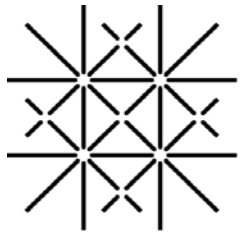
BITCOIN, BLOCKCHAIN, KRYPTOASSETS: VON DER „SHARING ECONOMY“ ZUR „BLOCKCHAIN ECONOMY“

ALEKSANDER BERENTSEN, UNIVERSITÄT BASEL



University of Basel

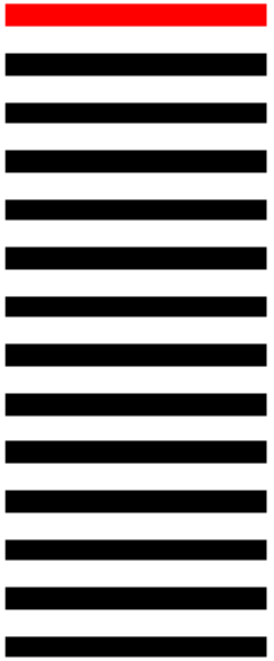
Center for Innovative Finance

PLAN

1. Was ist eine Blockchain?
   - Bitcoin Blockchain
   - DLT
   - Stärken und Schwächen der Technologie
2. Virtuelle Vermögenswerte
   - Bitcoin
   - Stablecoins wie Libra
3. Weitere Anwendungen

BLOCKCHAIN

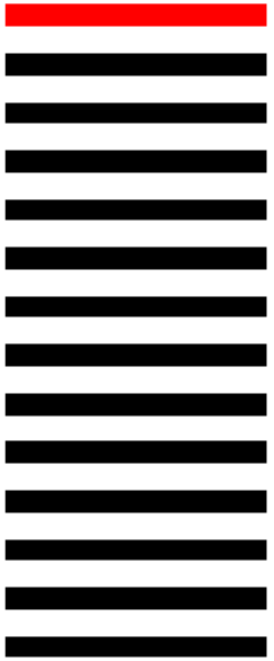
- Eine Blockchain ist eine Datenbank.
- Aufgebaut aus aufeinanderfolgenden Text-Blöcken.



DISTRIBUTED LEDGER TECHNOLOGY (DLT)

- DLT ist eine verteilte Datenbank.

- Eine verteilte Datenbank wird dezentral geführt.
  - Es sind viele Teilnehmer gleichberechtigt sich an der Fortführung zu beteiligen.
  - Sie speichern eine eigene Kopie und schreiben diese fort.



ZENSURRESISTENTE DATENBANK

Die Bitcoin-Entwickler haben erstmals die Technologien *Blockchain* und *DLT* kombiniert und dadurch eine zensurresistente Datenbank erschaffen.

ZENSURRESISTENT BEDEUTET

- Nicht manipulierbar und konsistent (widerspruchsfrei).
- Robust
  - Kein Single Point of Failure.
  - Keine Ausfallzeiten.
- Alle Benutzer sind gleich.
  - Permissionless (keine Zugangskontrolle).
  - Die Benutzer sind Eigentümer ihrer Daten.

ZENSURRESISTENTE DATENBANK

- Die Innovation einer zensurresistenten Datenbank ermöglicht erstmals den Besitz von virtuellem Eigentum ohne zentrale Instanzen.
- Diese Innovation hat das Potenzial, das derzeitige Finanzsystem und viele Bereiche in Wirtschaft und Verwaltung grundlegend zu verändern.

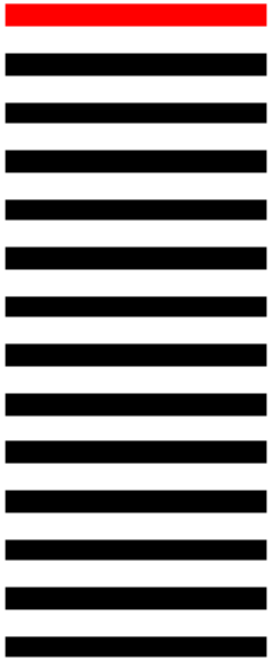
DIE WICHTIGSTEN REGELN, WELCHE ZU DIESEN EIGENSCHAFTEN FÜHREN

BITCOIN BLOCKCHAIN VS. NORMALE DATENBANK

- Konsistent (consistent)
- Nicht manipulierbar (immutable)
- Robust (resilient)
- Besitzbar (ownable)

