TeleTrusT-Informationstag "Blockchain"

Frankfurt a.M., 13.07.2017

Blockchain Technology
High Price Tag for Trustless Security

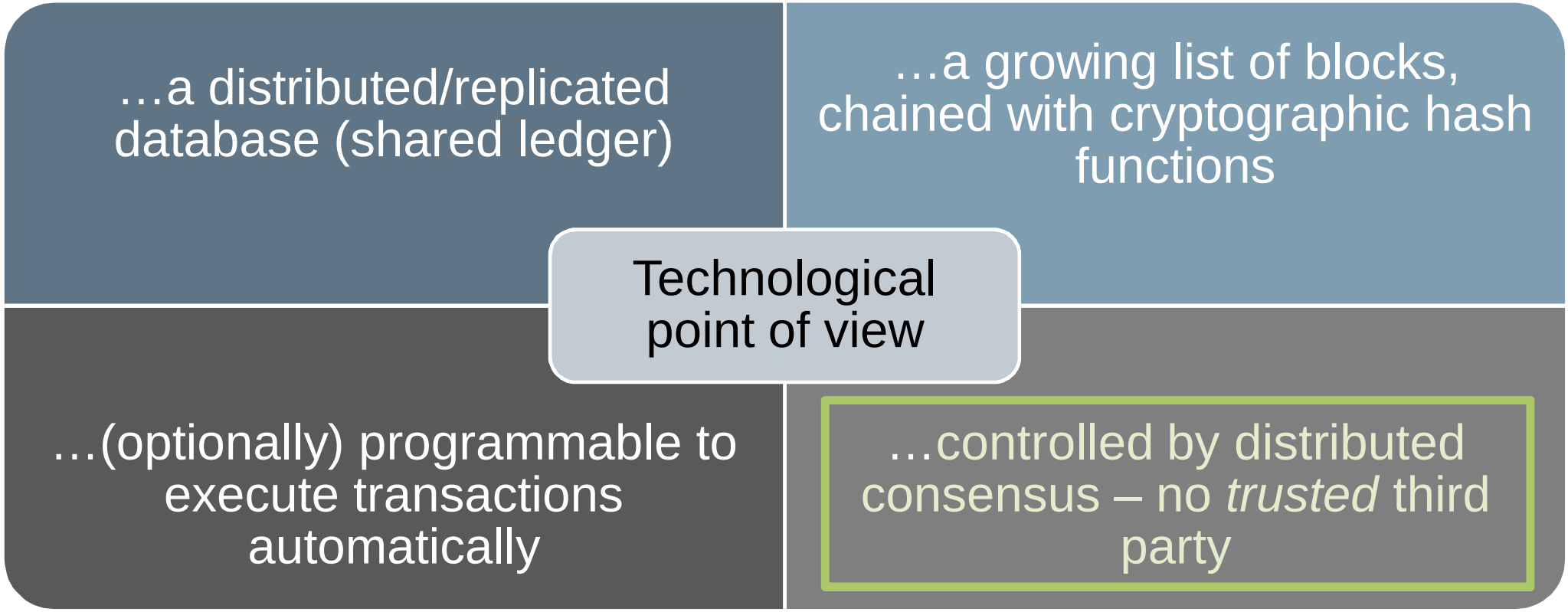
Dr. Hans Aschauer, Siemens AG

SIEMENS

Dr. Hans Aschauer, CT RDA ITS SES-DE

Blockchain Technology
High Price Tag for Trustless Security

Blockchain is…



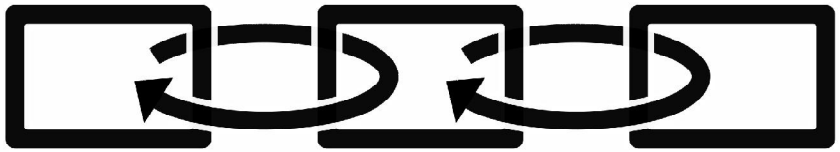
Blockchains realize Trustless Security

The blockchain consists of a data store and peer-to-peer communication

The data store is the key part of blockchains

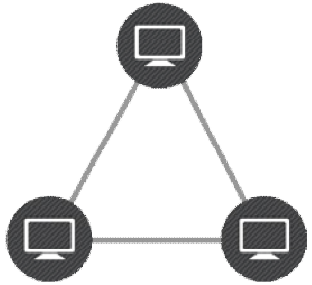
- **Data store** for a growing list of data records (e.g. transactions)
- **Temporal order** of data records
- **Distributed** consensus on the list of valid records
- **No central authority**
- **Non authenticated** by design

