VOM FRANKEN ZUM TOKEN
HAT UNSERE WÄHRUNG AUSGEDIENT?

ALEKSANDER BERENTSEN CIF.UNIBAS.CH

University of Basel

Center for Innovative Finance

Efficiency Club
Wirtschaft im Dialog
15 November 2018
THE DOLDER GRAND, Zürich

STOP TRYING TO CREATE MONEY!!!

‘Stop Trying to Create Money!’: BIS Chief Carstens on Cryptocurrency

CARSTENS ON BITCOIN

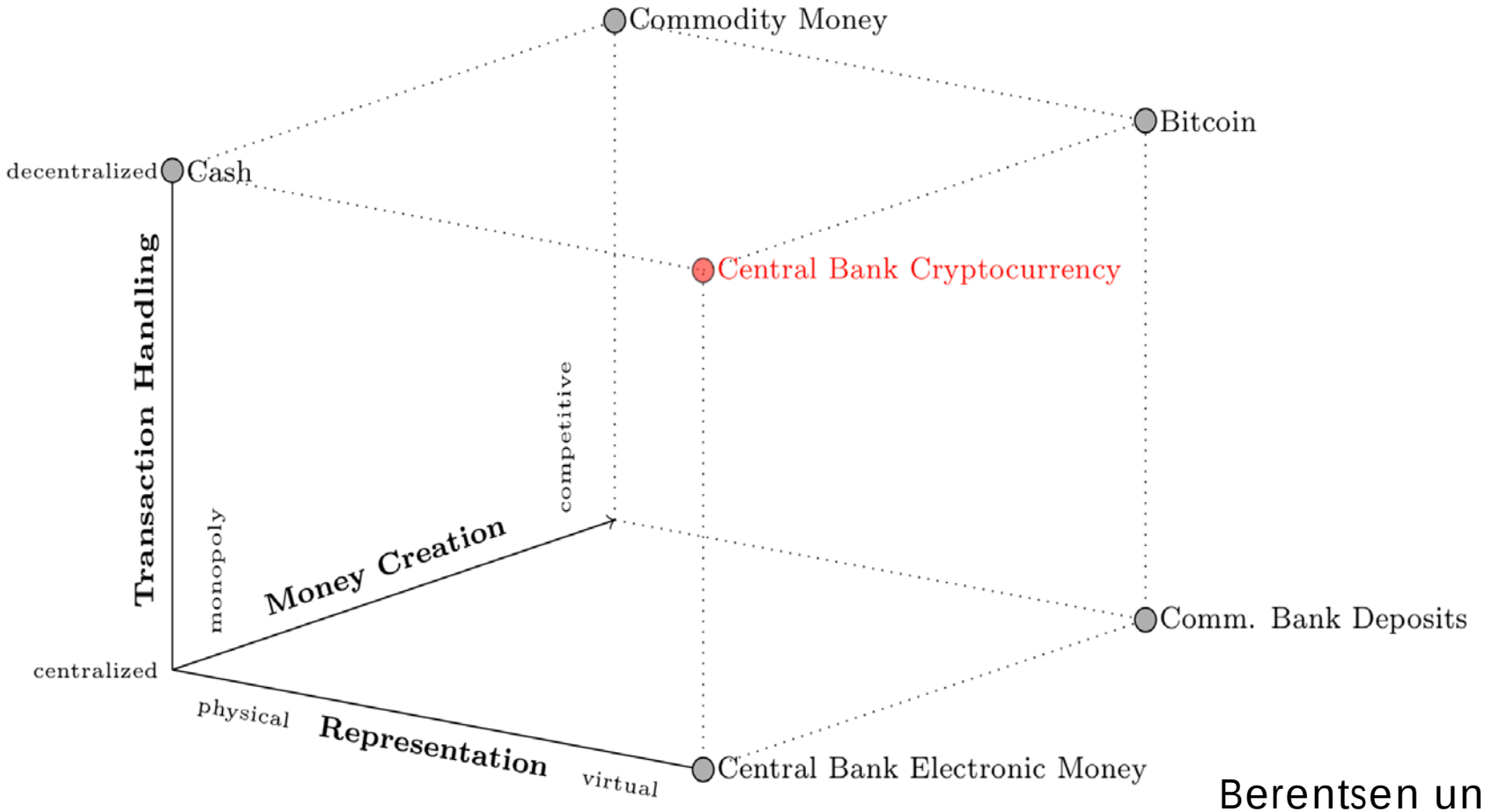
- “Die junge Generation sollte ihr Talent und ihre Fähigkeiten besser für Innovationen einsetzen, aber nicht, um Geld nochmals neu zu erfinden.”

