



Prinzipien von Blockchain-Systemen

Skalierbarkeit, Off-Chain-Transaktionen, Governance

Rainer Böhme

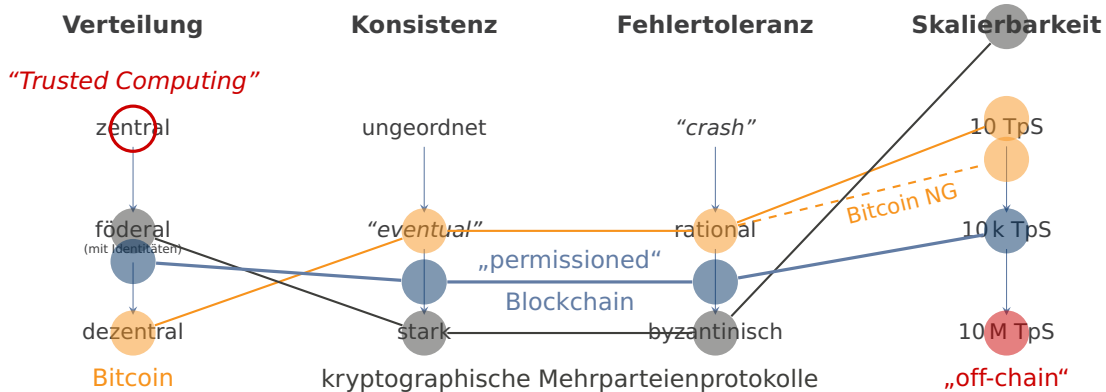
Skalierbarkeit

Motivation in Zahlen

Transaktionen pro Sekunde (TpS)	Bitcoin	Visa
Durchschnitt		2 000
aktuell (24 h)	3.1	
Spitze		56 000
1 MB Blockgröße	7	
90 % der Knoten	27	

Quellen: blockchain.info, 31. Mai 2020, Visa Tech Matters, 2014, Croman, K., et al. On Scaling Decentralized Blockchains. In Clark, J., et al. *3rd Workshop on Bitcoin and Blockchain Research*, LNCS 9604, Springer, Berlin, 2016, 106–125.

Gestaltungsspielraum für Blockchain-Systeme



adaptiert nach Wattenhofer, R., *An Efficient Blockchain?*, Oslo, 14. September 2017.

Besitznachweis statt Arbeitsnachweis



Proof of Stake ist im Prinzip ein Spezialfall föderaler Systeme:

- Pseudonyme aus vergangenen Zuständen (genauer: deren Verfügungsgewalt über eine knapper Ressource) werden als Identitäten zur Bestimmung des Leaders für zukünftige Zustände herangezogen.
- Durch diese Selbstreferenz entfällt die Notwendigkeit der Kopplung an knappe Ressourcen in der Realwelt.
(z. B. Rechenleistung, eindeutige und starke Identitäten)
- Identitäten ("*stake*") können übertragen und gehandelt werden.

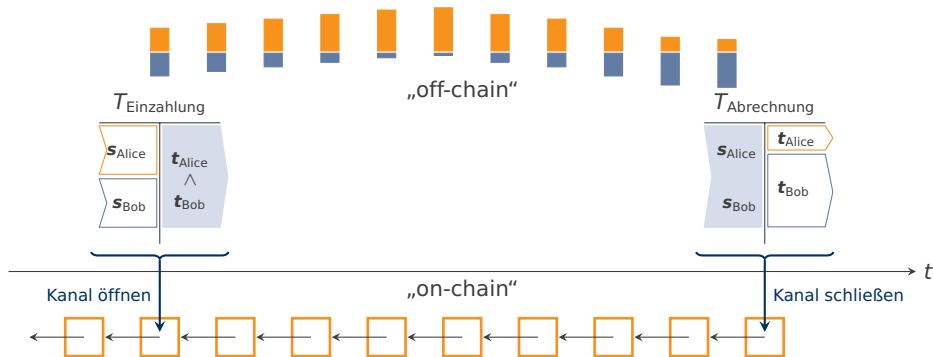
Details der Umsetzung

Nicht alle Parteien sind immer **online** und **riskieren** den Einsatz ihrer privaten Schlüssel für ein öffentliches Gut. Deshalb setzen PoS-Verfahren auf **Freiwilligkeit** und **belohnen** die Bereitschaft mit neuen bzw. umverteilten Werteinheiten.

