Table of Contents

# Kryptowerte: der Apparat und seine Verteilung

## Dach-Recherchеband des Clusters KRYPTOWERTE-VOLLWERK — Forschungsstand 2024–2026 in neun Achsen

**Thomas Schüller · Syntagma Forschung · Wien** · ORCID 0009-0003-9799-6747 Stand: 20. Oktober 2026 · Schwelle B · CC BY 4.0

---

## Kurzbefund

Das Feld der Kryptowerte lässt sich in neun Disziplinachsen vollständig aufarbeiten, und in jeder einzelnen zeigt sich dasselbe Muster: Die Verfügungsmacht liegt bei wenigen, die Kosten und Risiken tragen viele. Die Dezentralisierung ist auf der Protokollebene real, auf jeder tieferen Ebene aber stark konzentriert. Dieser Dachband bündelt den Forschungsstand 2024–2026 als Fundament für die Einzelbände des Clusters und macht die Risiko-Verfügungs-Asymmetrie (ρ/δ) zum Leitinstrument der Auswertung.

Drei Kennzahlen fassen die Lage: Für 51 Prozent der Bitcoin-Hashrate genügen drei Mining-Pools. Drei Hersteller liefern über 99 Prozent der Mining-Hardware (Bitmain ~82 %, MicroBT ~15 %, Canaan ~2 %). Und laut der Bank für Internationalen Zahlungsausgleich verloren 73 bis 81 Prozent der Kleinanleger mit ihren Erstinvestitionen in Bitcoin Geld, während große Halter in den Markteinbrüchen verkauften.

---

## 1. Die Leitmatrix: Verfügung gegen Risiko

Der eigenständige Beitrag dieses Clusters ist nicht die Nacherzählung der Technik, sondern ihre Lesart entlang einer einzigen Frage: Wer verfügt, und wer trägt? Die folgende Matrix ordnet jeden Stakeholder nach Verfügungsmacht (δ) und getragenem Risiko (ρ).

| Stakeholder | Verfügungsmacht (δ) | Getragenes Risiko / Kosten (ρ) | Evidenz |
|---|---|---|---|
| Kleinanleger | gering (Preisnehmer, Verwahrung meist bei Börse) | Kursverluste, Börsenpleiten, Betrug, Hacks | BIS 2023; FTX 2022 |
| Whales / frühe Halter | hoch (Marktmacht, Timing) | gering — verkaufen in Schocks zuerst | BIS Bulletin 69; Makarov/Schoar 2021 |
| Miner / Pool-Betreiber | hoch (Transaktionsauswa | Kapital-/Hardware-Risiko, Halving- | b10c 2025 |

| Stakeholder | Verfügungsmacht (δ) | Getragenes Risiko / Kosten (ρ) | Evidenz |
|---|---|---|---|
| | hl) | Schocks | |
| ASIC-Hersteller / Foundries | sehr hoch (Lieferengpass, Firmware) | Geopolitik (Taiwan, Zölle) | Cambridge 2025 |
| Validatoren / Liquid-Staking | hoch (Konsensgewicht bei PoS) | Slashing, Regulierung | Lido 2025/26 |
| Zentrale Börsen (CEX) | sehr hoch (Verwahrung, Listing) | Hack/Insolvenz trifft meist die Kunden | FTX 2022; Bybit 2025 |
| Entwickler / Foundations | hoch (Code, Upgrades, Governance) | strafrechtliche Haftung (Fall Storm) | SDNY 2025 |
| Stablecoin-Emittenten | sehr hoch (Seigniorage, Freeze-Funktion) | Run-Risiko auf die Halter abgewälzt | BIS 2025/26; GENIUS Act |
| Staat / Zentralbank | Regulierung, Sanktionen, Steuer | Verlust monetärer Souveränität | IWF/El Salvador |
| Netzanrainer | kaum | Strompreise, Lärm, Wasser | de Vries 2023; Cambridge 2025 |
| Künftige Generationen | keine | $CO_2$, Elektroschrott, Quanten-Altlasten | de Vries/Stoll 2021 |
| Globaler Süden | gering | Krypto-Dollarisierung, Schock-Verluste | BIS 2023 |

Die Asymmetrie ist kein Zufall, sondern folgt aus der Architektur: Skaleneffekte bei Hashrate, Stake und Liquidität sowie Netzwerkeffekte bei Börsen und Stablecoins wirken alle zentralisierend, und die externen Kosten (Emissionen, Netzlast, Elektroschrott) werden nicht im Preis abgebildet.

