Lastannahmen

Ethereum als fundamentale digitale Infrastruktur

Eine Prüfung des gegenwärtigen und des angestrebten Zustands

Henrik Asmus

Garbsen, Juli 2026

Inhalt

Vorwort

Das Jahr 2025 zählt zu den ereignisreichsten, die der Kryptomarkt bislang erlebt hat. Auf eine sommerliche Hochphase, in der selbst der amerikanische Präsident Donald Trump das Thema öffentlich aufgriff und positiv besetzte, folgte der 10. Oktober, der größte Liquidationstag der bisherigen Geschichte. An ihm wurden über neunzehn Milliarden Dollar an gehebelten Positionen liquidiert, und mehr als anderthalb Millionen Konten verloren ihre Einsätze. Was darauf einsetzte, waren zermürbende Monate, deren Nachwirkungen bis in das Jahr 2026 reichen. Ich verfolge den Markt seit etwa vier Jahren, und nach dem Abitur hatte ich freilich zum ersten Mal die Zeit, mich einem Gegenstand ausführlich zu widmen, an dem ich eigene Recherche betreiben, mein Systemdenken schulen und mein Urteil an einem tatsächlich anspruchsvollen Objekt schärfen konnte.

Gerade dieses Jahr hat mir eine Frage aufgedrängt, die ich als Investor sonst leicht übergehe: Worauf stützt sich das alles eigentlich? Es bewegen sich enorme Summen, es kursieren große Erzählungen über Zahlung, Identität und die Verwaltung des eigenen Vermögens ohne Mittelsmann, und dennoch bleibt seltsam unklar, worum es im Kern geht. Ginge es am Ende allein um Zahlungsverkehr und die Autonomie über die eigenen Schlüssel, ließen sich die Bewertungen kaum erklären, die viele der Netzwerke tragen. Und würde ihr Wert sich allein aus Knappheit speisen, wie beim Gold, wäre das Neue daran gering. Daraus ergibt sich die Frage, die die Arbeit antreibt: Was ermöglicht ein solches kryptographisches System über dezentralen Zahlungsverkehr hinaus, und muss es überhaupt darüber hinausgehen?

Um diese Frage an etwas Konkretem zu prüfen, brauchte ich ein System, das mir als Repräsentant dient und an dem sie sich beantworten lässt. Ich habe mich für Ethereum entschieden. Es ist die erste Layer 1 mit nativer, allgemeiner Programmierbarkeit für Smart Contracts und hält nach Bitcoin die zweitgrößte Marktkapitalisierung. Es verzeichnet nach Electric Capital 2025 die größte akti-

ve Entwicklerbasis[1] und nach gebundenem Wert das größte Anwendungsökosystem. Es bildet die größte Settlement-Schicht für institutionelle und dezentrale Finanzaktivität, hat den größten Anteil des on-chain gehaltenen Stablecoin-Werts und wird nach einer weit gefassten Roadmap fortentwickelt. Ethereum wird häufig als Infrastruktur bezeichnet, und an genau diesem Begriff präzisiert sich die weite Ausgangsfrage zu einer prüfbaren: Erfüllt Ethereums Architektur die Anforderungen, die an eine fundamentale digitale Infrastruktur zu stellen sind?

Ich will mir und dem Leser eine klare Übersicht über den gegenwärtigen Zustand einer solchen Infrastruktur verschaffen und über den Zustand, den sie unter vollständiger Umsetzung ihrer Roadmap erreichen könnte. Am Schluss steht mein eigenes Urteil, doch gleichberechtigt daneben steht die Absicht, dem Leser die Mittel zu geben, mit denen er sich sein eigenes bildet, frei von meinem. Dass ich selbst im Feld stehe, über Web3 schreibe und publiziere, lege ich offen und mache es zum Grund einer ausdrücklichen Verpflichtung zur Neutralität, denn wer dem Gegenstand nahesteht, schuldet dem Leser die Distanz umso mehr. Die Arbeit begleitet zugleich meine beruflichen Bewerbungen, was ich benenne, damit der Leser das Interesse kennt, vor dem er sie liest. Entstanden ist sie mithilfe digitaler Werkzeuge, darunter KI-gestützte Systeme, die ich zur Recherche, zur Strukturierung und zur sprachlichen Prüfung herangezogen habe. Die Fragestellung, der Bewertungsrahmen und jedes Urteil, das daraus folgt, verantworte ich selbst. Dass mit der Frage nach dem Nutzen eine Frage nach der Rendite mitläuft, ist unvermeidlich, ich behandle sie als Folge der Analyse und lasse mein Urteil an dem messen, was sich langfristig als tragfähig erweist. Ob Ethereum den Anforderungen einer fundamentalen digitalen Infrastruktur standhält, entscheidet sich auf den folgenden Seiten.