- “Es ist ein Trugschluss zu glauben, dass man aus dem Nichts Geld schaffen kann.”

Augustin Carstens, BIS

Quelle: BAZ-Artikel vom 25.06.2018

WAS IST BITCOIN?



Berentsen und Schär (2017)

WAS IST BITCOIN?

- Was ermöglicht diese Dezentralität?
  - Antwort: Bitcoin Blockchain

- Was ist der Vorteil der Dezentralität?
  - Antwort: Bitcoin ist ein zensurresistenter Vermögenswert.

WAS IST EINE BLOCKCHAIN?

- Bitcoin Blockchain ist eine Datenbank mit einigen besonderen Regeln.
- Die besondere Kombination von Regeln wurde 2008 von Satoshi Nakamoto - dem Erfinder von Bitcoin - entwickelt.
- Nakamotos Ziel war es, eine **zensurresistente** Peer-to-Peer-Version von Electronic Cash zu schaffen.

PEER-TO-PEER-VERSION VON ELECTRONIC CASH

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 network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

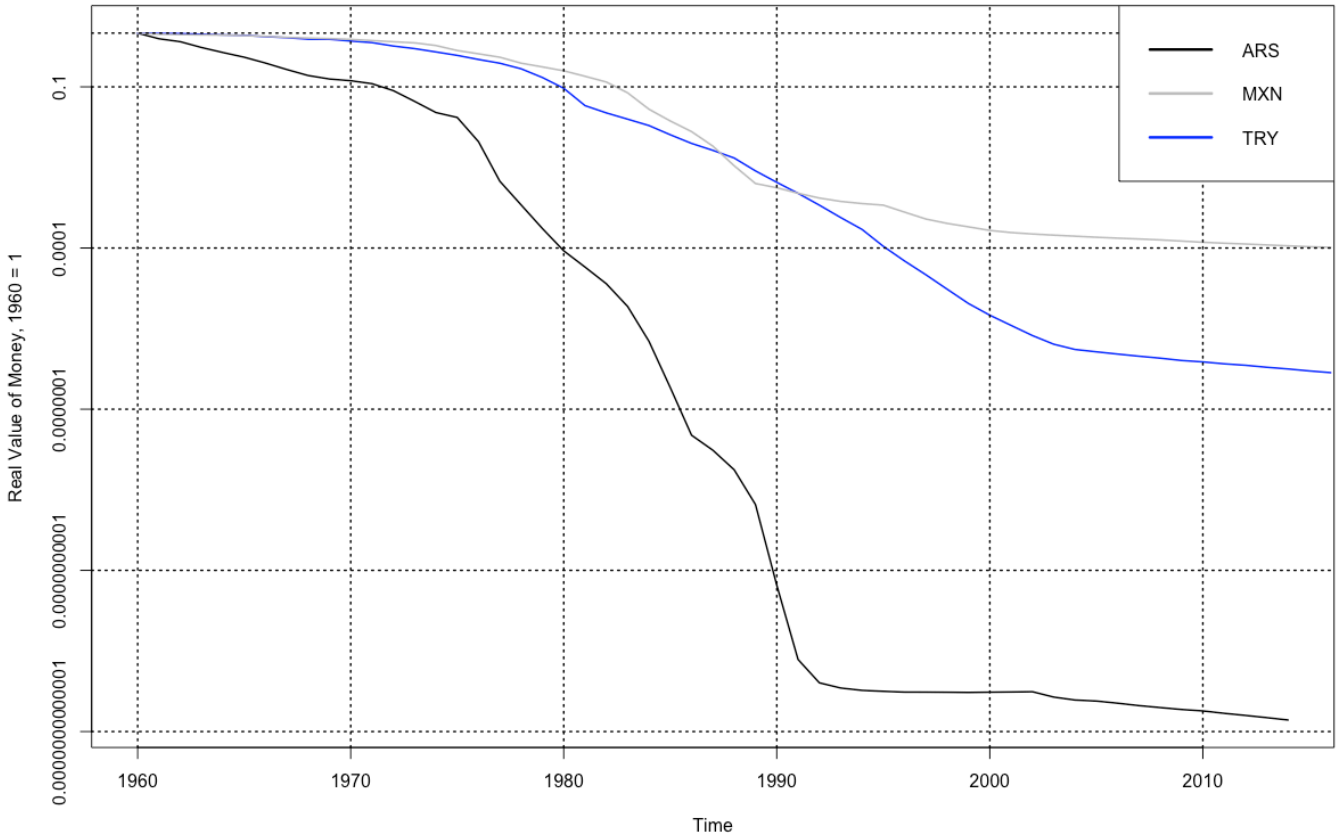
ZENSURRESISTENT BEDEUTET

- No single point of failure.
- Keine zentrale Instanz führt die Datenbank.
- Alle Bitcoin Benutzer sind in ihren Rechten zur Nutzung und Aktualisierung der Bitcoin Datenbank gleichberechtigt.

ZENSURRESISTENT BEDEUTET

- Die Benutzer sind Eigentümer ihrer Daten.
- Die Nutzer können ihre Daten ohne Erlaubnis verwenden.
- Es kann niemand ausgeschlossen werden.

