Der Zauber von Blockchain

Berner-Architekten-Treffen Nr. 38

Thomas Goetz

PostFinance

Intro
Der Zauber von Blockchain

Geniale Erfindung

Verzauberung

Fauler Zauber

Motivation
Bitcoin

Physisches Geld

Krypto-Geld

Bitcoin

2009 – die erste dezentrale Implementierung einer Kryptowährung

- Echtheit: gesichertes Register aller Transaktionen
- Besitz: Signatur der Transaktion

Kryptographische Grundfunktionen

- **Kryptographische Hash-Funktion** zur Sicherung des Registers gegen Veränderungen
  - Kompressionsfunktion → „Fingerabdruck“
  - Resistent gegen Kollisionen
- **Digitale Signatur** zum Nachweis des Besitzers
  - Öffentlicher Schlüssel als “Kontonummer“
  - Privater Schlüssel als „Pseudonym“

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.

Bitcoin: A Peer-to-Peer Electronic Cash System
Satoshi Nakamoto, 2008

Anwendungen von Blockchain

Anwendungen

Register

- Blockchain oder Distributed Ledger Technology
- Einträge → Tokens
- Autonom und automatisch → Kooperationen

Anwendungen

- **Geld**
  Token repräsentiert sich selbst → Kryptowährung
- **Vermögenswerte**
  Token repräsentiert ein Asset → Verbriefung oder Tokenization
- **Handel von Waren und Dienstleistungen**
  Token repräsentiert ein Event → Timestamping
- **Allgemeine Register**
  Token repräsentiert ein Recht, einen Fakt, eine Herkunft, einen Prozesszustand

Elemente

Lösungskomponenten von Bitcoin

Verteilte Systeme

- Kommunikation
- Robustheit (Ausfall, Byzantinisches Verhalten)

Kryptographie

- Digitale Signatur (Echtheit, Identität / Pseudonymität)
- Hash-Funktion (Fingerprint, Puzzle)

