



# DLT als Audit- und Vertrauensschicht für KI-Entscheidungen

*eine praxisbasierte architektur- und governance-orientierte Einordnung*

**MARKUS  
BEGEROW**



#gerneperDu



**DATENBANKEN  
VERSTEHEN**

*für Anfänger und Profis*



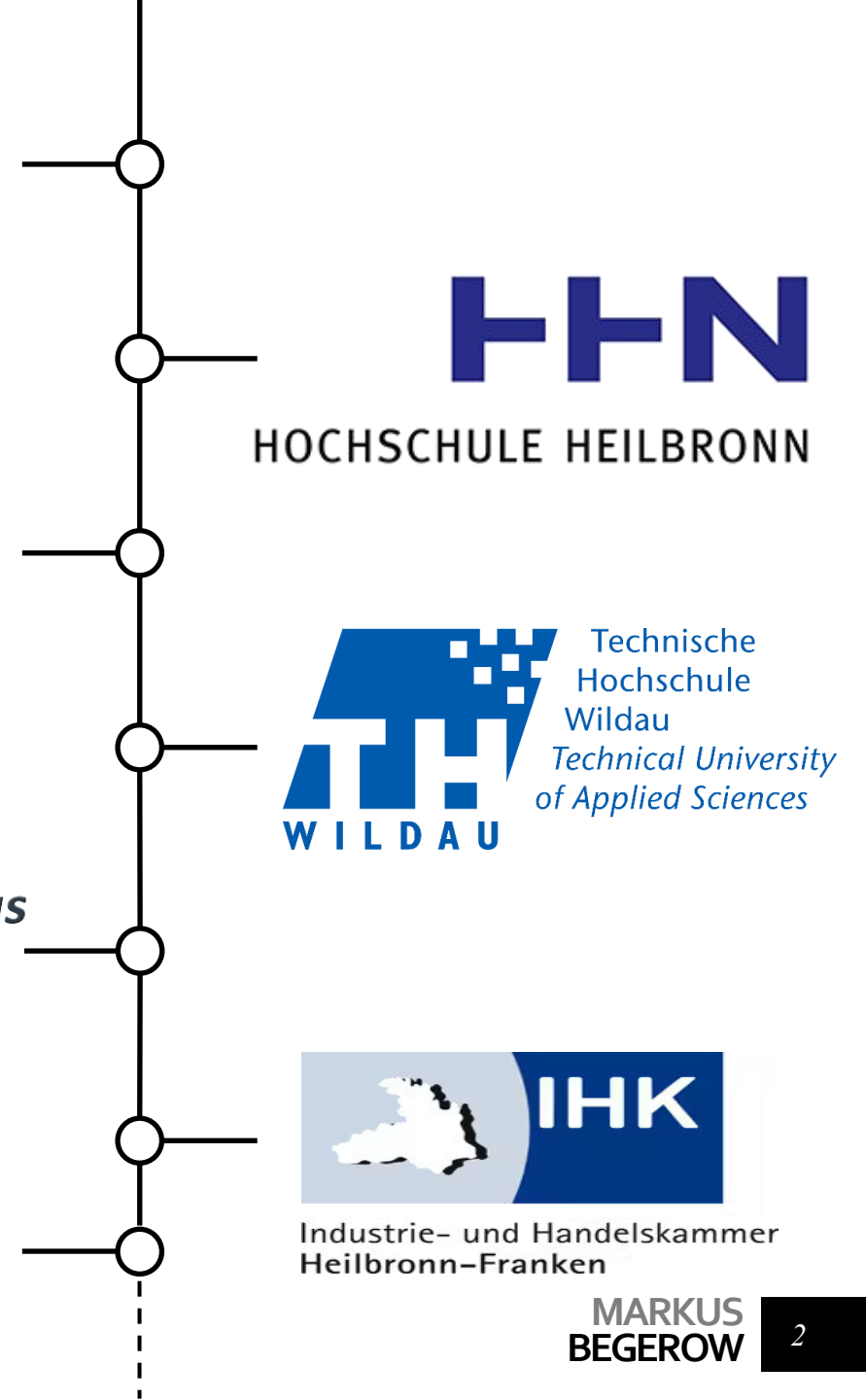
**Data & AI Campus**

*Your next level in Data & Analytics*



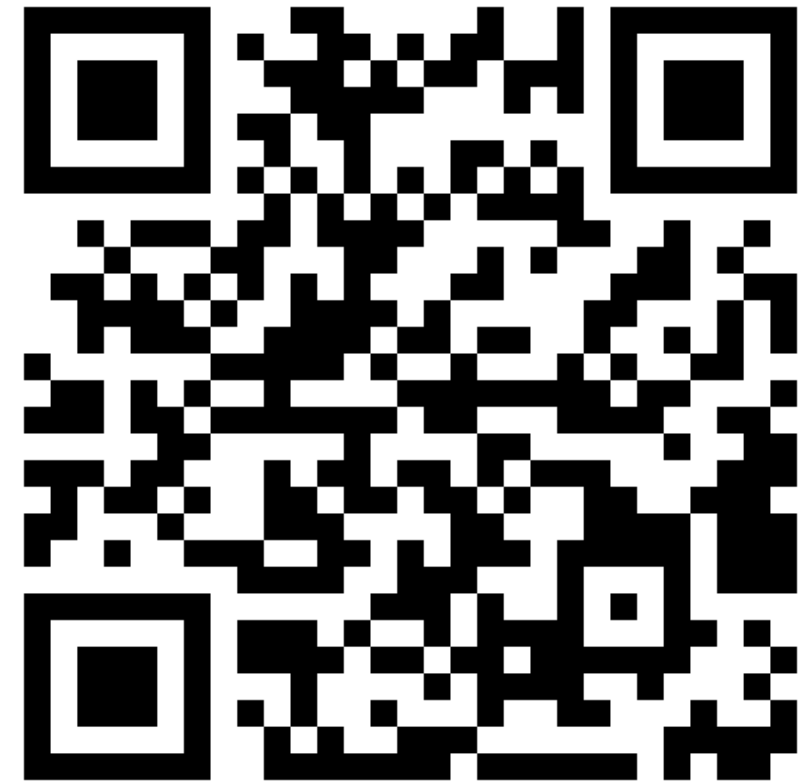
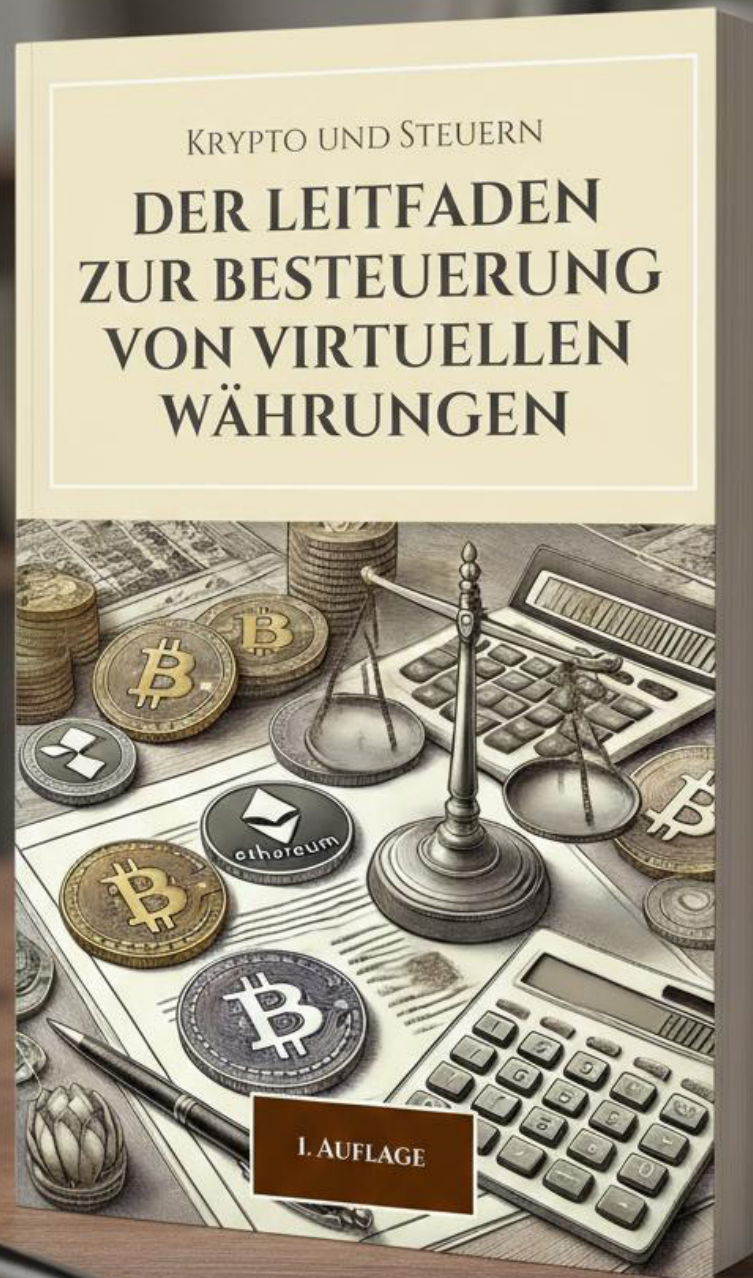
**wbh**

**WILHELM BÜCHNER  
HOCHSCHULE**



**MARKUS  
BEGEROW**





**SCAN MICH 😊**

# Wo stehen wir heute?



Source: [Gartner](#)

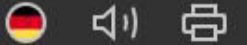


**Markus Begerow** • Sie  
Advisor for Data, AI & Blockchain | Speaker · Author · Mentor

Thanks for sharing. Okay and 60% of the projects will be successful or what?  
From 0 to 60% is a good start, I think 😊

## Artificial intelligence: Vibe coding service Replit deletes production database

According to a Replit user, the service has deleted its production database, made false statements about it and ignored instructions. The manufacturer responds.