ARGENTINIEN, MEXIKO, TÜRKEI

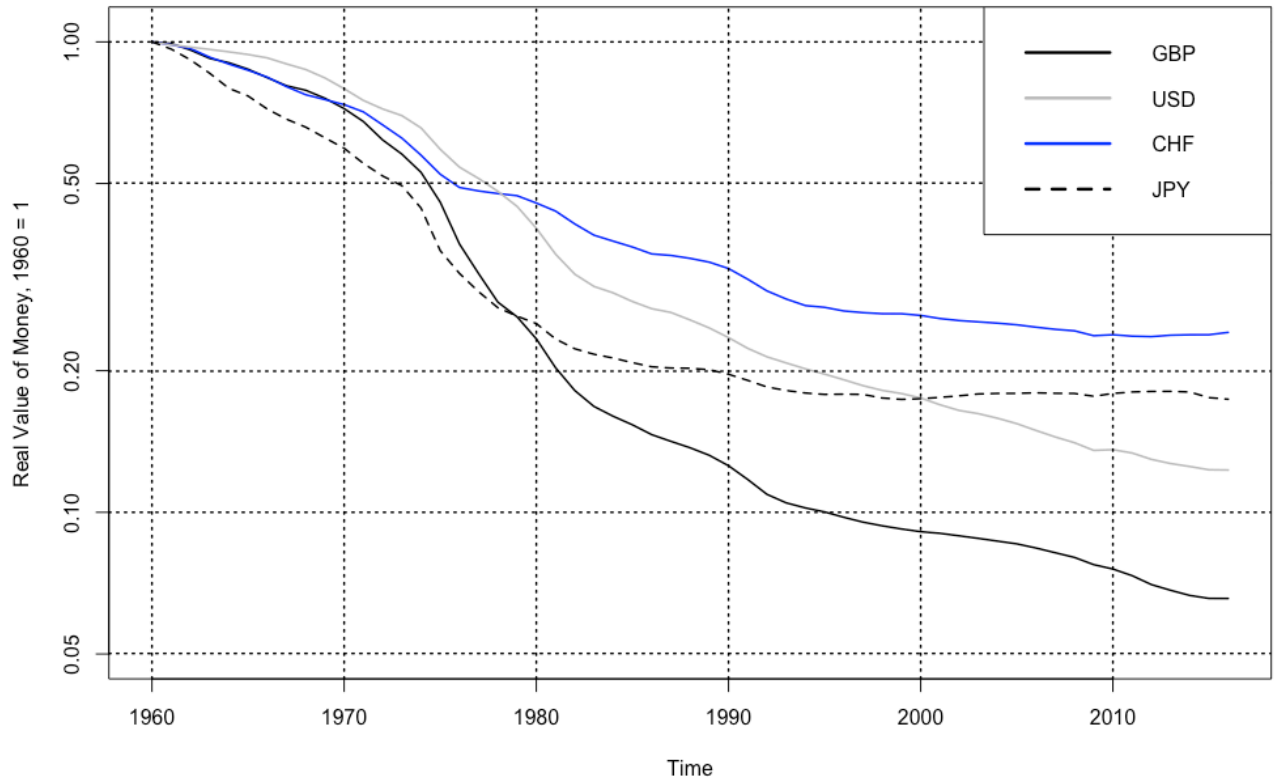


"Die Zentralbanken haben sich ihr Vertrauen während Jahrhunderten erarbeitet, und dafür gibt es derzeit keinen Ersatz." Augustin Carstens, BIS

Beispiele für nicht zensurresistente **zentralisierte** Währungen

Quelle: FRED, Federal Reserve Bank of St. Louis (FPCPITOTLZGTUR,FPCPITOTLZGARG,FPCPITOTLZGMEX)

USD, GBP, CHF, JPY



Weitere Beispiele für nicht zensurresistente **zentralisierte** Währungen

Quelle: FRED, Federal Reserve Bank of St. Louis (FPCPITOTLZGCHE,FPCPITOTLZGUSA,FPCPITOTLZGJPN,CPIIUKA)

WAS IST DAS PROBLEM MIT ZENTRALISIERTEN WÄHRUNGEN?

- Sie sind nicht zensurresistent.
  - Aktuelle Beispiele (dieses Jahr)
    - Türkei, Venezuela, Argentinien
    - Trumps Angriff auf das FED, Angriff UBS auf SNB, etc.
- Die Geschichte des Fiat-Geldes ist eine Geschichte von Misserfolgen, Katastrophen, Desaster …

BITCOIN BLOCKCHAIN VERSUS NORMALE DATENBANK

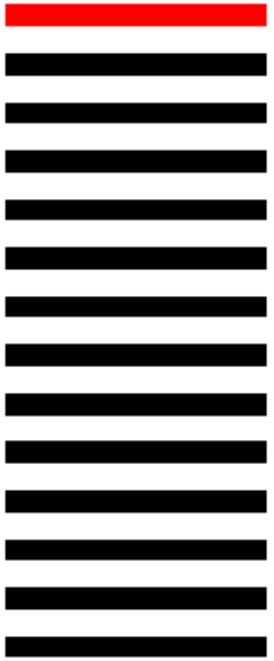
BITCOIN BLOCKCHAIN VS. NORMALE DATENBANK

- Unveränderlich (immutable)
- Konsistent (consistent)
- Besitzbar (ownable)
- Öffentlich (permissionless)
- Konsens (consensus)

