

# Demystifying Blockchain

Vortrag IDSt FA VI

Dirk Schuster, FGS Digital  
Stand: Oktober 2023

## Mythos 01 | Blockchains sind unreguliert und werden nur von Kriminellen verwendet

Regulierungsbehörden fangen an, Blockchains zu regulieren, insbesondere im Finanzsektor. Länder wie die USA, die EU und andere haben bereits Gesetze und Vorschriften erlassen oder sind dabei, dies zu tun, um die Verwendung von Blockchain und Kryptowährungen sicherer und transparenter zu machen.

**Fiktion:**



**Realität:**



**Markets in Crypto-Assets  
Regulation (MiCA)**

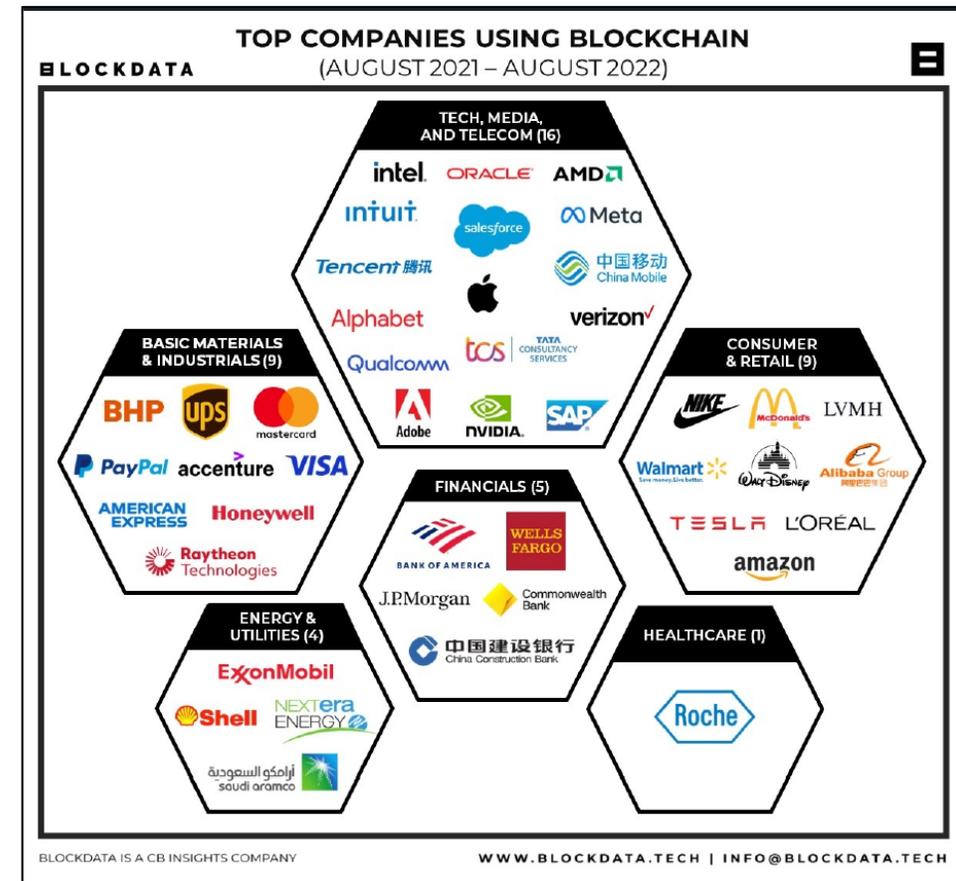
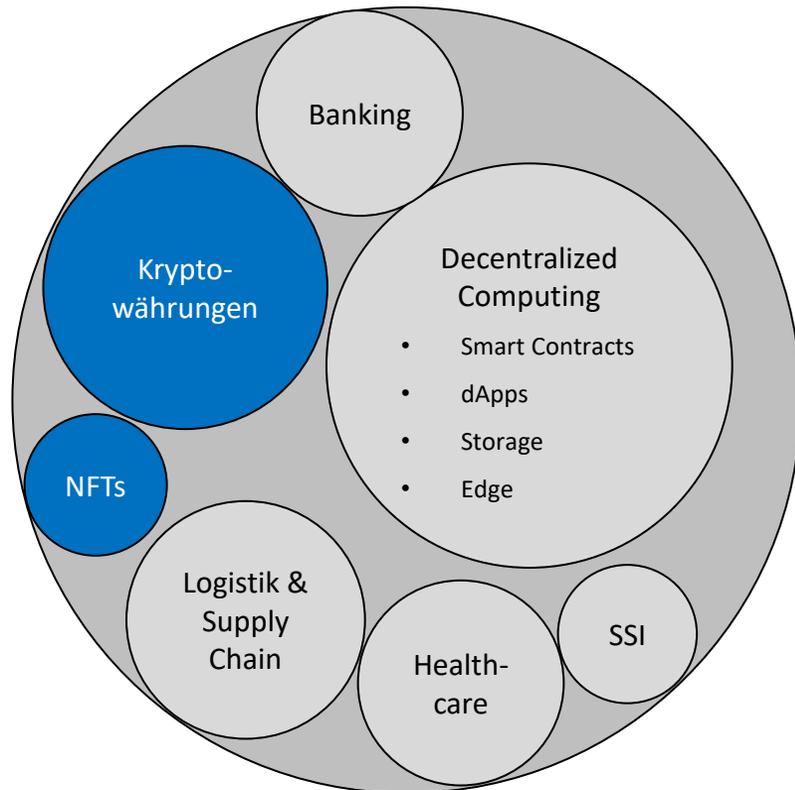
**Transfer of Funds  
Regulation (TFR)**