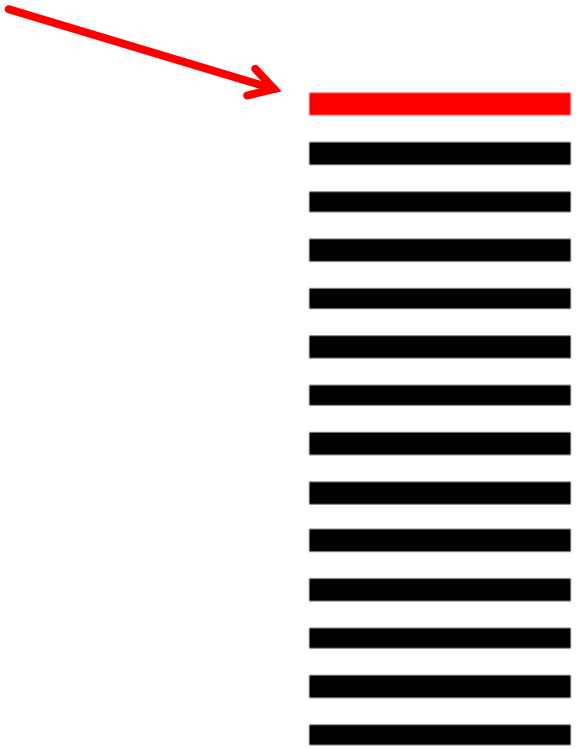
BITCOIN BLOCKCHAIN

- Bitcoin ist ein virtueller Vermögenswert (Marktkapitalisierung 150 Milliarden USD).
- Bitcoin Blockchain ist eine Aufzeichnung aller vergangenen Bitcoin-Transaktionen.
- Jeder Block enthält eine Liste von Transaktionen.



KONSISTENZ

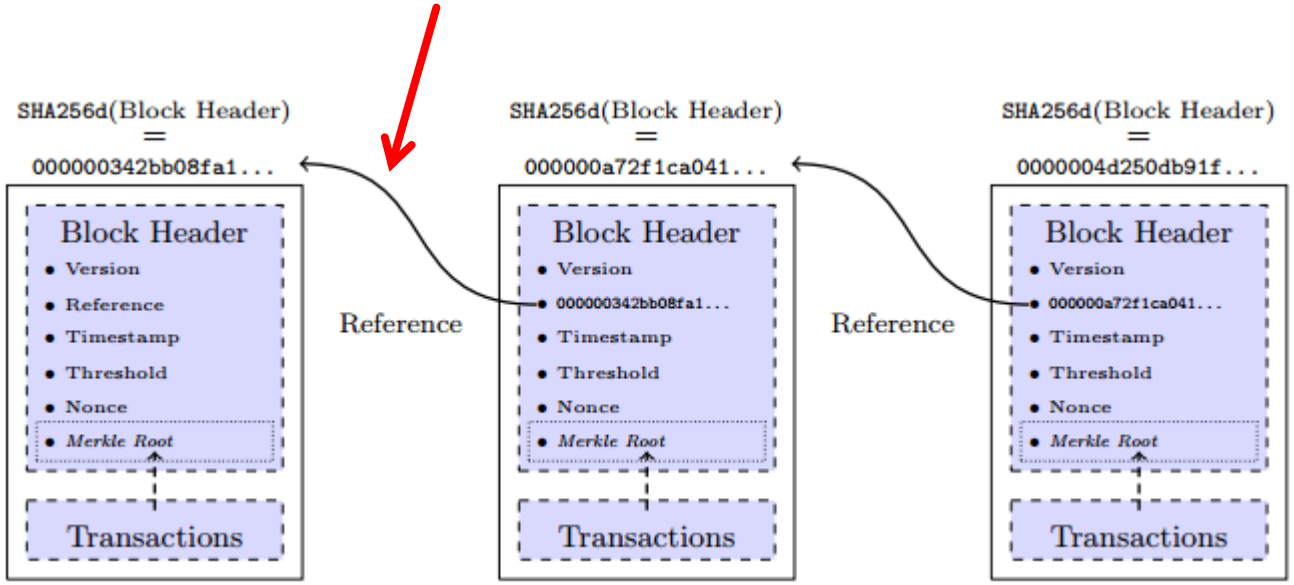
- Append only.

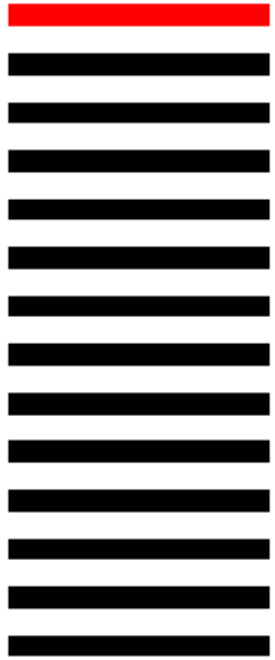


- Es dürfen nur Daten hinzugefügt werden.
- Neue Daten dürfen nicht im Widerspruch zu den bestehenden Daten sein.

