Vereinbarkeit von Blockchain-Technologie und Datenschutz-Grundverordnung?

(am Beispiel der Public Permissonless Blockchain Bitcoin)

Prof. Dr. Peter Preuss

How to make sure your love letter lasts forever? Put it on blockchain

Published: Feb. 14, 2018 at 4:39 p.m. ET

By Kari Paul

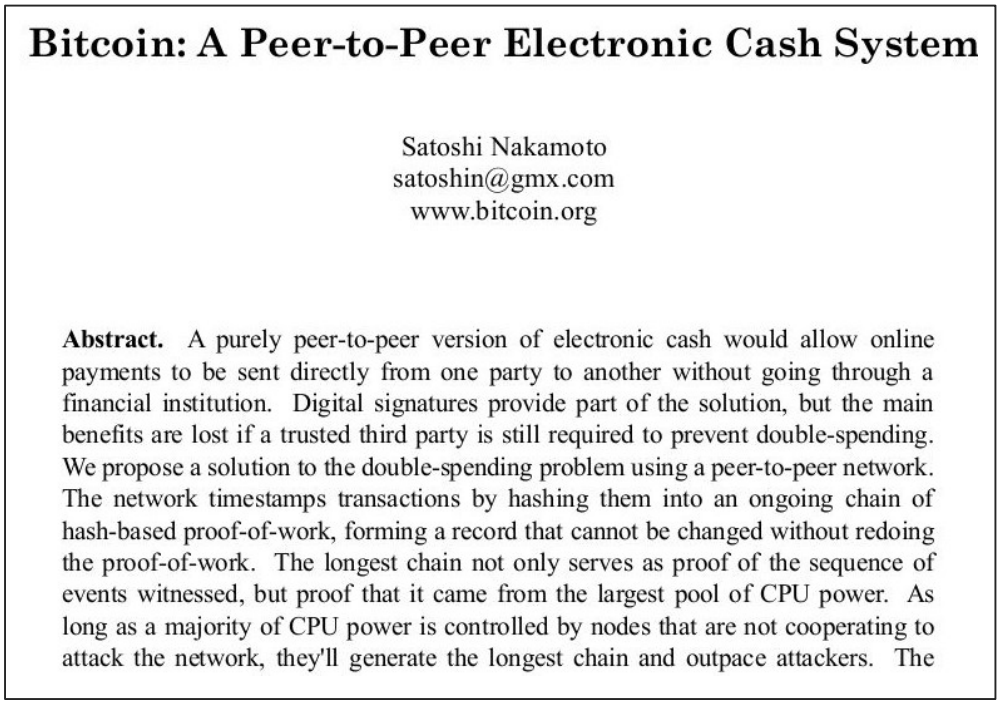
Diamonds are forever, but so is the blockchain

https://www.marketwatch.com/story/immortalize-your-love-on-the-blockchain-this-valentines-day-2018-02-14

Gliederung

1	Bitcoin - Public Permissonless Blockchain
2	Datenschutzgrundverordnung versus Bitcoin
3	Lösung: Anonymisierung mit Bitcoin-Mixer?
4	Schlussbetrachtung

