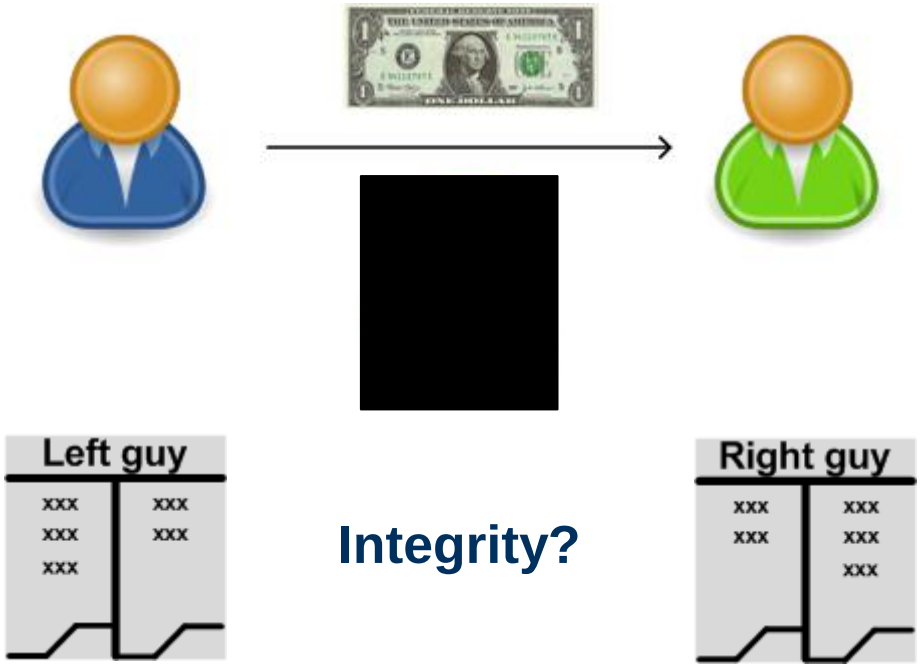
Electronic cash



Cryptographic cash



Cryptographic currency



Why Bitcoin?

- "Such a system has several disadvantages: It is costly. …" [Bitcoin Wiki about the banking system] https://en.bitcoin.it/wiki/Introduction
- "… they are taking up to 5% off of every transaction…" [Rick Falkvinge about banks – European Bitcoin Conference] http://www.youtube.com/watch?v=mjmuPqkVwWc
- "Transaction costs are also likely to be lower than those for traditional payment systems, …" [The Economist, Jun 13th 2011] http://www.economist.com/blogs/babbage/2011/06/virtual-currency

Research questions

- "How much transaction costs could be saved?"
- "What would be the environmental impact?"

