universität innsbruck

Prinzipien von Blockchain-Systemen

Skalierbarkeit, Off-Chain-Transaktionen, Governance

Rainer Böhme

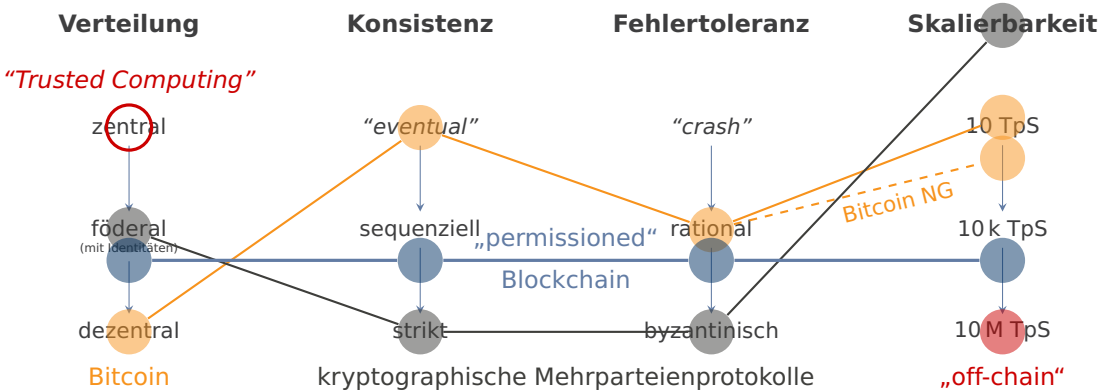
Skalierbarkeit

Motivation in Zahlen

Transaktionen pro Sekunde (TpS)	**Bitcoin**	**Visa**
Durchschnitt		2 000
aktuell (24 h)	3.5	
Spitze		56 000
1 MB Blockgröße	7	
90 % der Knoten	27	

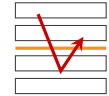
Quellen: blockchain.info, 30. Oktober 2017, Visa Tech Matters, 2014, Croman, K., at al. On Scaling Decentralized Blockchains. In Clark, J., et al. *3rd Workshop on Bitcoin and Blockchain Research*, LNCS 9604, Springer, Berlin, 2016, 106–125.

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)

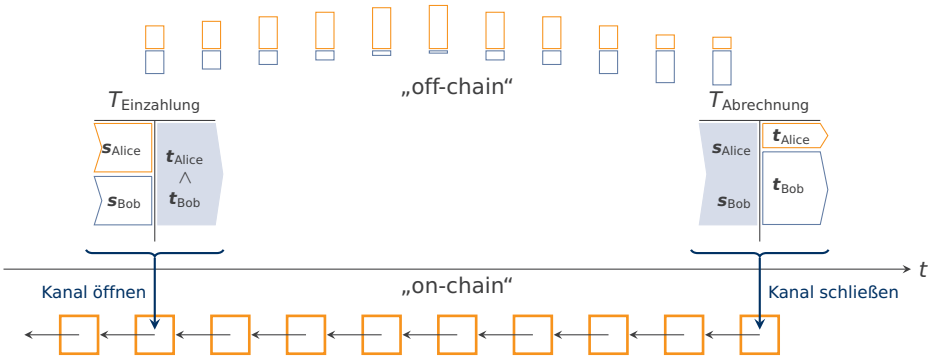
Details der Umsetzung

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.