Spieltheorie

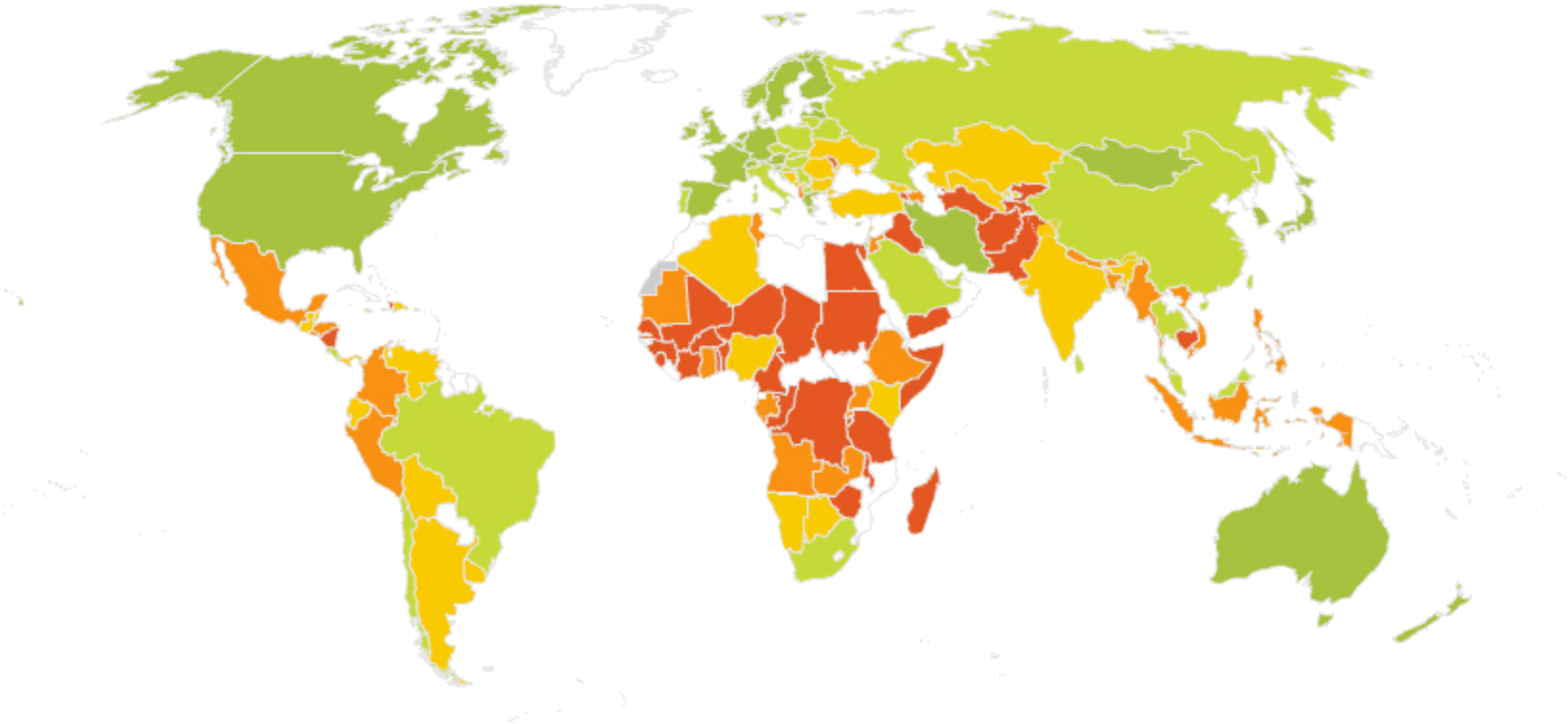
- Anreizsystem

Vertrauen

- **Vom Intermediär zum Mechanismus**
  - Algorithmus / Protokoll
  - Implementation
  - Community – Nutzung, Betrieb, Weiterentwicklung

- **Komponenten des Vertrauens**
  Informationssicherheit (Integrität, Vertraulichkeit, Verfügbarkeit)
  - Kryptographie – Grundlagen, Implementation, Verwendung
  - Code – Entwickler, Technologie
  - Betreiber, Nutzer
  - Governance
  - Rechtlicher Rahmen