Garbsen, im Juli 2026

Henrik Asmus

[1] Electric Capital: Developer Report 2025. https://www.developerreport.com

Kapitel 1

Einleitung

1.1 Problemstellung und Relevanz

Ethereum wird seit einigen Jahren als Infrastruktur bezeichnet, im Ökosystem selbst, in den Analysen der Beratungshäuser und zunehmend in den Erläuterungen der Regulierer. Widerspruch gegen die Zuschreibung erhebt sich durchaus, und er verweist auf die Volatilität der Bewertungen, auf die Komplexität des Systems und auf den spekulativen Charakter eines Marktes, in dem sich innerhalb weniger Stunden Milliarden an Positionen auflösen. Der Einwand der Spekulation berührt die Frage der Infrastruktureignung dabei unmittelbar, weil bei Ethereum die Bewertung des nativen Vermögenswerts mit der Sicherheit des Systems verbunden ist und eine solche Verbindung unter den etablierten Infrastrukturen ohne Entsprechung bleibt. Entscheiden lässt sich der Einwand gleichwohl nicht, solange niemand angibt, welchen Grad an Unabhängigkeit von der eigenen Bewertung ein System aufweisen muss, um als Infrastruktur zu gelten. Die Zuschreibung steht deshalb weitgehend unangefochten, obwohl ihre Prüfung an keiner Stelle ansetzen kann.

Der Ausdruck fasst dabei ein Bündel von Eigenschaften zusammen, das über die Bezeichnung selbst hinausgeht. Gemeint sind Dauerhaftigkeit über Jahrzehnte, Neutralität gegenüber den Teilnehmern, die Unmöglichkeit einseitiger Abschaltung und die Eignung für Nutzungen, die bei der Errichtung des Systems noch niemand kannte. Ob das Wort verwendet wird, bleibt folgenlos. Folgenreich ist, dass Akteure sich bereits so verhalten, als lägen diese Eigenschaften vor. J.P. Morgan legte im Mai 2026 einen tokenisierten Geldmarktfonds auf, der ausschließlich auf Ethereum operiert und binnen rund eines Monats von zweihundert Millionen auf annähernd siebenhundert Millionen Dollar anwuchs. Crédit Agricole gab über ihre Verwahrtochter einen MiCA-konformen Euro-Stablecoin auf derselben Kette aus, in produktivem Betrieb und nicht als Pilotversuch. In-

stitutionelle Kapitalgeber richten Allokationen an der Erwartung aus, das Netzwerk werde in zehn Jahren noch bestehen, und begründen es mit einem Jahrzehnt ununterbrochener Verfügbarkeit über fünfzehn Protokoll-Upgrades hinweg. Gesetzgeber wiederum entwerfen Regelwerke wie die europäische Verordnung über Märkte für Kryptowerte, die bereits eine Entscheidung darüber enthalten, ob eine Anwendung, eine Plattform oder eine Infrastruktur vorliegt. Alle diese Akteure prüfen sorgfältig, doch ihre Prüfung erstreckt sich auf den gegenwärtigen Zustand des Systems. Die Annahme über seinen dauerhaften Bestand entzieht sich der Prüfung und wird von jedem Akteur nach eigenem Ermessen getroffen.