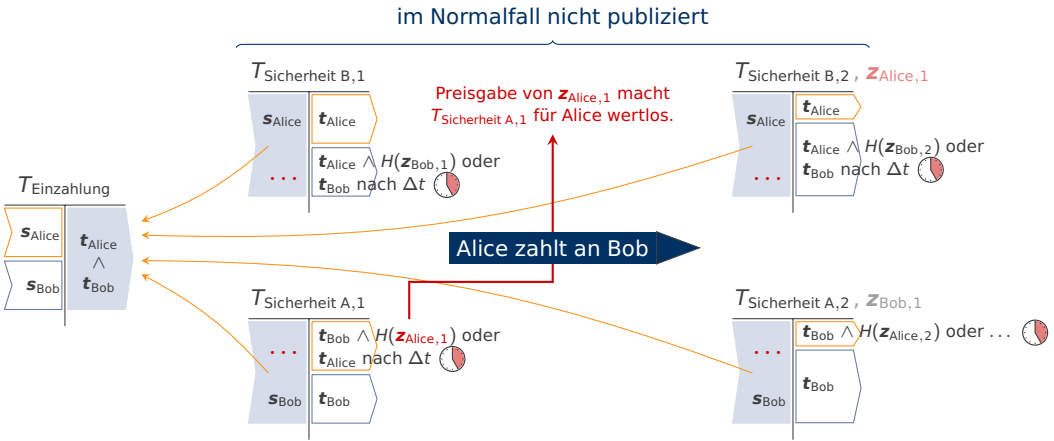
Prinzip von Off-Chain-Zahlungskanälen

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.



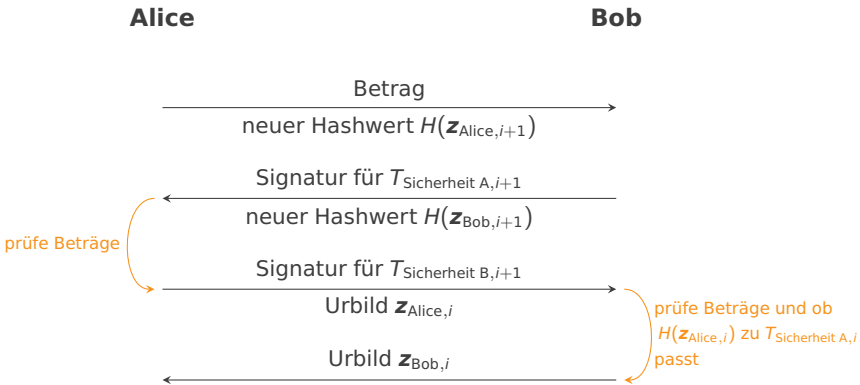
Off-Chain-Zahlungskanäle mit dem Lightning-Protokoll



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

Ablaufdiagramm

Beispiel Alice bezahlt Bob über einen bestehenden Kanal

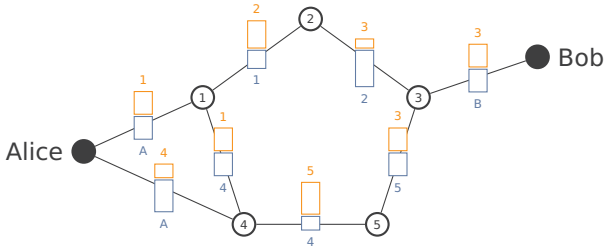


vgl. Abbildung 3 in McCorry, P., Möser, M., et al. Towards Bitcoin Payment Networks. In Liu, J., Steinfeld, R., eds., *Information Security and Privacy (Proceedings of ACISP)*, LNCS 9722, Springer, Berlin, 2016, 57–76.

Verallgemeinerung zu Off-Chain Zahlungsnetzen

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

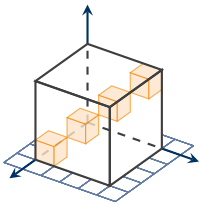
- Kopplung bilateraler Kanäle zu einem Zahlungsnetz
- Viel Forschungsbedarf: Routing, Gebühren, Optimierung, atomarer Ende-zu-Ende-Tausch, Sicherheit, Datenschutz, . . . , Unterstützung allgemeiner Smart Contracts ?



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 **Koordinationsspiel** 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

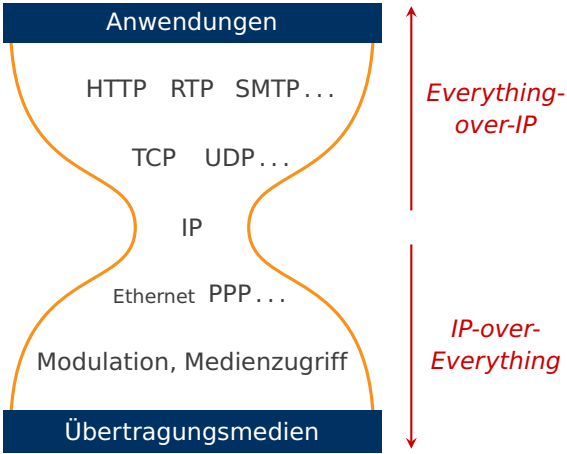
- Das gleiche **Protokoll** $\rightarrow$ vgl. Sanduhr-Metapher im TCP/IP-Protokollstapel
- Die gleiche **Währung** $\rightarrow$ „Geld ist ein soziales Konstrukt“