Bitcoin - Public Permissonless Blockchain

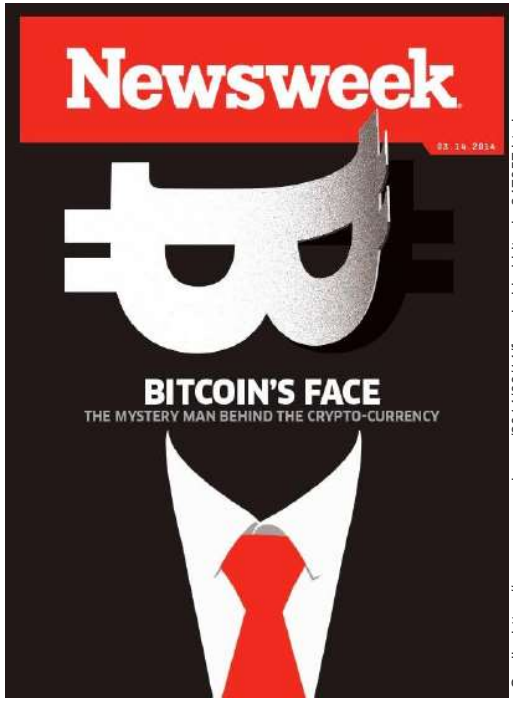


Bitcoin: A Peer-to-Peer Electronic Cash System

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

Quelle: https://bitcoin.org/bitcoin.pdf8

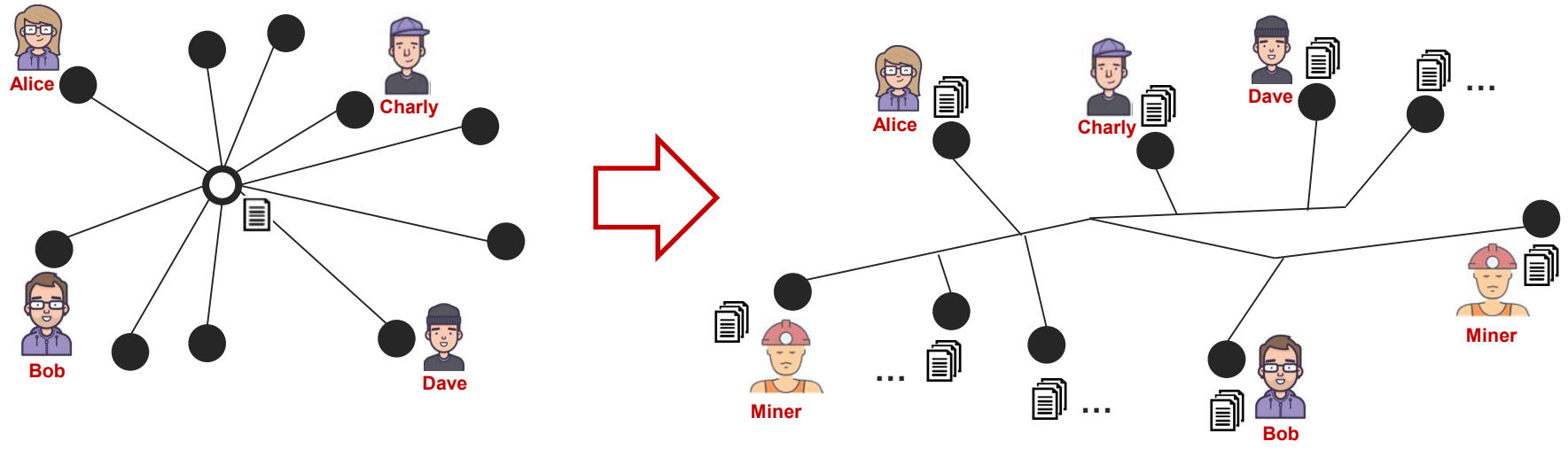


Quelle: https://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html

„Geburtsstunde“ von Bitcoin

- Im **November 2008** publizierte eine Person/Gruppe unter dem Pseudonym **Satoshi Nakamoto** ein technisches Konzept für eine **digitale Währung**

Bitcoin - Public Permissonless Blockchain

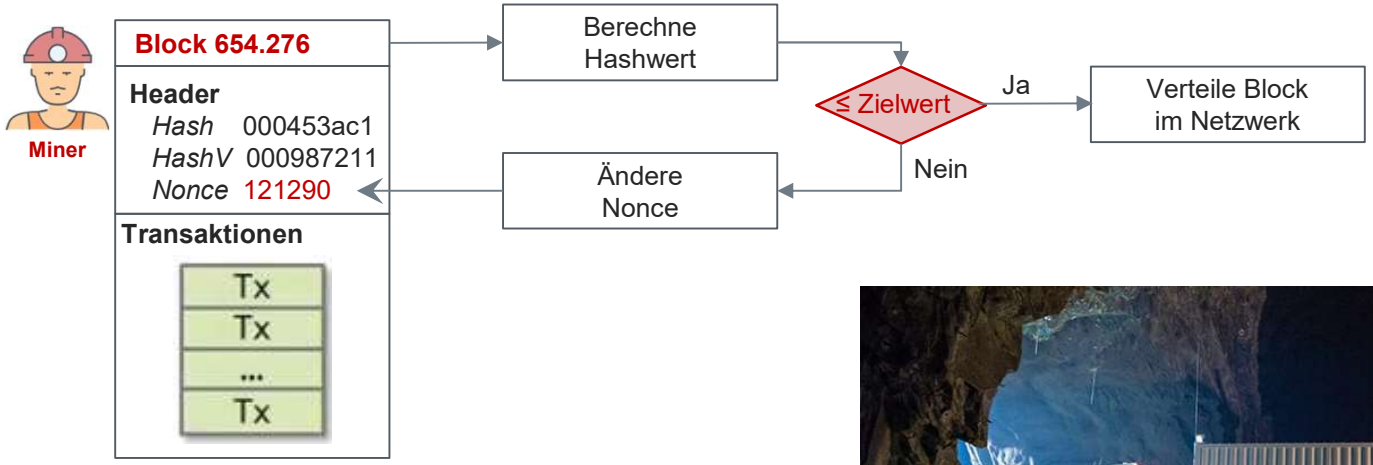


Legende: Intermediär Transaktionsteilnehmer Transaktionsbuch (Blockchain)

Verteilte Transaktionsdatenbank (Blockchain)

- Transaktionsdatenbank ist **nicht** auf einem zentralen Server sondern **replizierte, verteilte Datenbank**.
- Datenbank besteht aus verketteten Datenblöcken (**Blockchain**), in denen Transaktionen gespeichert sind.
- Teilnehmer besitzen **vollständige Kopie** der Blockchain.
- **Miner** erstellen Blöcke.

Bitcoin - Public Permissonless Blockchain



Quelle: https://www.gq-magazin.de/auto-technik/article/krypto-mining-in-der-kaelte-in-diesem-norwegischen-stollen-werden-bitcoins-geschuerft

- **Miner** wetteifern darum, wessen Block als nächstes an die Blockchain angehängt wird. Gewinner erhalten alle ~10 Minuten **6,25 BTC** (ca. 72.400 €) + **Transaction Fees**

