

Trustless Trust



12. April 2017

**The next big thing –
Chancen und Herausforderungen
durch Blockchain,
virtuelle Währungen,
Smart Contracts & Co.**

Walter Blocher
Universität Kassel

Ausführl. schriftl. Fassung:
bit.ly/blocher-dlt

„Machbarkeitsnachweis“

Bitcoin: A Peer-to-Peer Electronic Cash System

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

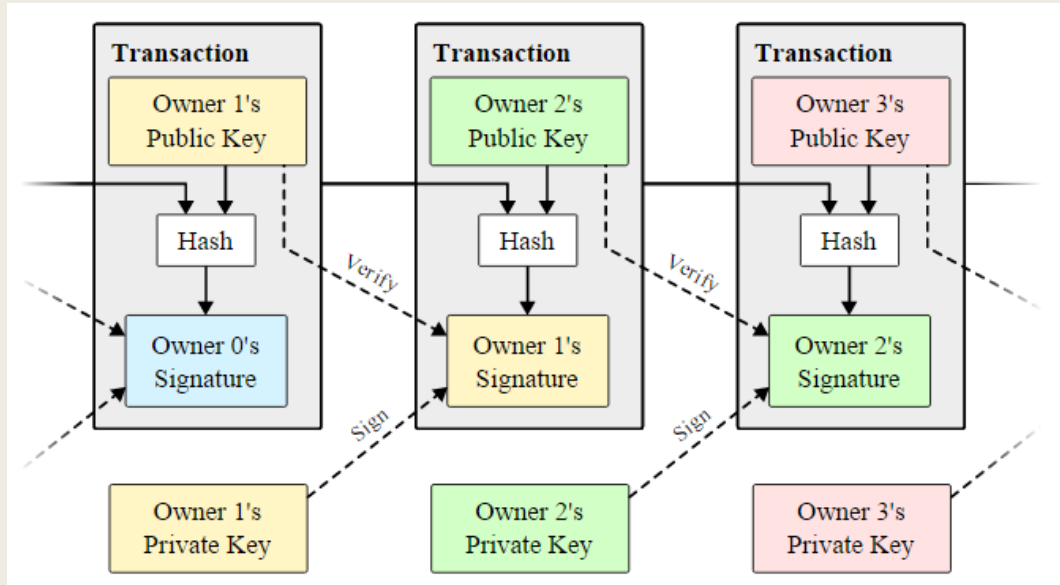
Geniestreich eines unbekannten Autors

Testimonial

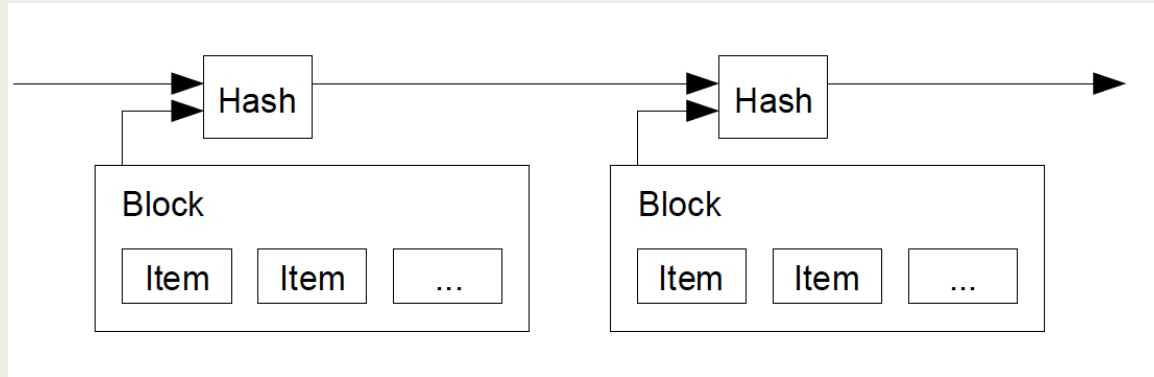
“Oh my god, this is it. This is the big breakthrough. This is the thing we’ve been waiting for. He solved all the problems. Whoever he is should get the Nobel Prize – he’s a genius. This is the thing! This is the distributed trust network that the Internet always needed and never had.”

