

Lucerne University of
Applied Sciences and Arts

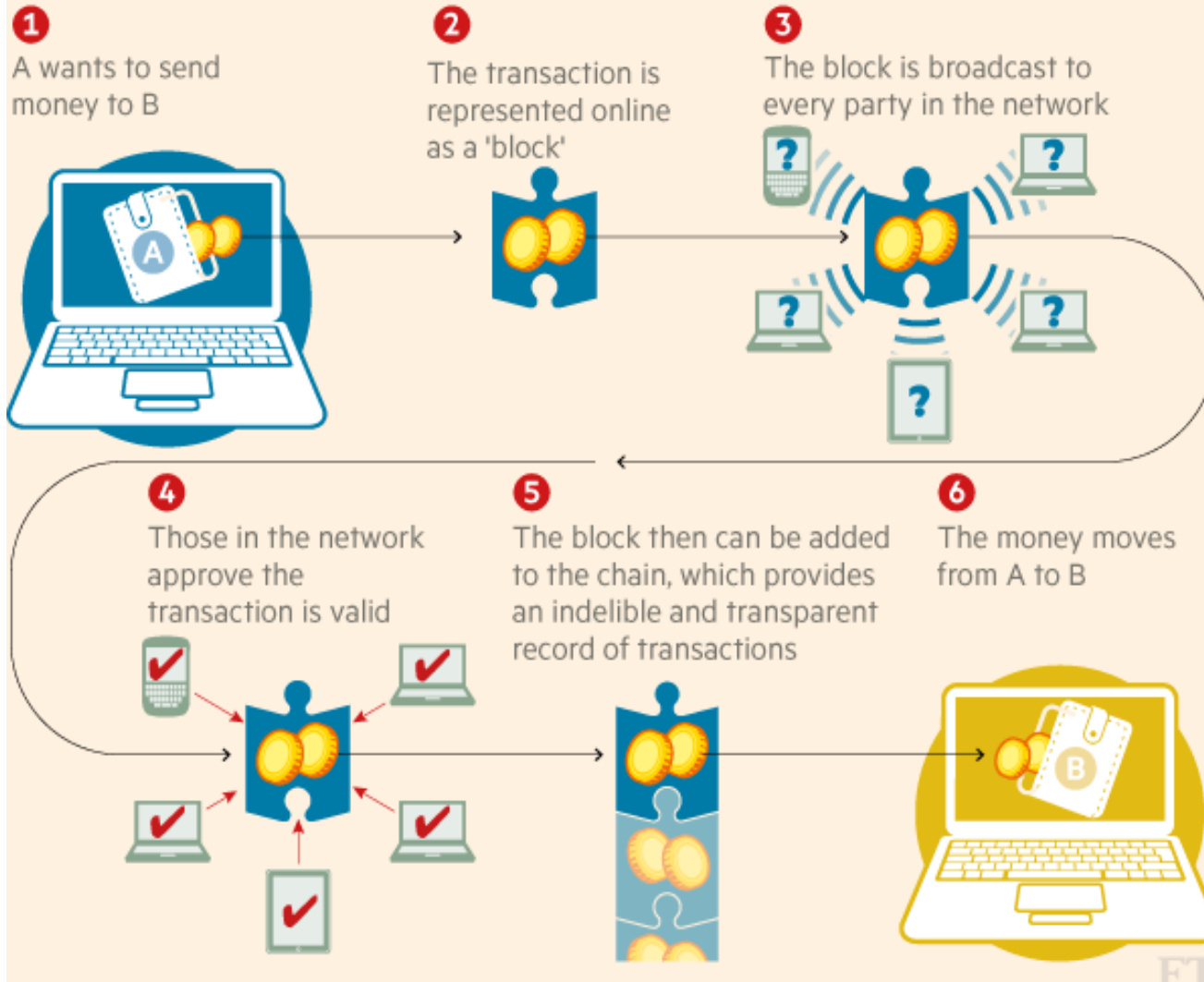
**HOCHSCHULE
LUZERN**

Hochschule Luzern
Informatik

Blockchain: Wie funktioniert diese wirklich?