NICHT MANIPULIERBAR

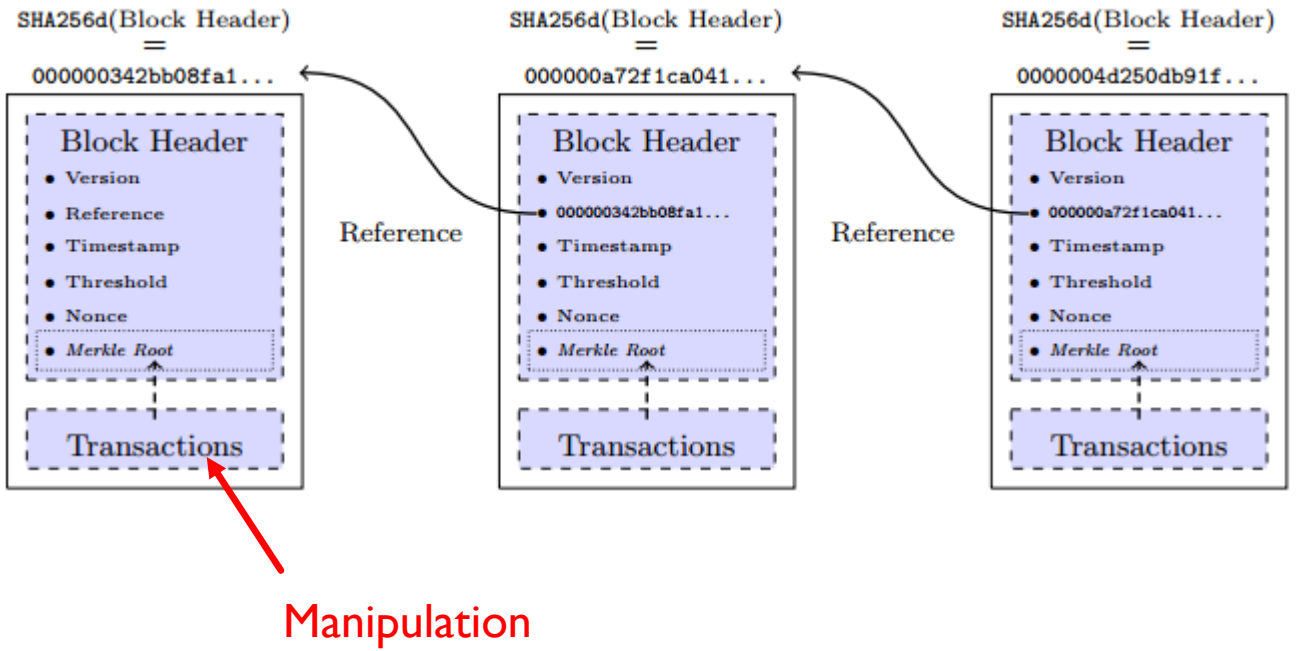
- Blöcke sind kryptographisch verknüpft.

