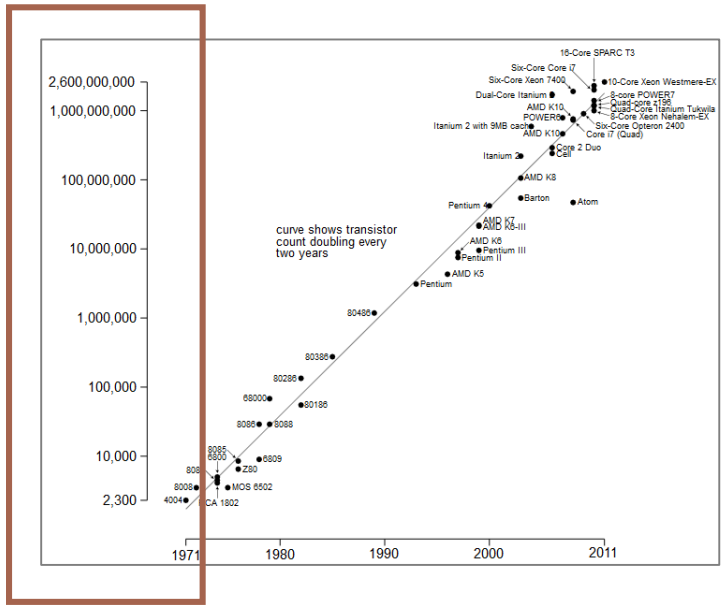
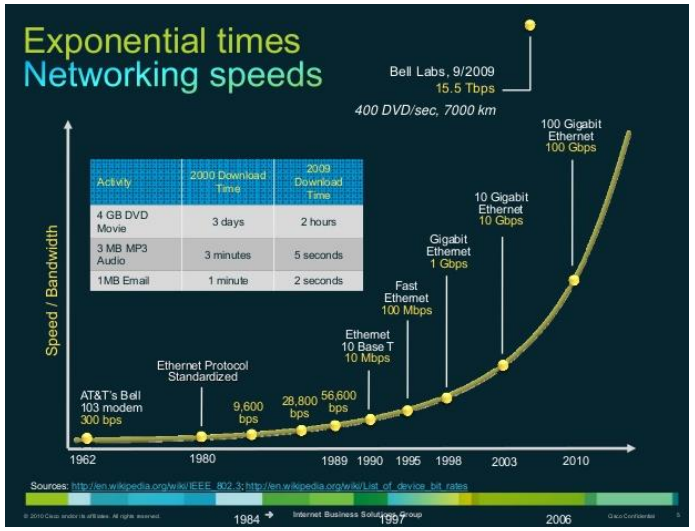
Sinn und Unsinn der Digitalisierung
Vertrauensmaschinen und Maschinenvertrauen

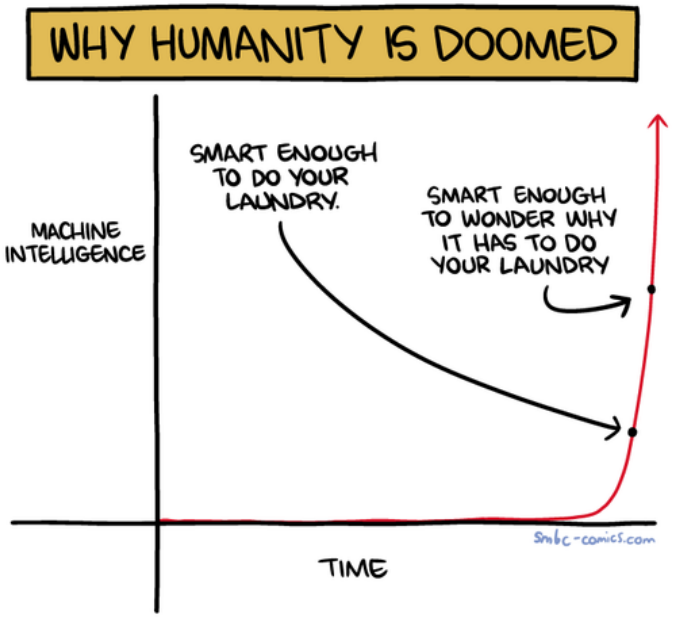
© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Exponentiell leistungsfähigere Werkzeuge…



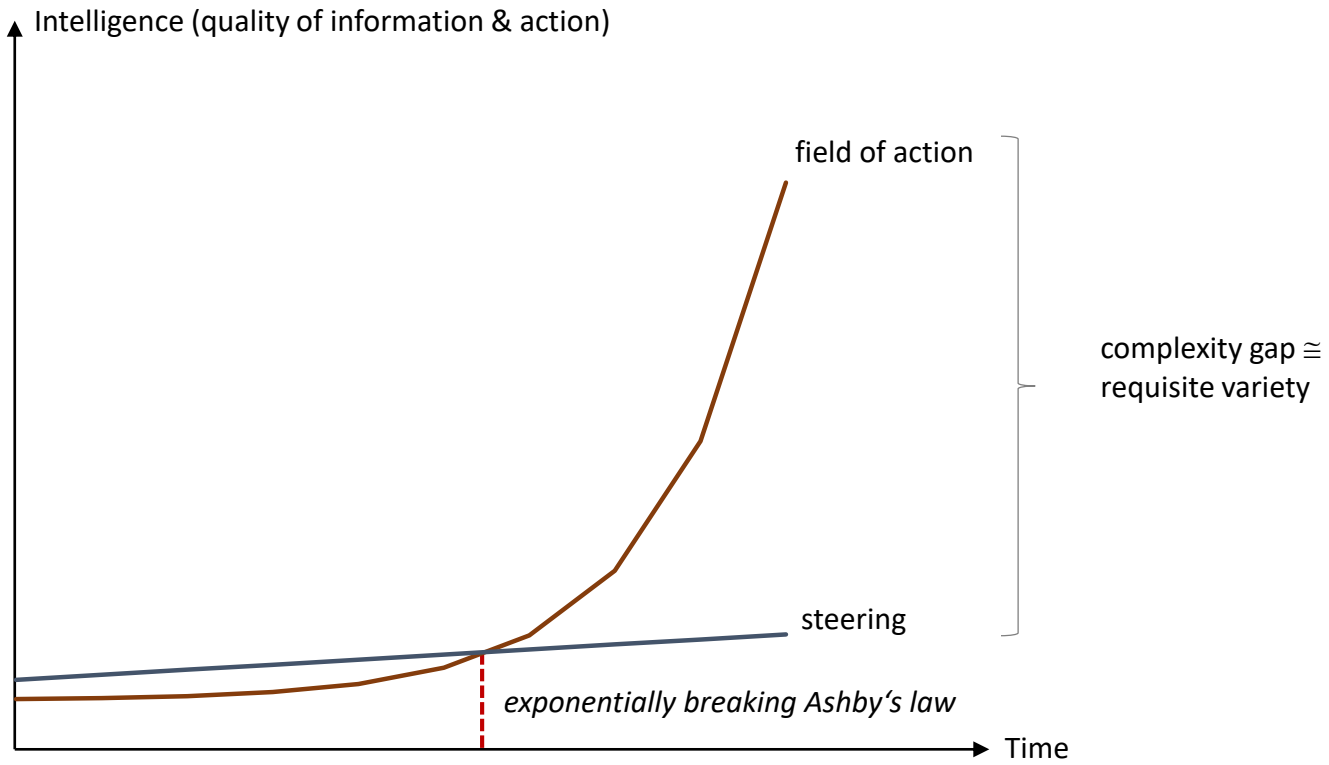


+ Netwerkkomplexität
+ content-Komplexität



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

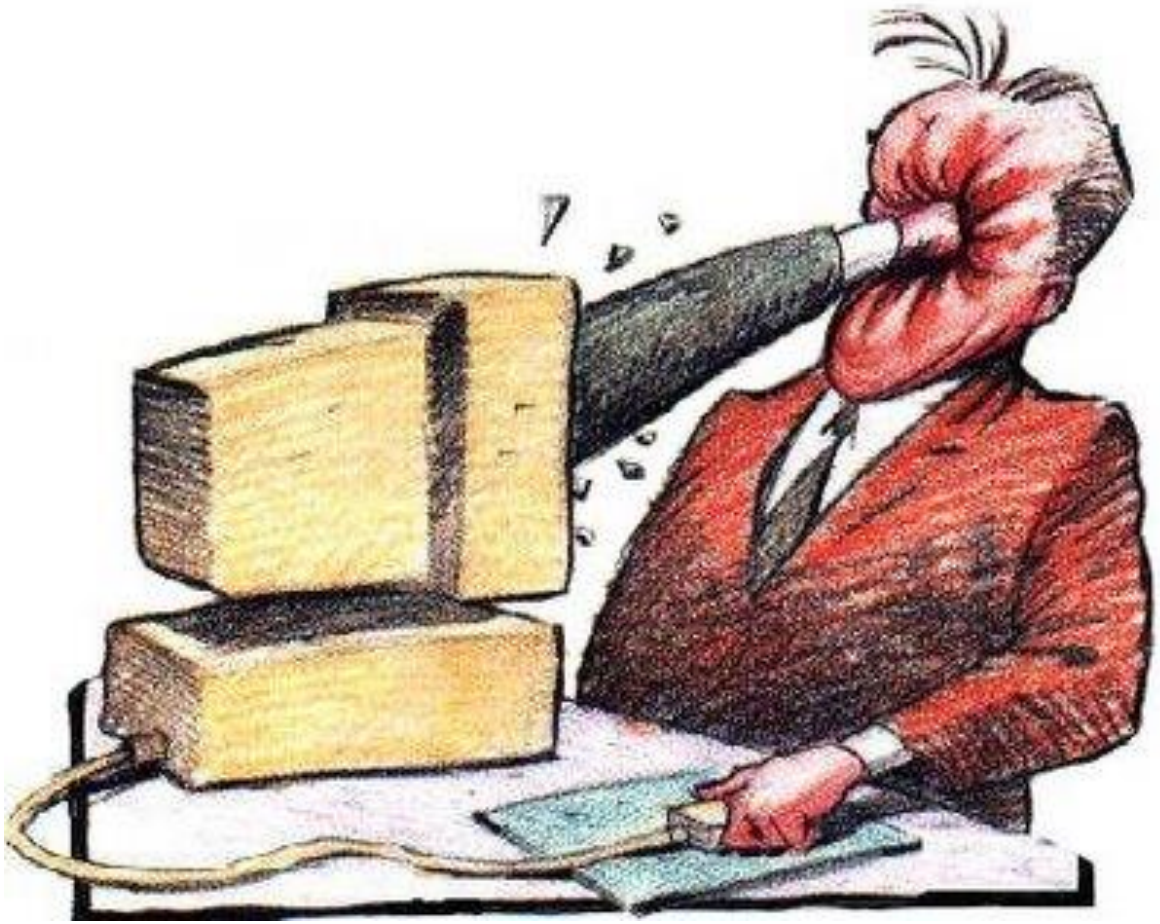
… deren Nutzung immer schneller und weiter hinter den Möglichkeiten zurückbleibt.



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Emergenz disruptiver Wettbewerber

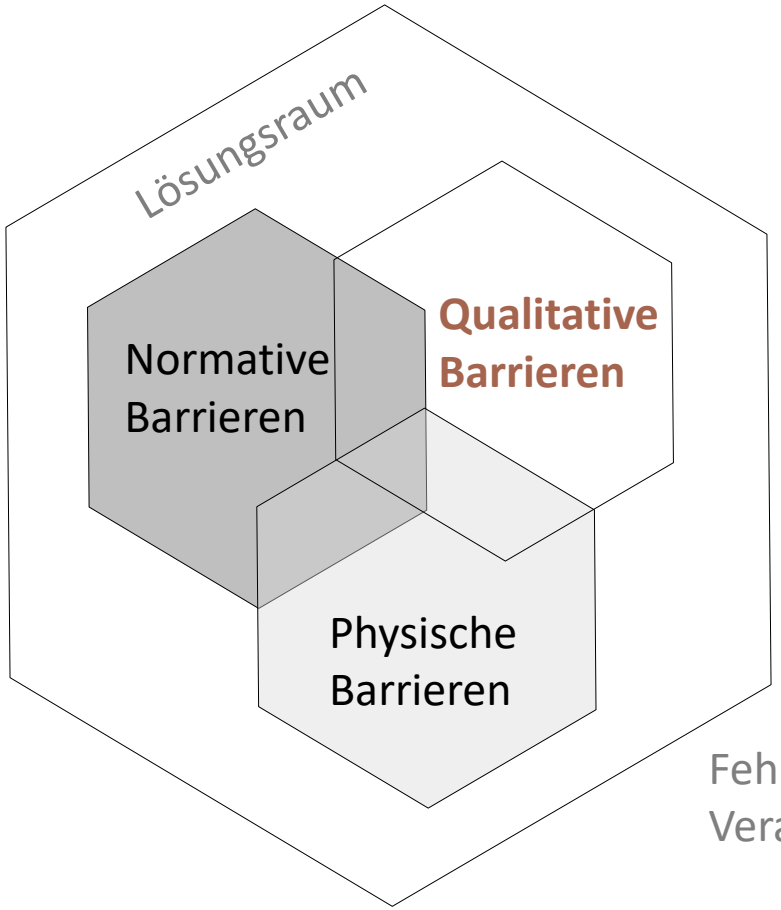
Besser ist besser als schlechter



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

(Be)Hinderungsgründe

Widerstand durch Begünstigte des Status Quo bzw. durch Benachteiligte einer Veränderung



Irrtümer, z.B. blindes Vertrauen

Fehlende Information bzw. Verarbeitungskompetenz

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

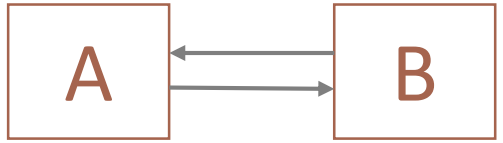
Vertrauen := Wahrscheinlichkeit

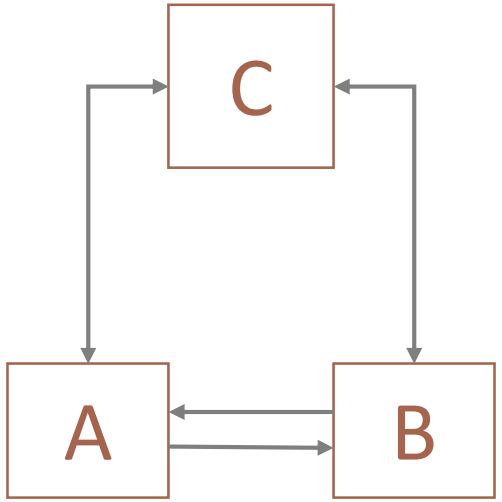
„Wahrheit ist die Erfindung eines Lügners“
Heinz von Foerster

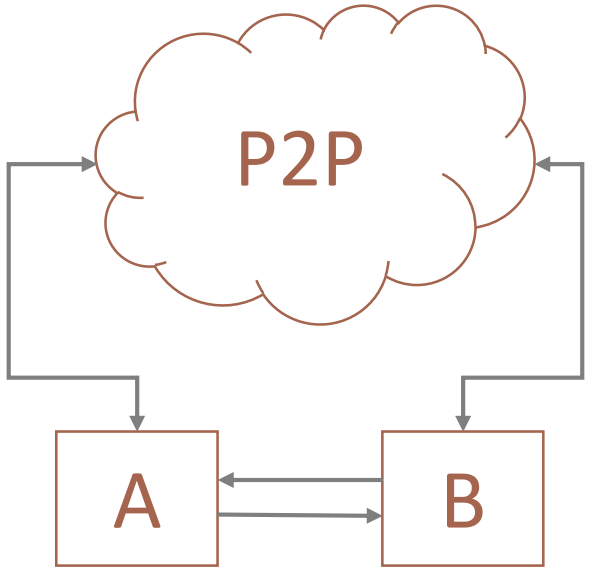
„Wenn ich irgendworin Räthselrather bin,
so will ich es mit diesem Satze sein! [...]
Das sind noch lange keine freien Geister:
denn sie glauben noch an die Wahrheit“
Nietzsche (Genealogie der Moral)

