Can we Afford Integrity by Proof-of-Work?

Scenarios Inspired by the Bitcoin Currency
Can we Afford Integrity by Proof-of-Work?

Motivation

Electronic cash
Cryptographic cash

Motivation
Can we Afford Integrity by Proof-of-Work?

Cryptographic currency

Integrity?
Why Bitcoin?

- “Such a system has several disadvantages: It is costly. …”
  [Bitcoin Wiki about the banking system]
- “… they are taking up to 5% off of every transaction…”
  [Rick Falkvinge about banks – European Bitcoin Conference]
- “Transaction costs are also likely to be lower than those for traditional payment systems, …”
  [The Economist, Jun 13th 2011]

Research questions

- “How much transaction costs could be saved?”
- “What would be the environmental impact?”
Can we Afford Integrity by Proof-of-Work?

Jörg Becker, Dominic Breuker, Tobias Heide, Justus Holler, Hans Peter Rauer, Rainer Böhme
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.
Can we Afford Integrity by Proof-of-Work?

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

Agenda

1. How Bitcoin works
2. The cost of Bitcoin-like currencies
3. Outlook
Comparison of two scenarios

PoW-based currency

Financial intermediation
Can we Afford Integrity by Proof-of-Work?

Jörg Becker, Dominic Breuker, Tobias Heide, Justus Holler, Hans Peter Rauer, Rainer Böhme
Can we Afford Integrity by Proof-of-Work?

Transacting 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)

Constructing the PoW network (3)

Dollar budget \times \text{Fraction of electricity cost} = \text{Electricity budget}

2.83E+11 [USD] \times 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)

<table>
<thead>
<tr>
<th>Electricity budget</th>
<th>Electricity price</th>
<th>Energy-efficiency</th>
<th>Computing power</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.49E+10 [USD]</td>
<td>0.1 USD/kWh</td>
<td>1.82E+08 [Ops/Ws]</td>
<td>1.76E+19 [Ops/s]</td>
</tr>
</tbody>
</table>

- Price in Russia
- Smallest among all major countries
- Median of Green500 Supercomputers
- Measured in FLOPS

---

- [Mosenergosbyt – 2012]
- [Green500.org – 2012]
Estimating environmental impact (4)

<table>
<thead>
<tr>
<th>Electricity budget</th>
<th>Electricity price</th>
<th>Emission rate</th>
<th>CO2 emissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.49E+10 [USD]</td>
<td>0.1 [USD/kWh]</td>
<td>1.99E-7 [kg/Ws]</td>
<td>6.10E+11 [kg]</td>
</tr>
</tbody>
</table>

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

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

[Lübbert – 2007]
[IEA – 2012]

[IEA – 2011]
Can we Afford Integrity by Proof-of-Work?

Sequoia Supercomputer
1.63E+16 [Ops/s]

PoW network
1.76E+19 [Ops/s]
**Attack 2: Botnet**

Size of botnet * Computing power of bot = Computing power

- Largest botnet ever seen (BredoLab)
- Based on participants of BOINC
- Average contribution per user

\[
\text{Size of botnet} = 3.00 \times 10^7
\]

\[
\text{Computing power of bot} = 1.23 \times 10^{10} \text{ [Ops/s]}
\]

\[
\text{Computing power} = 3.70 \times 10^{17} \text{ [Ops/s]}
\]

Can we Afford Integrity by Proof-of-Work?

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

**Attack 2: Botnet**

- **Botnet**: 3.70E+17 [Ops/s]
- **PoW network**: 1.76E+19 [Ops/s]
Attack 3: Virtual protest

Number of protestors \( \times \) Computing power of protestor = Computing power

8.45E+08 \( \times \) 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]
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

- 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.
References 2/2