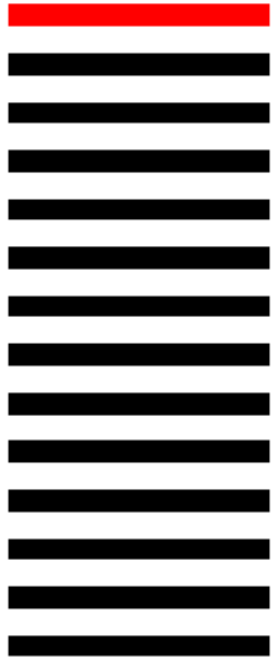




NICHT MANIPULIERBAR

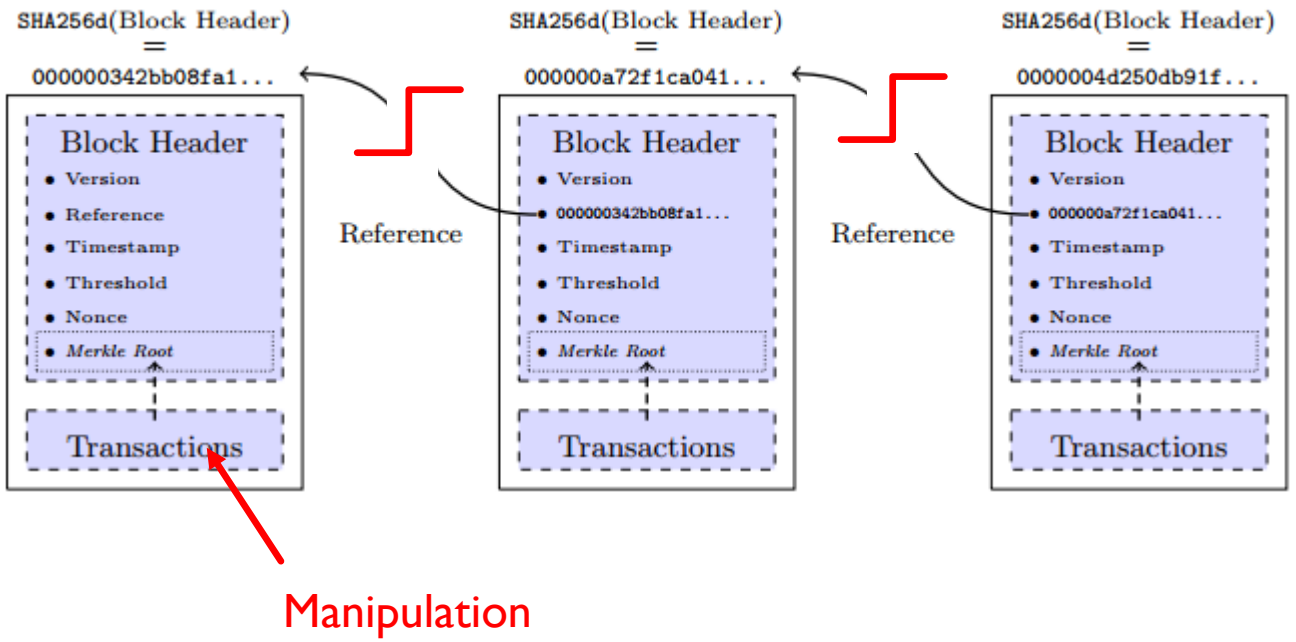
- Werden Daten manipuliert, ….

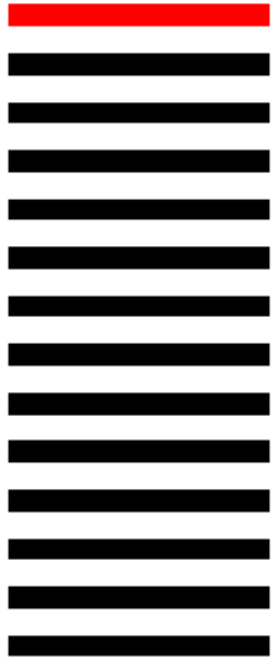




NICHT MANIPULIERBAR

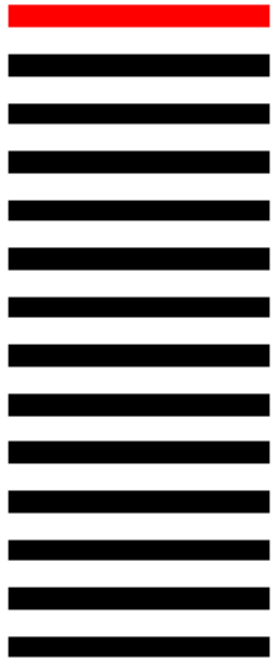
- Werden Daten manipuliert, fällt die Kette auseinander.





NICHT MANIPULIERBAR

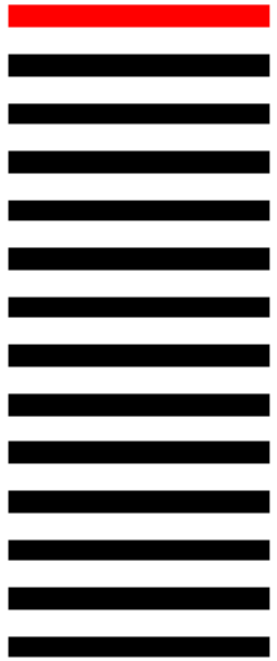
- Die Bitcoin Blockchain ist öffentlich und auf tausenden von Computern gespeichert.
- Jede Manipulation wird sofort entlarvt und abgelehnt.