JUMP

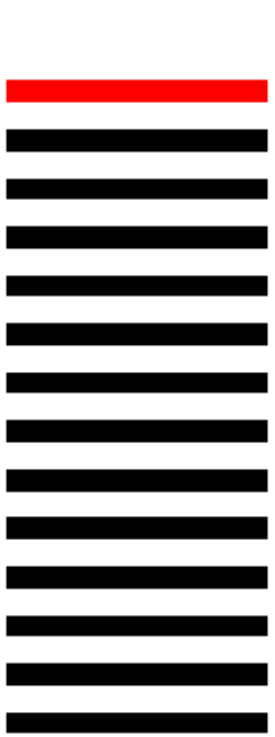
UNVERÄNDERLICH

- Bitcoin Blockchain speichert eine Aufzeichnung aller vergangenen Bitcoin-Transaktionen in Blöcken.
- Jeder Block enthält eine Liste von Transaktionen.
- Die Blöcke sind kryptographisch verbundenen.



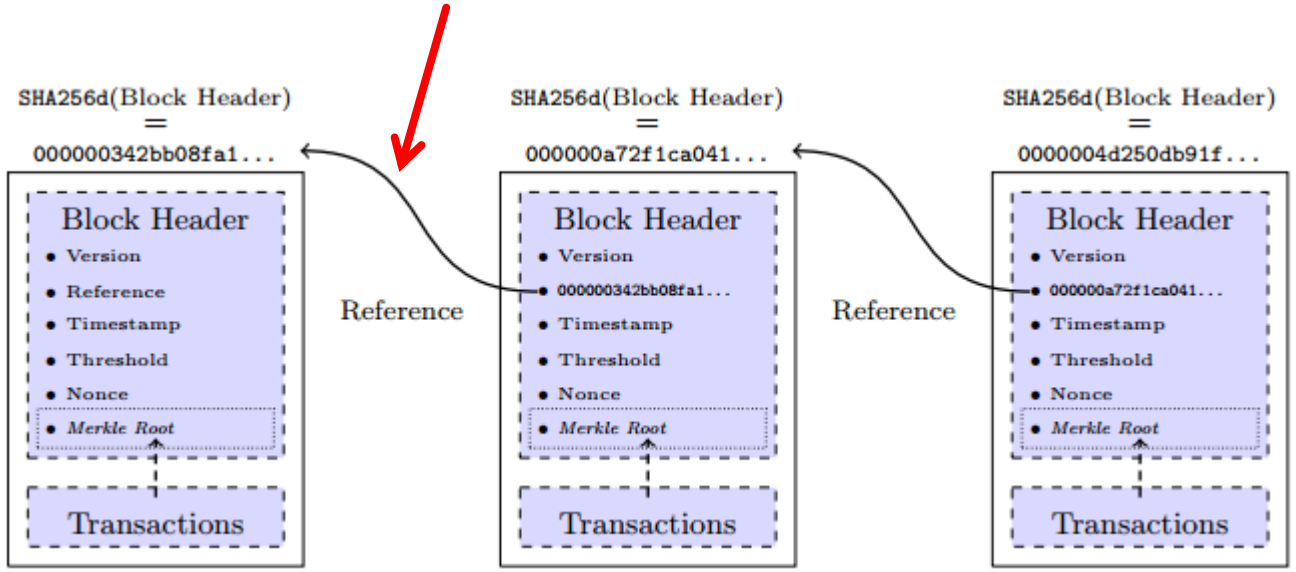
UNVERÄNDERLICH

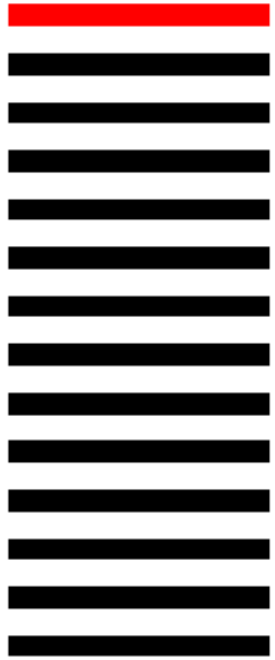
- Append only.



UNVERÄNDERLICH

- Blöcke sind kryptographisch verknüpft.