Die Kosten einer falschen Annahme fallen in beiden Richtungen an. Erweist sich das Vertrauen als unbegründet, so trifft der Ausfall die aufgebauten Positionen an allen Stellen zugleich, während die Ausweichwege im Zuge der Integration bereits aufgegeben wurden und die erreichte Verflechtung sich nur unter erheblichem Aufwand rückgängig machen lässt. Erweist sich die Ablehnung als unbegründet, so entfällt der Zugang zu einer Koordinationsschicht, die sich unter Netzwerkeffekten kein zweites Mal beliebig errichten lässt, und die Ausgestaltung ihrer Regeln, ihrer Zugangsbedingungen und ihrer Neutralitätsgarantien fällt anderen zu. Beide Fehlurteile sind teuer, und keines von beiden lässt sich ohne einen Maßstab vermeiden.

Ein solcher Maßstab liegt bislang nicht vor. Der Ausdruck fundamentale digitale Infrastruktur zirkuliert in all diesen Debatten als Prädikat, das zugesprochen oder verweigert wird, ohne dass jemals bestimmt wurde, welche Eigenschaften es dafür verlangt. Die vorliegende Arbeit konstruiert den Maßstab zunächst und wendet ihn anschließend auf ein System an, das sich weiterhin aktiv entwickelt.

1.2 Forschungslücke

Der im vorigen Abschnitt beschriebene Zustand ließe sich als Eigenheit des öffentlichen Diskurses abtun, sofern die Forschung den fehlenden Maßstab bereitstellte. Sie stellt ihn nicht bereit. Es existiert eine ausgearbeitete Infrastrukturtheorie, es existiert eine umfangreiche Blockchain-Forschung, und es existiert eine eingespielte Beurteilungspraxis für Infrastruktursysteme, doch jeder dieser drei Bestände leistet etwas anderes als das, was die Forschungsfrage verlangt.

Die Infrastrukturtheorie ist auf Blockchain übertragen worden, ohne dass ihr begrifflicher Apparat auf ein einzelnes System systematisch angewandt worden wäre. Die einschlägigen Arbeiten beschreiben ihren Gegenstand mit dem Vokabular der Infrastrukturforschung und leisten damit die Vorarbeit, auf der eine Bewertung aufsetzen könnte.[2] Zu einer Bewertung gelangen sie nicht, weil ihnen die Mittel dazu fehlen. Es fehlen operationalisierte Kriterien, es fehlen Schwellenwerte, und es fehlt ein Verfahren, das aus Einzelbefunden ein Urteil bildet.

Die Blockchain-Forschung verfügt über ein ausgereiftes Instrumentarium der Messung, das jedoch auf andere Eigenschaften zielt. Ihre Verfahren erfassen den Grad der Dezentralisierung eines Systems oder die Frage, ob eine Organisation den Einsatz dieser Technologie erwägen sollte.[3] Dass Dezentralisierung mit Infrastruktureignung nicht zusammenfällt, zeigt sich am globalen Finanznachrichtensystem SWIFT, das von einer einzigen Organisation betrieben wird und gleichwohl als fundamentale Infrastruktur des internationalen Zahlungsverkehrs gilt. Ein Verfahren, das Dezentralisierung misst, erfasst deshalb eine Eigenschaft, aus deren Ausprägung sich die Eignung nicht ableiten lässt.

Die Beurteilungspraxis schließlich, die sich für Infrastruktursysteme eingespielt hat, setzt voraus, was der Gegenstand nicht bietet. Ihre Kriterien richten sich an eine Betreiberorganisation, die Investitionsverpflichtungen eingeht und einer Aufsicht untersteht. Kapitel 3 prüft diese Voraussetzung an sieben Referenzinfrastrukturen und zeigt, dass sie dort die Regel, aber keine Bedingung der Infrastrukturfunktion ist. Ein System, dessen Regeln aus der Zustimmung unabhängiger Teilnehmer hervorgehen und für dessen Fortbestand keine Instanz ein-

[2] Vgl. Ølnes, Svein / Jansen, Arild (2018): Blockchain Technology as Infrastructure in Public Sector: An Analytical Framework, sowie dies. (2021): Blockchain Technology as Information Infrastructure in the Public Sector; ferner Grimmelmann, James / Windawi, A. Jason (2023): Blockchains as Infrastructure and Semicommons, Dimitropoulos, Georgios (2020): The Law of Blockchain, und Nabben, Kelsie (2023): Web3 as 'Self-Infrastructuring'. Die vollständigen Angaben stehen in den Fußnoten zu Abschnitt 2.1.