**DLT pilot regime**

**OTHERS**  
**(investopedia.com)**

## Mythos 02 | Blockchain und Bitcoin sind dasselbe

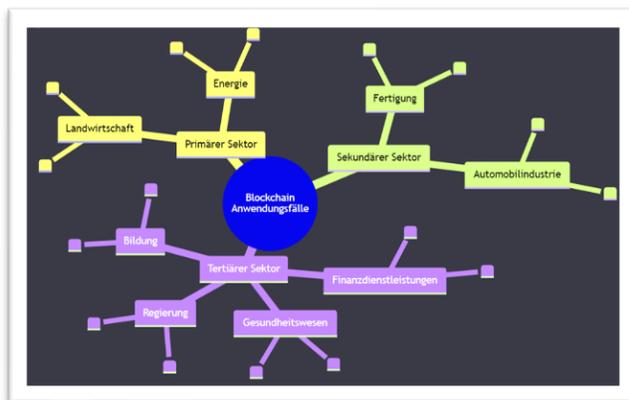
Blockchain und Bitcoin sind nicht dasselbe. Bitcoin ist eine Kryptowährung, die auf der Blockchain-Technologie basiert. Blockchain ist die zugrundeliegende Technologie, die es ermöglicht, verteilte und sichere Transaktionsverzeichnisse zu führen. Bitcoin ist nur eine von vielen Anwendungen der Blockchain.



## Mythos 03 | “Krypto ist nur ein Hype”? Wir fragen einen „Experten“

Blockchain hat real-world Anwendungen, die weit über den Hype hinausgehen.

Sie wird in verschiedenen Branchen wie Supply-Chain-Management, Gesundheitswesen und im Finanzsektor erfolgreich eingesetzt und hat das Potenzial, viele bestehende Systeme zu revolutionieren.



ChatGPT Plugins

**You**  
Welche Anwendungsfälle für Blockchain Technologie gibt es?  
Ordne sie nach den Wirtschaftssektoren und füge auch Branchen ein : Als Wirtschaftssektoren werden in der Wirtschaftswissenschaft zumeist die Urproduktion (sogenannter primärer Sektor), die Industrie und das Gewerbe (sogenannter sekundärer Sektor) und die Dienstleistungen (sogenannter tertiärer Sektor) bezeichnet.  
  
Erzeuge eine Tabelle mit Anwendungsfällen nach Branchen

**ChatGPT**  
Natürlich, ich kann eine Tabelle erstellen, die die Anwendungsfälle der Blockchain-Technologie nach Branchen aufschlüsselt. Hier ist eine übersichtliche Darstellung:

Wirtschaftssektor	Branche	Blockchain-Anwendungsfälle
Primärer Sektor	Landwirtschaft	- Lebensmittelverfolgung - Lieferkettenmanagement
	Energie	- Energiehandel - Smart Grids
Sekundärer Sektor	Fertigung	- Produktionsverfolgung - Qualitätssicherung
	Automobilindustrie	- Fahrzeugwartungshistorie - Ersatzteilauthenzität
Tertiärer Sektor	Finanzdienstleistungen	- Kryptowährungen - Smart Contracts
	Gesundheitswesen	- Patientendatenmanagement - Arzneimittelrückverfolgung
	Bildung	- Zertifizierungsmanagement - Urheberrechtsschutz
	Regierung	- Wählerregistrierung 

## Mythos 04 | Blockchain ist nur für Kryptowährungen geeignet

Kryptowährungen sind ein bekannter Anwendungsfall, aber Blockchain-Technologien werden ebenfalls in Bereichen wie Supply Chain Management, Identitätsverwaltung, E-Voting und vielen weiteren genutzt.

Anwendungsfälle, wo Transparenz, Unveränderbarkeit und Dezentralisierung von höherer Bedeutung sind, bietet Blockchain Vorteile gegenüber anderen Technologien. In diesen Bereichen kann die Blockchain-Technologie Lösungen anbieten, die durch herkömmliche Systeme nicht in gleicher Weise erzielt werden können. Beispiele (mit Links):

Supply Chain	Gaming	Metaverse / Spacial Web	Climate Action	Retail, Payment, Comms	Cloud Computing & Edge Services
 	  	 	  <p><u>Viele weitere (bald)</u></p>	  	  

## Mythos 05 | Auf Blockchains ist man anonym

In öffentlichen Blockchain-Netzwerken sind alle Transaktionen öffentlich einsehbar und könnten theoretisch zurückverfolgt werden. Dadurch ist Transparenz gewährleistet, allerdings kann die Identität der Teilnehmer bis zu einem gewissen Grad durch die Transaktionshistorie enthüllt werden, falls genügend Analyse-Aufwand betrieben wird.

