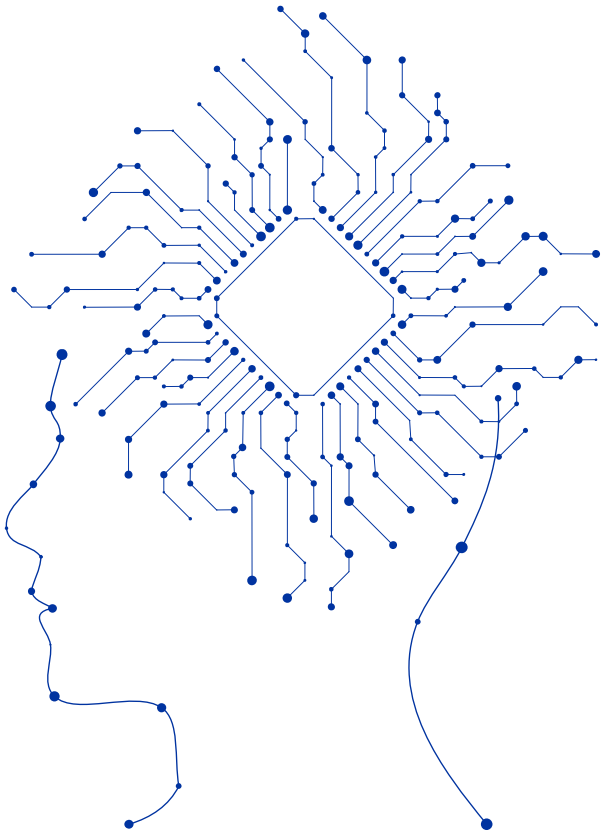
fortiss

Blockchain Technologie in einer



Prof. Helmut Krcmar

Sprecher des Direktoriums fortiss

Lehrstuhl Wirtschaftsinformatik TU München

fortiss GmbH
An-Institut Technische Universität München

Worum geht es überhaupt?

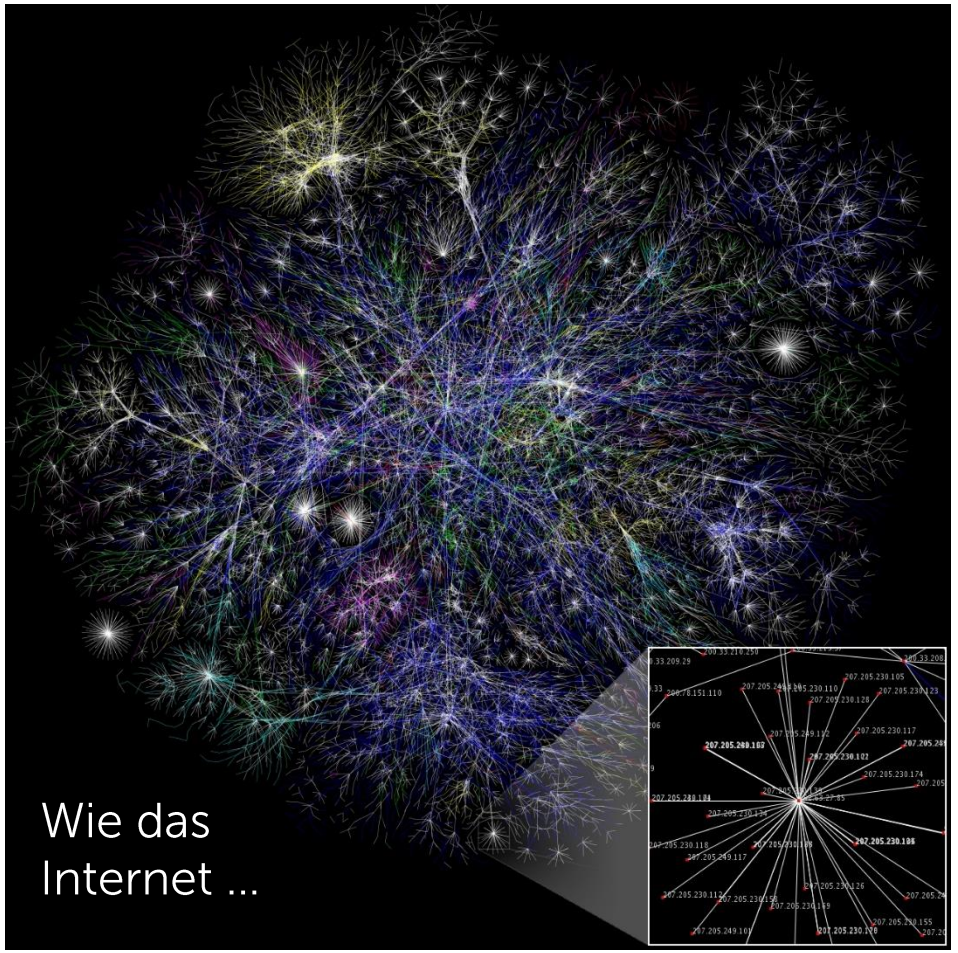
P2P	• Vernetzte Computer …
Konsens	• … erzielen Einigung …
Blockchain	• … über geteilte Daten.