Bitcoin - Public Permissonless Blockchain

Explorer › Bitcoin Explorer › Blöcke

Suchen Sie Ihre Transaktion, eine Adresse oder einen Block

Blöcke

Höhe	Hash	Mined	Bergmann	Größe
654276	0..475516eecd66c824705ede7a0b807ee103d4a3831a874	45 Minuten	Poolin	1.526.877 bytes
654275	0..116316896c516ebb9967effc58706f1ae2738b6896559	50 Minuten	Unknown	1.404.677 bytes
654274	0..c00f831f923433563400dc3405a80776bfc9f2c313893	eine Stunde	AntPool	1.505.463 bytes
654273	0..764847e18728d3f9e37637b68775600e5e96667a65a45	eine Stunde	Unknown	1.548.380 bytes
654272	0..c89c96ff12d3c3730d3907a667affe95aed3aab32c6c0	eine Stunde	Unknown	1.318.560 bytes
654271	0..18d138c0d27cae1eea65e706cd173de5e27c111bd6d76	2 Stunden	BTC.com	1.177.720 bytes
654270	0..ae8ade1f02c965d7d6ec79ea2772cb31abd4fbb6efc30	2 Stunden	F2Pool	1.420.437 bytes
654269	0..2b6f6878adce8b643f998ae9de39691de8672709538af	2 Stunden	F2Pool	1.401.762 bytes
654268	0..2aa642e7e052ceaff37777b04a2a934f26d47f43e7932	2 Stunden	AntPool	1.270.434 bytes
654267	0..7a219accc04a369f978457c00729f9b7b3780c23ba892	3 Stunden	Unknown	1.076.543 bytes
654266	0..262a954be08f815ad96e3e776c3a971fca8786bcb5b9c	3 Stunden	Unknown	1.331.764 bytes
654265	0..8cea746f82fc69d7d62941870f94f8e3d67d38c2d4e86	3 Stunden	Unknown	1.208.512 bytes

Quelle: https://www.blockchain.com/btc/blocks?page=1

Jeder Währungsteilnehmer hat Paare aus öffentlichen und privaten Schüsseln

Bobs Wallet

Electrum 4.0.3 - wallet_bob [standard]

Datei Geldbörse Ansicht Werkzeuge Hilfe

Transaktionen | Senden | Empfangen | Adressen | Kontakte

Typ	Adresse	Beschreibung	Guthaben	Tx
eingehend	bc1q6lvcxc4tkrw4wmgpm6t5fxu03f7rfjez7ltxfg		0.00000000	0

Guthaben: 0.00000000 BTC

Adresse

Adresse: bc1q6lvcxc4tkrw4wmgpm6t5fxu03f7rfjez7ltxfg

Öffentliche Schlüssel: 032e5ac8e9f7c8be72101e5d7e1a2bb89a880be412b0152c7e2dbfa08faeca0198

Derivation path: m/0/0

Transaktionen

Datum	Beschreibung	Betrag	Guthaben

Privater Schlüssel

Adresse: bc1q6lvcxc4tkrw4wmgpm6t5fxu03f7rfjez7ltxfg

Skript-Typ: p2wpkh

Privater Schlüssel:

p2wpkh:KznpsxbytiBXLApBATs4zBP1hc4mbrSAuZsGbR1ktCjT5ERtG522

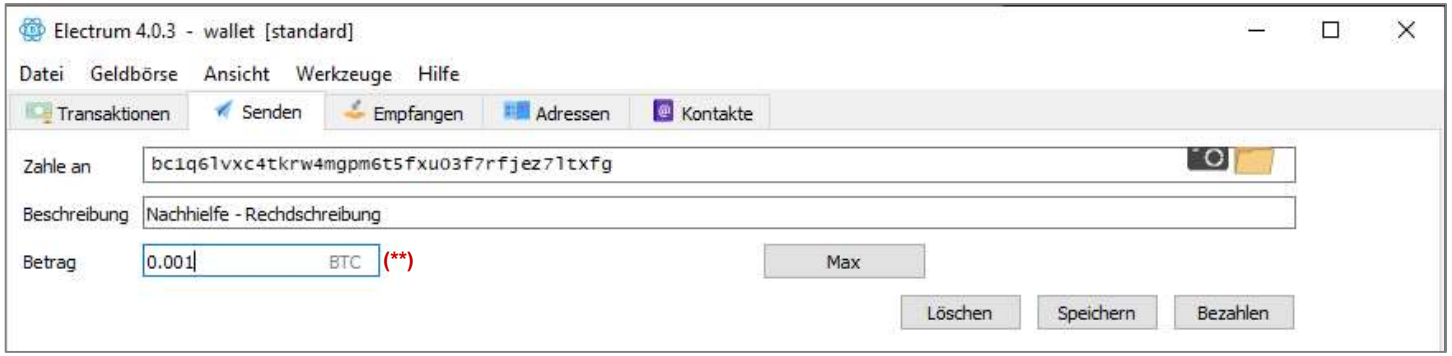
Schließen

Bitcoin-Transaktionen

Alice

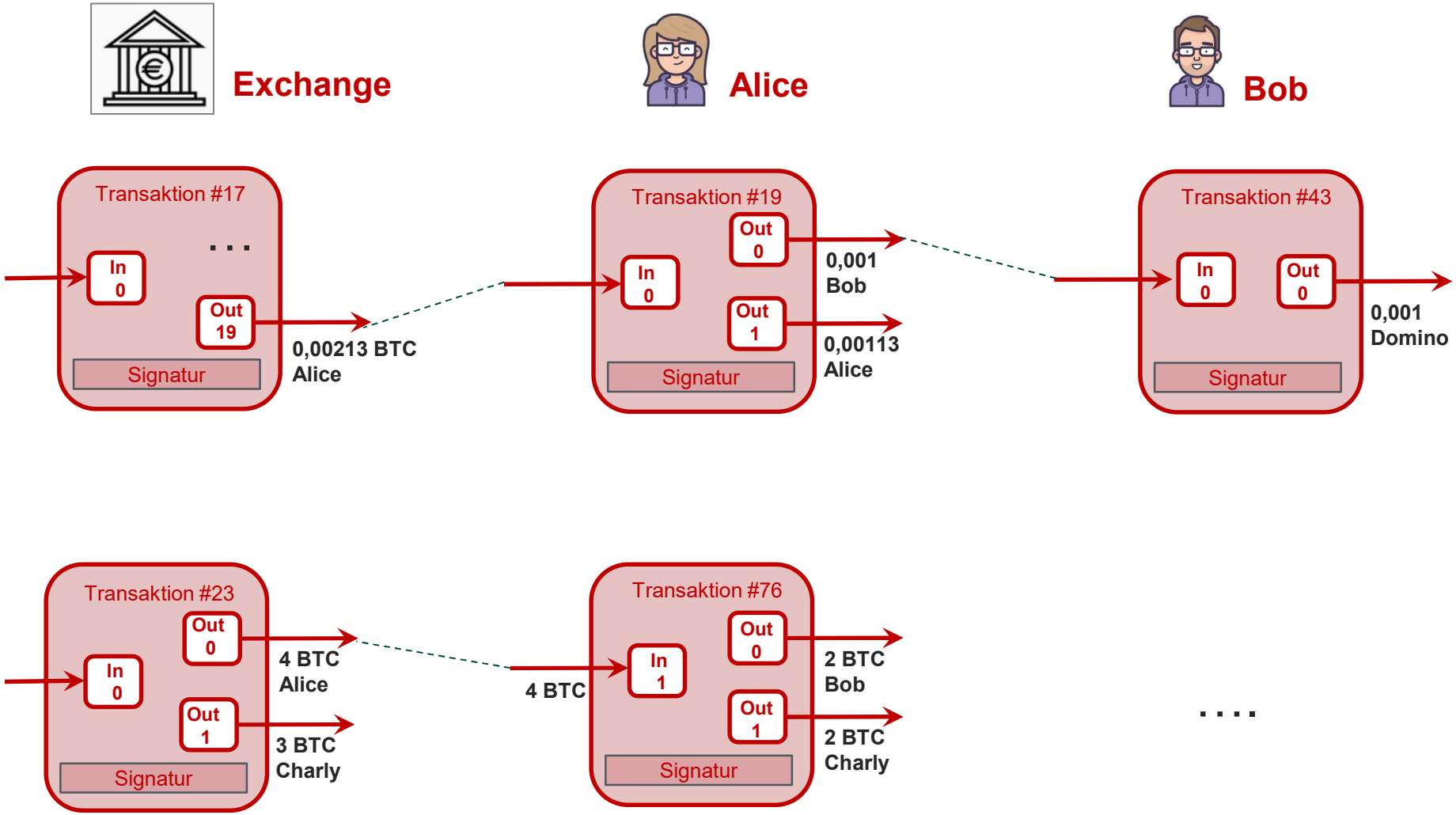
Bob

(*) 0,00213 BTC entspricht ca. 24 €



(**) 0,001 BTC entspricht ca. 12 €

Bitcoin - Public Permissonless Blockchain



Bitcoin - Public Permissonless Blockchain

Quelle: https://www.blockchain.com/de/btc/address/bc1qkkwtuau0vg4x3vywcsvytwl8w3vr5sgl95xvyw

Bitcoin - Public Permissonless Blockchain

Zwischenfazit

- Bitcoin-Transaktionen werden in **dezentraler Blockchain** gespeichert
- **Blockerstellung** von (anonymen) **Minern**
- **Verschleierung der Identifikationsparameter** durch kryptographische Schlüssel
- Alle Transaktionen sind **öffentlich einsehbar**
- **Unveränderlichkeit** der Transaktionen
- Transaktionen können **nicht gelöscht** werden

Bitcoin - Public Permissonless Blockchain

Marktkapitalisierung (28. Oktober 2020)

CoinGecko Startseite Märkte DeFi Farms Börsen Neuigkeiten Tools Ressourcen Lernen Community Suche

Kryptowährungen: 5968 **Börsen:** 406 **Marktkapitalisierung:** 339.171.808.803 € -0.4% **24-Stunden-Volumen:** 37.635.965.771 € **Dominanz:** BTC 60% ETH 11% USDT 4,0% **ETH Gas :** 15 gwei

Die 100 besten Kryptowährungen nach Marktkapitalisierung

EUR | Filter | Portfolio New | Alle Kryptowährungen entdecken | Recently Added | Markt | Allzeithöchstwert | Entwickler | Social Media

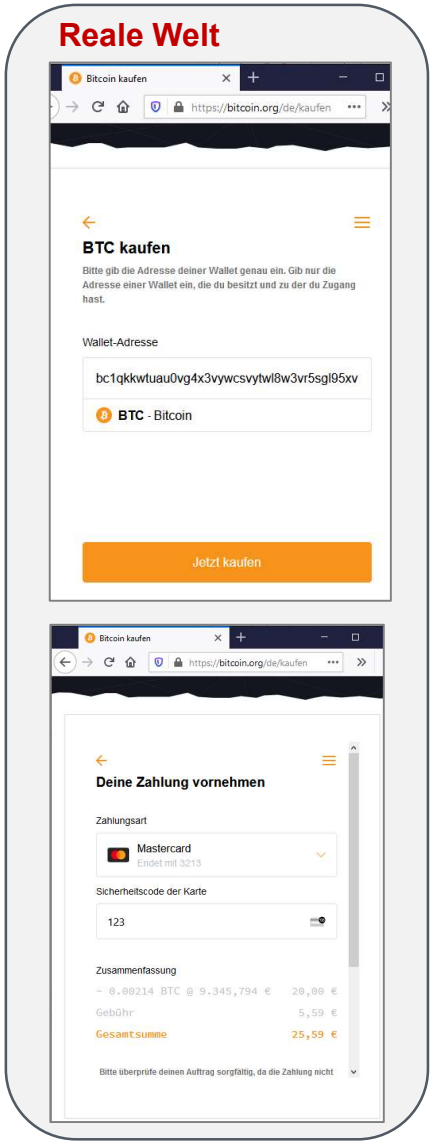
#	Kryptowährung		Kurs	1 h	24 h	7 d	24-Stunden-Volumen	Marktkapitalisierung	Letzte 7 Tage
1	Bitcoin	BTC	11.562,79 €	-0.4%	4.0%	14.9%	22.221.075.758 €	214.239.764.751 €	
2	Ethereum	ETH	334,95 €	-0.7%	0.8%	7.6%	9.148.065.153 €	37.900.489.673 €	
3	Tether	USDT	0,851004 €	0.1%	0.3%	0.4%	27.722.619.247 €	13.996.944.054 €	
4	XRP	XRP	0,211758 €	-1.0%	-0.1%	2.9%	1.296.667.603 €	9.574.110.598 €	
5	Bitcoin Cash	BCH	222,42 €	-0.5%	1.1%	9.3%	2.140.699.781 €	4.111.928.271 €	