(Image: Shutterstock/Usa-Pyon)

Jul 25, 2025 at 10:23 am CEST 4 min. read Developer

By [Maika Möbus](#)

Source: [Heise](#)



## News & Media

- News
- Press releases
- Press summaries
- Newsletter - EESC Info
- Reporting From Plenary
- Members' Voices
- Podcasts - The Grassroots View
- The EESC on social media

HOME / NEWS & MEDIA / DECENTRALISED AND AGENTIC AI: BOOSTING INNOVATION, COMPETITIVENESS AND RESPONSIBLE AI

# Decentralised and Agentic AI: boosting innovation, competitiveness and responsible AI

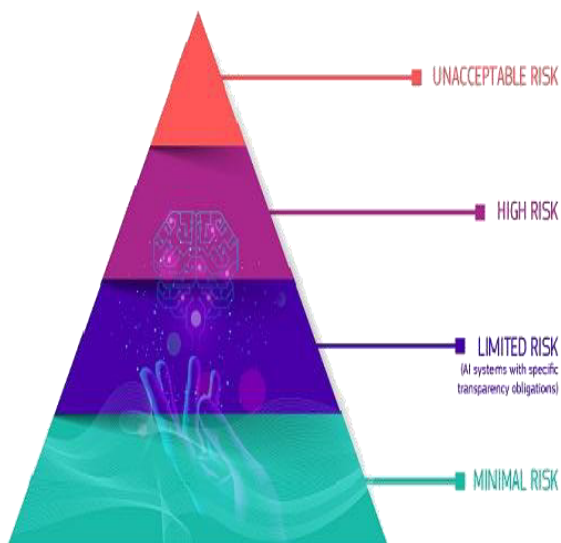
This page is also available in: **FR**

09/02/2026



On 5 February 2026, the EESC Employers' Group hosted a high-level policy roundtable, organised by the Digital Currencies Governance Group (DCGG) titled "Decentralised & Agentic AI: Opportunities and Solutions in the EU for Innovation, Competitiveness and Responsible AI".

Source: [European Economic and Social Committee](#)



# Gartner Predicts by 2028, 50% Of Organizations Will Adopt Zero-Trust Data Governance as Unverified AI-Generated Data Grows

STAMFORD, Conn., January 21, 2026

## Increasing Volume of AI-Generated Data Threatens Future Large Language Model Reliability

By 2028, 50% of organizations will implement a zero-trust posture for data governance due to the proliferation of unverified AI-generated data, according to Gartner, Inc., a business and technology insights company.

“Organizations can no longer implicitly trust data or assume it was human generated,” said **Wan Fui Chan**, Managing VP at Gartner. “As AI-generated data becomes pervasive and indistinguishable from human-created data, a zero-trust posture establishing authentication and verification measures, is essential to safeguard business and financial outcomes.”

Source: [Gartner](#)



Peter Steinberger is joining OpenAI to drive the next generation of AI agents. He is a genius with a lot of amazing ideas about how smart agents interacting with each other to do very useful things for people. We expect this will quickly become core to our mission.

OpenClaw will live in a foundation as an open source project that we will continue to support. The future is going to be exciting and it's important to us to support open source as part of our mission.

[Post übersetzen](#)

10:39 nachm. · 15. Feb. 2026 · **16,2 Mio.** Mal angezeigt

4.899

8.822

46.299

Relevant ▾

OpenClaw

What People Say



BUSINESS INSIDER

## OpenClaw: Meta-Managerin verliert plötzlich die Kontrolle und erlebt einen KI-Albtraum

Henry Chandonnet

Di., 24. Februar 2026 um 12:50 PM MEZ



In diesem Artikel:

BTZI -6,25 % ☆



Meta's Summer Yue bezeichnete Ihre OpenClaw-Horrorgeschichte als „Anfängerfehler“. - Copyright: Tayfun Coskun/Anadolu Agency via Getty Images

MARKUS  
BEGEROW

6

Source: [Forbes](#)

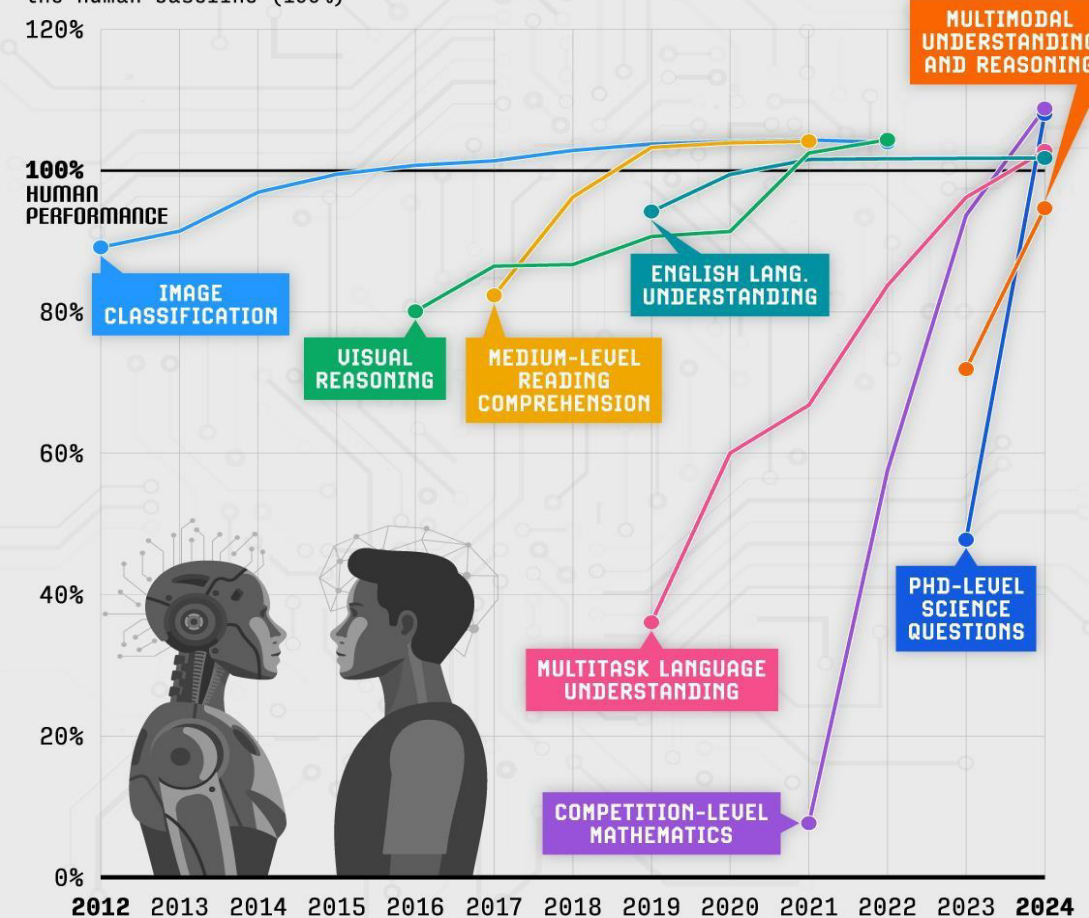




KI wird den Menschen in allen Bereichen, die wir trainieren und testen können, übertreffen - oder hat dies bereits getan.

# AI VS. HUMAN PERFORMANCE IN TECHNICAL TASKS

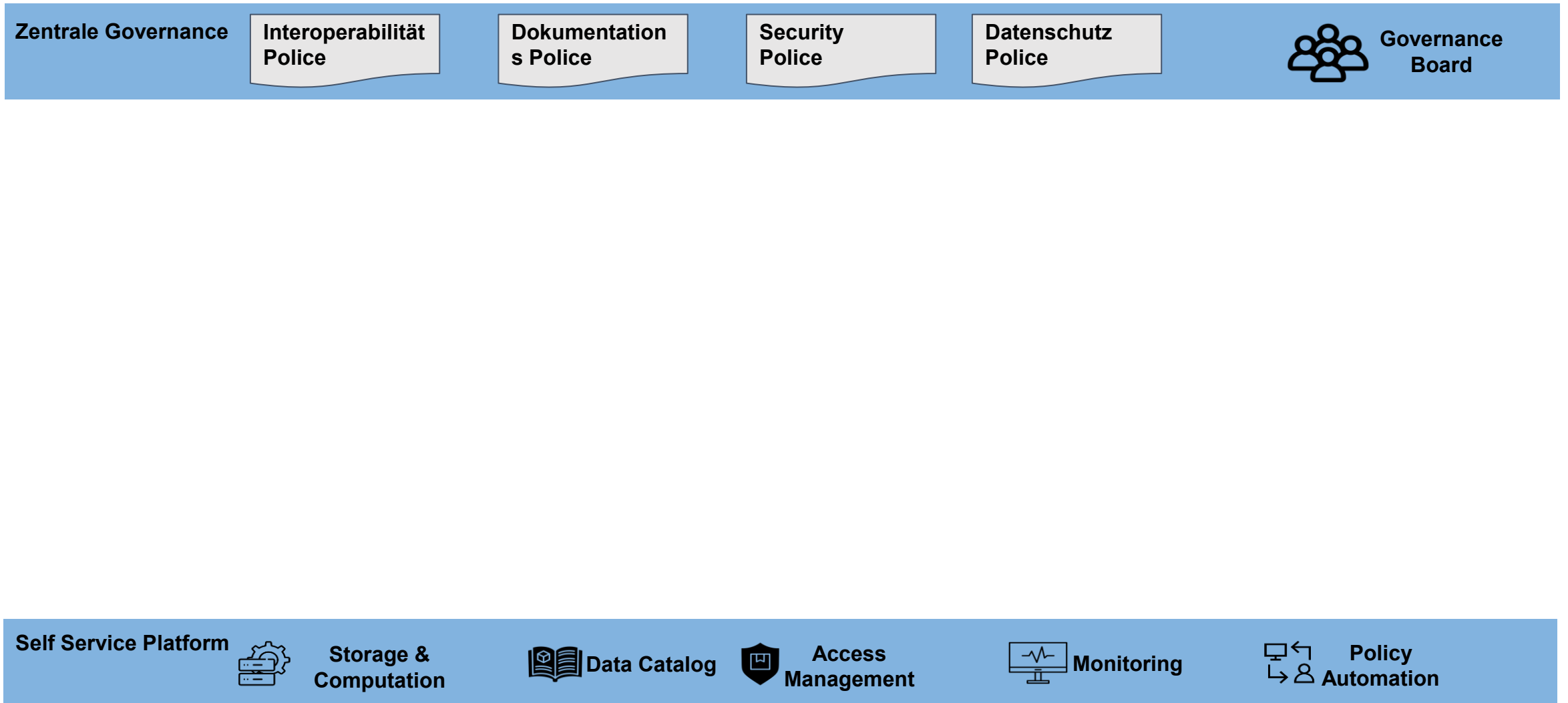
Performance relative to the human baseline (100%)