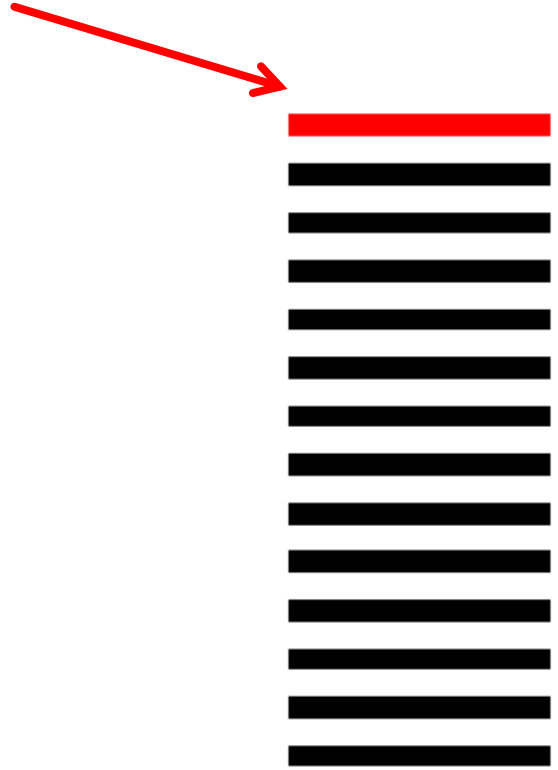




KONSISTENT

Neue Daten dürfen nicht mit anderen Daten kollidieren.

z.B. no double spends



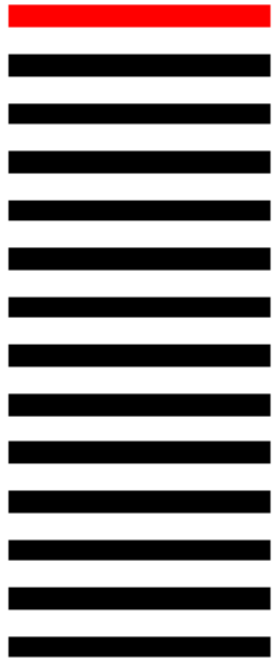
- Miners (die Buchhalter) überprüfen die Rechtmäßigkeit neuer Transaktionen.
- Miners verhindern Betrug.

BESITZBAR

- Eine nicht ausgegebene Transaktion (UTXO) ist einem öffentlichen Schlüssel (oder mehreren Schlüsseln) zugeordnet. Nur der Inhaber des zugehörigen privaten Schlüssels kann UTXO ausgeben.
- Asymmetrische Kryptographie: Nachweis der Legitimität und Integrität einer Nachricht (Signatur)

ÖFFENTLICH

- Bitcoin Blockchain ist eine öffentliche Datenbank.
  - Jeder kann sie herunterladen und lesen.
  - Jeder kann Buchhalter (Miner) werden.



KONSENS

- Implizite Einigung über die Verteilung der Eigentumsrechte für alle Bitcoin-Einheiten.
- Der Proof-of-Work-Konsensmechanismus ist die Kerninnovation der Bitcoin-Entwickler.

Resümee: Konsens in einer öffentlichen Datenbank mit einer großen Anzahl von pseudonymen Teilnehmern.

WAS IST DER ZWECK DES BITCOIN-MINING?

- Bitcoin-Mining ist ein Element des Proof-of-Work-Konsensmechanismus.
  - Das Mining bietet Anreize für die "Buchhalter" Transaktionen zu überprüfen und ein verteiltes öffentliches Register aller Bitcoin-Transaktionen zu führen (öffentliches Gut).
  - Sie erhalten für diese Aktivität neu geschaffene Bitcoins als Entlohnung.