Quelle: https://www.coingecko.com/de

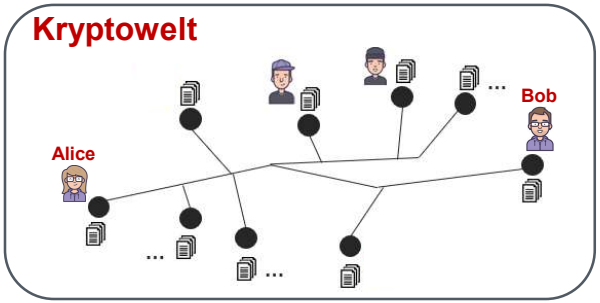
Gliederung

1	Bitcoin - Public Permissonless Blockchain
2	Datenschutzgrundverordnung versus Bitcoin
3	Lösung: Anonymisierung mit Bitcoin-Mixer?
4	Schlussbetrachtung

Datenschutzgrundverordnung versus Bitcoin

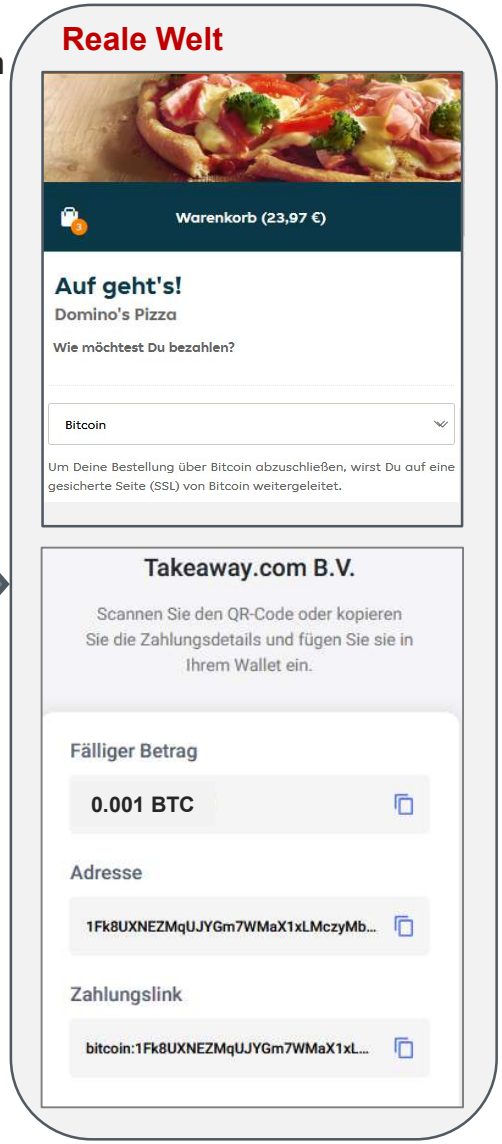


Kauf von Bitcoins mit Kreditkarte bei einem Exchange



Identifikationsparameter können indirekt mit Benutzern der realen Welt in Verbindung gebracht werden

Kauf eines realen Guts mit Bitcoin



Datenschutzgrundverordnung versus Bitcoin

Artikel 2

Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Artikel 4

Begriffsbestimmungen

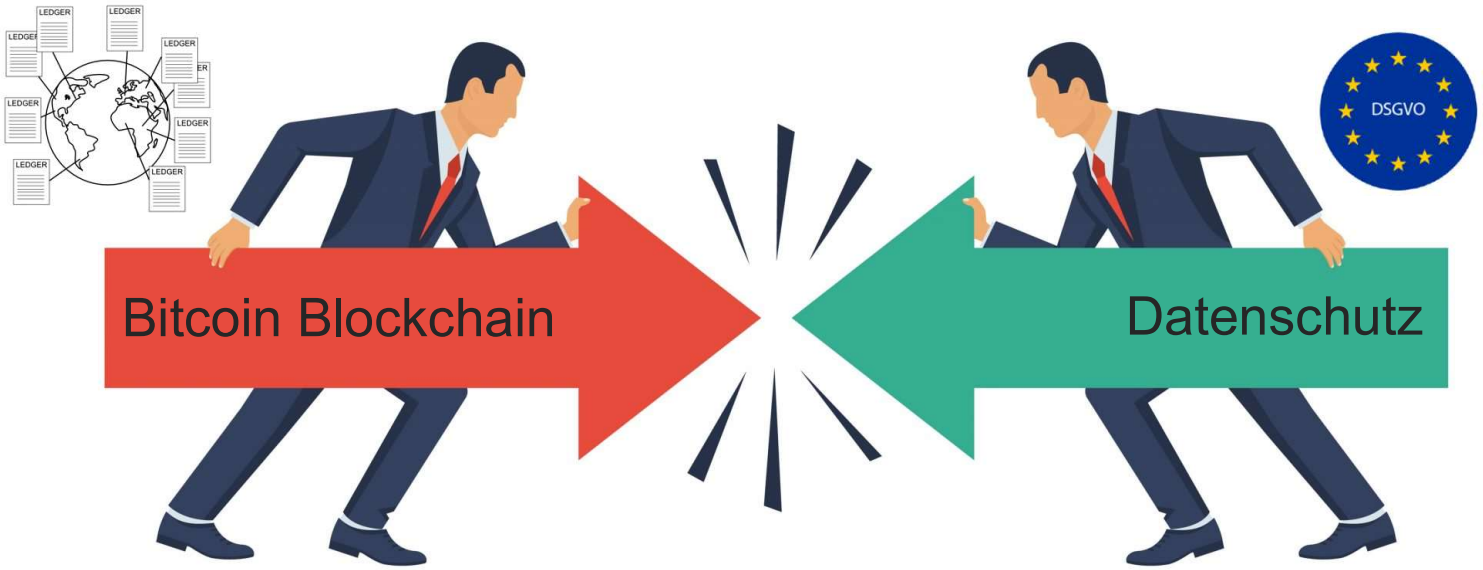
Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