Prinzip von Off-Chain-Zahlungskanälen

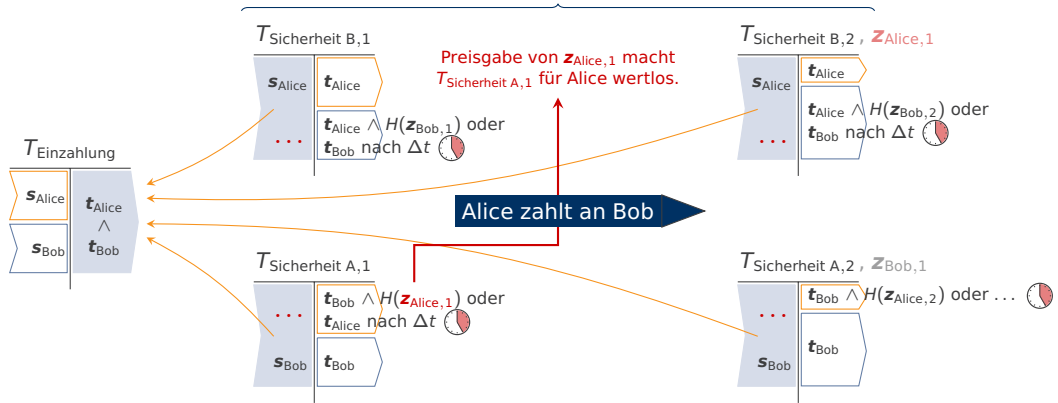
Analogie Die Blockchain ist nicht mehr globaler Kassenzettel, sondern Gerichtsbuch.

- Transaktionspartner legen Geld zur Seite und rechnen darüber lokal ab.
- Im Streitfall wird der letzte Zustand mithilfe der Blockchain durchgesetzt.



Off-Chain-Zahlungskanäle im Lightning-Protokoll

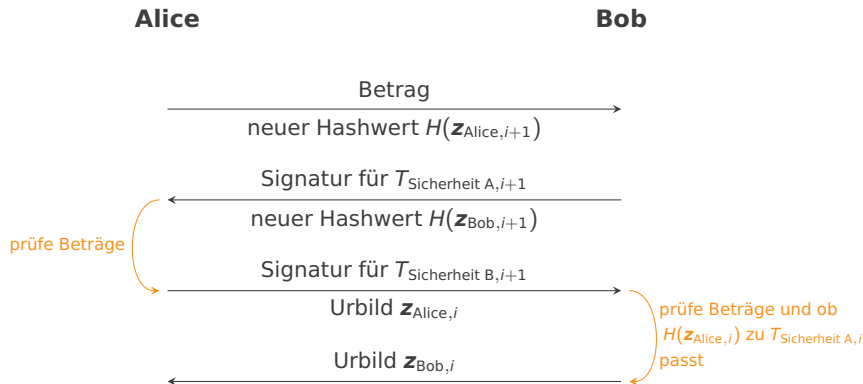
im Normalfall nicht publiziert



Poon, J., Dryja, T. *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*, 2016.

Ablaufdiagramm

Beispiel Alice bezahlt Bob über einen bestehenden Kanal

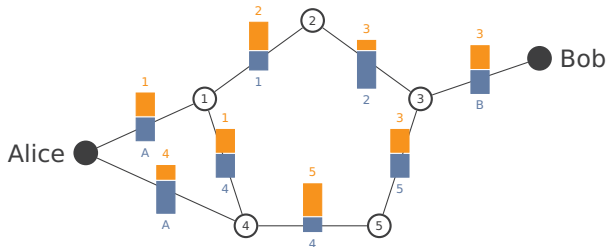


vgl. Abbildung 3 in McCorry, P., Möser, M., et al. Towards Bitcoin Payment Networks. In Liu, J., Steinfeld, R., eds., *Information Security and Privacy (Proceedings of ACISP)*, LNCS 9722, Springer, Berlin, 2016, 57–76.

