universität innsbruck

VIRTCRIME

AUSTRIAN INSTITUTE OF TECHNOLOGY

Aktuelle Entwicklungen und Ausblick

VIRTCRIME Kryptowährungs-Forensik-Training

Rainer Böhme

Gliederung

1. Off-chain Payment Channels
2. Kommerzielle und staatliche Kryptowährungen

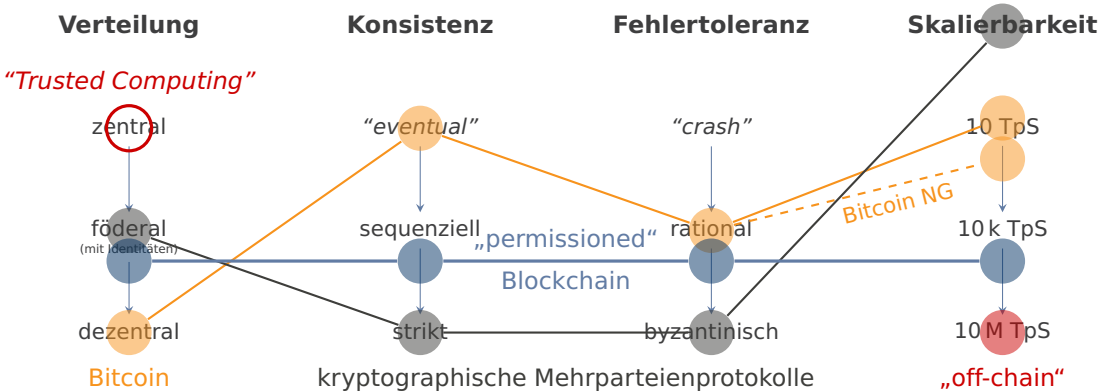
Skalierbarkeit

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 P2P-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.

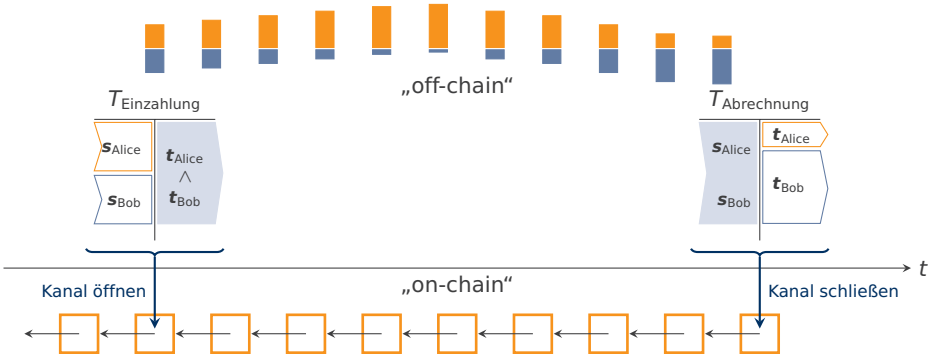
Gestaltungsspielraum für Blockchain-Systeme



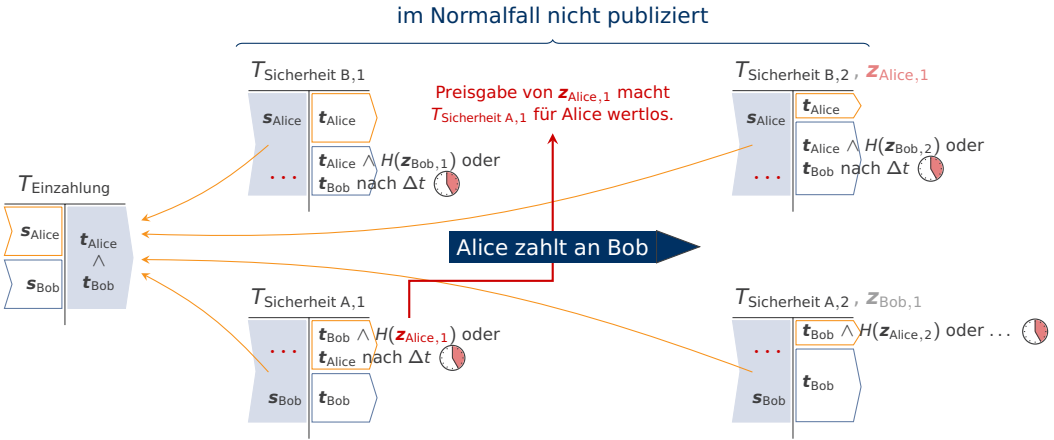
Prinzip von Off-Chain-Zahlungskanälen

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

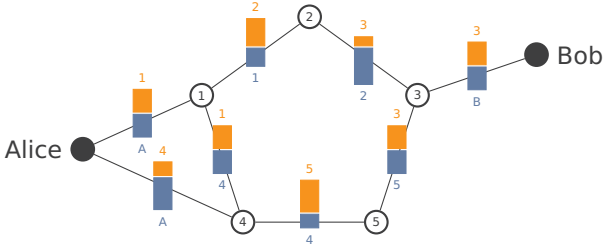


Poon, J., Dryja, T. *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*, 2016.