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“, 8. Juni 2017, S. 32

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

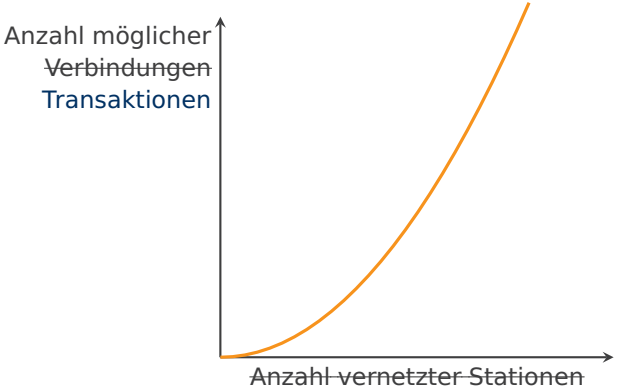
> *„Geld ist, was die Geldfunktionen erfüllt.“*

Geldfunktionen

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

J. Metzger, Gabler Wirtschaftslexikon

Metcalfe’sches Gesetz



Vgl. VO Rechnernetze und Internettechnik, Kapitel „Einführung“, 9. März 2017, 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 signalisieren.

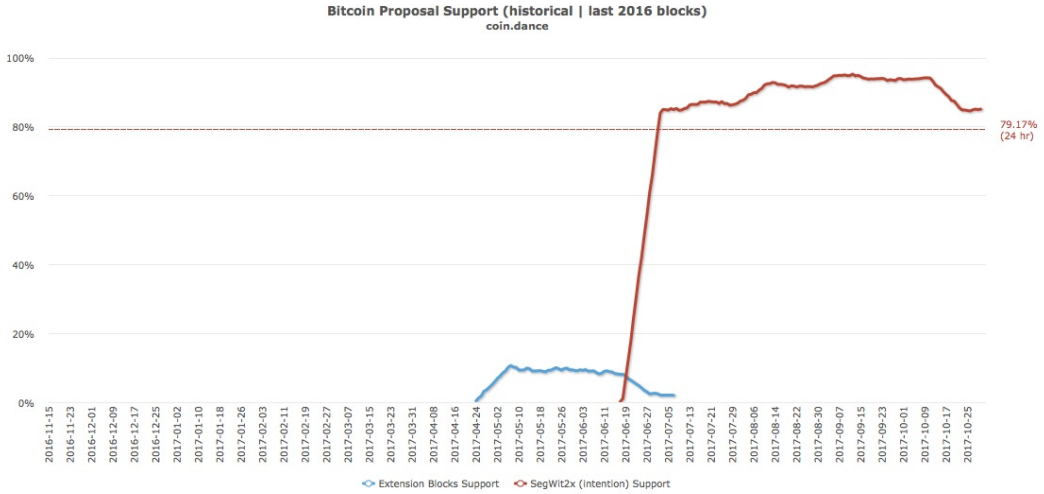
  Im einfachsten Fall ohne Konsequenzen als **“cheap talk”**: d. h. bluffen erlaubt.
- **Signale** im engeren Sinn sind Zeichen, die teurer zu produzieren sind, wenn ihr Wert von der eigenen Präferenz abweicht, als wenn er damit übereinstimmt.