VISUAL CAPITALIST

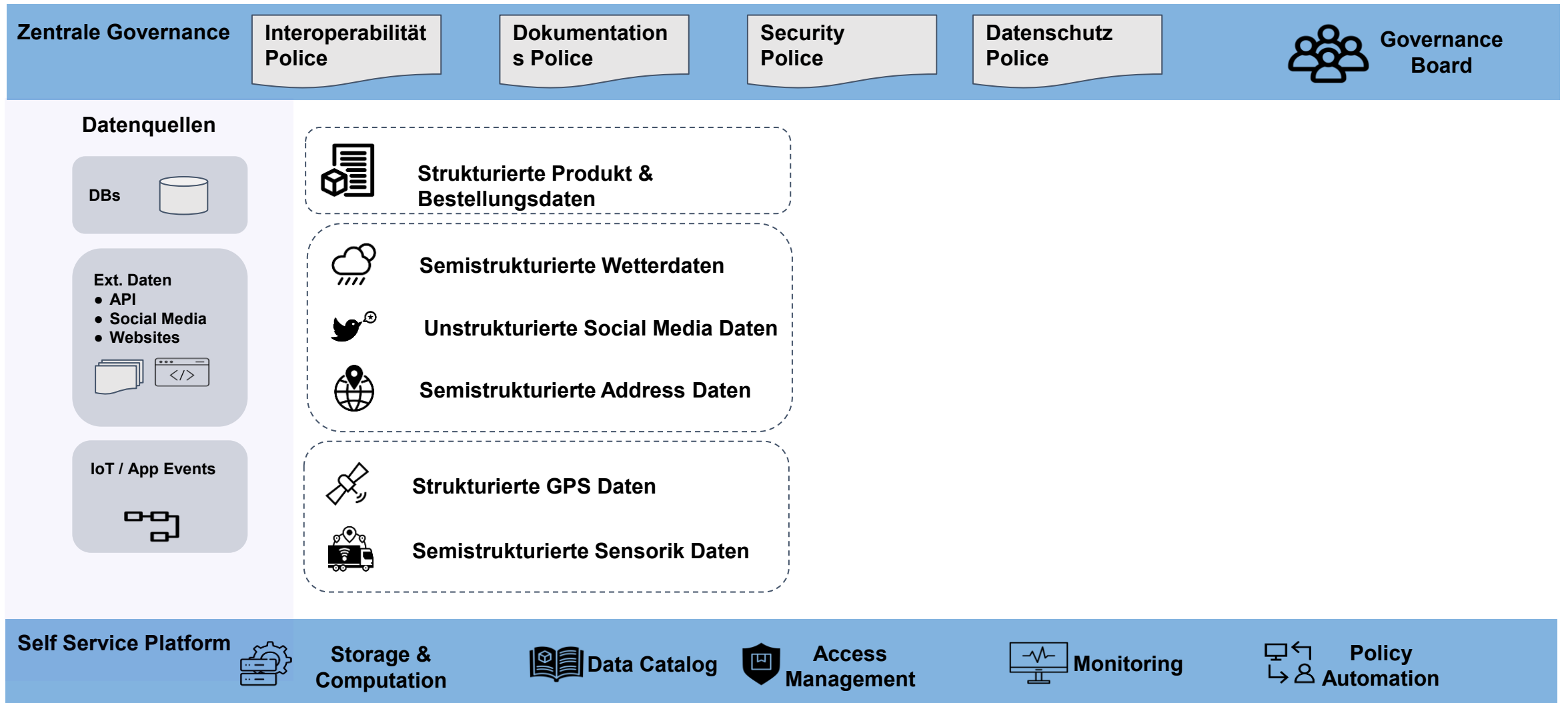
Source: Stanford University, 2025 AI Index Report