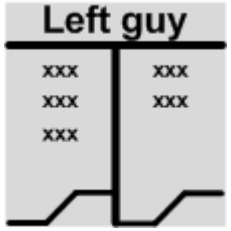
Agenda

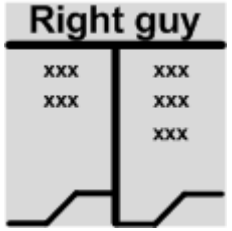
1 How Bitcoin works

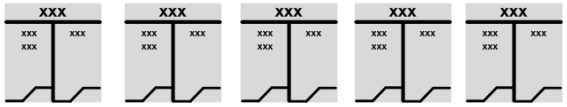
2 The cost of Bitcoin-like currencies

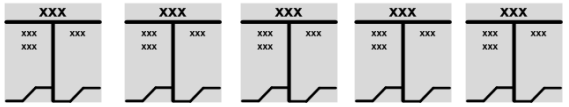
3 Outlook

Global state replication

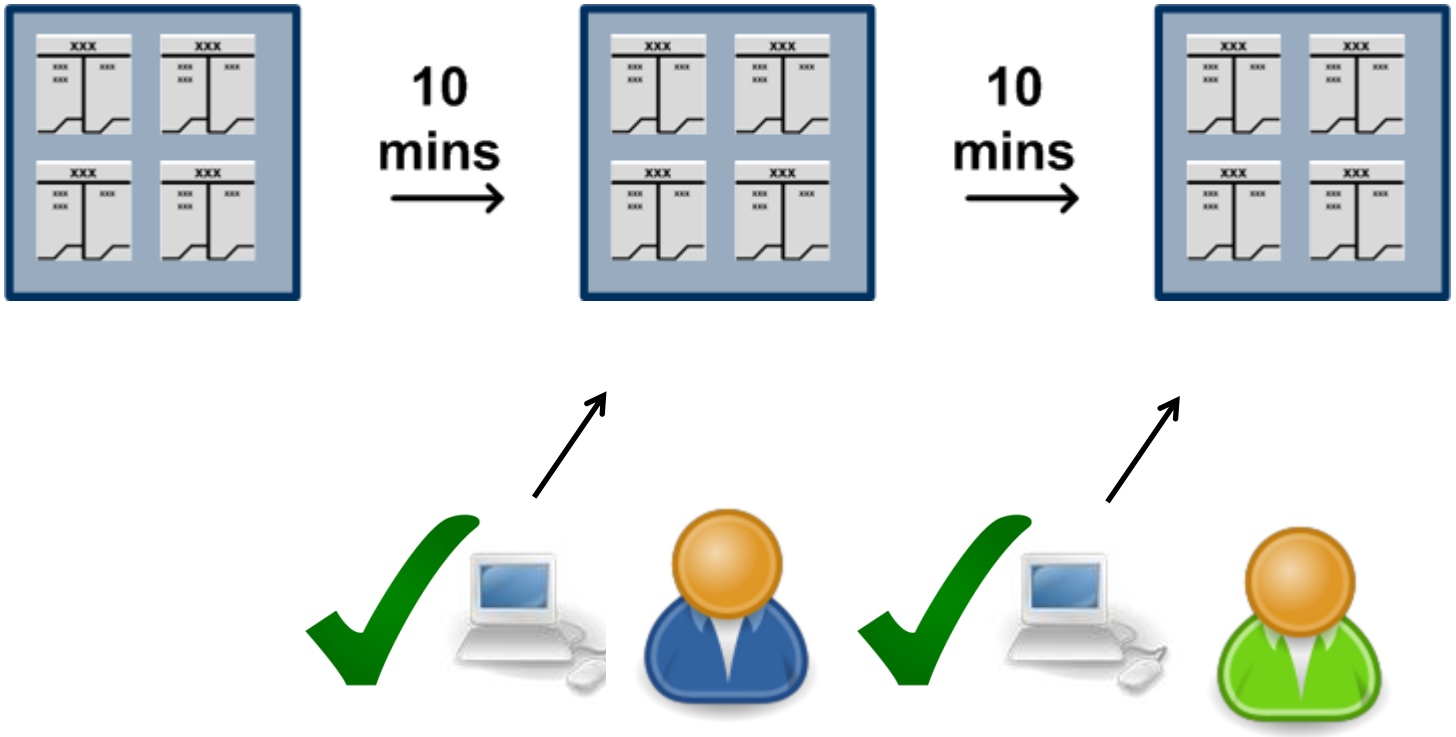




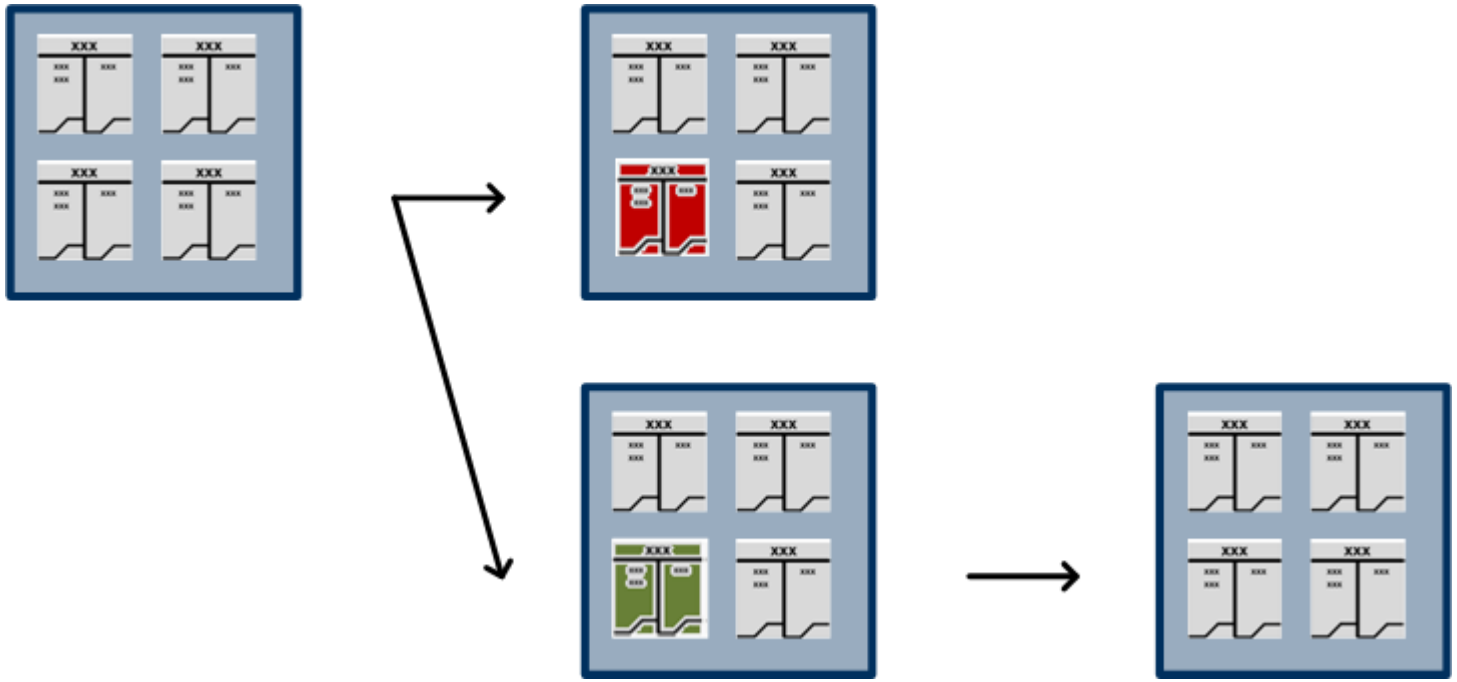




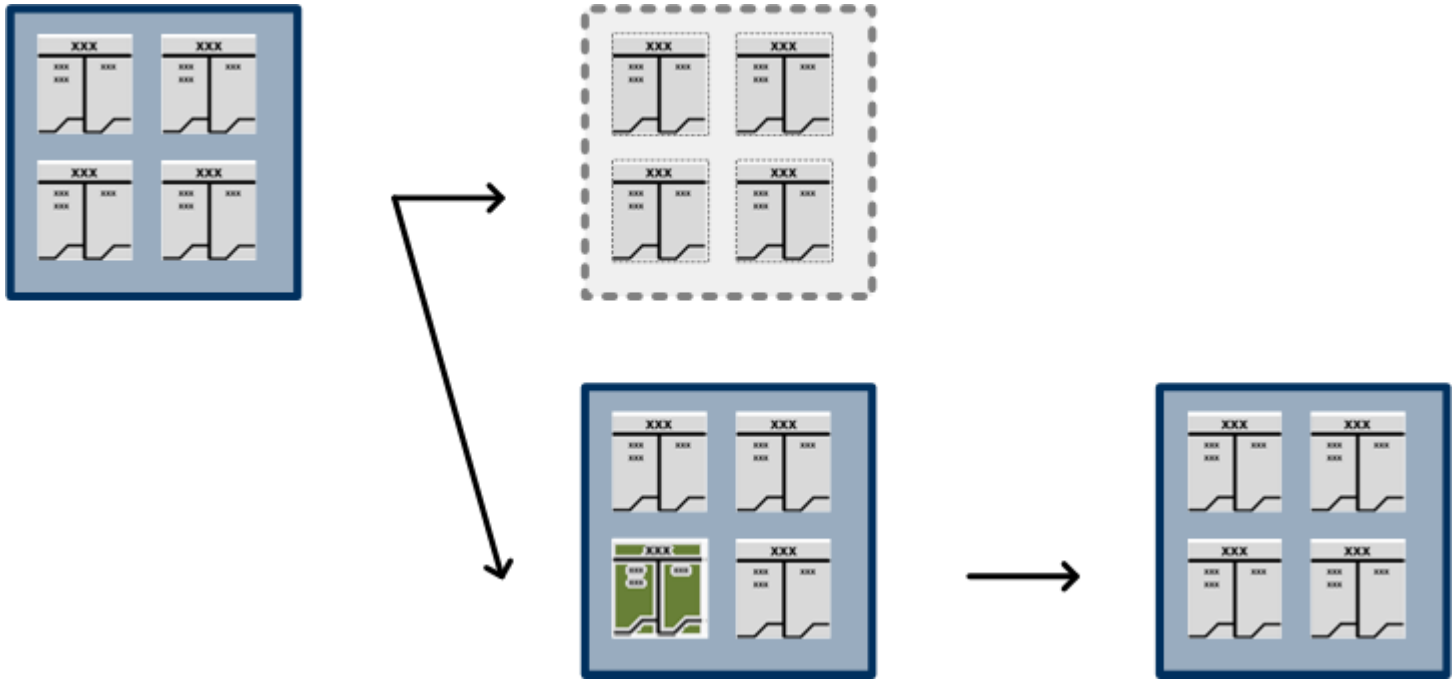
Block chain: Proof-of-Work (PoW)