Nach Peter van Valkenburgh, What is „Blockchain“ anyway?

P2P

Vernetzte Computer …

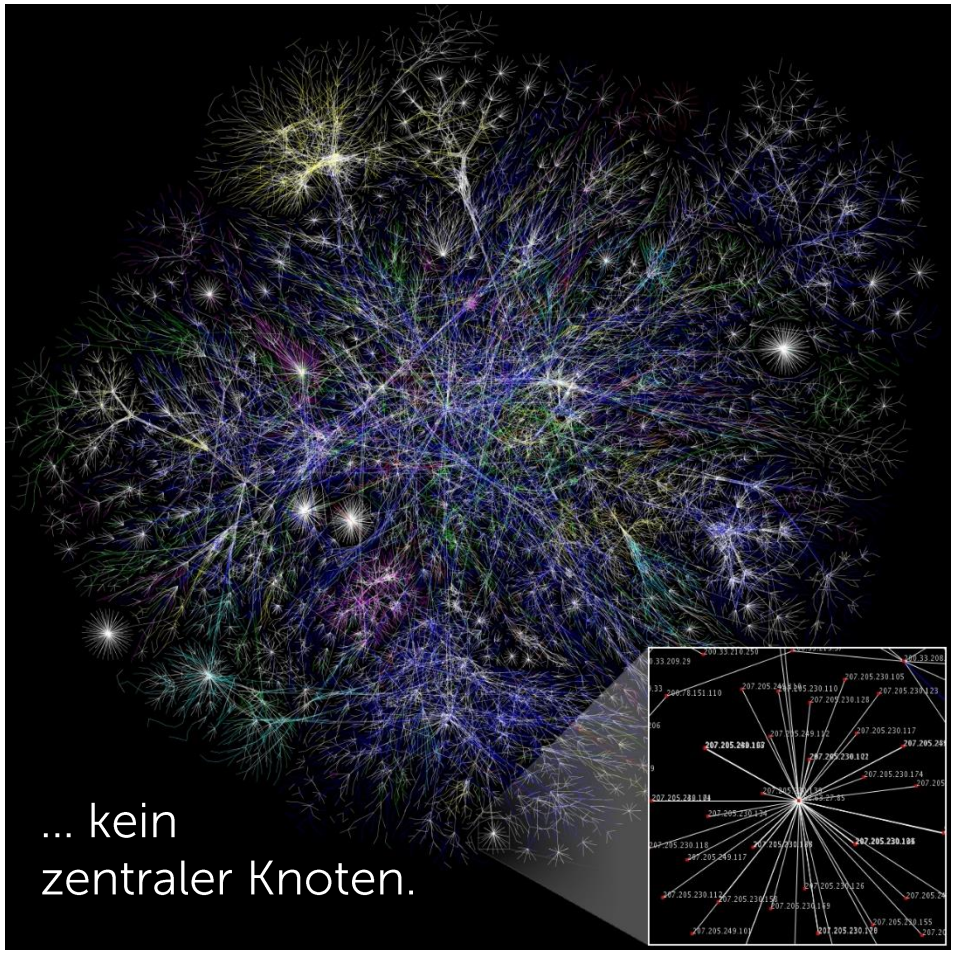
- Alle Computer im Netzwerk sind gleichwertig
- „Peers“ statt „Client-Server“
- Design sieht Ausfall einzelner vor



P2P

Stellen Sie sich vor ...

- „eBay“ ohne eBay Inc.
- „Uber“ ohne Uber Inc.
- „airBnB“ ohne airBnB Inc.
- „Facebook“ ohne Facebook Inc.
- „Twitter“ ohne Twitter Inc.