Trustless Security



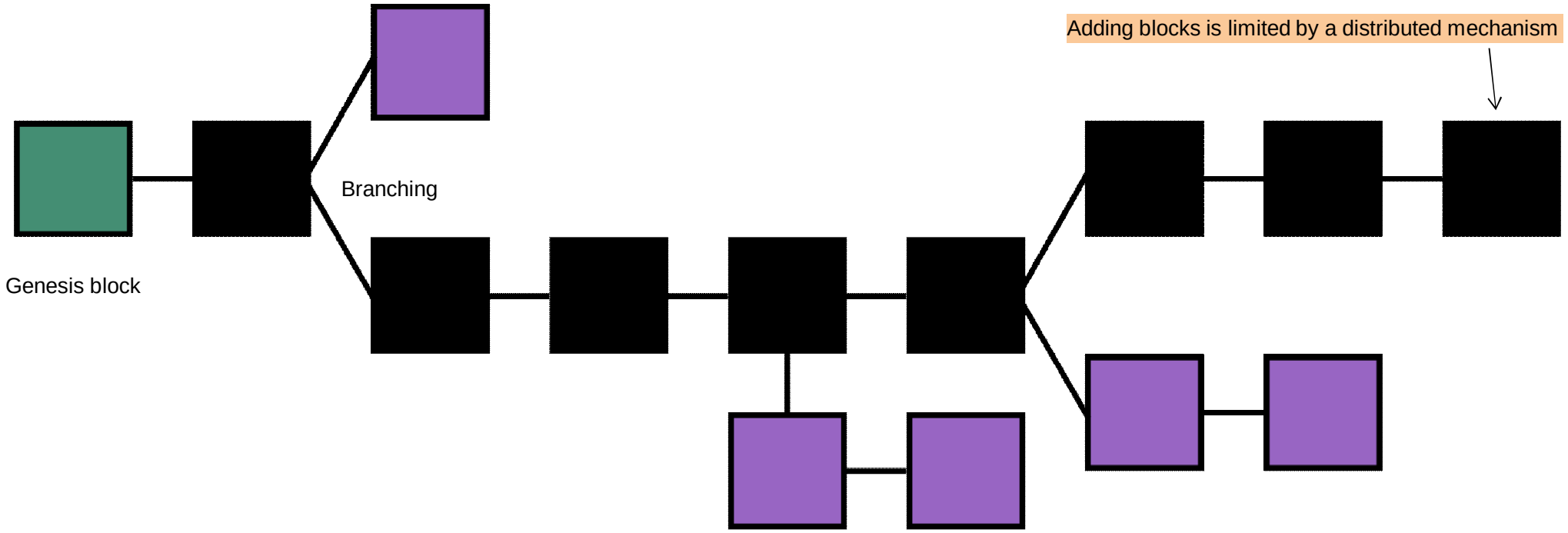
Blockchain applications use peer-to-peer communication

- **Standard protocols** are used
- **No explicit infrastructure** is required
- **Simple setup** without involving the IT department
- **Fail-save operation** due to redundant data storage
- **Proven and tested**



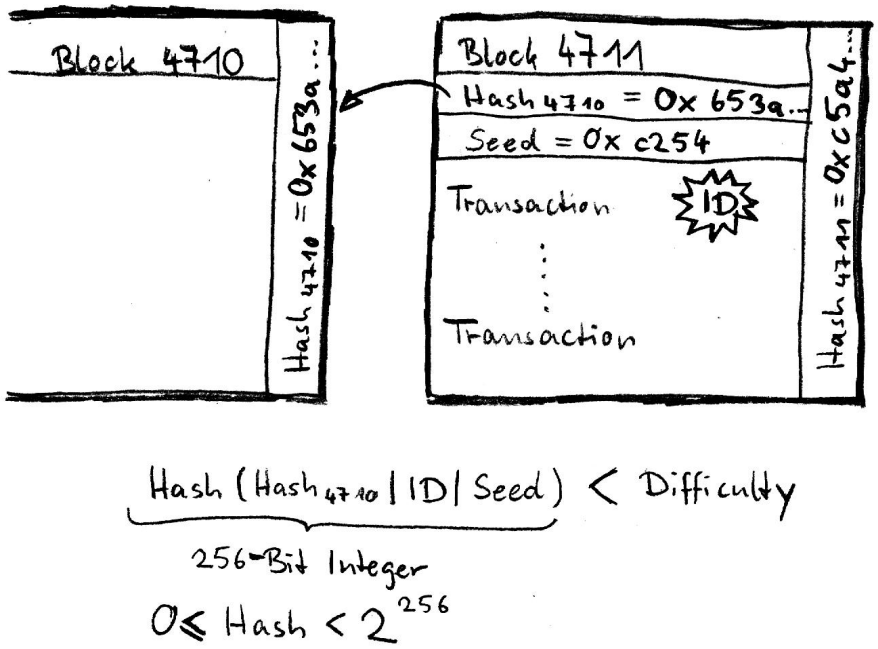
The design of the blockchain data store is novel and realizes trustless security