Verallgemeinerung zu Off-Chain-Zahlungsnetzen

Problem Zu viele potenzielle Tauschpartner, um mit jedem einen Kanal zu finanzieren.

- Kopplung bilateraler Kanäle zu einem Zahlungsnetz
- Viel Forschungsbedarf: Routing, Gebühren, Optimierung, atomarer Ende-zu-Ende-Tausch, Sicherheit, Datenschutz, . . . , **Unterstützung allgemeiner Smart Contracts?**



Decker, C., Wattenhofer, R. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels. In Pelc, A., Schwazmann, A., eds., *Stabilization, Safety, and Security of Distributed Systems*. LNCS 9212, Springer, Berlin, 2015, 3–28.

Governance

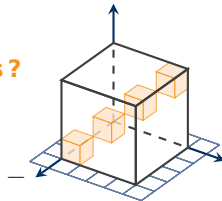
Frage Wer entscheidet über die (Weiter-)Entwicklung eines Blockchain-Systems?
Entwickler-Community, Nutzer, Miner, Firmen, Staaten, ...

Wie finden wir einen Konsens über den Konsens-Mechanismus?

Modellierung als **Koordinationspiel** in strategischer Form:

Spieler 1 \ Spieler 2	Protokoll A	Protokoll B
Protokoll A	1, 1	0, 0
Protokoll B	0, 0	1, 1

Nash-
Gleichgewichte



Schelling, T. *The Strategy of Conflict*, Wiley, 1960.

Kritische Masse

Modellvariante für n Spieler: Der Nutzen ist nicht $\in \{0, 1\}$, sondern proportional zur Anzahl der Spieler, die die gleiche Strategie wählen.

Beispiele

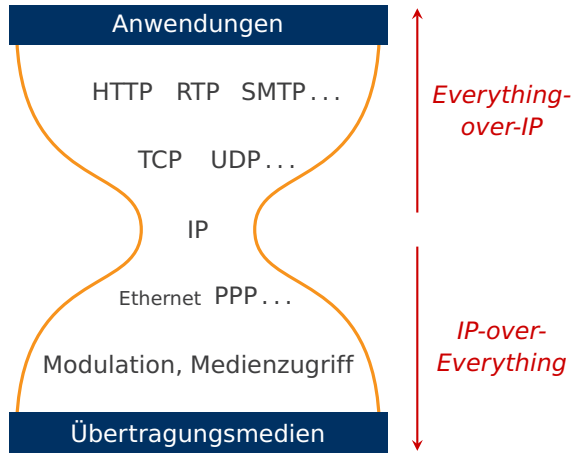
- Das gleiche **Protokoll** → vgl. Sanduhr-Metapher im TCP/IP-Protokollstapel
- Die gleiche **Währung** → „Geld ist ein soziales Konstrukt.“

Konsequenzen

- Ist eine **kritische Masse** erreicht, lohnt sich abweichen nicht. (Wechselkosten)
- **Wettbewerb** nur zur Adoptionsphase: Winner-takes-it-all

These zu Bitcoin: Darknet-Nutzer ohne Zahlungsalternative brachten kritische Masse.

Sanduhr-Metapher für Internet-Protokolle



Vgl. VO Rechnernetze und Internettechnik, Kapitel „Verteilte Systeme“, 13. Juni 2019, S. 33

Exkurs: Geldbegriff

Ansatz 1: Institutionell

„Das in einer Gesellschaft allgemein anerkannte Tausch- und Zahlungsmittel, das unterschiedliche Geldformen annehmen kann. Als Geld bezeichnet man üblicherweise die Verbindlichkeit einer Bank gegenüber einer Nichtbank, also z. B. Bargeld oder eine Einlage.“