[3] Vgl. Ovezik, Christina u. a. (2025): SoK: Measuring Blockchain Decentralization; Srinivasan, Balaji S. / Lee, Leland (2017): Quantifying Decentralization; Wachter, Victor / Ross, Omri (2021): How Decentralized is the Governance of Blockchain-based Finance. Die vollständigen Angaben stehen in den Fußnoten zu Abschnitt 2.1.

steht, entzieht sich diesen Kriterien, ohne dass daraus etwas über seine Eignung folgte.

Die Lücke ist damit bestimmt. Die Theorie liefert Begriffe ohne Bewertungsmaßstab, die Blockchain-Forschung liefert Maßstäbe für andere Eigenschaften, und die eingespielte Praxis liefert Kriterien für einen Systemtyp, dem der Gegenstand nicht angehört.

1.3 Forschungsfrage

Die Frage, auf die die vorliegende Arbeit antwortet, lautet im Wortlaut:

Erfüllt Ethereums Architektur die Anforderungen, die an eine fundamentale digitale Infrastruktur zu stellen sind?

Wer so fragt, setzt voraus, dass die Anforderungen feststehen, an denen ein System sich messen lassen soll. Sie stehen nicht fest, und die Bestimmung der Anforderungen geht der Prüfung Ethereums deshalb voraus. Erst wenn sie vorliegt, lässt sich die Frage überhaupt entscheiden.

Die Frage zielt auf den Aufbau des Systems und auf das, was der Aufbau leistet. Sie fragt, wie Ethereum gebaut ist, was aus der Bauweise folgt und ob das den Anforderungen genügt. Ob sich Ethereum gegenüber anderen Systemen durchsetzt, gehört nicht zu dieser Frage, weil die Durchsetzung eines Systems von Umständen abhängt, die seinem Aufbau äußerlich bleiben. Eine Architektur kann jede Anforderung erfüllen und sich dennoch nicht durchsetzen. Über die Etablierung Ethereums trifft diese Arbeit keine Aussage.

Das System, das geprüft werden soll, verändert sich, während die Prüfung läuft. Ethereum wird nach einer Roadmap weiterentwickelt, deren Vorhaben aus Vorschlägen hervorgehen, die unabhängige Entwickler in einem offenen Verfahren verhandeln, überarbeiten und gelegentlich verwerfen, ohne dass eine Instanz sie erließe. Der Schutz der kryptographischen Verfahren vor Quantencomputern, deren Rechenleistung die heute verwendeten Signaturen brechen könnte, wird seit Jahren erforscht. Neue Aufwandsschätzungen, unter ihnen ein Whitepaper von Google Quantum AI aus dem März 2026, haben der Bedrohung zusätzliches Gewicht gegeben.[4] Die Ethereum Foundation unterhält seit Januar 2026 ein eigenes Post-Quantum-Forschungsteam und erprobt erste Bausteine in frühen Implementierungen.[5] Der Post-Quantum-Umbau läuft als paralleler

[4] Google Quantum AI / Ethereum Foundation / Stanford University: Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities. Resource Estimates and Mitigations, 30. März 2026. Die Veröffentlichung erfolgte drei Tage nach dem Stichtag der IST-Bewertung.

[5] Ethereum Foundation: Post-Quantum-Security-Team, eingerichtet im Januar 2026 unter der Leitung von Tho-

Langfriststrang mit einem Zielhorizont um 2029, während die Roadmap der nächsten Jahre von Skalierung und Nutzbarkeit geführt bleibt. Was die Vorhaben verändern, betrifft den Kern des Systems: wie die Teilnehmer sich auf einen gemeinsamen Zustand einigen, wie das System Code ausführt und wie ein einzelner Nutzer nachprüfen kann, ob das Ergebnis stimmt.