Konsens

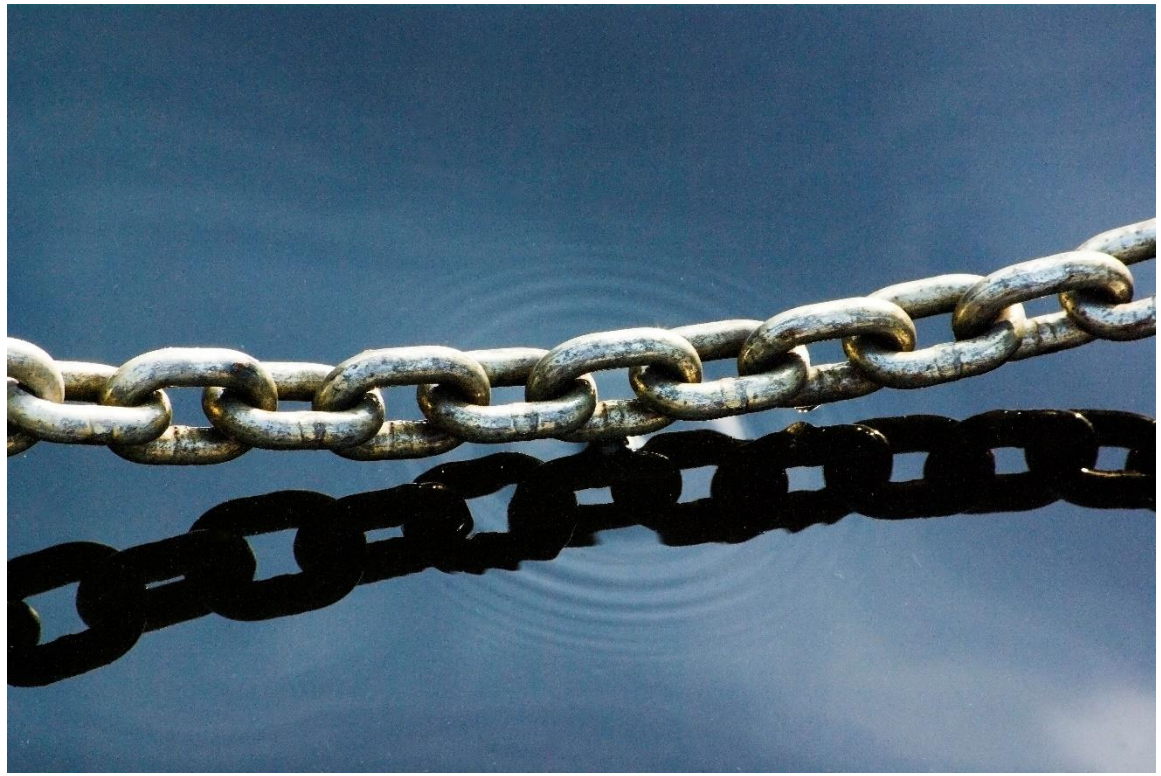
[Vernetzte Computer …] erzielen Einigung …

- Notwendig, weil alle gleich sind.
- Verschiedene Möglichkeiten
  - Zugang offen oder geschlossen
  - Daten lesbar für alle oder nicht

Blockchain

[Konsens] … über geteilte Daten.