Block chain: conflict resolution



Block chain: conflict resolution



To attack, you have to control 50% of the network's computing power

Agenda

1 How Bitcoin works

2 The cost of Bitcoin-like currencies

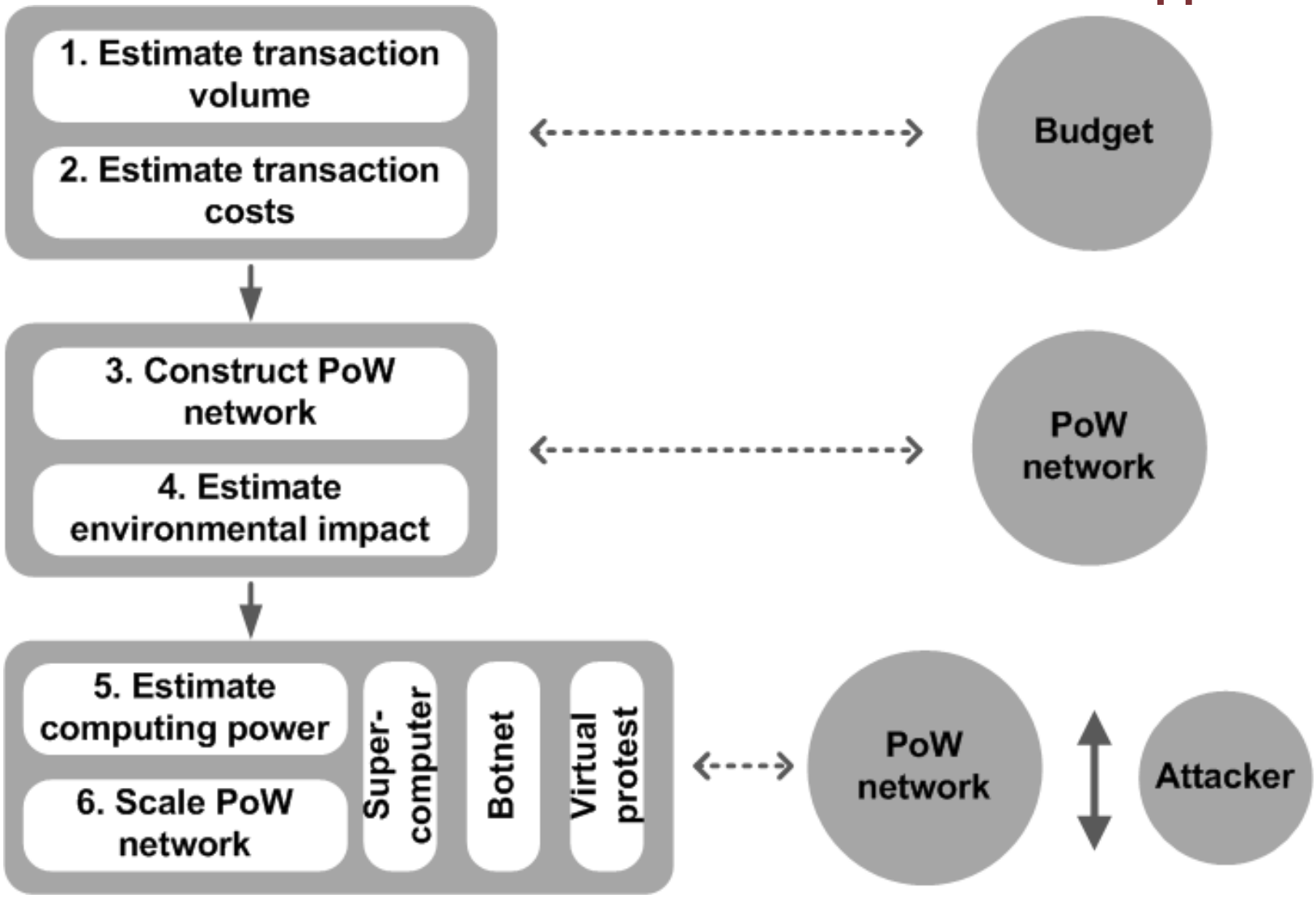
3 Outlook

Comparison of two scenarios

PoW-based currency

Financial intermediation

Approach


1. Estimate transaction volume
2. Estimate transaction costs
Budget
3. Construct PoW network
4. Estimate environmental impact
PoW network
5. Estimate computing power
6. Scale PoW network
Super-computer
Botnet
Virtual protest
PoW network
Attacker

Estimating a budget (1+2)

Transaction volume	*	Transaction fee	=	Transaction cost
9.44E+13 [USD]		0.3%		2.83E+11 [USD]

- Global volume in 2010
- Includes all „small scale transactions“

- Debit card system of Germany
- Fixed cost ignored (~8 Cent minimum)

[Bank for International Settlements – 2011]