Ein Urteil über das heutige System verliert seine Gültigkeit in dem Maß, in dem diese Vorhaben umgesetzt werden, weil sie an dem ansetzen, worüber geurteilt wurde. Ein Urteil über das künftige System wiederum sagt nichts darüber, worauf ein Nutzer sich heute verlassen kann, weil es Bedingungen voraussetzt, die noch nicht bestehen. Die Arbeit beantwortet die Forschungsfrage deshalb zweimal, einmal für den IST-Zustand und einmal für den SOLL-Zustand, den das System unter vollständiger Umsetzung seiner Roadmap erreichen würde. Einen Zeitpunkt der vollständigen Umsetzung nennt sie ebenso wenig wie eine Wahrscheinlichkeit.

Die Reihenfolge, in der die beiden Antworten gegeben werden, folgt aus dem Gegenstand. Der Umbau setzt an dem an, was existiert, und wer nicht versteht, wie Ethereum heute funktioniert, kann nicht beurteilen, was die Vorhaben daran ändern. Die Bewertung des IST-Zustands leistet deshalb zweierlei, indem sie die Forschungsfrage für die Gegenwart beantwortet und das System zugleich so beschreibt, dass die Bewertung des SOLL-Zustands auf der Beschreibung aufsetzen kann.

1.4 Methodisches Vorgehen

Da kein vorhandenes Verfahren die Anforderungen an fundamentale digitale Infrastruktur prüfbar macht, stellt die Arbeit den Maßstab selbst her. Sie leitet zwölf Kriterien aus dem Begriff der fundamentalen Infrastruktur ab, aus der Frage, was ein System aufweisen muss, damit andere sich dauerhaft auf es stützen können. Die Herleitung folgt einem etablierten Verfahren der Begriffsbildung, das jedes Kriterium einzeln aus dem Begriff entwickelt und seine Geltung aus der Herleitung bezieht.[1]

Die zwölf Kriterien stehen fest, bevor sie an sieben etablierten Infrastrukturen geprüft werden, dem Stromnetz, dem Internet, dem Straßennetz, dem Finanznachrichtensystem SWIFT, dem Satellitennavigationssystem GPS, der Cloud-Infrastruktur und dem Rechtssystem. An diesen Systemen zeigt sich, ob ein Kriterium der Konfrontation mit tatsächlicher Infrastruktur standhält und ob es

mas Coratger. https://pq.ethereum.org

Eigenschaften erfasst, die reale Infrastrukturen teilen. Die Aussagekraft der Prüfung beruht auf der Verschiedenheit der sieben Systeme, denn ein Kriterium, das sich am physischen Stromnetz ebenso bewährt wie an der institutionellen Ordnung des Rechts, ist an der Breite dieser Fälle erprobt.

Jedes der zwölf Kriterien wird auf einer vierstufigen Skala bewertet, die von voller Erfüllung bis zum offenen Befund reicht. Die zwölf Kriterien stehen dabei in einer Hierarchie, in der einige als Schwelle wirken. Versagt ein solches Kriterium, begrenzt das schon das erreichbare Gesamturteil, so gut die übrigen elf auch abschneiden. Eine Infrastruktur, an der eine tragende Anforderung ausfällt, wird durch Stärke an anderer Stelle nicht ausgeglichen. Aus den zwölf Einzelbefunden entsteht das Gesamturteil über feste Regeln, deren Anwendung ein zweiter Prüfer mit demselben Material nachvollziehen und zum selben Ergebnis führen kann.

Aus dieser Anlage folgen drei Züge der Antwort. Die Antwort auf die Forschungsfrage ist gestuft und fällt nicht in ein bloßes Ja oder Nein, weil das Gesamturteil ein Spektrum von Kategorien kennt. Die Antwort für den IST-Zustand steht auf gemessenen Zuständen des heute laufenden Systems, die Antwort für den SOLL-Zustand auf Spezifikationen, Prototypen und Forschungsentwürfen, deren Umsetzung noch aussteht. Der SOLL-Zustand schließlich wird über die Leistungen beschrieben, die das fertig gedachte System erbringt, denn eine solche Beschreibung überdauert Änderungen der Roadmap, an denen eine Liste geplanter Funktionen veraltete.