# Datenarchitekturen und Grenzen

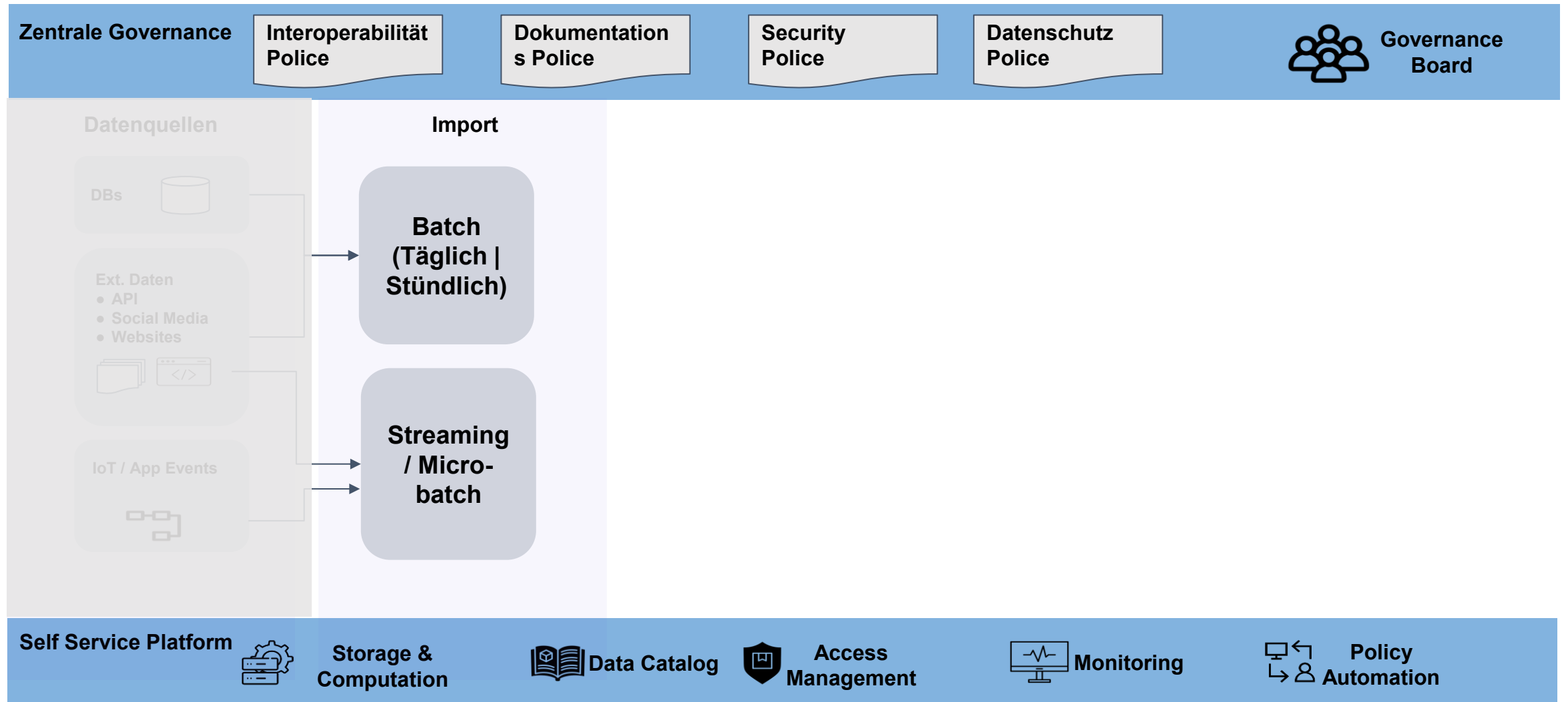




# Datenarchitekturen und Grenzen

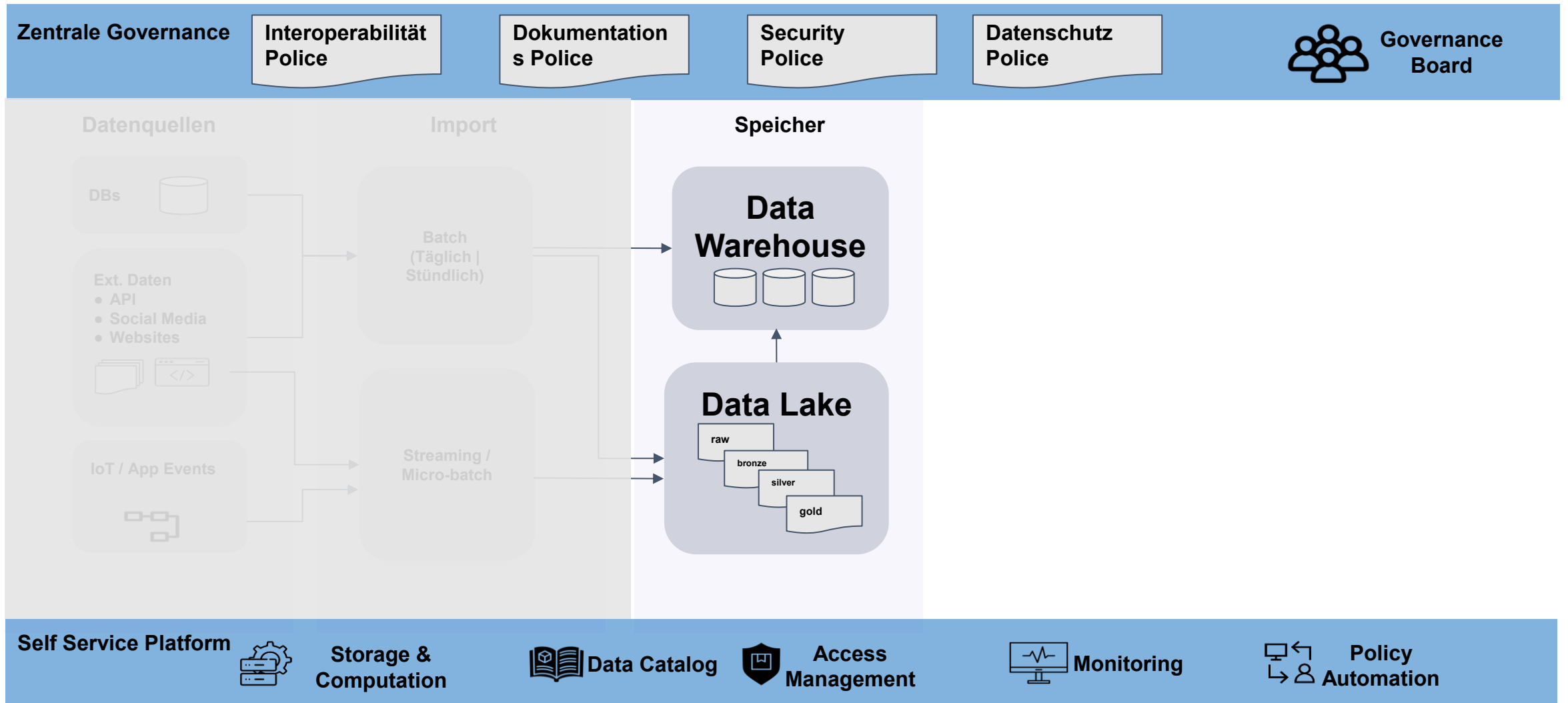


# Datenarchitekturen und Grenzen

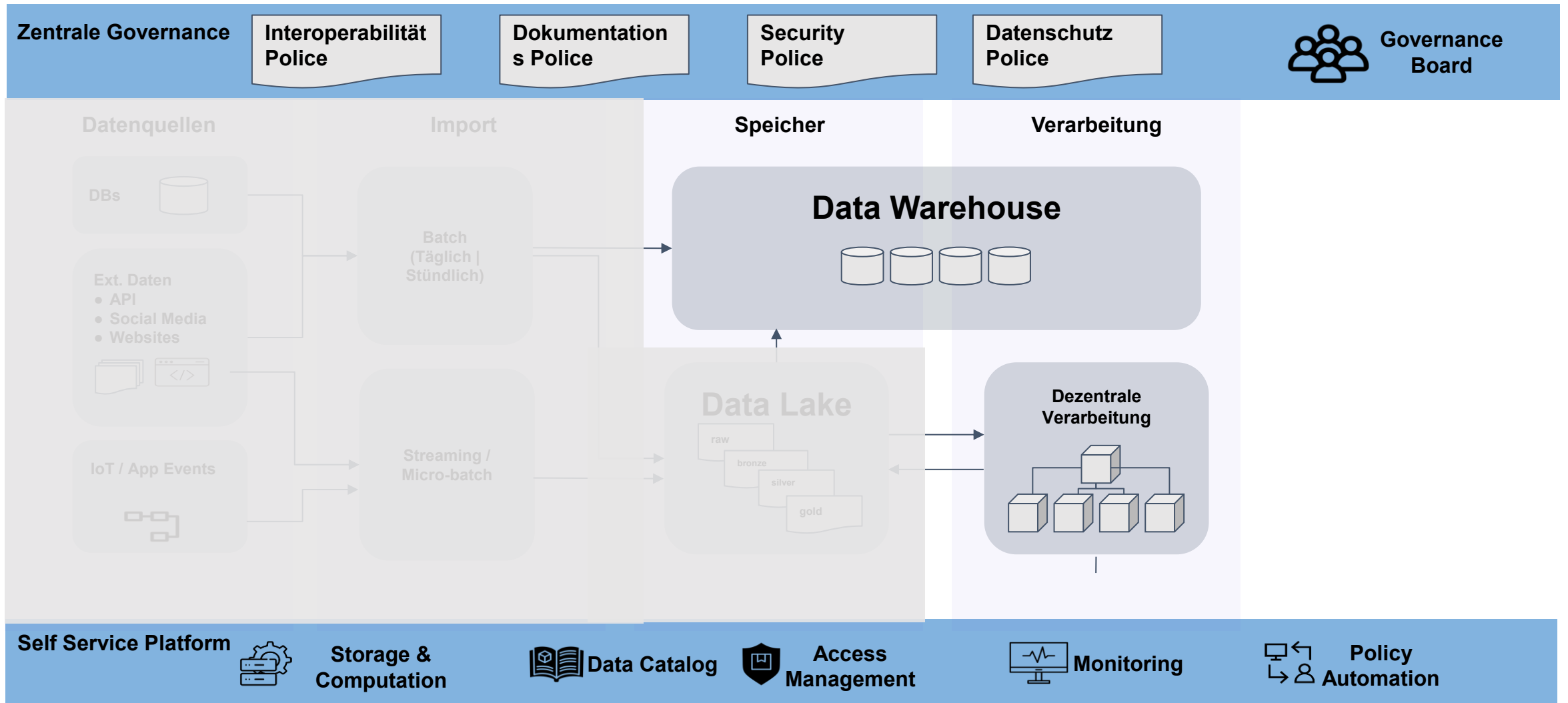




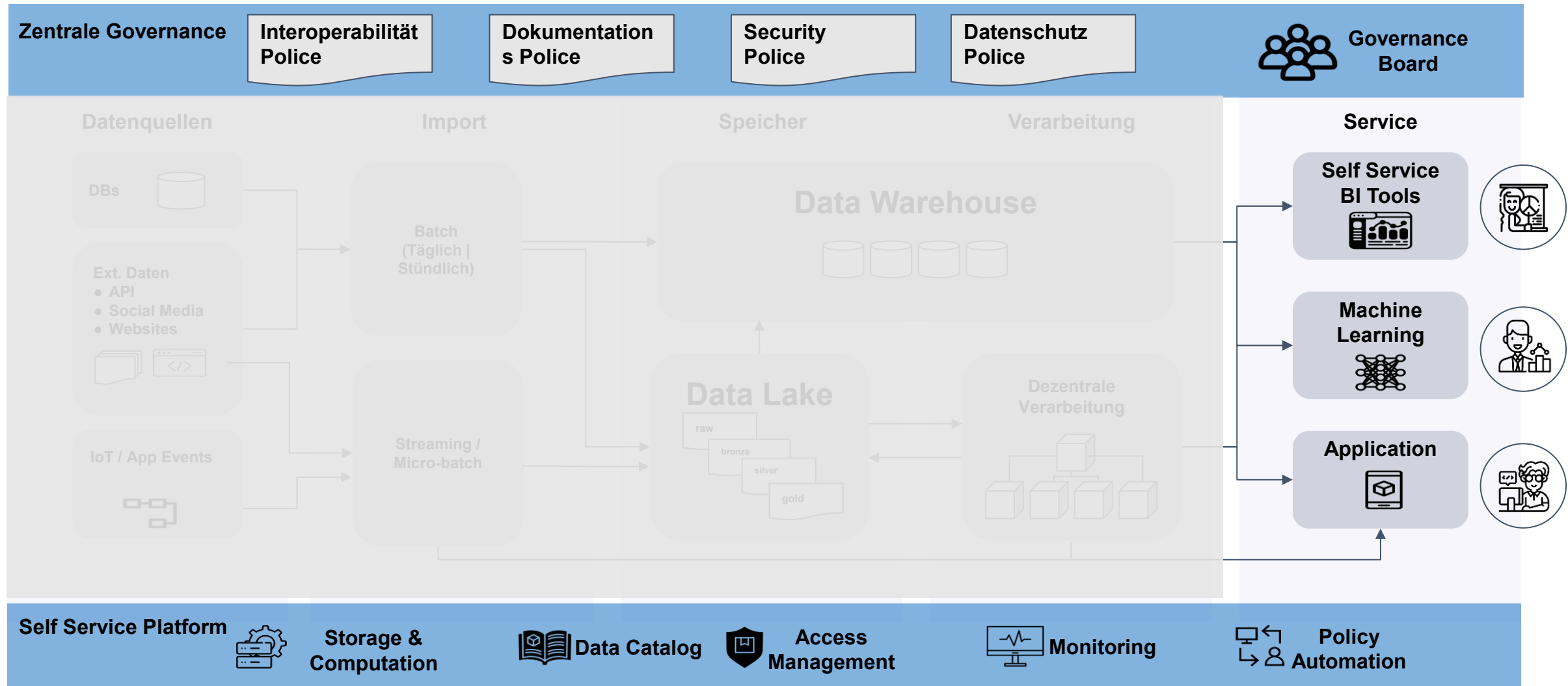
# Datenarchitekturen und Grenzen



# Datenarchitekturen und Grenzen

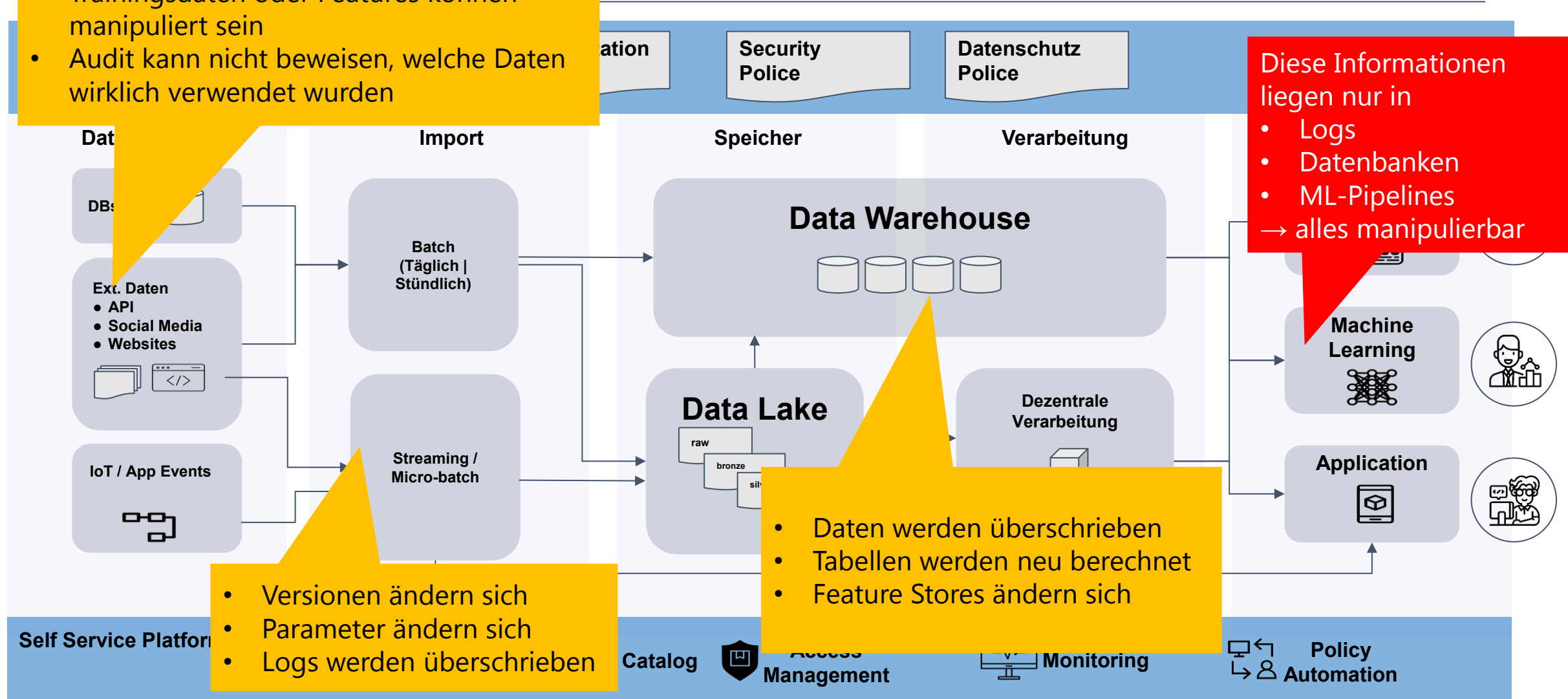


# Datenarchitekturen und Grenzen





- Daten können nachträglich verändert werden
- Trainingsdaten oder Features können manipuliert sein
- Audit kann nicht beweisen, welche Daten wirklich verwendet wurden