Dr. Tim Weingärtner

How a blockchain works



Was ist eine Blockchain?

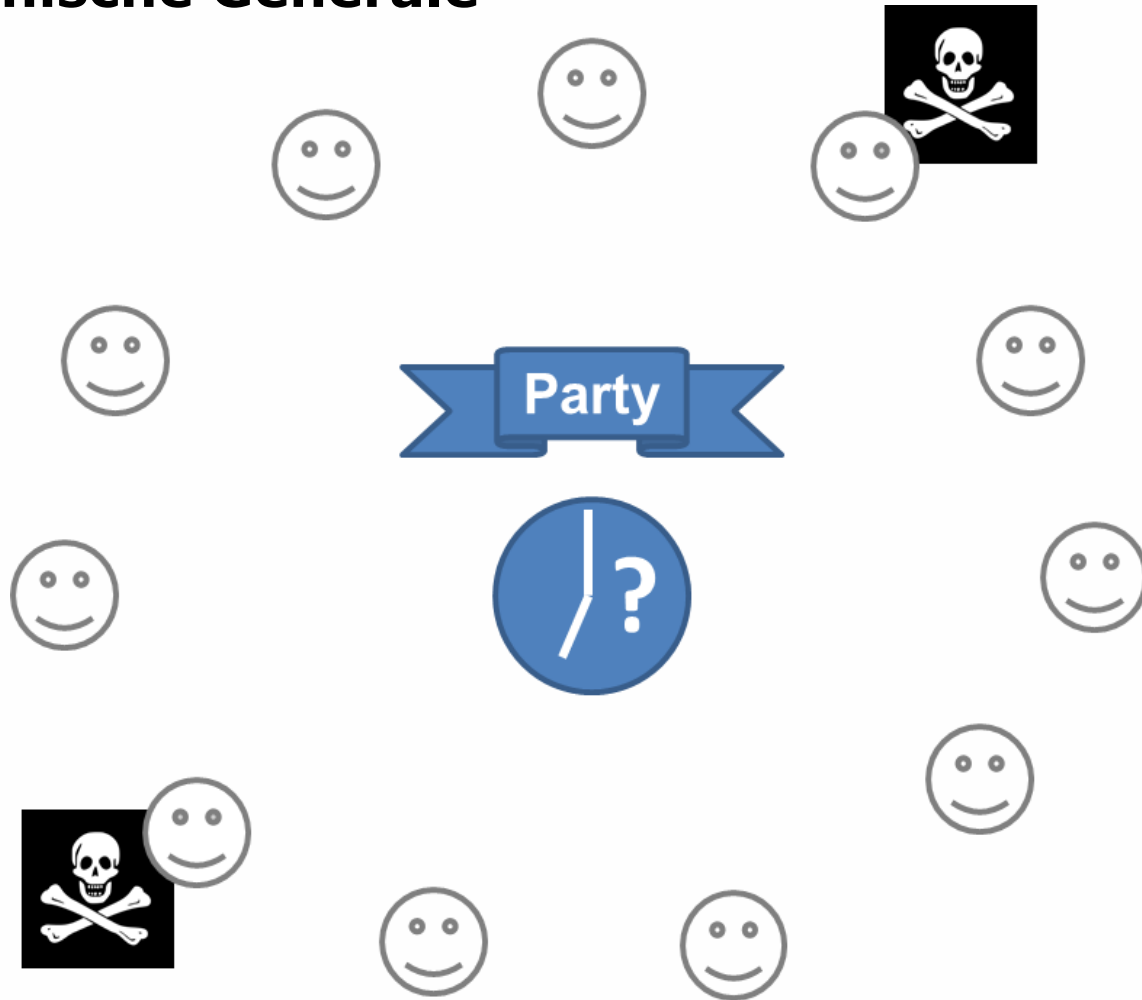
- **Verteilte, öffentliche Datenbank**
- Dort, wo heute eine «**Trusted Thirdparty**» benötigt wird