Marc Andreessen, Entwickler des ersten Webbrowsers und Technologie-Investor

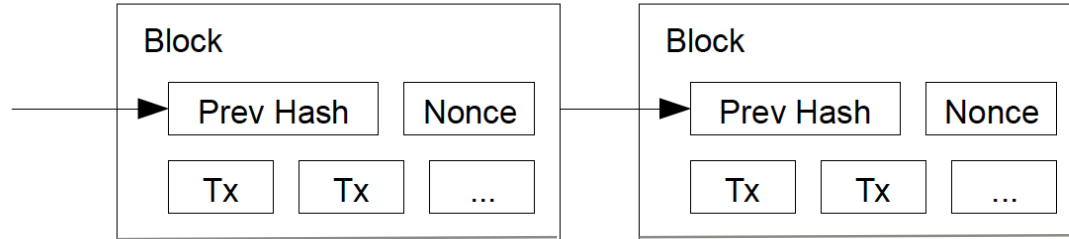
Transaktionen (vereinfacht)



„Zeitstempeldienst“



Proof-of-Work



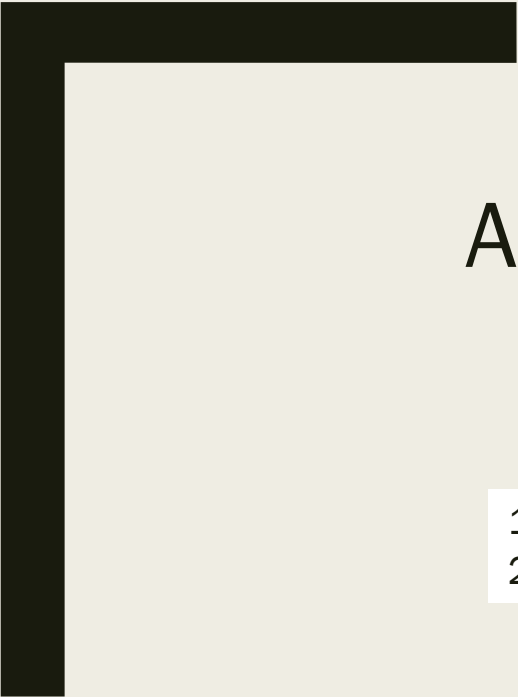
Proof-of-Work Function

$$\mathcal{F}_d(c, x) \rightarrow \text{SHA256}(\text{SHA256}(c|x)) < \frac{2^{224}}{d}$$