---

## 2. Die neun Achsen im Überblick

### 2.1 Technik und Protokolle

Proof of Work (Bitcoin, SHA-256d, Halving auf 3,125 BTC im April 2024, Hashrate ~850–1.000 EH/s) steht Proof of Stake (Ethereum seit dem Merge 2022, 32 ETH je Validator, Slashing) gegenüber, dazu DPoS, Proof of Authority, Solanas Proof of History und die BFT-Familie (PBFT, Tendermint). Nakamoto-Konsens liefert probabilistische Finalität über die längste Kette; klassischer BFT-Konsens liefert sofortige Finalität bei bekannter Validatormenge. 51-Prozent-Angriffe sind real (Bitcoin Gold 2018/2020, Ethereum Classic viermal 2019/2020), meist mit

gemieteter Hashrate. Skalierung läuft über Layer-2 (Optimistic- vs. ZK-Rollups), Lightning und Sharding; die verwundbarste Stelle sind Bridges (Ronin ~625 Mio. USD, Wormhole ~320 Mio. USD).

### 2.2 Kryptographie

Signaturen über ECDSA/secp256k1, seit Taproot auch Schnorr; Hashfunktionen SHA-256 und Keccak; Zero-Knowledge-Verfahren (zk-SNARKs mit Trusted Setup, transparente zk-STARKs, Bulletproofs). Privacy-Primitive: Monero (Ring-Signaturen, RingCT, Stealth-Adressen), Zcash (zk-SNARKs, shielded/transparent). Die Post-Quanten-Bedrohung ist konkret: Shors Algorithmus bricht die elliptische Kurve, sobald ein öffentlicher Schlüssel offenliegt — nach einer Schätzung sind ~6,7 Mio. BTC exponiert. Bitcoins Migrationspfad (BIP-360) ist seit September 2024 in Arbeit; das erste plausible Zeitfenster für relevante Quantencomputer wird mit 2027–2033 angegeben (mit großen Fehlerbalken, als Prognose zu kennzeichnen).

### 2.3 Hardware

Die Mining-Hardware entwickelte sich von CPU über GPU und FPGA zum ASIC. Der Markt ist oligopolistisch: über 99 Prozent von drei Herstellern, alle fabless (Fertigung bei TSMC und Samsung). Damit hängt die Sicherheit Bitcoins geopolitisch an Taiwan und konkurriert mit KI-Chips um Fertigungskapazität. Hardware-Wallets (Ledger, Trezor) nutzen Secure Elements; der Bybit-Hack 2025 zeigte, dass die Schwachstelle in der Signier-Orchestrierung lag, nicht in der Kryptographie.

### 2.4 Strom, Energie, Ressourcen, Umwelt

Der Cambridge-Index schätzt den Bitcoin-Stromverbrauch auf ~138 TWh pro Jahr (~0,5 % des Weltstroms), mit methodischer Spanne von 74 bis 242 TWh; Digiconomist nennt ~204 TWh. Die Emissionen liegen bei ~39,8 Mt $CO_2e$. Der Strommix ist zu ~52 % „nachhaltig“ (erneuerbar plus Kernkraft), zu ~38 % Erdgas. Hinzu kommen Wasserverbrauch (~2.237 GL 2023 nach de Vries) und Elektroschrott (~30,7 kt/Jahr). Ethereums Merge senkte den Verbrauch um ~99,99 Prozent — die Konsenswahl ist zugleich eine Umweltentscheidung. Ökologisch ist PoW ein Allmende- und Externalitätsproblem: Der Verbrauch ist an den Preis gekoppelt, die Kosten tragen Atmosphäre und Wasserressourcen.

### 2.5 Volkswirtschaft, Makro und Mikro

Geldtheoretisch ist Bitcoin ein digitaler Metallismus (fixe Menge, kein Lender of Last Resort), nahe Hayeks Entnationalisierung des Geldes; Chartalismus und MMT verorten den Geldwert dagegen in der Steuerpflicht. Fiat gegen Krypto unterscheidet sich in jeder Dimension (Recheneinheit, Elastizität, Einlagensicherung, Seigniorage). Makroökonomisch drohen Krypto-Dollarisierung (~99,5 % der Stablecoins lauten auf US-Dollar) und Souveränitätsverlust; die BIS bescheinigt Stablecoins 2026 Schwächen bei „singleness, elasticity, integrity“. El Salvador nahm sein Bitcoin-Gesetz am 29.01.2025 auf IWF-Druck zurück. Mikroökonomisch: 73–81 Prozent Kleinanlegerverluste (BIS), über 70 Prozent Wash Trading an unregulierten Börsen (Cong et al. 2023), Tether-getriebene Preisstützung 2017 (Griffin/Shams 2020), extreme Bestandskonzentration (Top 0,1 % der Miner ~50 % Kapazität).