The longest series of blocks forms the "valid" blockchain



(source: https://en.bitcoin.it/wiki/File:Blockchain.png, rotated. Distributed under CC BY 3.0)

Block-adding limitation by Proof-of-Work (PoW)



- Prepare block: add hash of previous block
- Ongoing: collect transactions
- Try many seed values to solve inequality
- Seed found: congratulations, you may form a new block
- Calculate and append hash

Trustless Security is not for free – functional "costs" are substantial

Trustless Security enables new use cases, but is highly inefficient compared to traditional solutions without trustless security

Energy

- Computations for proof-of-work are energy intense
- Bitcoin:
- 2.8 Mio USD per day (for mining) (*)
- 1.3 GW (**)
- Currently 8-12 USD per transaction (*)

Storage

- Shared ledger is provided
- Database is replicated, not distributed
- Bitcoin ledger: currently 113 GB and growing (*)

Computation

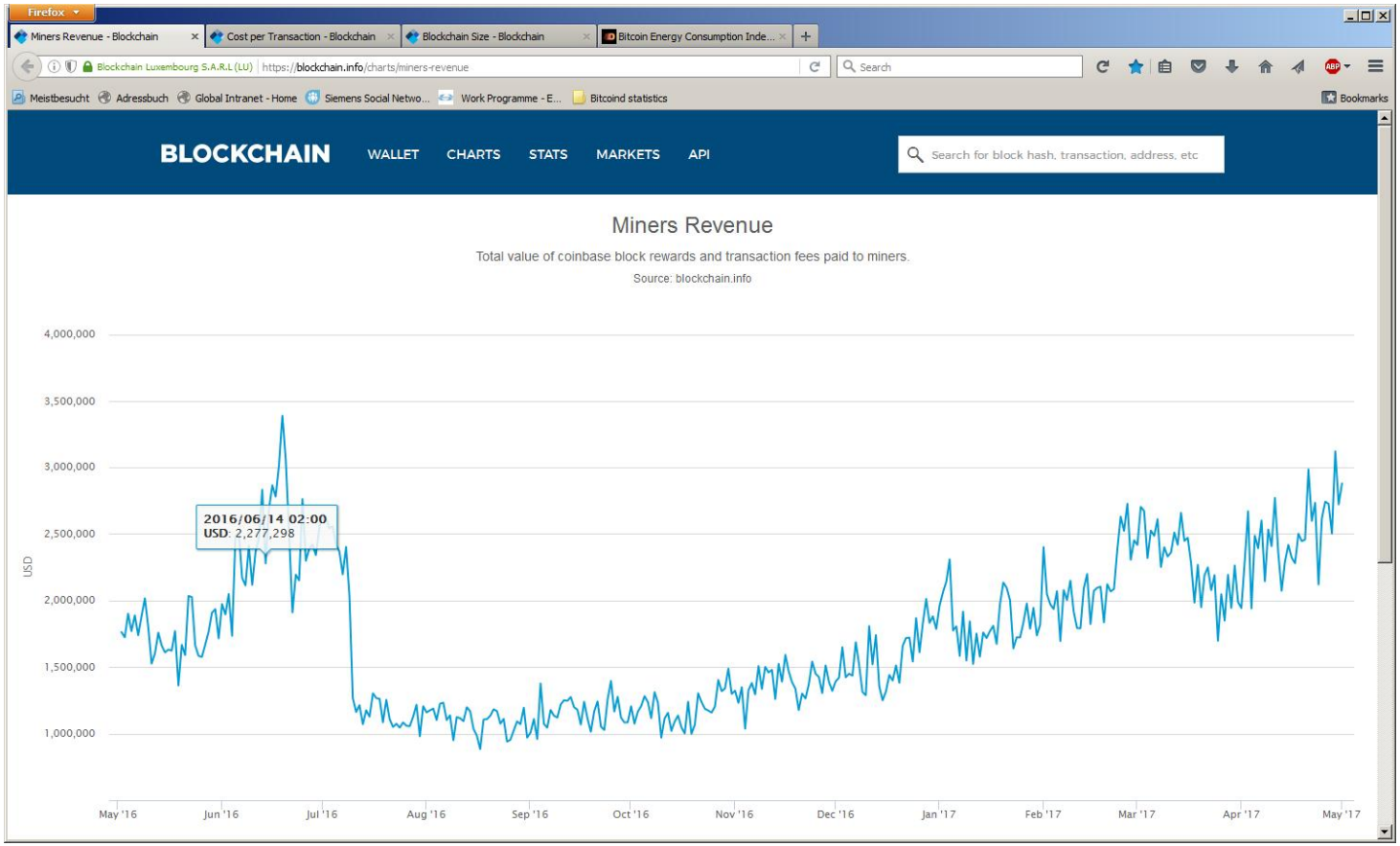
- Smart contracts based business logic
- All computations of business logic replicated by all nodes
- Vulnerable to denial-of-service attacks (***)