Diese Informationen liegen nur in

- Logs
- Datenbanken
- ML-Pipelines

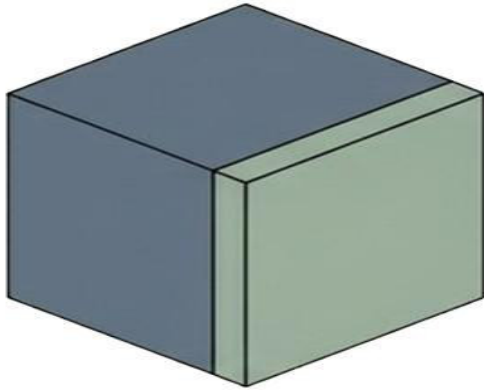
→ alles manipulierbar

- Versionen ändern sich
- Parameter ändern sich
- Logs werden überschrieben

- Daten werden überschrieben
- Tabellen werden neu berechnet
- Feature Stores ändern sich

# Interne Governance und Erklärbarkeit stoßen an strukturelle Grenzen

---



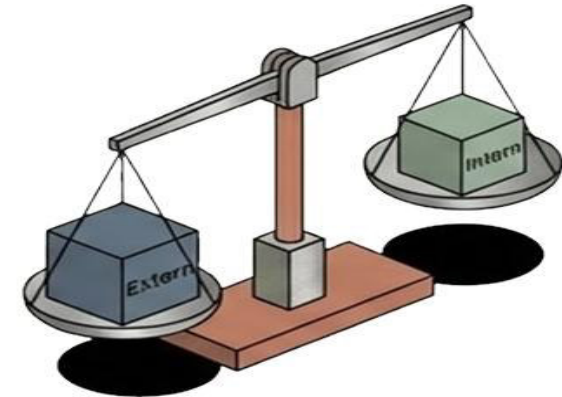
## **Silo-Denken**

Komplexe, historisch gewachsene IT-Landschaften verhindern eine konsistente Dokumentation.



## **Manipulierbarkeit**

Klassische systeminterne Logging-Ansätze können unbemerkt verändert werden.



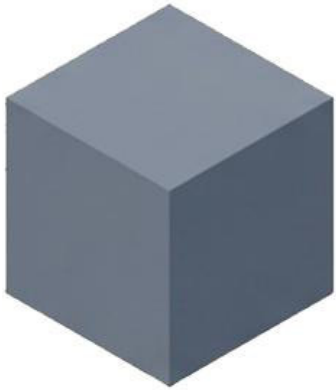
## **Fehlender externer Beweis**

Interne Kontrollen schaffen kein vertrauenswürdiges Fundament für organisationsübergreifende Audits.

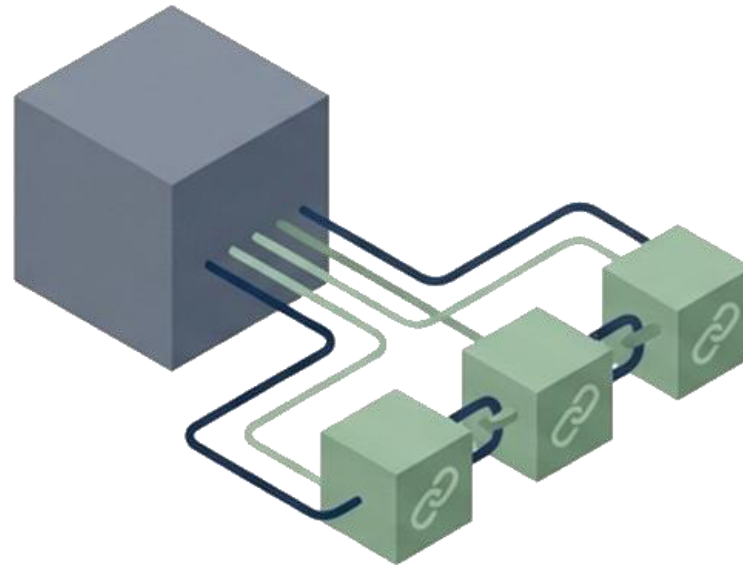
# Vertrauen als Systemeigenschaft

Nachhaltiges Vertrauen in KI-Entscheidungen erfordert eine eigenständige Audit- und Vertrauensschicht, die über rein daten- und modellzentrierte Ansätze hinausgeht.

Status Quo



Ansatz: DLT-Auditierung



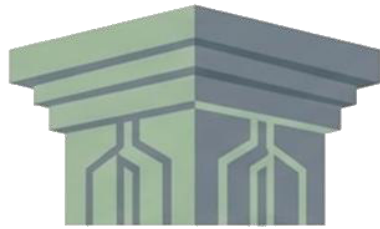
- KI-Modelle scheitern oft am Übergang von Pilot- zu Produktivumgebungen aufgrund fehlender Revisionssicherheit.
- Interne Kontrollen erklären Modelle, sichern sie aber nicht extern ab.
- Distributed-Ledger-Technologien (DLT) bieten die fehlende unabhängige, unveränderliche Infrastruktur zur Protokollierung von Ergebnissen.



# DLT als infrastruktureller Vertrauensmechanismus

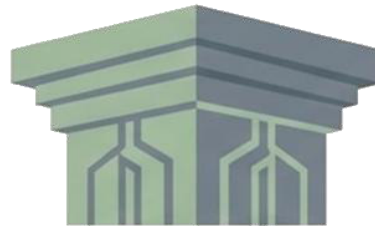
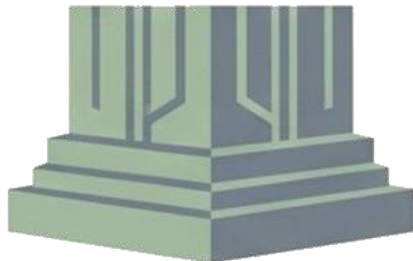
---

Distributed Ledgers fungieren hier **nicht als klassische Datenbank**, sondern als neutrale Referenzinstanz zur Reduktion von Manipulationsmöglichkeiten.



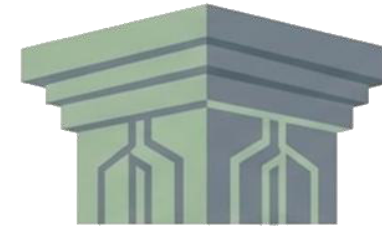
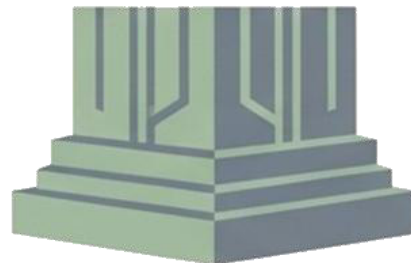
## Unveränderlichkeit

Einmal bestätigte Einträge sind **nachträglich nicht unbemerkt veränderbar**.  
Sichert die Integrität der zeitlichen Historie.



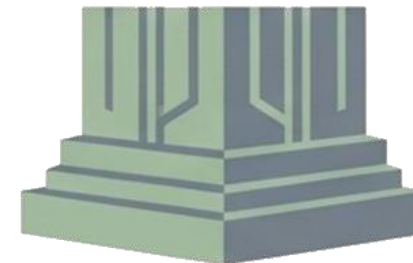
## Verteilte Kontrolle

Konsistenter **Datenbestand** über organisatorisch getrennte Instanzen hinweg. **Keine alleinige Kontrolle** durch den Systembetreiber.



## Permissioned Access

Kontrollierte Teilnahme definierter **Akteure** (Auditoren, Regulierer) mit klaren, oft **durch Smart Contracts** technisch verankerten Governance-Regeln.

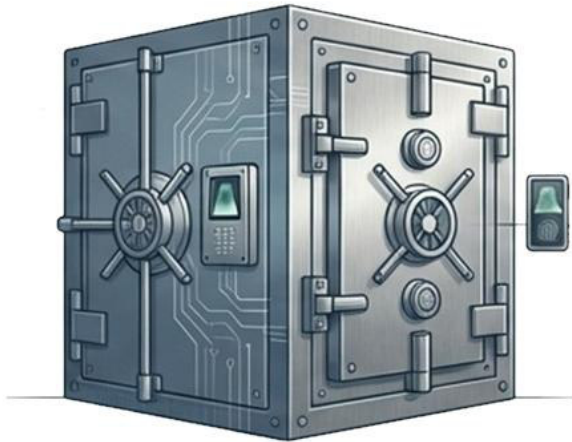


# Die strikte Trennung von Daten und Nachweis ermöglicht Skalierbarkeit

---

Sensible Daten und operative Logik werden niemals auf dem Ledger gespeichert.  
Vertrauen entsteht durch referenzielle Integrität.

## Off-Chain (Der Tresor)



### Sensible und große Daten

Trainingsdaten, Modellparameter,  
detaillierte KI-Entscheidungen  
**verbleiben in den bestehenden,**  
geschützten Systemen.