[EURO Kartensysteme GmbH – 2008]

Constructing the PoW network (3)

Dollar budget	*	Fraction of electricity cost	=	Electricity budget
2.83E+11 [USD]		30%		8.49E+10 [USD]

- Typical cost structure of data centers
- Other cost are ignored from now on

[Belady – 2007]

Constructing the PoW network (3)

Electricity budget	/	Electricity price	*	Energy-efficiency	=>	Computing power
8.49E+10 [USD]		0.1 [USD/kWh]		1.82E+08 [Ops/Ws]		1.76E+19 [Ops/s]

- Price in Russia
- Smallest among all major countries

[Mosenergosbyt – 2012]

- Median of Green500 Supercomputers
- Measured in FLOPS

[Green500.org – 2012]

Estimating environmental impact (4)

Electricity budget	/	Electricity price	*	Emission rate	=	CO2 emissions
8.49E+10 [USD]		0.1 [USD/kWh]		1.99E+-7 [kg/Ws]		6.10E+11 [kg]

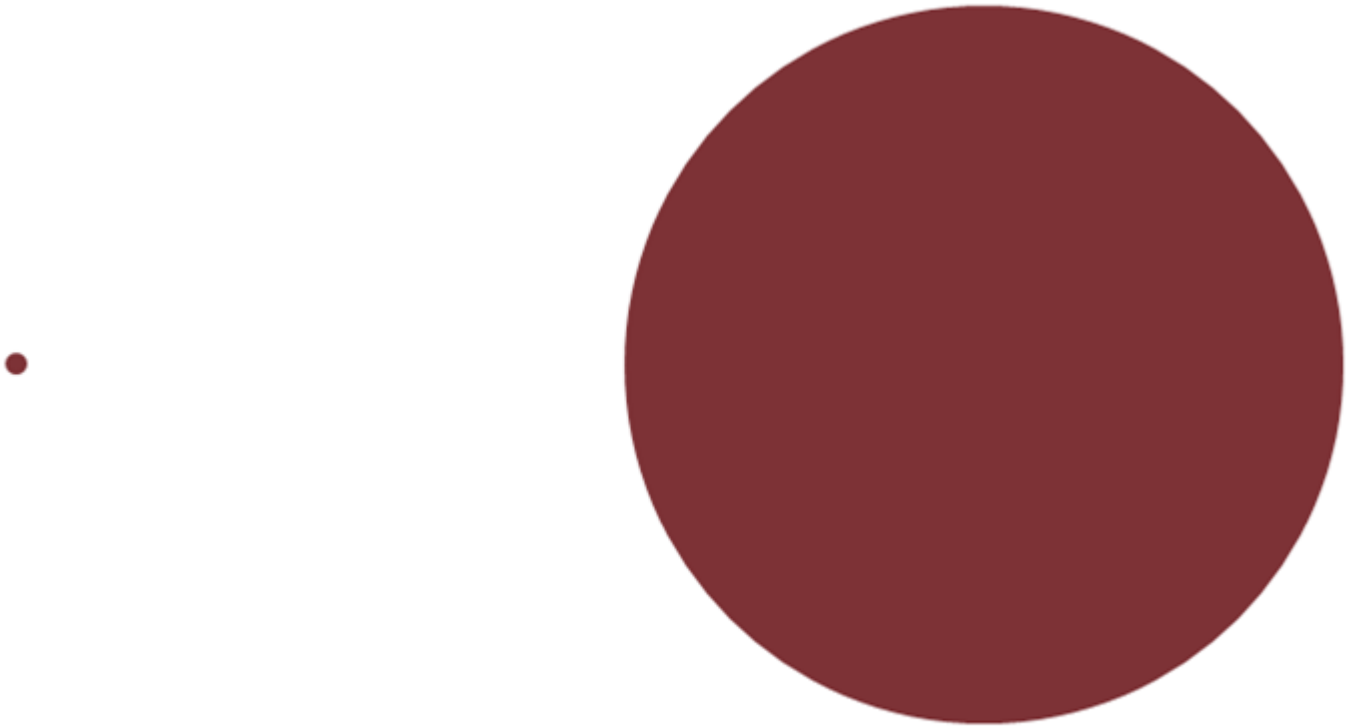
- Average over all energy carriers
- Weighted by energy carrier importance