Performance

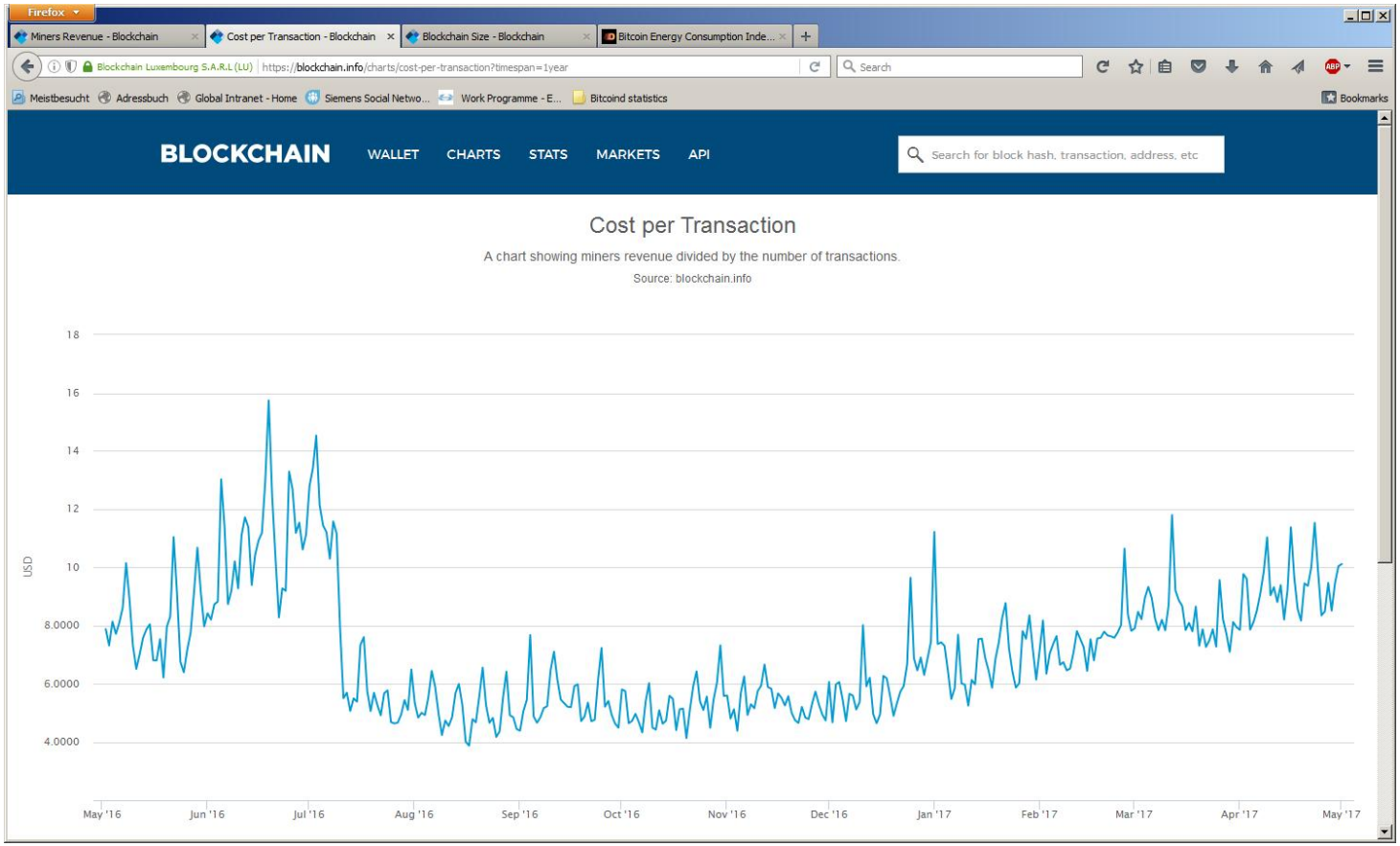
- Transactions times from several seconds to hours
- Depends on the timing parameters of the blockchain
- Bound by synchronization time of the global network