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Vertrauenskomplexität





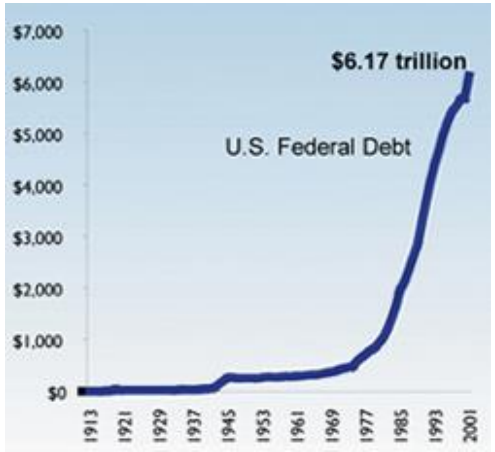


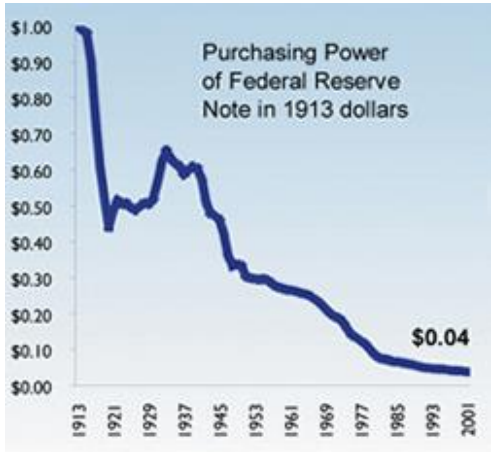
	Bilaterales Vertrauen (1:1)	**Hierarchisches Vertrauen (1:n)**	**Heterarchisches Vertrauen (n:m)**
Bewertungsbasis	persönlich/individuell	zentral/intermediär	vernetzt (konsensorientiert)
Wertsurrogat	Unmittelbarer Tausch (incl. Güter sui generis)	„Fiat Geld“	Kryptowährungen
Techn. Vertrauensorganisation		Trust Center (z.B. PKI)	Web of Trust (z.B. PGP)

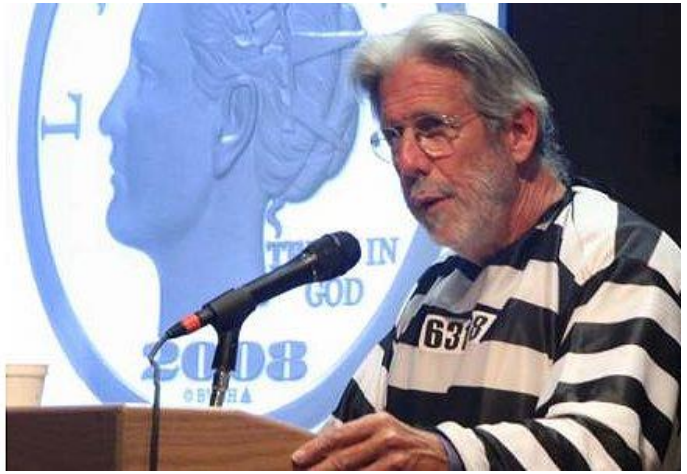
© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Hierarchischer Vertrauensschwund

z.B. Liberty Dollar







Bernard von NotHaus

www.libertydollar.org

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Lesson Learned

Pseudonymer Geniestreich: Bitcoins immaculate conception

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
- Double-spending is prevented with a peer-to-peer network.
- No mint or other trusted parties.
- Participants can be anonymous.
- New coins are made from Hashcash style proof-of-work.
- The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Full paper at:
http://www.bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Fehlerfreier Konsens in Netzwerken

Wie hütet man einen löchrigen Sack Flöhe?

„Byzantinische Generäle“:
Koordinationsprobleme in Mehrpersonen-Mehrzielsystemen

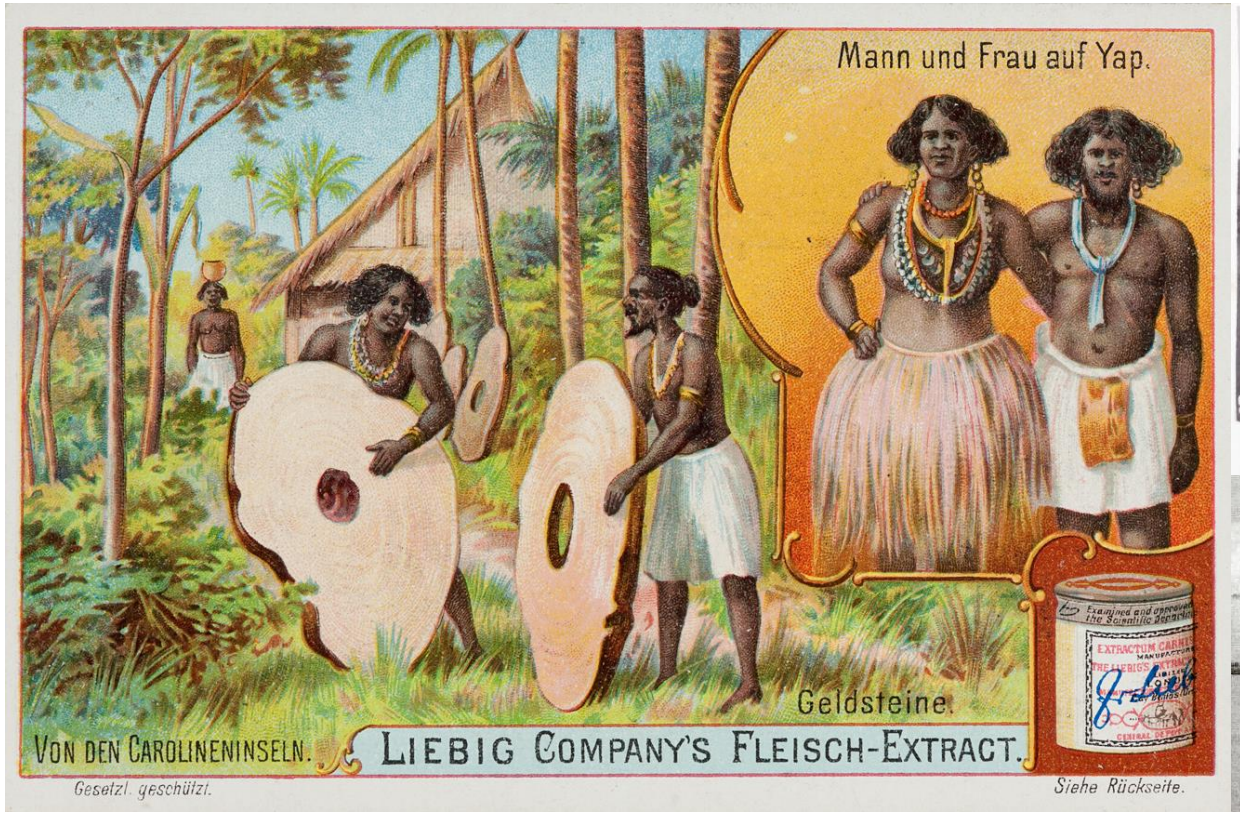
→ **generelle Lösung durch Nakamotos Blockchain-Konzept (verteiltes Buchungsjournal)**
fälschungssicherer Konsens in komplexesten Netzwerken durch Kombination von Spieltheorie und Verschlüsselungsalgorithmen:
- radikal einfach
- elegant
- robust („trustless“) bis antifragil

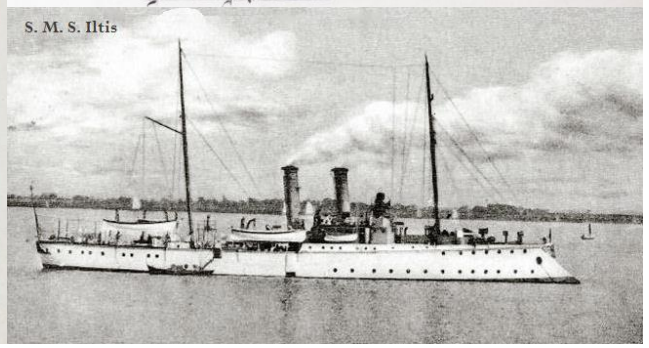
⇒ emergentes Ökosystem für ein „Internet of Value“ mit Anwendungsmöglichkeiten weit über den Kryptowährungskontext hinaus: „distributed ledger technology“ (DLT)

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Frühe DLT auf Wetware-Basis

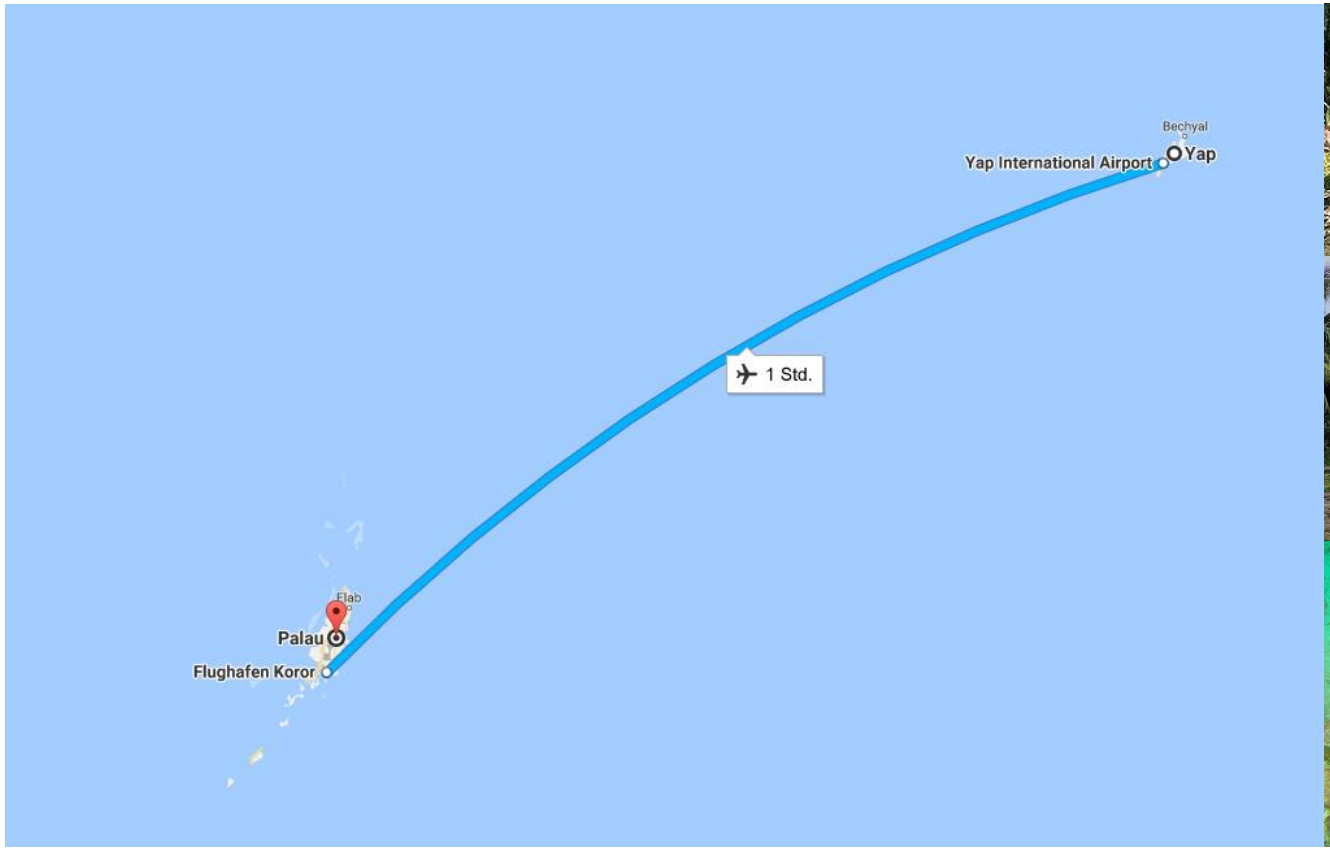
Steinreiche Mikronesier: Rai





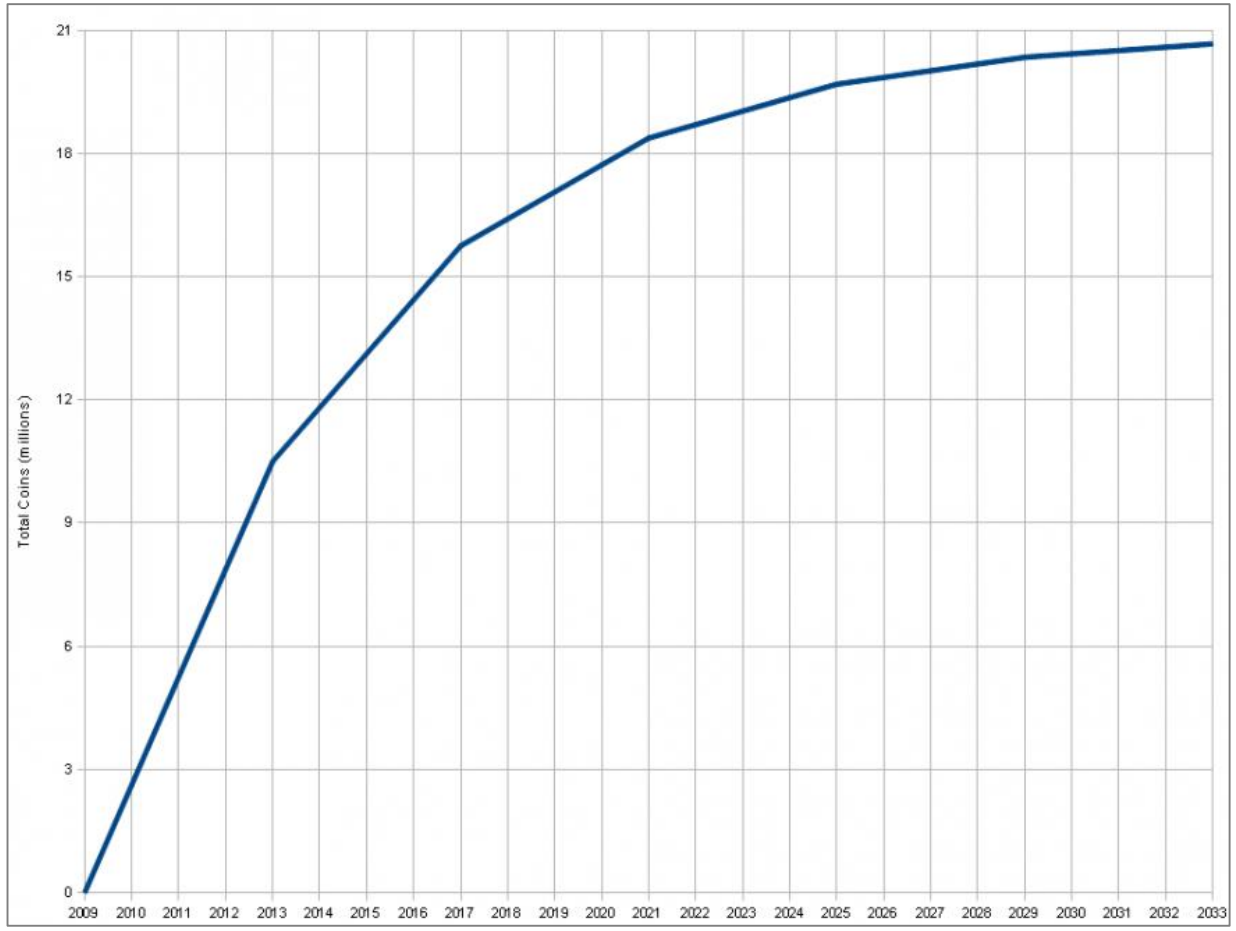
© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