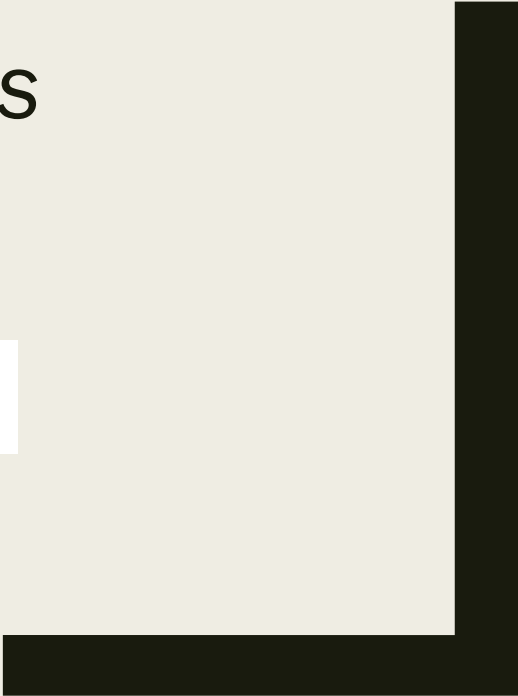


„Kryptographischer
Fliehkraftregler“





Anreize für *Miners*

1. Belohnung (derzeit 12,5 BTC)
 2. (Freiwillige) Transaktionsgebühren
- 

Das Netzwerk

1. Neue **Transaktionen** werden allen **Knoten** bekanntgegeben.
2. Jeder sich am **Mining-Prozess** beteiligende Knoten ("Miner") sammelt die neuen Transaktionen in einem "**Block**".
3. Jeder Miner versucht, den extrem rechenaufwändigen "**Proof-of-Work**" für seinen Block zu erbringen, indem er ein "**Nonce**" sucht, das gemeinsam mit den in den Block einzubindenden Transaktionen und dem **Hash-Wert** des unmittelbar vorangehenden Blocks die durch die jeweilige "Difficulty" vorgegebene Anforderung erfüllt, dass eine bestimmte Anzahl (z.B. 68) der führenden Stellen des 256 Bit langen Hash-Werts „0“ sind.
4. Wenn ein Miner den "Proof-of-Work" erbringt, gibt er den so gebildeten **neuen Block** allen Knoten bekannt.
5. **Andere Knoten** akzeptieren den Block nur, wenn alle enthaltenen Transaktionen gültig und nicht bereits früher vorgekommen („ausgegeben“ worden) sind.
6. **Miner** zeigen, dass sie einen Block akzeptieren, indem sie bei ihrer Arbeit am nächsten Block für die Blockchain den Hash des dadurch akzeptierten Blocks als vorangehenden Hash verwenden.

Statistik

Bitcoin Network

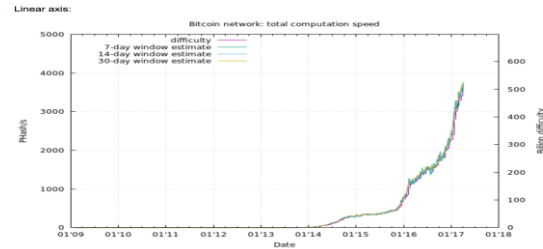
Economy

Total BTC	16,263,988 BTC
Market Cap based on latest prices	19,307,792,761 USD or 18,197,775,614 EUR or 75,952,821,625 PLN or 15,711,011,925 GBP
Transactions last 24h	229,939
Transactions avg. per hour	9580.79
Bitcoins sent last 24h	4,231,620.81 BTC
Bitcoins sent avg. per hour	176,317.53 BTC

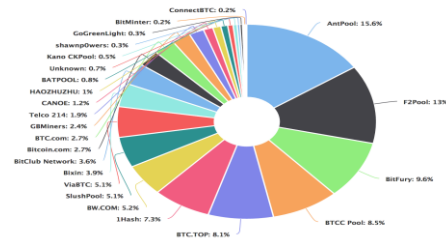
Blocks

Count	461,118
Blocks last 24h	148
Blocks avg. per hour	6.17
Difficulty	499,635,929,817
Next Difficulty in 546 blocks	508,594,022,119
Network Hashrate Terahashes/s	3640657.82
Network Hashrate PetaFLOPS	46236354.31

Network Hashrate



Hashrate Distribution



Von Crypto-Currency zu Crypto-Law?



Quelle: Ethereum

Konzept von Ethereum

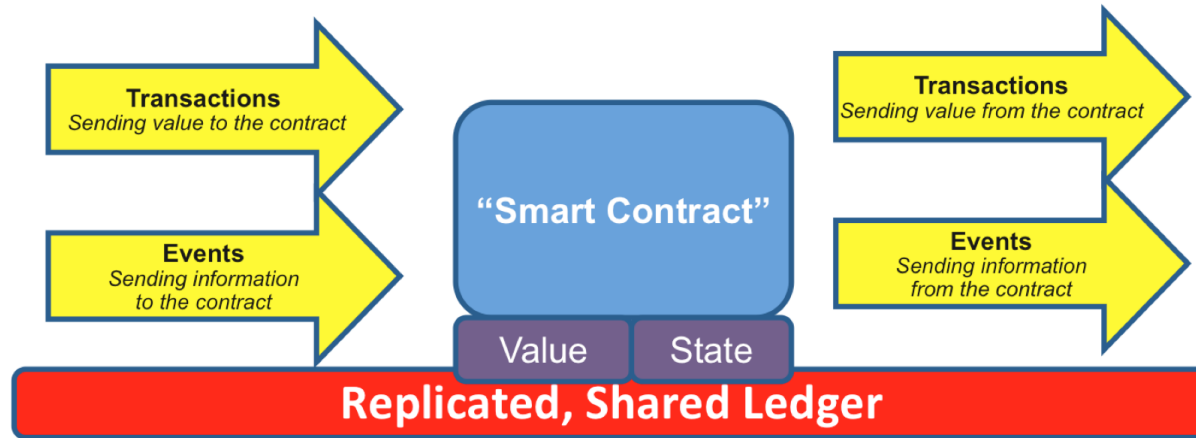
(und ähnlichen Projekten)