(*) https://blockchain.info/en/charts
(**) http://digiconomist.net/bitcoin-energy-consumption
(***) https://blog.ethereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/

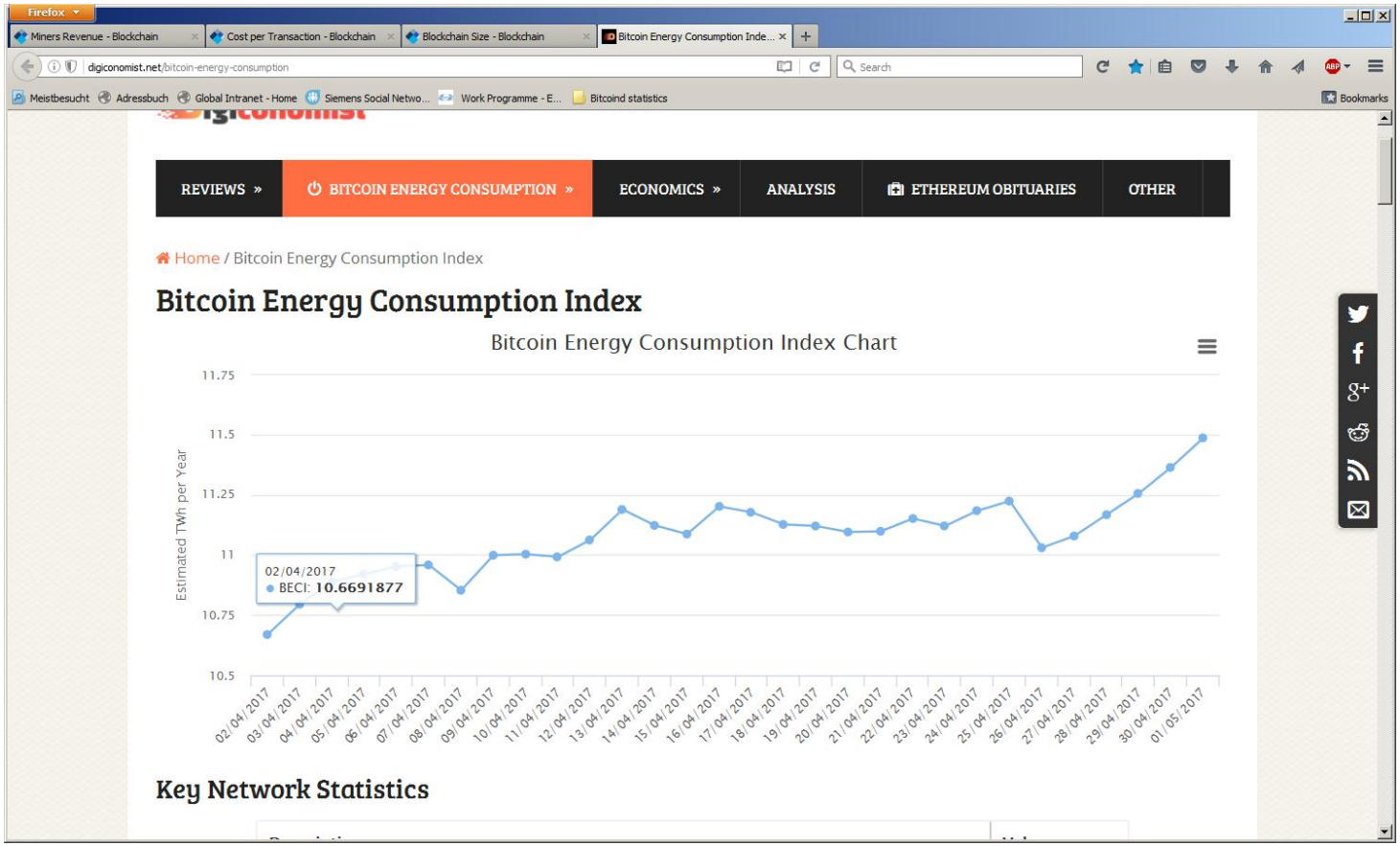
Bitcoin: The Miner's Revenue is invested into energy and hardware