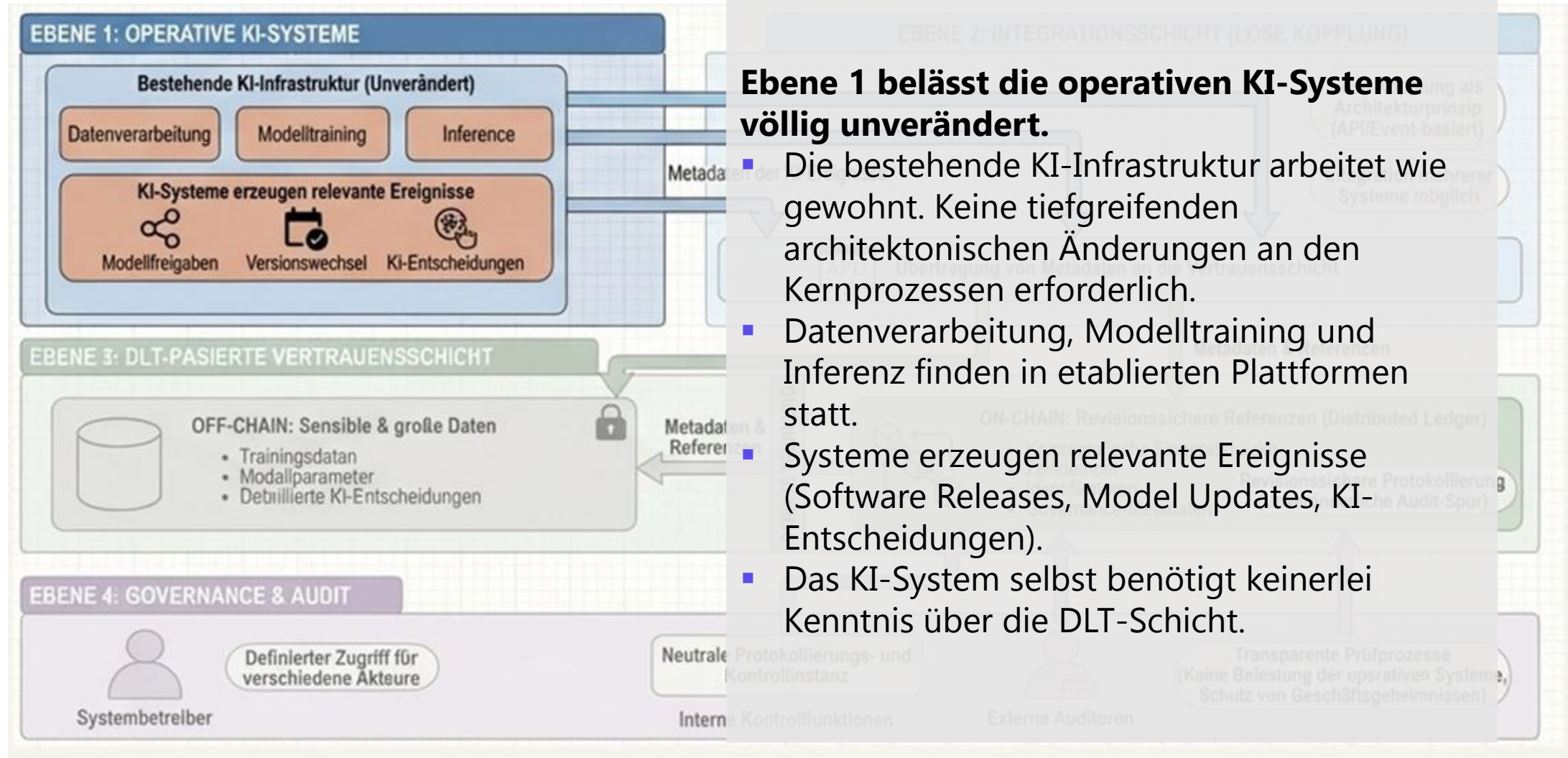
## On-Chain (Der Fingerabdruck)



### Revisionssichere Referenzen

Ausschließlich kryptographische  
Fingerabdrücke (Hashes),  
**Zeitstempel, Identifikatoren**  
**und Governance-Metadaten.**

# Vorgehensmodell



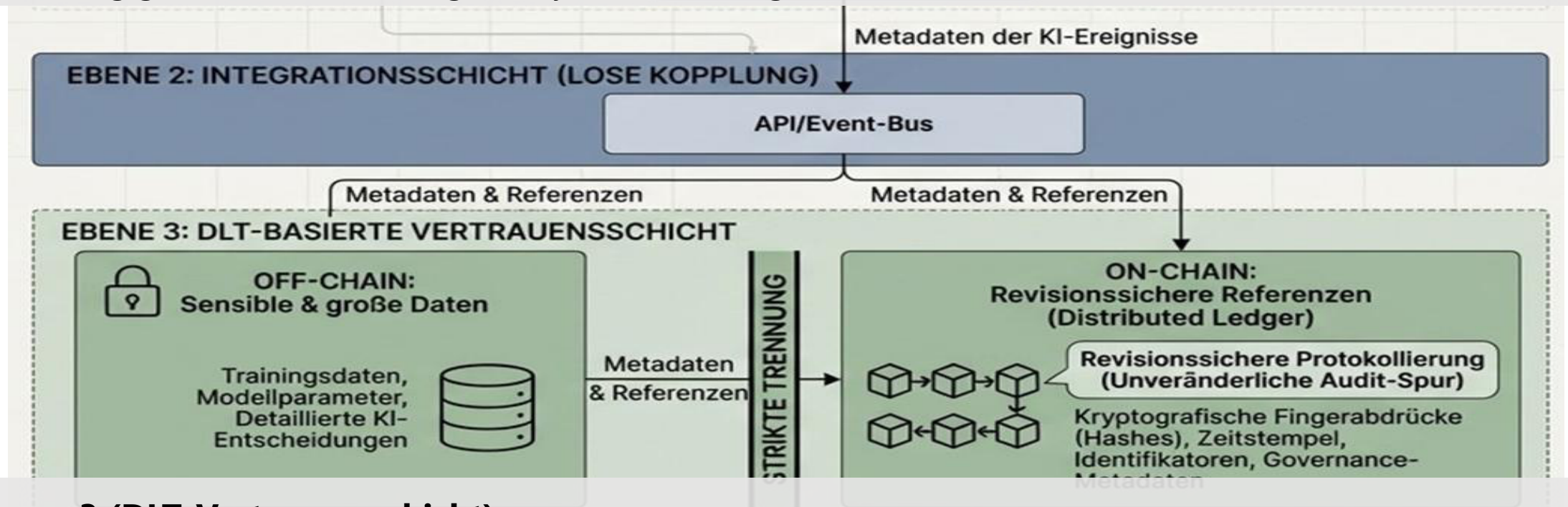
## **Ebene 1 belässt die operativen KI-Systeme völlig unverändert.**

- Die bestehende KI-Infrastruktur arbeitet wie gewohnt. Keine tiefgreifenden architektonischen Änderungen an den Kernprozessen erforderlich.
- Datenverarbeitung, Modelltraining und Inferenz finden in etablierten Plattformen statt.
- Systeme erzeugen relevante Ereignisse (Software Releases, Model Updates, KI-Entscheidungen).
- Das KI-System selbst benötigt keinerlei Kenntnis über die DLT-Schicht.

# Vorgehensmodell

## Ebene 2 (Integrationsschicht)

API/Event-Bus Mechanismen extrahieren flexibel Metadaten der KI-Ereignisse. Unabhängige Weiterentwicklung der Systeme bleibt gewährleistet. Integration mehrerer Systeme möglich

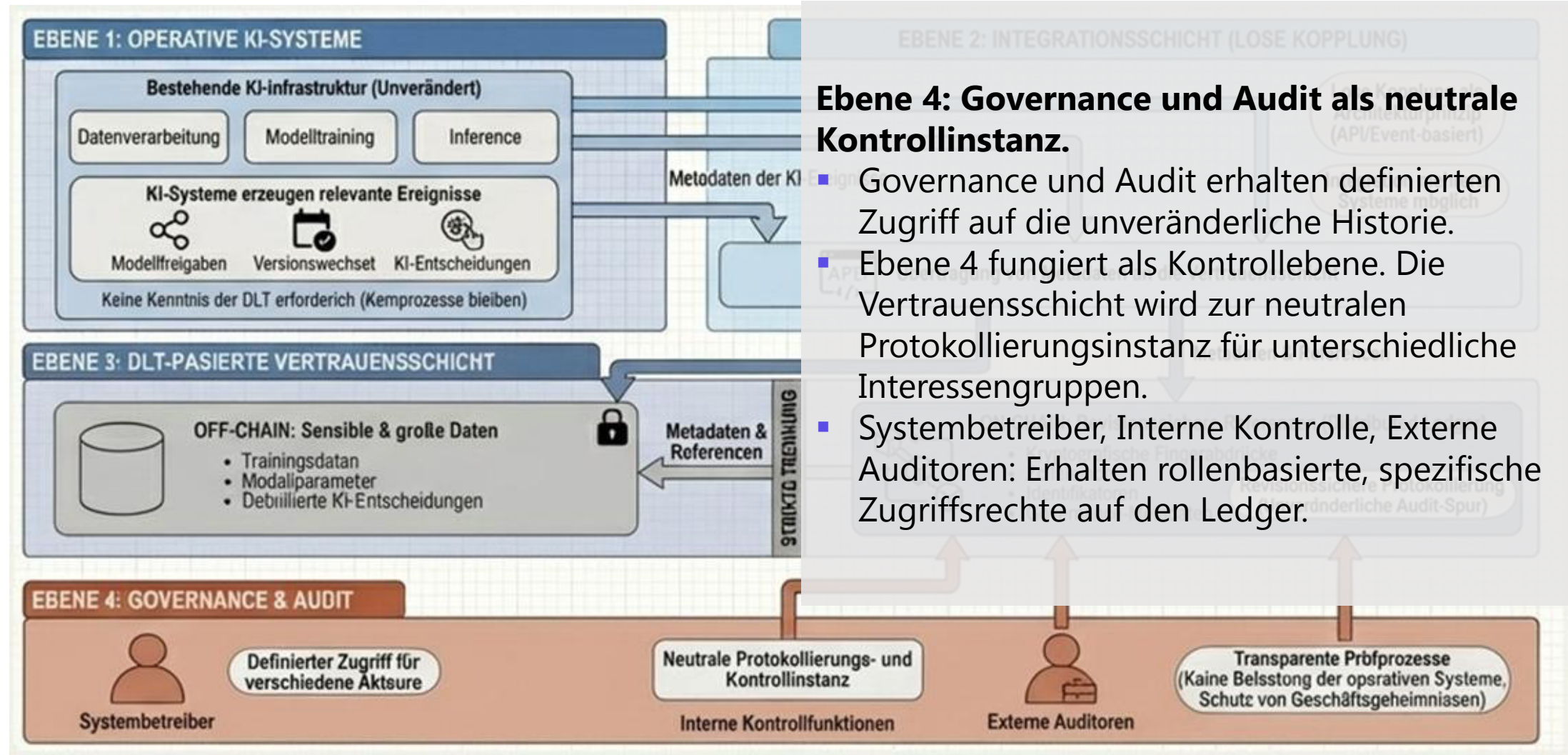


## Ebene 3 (DLT-Vertrauensschicht)

Revisionssichere Protokollierung der Metadaten On-Chain, während sensible Daten Off-Chain bleiben. Die lückenlose, unveränderliche Audit-Spur entsteht.



# Vorgehensmodell



# Die Vertrauensschicht löst konkrete Herausforderungen in der Praxis

**Relevanz** zeigt sich dort, wo **Entscheidungen prüfbar** und langfristig verantwortbar sein müssen!



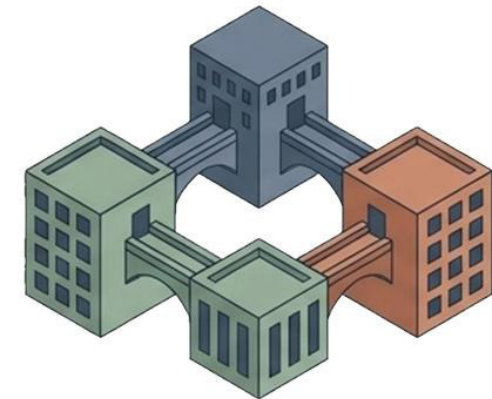
## Hochregulierte Domänen

Einsatz in  
**Finanzdienstleistungen**,  
**Verwaltung** oder kritischen  
Infrastrukturen (**KRITIS**).  
Ermöglicht regulatorische  
Kontrollen ohne Eingriff in  
operative Systeme.