„Rai-Mining“



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

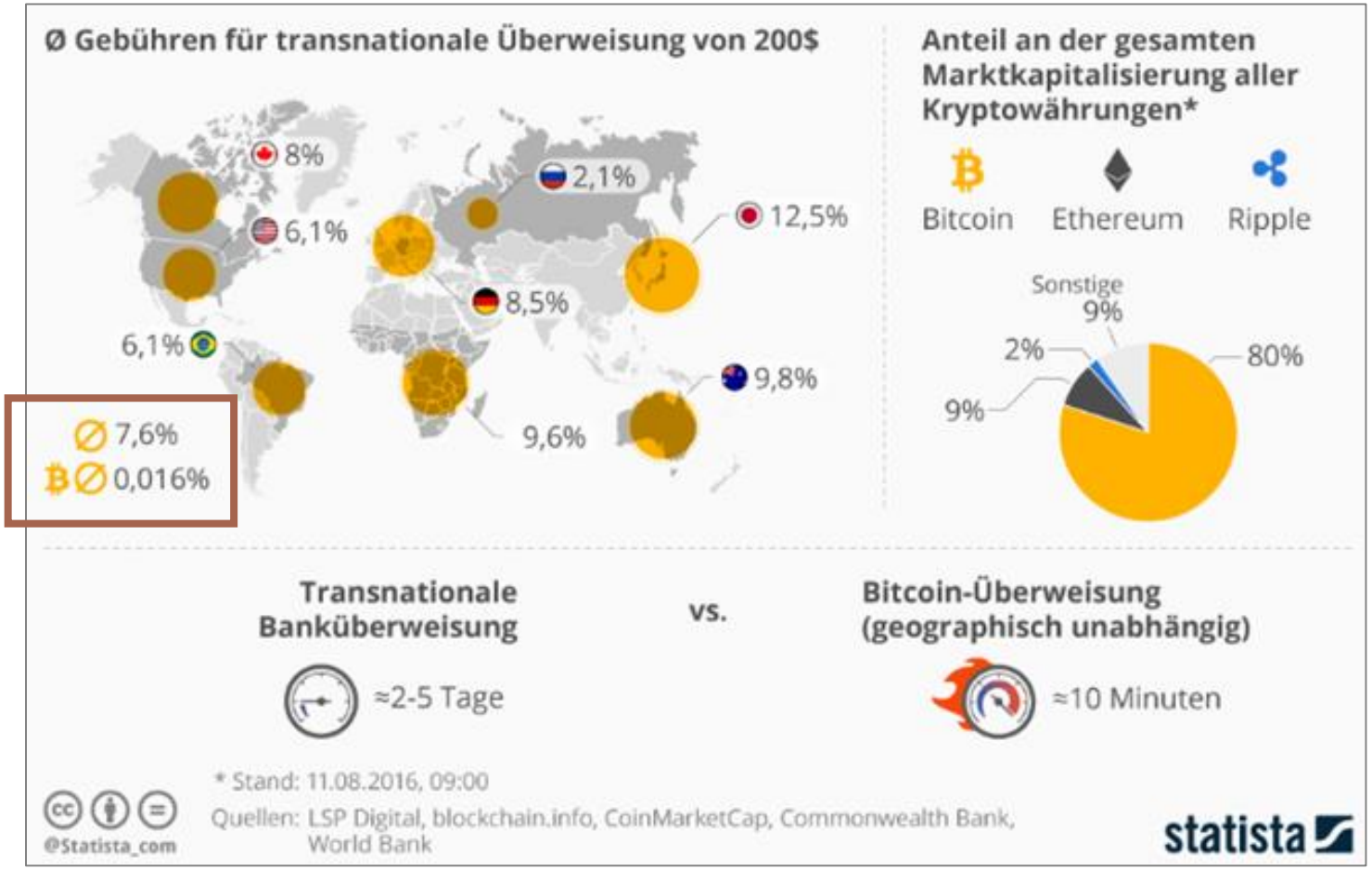
Geldmengeninflation: Rai vs. BTC



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Banken-Killerapplikation Bitcoin

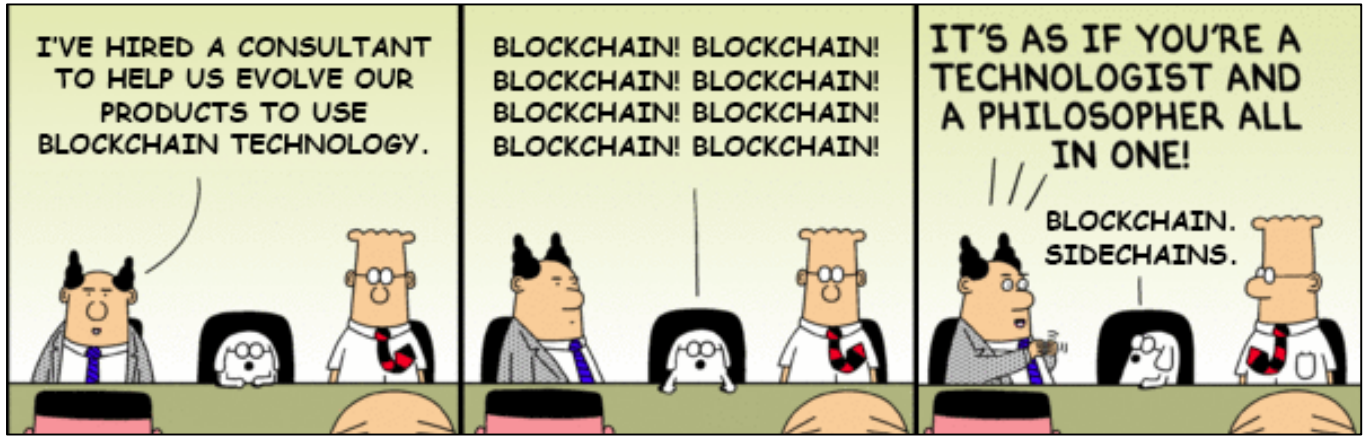
Deutlich günstiger, schneller und kleinteiliger als Fiat



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Das Blöken der Schafe

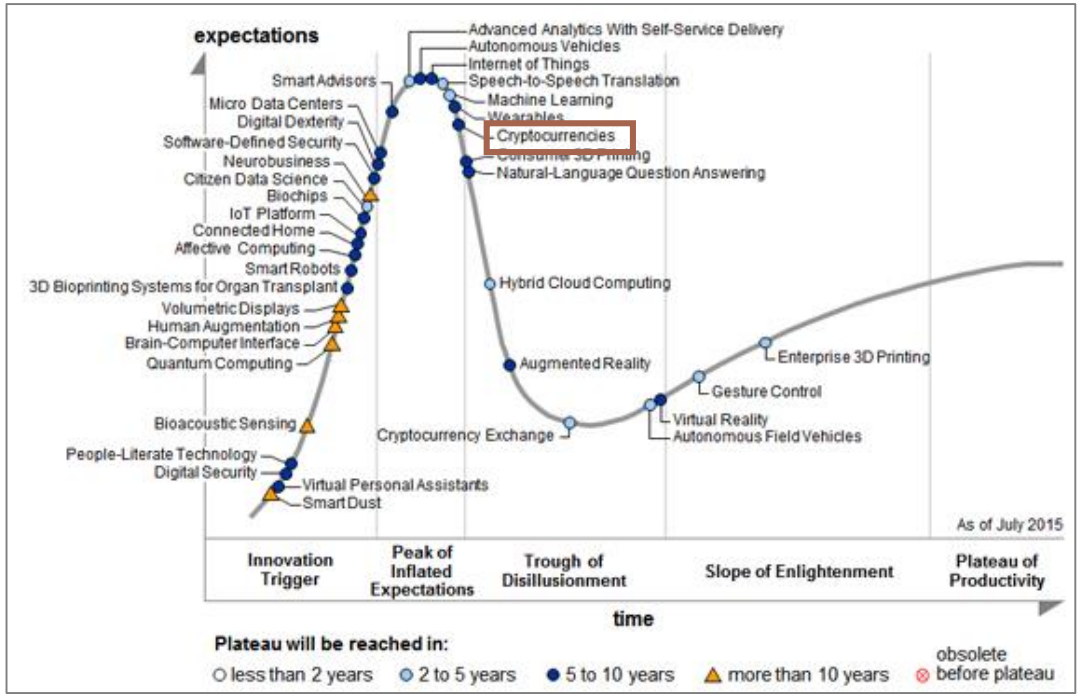
Welche Farbe hat am meisten RAM?

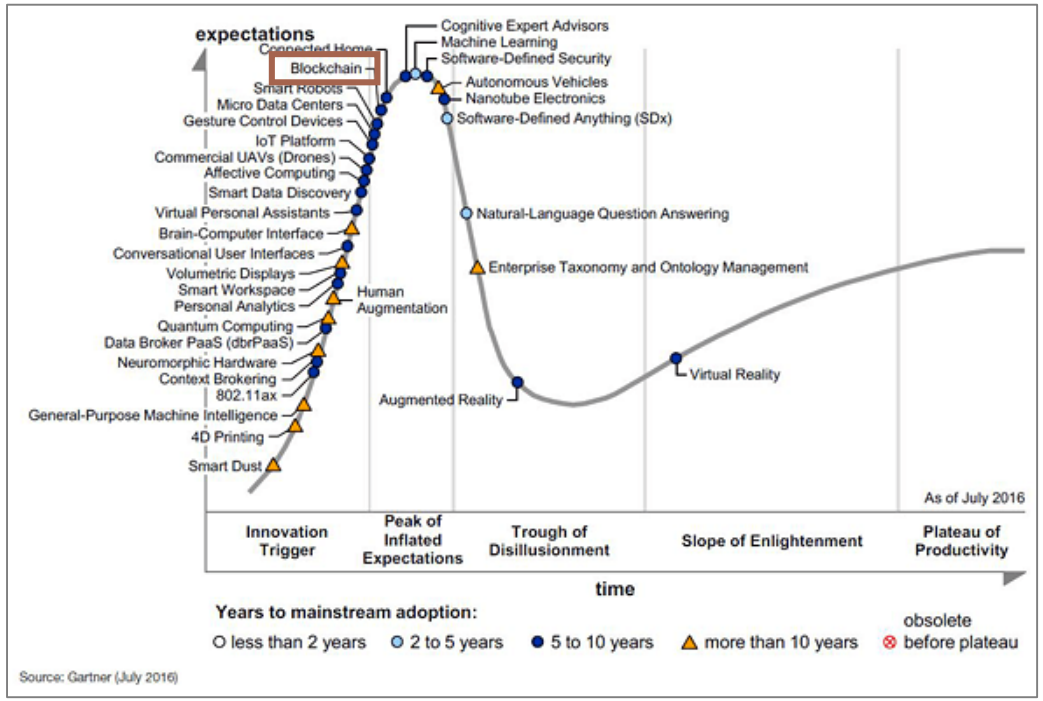


© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Das Blöken der Schafe

Gartner Hype Cycle 2015 - 2016

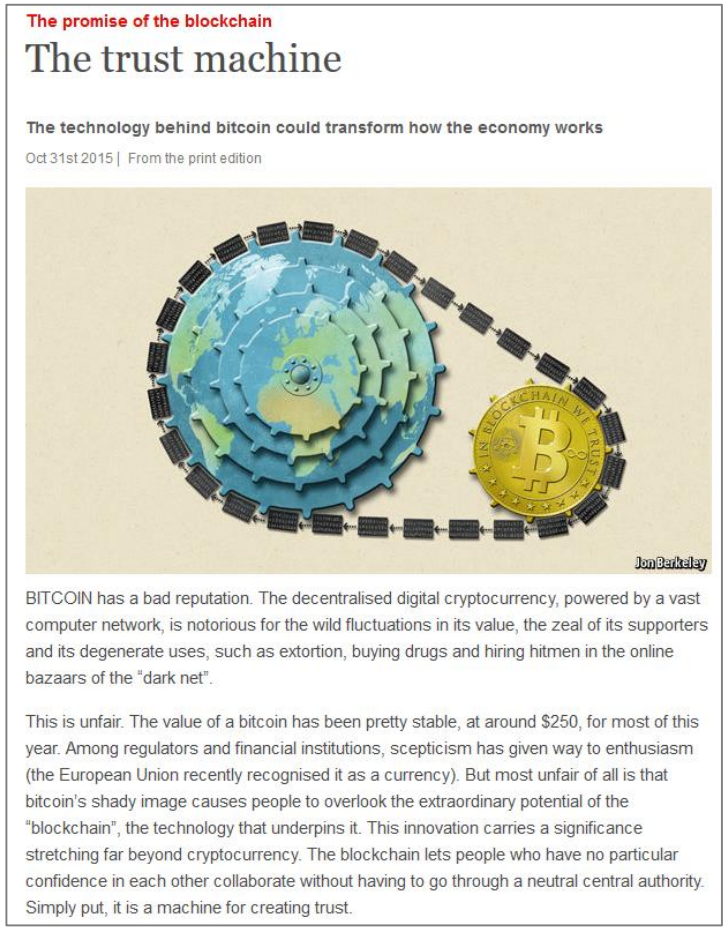




© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Vertrauensmaschine Bitcoin

Sexiest invention since double-entry book-keeping



The promise of the blockchain

The trust machine

The technology behind bitcoin could transform how the economy works

Oct 31st 2015 | From the print edition

Jon Berkeley

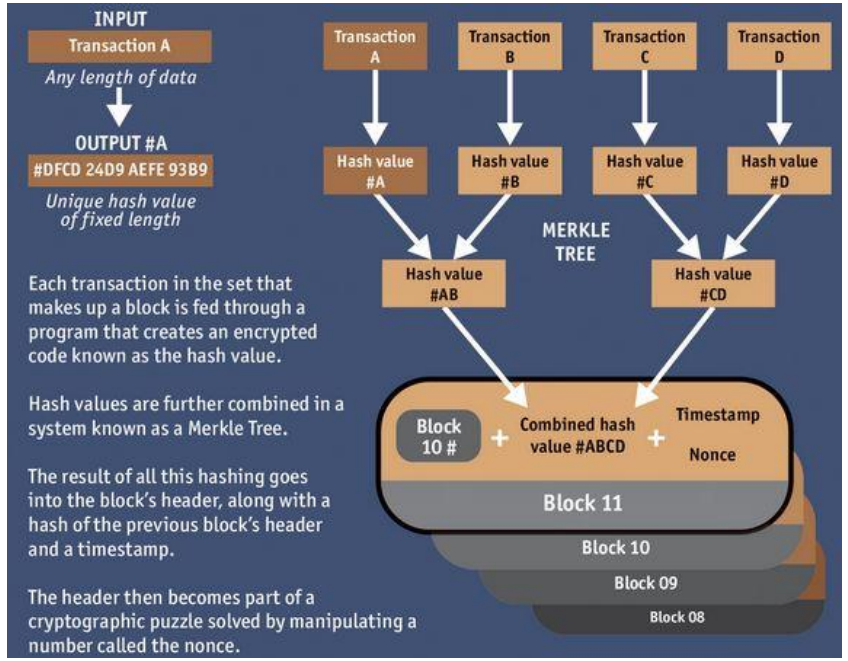
BITCOIN has a bad reputation. The decentralised digital cryptocurrency, powered by a vast computer network, is notorious for the wild fluctuations in its value, the zeal of its supporters and its degenerate uses, such as extortion, buying drugs and hiring hitmen in the online bazaars of the "dark net".

This is unfair. The value of a bitcoin has been pretty stable, at around $250, for most of this year. Among regulators and financial institutions, scepticism has given way to enthusiasm (the European Union recently recognised it as a currency). But most unfair of all is that bitcoin's shady image causes people to overlook the extraordinary potential of the "blockchain", the technology that underpins it. This innovation carries a significance stretching far beyond cryptocurrency. The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. Simply put, it is a machine for creating trust.