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

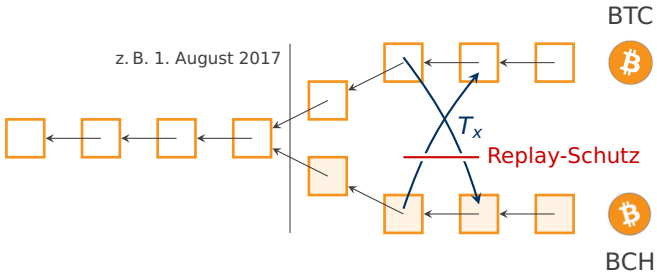


Quelle: `https://coin.dance/blocks#proposals`, Stand: 30. Oktober 2017

Blockchain-Fork

Dissens mit gemeinsamer Vergangenheit

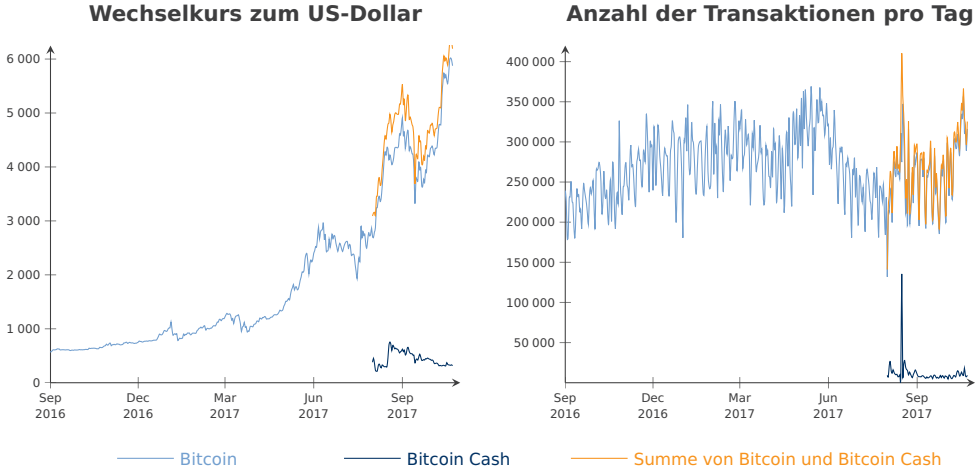
- Unterschiedliche Regeln zur Fortschreibung der öffentlichen Datenbasis
- Die Miner entscheiden über Erfolg oder Untergang jedes Asts.



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

Prognose: Forks werden die neuen ICOs.

Marktbewertung des Bitcoin-Cash-Forks



blockchain.info, bitinfocharts.com, Stand: 23. Oktober 2017

Größenordnung der Bitcoin-Ökonomie

	Euroraum		Bitcoin	
Marktwert der Bitcoins im Umlauf			88	927.3
Bargeldumlauf	1 103	3.4		
Sichteinlagen	6 579	10.8		
M1	7 682	9.7		
M3	11 797	5.1		

Bestände in Mrd. Euro. Jährliche Wachstumsraten in %.

Quellen: Europäische Zentralbank (September 2017, veröffentlicht am 26. Oktober 2017), blockchain.info (30. Oktober 2017)

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`

Vorlesungsplan

03.10.17	1. Einführung und Grundlagen
10.10.17	2. Infrastruktur für Blockchain-Systeme
17.10.17	3. Transaktionslogik in Bitcoin und Ethereum
24.10.17	4. Datenschutz und Sicherheit
31.10.17	5. Skalierbarkeit, Off-Chain-Transaktionen, Governance
07.11.17	6. Wiederholung, Fragestunde, Anmeldefrist zur Klausur
21.11.17	Klausur (HSB 3)

Änderungen vorbehalten.

Proseminarplan

11.10.17	1. Besprechung von Übungszettel 1 (wird im OLAT bereitgestellt)
18.10.17	2. Besprechung von Übungszettel 2
25.10.17	3. Besprechung von Übungszettel 3
08.11.17	4. Besprechung von Übungszettel 4
15.11.17	5. Besprechung von Übungszettel 5
06.12.17	6. Aufbau eines Bitcoin-Testnetzes
12.–13.12.17	7./8./9. Blockveranstaltung: Blockchain-Analyse mit BlockSci
10.01.18	10. Besprechung von Übungszettel 6
17.01.18	11. Konzepte der Ethereum-Programmierung mit Solidity
23.–24.01.18	12./13./14. Blockveranstaltung: Smart-Contract-Programmierung
31.01.18	15. Zusammenfassung und Ausblick

Änderungen vorbehalten.