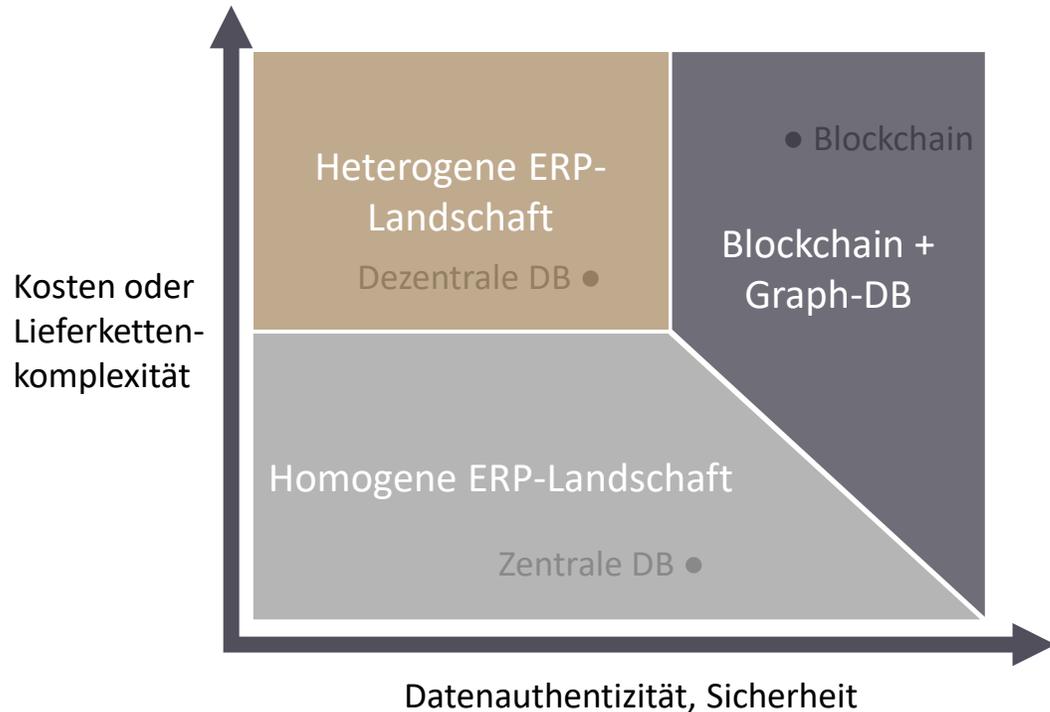
Private Blockchains könnten weitere Datenschutzmaßnahmen bieten, aber sie sind oft transparent für die teilnehmenden Parteien. Neue Technologien und Protokolle, wie z.B. zk-Proofs, erhöhen den Datenschutz auf Blockchain-Netzwerken, ermöglichen aber auch die Verifizierung von Transaktionen ohne Offenlegung sensibler Informationen.



Merke: Auch wenn Blockchain-Netzwerke ein hohes Maß an Pseudonymität bieten können, sind sie nicht zwangsläufig anonym

## Mythos 06 | Blockchains sind dezentrale Datenbanken 1/2

Die Dezentralisierung ist ein Merkmal vieler, aber nicht aller Blockchain-Systeme. Es gibt auch zentralisierte oder semi-dezentrale Blockchain-Modelle, die besonders in Einsatzszenarien in denen hohe Geschwindigkeit und Effizienz wichtiger sind als vollständige Dezentralisierung.