## Externe Audits und Zertifizierungen

Standardisierte Prüfprozesse für  
**Aufsichtsbehörden** oder  
Geschäftspartner.  
Die Vertrauensschicht dient als  
**neutrale Referenz für alle  
Beteiligten**.



## Organisationsübergreifende KI- Wertschöpfungsketten

Eindeutige  
Verantwortungszuordnung in  
Plattformökosystemen, wenn sich  
**Akteure nicht vollständig  
vertrauen**.

# Der Governance-Shift: Von manueller Kontrolle zur Systemverantwortung

Die Verantwortlichkeit verschiebt sich von der singulären Modellkontrolle auf das Zusammenspiel der gesamten sozio-technischen Architektur.

## Die Rolle von Smart Contracts



- **Automatisierung von Governance-Regeln** (z. B. Protokollierungszwang für Modellfreigaben).
- **Einschränkung von Entscheidungen** auf verifizierte Modellversionen.
- **Governance wird explizit**, überprüfbar und technisch verankert.

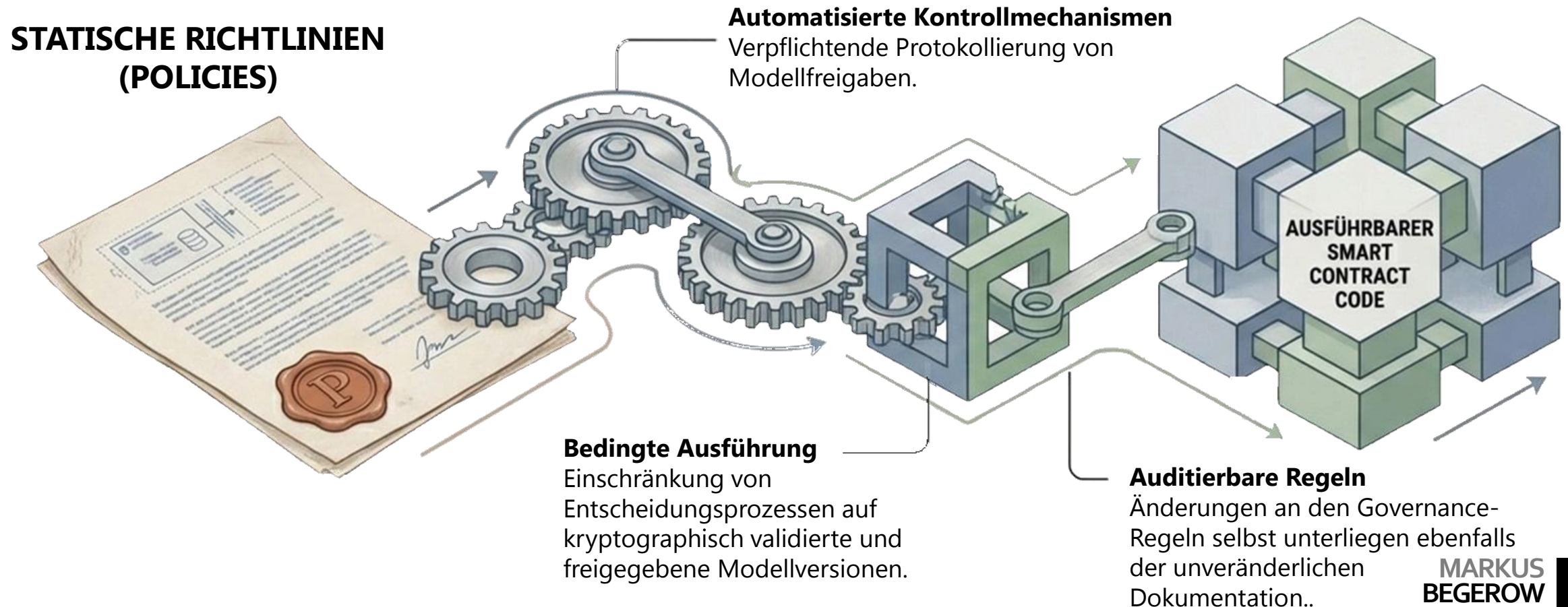
## Vorteil für Prüfinstanzen



Externe **Auditoren** erhalten eine **manipulationsresistente Bewertungsgrundlage**, ohne operativen Systemzugriff zu benötigen.

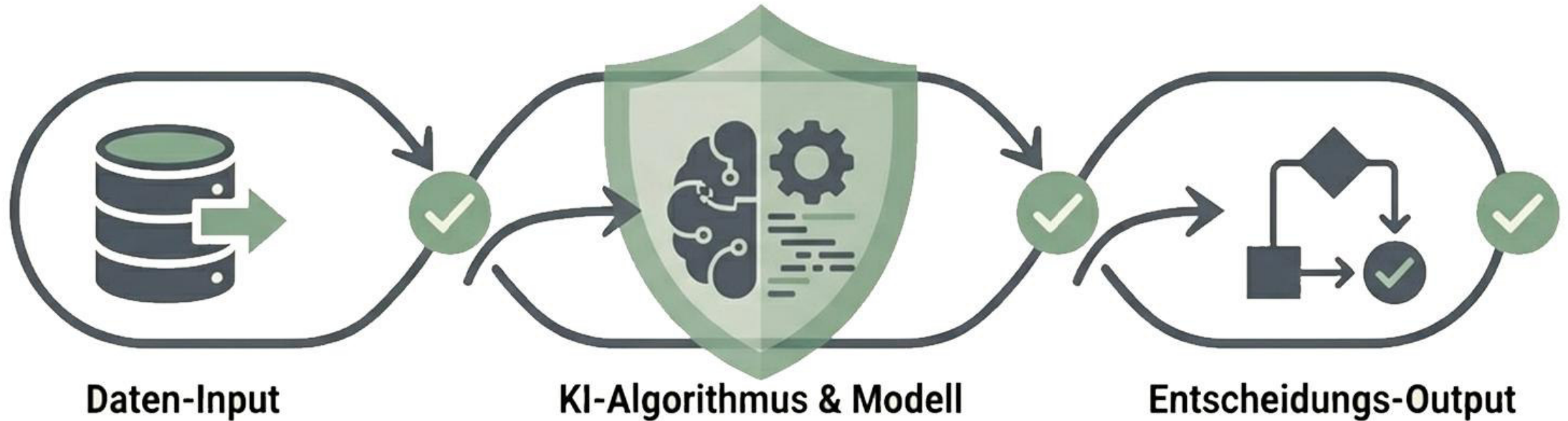
# Smart Contracts überführen statische Richtlinien in ausführbaren Code

Governance wird nicht nur organisatorisch definiert, sondern technisch in der Vertrauensschicht verankert.





# Governance-Implicationen: Institutionelle Verantwortung



**Lückenlose Historie**  
Eindeutige Zuordnung von Verantwortlichkeiten entlang der gesamten **KI-Wertschöpfungskette** (Wer hat wann welches Modell auf Basis welcher Daten freigegeben?).

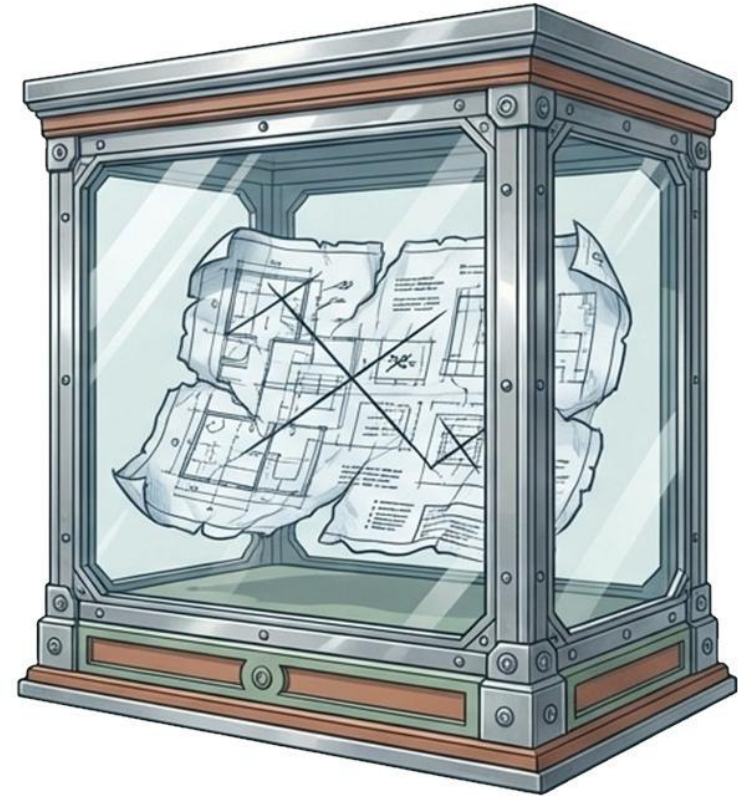
**Schutz von Geschäftsgeheimnissen**  
Erfüllung von regulatorischen **Dokumentationspflichten**, ohne interne Quellcodes oder sensible **Daten** gegenüber Dritten **offenzulegen**.

**Vom Modell zum System**  
Verschiebung des Fokus – Vertrauen entsteht durch das **Zusammenspiel von Architektur, Prozessen und institutionellen Rollen**, nicht nur durch bessere Algorithmen.

# Die Unveränderlichkeit der Historie garantiert keine korrekten Entscheidungen

Ein realistischer Blick auf die Grenzen des DLT-Einsatzes bewahrt vor technologischem Lösungs determinismus.

- **Gefahr der Scheinsicherheit: „Garbage in, garbage out“**  
Fehlerhafte Modelle werden lediglich revisionssicher protokolliert, nicht korrigiert.
- **Komplexität und Kosten:** Zusätzliche Schnittstellen, Latenzen und Betriebsprozesse erfordern sorgfältige Aufwandsbewertung.
- **Datenschutz (DSGVO & EU AI Act):** Die langfristige Speicherung von Metadaten erfordert rechtliche Bewertung im Umgang mit indirekten Rückschlüssen.



Das „Garbage in, garbage out“ Problem in DLT-Systemen  
Die perfekte Konservierung fehlerhafter Eingaben.

# Blockchain als Vertrauensschicht in der Zukunft



AI translated #artificial intelligence #ethereum

## Ethereum to Serve as a Trust Layer for AI Agents

Ethereum shifts focus to trust environment for AI, says Davide Cripis from EF.