ROBUST

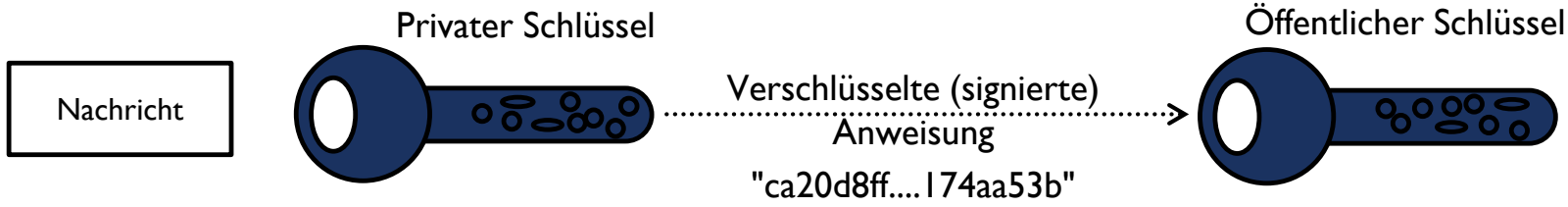
- Die Bitcoin Blockchain ist auf tausenden von Computern gespeichert und wird von tausenden von Benutzern gepflegt (verteilte Datenbank).

- Teile des Netzwerks können ausfallen ohne dass die Buchführung unterbrochen wird.



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)



INNOVATION: PROOF-OF-WORK-KONSENSMECHANISMUS

- Der Proof-of-Work Konsensmechanismus ermöglicht, dass sich alle Netzwerkteilnehmer immer einig über die Eigentumsrechte über alle Bitcoin-Einheiten sind.
  - Die Teilnehmer sind pseudonym.
  - Der Zugang zum Bitcoin Netzwerk ist offen.

…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

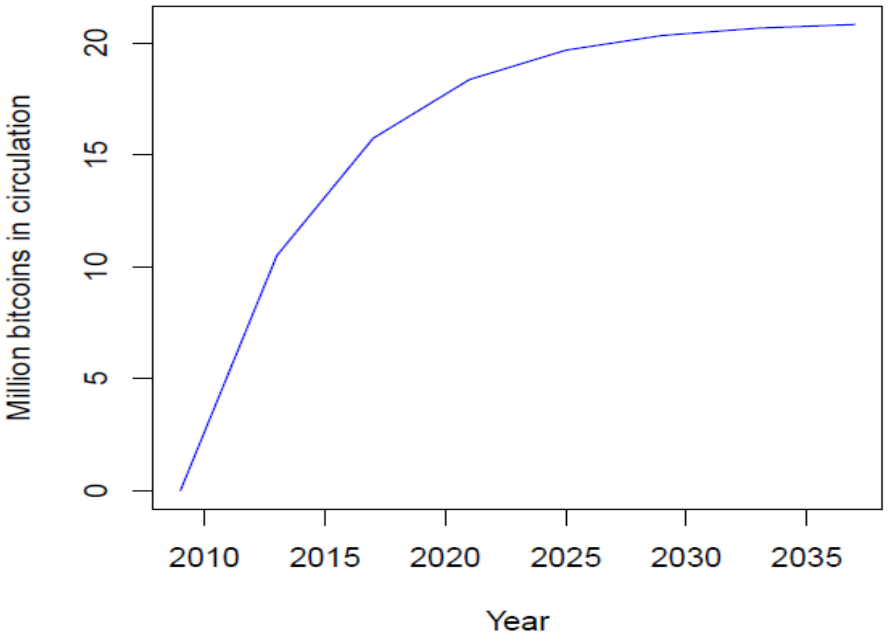
- Teilt Eigenschaften von Gold/Kunst:
  - Keine zentrale Instanz kann Gold/Kunst entwerten.
  - Keine zentrale Instanz kann Gold/Kunst konfiszieren, falls es gut versteckt ist.
- Bitcoin ist besser als Gold/Kunst:
  - Deutlich effizienter zu transferieren.
  - Weniger kostspielig zu speichern.

WAS SIND DIE SCHWÄCHEN VON BITCOIN?

- Preisvolatilität
- Skalierbarkeit
- Governance

GELDPOLITIK UND PREISVOLATILITÄT

- Geldpolitik vorimplementiert im Quellcode:
  - 21-Millionen-Grenze
  - Derzeit 12,5 neue Bitcoins alle 10 Minuten.
  - Alle 4 Jahre (210.000 Blöcke) wird die Belohnung halbiert.
- Starres Angebot führt zu einer enormen Preisvolatilität.