[Lübbert – 2007]
[IEA – 2012]

- 2.1 % increase of global emissions
- About the share of global commercial air traffic

[IEA – 2011]

Attack 1: Supercomputer

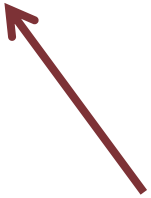


Sequoia Supercomputer
1.63E+16 [Ops/s]

PoW network
1.76E+19 [Ops/s]

Size of botnet	*	Computing power of bot	=	Computing power
3.00E+07		1.23E+10 [Ops/s]		3.70E+17 [Ops/s]

- Largest botnet ever seen (BredoLab)

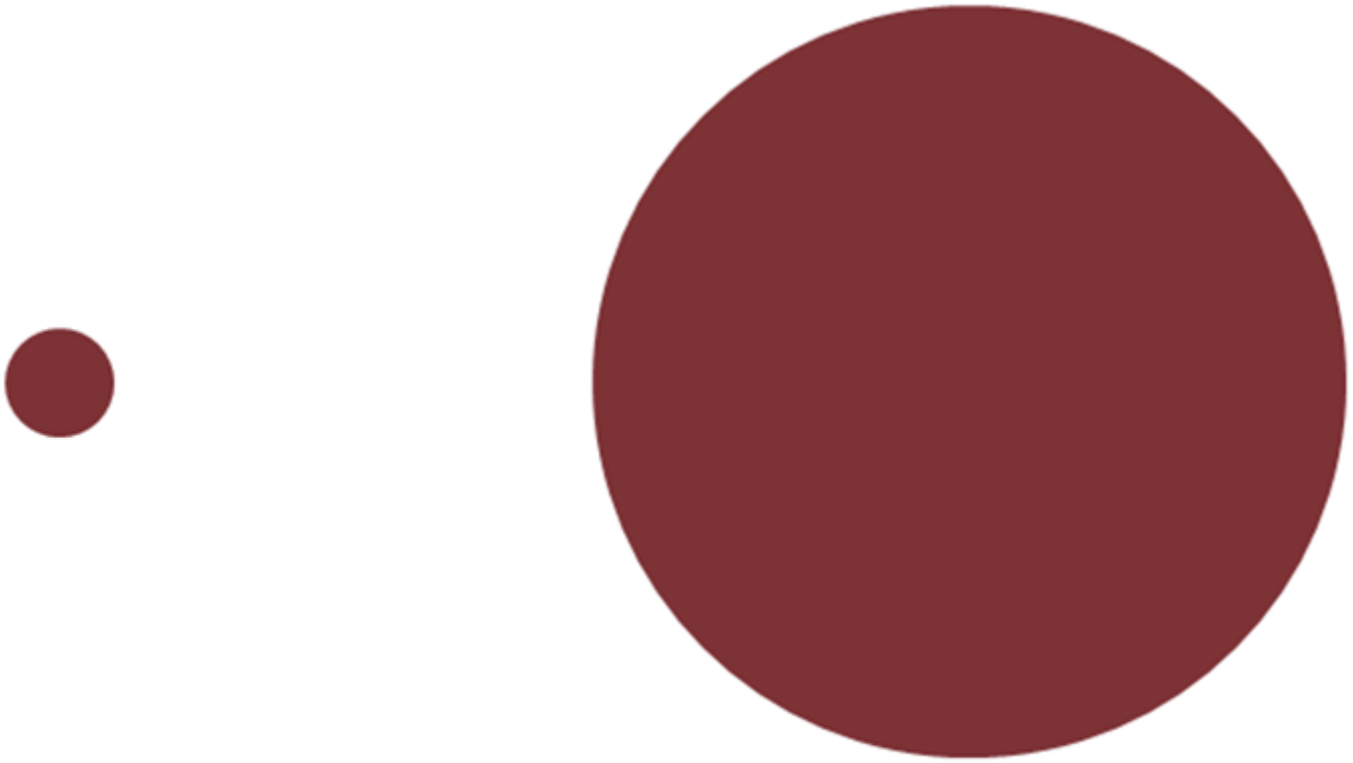


- Based on participants of BOINC
- Average contribution per user

[Wikipedia – 2012: Botnet]

[Boincstats.com – 2012]

Attack 2: Botnet



Botnet
3.70E+17 [Ops/s]

PoW network
1.76E+19 [Ops/s]