05.03.2026 • ForkLog

Ethereum will shift away from on-chain computations for neural networks, opting instead to create a trust environment for autonomous programs. This was stated by Davide Cripis, head of AI at the Ethereum Foundation (EF), in an interview with [CoinDesk](#) at NEARCON 2026.

Source: [forklog](#)

## Blockchain Infrastructure as a Trust Layer for Artificial Intelligence Systems: A Comprehensive Analysis of Decentralized Solutions for AI-Era Identity, Payments, and Privacy Challenges



Jung-Hua Liu

Follow

20 min read • Feb 6, 2026



51



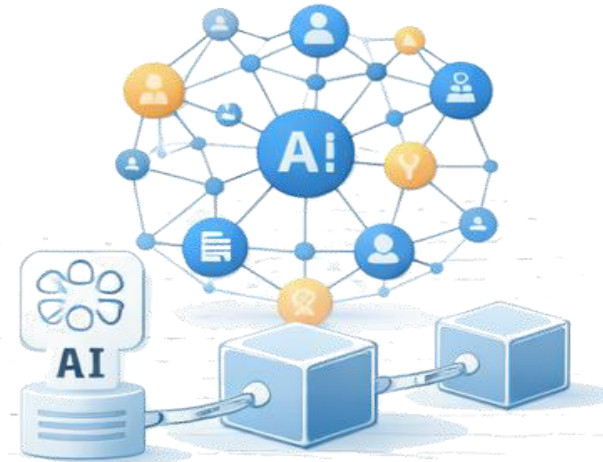
Source: [Medium](#)

# 3 Gedanken zum Mitnehmen...



**Vertrauen entsteht durch  
Architektur - nicht nur durch  
Modelle**

- KI-Erklärbarkeit reicht nicht aus
- Vertrauen entsteht durch nachvollziehbare Systemprozesse
- Governance muss technisch verankert sein



**Auditierbarkeit benötigt eine  
externe Referenzinstanz**

- Interne Logs sind manipulierbar
- organisationsübergreifende Systeme benötigen neutralen Nachweis
- Distributed Ledger ermöglichen unveränderliche Audit-Spuren

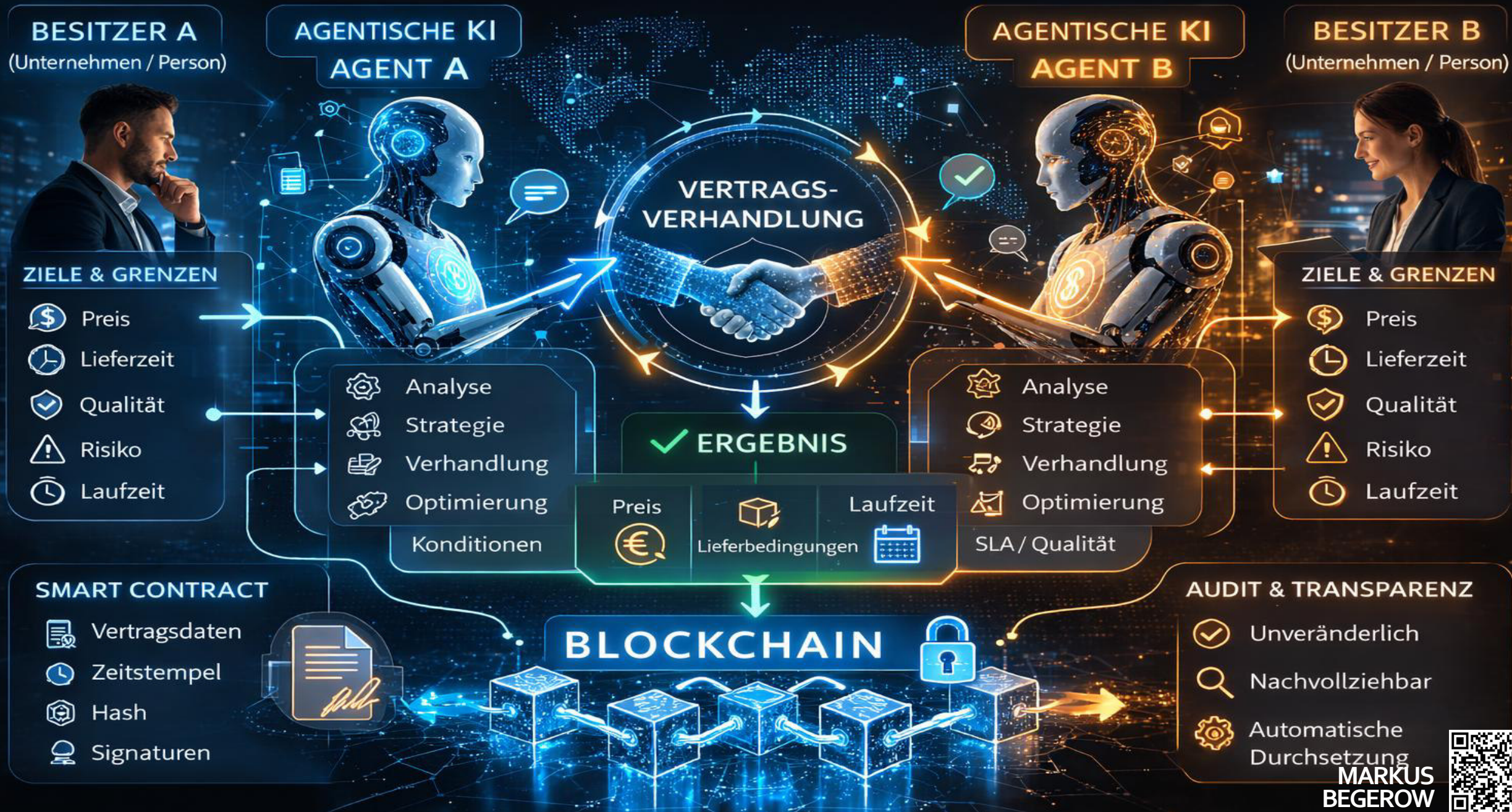


**Die Verantwortung verschiebt  
sich vom Modell zum System**

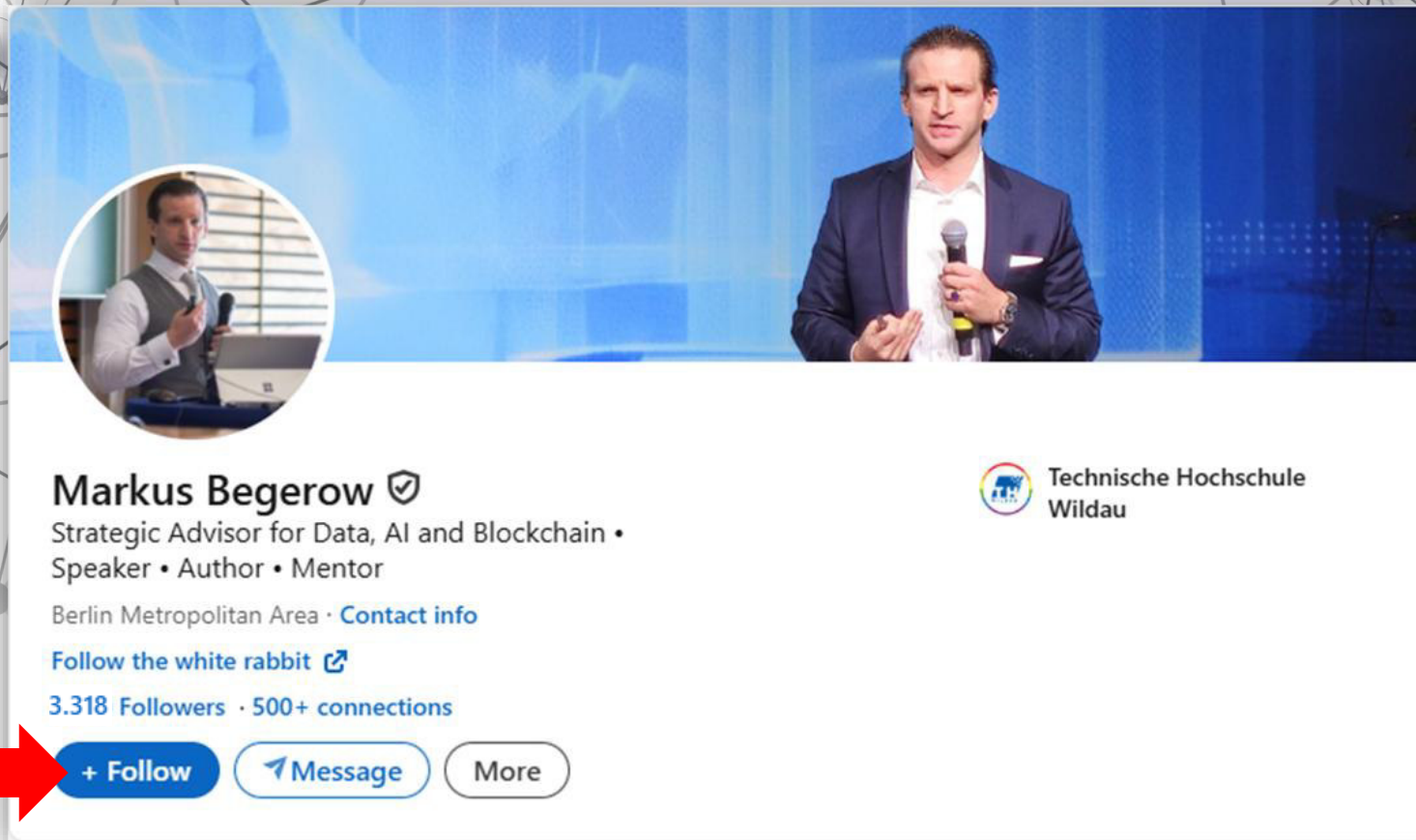
- KI-Verantwortung betrifft Daten, Modelle, Prozesse und Organisation
- Governance wird Teil der Architektur
- Vertrauen wird zur Systemeigenschaft



# Prognosen für 2030-2035







Markus Begerow ✓  
Strategic Advisor for Data, AI and Blockchain •  
Speaker • Author • Mentor  
Berlin Metropolitan Area · [Contact info](#)  
[Follow the white rabbit](#) ↗  
3.318 Followers · 500+ connections

[+ Follow](#) [Message](#) [More](#)

Technische Hochschule Wildau

A red arrow points to the '+ Follow' button.

# THANK YOU!

Slides, Sources, Tools:  
[markus-begerow.de](https://markus-begerow.de)



📱 [@markusbegerow](#)

✉ [mail@markus-begerow.de](mailto:mail@markus-begerow.de)

🌐 [linkedin.com/in/markusbegerow](https://linkedin.com/in/markusbegerow)