PREISVOLATILITÄT

- Stablecoins sind Kryptowährungen welche gegenüber einer Referenzwährung stabil gehalten werden.
- Beispiele:
  - Tether (USD)
  - Facebook's Libra (Währungskorb)
  - DAI (USD)

STABLECOINS

- Tether und Libra werden mit Währungsreserven hinterlegt (off-chain Kollateral).
  - Währungsreserven sind bei Banken hinterlegt.
    - Keine Dezentralität
    - Zensurresistenz geht verloren

STABLECOINS

- Libra plant eine permissioned Blockchain.
  - Zugangskontrolle durch die Libra Association in Genf.
    - Dezentralität ADIEU
    - Zensurresistenz ADIEU

STABLECOINS

- DAI stablecoin basiert auf smart contracts und on-chain Kollateral.
  - Oracles
  - Offenes Komitee bestimmt stability fee (Zinssatz)
- Teile der Dezentralität und damit der Zensurresistenz gehen verloren.

…WEITERE ANWENDUNGEN

BEYOND BITCOIN

Virtuelle Währungen
und virtuelles Gold

BEYOND BITCOIN

Virtuelle Währungen
und virtuelles Gold

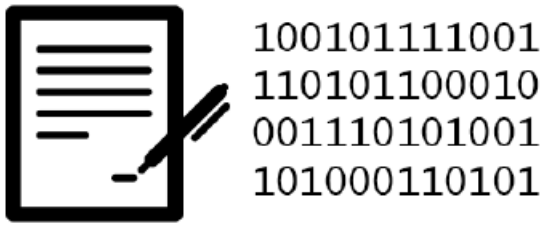
Tokenisierung

BEYOND BITCOIN

Virtuelle Währungen
und virtuelles Gold

Tokenisierung

Smart Contracts

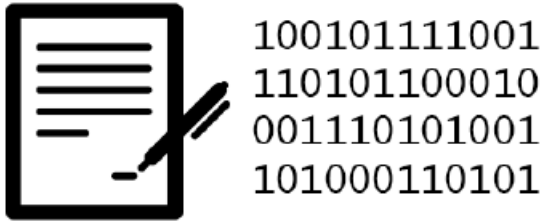


BEYOND BITCOIN

Virtuelle Währungen
und virtuelles Gold

Tokenisierung

Smart Contracts



Integrität von Daten

SMART CONTRACTS

ethereum

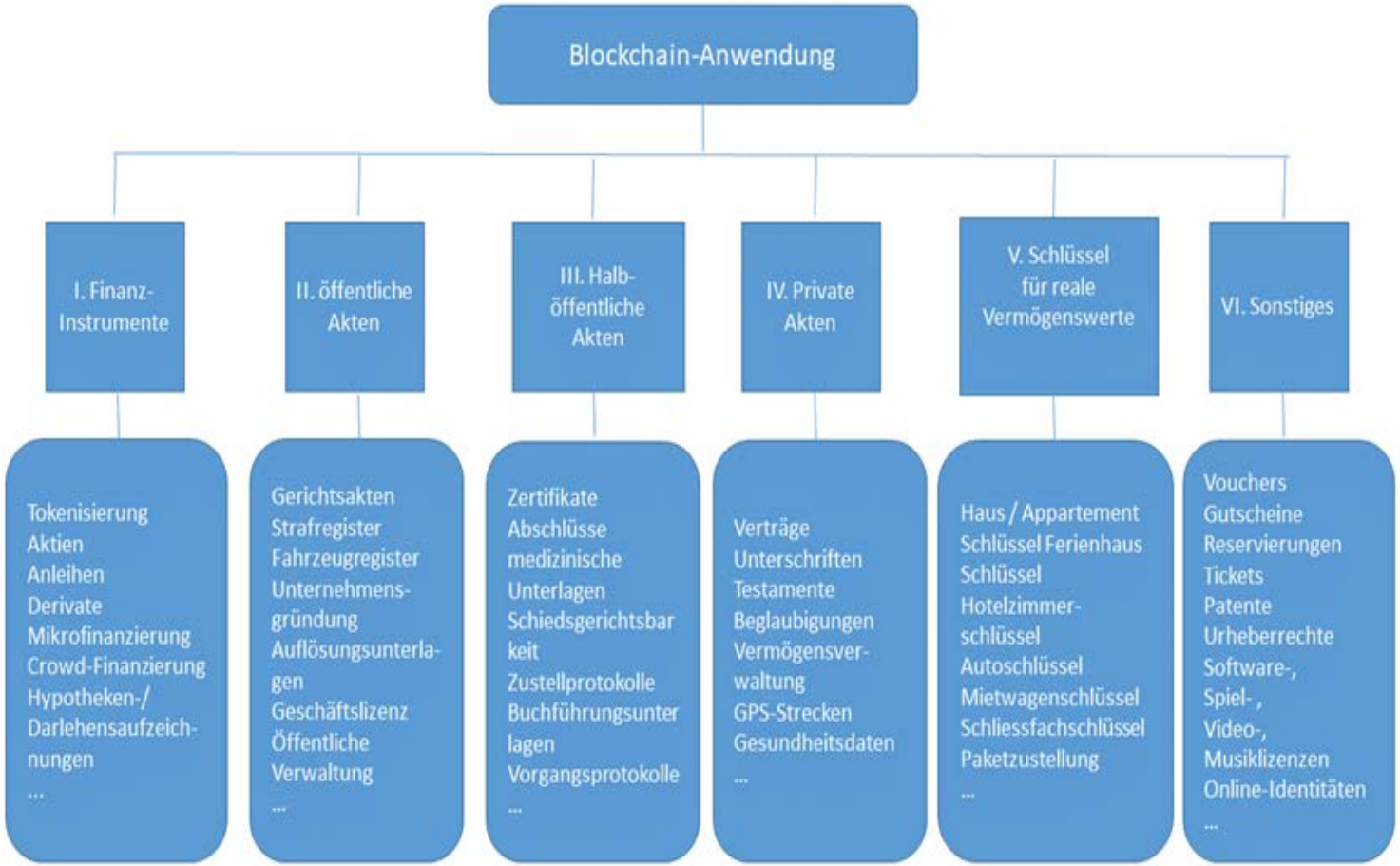
Open Source Plattform für Smart Contracts und Dezentrale Applikationen