Historie von Blockchain und Bitcoin

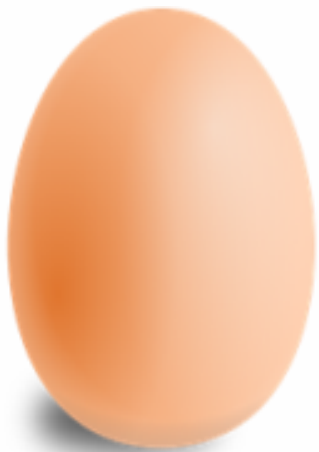
- Oktober 2008:
Paper von Satoshi Nakamoto
- Nakamoto ist ein Pseudonym
- Blockchain = Technologie
Bitcoin = Wahrung



Byzantinische Generäle



Hash Code

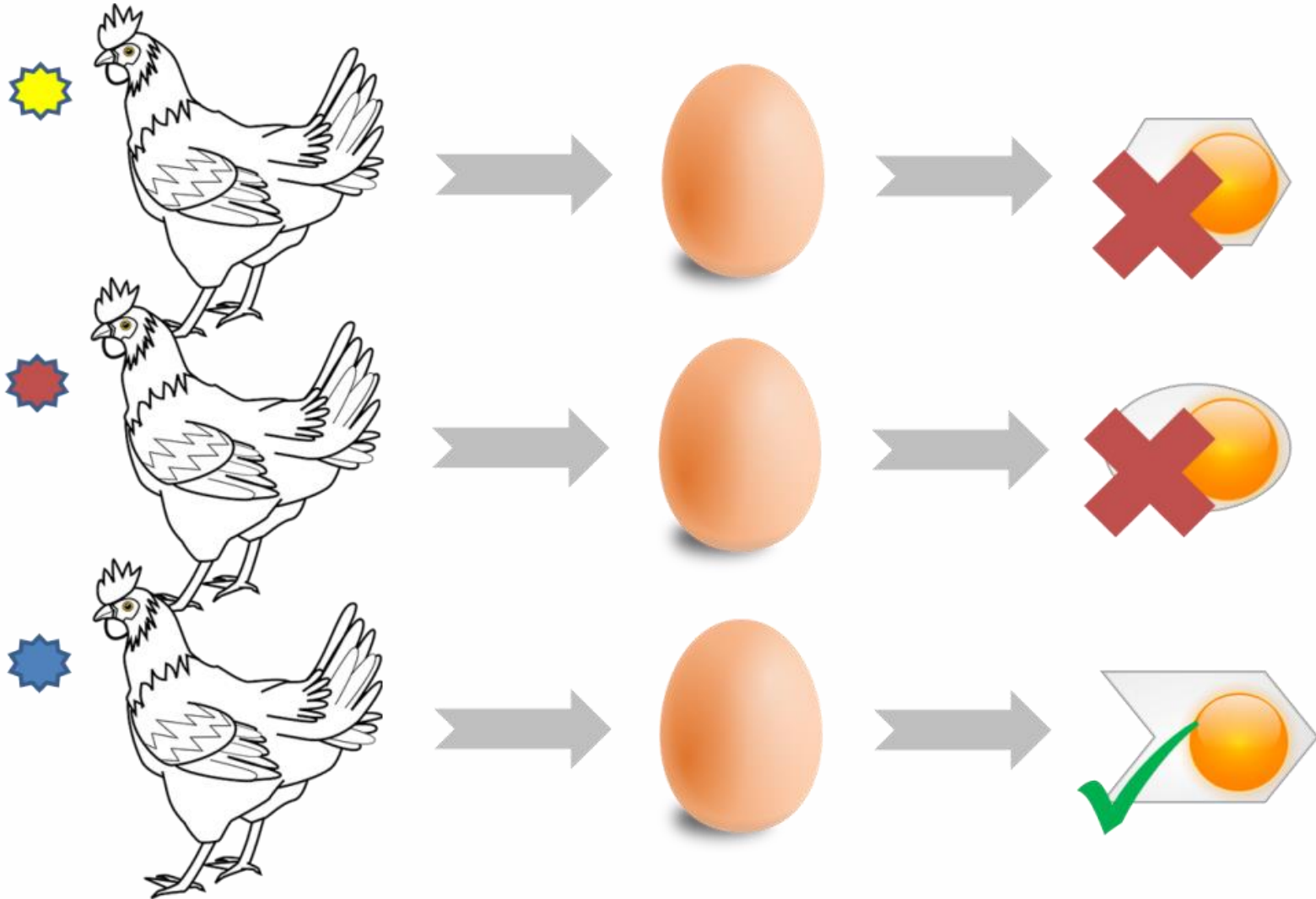


PASSWORD!



09bffa954fe
f56de82867
1a2b64da71
009bae89de
f060eb355a
7d

Proof of Work



Nonce



~~001b0~~9bffa...

? +

PASSWORD!



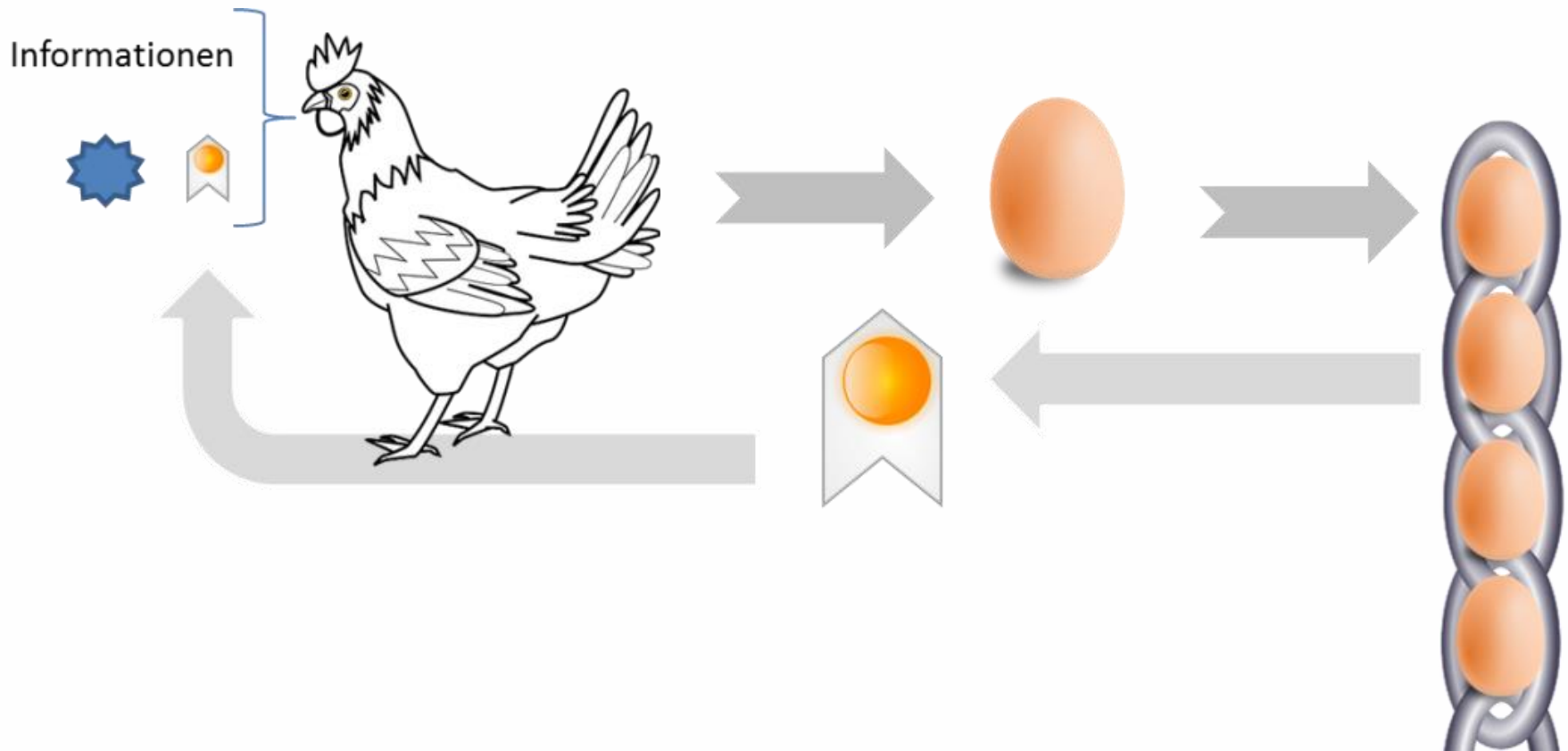
~~0f45d~~9bffa...