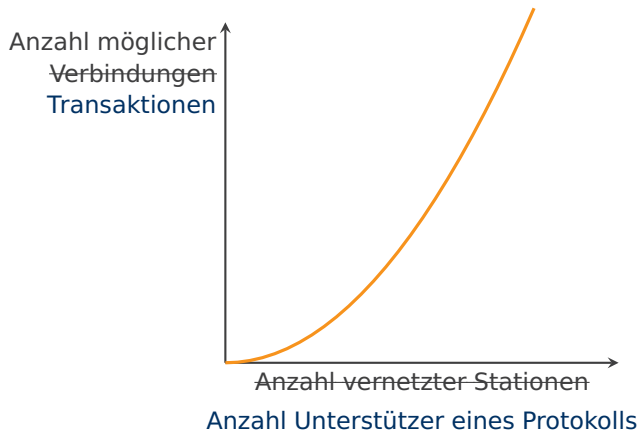
Ansatz 2: Pragmatisch

„Geld ist, was die Geldfunktionen erfüllt.“

Geldfunktionen

- Tauschmittelfunktion → ausreichend Tauschpartner
- Wertaufbewahrungsfunktion → Erwartungen für die Zukunft
- Rechenmittelfunktion → Preisangaben

Metcalfe'sches Gesetz



Vgl. VO Rechnernetze und Internettechnik, Kapitel „Einführung“, 7. März 2019, S. 5

Signale

Wie findet ein laufendes System andere mögliche Nash-Gleichgewichte?

(Die Frage, welches Gleichgewicht sich einstellt, wird in der klassischen Spieltheorie nicht beantwortet.)

- Teilnehmer verständigen sich auf Zeichen, die Reaktion auf andere Strategien kommunizieren.

Im einfachsten Fall ohne Konsequenzen als **“cheap talk”**: d. h. bluffen erlaubt.

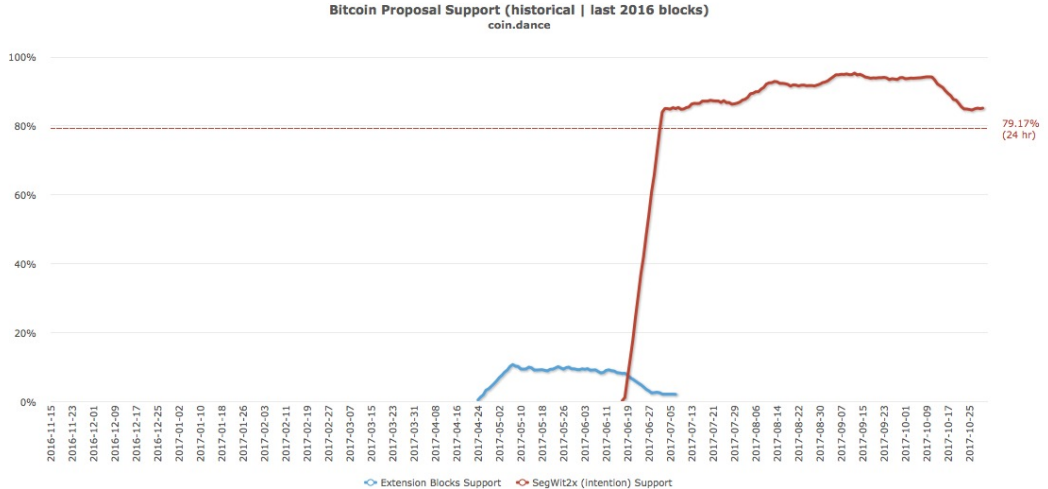
- **Signale** im engeren Sinn sind Zeichen, die teurer zu produzieren sind, wenn ihr Wert von der eigenen Präferenz abweicht, als wenn er damit übereinstimmt.

Beispiel bei Blockchain-Systemen: Protokolländerung

Miner Activated Soft Fork (MASF) nach BIP 9:

- Miner setzen vereinbarte Bits im Block-Header.
- Wenn ein Quorum erreicht ist, wird nach einer Wartezeit verbindlich auf das neue Protokoll gewechselt.