(Geburt 30 Juli 2015)

SMART CONTRACTS

ethereum

BLOCKCHAIN ANWENDUNGEN

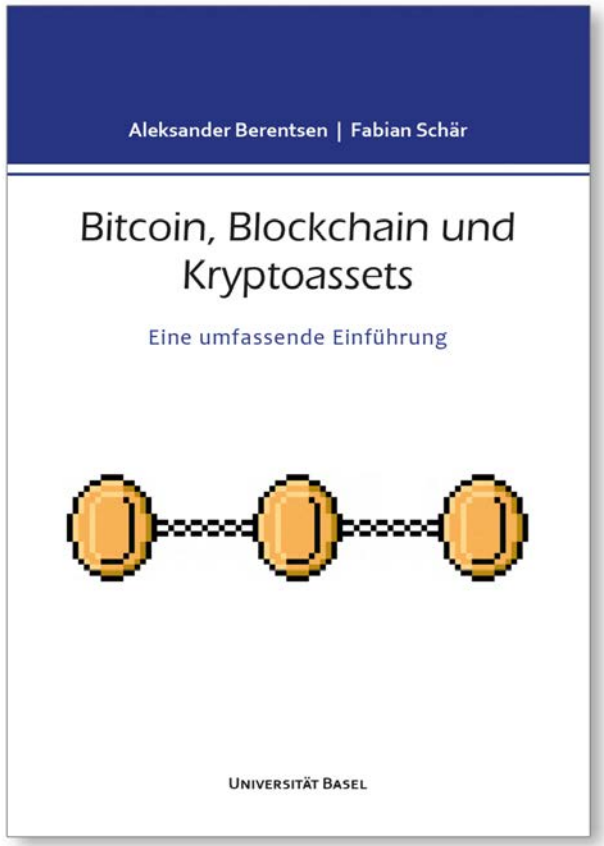


Markheim (2019)

SCHLUSSFOLGERUNG

- Die Bitcoin-Entwickler haben eine zensurresistente Datenbank entwickelt, welche zum ersten Mal in der Geschichte der Besitz von virtuellem Eigentum ohne zentrale Instanzen ermöglicht.
- Viele Projekte bauen wieder zentralisierte Elemente ein:
  - Regulatorische und technische Gründe
  - Projekte wollen Kontrolle behalten
  - Profitorientierte Projekte