- Öffentliche Blockchain mit programmierbarer Transaktions-Funktionalität
- Bietet eine virtuelle Maschine (Ethereum Virtual Machine = EVM).
- Auf dieser läuft eine Turing-vollständige Programmiersprache.
- Bildet dadurch eine Plattform für programmierbare Smart Contracts.
- Smart Contracts können in verschiedenen Programmiersprachen geschrieben werden.
- Smart Contracts werden in den Bytecode der EVM kompiliert, bevor sie in die Blockchain aufgenommen werden.
- Rechenzeit und Speicherplatz werden mit der Währung “Ether” bezahlt, die als „Treibstoff“ (“Gas”) dient.

Versuch einer Definition

Smart Contract: Programmcode, der auf einer Blockchain läuft und dort digitale Assets oder Repräsentationen körperlicher Gegenstände auf der Grundlage von anderen (externer) Daten, die zum Zeitpunkt der Programmierung des Codes noch nicht feststanden, zwischen zwei oder mehreren Parteien in Form von Transaktionen neu zuordnet.

Schema eines „Smart Contracts“



Quelle: Peter Todd, A Simple Model for Smart Contracts

Passende Metapher für „Smart Contract“?



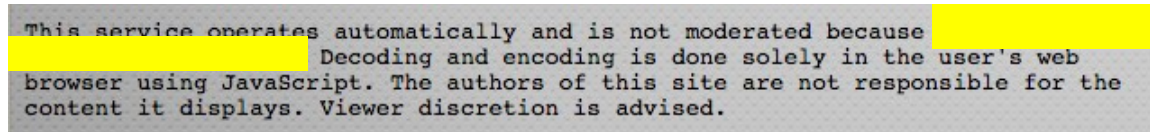
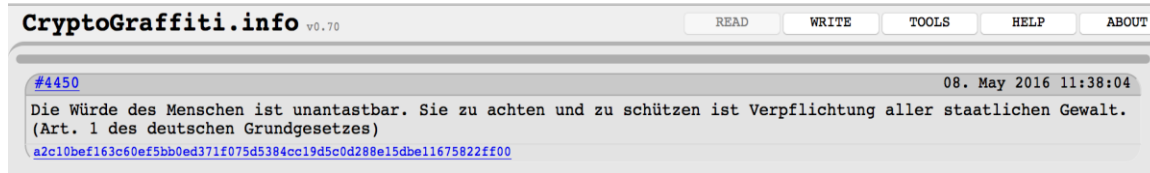
Anwendungsbeispiele

- Versicherungen (ohne zentralen Versicherer)
- Wertpapierhandel (Clearing & Settlement)
- Crowdfunding
- Micro-Tipping (etwa für Dienste in sozialen Netzwerken)
- M2M-Kommunikation (IoT)
- Peer-to-peer-Kredite
- Verteilter Speicherplatz (z.B. Storj)
- Smart Locks (z.B. Slock.it)
- Rechnungswesen
- Digitales Notariat
- Handel mit Immaterialgütern (z.B. Ascribe)
- Dezentraler Energiehandel
- Grundbuch (Tests z.B. in Schweden und Georgien)
- Identitätsmanagement
- Herkunftszertifikate
- Handel mit herkömmlichen Waren
- Dezentralisierte Vorhersage-Märkte (z.B. Augur)
- Wahlen
- KYC
- Kranken-/Gesundheitsakten
- ... (you name it)

Anwendungsmöglichkeiten mit spezifischer Verbraucherperspektive

- Sparpotential bei Banken- und Versicherungsgebühren
- Portabilität von Gesundheitsdaten
- Rufnummernportierung (TKG)
- Bonus- oder Punktesysteme zur Kundenbindung
- **C2B statt B2C**
- **Verwaltung von Dauerschuldverhältnissen mittels „Dashboard“**
- **Erleichterung der Rechtsdurchsetzung**

Chance oder Grenze?