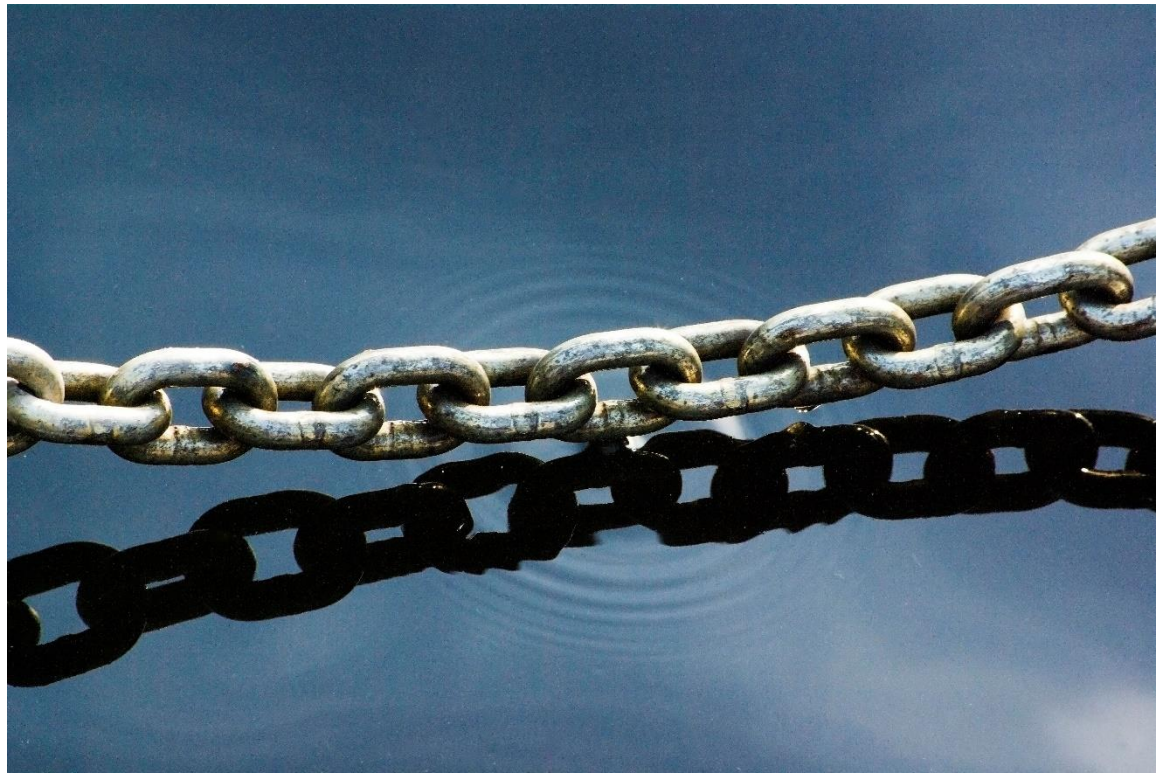
- Worüber Konsens?
  Über Zustand, Aktualität der geteilten Daten im Netzwerk.
- Nachträgliche Manipulation ausgeschlossen



Blockchain

[Konsens] … über geteilte Daten.

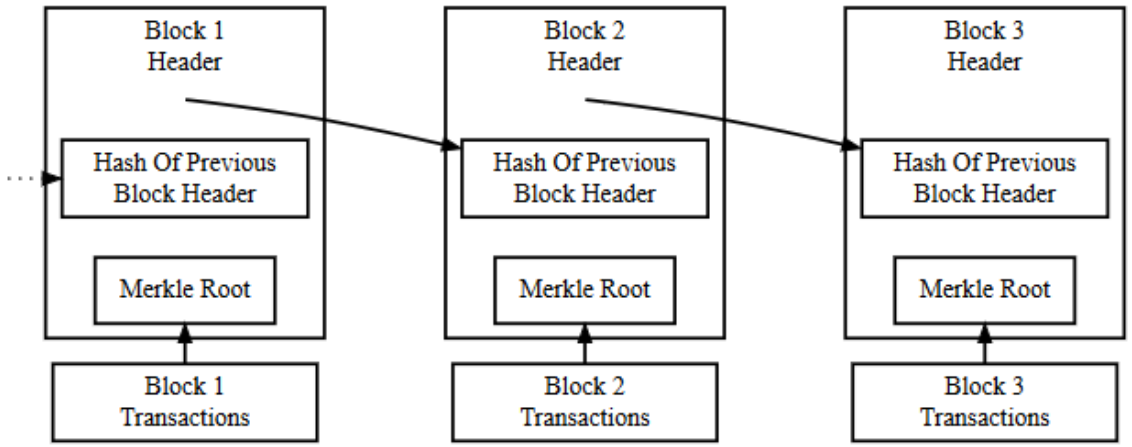
- Welche Daten?
  - Identität
  - Eigentum
  - Rechte
  - Stimmen (votes)
  - Gesundheitsdaten
  - u.v.a.m.
- Nicht nur Personen!
  - Geräte im Internet of Things



Wie funktioniert eine Blockchain konkret?

Transaktionen → Blöcke → Kette → Konsens

- Transaktionen formen einen Block
  - Transaktionen werden gesammelt und paarweise gehasht.
  - Root eines Merkle Baums generiert und gespeichert.
- **Blöcke** formen eine Kette
  - Jeder Block speichert Hash der vorherigen Blocks, was die Blöcke miteinander verkettet. Dies stellt sicher, dass man eine Transaktion nicht verändern kann, ohne den Block und alle Folgeblöcke auch anzupassen (damit alle Hashes wieder stimmen).
- Die **Blockchain** bildet dadurch ein geordnete Aufzeichnung von Transaktionen der Netzknoten, die im nachhinein nicht (unbemerkt) veränderbar ist.