BESTEN DANK FÜR IHRE AUFMERKSAMKEIT

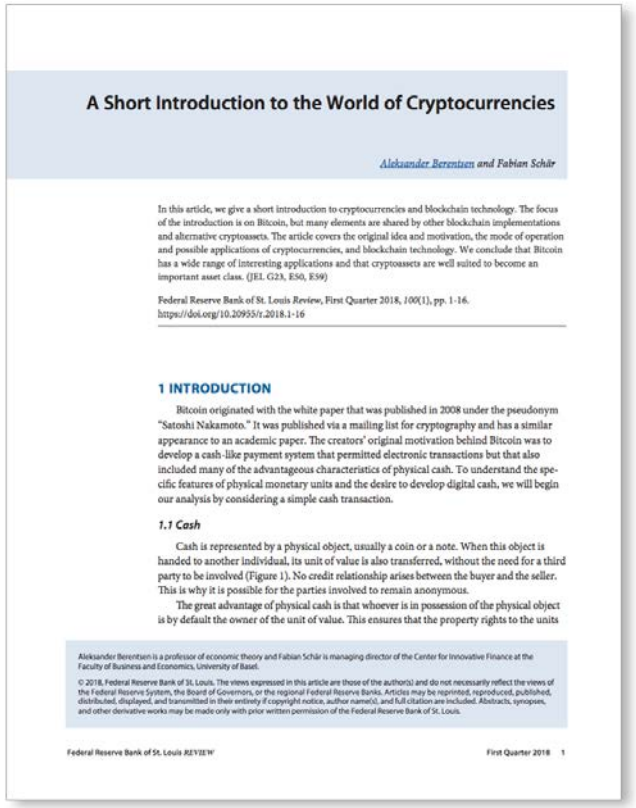


Die Blockchain wird als Innovation des Jahrzehnts gehandelt und hat das Potential die Welt auf ähnliche Weise zu verändern, wie dies das Aufkommen des Internets tat.
Dieses Buch beinhaltet sämtliche Informationen, die zum Verständnis dieser faszinierenden Technologie benötigt werden.

Der interdisziplinäre Blickwinkel und die fachliche Vollständigkeit sorgen dafür, dass das Buch für Neueinsteiger und Fortgeschrittene gleichermaßen interessant und lesenswert ist. Damit wird es zur unverzichtbaren Lektüre für alle, die sich mit dem Thema auseinandersetzen möchten.

www.blockchainbuch.de

EINFÜHRENDER ARTIKEL ZUM THEMA



A Short Introduction to the World of Cryptocurrencies

Aleksander Berentsen and Fabian Schär

In this article, we give a short introduction to cryptocurrencies and blockchain technology. The focus of the introduction is on Bitcoin, but many elements are shared by other blockchain implementations and alternative cryptoassets. The article covers the original idea and motivation, the mode of operation and possible applications of cryptocurrencies, and blockchain technology. We conclude that Bitcoin has a wide range of interesting applications and that cryptoassets are well suited to become an important asset class. (JEL G23, E50, E59)

Federal Reserve Bank of St. Louis *Review*, First Quarter 2018, *100*(1), pp. 1-16.
https://doi.org/10.20955/r.2018.1-16

1 INTRODUCTION

Bitcoin originated with the white paper that was published in 2008 under the pseudonym "Satoshi Nakamoto." It was published via a mailing list for cryptography and has a similar appearance to an academic paper. The creators' original motivation behind Bitcoin was to develop a cash-like payment system that permitted electronic transactions but that also included many of the advantageous characteristics of physical cash. To understand the specific features of physical monetary units and the desire to develop digital cash, we will begin our analysis by considering a simple cash transaction.

1.1 Cash

Cash is represented by a physical object, usually a coin or a note. When this object is handed to another individual, its unit of value is also transferred, without the need for a third party to be involved (Figure 1). No credit relationship arises between the buyer and the seller. This is why it is possible for the parties involved to remain anonymous.

The great advantage of physical cash is that whoever is in possession of the physical object is by default the owner of the unit of value. This ensures that the property rights to the units

Aleksander Berentsen is a professor of economic theory and Fabian Schär is managing director of the Center for Innovative Finance at the Faculty of Business and Economics, University of Basel.

Das kürzlich im Federal Reserve Bank of St. Louis Review erschienene Papier bietet einen optimalen Kurzeinstieg in die Welt der Kryptoassets und der Blockchain. Es vermittelt die Grundlagen sowie das Potential und mögliche Anwendungen der Blockchain.

Das Paper wurde von den beiden CIF Forschern Aleksander Berentsen und Fabian Schär verfasst.

download

PROF. DR. ALEKSANDER BERENTSEN

Aleksander Berentsen ist seit 2005 Professor für Wirtschaftstheorie an der Wirtschaftswissenschaftlichen Fakultät der Universität Basel, wo er zurzeit das Amt des Dekans innehat. Seine Forschungsinteressen umfassen Geldtheorie, Geldpolitik, Makroökonomie und Finanzwirtschaft.

Er studierte an den Universitäten Basel und Bern und an der London School of Economics. Längere Forschungsaufenthalte führten ihn an die University of California in Berkeley, die University of Pennsylvania, die Université Paris Dauphine und als Bundesbankprofessor an die Freie Universität Berlin. Zwischen 2014 und 2016 war Aleksander Berentsen externer Berater bei der Schweizerischen Nationalbank. Seit 2009 ist er Research Fellow an der Federal Reserve Bank von St. Louis.