Chancen

Blockchain

- Ersetzung soziologischen Vertrauens durch kryptographische Sicherheit (“trustless trust”)
- Fehlertoleranz, Ausfallsicherheit, Zensurresistenz
- Vermeidung kostentreibender Intermediäre durch die Ermöglichung dezentraler Transaktionsmodelle einschließlich der finanziellen Abwicklung
- Aus Sicht der staatlichen Verwaltung: Konzentration auf das „Kerngeschäft“
- Demokratieförderndes und die Teilhabe an der globalen Wirtschaft ermöglichendes Potenzial in “unbanked” oder “underbanked” Regionen
- C2B statt B2C → mehr Wettbewerb, Stärkung kleinerer Unternehmen, günstigere Preise
- Ermöglichung von Micropayments durch fehlende oder minimale Transaktionsgebühren (trifft derzeit auf die Bitcoin-Blockchain nicht zu)
- „Eingebauter“ Verbraucherschutz: Zahlungen an den Vertragspartner, ohne ihm irgendwelche Finanzdaten zukommen lassen zu müssen; keine Gefahr des „Identitätsdiebstahls“
- Einfache Festlegung transaktionsbegrenzender Parameter
- Multisig-Transaktionen als zusätzlicher Schutz gegenüber unbekannten Transaktionspartnern oder zur Streitbeilegung
- Transparenz
- Situative und temporäre Freigabe personenbezogener Daten → wesentliche Verbesserung des Datenschutzes

Smart Contracts

- „Automatische“ Rechtsdurchsetzung (Bsp.: Fluggastrechte)
- Ermöglichung komplexer Streitbeilegungsszenarien