- Identifikationsparameter sind nicht anonym, sondern nur **pseudonymisiert**.
- Es kann nicht ausgeschlossen werden, dass ein Personenbezug (zukünftig) möglich ist.

→ **DS-GVO ist grundsätzlich anwendbar**.

Datenschutzgrundverordnung versus Bitcoin



Artikel 16 DS-GVO: Recht auf Berichtigung

- *Problem*: **Unveränderlichkeit** der Transaktionen

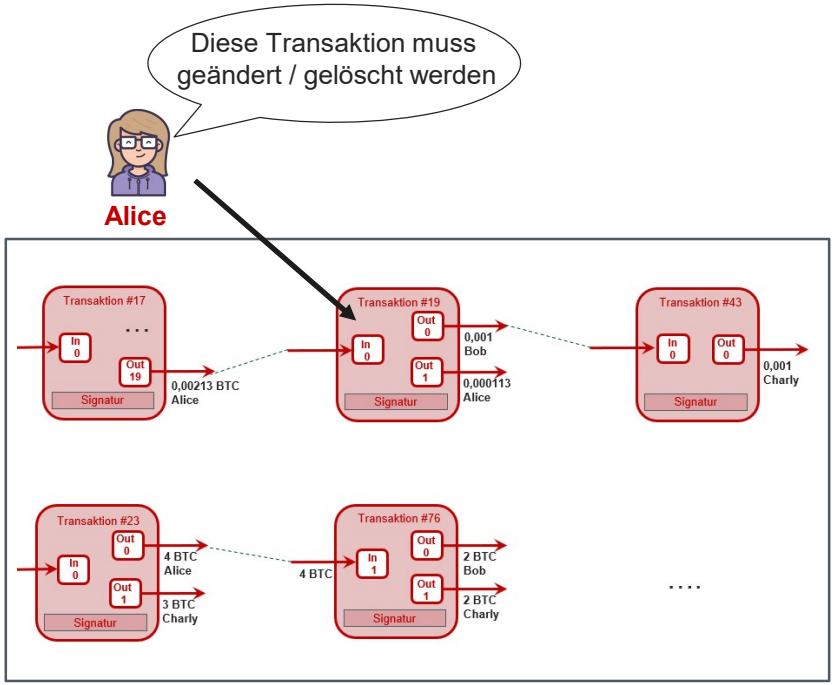
Artikel 17 DS-GVO: Recht auf Löschung („Recht auf Vergessenwerden“)

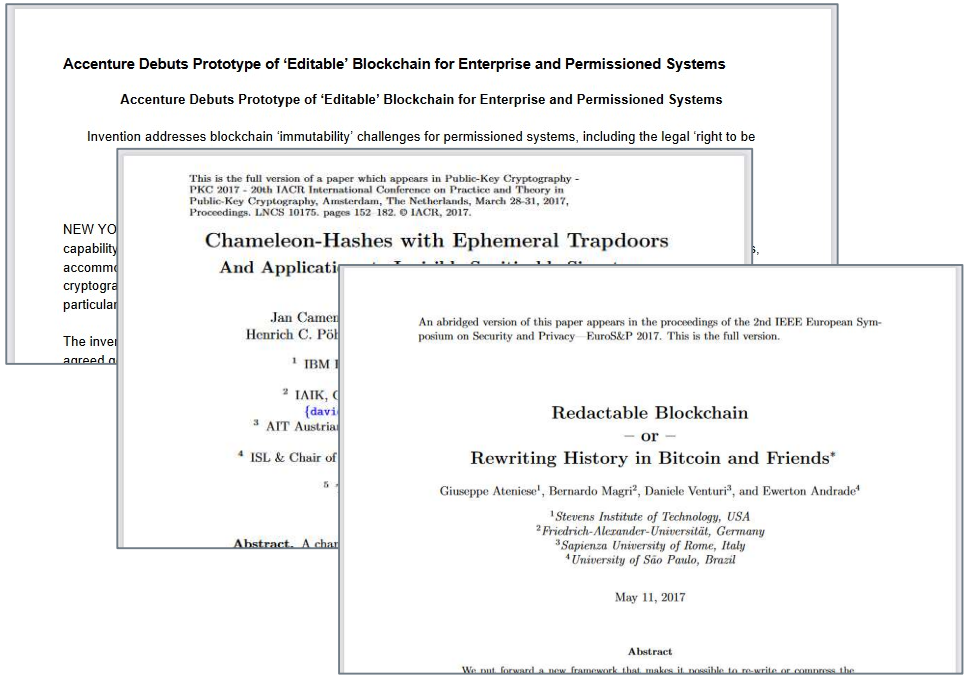
- *Problem*: Transaktionen können **nicht gelöscht** werden.