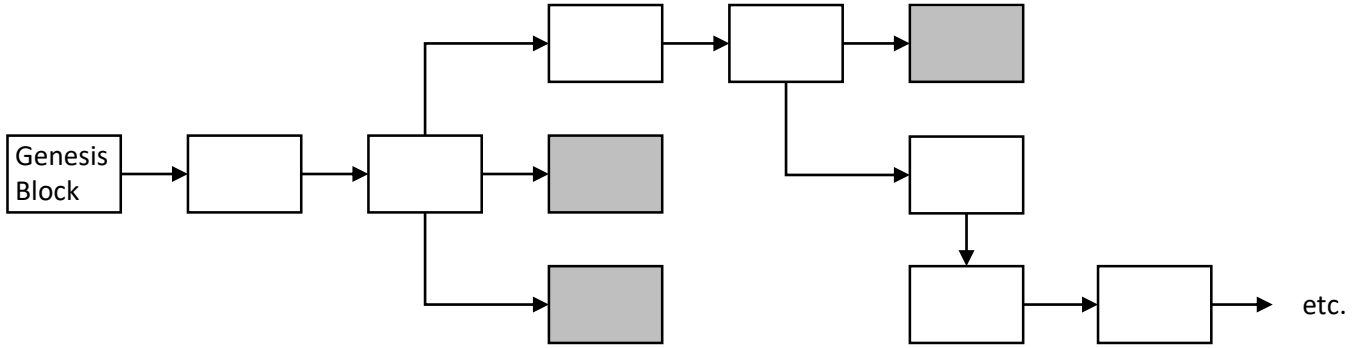
© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Bitcoin-Genetik: Es werde Geld

Proof of Work-Mining: Internationales Rätselrennen



economist 31.10.15



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Kryptographische Falltürfunktionen

Rätsel auf Basis von SHA256

Hello World
`a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e` Hashcode (“Fingerprint“)

Hello World.
kleine Ursache, große Wirkung
`f4bb1975bf1f81f76ce824f7536c1e101a8060a632a52289d530a6f600d52c92`

Hello World.**1**
„Nonce“. **Rätsel: mit welcher „number used once“ erhält man eine führende 0 im Hash?**
`C62fcf178bce4c73a6982f9524bd2015bbe0afe81637cb393c0289ece672a142`

Hello World.2
`3988a8f9a73e2a72474e1d5065d552e3dc56e8cbd214a9158e90e3e79cca6364`

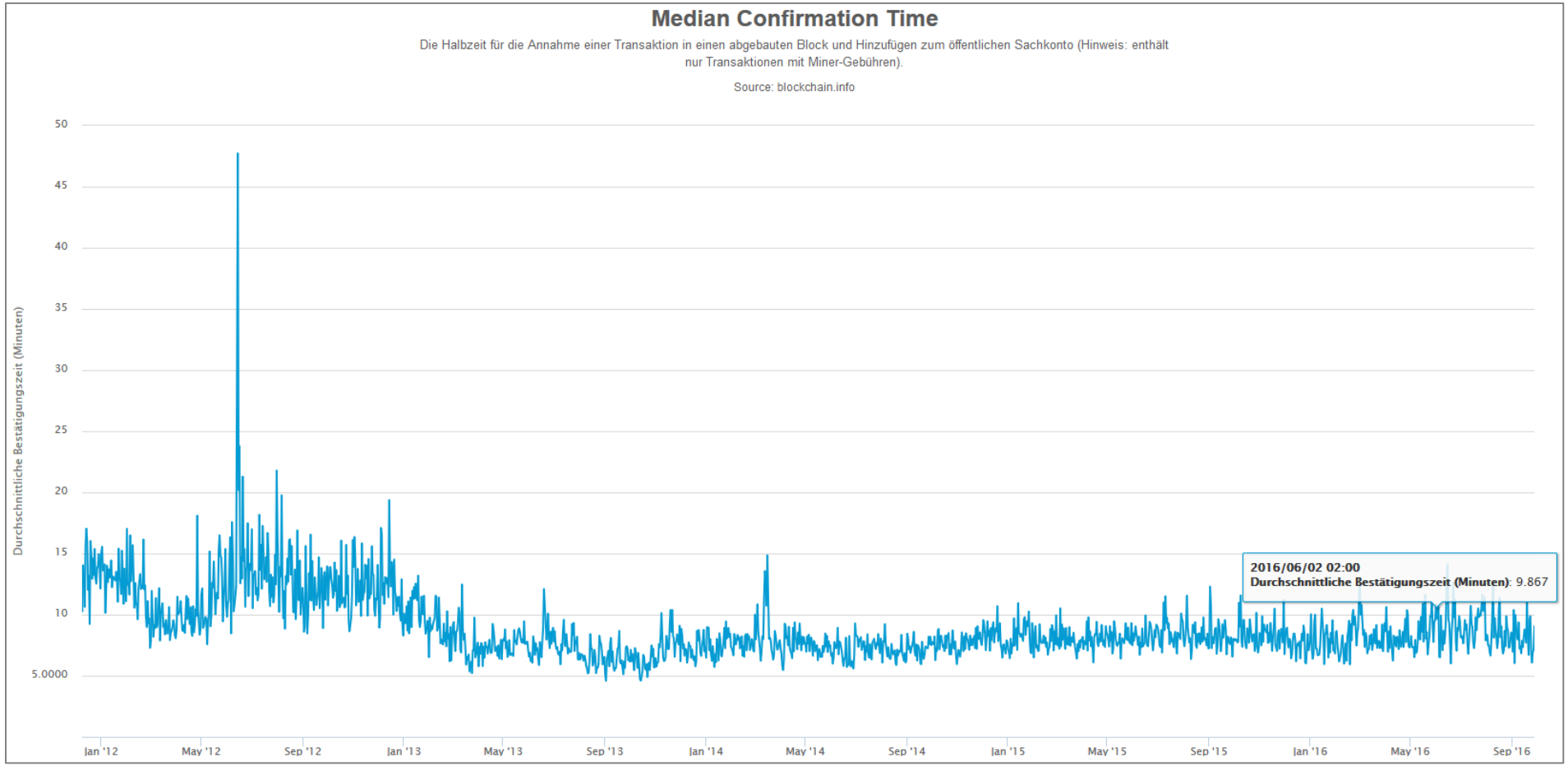
…

Hello World.26
`0260cc2d164dac27a9640a0116ea8e63771fd0ca03bd4366d690c33dec39543e`

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Vertrauen = f(Schwierigkeitsgrad)

Empfehlung Nakamoto: 10 min. Lösungsbedarf



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Bitcoinstatus am 30.09.16, 06:20

432.173 Blöcke

BLOCKCHAIN info | Startseite | Charts | Statistiken | Märkte | API | Wallet | Suche

Startseite Die aktuell gefundenen Blöcke in der Bitcoin Blockchain

Höhe	Alter	Transaktionen	Insgesamt gesendet	Weitergeleitet von	Größe (kB)
432173	2 minutes	1767	14,055.90 BTC	BitClub Network	998.1
432172	5 minutes	2381	15,426.01 BTC	BitClub Network	998.06
432171	14 minutes	2560	37,480.61 BTC	BTCC Pool	998.93
432170	50 minutes	2458	26,740.92 BTC	Unknown	933.12
432169	1 hour 8 minutes	2145	15,362.43 BTC	AntPool	998.09
432168	1 hour 28 minutes	1597	13,512.22 BTC	BTCC Pool	998.77

Neueste Transaktionen

b9fcca7abfa10f253511d6ca8...	< 1 minute	0.46722881 BTC
0056b837b1b840f651d29103d...	< 1 minute	0.77123072 BTC
d07af297e072b44952218de62...	< 1 minute	299.6566 BTC

Suchen

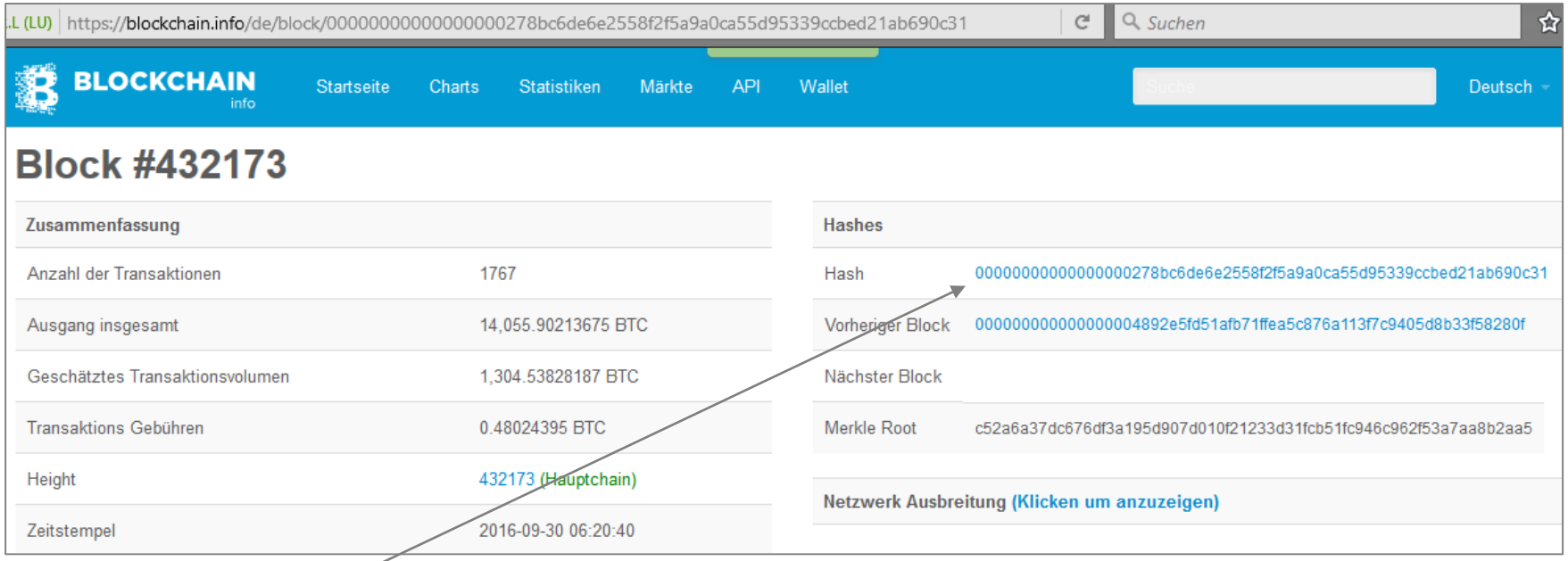
Hier können Sie nach Blockhöhe, Adresse, Blockhash, Transaktions-Hash, hash1 IPv4-Adresse suchen.

Adresse / Firstbits / IP / SHA-Hash | Search

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Aktuelle Lösungswahrscheinlichkeit

$3{,}4 * 10^{-21}$



0000000000000000278bc6de6e2558f2f5a9a0ca55d95339ccbed21ab690c31

17 führende hexadezimale Nullen

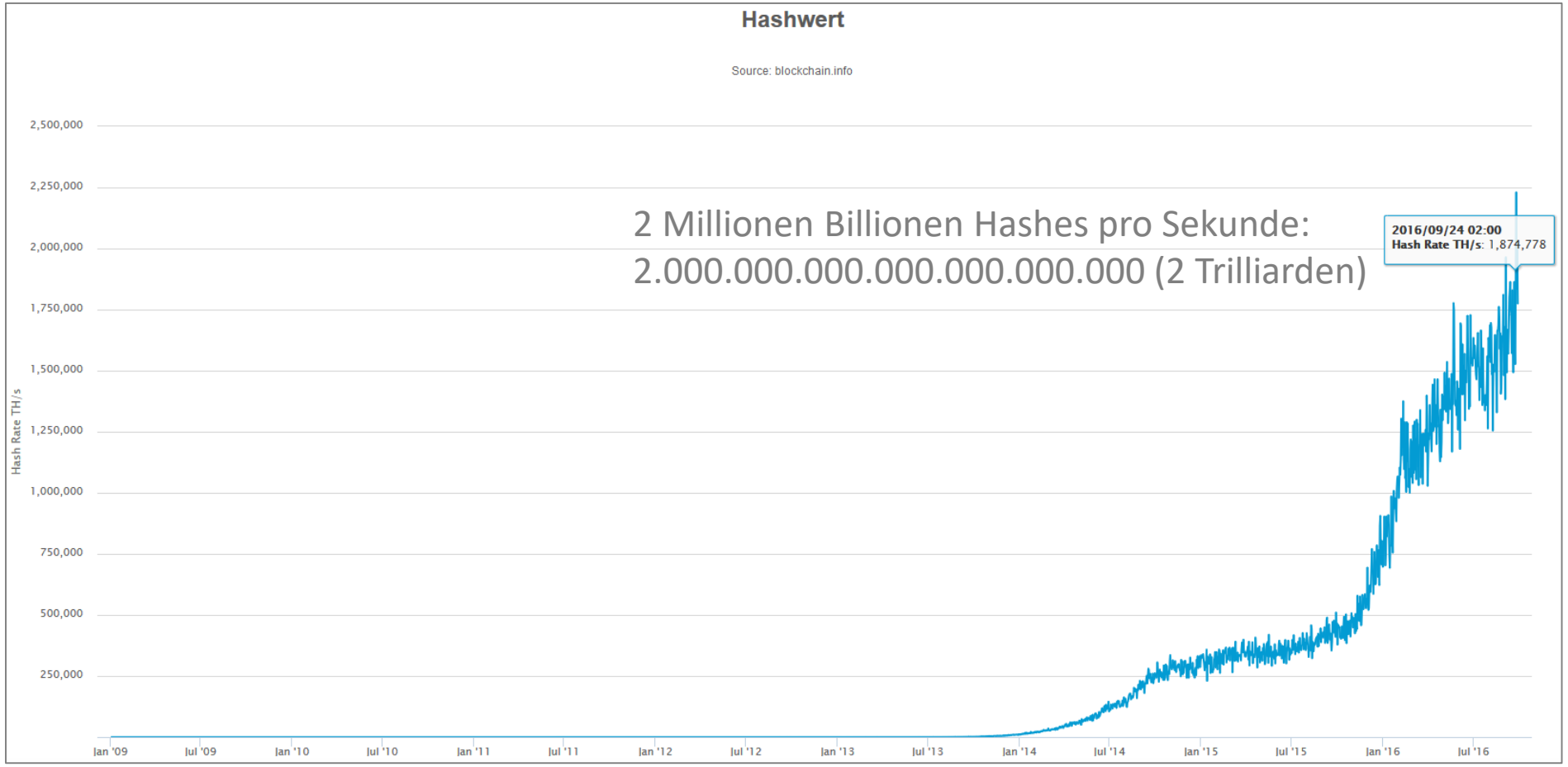
$\Rightarrow$ theoretische Wahrscheinlichkeit = $\left(\frac{1}{16}\right)^{17}$ = 0,0000000000000000000034

$\Leftrightarrow$ Gewinnwahrscheinlichkeit Lotto (6 aus 49) = 0,000000072

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Entwicklung der Netzwerk-Leistung

