universität innsbruck

Von Kryptowährungen zum digitalen Euro

Technische Grundlagen

Rainer Böhme

Innsbruck, 10. Dezember 2020

Sorry . . .

Die Technik hinter Blockchain-Systemen in 15 Minuten – das geht nicht.

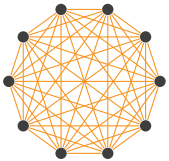
VU Prinzipien von Blockchain-Systemen

Zum Nachlesen und Nachsehen aus dem virtuellen Sommersemester 2020:

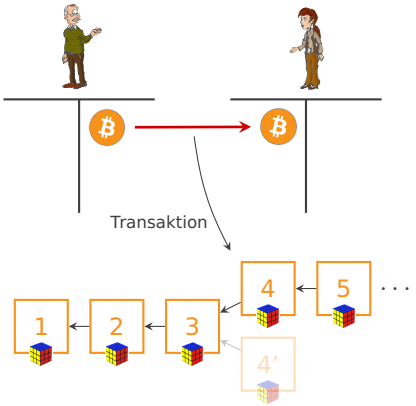
`https://informationsecurity.uibk.ac.at/teaching/blockchain/`

Zielgruppe: Drittes Studienjahr Informatik-Bachelor

Bitcoin auf einer Folie



P2P-Netzwerk



Bitcoin-Blockchain

Nakamoto 2008

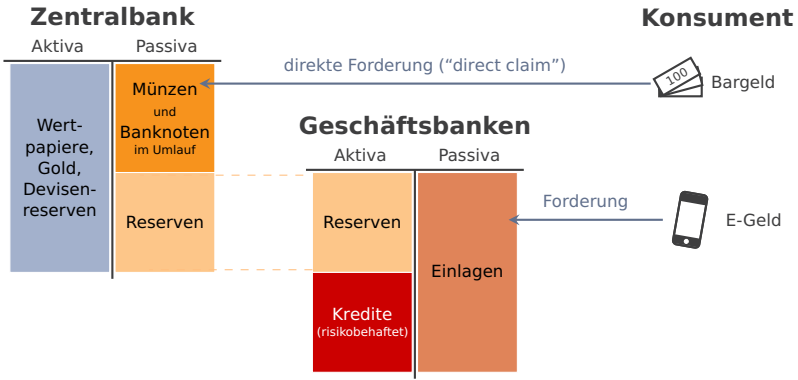
Geld als kollektives Gedächtnis

“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.”

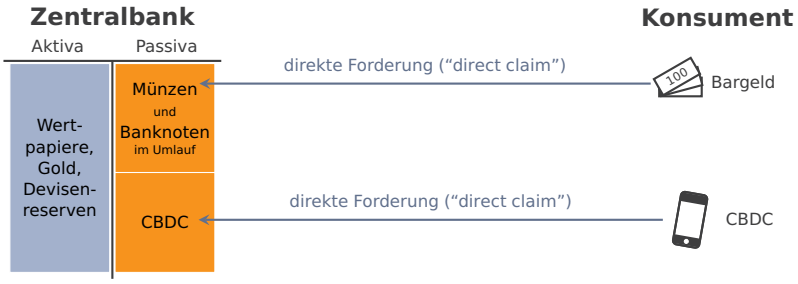
Narayana R. Kocherlakota, 1996, S. 28

Bargeld und E-Geld im Geldsystem



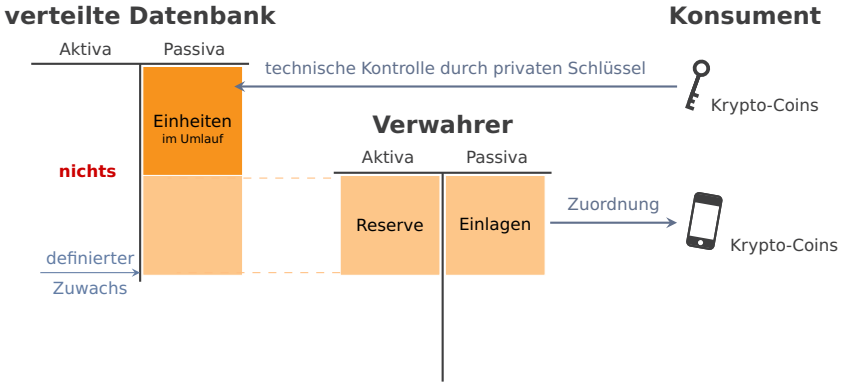
Zum Vergleich: Zentralbank-Digitalgeld (CBDC)