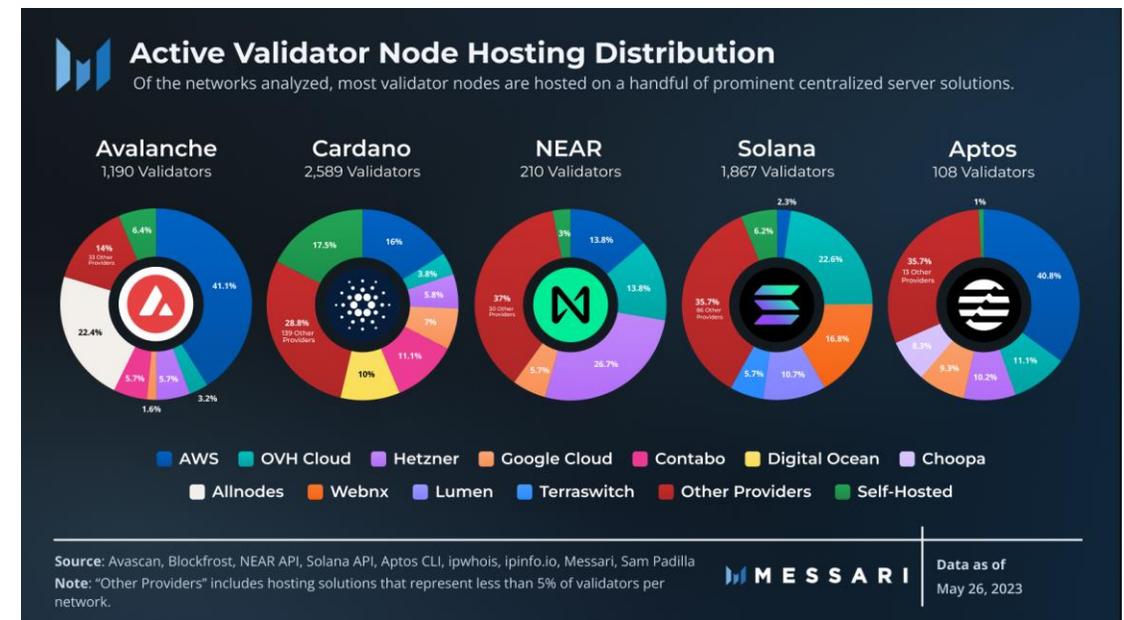
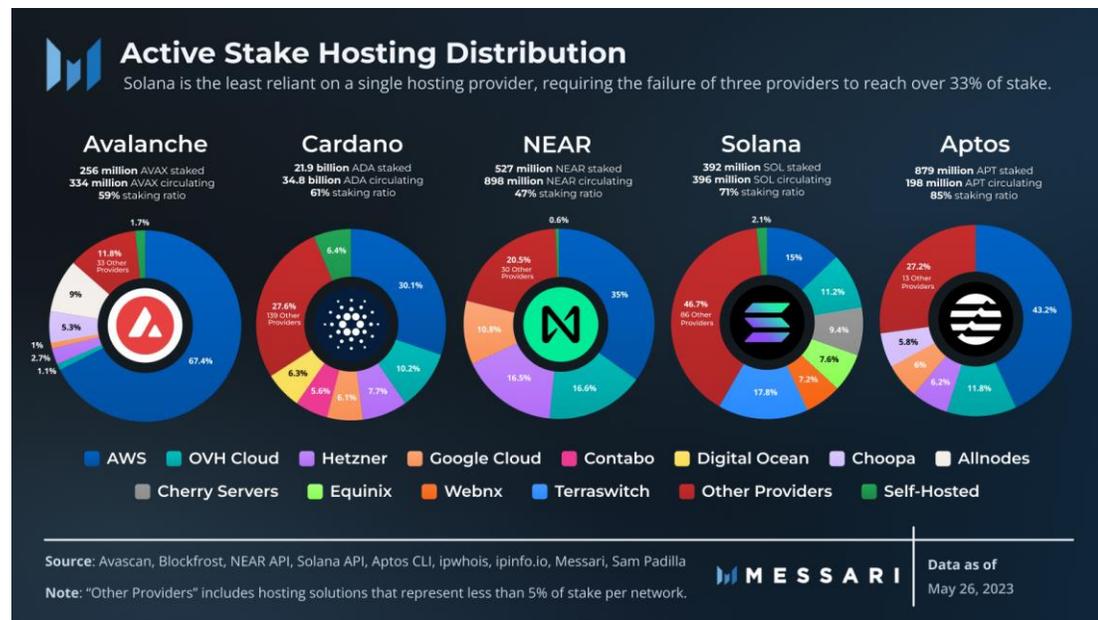
### Core Differences Between Blockchain and Distributed Database

BLOCKCHAIN	DISTRIBUTED DATABASES
<b>Decentralization</b>	
Fully Decentralized	May Have Central Control Points
<b>Transparency</b>	
Shared Transparency	Controlled Access
<b>Specific Use Cases</b>	
Trust and Transparency	Managing Large Data Volumes

Quelle: Finance Strategists

## Mythos 07 | Alle Blockchains sind dezentralisiert 2/2

Die Dezentralisierung ist ein Merkmal vieler, aber nicht aller Blockchain-Systeme. Es gibt auch zentralisierte oder semi-dezentrale-blockchain-Modelle, die besonders in Einsatzszenarien in denen hohe Geschwindigkeit und Effizienz wichtiger sind als vollständige Dezentralisierung. Dennoch: Nicht alle Blockchains sind dezentralisiert – viele Verlassen sich noch immer auf zentrale Cloud-Infrastrukturen von Anbietern wie AWS, Google Cloud und Hetzner.