Grenzen und Herausforderungen

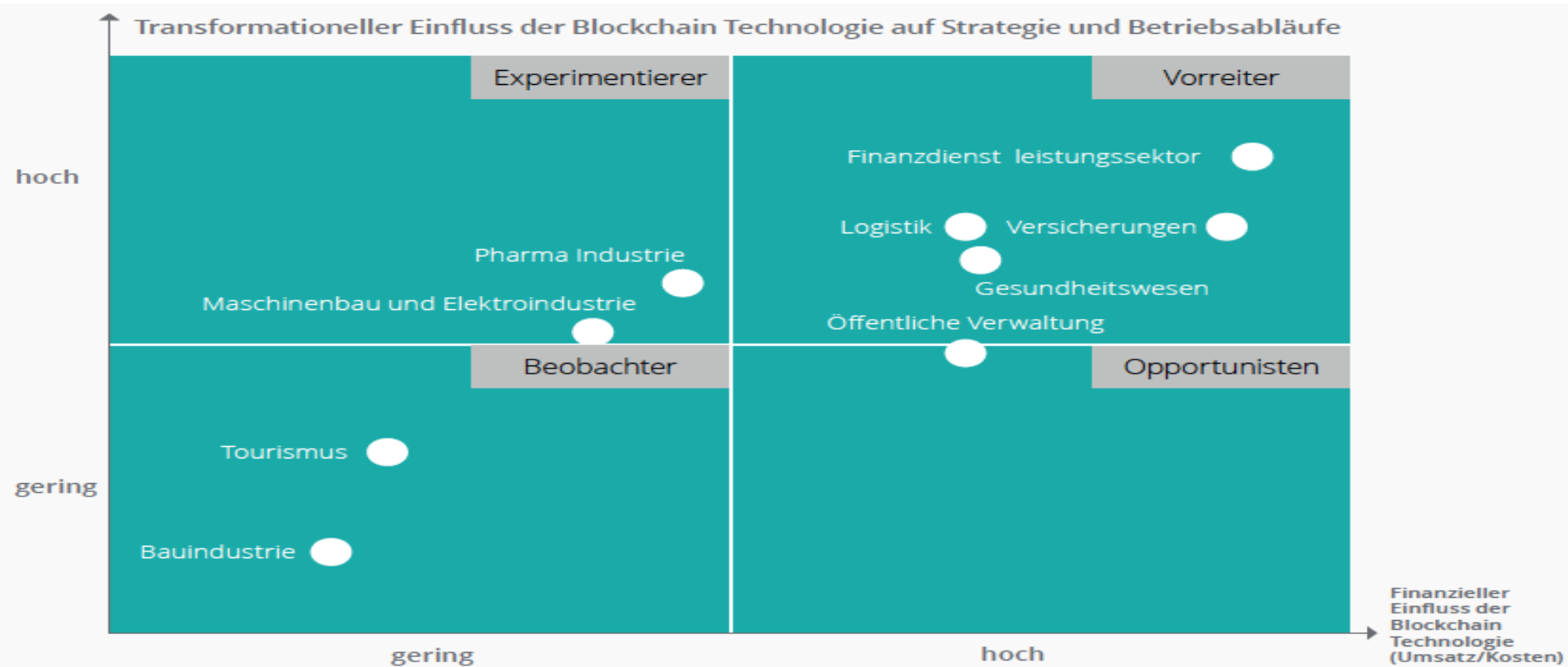
Blockchain

- Instabilität des „Ökosystems“
- Energieverbrauch
- Konzentration (mangelnde Verteilung) der Network Hashrate
- Mangelnde Skalierbarkeit („block size debate“)
- Kein Consensus System für Änderungen des Protokolls
- Regulierungsresistenz
- Fehlende Zurechenbarkeit („Adressat“)
- Quantencomputer

Smart Contracts

- Problematische Korrigierbarkeit von Fehlern (vgl. „The DAO“)
- Reaktion auf Unvorhergesehene Ereignisse
- Kein Raum für Interpretation im jur. Sinne
- Haftungsfragen
- Kriminelle Smart Contracts
- Anwendbares Recht
- Regulierung

Blockchain-Strategien



GLOBAL BITCOIN NODES
DISTRIBUTION

Reachable nodes as of Thu Apr 06 2017
16:30:33 GMT+0200 (CEST).

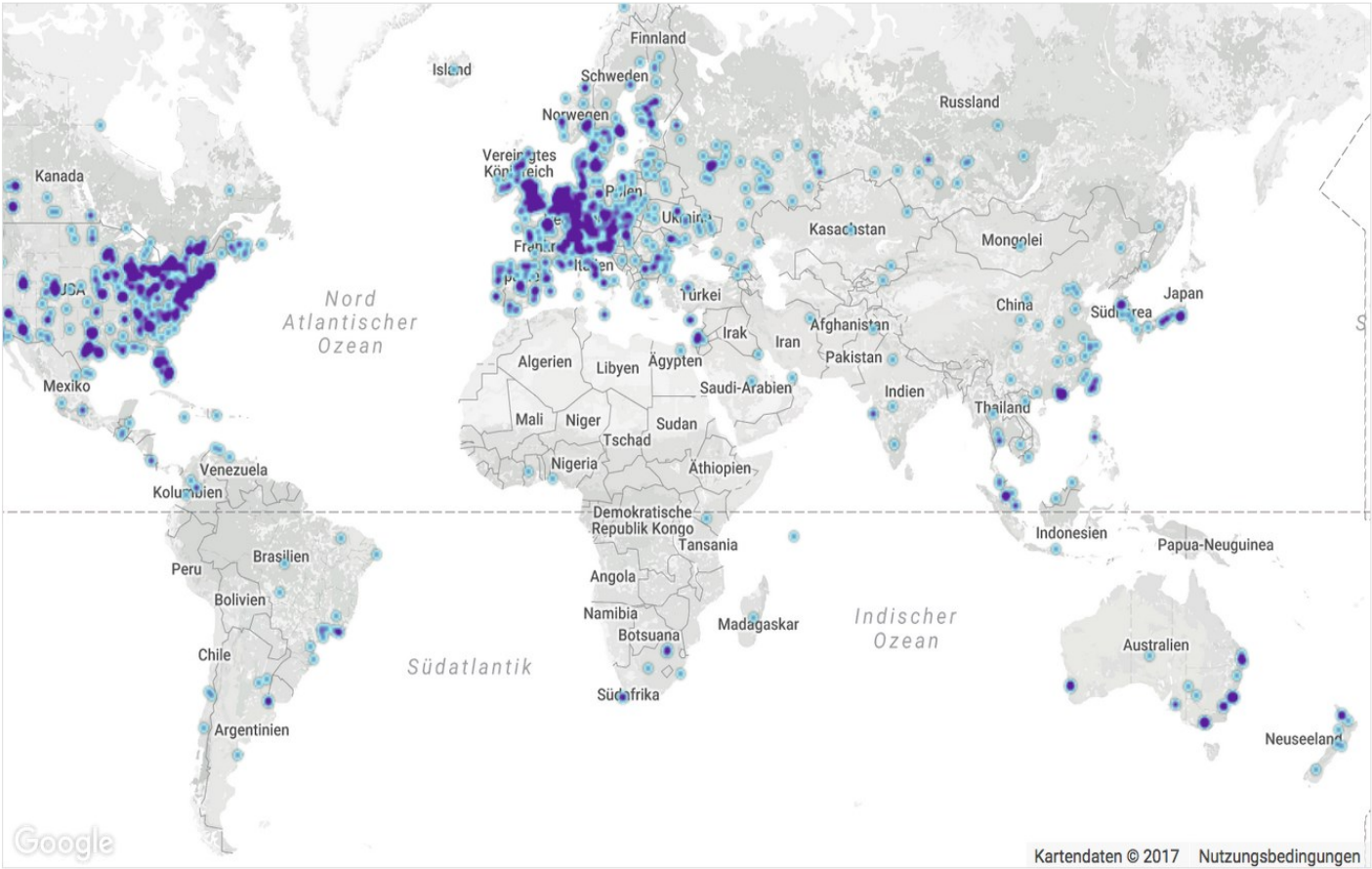
7033 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	1953 (27.77%)
2	Germany	1404 (19.96%)
3	France	463 (6.58%)
4	Netherlands	395 (5.62%)
5	United Kingdom	289 (4.11%)
6	Canada	286 (4.07%)
7	n/a	248 (3.53%)
8	China	228 (3.24%)
9	Russian Federation	183 (2.60%)
10	Switzerland	108 (1.54%)