Annahme: aktuelle Überlegungen werden umgesetzt



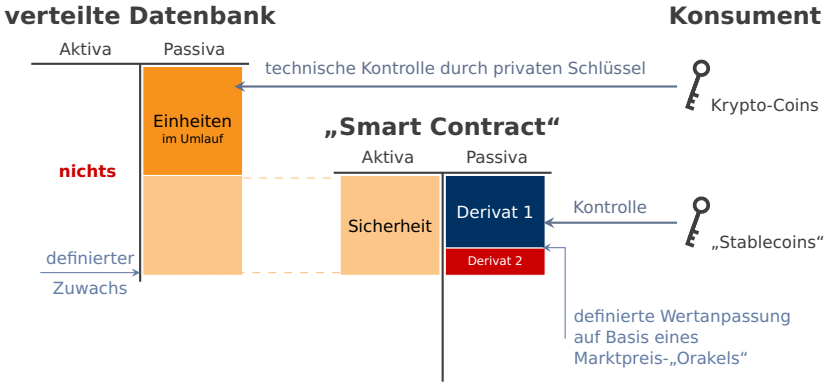
Zum Vergleich: Kryptowährungen

Annahme: technisch versierte Nutzung



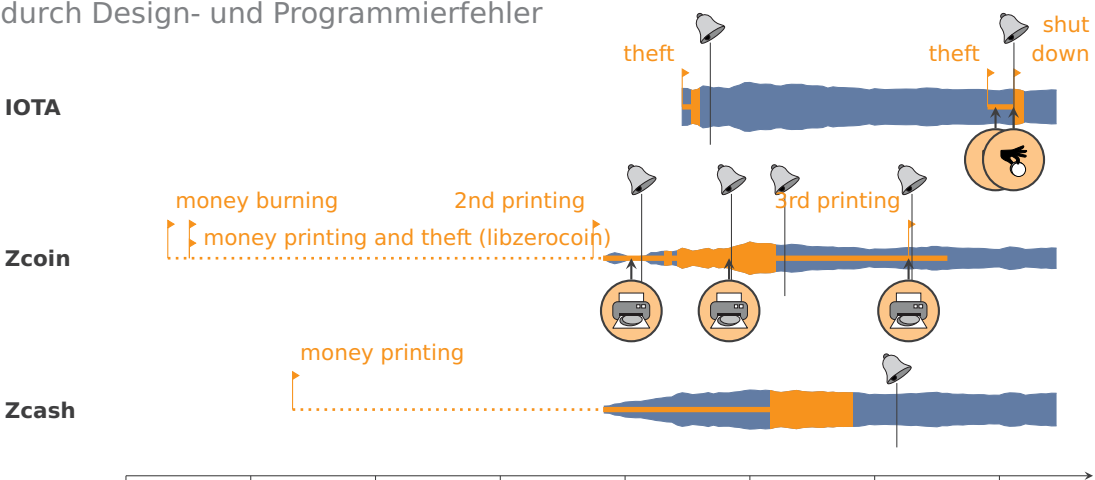
Ausblick: Krypto-Finanzinstrumente

Vermutung: Umgehung bestehender Finanzmarkt-Regulierung



Bekannte Schwachstellen

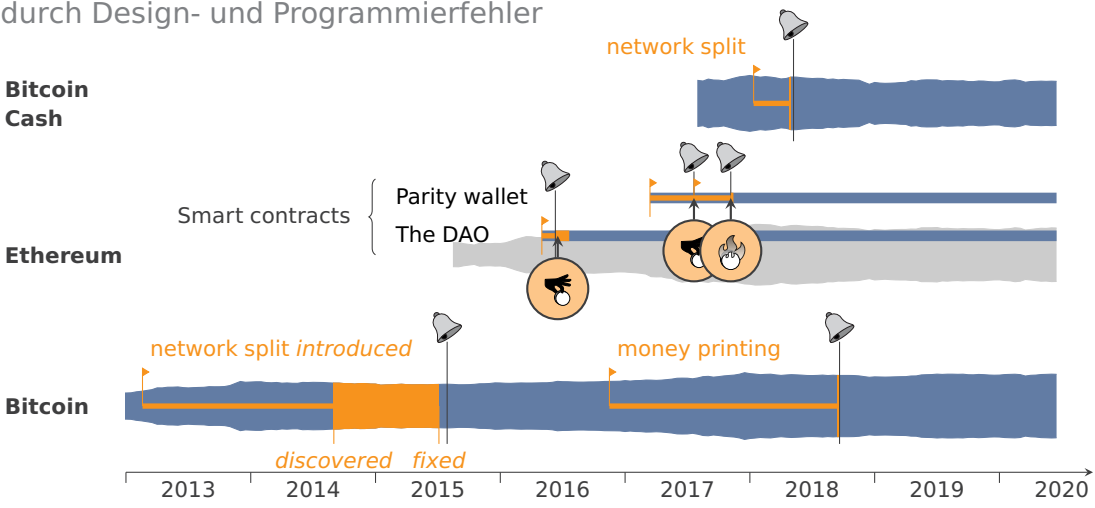
durch Design- und Programmierfehler



Böhme et al. (2020): Responsible vulnerability disclosure in cryptocurrencies. *Communications of the ACM* **63** (10), S. 62–71.

Bekannte Schwachstellen (Forts.)

durch Design- und Programmierfehler



Böhme et al. (2020): Responsible vulnerability disclosure in cryptocurrencies. *Communications of the ACM* **63** (10), S. 62–71.

Fazit

1. Verstehen Sie die Technik – sie ist faszinierend, aber sehr anspruchsvoll
2. Verstehen Sie die Risiken – es gibt viele Déjà-vus
3. Im Gegensatz zu Kapitalmärkten sind Kryptomärkte selbst in der Theorie nicht wohlfahrtsfördernd.