…KOSTEN EINER ZENSURRESISTENTEN DATENBANK

INEFFIZIENT UND LANGSAM

- Ineffizient:
  Anstatt eine einzige Datenbank zu führen, werden die gleichen Daten auf Tausenden von Computern übertragen, verifiziert und gespeichert.
- Langsam:
  Der Konsens braucht Zeit. Verteilte Datenbanken sind langsamer als eine zentralisierte Datenbank.

DER TRADE-OFF:

Was wollen wir?

1. Zensurresistente Datenbank, die ineffizient und langsam ist.

2. Effiziente und schnelle zentralisierte Datenbank, die nicht zensurresistent ist.

FÜR WELCHE ANWENDUNGEN SOLLTEN WIR 1) ÜBER 2) WÄHLEN?

- Zensurresistente virtuelle Vermögensanlagen sind die beste Anwendung für die Blockchain-Technologie.

- Bitcoin als virtuelle Vermögensanlage
  - 1) ist viel wichtiger als 2)

BITCOIN IST VIRTUELLE(S) KUNST/GOLD

- Teilt Eigenschaften von Gold/Kunst:
  - Keine zentrale Instanz kann Gold/Kunst entwerten.
  - Keine zentrale Instanz kann Gold/Kunst konfiszieren, falls es gut versteckt ist.

- Bitcoin ist besser als Gold/Kunst:
  - Deutlich effizienter zu transferieren.
  - Weniger kostspielig zu speichern.

PEER-TO-PEER-VERSION VON ELECTRONIC CASH

- Für ein Zahlungssystem ist Bitcoin im Moment
  - zu langsam
  - zu teuer
- Kann sich noch ändern
  - Skalierungsdebatte
  - Lightning Netzwerk als Lösung
  - Proof of stake als Alternative zu Proof of work

ZWEI VORSCHLÄGE FÜR VIRTUELLES ZENTRALBANKEN GELD

ZWEI VORSCHLÄGE FÜR VIRTUELLES ZENTRALBANKEN GELD

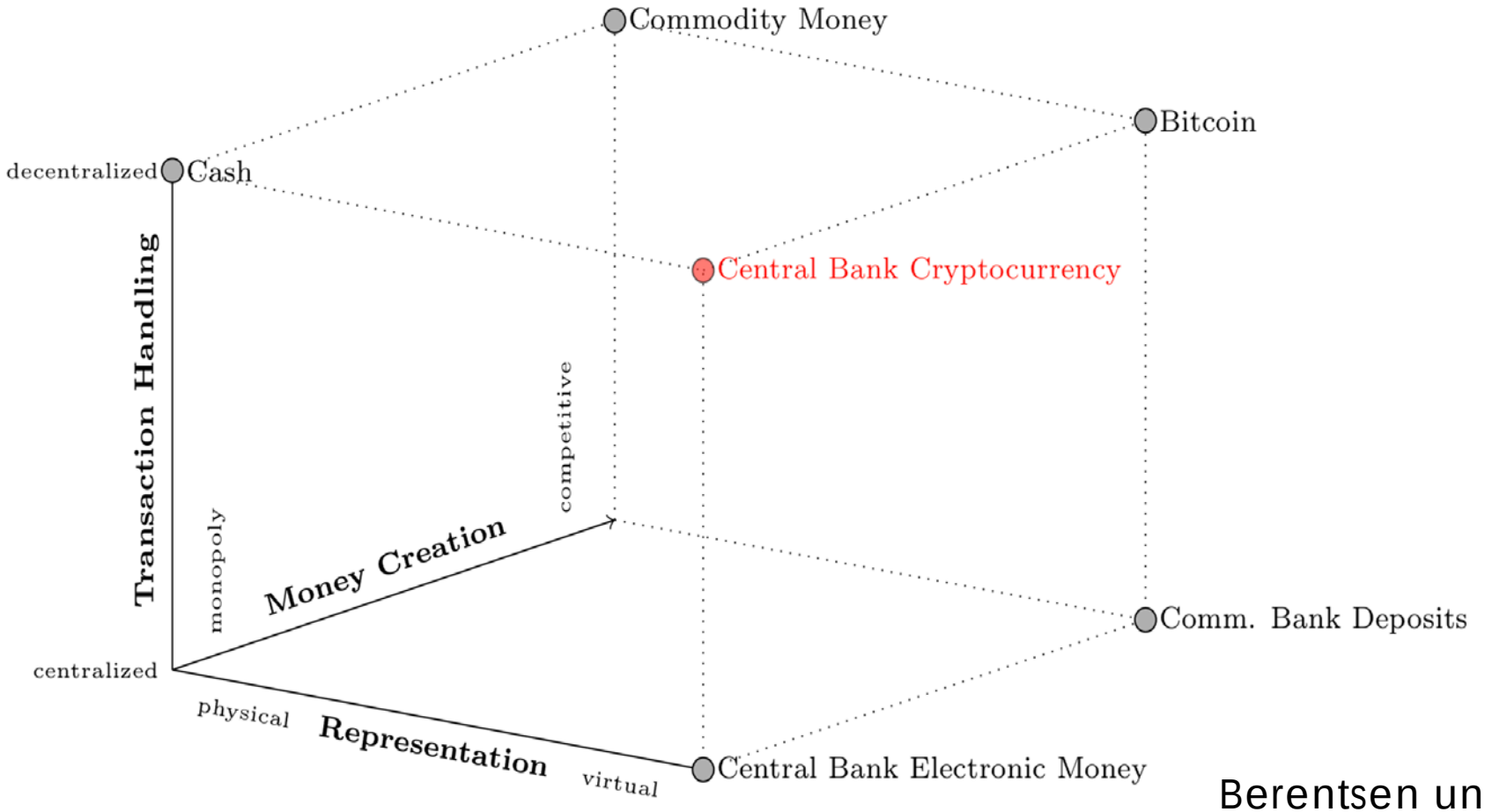
- Zentralbanken Kryptowährung (z.B. Fedcoin)