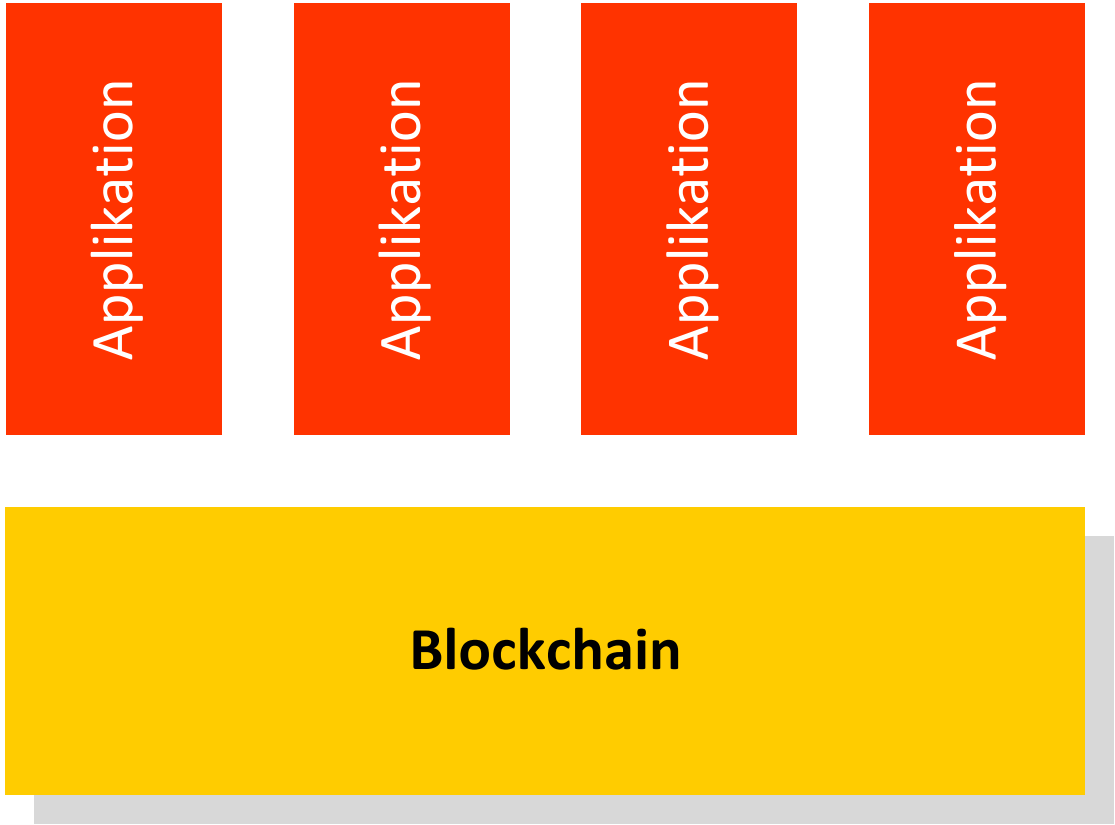
Finanzdienstleistungen



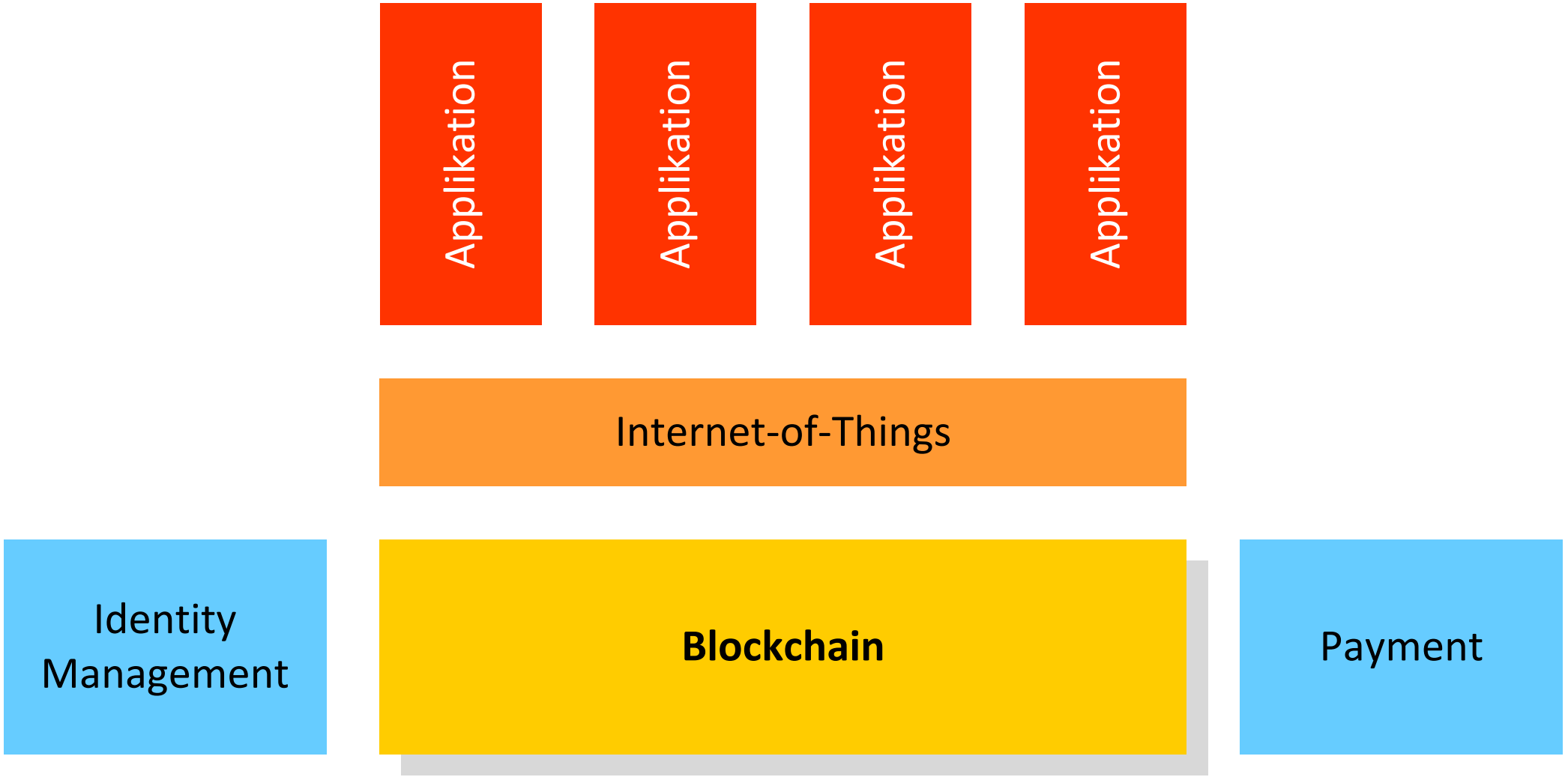
Comments:
Indicator: Account at a financial institution (% age 15+) [ts]
Year: 2014