More (93) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

LOCATION	NETWORK
Rainbach, Austria	Incero LLC
Loipersdorf, Austria	A1 Telekom Austria AG
Erpersdorf, Austria	A1 Telekom Austria AG
Vienna, Austria	kabelplus GmbH
Vienna, Austria	A1 Telekom Austria AG
Modling, Austria	A1 Telekom Austria AG
Vienna, Austria	Liberty Global Operations B.V.
Vienna, Austria	Liberty Global Operations B.V.
Vienna, Austria	A1 Telekom Austria AG
Austria	Liberty Global Operations B.V.
Vienna, Austria	A1 Telekom Austria AG
Vienna, Austria	Liberty Global Operations B.V.
Vienna, Austria	Liberty Global Operations B.V.
Wiener Neustadt, Austria	Liberty Global Operations B.V.
Graz, Austria	Citycom Telekommunikation GmbH
Engerwitzdorf, Austria	LIWEST Kabelfernsehen Errichtungs- und Betriebs Ges.m.b.H.
Austria	Hutchison Drei Austria GmbH
Vienna, Austria	Liberty Global Operations B.V.
Vienna, Austria	Liberty Global Operations B.V.
Uttendorf, Austria	SALZBURG AG für Energie, Verkehr und Telekommunikation
Reinprechtspolla, Austria	A1 Telekom Austria AG

	NETWORK
Austria	Liberty Global Operations B.V.
Wiener Neustadt, Austria	Liberty Global Operations B.V.
Austria	A1 Telekom Austria AG
Traiskirchen, Austria	kabelplus GmbH
Austria	Liberty Global Operations B.V.
Austria	Liberty Global Operations B.V.
Vienna, Austria	Liberty Global Operations B.V.
Vienna, Austria	A1 Telekom Austria AG
Rainbach, Austria	Incero LLC
Austria	Thor Data Center ehf
Austria	Liberty Global Operations B.V.
Vienna, Austria	Liberty Global Operations B.V.
Graz, Austria	Liberty Global Operations B.V.
Austria	A1 Telekom Austria AG
Austria	EDIS GmbH
Austria	EDIS GmbH
Tirol, Austria	A1 Telekom Austria AG
Austria	EDIS GmbH
Austria	EDIS GmbH
Austria	EDIS GmbH
Austria	Nessus GmbH
Innsbruck, Austria	nemox.net
Kufstein, Austria	Stadtwerke Kufstein GmbH