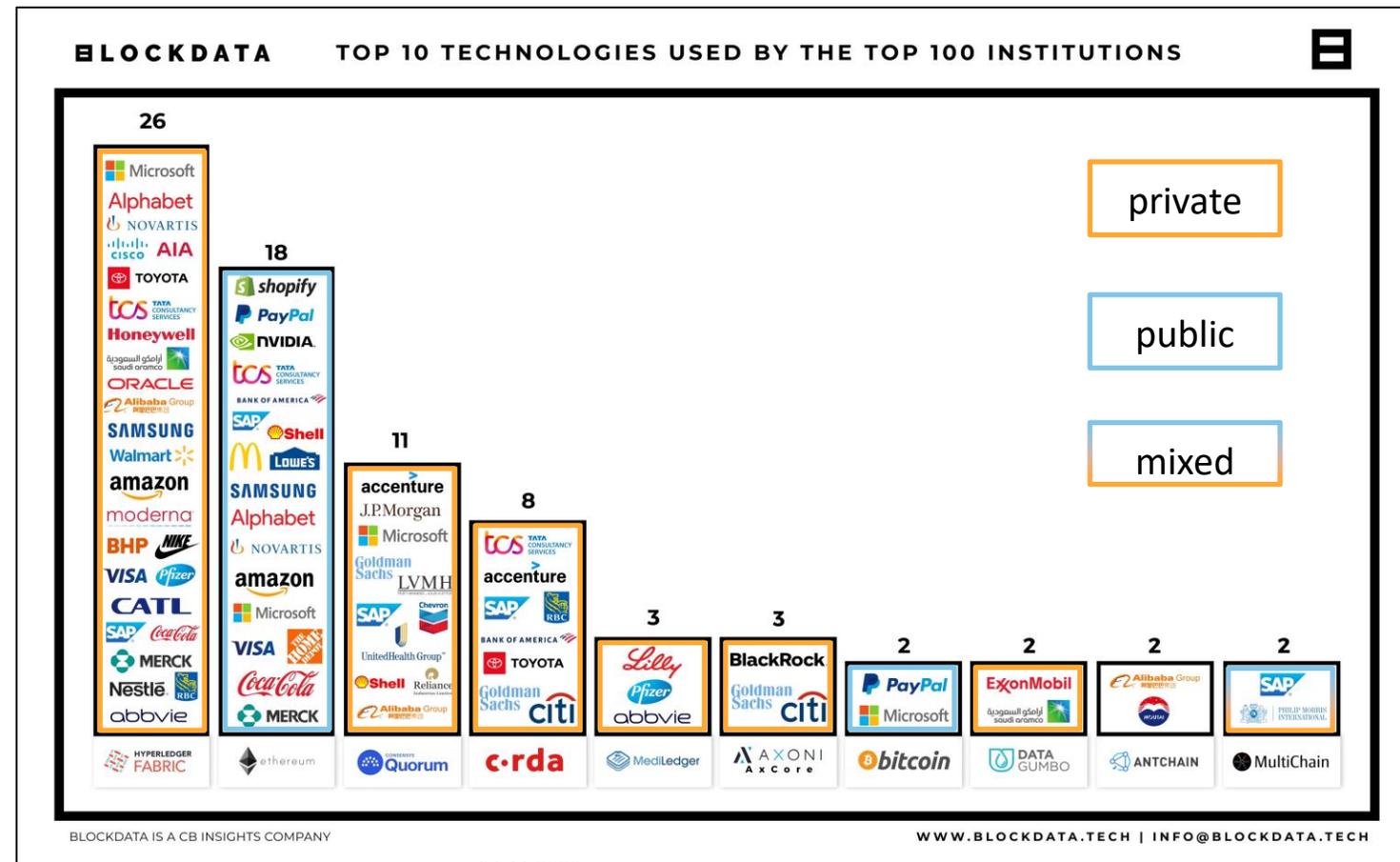
Quelle: [messari.io/report/evaluating-validator-decentralization-geographic-and-infrastructure-distribution-in-proof-of-stake-networks](https://messari.io/report/evaluating-validator-decentralization-geographic-and-infrastructure-distribution-in-proof-of-stake-networks)

## Mythos 08 | Alle Blockchains sind öffentlich einsehbar

Nicht alle Blockchains sind öffentlich. Es gibt öffentliche, private und konsortiale Blockchains. Öffentliche Blockchains sind für jeden zugänglich, während private und konsortiale Blockchains beschränkten Zugang haben und in der Regel von Unternehmen für interne Prozesse verwendet werden.

Sowohl Public als auch Private Blockchains werden von Konzernen genutzt. Je nach Anwendungsfall kann beides sinnvoll sein.

Für steuerliche, unternehmensübergreifende Zwecke empfiehlt das IDSt grundsätzlich private Blockchainlösungen.



## Mythos 09 | Blockchains verbrauchen unglaublich viel Strom

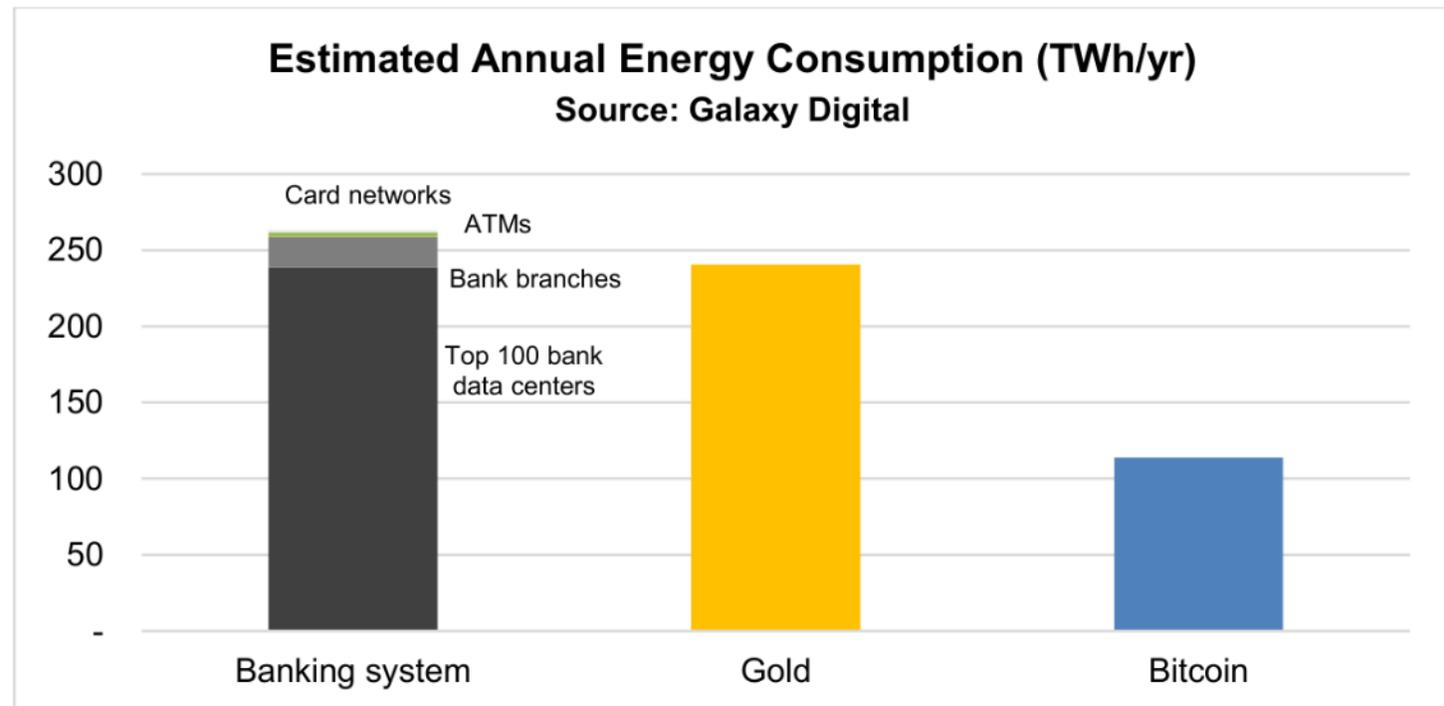
Besonders Proof-of-Work-Blockchain-Netzwerke können sehr energieintensiv sein. Es gibt allerdings alternative Konsensmechanismen, wie Proof-of-Stake, die wesentlich energieeffizienter sind und zur Reduktion des Energiebedarfs beitragen können. Proof-of-Authority und Proof-of-Stake verbrauchen um Größenordnungen weniger Strom als PoW.