### 2.6 Coins und Systeme

Bitcoin als Wertspeicher, Ethereum als Smart-Contract-Basis, dazu Layer-1-Konkurrenten (Solana, Cardano, Avalanche, Polkadot, BNB), Stablecoins (Markt ~308–322 Mrd. USD, USDT ~59 %, USDC ~23 %), Privacy-Coins, Memecoins, Utility-/Security-/Governance-Token. DeFi (Uniswap, Aave, Lido) verlagert Finanzfunktionen in Smart Contracts; NFT erlebte Boom und Bust 2021/22; DAOs sind formal Mitgliederherrschaft, faktisch Token-Plutokratie. Die ICO-Welle 2017/18 (~12 Mrd. USD) brachte nach Satis ~78–81 Prozent Betrug nach Projektzahl; nur 44,2 Prozent der Startups existierten 120 Tage nach dem ICO noch.

### 2.7 Anonymität gegen Transparenz

Bitcoin und Ethereum sind pseudonym, nicht anonym; Clustering-Heuristiken und KYC-Punkte ermöglichen De-Anonymisierung. Blockchain-Forensik (Chainalysis, TRM) attribuiert illegale Ströme — weiterhin unter 1 Prozent des Volumens, davon ~84 Prozent in Stablecoins. Privacy-Coins (Monero, Zcash) stehen unter regulatorischem Druck: Die EU-AMLR verbietet ab 2027 anonymitätsfördernde Coins bei Dienstleistern; Binance, Kraken und OKX delisteten Monero 2024. Der Fall Tornado Cash markiert die Bruchlinie: Code selbst ist nicht sanktionierbar (Van Loon v. Treasury, 2024; Delisting 2025), Entwickler haften aber strafrechtlich (Storm, 2025).

### 2.8 Zentral gegen dezentral

Mining-Pools sind konzentriert (Foundry und AntPool zusammen 60–70 %); beim Ethereum-Stake hält Lido ~21–25 Prozent. Zentrale Börsen sind die wiedererrichtete Mitte: FTX kollabierte 2022 (Bankman-Fried, 25 Jahre Haft), Bybit erlitt 2025 den größten Kryptodiebstahl der Geschichte. „Dezentralisierungstheater“ meint Admin-Keys, zentrale Sequencer, Foundation-Treasuries und konzentrierte Token-Governance.

### 2.9 Recht und Regulierung

MiCA (EU-Verordnung 2023/1114) gilt seit dem 1. Juli 2026 vollständig, ohne Übergangsfrist; ergänzend DORA und die Transfer-of-Funds-Verordnung (Travel Rule). Die USA vollzogen 2025 eine Wende: GENIUS Act (18.07.2025) legalisiert Stablecoins mit 1:1-Reserve und Halter-Vorrang in der Insolvenz; das SEC-Verfahren gegen Coinbase wurde eingestellt, Tornado Cash entlistet. China verbietet Mining und Handel seit September 2021. In Deutschland bleiben private Veräußerungsgewinne nach einem Jahr steuerfrei; ab 2026 greift die DAC8-Meldepflicht.

---

## 3. Transdisziplinäre Querverbindungen

Die Konvergenz der Achsen ist der eigentliche Ertrag. Die Konsenswahl ist zugleich Umweltentscheidung (Achse 1 ↔ 4). Die Unveränderlichkeit von Smart Contracts setzt die Sanktionsgewalt außer Kraft und zwingt das Recht auf Entwicklerhaftung und Gatekeeper aus (1 ↔ 9). Bitcoins Sicherheit hängt an TSMC und der Zollpolitik (3 ↔ 5). Die BIS-Daten widerlegen das Demokratisierungs-Narrativ empirisch (5 ↔ 8). Die Quantenmigration ist ein Verteilungsproblem zwischen den Generationen (2 ↔ Ethik). Und GENIUS Act wie MiCA

regulieren Emittenten im Norden, während die Dollarisierungsfolgen der globale Süden trägt (9 ↔ Stakeholder).