No Data | 0 - 20.0 | 20.0 - 39.0 | 39.0 - 63.2 | 63.2 - 87.5 | 87.5 - 100

Digitale Welt



Physische und digitale Welt



Smart contracts

The code is the contract.

The executed code is the contract.

- Betrieb
- Qualität und Sicherheit der Software
- Wartung und Weiterentwicklung der Software

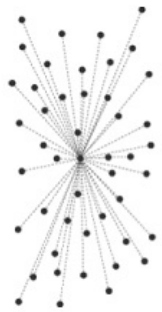
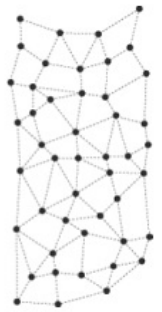
The executed code and its context is the contract.

- Soziotechnisches Gesamtsystem
- Rechtsrahmen
  - Ansprüche des Staats an uns – beispielsweise Steuergesetzgebung, Geldwäschereigesetz
  - Ansprüche von uns an den Staat – beispielsweise Eskalationsinstanz, Anlegerschutz

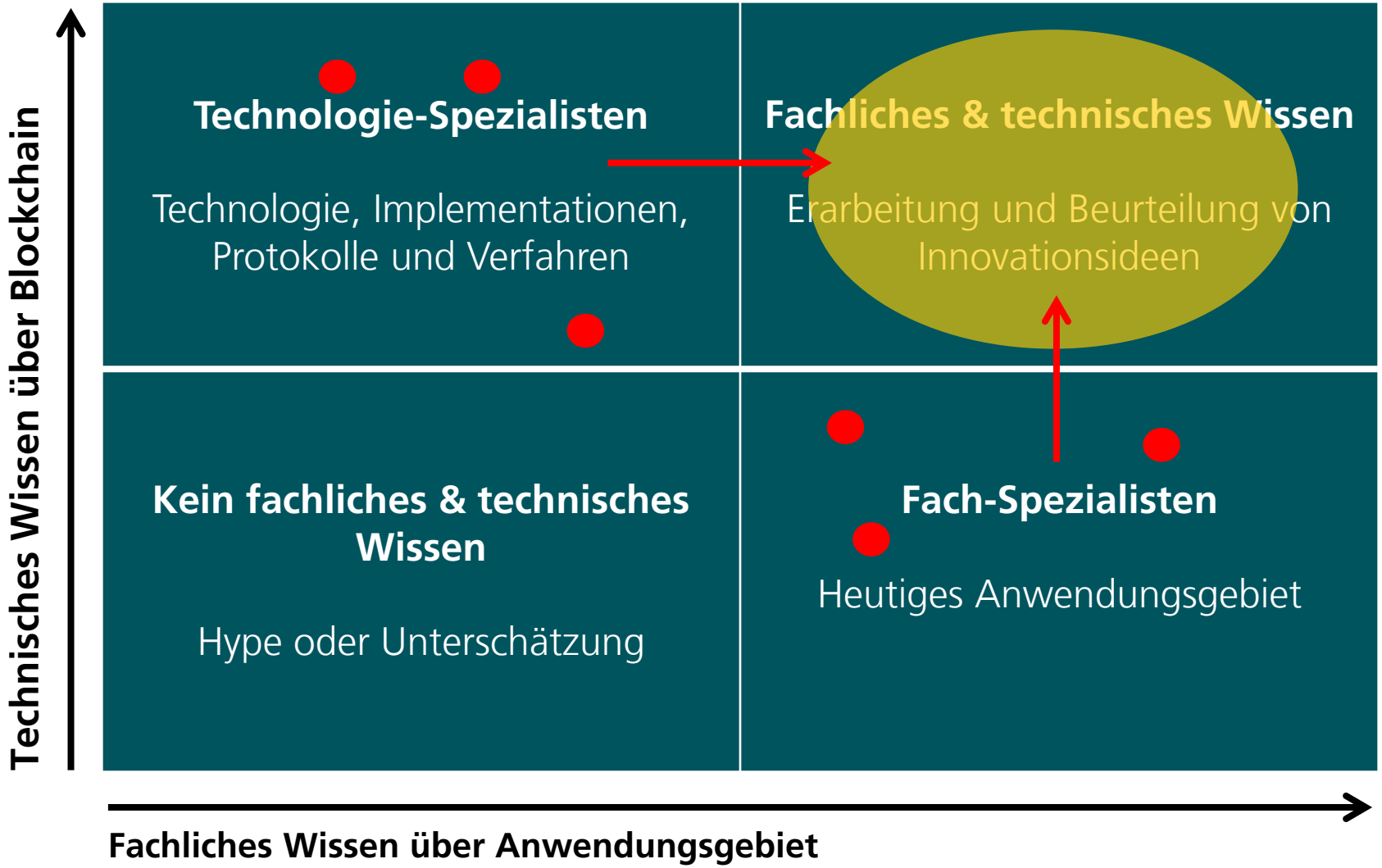
Eigenschaften von Blockchain-Plattformen