Bereits in 2021 hätte ein versuchter 51%-Angriff zwischen 8 GW und 16 GW Rechenleistung benötigt (fast 3x das größte Atomkraftwerk Europas „Saporischja“ in der Ukraine)

Im November 2022 (40 Cent je kWh) hätte der Betrieb des gesamten Bitcoin Netzwerks in Deutschland je Sekunde 1,5Mio Euro gekostet – etwa 133 Mio Euro pro Tag ([Quelle](#)). Das beinhaltet nicht die Kosten für Hardware und Immobilien.

Ein Angriff auf Bitcoin ist technisch kaum möglich und mit enormem finanziellen Aufwand verbunden.

>>It's not a bug, it's a feature!<<

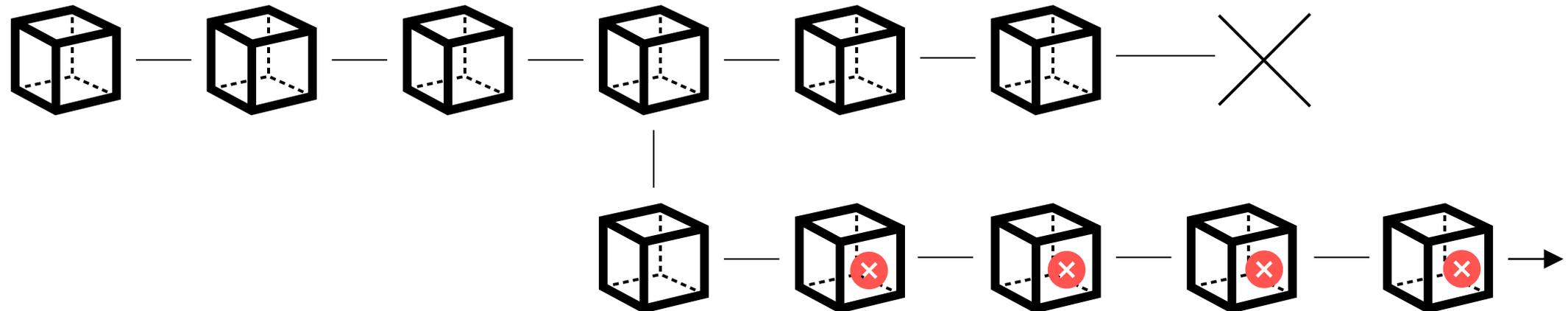


Galaxy Digital > Deutscher Bundestag, WD 5 - 3000 - 043/22

## Mythos 10 | Blockchain ist unveränderlich und unangreifbar

Obwohl die Blockchain-Technologie sicherer als viele traditionelle Systeme ist, ist sie nicht vollständig unhackbar. Es gibt Möglichkeiten, eine Blockchain zu kompromittieren, aber die Anforderungen dafür sind extrem hoch (teuer) und in der Regel nicht praktikabel.

Um eine Blockchain zu hacken, muss man entweder den Konsensmechanismus verwenden bzw. überwinden (>51% Angriff) oder man muss Fehler in der Programmierung der Blockchain oder eines Smart Contracts finden und ausnutzen.