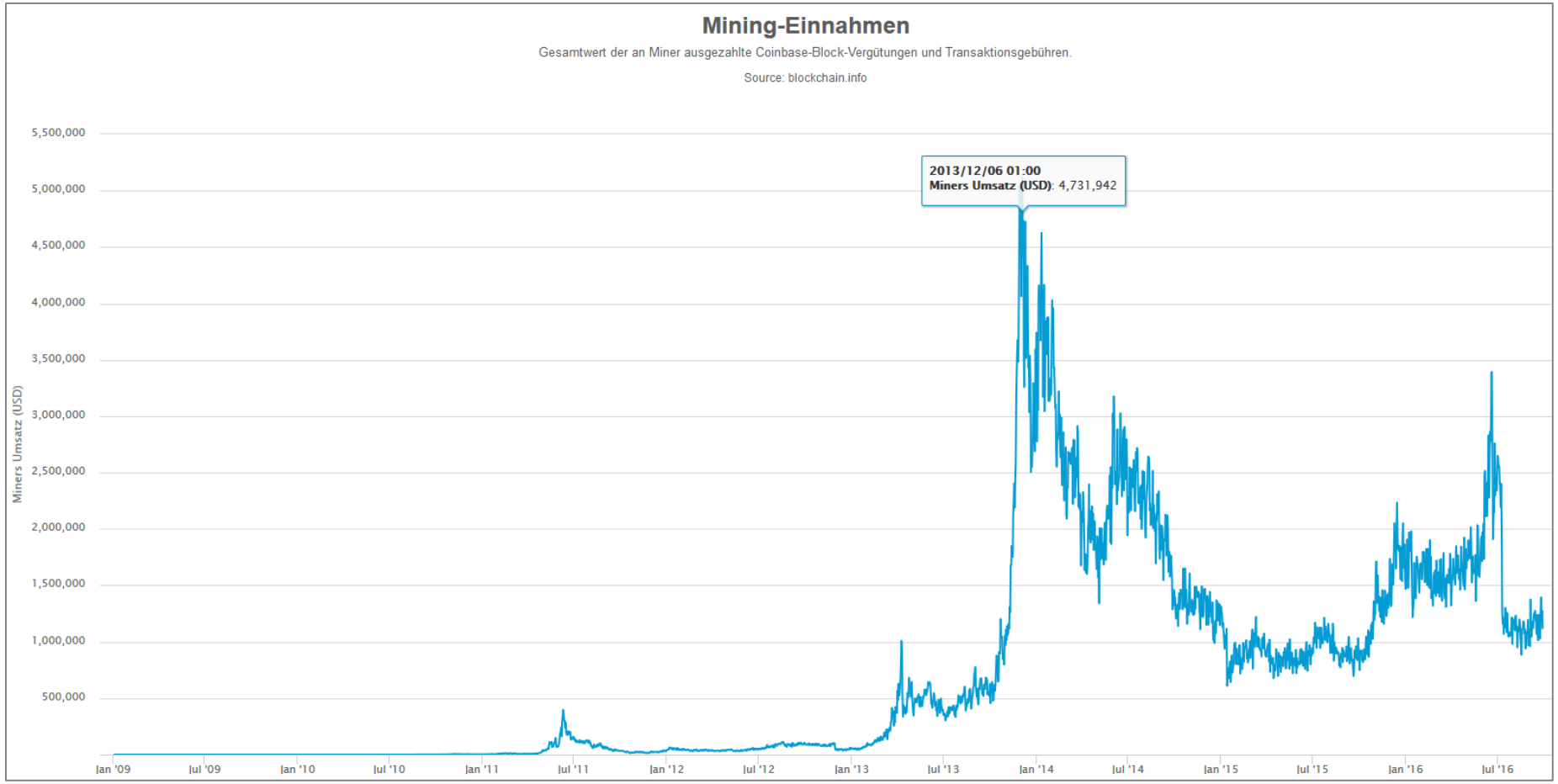
Tera (T) = 10^{12}



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Digitaler Goldrausch

bis zu 5 Mio USD pro Tag



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

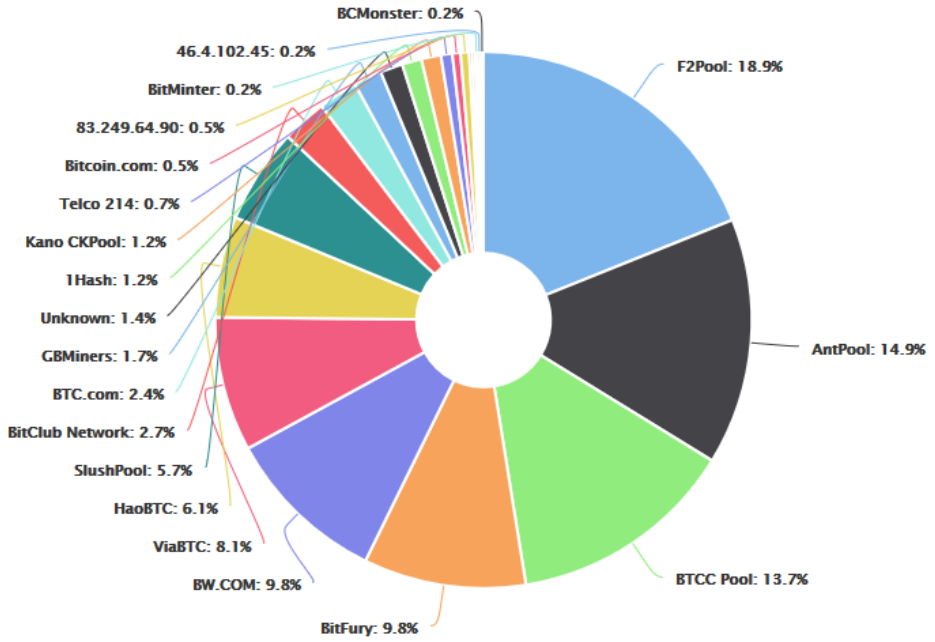
Koordinierte Bemühungen

CPUs → GPUs → ASICs und Mining-Pools (incl. Bot-Netze)

Hashrate Verteilung Eine Abschätzung der Hashrate-Verteilung unter den größten Mining-Pools

Das folgende Diagramm zeigt den Marktanteil der größten Bitcoin Mining Pools. Es sollte jedoch nur für eine grobe Abschätzung verwendet werden und ist aus verschiedenen Gründen nicht zu 100% korrekt.

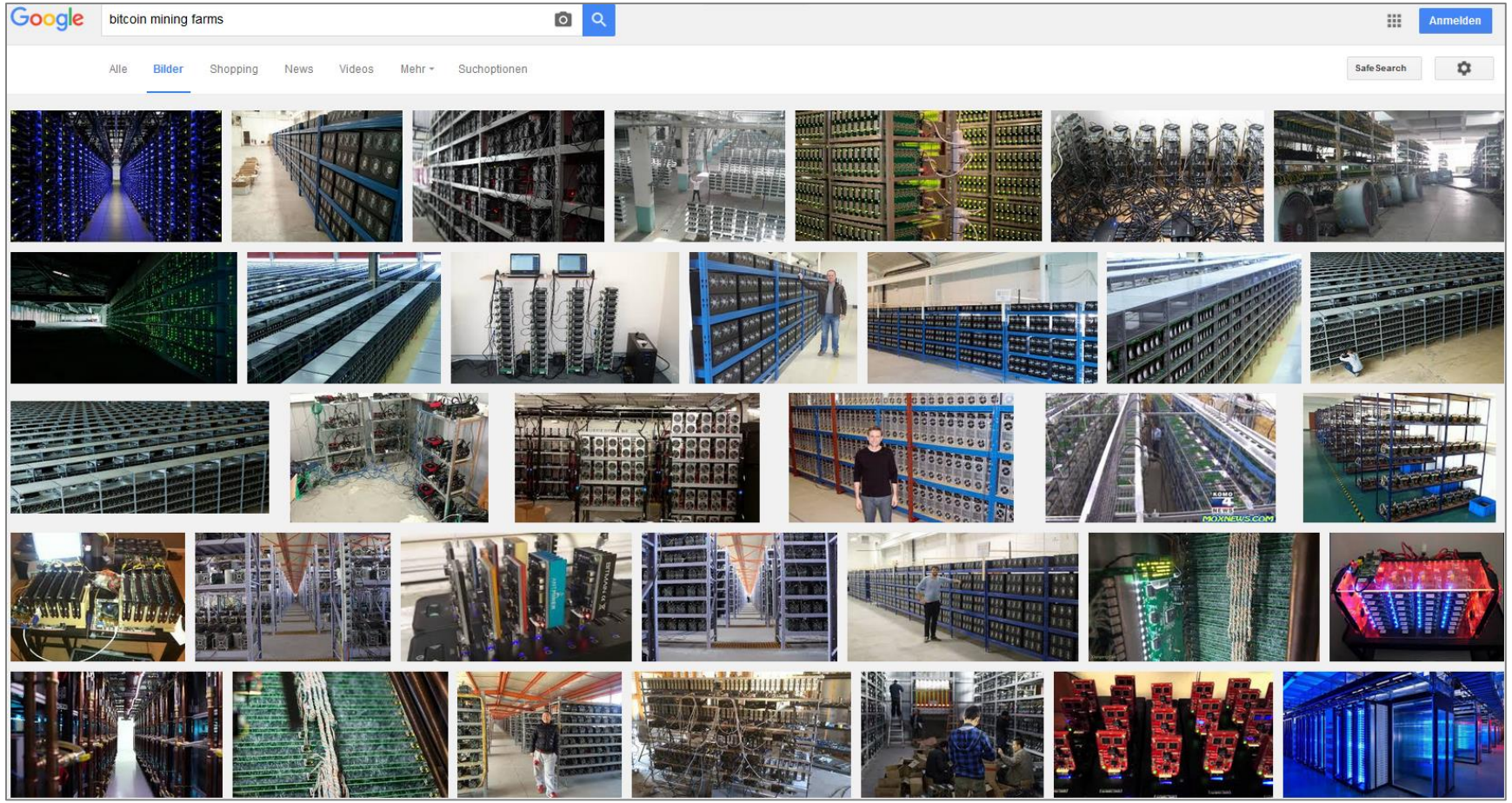
24 Stunden - 48 Stunden - 4 Tage



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Serverfarmen

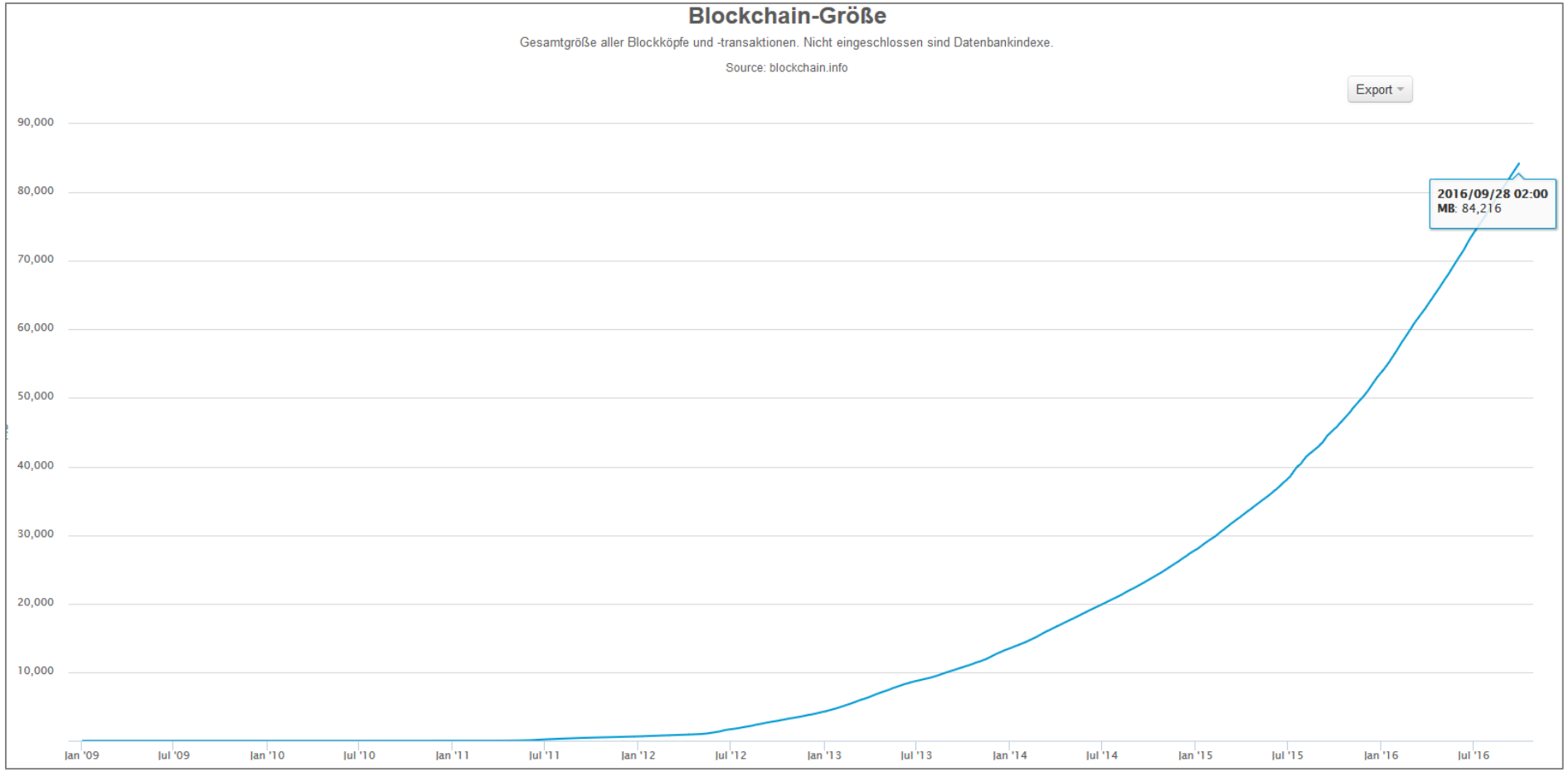
bis zweistellige Millionengewinne p. Mt.



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Exponentiell korrespondierende Komplexität

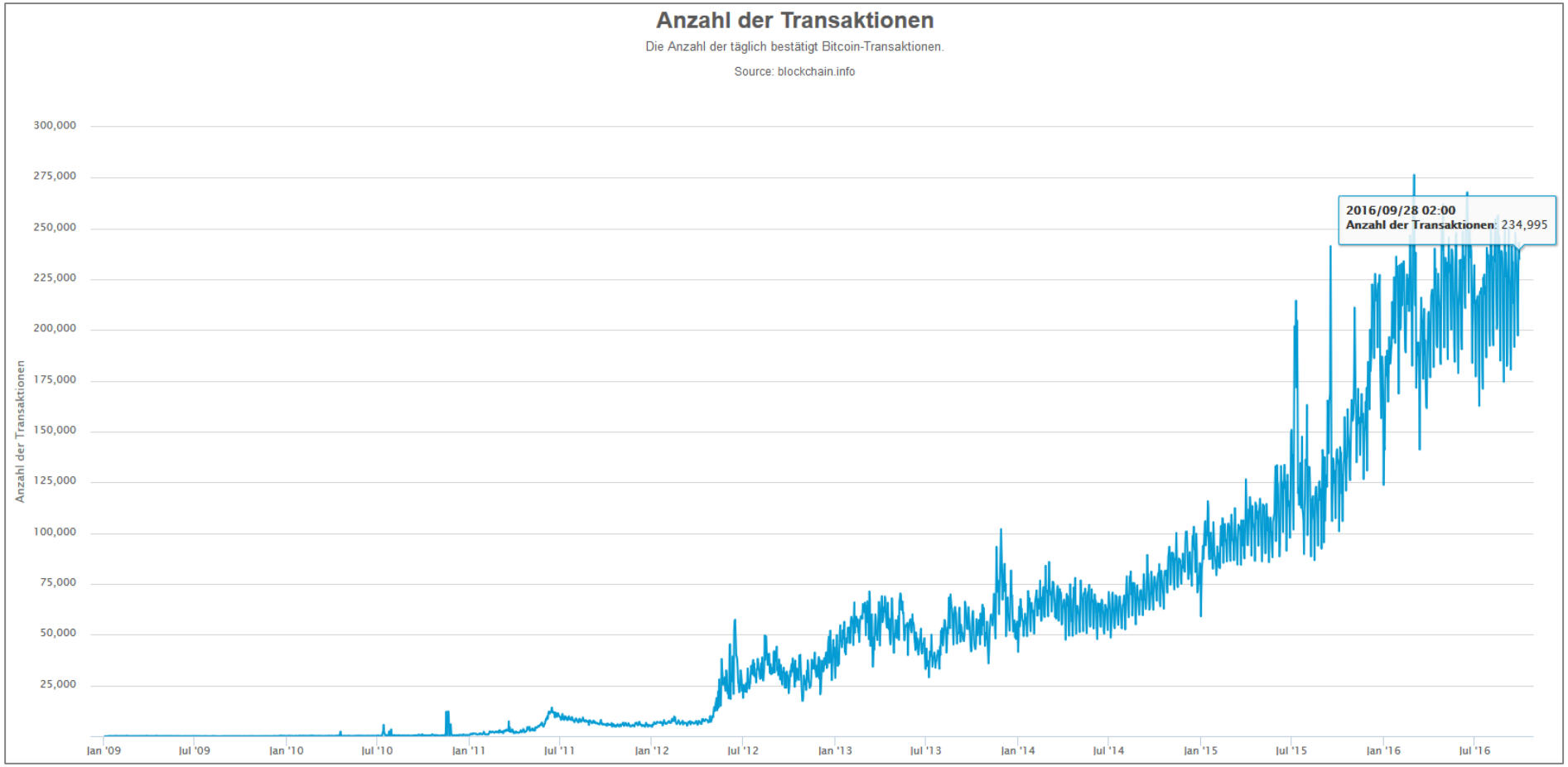
aktuelle Blockchain-Größe ca. 85 GB



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Anzahl bestätigter Transaktionen pro Tag