Artikel 18 DS-GVO: Recht auf Einschränkung der Verarbeitung

- *Problem*: Transaktionen sind **öffentlich** → Keine Kontrolle, wer Transaktionen dezentral verarbeitet

Datenschutzgrundverordnung versus Bitcoin




Accenture Debuts Prototype of 'Editable' Blockchain for Enterprise and Permissioned Systems

Accenture Debuts Prototype of 'Editable' Blockchain for Enterprise and Permissioned Systems

Invention addresses blockchain 'immutability' challenges for permissioned systems, including the legal 'right to be

This is the full version of a paper which appears in Public-Key Cryptography - PKC 2017 - 20th IACR International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, The Netherlands, March 28-31, 2017, Proceedings. LNCS 10175. pages 152–182. © IACR, 2017.

Chameleon-Hashes with Ephemeral Trapdoors

An abridged version of this paper appears in the proceedings of the 2nd IEEE European Symposium on Security and Privacy—EuroS&P 2017. This is the full version.

Redactable Blockchain
— or —
Rewriting History in Bitcoin and Friends*

Giuseppe Ateniese[1], Bernardo Magri[2], Daniele Venturi[3], and Ewerton Andrade[4]

[1]Stevens Institute of Technology, USA
[2]Friedrich-Alexander-Universität, Germany
[3]Sapienza University of Rome, Italy
[4]University of São Paulo, Brazil

May 11, 2017

Abstract

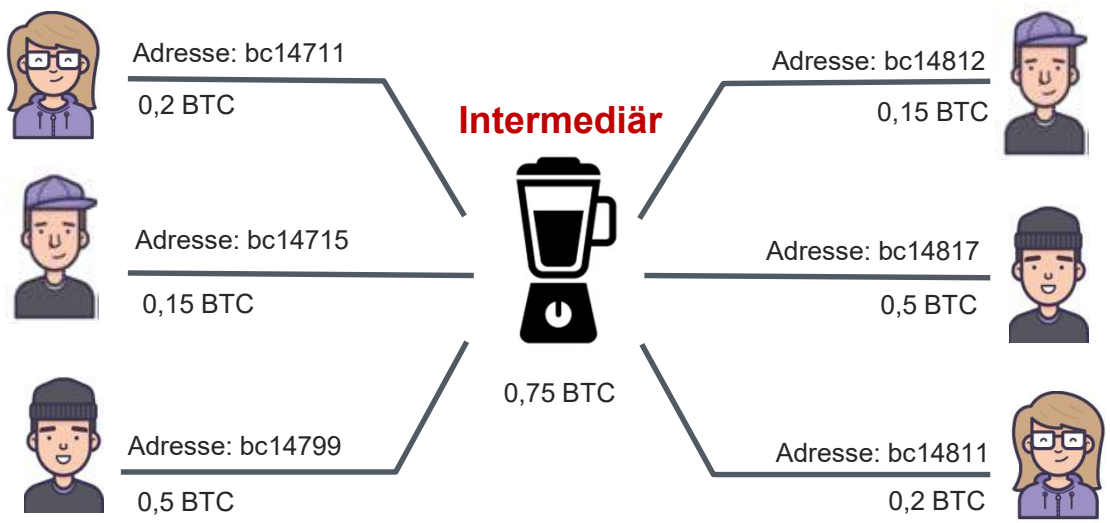
- **Änderung / Löschung / Einschränkung von Transaktionen** widerspricht Grundprinzip der Bitcoin Blockchain
- Kein **vertrauenswürdigen Intermediär, der Transaktionen ändern/löschen könnte**
- Änderungen an Bitcoin-Protokoll würden nicht akzeptiert werden (**hohe Marktkapitalisierung**)

→ **Praktikable Lösung**: **Anonymisierung der pseudonymen Identifikationsparameter**

Gliederung

1	Bitcoin - Public Permissonless Blockchain
2	Datenschutzgrundverordnung versus Bitcoin
3	Lösung: Anonymisierung mit Bitcoin-Mixer?
4	Schlussbetrachtung

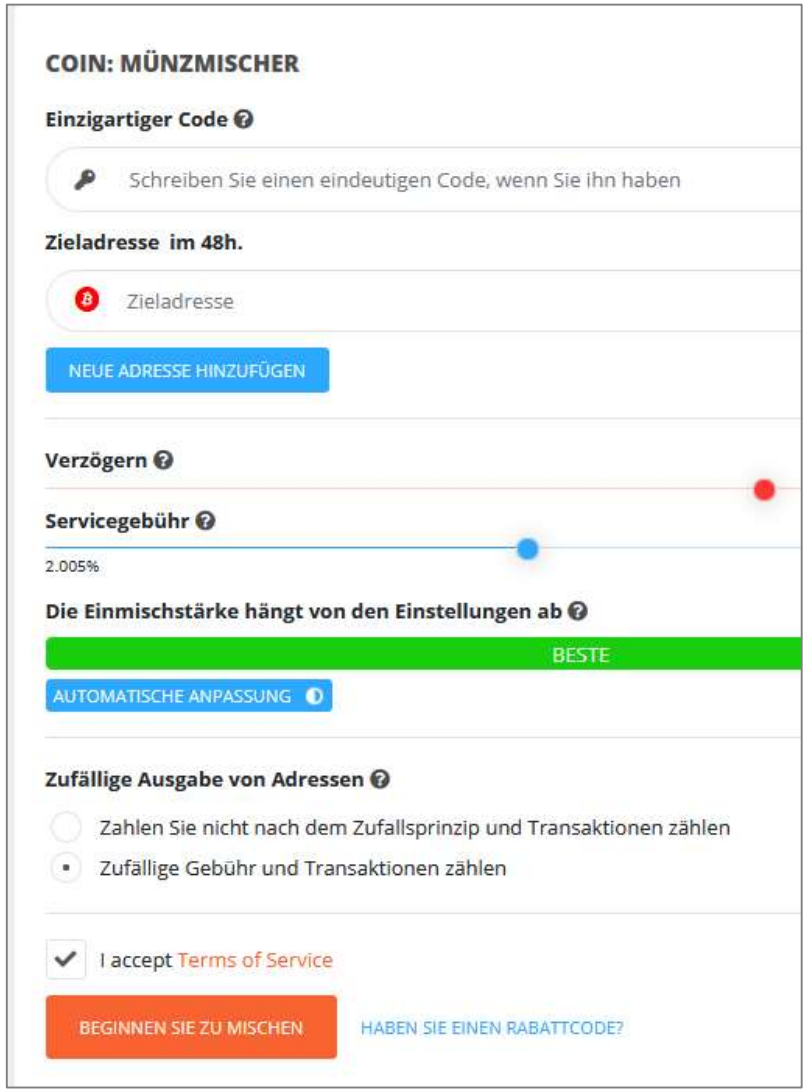
Lösung Bitcoin Mixer?