- Elektronisches Zentralbanken Geld für Alle

ZENTRALBANK KRYPTOWÄHRUNG

- Fedcoin ist eine widersprüchliche Idee.
- Warum sollte eine **Zentral**bank eine **dezentrale** Währung ausgeben?

ZENTRALBANK KRYPTOWÄHRUNG



Berentsen und Schär (2017)

ELEKTRONISCHES ZENTRALBANKEN GELD FÜR ALLE

- Dieser Vorschlag ermöglicht es Haushalten und Unternehmen Konten bei der Zentralbank zu eröffnen.
  - Und/oder Privatbanken sind verpflichtet, mindestens ein von ihrer Bilanz getrenntes Zahlungsverkehrskonto anzubieten.

- Ist bereits vor 30 Jahren möglich gewesen.
  - Keine Blockchain-Technologie erforderlich.
  - Zentralbank führt eine **zentralisierte** Datenbank über die Besitzstände.

ELEKTRONISCHES ZENTRALBANKEN GELD FÜR ALLE

- Vorteile:
  - Erhöht die Finanzstabilität.
  - Vereinfacht die Geldpolitik.
  - Die Verzinsung von Geld ist weniger umstritten.
  - Evolutionärer Ansatz, bestehende private Zahlungskonten sind nach wie vor legal.

TAKE AWAY

1. Bitcoin ist eine neue Anlageklasse:
   - Zensurresistent
   - Eigenschaften von Gold und Kunst aber virtuell
   - Interessant für Portfolio Diversifikation

2. Zentralbanken werden elektronisches Geld anbieten:
   - Zentralisierte Datenbank
   - Bitcoin Konkurrenz für schlechte Zentralbanken

LITERATURHINWEISE

University of Basel

Center for Innovative Finance

Herunterladen

LITERATURHINWEISE

University of Basel

Center for Innovative Finance

Herunterladen

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

University of Basel

Center for Innovative Finance

www.blockchainbuch.de