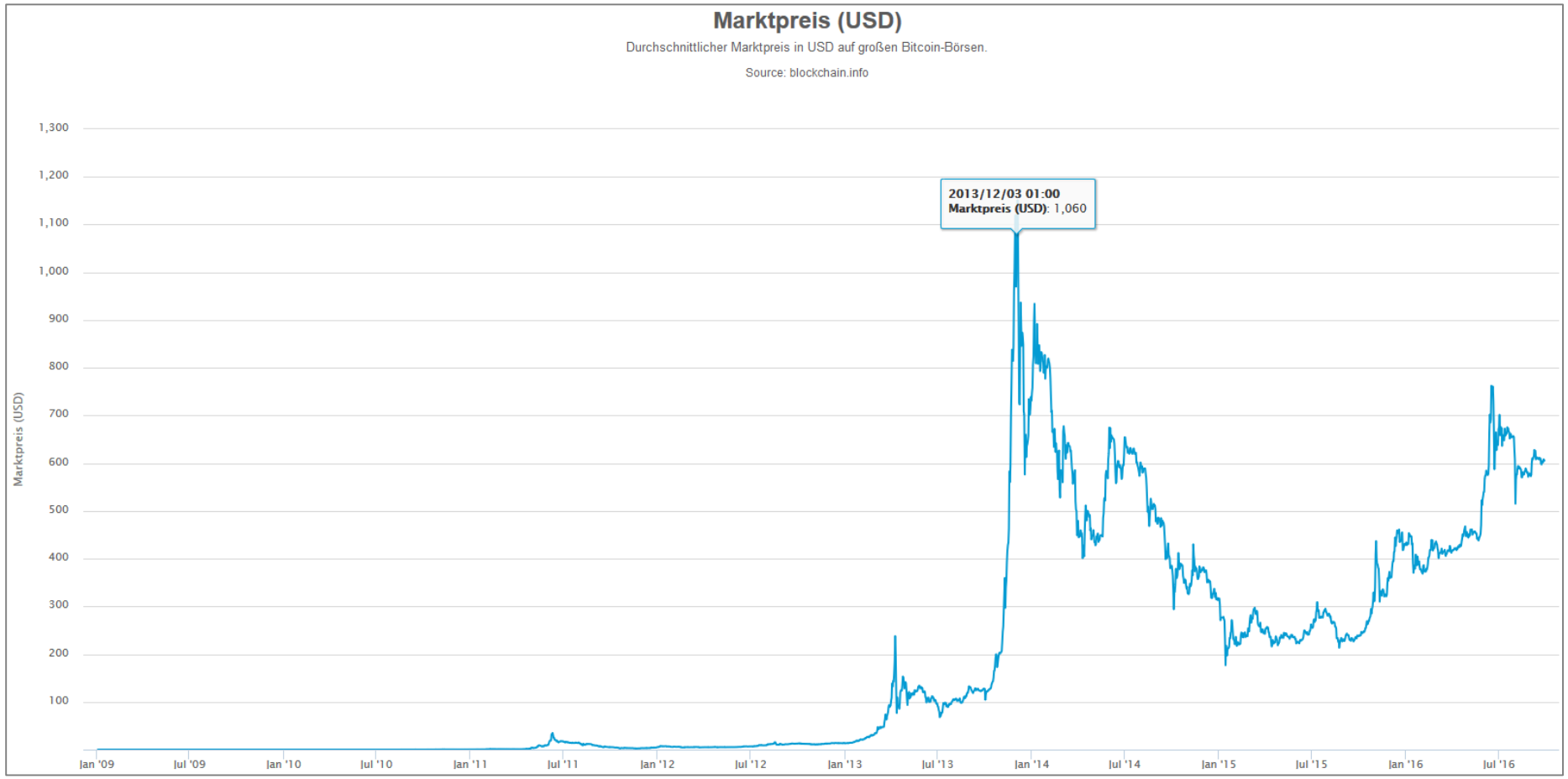
aktuell ca. 235.000



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Bitcoin-Kursentwicklung

aktuell ca. 500 USD



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

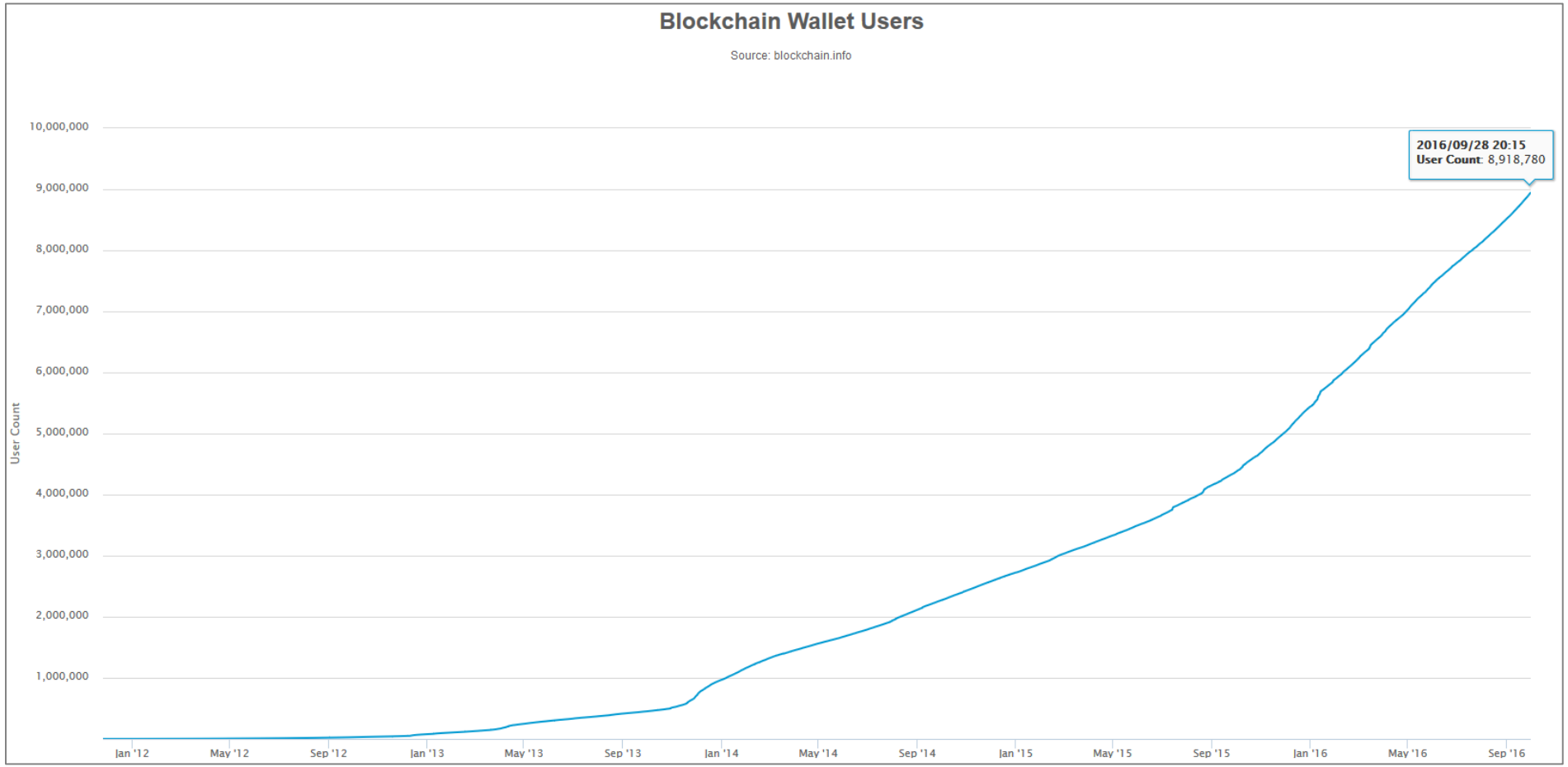
Bitcoin-Marktkapitalisierung

aktuell ca. 10 Mrd. USD

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Bitcoin-Userentwicklung

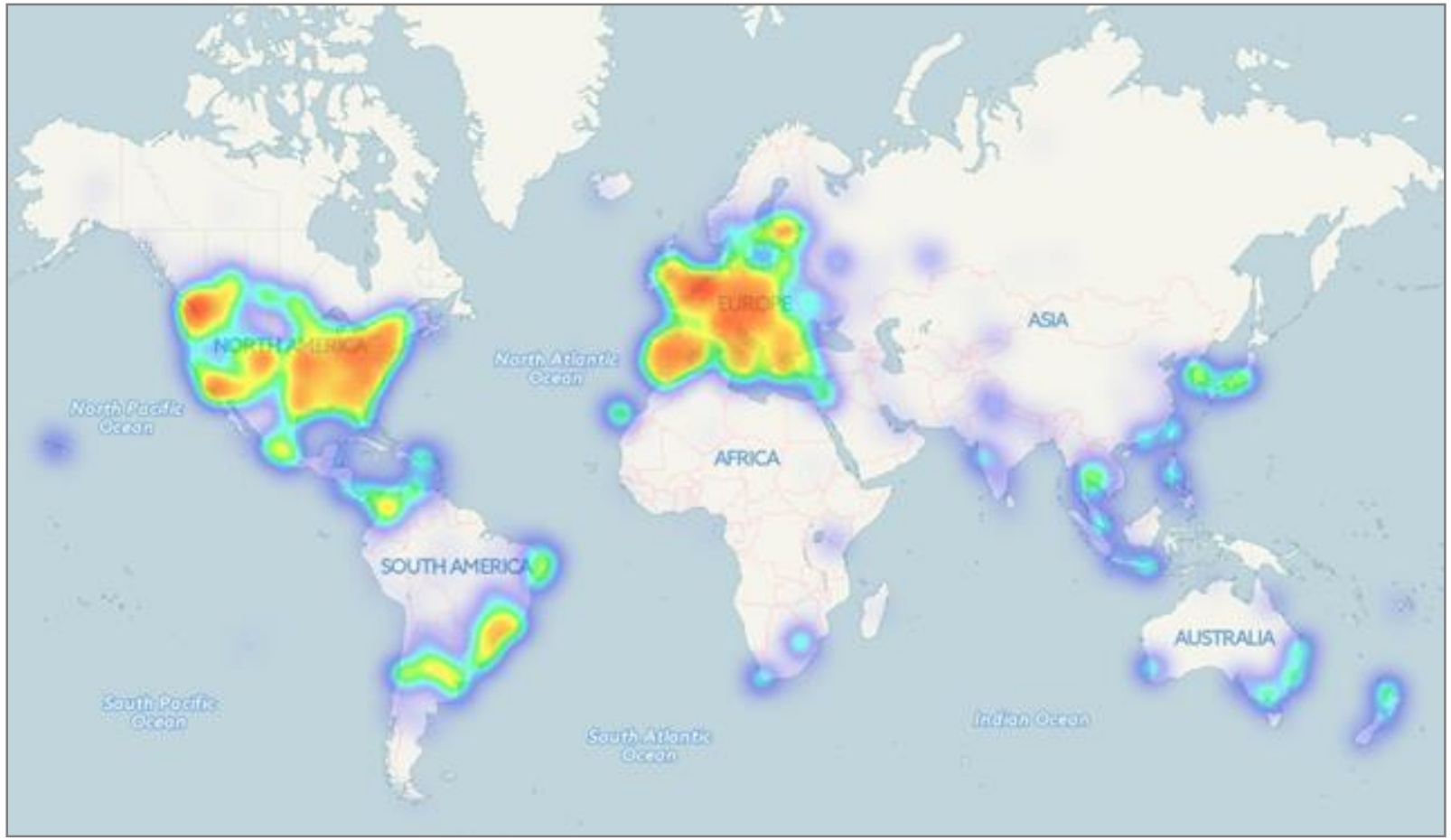
aktuell ca. 9 Mio. Keychains



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Internationale Akzeptanz als Zahlungsmittel

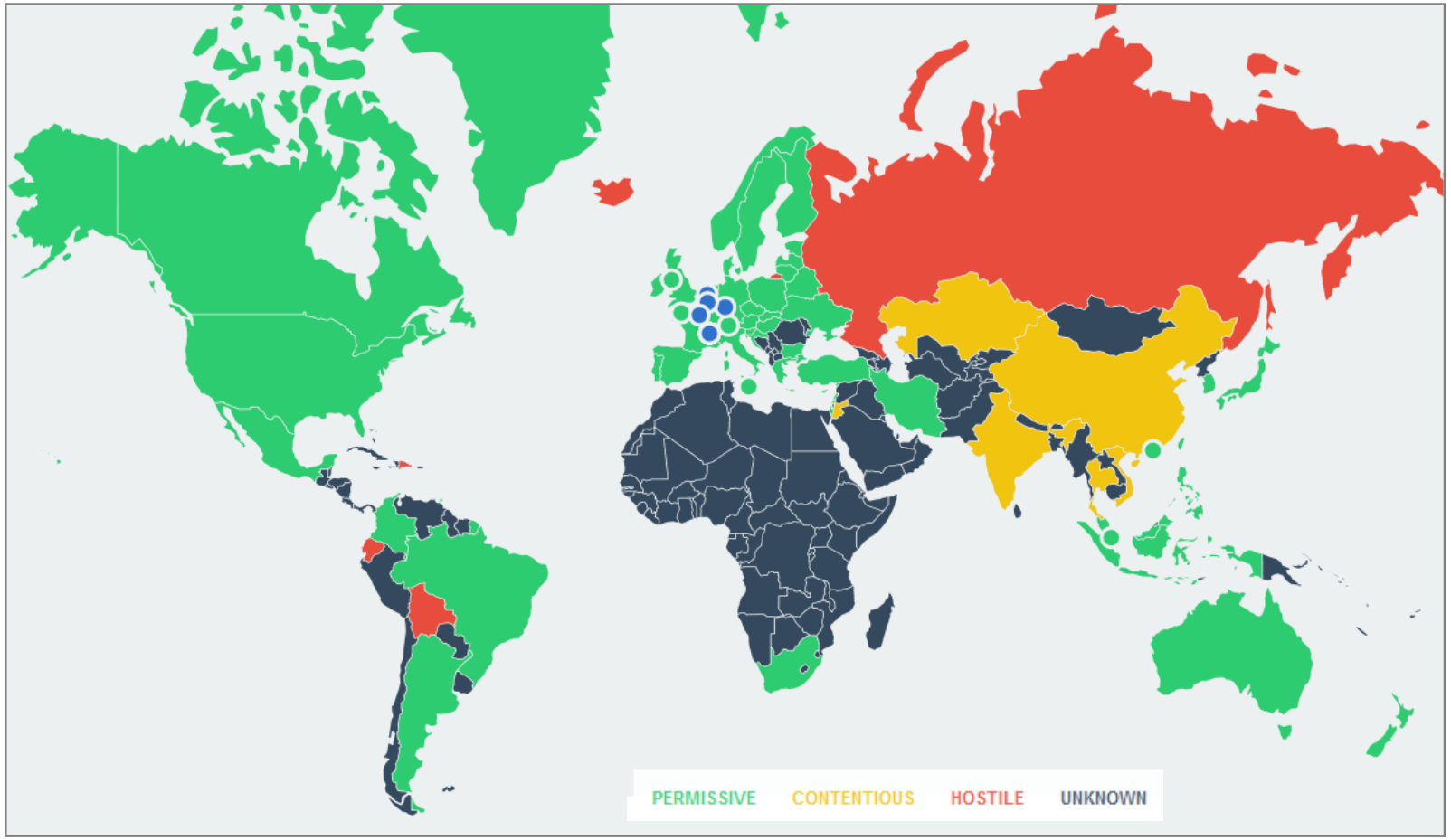
aktuell 8.222 Marktteilnehmer (Stand 4.10.16)