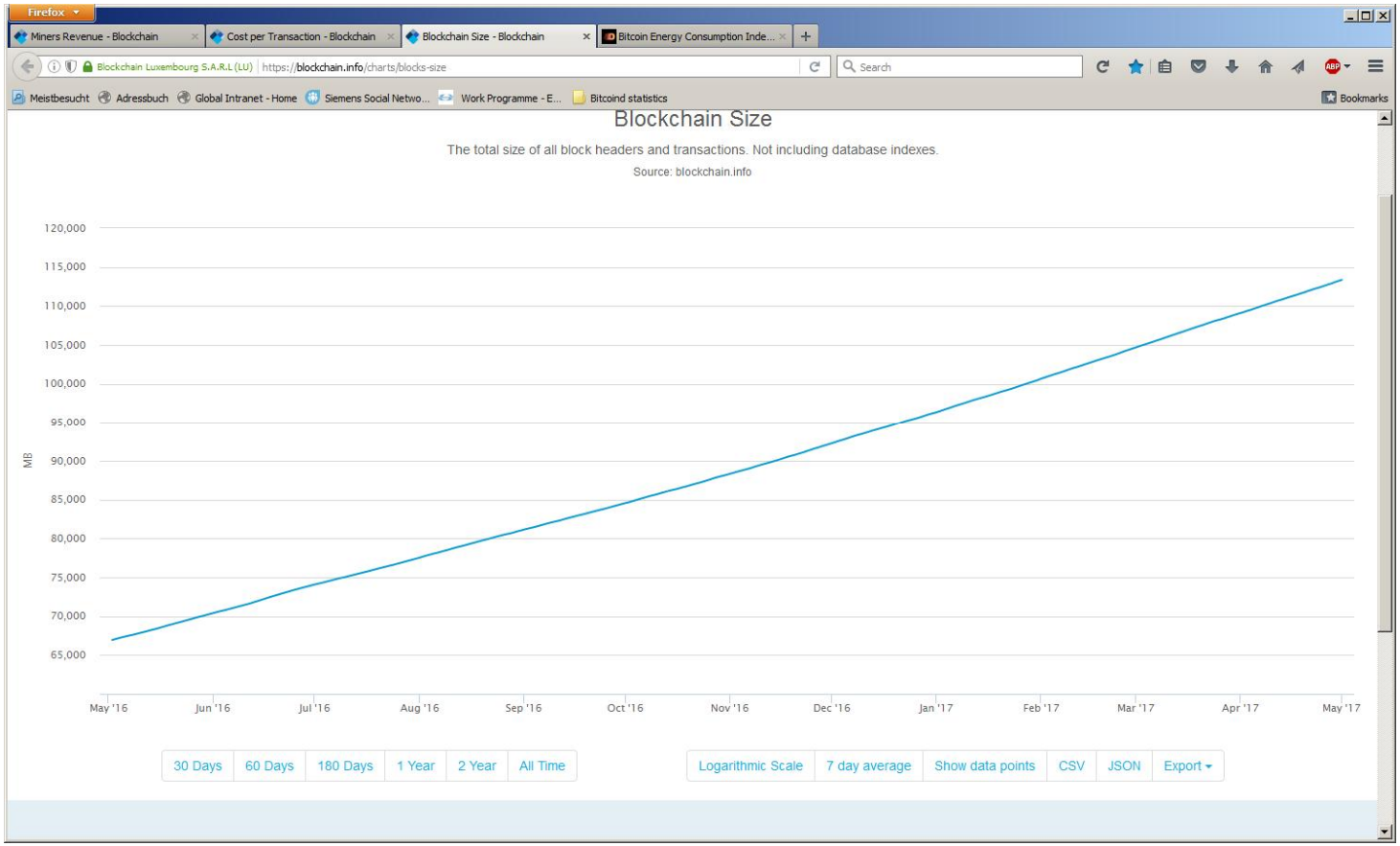
Cost per Transaction is ~10 USD per transaction