000009bffa...

Mining

Blockchain



Informationen

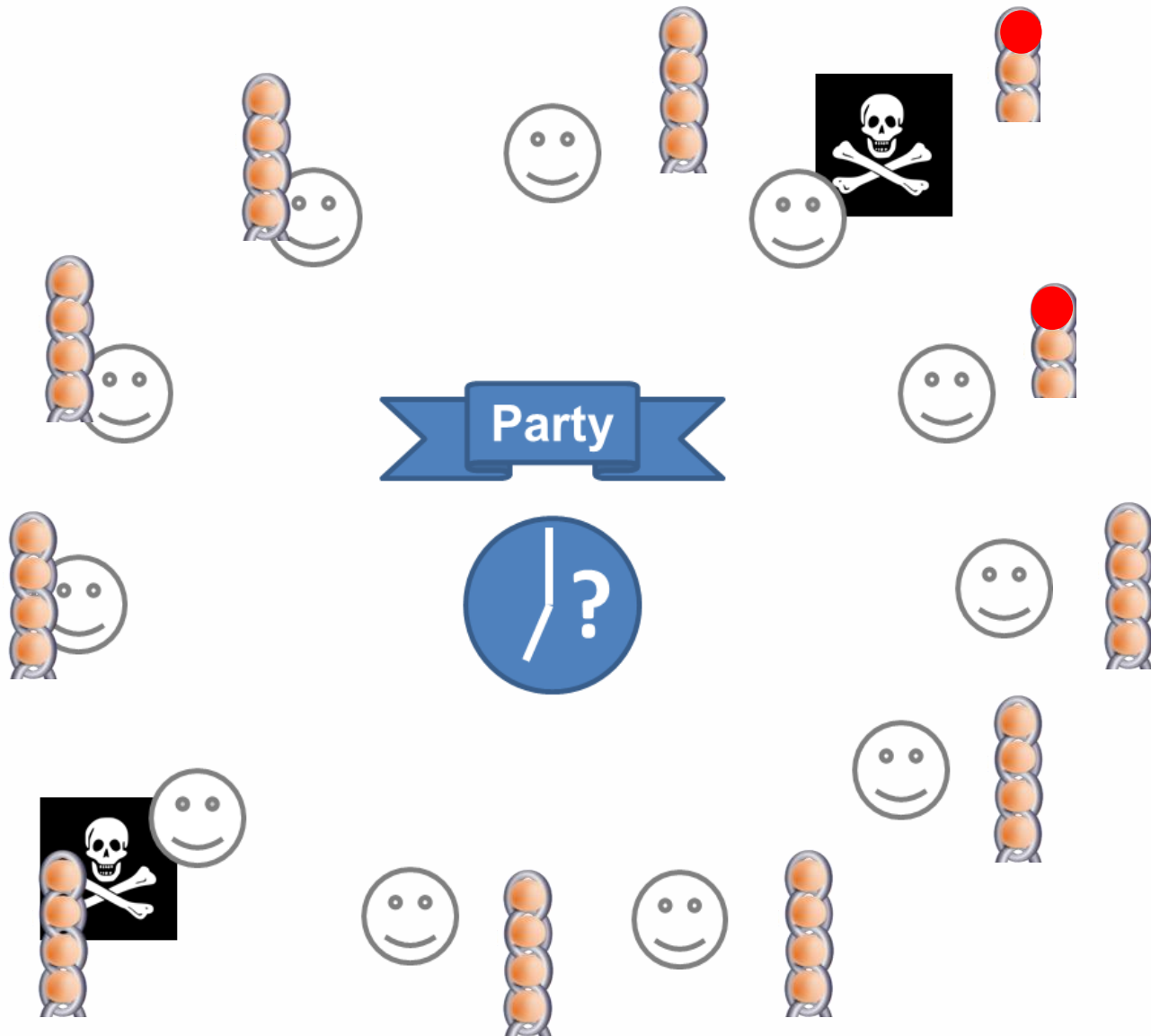
+
Nonce

+
0000044hb2...



000009bffa...





Wallet – Wo liegt das Geld?

Bitcoin Address



SHARE

13jzY4RNCBGmiCNj5uht4FLkj2jQrQjJjk

Private Key



SECRET

5HqDBL1ej5FdcHf4HoM5iq2XQx2RPKvzMedSA7ZLbPTxnJW8ejD

Blockchain ist zentral und transparent einsehbar

BTC.com Pool Blöcke Statistik Tools Apps/Erweiterungen Brieftasche Adresse/Höhe/Hash... **Deutsch**

Home / Adresse - 1EQPyk3zsNTnbFAeWhcACUziVcXr5Di63L

Summary

Adresse	1EQPyk3zsNTnbFAeWhcACUziVcXr5Di63L	Empfangener Gesamtbetrag	231.20280000 BTC
Saldo	0.00000000 BTC	Anzahl der Transaktionen	2

↔ Transaktion 2 | 📊 Stats | 🔗 Erwähnungen 0

Transaktion	Betrag	Bestätigungen	Datum
383b584096bcc6725d00d0615d951d89a5b4e0e5acdcafc32970ebb3f6190c142c	0.00060000 BTC	434,839	2016-10-18 10:47:07
1EQPyk3zsNTnbFAeWhcACUziVcXr5Di63L	231.20280000	1 Bestätigungen	- 231.20280000
42969a387015f52441ce073e7f41a689971d7691f3ebbd39861ff2f9f83dca2c	0.00060000 BTC	434,839	2016-10-18 10:47:07
1NrgszFGFjHGhprjyqQLTQzMLzK4ymoeAX	231.25540000	1 Bestätigungen	+ 231.20280000

Risiken

Bitcoin is facing a major problem as the time it takes transactions to be processed has increased dramatically leading businesses to stop accepting the cryptocurrency. Some have issued warnings that the problems could be terminal.

Bitcoin Could Consume as Much Electricity as Denmark by 2020

WRITTEN BY SEBASTIAAN DEETMAN
March 29, 2016 // 11:30 AM EST

Chinesen bauen gigantisches RZ - nur für Bitcoin-Mining



Conclusion: Mining bitcoin is now a business, in the hands of professional miners that have invested significant money in infrastructure. If you don't want to be a professional miner and invest at very least a few thousands of €\$£ in it, just give up mining.

Quellen:

<http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020>
<https://www.quora.com/How-much-CPU-time-is-needed-to-mine-1-bitcoin>
<http://www.inside-it.ch/articles/45619>
<http://www.ibtimes.com/bitcoins-big-problem-transaction-delays-renew-blockchain-debate-2330143>

Anwendungsmöglichkeiten