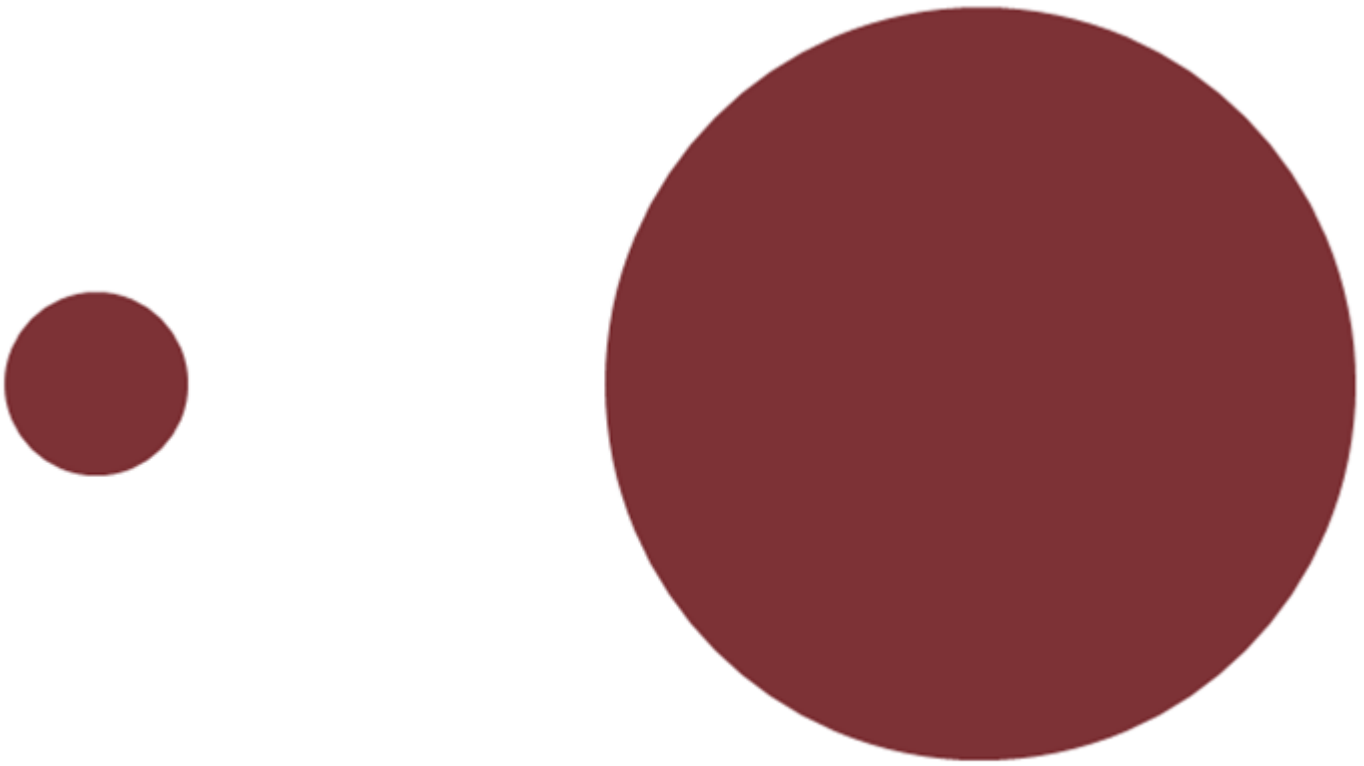
Attack 3: Virtual protest

Number of protestors	*	Computing power of protestor	=	Computing power
8.45E+08		1.23E+10 [Ops/s]		1.04E+18 [Ops/s]

- 10% of all Facebook users
- Again, based on participants of BOINC

[Facebook – 2012]

Attack 3: Virtual protest



„Occupy Bitcoin“
1.04E+18 [Ops/s]

PoW network
1.76E+19 [Ops/s]

Agenda

1 How Bitcoin works

2 The cost of Bitcoin-like currencies

3 Outlook

Cost of PoW-based, decentralized currencies

- Security constantly requires enormous compute power
- For virtual protest, systems are only one order of magnitude apart
- Cost saving potential is not proven beyond doubt
- Environmental impact could be significant on a global level

Limitations

- “Upper bound” estimation (global usage, no communication cost, …)
- Interest in solving PoW tasks would trigger innovation
- FLOPS are a bad performance measure for hash operations

Future developments might change the picture completely

- Recycle results: computations might deliver useful results as a byproduct (instead of a hash with leading zeros)
- Recycle electricity: computations generate heat, which could be reused for other purposes
- Extend scope: a PoW-based timestamping service could also serve other purposes

[Clark & Essex – 2012: CommitCoin]

References 1/2

- Bank for International Settlements. (2011). Statistics on payment, clearing and settlement systems in the CPSS countries - Figures for 2010. Retrieved from http://www.bis.org/publ/cpss99.htm
- EURO Kartensysteme GmbH. (2008). Händlerbedingungen - Bedingungen für die Teilnahme am electronic cash-System der deutschen Kreditwirtschaft. Retrieved from http://www.electronic-cash.de/media/pdf/haendlerbedingungen.pdf