Energy consumption of Bitcoin mining is at ~ 1.3 GW



Bitcoin Blockchain is ~110 GBytes



Trustless Security provides only limited security

Trustless Security is vulnerable to security attacks

Low security guarantees compared to other cryptographic methods

- Intrinsic **consequence of distributed consensus**
- **51% attack is feasible** by definition, since 100% of computational power is available
- **Highlander property** ("there can be only one blockchain") leads to attacks (*).
- Limited or missing security of **private** (closed group) **blockchains**
- Problems expected during **blockchain life cycle**

Open traditional IT security leaks

- System is not immune against traditional weaknesses
- Cryptography guarantees immutability of the ledger, but this is no guarantee for the security of the system
- Storage and management of private keys may be exploitable

Additional **trust requirements** for **off-blockchain assets**

- Interaction of digital world and physical world requires trusted secure hardware
- No trustless security possible in this case
- Example: Who builds and installs a smart-contract based power switch?

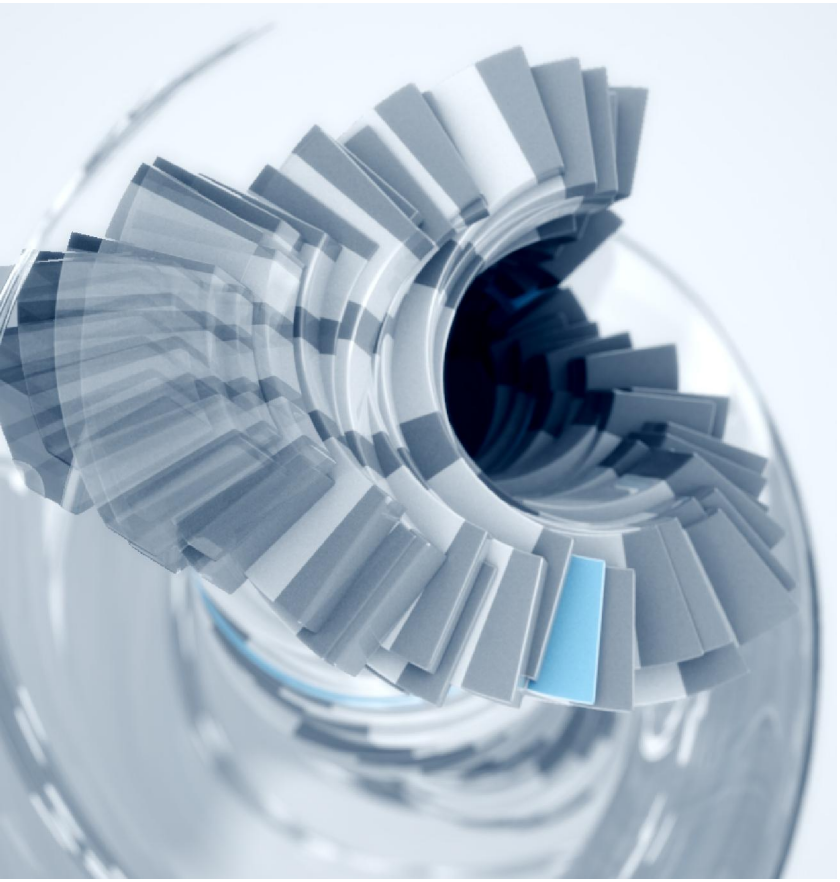
(*) One per hardware class. For a recent attack, see https://news.bitcoin.com/ethereum-clones-susceptible-51-attacks/

High costs of blockchain are a well-known fact in the blockchain community

"Blockchains in the use of Bitcoin with a decentralized consensus algorithm are inefficient because the inefficiency is the price you pay to get freedom. And if you don't care about freedom, why take the inefficiency? Install a database."

(Andreas M. Antonoupulos, author of "Mastering Bitcoin", O'Reilly)

Contact



Dr. Hans Aschauer
CT RDA ITS SES-DE

Otto-Hahn-Ring 6
81739 München

Telefon:
+49 (89) 636-633706

E-Mail:
hans.aschauer@siemens.com