---

## 4. Forschungslücken für die Einzelbände

Fünf Lücken, die der Cluster füllen sollte, mit Literatur-Sondierung als offen markiert:

- **O-1 — Neutrale Ökobilanz.** Ein methodisch sauberer Vergleich von PoW mit Gold und Bankensystem über eine gemeinsame funktionale Einheit fehlt; vorhandene Vergleiche stammen von Interessengruppen. [offen → Band Ressourcen/Ökologie]
- **O-2 — Kleinanlegerverluste in der EU nach MiCA.** Mikrodaten zur Verlustverteilung unter dem neuen Rahmen fehlen. [offen → Band Finanzökonomik]
- **O-3 — Stablecoins und Geldsouveränität.** Die Wirkung auf Bankeinlagen und Kapitalverkehrskontrollen in Schwellenländern ist empirisch nicht abschließend untersucht. [offen → Band Finanzökonomik/Recht]
- **O-4 — Governance-Konzentration.** Konzentrationsmaße bei DAOs und Layer-2 fehlen systematisch. [offen → Band Zentral/Dezentral]
- **O-5 — Verteilungsfolgen der Quantenmigration.** Wer trägt das Risiko nicht migrierter Schlüssel, wer gewinnt durch frühe Quanten-Hardware? [offen → Band Kryptographie/Ethik]

---

## 5. Methodische Vorbehalte

Der Forschungsstand ist mit Bandbreiten statt Punktwerten zu führen: Strom 138 TWh (Spanne 74–242) gegen Digiconomist ~204 TWh; illegales Volumen Chainalysis 154 Mrd. gegen TRM 158 Mrd. USD. Interessengebundene Quellen (Chainalysis, TRM, Lido-Selbstauskünfte, CCRI im Auftrag von ConsenSys, Cambridge-Befragung mit 48 % Abdeckung und US-Übergewicht) sind als solche zu kennzeichnen. Makarov/Schoar ist ein nicht begutachtetes Working Paper; die Zahl der quantengefährdeten BTC stammt von einem Anbieter von Quantensicherheit. Prognosen (Quantenfenster 2027–2033, Stablecoin-Projektionen bis 2030, Wirkung des noch nicht voll in Kraft getretenen GENIUS Act) sind ausdrücklich als Prognosen zu markieren. Datenstand Oktober 2026; Markt und US-Regulierung ändern sich schnell. Vor Veröffentlichung sind Pool-Anteile, Stablecoin-Marktdaten, die Zahl der zugelassenen CASPs und die Bridge-Hack-Summen an der Primärquelle zu verifizieren.

---

## 6. Clusterstruktur (slug-primär)

Anker-Werke bereits erstellt: `anleitung-und-risiko` (Hosp-Werkkritik, Zeitdokument), `vertrauen-ohne-mitte` (Gesamtabhandlung), `geld-die-erste-mitte` (A01 Geldtheorie), `die-abgeschaffte-mitte` (A02 Kryptographie-Vorgeschichte). Geplante Einzelbände: Konsens/Protokoll-Informatik, Finanzökonomik/Markt, Recht/Regulierung, Ressourcen/Ökologie, Zentral/Dezentral, Anonymität/Transparenz, Ethik/ρδ-Formalisierung,

Ausblick/Governance. Alle Nummern provisorisch; final gegen `forsch-reg` zu fixieren (Frontier Stand 2026-10-20 bei PROV ~0470).

---

## Quellen

Primär: EUR-Lex (VO 2023/1114 MiCA; VO 2022/2554 DORA; VO 2023/1113 Transfer-of-Funds); ESMA-Statements 2026; GENIUS Act (Public Law 119-27, 18.07.2025); IWF Country Reports El Salvador 25/58 und 25/68; BIS Bulletin 69 (Cornelli et al. 2023) und BIS-Jahresbericht 2025/2026; FATF Targeted Update 2026; Nakamoto 2008; Haber/Stornetta 1991; BIP-360. Studien: Cong/Li/Tang/Yang, *Crypto Wash Trading*, Management Science 69(11) 2023; Griffin/Shams, *Is Bitcoin Really Untethered?*, Journal of Finance 75(4) 2020; Makarov/Schoar, NBER WP 29396 (2021); de Vries, *Bitcoin's growing water footprint*, Cell Reports Sustainability 1(1) 2023; de Vries/Stoll 2021; Benedetti/Kostovetsky, *Digital Tulips?*, Journal of Corporate Finance 66 (2021). Branchen-/Messquellen (interessengebunden, gekennzeichnet): Cambridge CBECI und Digital Mining Industry Report 2025; Digiconomist; Chainalysis/TRM Crime Reports 2026; Lido-Berichte; CCRI 2022.

*Alle Forschung: Thomas Schüller · Syntagma Forschung · Wien · ORCID 0009-0003-9799-6747 · CC BY 4.0. Gewonnen aus einer strukturierten Extended-Research-Auswertung (Stand 2024–2026); interessengebundene Quellen gekennzeichnet, Prognosen als solche markiert.*