coinmap.org

Regulierungsstatus

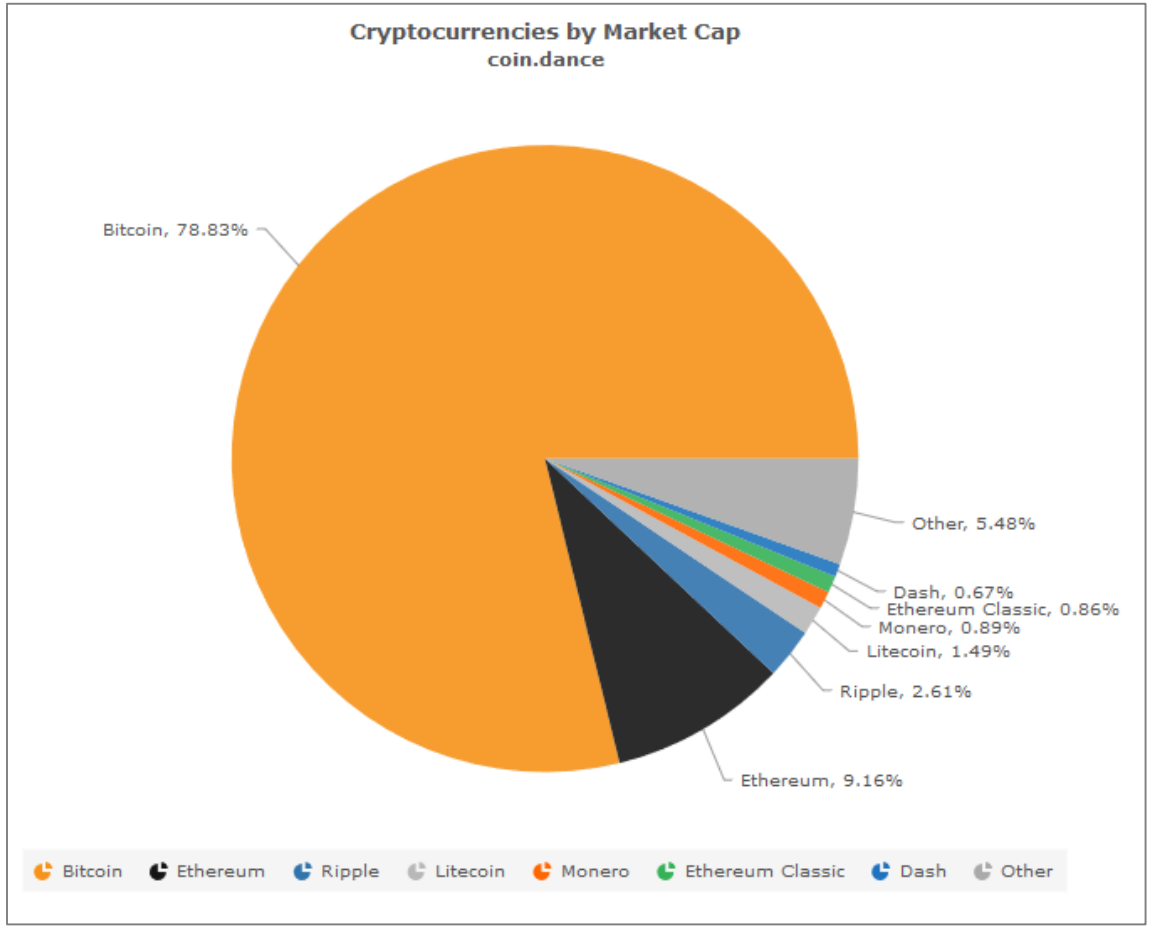
map.bitlegal.io



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

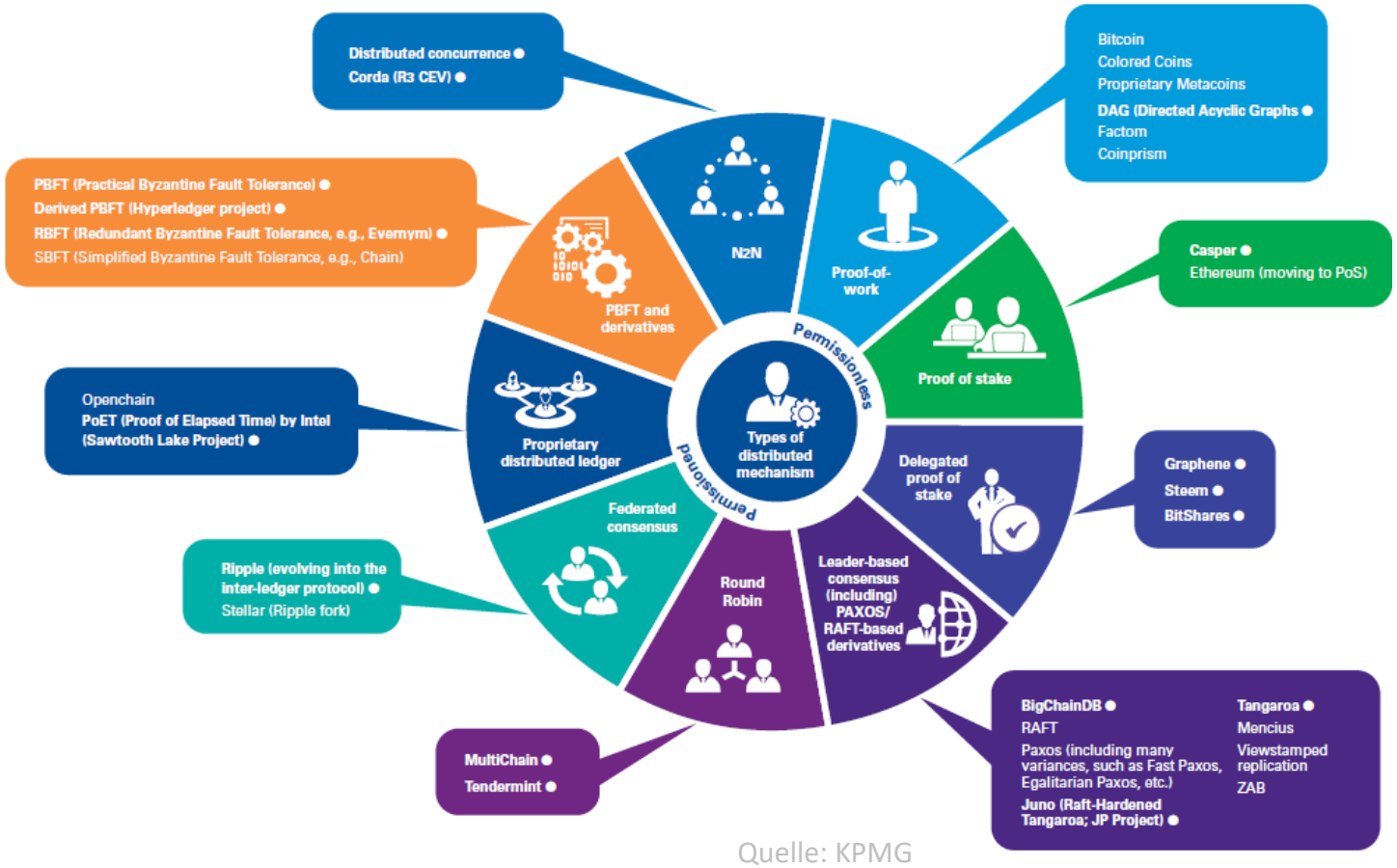
Marktübersicht Kryptowährungen

Unzählige Derivate



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Bunte Beispielkategorisierung von Konsens- und Nonsensemechanismen



Quelle: KPMG

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent m

et cetera...

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Der Vater von Skynet?

Vitalik Buterin, Gründer Ethereum

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Ethereum‘s greater fools

Wertentwicklung ETH seit meiner Empfehlung vom 10.10.15: zwischen 1.600 % und 4.200 % Gewinn

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Inspirierender Dämon

Vision: unaufhaltsame Maschinen

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Ethereum Vision

Supposedly unstoppable Smart-Contract-Applications

Build unstoppable applications

Ethereum is a **decentralized platform that runs smart contracts:** applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.

These apps run on a custom built **blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property.** This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk.

The project was bootstraped via an ether pre-sale during August 2014 by fans all around the world. It is developed by the Ethereum Foundation, a Swiss nonprofit, with contributions from great minds across the globe.

On traditional server architectures, every application has to set up its own servers that run their own code in isolated silos, making sharing of data hard.

If a single app is compromised or goes offline, many users and other apps are affected.

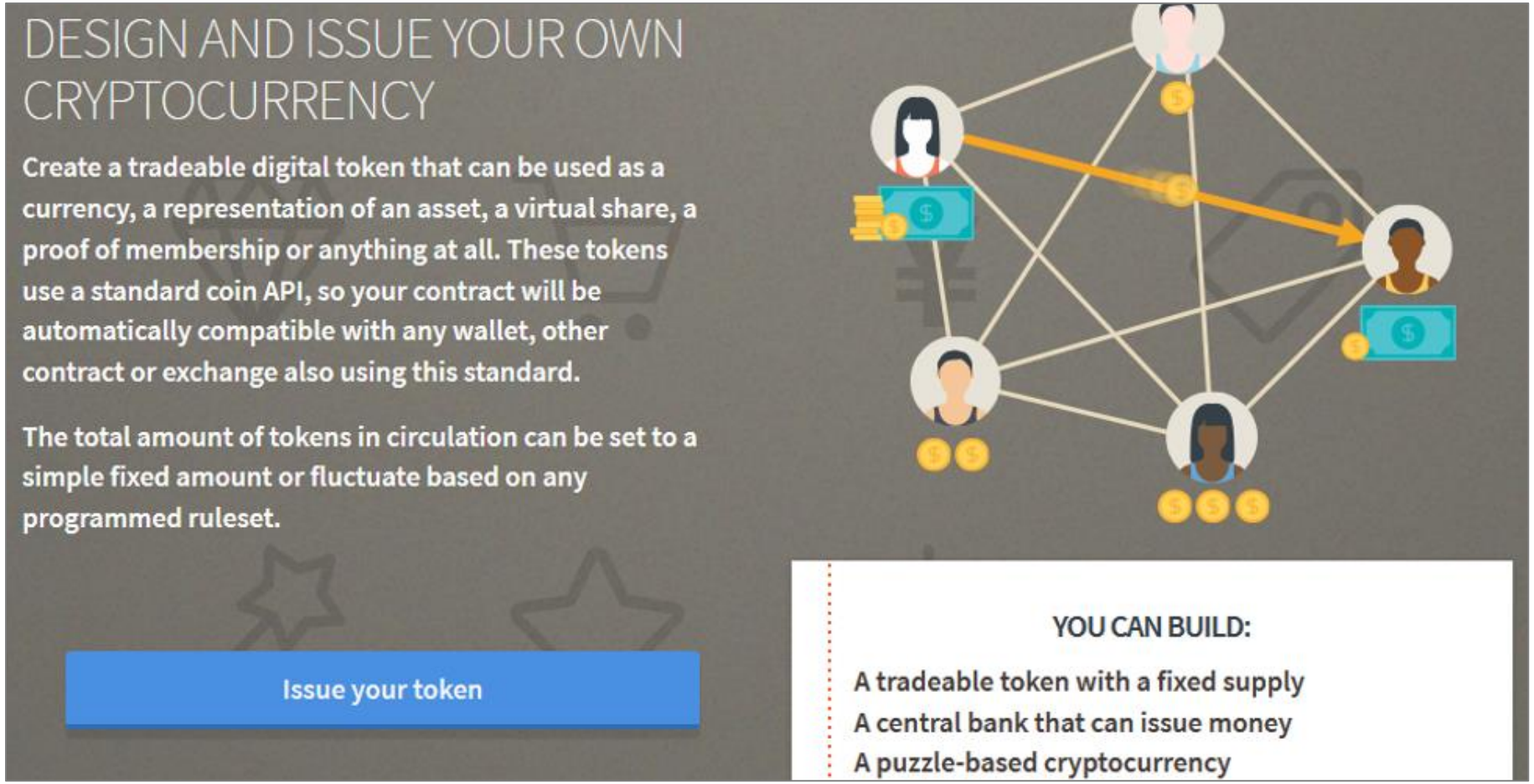
On a blockchain, anyone can set up a node that replicates the necessary data for all nodes to reach an agreement and be compensated by users and app developers.

This allows user data to remain private and apps to be decentralized like the Internet was supposed to work.

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Ethereum Vision

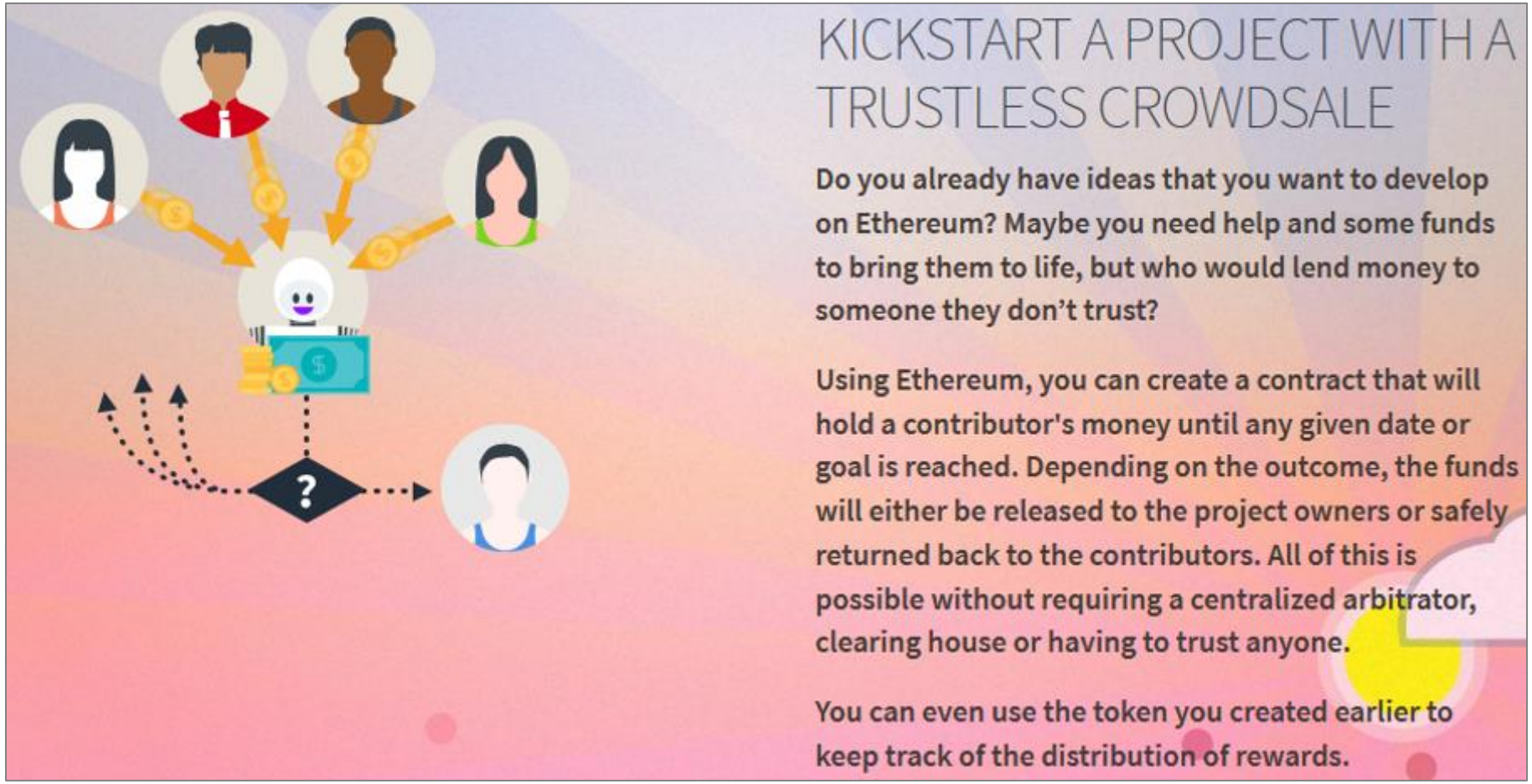
Jedem seine eigene Währung: die „Altcoin“-Übermutter



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Ethereum Vision

Trustless Crowdsales...