- Belady, C. L. (2007). In the data center, power and cooling costs more than the it equipment it support. *Electronics Cooling*, *13*(1), 24-27.
- Mosenergosbyt. (2012). Electricity tariffs for the population of the city of Moscow in 2012. Retrieved February 22, 2012, from http://www.mosenergosbyt.ru/portal/page/portal/site/personal/tarif/msk
- Green500.org. (2012). Green500. Retrieved from http://www.green500.org/
- Lübbert, D. (2007). *CO2-Bilanzen verschiedener Energieträger im Vergleich - Zur Klimafreundlichkeit von fossilen Energien, Kernenergie und erneuerbaren Energien*. Retrieved from http://www.bundestag.de/dokumente/analysen/2007/CO2-Bilanzen_verschiedener_Energietraeger_im_Vergleich.pdf

References 2/2

- IEA. (2012). Electricity/Heat in World in 2009. Retrieved February 15, 2012, from http://www.iea.org/stats/electricitydata.asp?COUNTRY_CODE=29
- IEA. (2011). *CO2 Emissions from Fuel Combustion 2011*. Retrieved from http://www.iea.org/co2highlights/co2highlights.pdf
- Wikipedia. (2012). Botnet. Retrieved February 22, 2012, b from http://en.wikipedia.org/wiki/Botnet#cite_note-19
- Boincstats.com. (2012). BOINC Combined Project Statistics. Retrieved February 16, 2012, from http://boincstats.com/stats/project_graph.php?pr=bo
- Facebook. (2012). Fact Sheet. Retrieved February 22, 2012, from http://newsroom.fb.com/content/default.aspx?NewsAreaId=22
- Clark, J., & Essex, A. (2012). CommitCoin: Carbon Dating Commitments with Bitcoin. *16th International Conference on Financial Cryptography and Data Security*. Bonaire, Caribbean Netherlands.