- **Zugang**
  Public vs. Permissioned
- **Konsens**
  pseudonym (Proof-of-Work, Proof-of-Stake) vs. identifiziert (Paxos, Byzantine)
- **Identifikation**
  Identität vs. Pseudonym
- **Verteilung**
  Peer-to-Peer vs. Distributed System vs. Centralized System
- **Betrieb**
  Community vs. Konsortium vs. vertrauenswürdiger Dienstleister
- **Graph des Registers**
  Baum, Azyklischer gerichteter Graph, Fragmente

Blockchain-Typen

	Zentrale Datenbank	Private Blockchain	Öffentliche Blockchain
			
Organisation	Firma	Konsortium	Öffentlichkeit
Zugang beschränkt	ja	ja	nein
kryptographisch geschützt	nein	ja	ja
Konsens-verfahren	nein	Diverse Protokolle	Nakamoto Proof-of-Work
Tx final	sofort	sofort	mit der Zeit
Tx/s	> 1000	> 100	< 10
Veränderung	klassisch	evolutionär	radikal

Interdisziplinäres Arbeiten als Erfolgsfaktor



Blockchain-Technologie unterstützt kooperative Geschäftsmodelle und bietet neue Chancen für Intermediäre.

TG, 2017

Literatur - klassische Artikel

- **Satoshi Nakamoto**
  "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008
  https://bitcoin.org/en/bitcoin-paper
- **Nick Szabo**
  „Smart Contracts", 1994
  http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Literatur – Bücher und Online-Kurse

- **Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction**
  Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder
  Princeton University Press
- **A graduate course in applied cryptography**
  Dan Boneh, Victor Shoup
  https://crypto.stanford.edu/~dabo/cryptobook/

- **Coursera “Bitcoin and Cryptocurrency Technologies”**
  https://www.coursera.org/learn/cryptocurrency
- **edX “Blockchain for Business”**
  https://www.edx.org/course/blockchain-business-introduction-linuxfoundationx-lfs171x
- **Coursera “Cryptography I”**
  https://www.coursera.org/learn/crypto

Kryptowährungen in der Schweiz

- **Bericht des Bundesrates über virtuelle Währungen wie Bitcoin**
  BUND, 25.6.2014
  https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-53513.html
  http://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf
- **Faktenblatt Bitcoins**
  FINMA, 25. Juni 2014
  https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/faktenblaetter/faktenblatt-bitcoins.pdf?la=de
- **FINMA zieht Coin-Anbieter aus dem Verkehr und warnt vor Scheinkryptowährungen**
  FINMA, 19. September 2017
  https://www.finma.ch/de/news/2017/09/20170919-mm-coin-anbieter/
- **Aufsichtsrechtliche Behandlung von Initial Coin Offerings**
  FINMA, 29. September 2017
  https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20170929-finma-aufsichtsmitteilung-04-2017.pdf

Fragen?
Antworten!

PostFinance