4. CBDC wird bestenfalls ein unvollständiger Ersatz für Bargeld.

Literatur

A. Böhme, R., Christin, N., Edelman, B., and Moore, T.
Bitcoin: Economics, Technology, and Governance.
Journal of Economic Perspectives, 29, 2 (2015), S. 213–238.

B. Auer, R. and Böhme, R.
The Technology of Retail Central Bank Digital Currency.
BIS Quartely Review, (März 2020), S. 85–100.

C. Böhme, R., Eckey, L., Moore, T., Narula, N., Ruffing, T., and Zohar, A.
Responsible Vulnerability Disclosure in Cryptocurrencies.
Communications of the ACM, 63, 10 (Oktober 2020), S. 62–71.

universität innsbruck

Danke fürs Zuhören

Von Kryptowährungen zum digitalen Euro

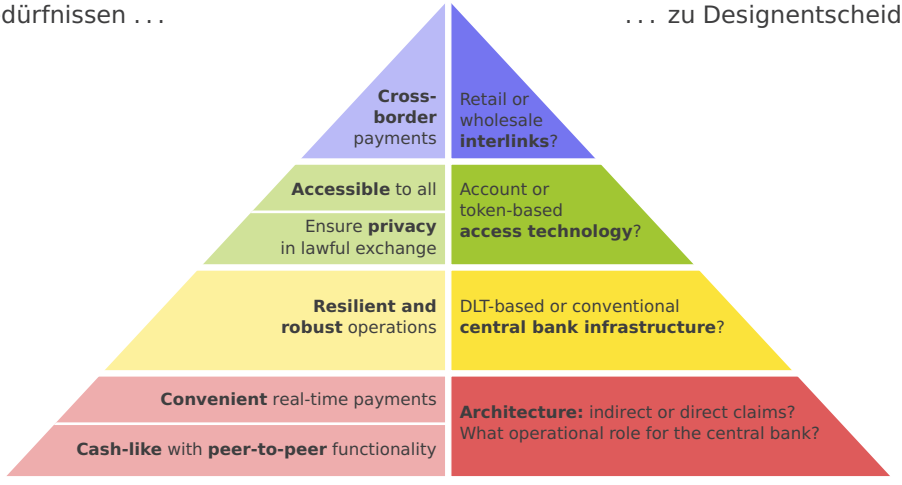
Rainer Böhme

https://informationsecurity.uibk.ac.at/people/rainer-boehme/

Die CDBC-Pyramide

Von Bedürfnissen . . .

. . . zu Designentscheidungen



Auer & Böhme, *BIS Quarterly Review*, März 2020, S. 87.