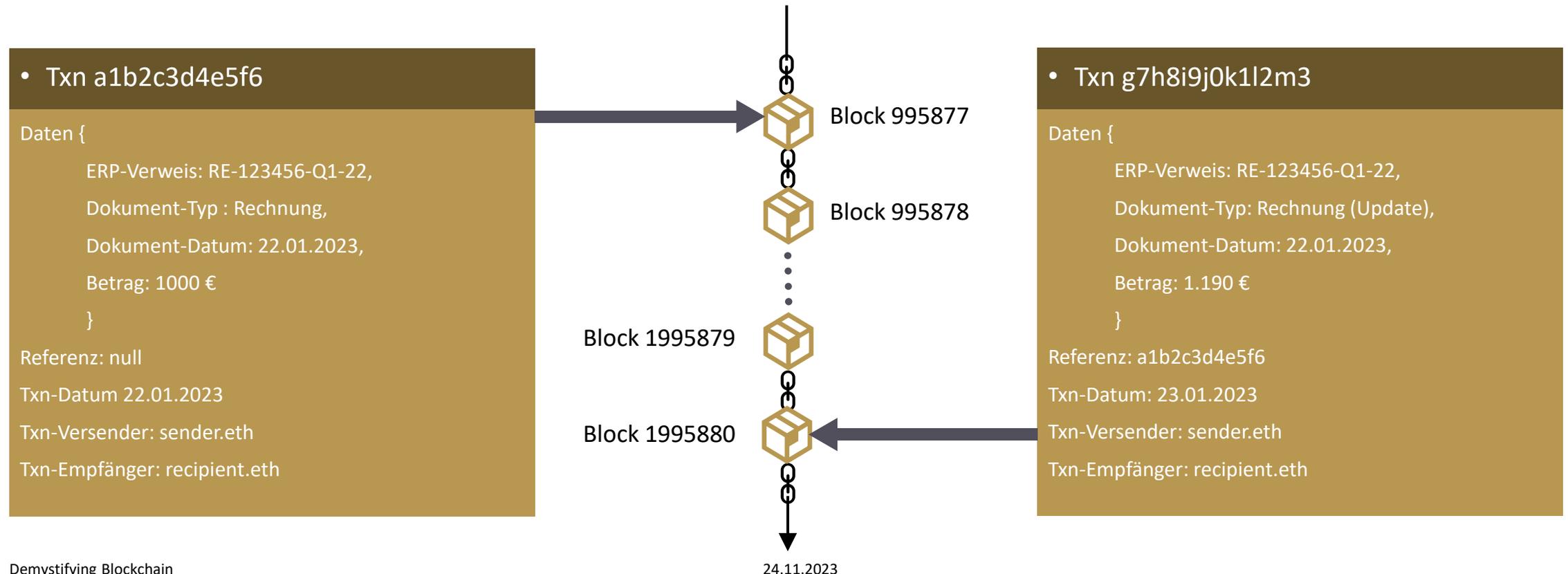


Merke: Keine Technologie ist unhackbar!

## Mythos 11 | Auf Blockchains können Daten geschwärzt werden

In einer Blockchain ist es nicht möglich, einmal eingetragene Daten zu löschen oder zu schwärzen.

Sollte eine Korrektur notwendig sein, muss eine neue Transaktion durchgeführt werden, welche die Korrektur beinhaltet; die ursprüngliche Transaktion bleibt jedoch sichtbar. Die alte Transaktion wird dabei nicht als ungültig/korrigiert markiert.



## Mythos 12 | Blockchain garantiert Korrektheit von Daten

Die Blockchain speichert Informationen in einer dezentralisierten Form, aber das garantiert nicht die Wahrheit dieser Informationen.

Grundsatz: Garbage in = garbage out

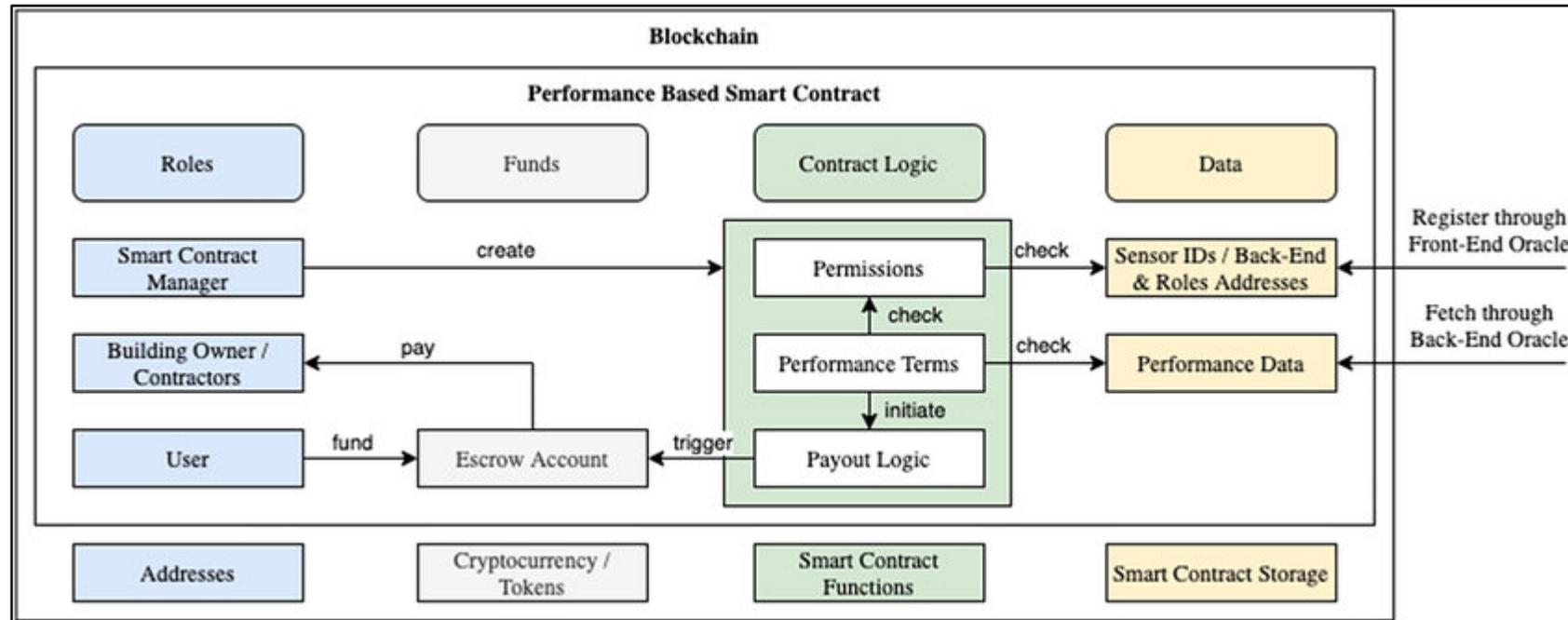
Ablauf der Datenspeicherung:

1. Transaktionserstellung
2. Transaktionsvalidierung (Authentifizierung der Signatur und Prüfung des Saldo vor der „Buchung“ der Transaktion)
3. Transaktionspool (beinhaltet alle validierten Txn)
4. Blockerstellung (beinhaltet die jeweils ältesten, validierten Txn)
5. Blockvalidierung (
6. Hinzufügen zur Blockchain
7. Aktualisierung der Ledger
8. Transaktionsabschluss

Merke: Daten können nur dann als wahr betrachtet werden, wenn sie aus einer vertrauenswürdigen Quelle stammen und **entsprechend verifiziert wurden.**

## Mythos 13 | Smart Contracts sind immer intelligent und zuverlässig

Der Begriff "Smart Contract" kann irreführend sein. Smart Contracts sind selbstausführende Programme, aber sie sind nur so "intelligent" oder "zuverlässig", wie sie programmiert wurden. Fehler im Code können zu unerwarteten Ergebnissen oder Sicherheitslücken führen.



© Jens Hunhevicz

## Mythos 14 | Blockchains sind Datenbanken, in die ich alle ERP-Daten schreiben kann.

Grundsätzlich korrekt. Zwar teilen sich Blockchains einige Eigenschaften mit Datenbanken, wie die Speicherung von Daten, aber sie sind aufgrund ihrer Struktur und Zweckbestimmung nicht für jede Art von Daten oder Transaktionsvolumen geeignet. Für die Abwicklung kleiner und häufiger Transaktionen eignen sich traditionelle Datenbanken oft besser. Blockchains sind eine Art Transaktionsbuch, das Transaktionen über eine Vielzahl von Computern redundant aufzeichnet.

Blockchain ist im Vergleich zu herkömmlichen Datenbanken ineffizient für die Massendatenspeicherung. Sie ist besser geeignet für Anwendungen, bei denen Sicherheit und Transparenz von höchster Bedeutung sind, wie z.B. im Finanzsektor oder in der Lieferkette.

### Ethereum Transaktionskosten vom 13.11.2023



Last Refreshed: Mon, 13 Nov 2023 16:33:16 UTC

Featured Actions

Action	Low	Average	High
🔍 Swap	\$112.83	\$113.59	\$118.85
🔍 NFT Sale	\$190.69	\$191.96	\$200.86
🔍 Bridging	\$36.29	\$36.53	\$38.22
🔍 Borrowing	\$95.72	\$96.36	\$100.83

## Blockchain Mythen zusammengefasst

Blockchain ist eine leistungsstarke Technologie mit vielen potenziellen Anwendungen, aber es ist wichtig zu verstehen, was sie ist und was nicht.

- Blockchain und Bitcoin sind nicht dasselbe; Bitcoin ist eine Kryptowährung, die auf der Blockchain-Technologie basiert.
- Nicht alle Blockchains sind öffentlich; es gibt auch private oder konsortiale Blockchains.
- Nicht jede Blockchain ist dezentralisiert. Es gibt Blockchains, bei denen zentrale Akteure maßgebliche Entscheidungen ohne Zustimmung aller Netzwerkteilnehmer treffen können.
- Die Erstellung und Wartung einer Blockchain ist nicht kostenlos; es fallen Strom- und Hardwarekosten an.
- Der Stromverbrauch ist hauptsächlich ein Kritikpunkt bei Proof-of-Work-Blockchains wie Bitcoin, aber es gibt auch umweltfreundlichere Alternativen wie Proof-of-Stake (PoS) oder Proof-of-Authority (PoA).
- Während die Blockchain-Technologie sicherer als traditionelle Systeme sein kann, ist sie nicht vollständig unhackbar.
- Die Blockchain speichert Informationen, aber die Wahrheit dieser Informationen muss verifiziert werden.
- Blockchain ist ineffizient als eine reine Datenbank für Massendatenspeicherung, sie ist besser geeignet für sicherheitskritische Anwendungen, bei denen die Authentizität von Informationen oder Berechtigungen im Vordergrund steht.
- Blockchain hat real-world Anwendungen, insbesondere in Bereichen wie Supply-Chain-Management und Gesundheitswesen.
- Blockchains werden fast ausschließlich für legale Transaktionen verwendet und dienen z.B. Geldwäschezwecken seltener als Bargeld und ähnliche, physisch austauschbare Werte. Auf der Blockchain ist man nicht anonym, sondern pseudonym.

**Vielen Dank!**

Dirk Schuster  
FGS Digital GmbH | Tax Technology & Innovation  
Senior Associate  
dirk.schuster@fgs.de  
Tel: +49 30 210020-258