Bitcoin Mixer (Tumbler)

- Etablierung (anonymer) **Intermediäre**, die **Anonymisierung** übernehmen
- Mixer vermengt pseudonyme Bitcoin-Transaktionen und bildet daraus **anonymen Bitcoin-Pool**
- Aus dem Pool werden **Bitcoins an anonyme Bitcoin-Adressen zurücküberwiesen** (abzgl. Servicegebühr)

Lösung Bitcoin Mixer?



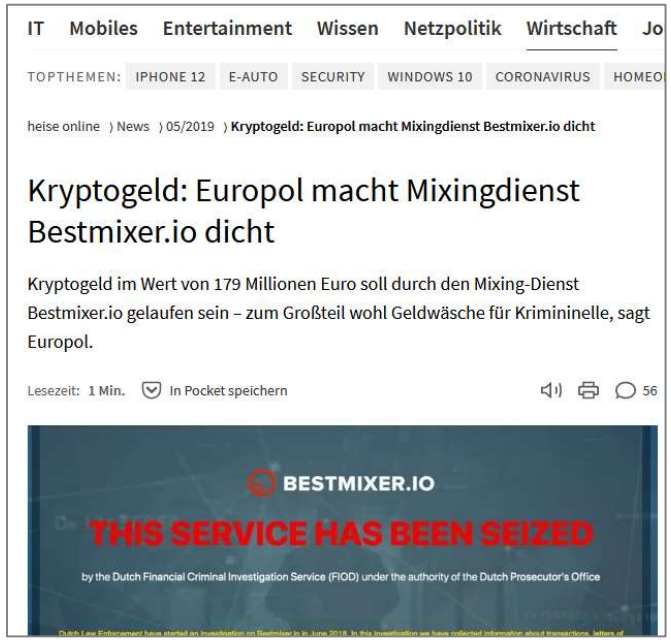
https://bitmix.biz/de/bitcoin-mixing

Bitcoin Mixer (Tumbler)

- Es werden **keine Identitätsinformationen** abgefragt
- Nutzer definiert **eine oder mehrere Zieladresse(n)**
- Nutzer legen **Verzögerungsdauer fest**
- **Nutzer legen** individuelle **Servicegebühr** fest

Lösung Bitcoin Mixer?

Quelle: https://t3n.de/news/bitcoin-mixer-tumbler-mixing-service-1329474/



https://www.heise.de/newsticker/meldung/Kryptogeld-Europol-macht-Mixingdienst-Bestmixer-io-dicht-4429704.html

- Bitcoin-Mixer vertrauen im Bezug auf **Wahrung der Anonymität**
- Bitcoin-Mixer vertrauen im Bezug auf **Durchführung der Rückzahlung**
- **IP-Traffic** zum Mixer muss zusätzlich verschleiert werden, z.B. über TOR-Browser
- Service wird auch von **Kriminellen für Geldwäsche** genutzt („Laundry Service“)
- **US-Behörden** stufen Bitcoin-Mixer als **illegal** ein

Gliederung

1	Bitcoin - Public Permissonless Blockchain
2	Datenschutzgrundverordnung
3	Lösung Anonymisierung mit Bitcoin-Mixer?
4	Schlussbetrachtung

Schlussbetrachtung

- Öffentliche, dezentrale Bitcoin-Blockchain enthält **vollständige Transaktionshistorie**
- Historie ist nicht veränderbar (**append-only Architektur)**
- Bitcoin verwendet **pseudonyme Identifikationsparameter**
  - **Personenbezug** kann ggf. durch **Verknüpfung mit weiteren Daten** hergestellt werden
  - Gefahr, dass es **irgendwann in Zukunft** durch **leistungsstarke Analysemöglichkeiten** passiert
- Änderungen an dem seit 2008 bestehenden Blockchain-Protokoll nicht umsetzbar (**hohe Marktkapitalisierung**)
- Anonymisierung mit **Bitcoin Mixer ist nicht wirklich eine Lösung**
- Wer ist **Verantwortlicher (Controller)** bei Verstößen gegen die DSG-VO? (Alle Bitcoin-Knoten-Betreiber, Alle Miner, Exchange-Anbieter, Wallet-Service, …?)

→ **Vereinbarkeit von Bitcoin und DS-GVO ist problematisch**
Besser: alternative Kryptowährung mit **Datenschutz als Entwurfsziel** verwenden (z.B. Zcash)