Simplified Bitcoin Block Chain

S: Bitcoin.org/en/developer-guide

“Banking ist nur der Anfang…”

Breites Einsatz- und Branchenspektrum für Blockchain-Technologie

Branche	Beispiel	Branche	Beispiel	Branche	Beispiel
Banking	*vault OS, R3CEV*	Gift card/loyalty programs	*Gyft*	Ride sharing	*La'Zooz*
Stock trading	*t0*	Cyber security	*Guardtime*	Government, public benefits	*GovCoin*
Charity	*GiveTrack*	Insurance	*Stratumn*	Healthcare	*Gem, Tierion*
Cloud storage	*Storj, IPFS*	Wills/Inheritance		Gun tracking	*BlockSafe*
Car leasing and sales	*DocuSign*	Forecasting	*Augur*	Energy management	*TransactiveGrid, LO3*
Real estate	*Ubitquity*	Sports management	*Jetcoin*	Supply chain mangement	*Provenance, Fluent*
Payments & money transfer	*Abra*	Voting	*FollowMyVote*	Social Networks	*Steem.it, ZeroNet*
Retail	*OpenBazaar*	Online music	*ujomusic*	Law enforcement	*Chronicled, Elliptic*
Academic certificates	*Holbertson*	Networking / IoT	*Filament, IOTA, IBM Adept*	HR Certificates	*ascribe*

https://www.cbinsights.com/blog/industries-disrupted-blockchain/

Was das alles bedeutet (1)

Digitale Äquivalente von „Trusted third parties“ möglich

Kirche

Staat

Wirtschaft

- Seit Anbeginn haben wir Drittparteien eingesetzt (gebraucht), um Verträge/Transaktionen zwischen Menschen abzuwickeln. Die Institutionen kamen von der Kirche, dem Staat oder, seit Kurzem, aus der Wirtschaft.
- Blockchain-Technologie verspricht ebenfalls Vertrauen zwischen unbekannten Partnern zu ermöglichen.

- Welche „trusted third parties“ brauchen wir weiterhin? Welche ggf. nicht mehr?

Was das alles bedeutet (2)

Nicht nur Digitalisierung sondern Transformation

Die Blockchain wird für Banking, Recht und Buchführung das sein, was das Internet für die Medien, Handel und Werbung war.
– Joichi Ito, Director MIT Media Lab

Blockchain [Bitcoin] gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate.
– Marc Andreessen, Why Bitcoin matters (NYT)

Was das alles bedeutet (3)