Beispiel

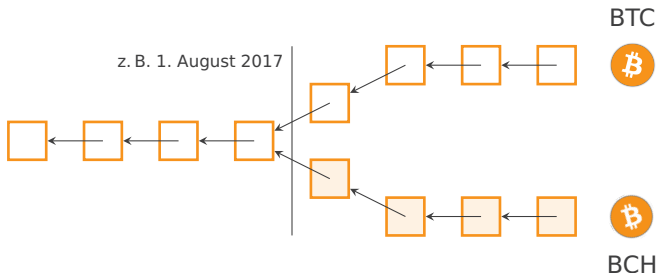


Quelle: <https://coin.dance/blocks#proposals>, Stand: 30. Oktober 2017

Blockchain-Fork

Dissens mit gemeinsamer Vergangenheit

- Unterschiedliche Regeln zur Fortschreibung der öffentlichen Datenbasis
- Die Miner entscheiden über Erfolg oder Untergang jedes Asts.

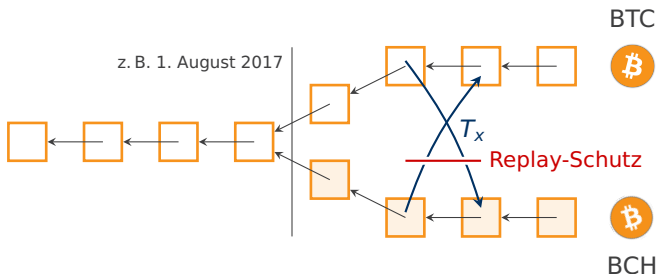


- (Alt-)Nutzer genießen eine „Verdopplung“ der Einheiten.
- Im Gegensatz zu einem Altcoin-Launch ist die kritische Masse damit sofort erreicht.

Blockchain-Fork

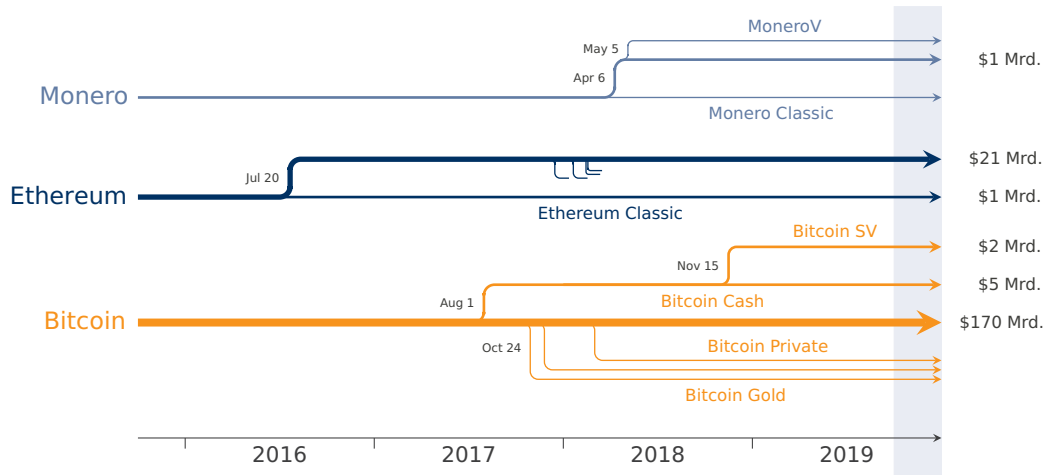
Dissens mit gemeinsamer Vergangenheit

- Unterschiedliche Regeln zur Fortschreibung der öffentlichen Datenbasis
- Die Miner entscheiden über Erfolg oder Untergang jedes Asts.



- (Alt-)Nutzer genießen eine „Verdopplung“ der Einheiten.
- Im Gegensatz zu einem Altcoin-Launch ist die kritische Masse damit sofort erreicht.