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

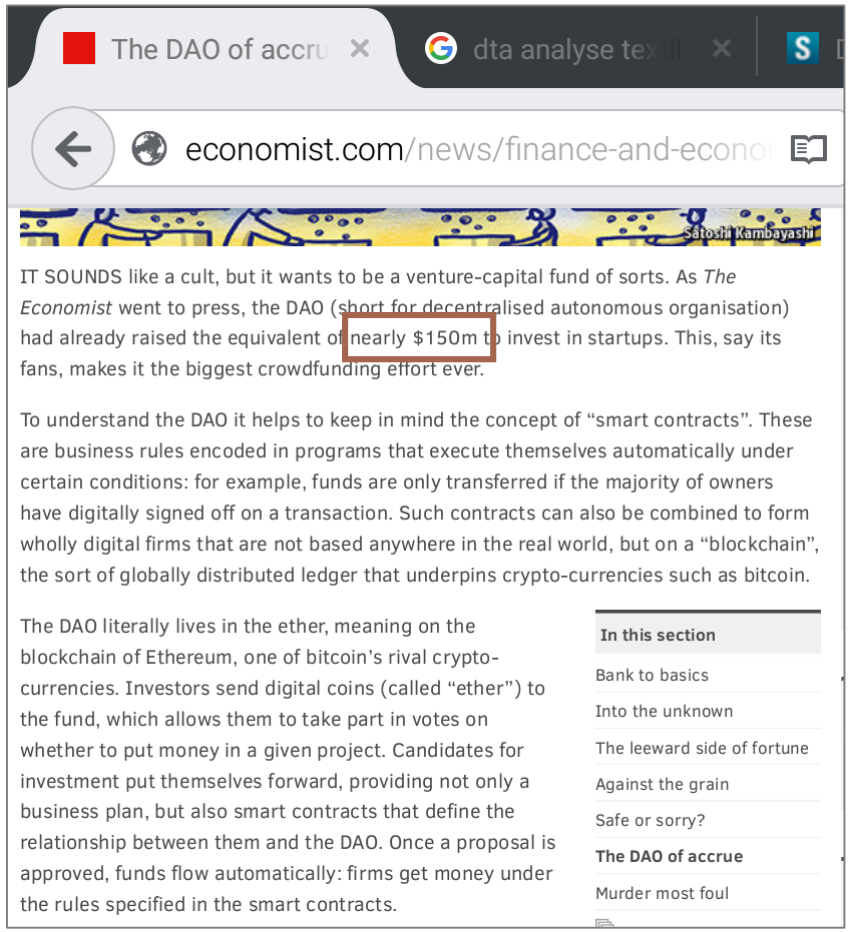
Ethereum Vision

… bis hin zu dezentralen autonomen Organisationen

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

The DAO: ein virtueller Venture Capitalist

Bis dato erfolgreichstes Crowdfunding-Projekt aller Zeiten(!)



The DAO of accru

dta analyse tex

economist.com/news/finance-and-econo

Satoshi Kambayashi

IT SOUNDS like a cult, but it wants to be a venture-capital fund of sorts. As *The Economist* went to press, the DAO (short for decentralised autonomous organisation) had already raised the equivalent of nearly $150m to invest in startups. This, say its fans, makes it the biggest crowdfunding effort ever.

To understand the DAO it helps to keep in mind the concept of "smart contracts". These are business rules encoded in programs that execute themselves automatically under certain conditions: for example, funds are only transferred if the majority of owners have digitally signed off on a transaction. Such contracts can also be combined to form wholly digital firms that are not based anywhere in the real world, but on a "blockchain", the sort of globally distributed ledger that underpins crypto-currencies such as bitcoin.

The DAO literally lives in the ether, meaning on the blockchain of Ethereum, one of bitcoin's rival crypto-currencies. Investors send digital coins (called "ether") to the fund, which allows them to take part in votes on whether to put money in a given project. Candidates for investment put themselves forward, providing not only a business plan, but also smart contracts that define the relationship between them and the DAO. Once a proposal is approved, funds flow automatically: firms get money under the rules specified in the smart contracts.

In this section

Bank to basics

Into the unknown

The leeward side of fortune

Against the grain

Safe or sorry?

The DAO of accrue

Murder most foul

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

The DAO: ein virtueller Venture Capitalist…

… der grundlegende Fragestellungen aufwirft

Mitte Juni machte DAO Schlagzeilen, weil ein bisher Unbekannter das Projekt um 56 Mio. US-Dollar „virtuell beraubte". Ob es tatsächlich ein Raub war oder nur eine Umbuchung, die zwar unerwartet war, jedoch den DAO-Regeln entsprach, ist unter Fachleuten umstritten. Einige schreiben, der Angreifer habe einen Fehler im Programmcode genutzt und das Geld ohne Zustimmung der anderen DAO-Investoren in eine Art „Tochtergesellschaft" abzweigen können. Dort war es dem Zugriff der anderen Anteilseigner entzogen. Der vermeintliche Angreifer selbst spricht davon, er habe nur die Regeln der Smart Contracts ausgenutzt, weswegen man nicht von Diebstahl sprechen könne. Er habe nur vertragskonforme Möglichkeiten genutzt.

DAO wurde mittlerweile unter Federführung der Entwickler auf eine sichere Ethereum-Adresse (WhiteHatDAO) übertragen, übrigens unter Ausnutzung der gleichen Lücke. Die Communities von DAO und Ethereum diskutieren über verschiedene weitere Maßnahmen. Es ist aber umstritten, ob diese im Einklang mit der bisherigen Philosophie von Smart Contracts stehen. Hier soll ja eigentlich gelten: "Code is law."

Das Konzept der Smart Contracts wegen der Probleme abzuschreiben, ist vollkommen verfrüht. Viele Innovationen in den letzten Jahrhunderten haben Jahre oder Jahrzehnte bis zur Anwendungsreife gebraucht. Man hat etwa die Weiterentwicklung des Autos auch nicht nach den ersten Unfällen eingestellt. Der Hype um die Blockchain war zu groß geworden und bisher hat kaum jemand über die praktischen Fragen konkreter Anwendungsfälle geredet. Das hat sich nun geändert und ist gut so. Gescheitert ist hier nichts. Erwachsen werden neue Technologien erst nach Rückschlägen.

Quelle: Capital, 30. Jun 2016, Dirk Elsner

Traduttore – traditore:
der Code ist der Vertrag

↓

Nutzung einer Codeschwäche
legal oder illegal?

Umstrittene Lösung:
hard fork

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Blockchain Graveyard

coulda, shoulda, woulda und IT-Darwinismus

https://magoo.github.io/Blockchain-Graveyard/

BLOCKCHAIN GRAVEYARD

These cryptocurrency institutions have suffered intrusions resulting in stolen financials, or shutdown of the product. Nearly all closed down afterward.

Nearly every attack could have been prevented:

- Social Engineering / Credential Reuse
- Account Takeover of Cloud Hosting
- Application Vulnerability

Each root cause is below, with a link to more information in the breach.

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Totgesagte…

Bitcoin Obituaries

Bitcoin has died 111 times

Obituary Stats | Submit Obituary

Stats:

Bitcoin has died:

111 times (and counting...)

Most Recent Death:

September 16, 2016 - Cryptocurrencies are Dead

Oldest Death:

December 15, 2010 - Why Bitcoin can't be a currency

www.bitcoinobituaries.com

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Mehr oder weniger robuste Blockchains, nicht ganz so robuste Ökosysteme

Bitfinex-Hack: 58 Millionen Euro gestohlen – Bitcoin-Kurs eingebrochen

Alle Heise-Foren > heise online > News-Kommentare > Bitfinex-Hack: 58 Millionen E... > Schnellste Weg um steuerfrei...

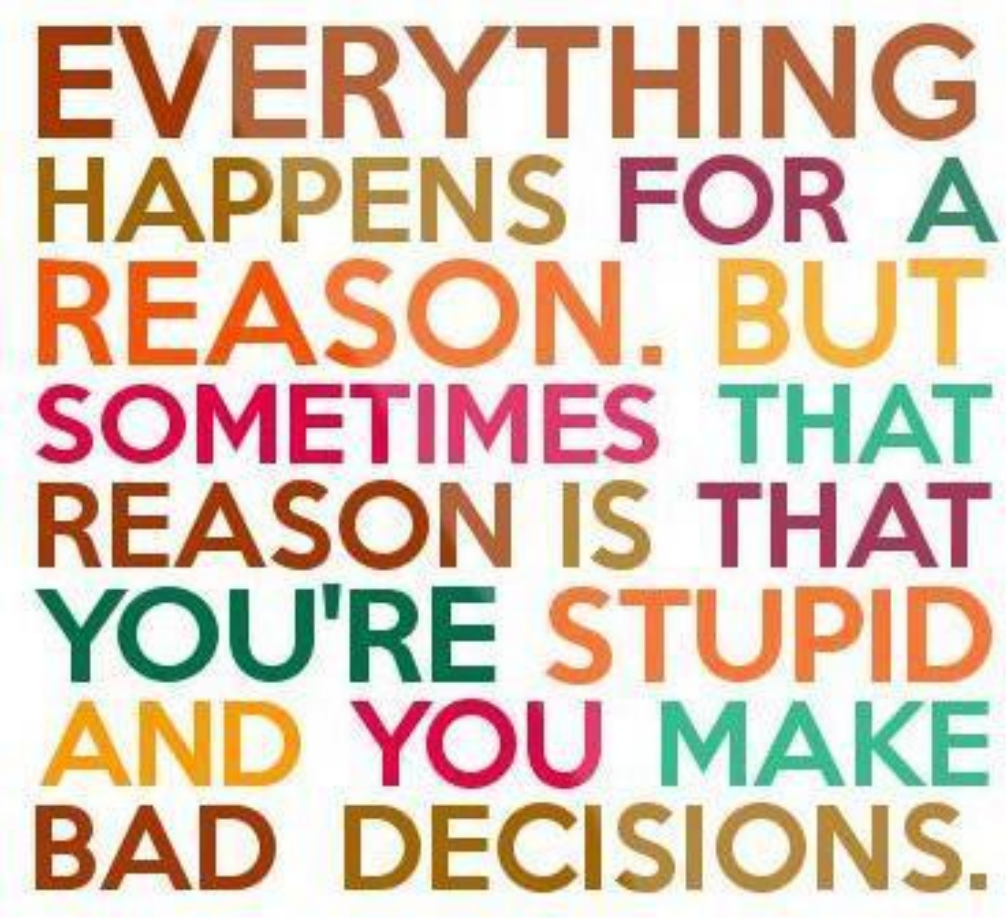
Beitrag | Thread | Antworten | Zitieren | E-Mail

Michael9
mehr als 1000 Beiträge seit 11.01.2000

03.08.2016 20:07

Schnellste Weg um steuerfrei Millionär zu werden? Gründe eine Crypto"bank"

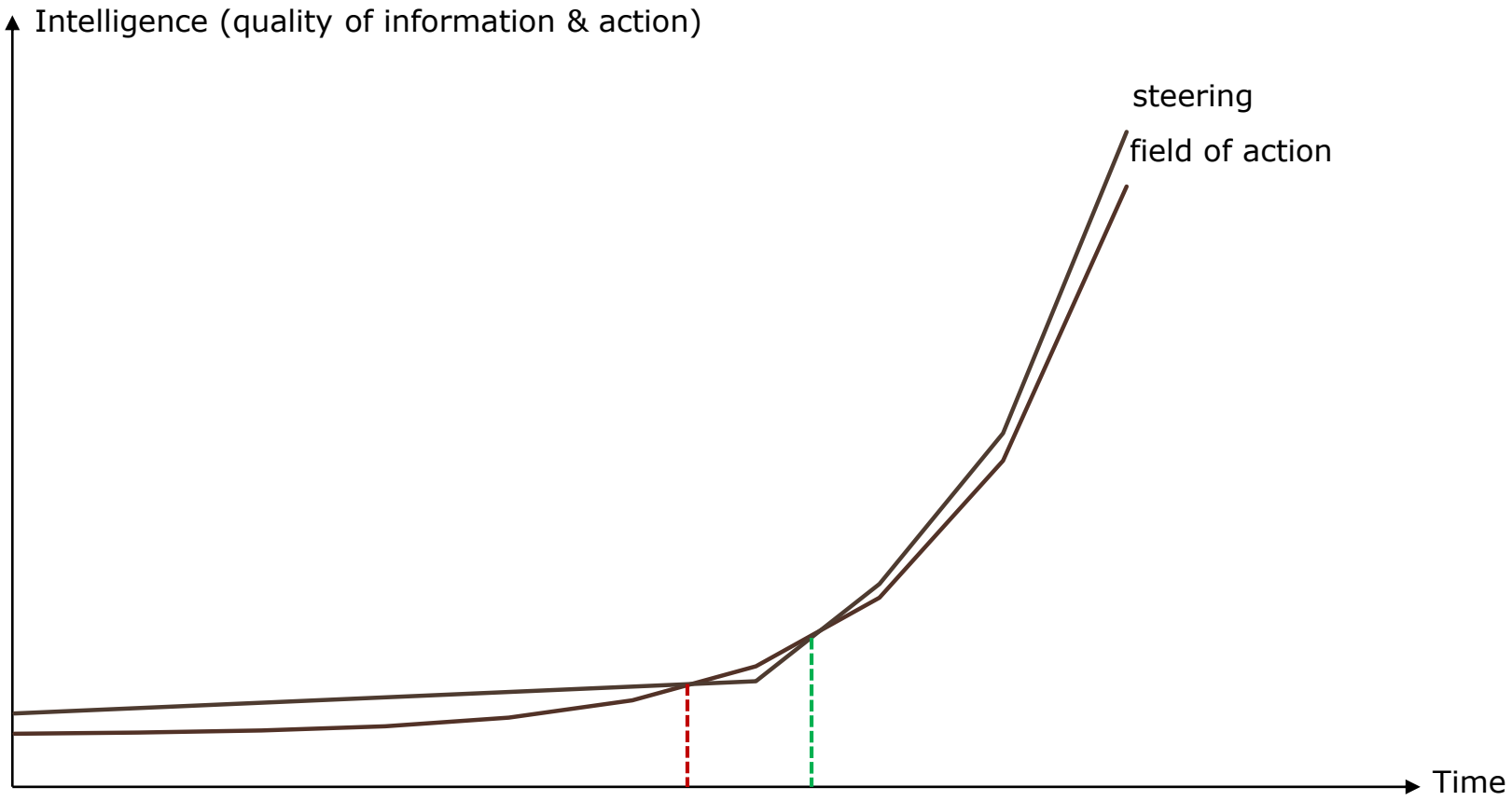
1. Schritt: Cooler Name
2. Schritt: Fasele was von tollen verschlüsselten Wallets und sonstigem Buzzword Bingo
3. Schritt: Hole dir Millionen, für die du defakto NULL juristisch verantwortlich bist
4. Schritt: Wenn sich deine Pseudo-Glaubwürdigkeit eingespielt hat, hast du ganz plötzlich einen sehr simplen bis sehr schwierigen Hack (je nach dem was du verkaufen kannst)
5. Schritt: Du erklärst x% des Geldes für verloren (ideal 90% sowas)
6. Schritt A: Wenn du zu viel Forderungen nach Schadensersatz bekommst, gehst du einfach in den Bankrott. Wichtig ist hier, dass deine Kunden alle aus dem Ausland kommen und ihrem Geld nicht wirklich nachlaufen werden
6. Schritt B: Wenn die meisten ihr Geld einfach abhaken, kannst du sogar bis zum nächsten "Hack" weitermachen, die Millionen tauscht du dann einfach mit den großen Mafia-Familien der Welt für 1:2 in steuerfreies Geld. Die verteilten das auf ihre Hundertschaften die dann ganz regulär ihren Geschäften nachgehen
7. Schritt: Beteuern, dass man jetzt das hastig gebastelte PHP-Crypto"bank"-Modul total absolut sicher gemacht hat. Weil, man kann jetzt nur via SSL auf die Seite, da hat man was in den Apache Dokumentationen gefunden. Das ging ganz einfach.
8. Schritt: Die nächsten 10 Millionen werden von IDIOTEN überwiesen.



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

Intelligente(re) Organisationsgestaltung für exponentielle Zeiten

www.antea-management.de



© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights reserved

?

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights

Vielen Dank :-)

© Dr. Thomas R. Glück, München/Lüneburg, 2016, all rights