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, . . . , Forensik ?



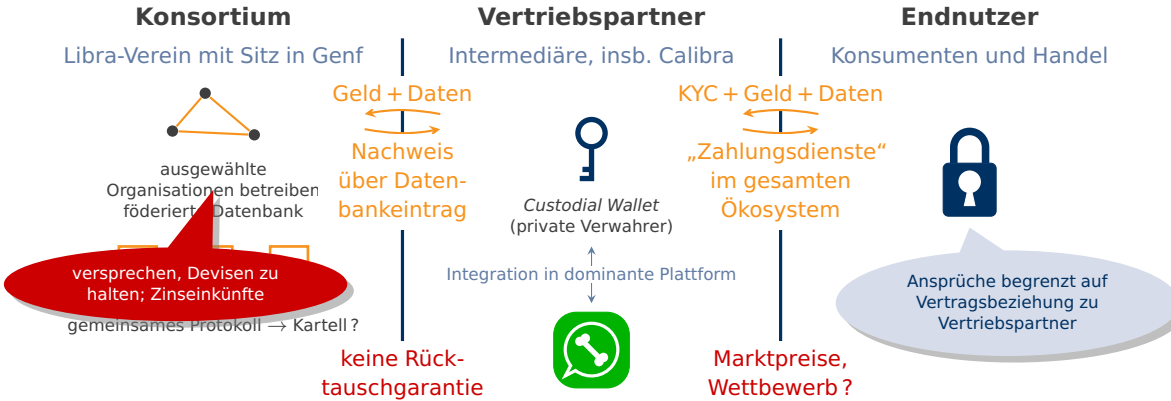
Decker, C., Wattenhofer, R. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels. In Pelc, A., Schwazmann, A., eds., *Stabilization, Safety, and Security of Distributed Systems*. LNCS 9212, Springer, Berlin, 2015, 3–28.

Gliederung

1. Off-chain Payment Channels
2. **Kommerzielle und staatliche Kryptowährungen**

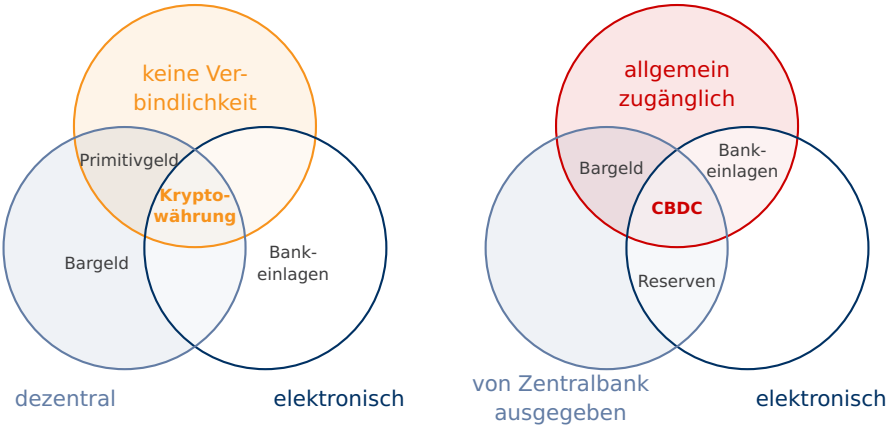
Facebooks Libra auf einer Folie

Irreführende Analogien: Libra wäre weder eine Kryptowährung noch ein Stablecoin.



Gedankenexperiment: Digitales Zentralbankgeld

Einordnung von alten und neuen Geldformen



M. Bech & R. Garratt. Central bank cryptocurrencies. *BIS Quartely Review*, September 2017, S. 59.

Geld als kollektives Gedächtnis

“Money may only be an imperfect substitute for high quality information storage and access. [. . .]

Government’s monopoly on seignorage might be in some jeopardy as information access and storage costs decline.”

→ Wenn Kriminelle digital kommunizieren können, dann können sie Werte austauschen und eine Art Schatten-Rechtssystem aufbauen.

Narayana R. Kocherlakota, 1996, S. 28

Gretchenfrage für Blockchain-Systeme

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