Zeitleiste ausgewählter Forks



Quelle: coinmarketcap.com · Stand: November 2019

Größenordnung der Bitcoin-Ökonomie

	Euroraum		Bitcoin	
Marktwert der Bitcoins im Umlauf			157	14.8
Bargeldumlauf	1 277	8.0		
Sichteinlagen	8 231	12.5		
M1	9 508	11.9		
M3	13 639	8.3		

Bestände in Mrd. Euro. **Jährliche Wachstumsraten in %.**

Quellen: Europäische Zentralbank (April 2020, veröffentlicht am 29.05.2020), blockchain.info (31.05.2020)

Öffentliche Wahrnehmung

von Bitcoins und Alt-Coins als Ausgangspunkt für die rechtliche Einordnung

Bitcoin: A Peer-to-Peer Electronic Cash System

Client Dell Now Accepts Bitcoin

**Microsoft Now Accepts Bitcoin
Through BitPay**

Caleb Chen on 11/12/2014

„Zahlung“ mit Bitcoins

Sind Bitcoins Geld ?



Abgrenzung von Geldbegriffen im Recht



Ökonomische Geldfunktionen

- Tauschmittelfunktion
- Wertaufbewahrungsfunktion
- Rechenmittelfunktion

Rechtliche Einordnung

Tauschmittelfunktion

„Zahlungen“ mit Cryptocoins finden überwiegend über spezielle Zahlungsdienste statt, begleitet von zwei **Wechselgeschäften**.

Cryptocoin-Transaktionen dienen insofern nur als Vehikel für Geld.

Wertaufbewahrungsfunktion

Wertaufbewahrung setzt eine gewisse Preisstabilität voraus.

Die **Volatilität** ihrer Preise macht Cryptocoins als Wertaufbewahrungsmittel unattraktiv. Gehalten werden Cryptocoins eher zu Spekulationszwecken.

Rechenmittelfunktion

Cryptocoin-Beträge sind zwar skalierbar und der Wert von Marktoobjekten lässt sich in ihnen ausdrücken.

Die Rechenmittelfunktion ist aber technisch nicht abgesichert, wenn **Fungibilität** nicht gewährleistet ist.

Chancen

„Endlich ein **Zahlungssystem**, das dem Internet gerecht wird!“

— Wirtschaftlichkeit, Bequemlichkeit

Das Prinzip der **verteilten Kontrolle** im praktischen Einsatz

— Mitbestimmung, technische Eleganz

Eine Technologie, die mehr **Transparenz** in das Finanzsystem bringt

— Gerechtigkeit, Effizienz

Chancen (Forts.)

Ein **Plattform** für neue Erfindungen

— Innovation, Wachstum

Ein **Technologie-Trend**, der die Ablösung alter Systeme beschleunigt

— Impuls, wirtschaftliche Chance

Ein alternatives **Gesellschaftsmodell** für anspruchsvolle „Digital Natives“

— Partizipation, Vision

Problemfelder

(langfristige Risiken unter der **Annahme** massiver Verbreitung)

- Verlust geldpolitischer Steuerungsmöglichkeit
- Verlust von Seniorage-Gewinnen
- Verstärkung der digitalen Spaltung
- Weitere Erosion des Datenschutzes
- Machtverschiebung zu rechenschaftslosen Wirtschaftssubjekten
- Kontrollverlust durch Umgehung rechtsstaatlicher Institutionen

Gut gestaltete Technik kann einige, aber nicht alle Bedenken zerstreuen.

Gretchenfrage für Blockchain-Systeme



James Tissot. Faust und Gretchen im Garten, 1861. Quelle: <http://www.bilder-geschichte.de>

Syllabus

05.03.20	1. Einführung und Grundlagen	
23.04.20	2. Infrastruktur für Blockchain-Systeme	
30.04.20	3. Transaktionslogik in Bitcoin und Ethereum	
07.05.20	Übung: Blockchain-Analyse mit BlockSci	(Martin Plattner)
14.05.20	4. Datenschutz und Sicherheit	
28.05.20	Übung: Ethereum-Programmierung mit Solidity	(Michael Fröwis)
04.06.20	5. Skalierbarkeit, Off-Chain-Transaktionen, Governance	
18.06.20	6. Wiederholung, Fragestunde	
25.06.20	Klausur	(15:30–16:30, HSB1)

Stand: 3. Juni 2020. Änderungen vorbehalten.