Für Staat/Verwaltung

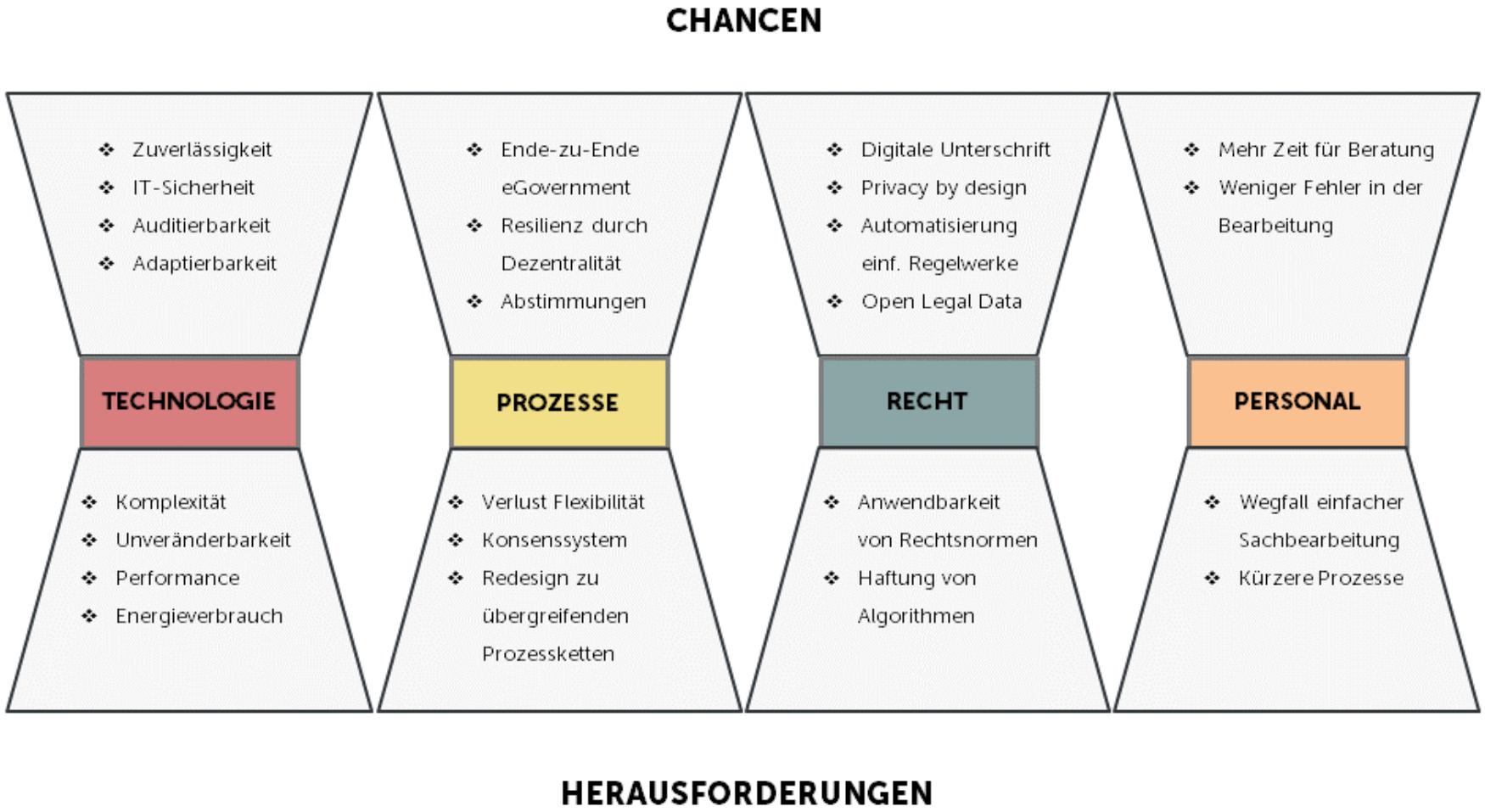
„Manipulationssichere Registerführung und Beglaubigung stellen gleichermaßen zentrale Aufgaben der Verwaltung sowie das Kernversprechen der Blockchain dar.

Sie hat deshalb das Potential, die durch zentrale Organisationsparadigmen geprägte Verwaltung nachhaltig zu verändern."

(Dapp, Balta, Krcmar 2017, S. 7)

Was das alles bedeutet (4)

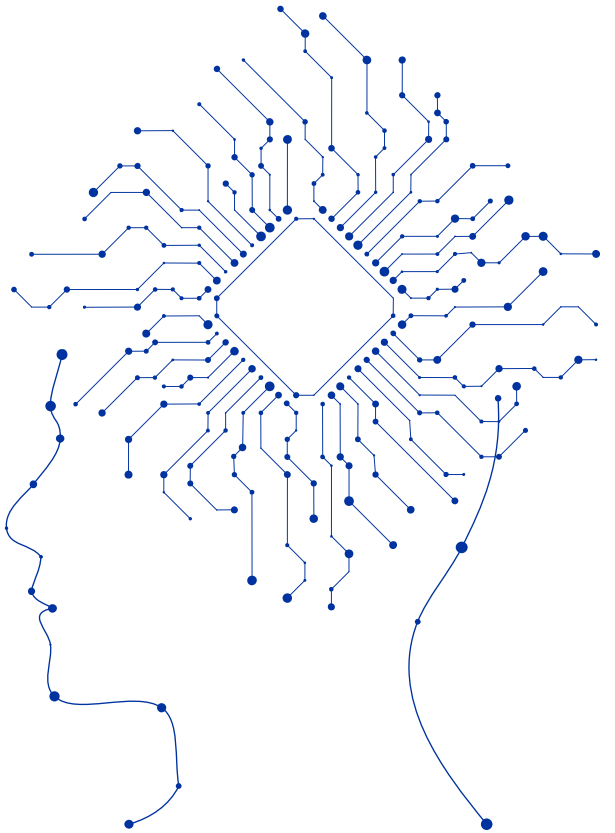
Für Staat/Verwaltung



fortiss

Vielen Dank!

Einführung in Blockchain Technologie

Prof. Helmut Krcmar
Lehrstuhl Wirtschaftsinformatik TU München
Sprecher des Direktoriums fortiss

fortiss GmbH
An-Institut Technische Universität München