□ *Jabareen, Yosef (2009): Building a Conceptual Framework. Philosophy, Definitions, and Procedure.* International Journal of Qualitative Methods*, 8(4), S. 49–62.*

1.5 Positionierung, Neutralität und Abgrenzung

Die Arbeit wahrt gegenüber ihrem Gegenstand analytische Neutralität, zu der sie sich ausdrücklich verpflichtet. Negative Befunde sind ihr so willkommen wie positive, und ihr Verfahren liegt offen. Das dient einem doppelten Ziel. Am Ende steht ein Urteil, und die Arbeit gibt dem Leser zugleich die Mittel, mit denen er selbst urteilt. Die Arbeit bleibt deshalb auch dann brauchbar, wenn der Leser ihrem Urteil nicht folgt.

Sie wendet sich an unternehmerische Entscheider, institutionelle Investoren, technische Architekten, politische Entscheidungsträger und kritische Akademiker, die Ethereum in aller Regel nicht von innen kennen. Aus dieser Wahl folgt das Register der Arbeit. Sie erklärt, was einem solchen Publikum erklärt werden muss, und setzt kein Vorwissen voraus, das nur im Ökosystem selbst verbreitet ist. Sie erscheint selbstpubliziert und ohne externe Begutachtung, was hier offen benannt wird. Gerade weil keine prüfende Instanz zwischen die Arbeit und ihren Leser tritt, macht sie ihr Vorgehen an jeder Stelle nachvollziehbar und überlässt ihm das Urteil über ihre Schlüssigkeit.

Der Maßstab, den die Arbeit anlegt, reicht so weit wie das, was sich am System selbst ablesen lässt. Was innerhalb des Protokolls messbar ist, kann sie bewerten. Was außerhalb liegt, bleibt außer Reichweite. Dazu gehört die Qualität der Daten, die von außen in das System gelangen und deren Richtigkeit das Protokoll selbst nicht sicherstellt, ebenso wie die regulatorische Umgebung und die gesellschaftliche Akzeptanz, die über die tatsächliche Nutzung mitentscheiden. Diese Beschränkung ist gewollt, weil die Arbeit bewertet, was sie messen kann, und ausweist, was sie nicht messen kann. Ebenso prüft sie die Infrastruktur selbst und nicht die Anwendungen, die auf ihr aufsetzen. Die Trennlinie zwischen beiden folgt einer Frage: Beeinflusst eine Anwendung die Eignung der Infrastruktur? Ein Dienst, dessen Anteil an der Absicherung des Netzwerks die Schwellen des Konsensverfahrens berührt, gehört in die Prüfung. Ein Dienst, der auf der Infrastruktur aufsetzt, ohne auf sie zurückzuwirken, gehört nicht hinein. Abschnitt 2.3.4 führt die Trennlinie an Beispielen aus.

Die Arbeit trennt zudem den heutigen Zustand vom künftigen und beantwortet die Forschungsfrage für beide getrennt, aus den Gründen, die der Abschnitt zur Forschungsfrage genannt hat. Der IST-Zustand hat einen Datenstichtag, den 27. März 2026. Der Stichtag bindet allein die Bewertungsdaten, während die rahmenden Angaben der Einleitung bis zum Redaktionsschluss reichen. Die Kennzahlen, die ihn beschreiben, sind Momentaufnahmen eines Systems, das sich fortwährend verändert, während sein Aufbau und die daraus folgenden

strukturellen Befunde beständiger bleiben. Für die Argumentation zählt deshalb, in welcher Größenordnung eine Zahl liegt und in welche Richtung sie weist, und nicht ihr genauer Betrag zu einem bestimmten Tag.

Aus alldem ergibt sich, was die Arbeit nicht ist. Sie ist kein technisches Handbuch, das erklärt, wie man auf Ethereum baut, und keine Anlageberatung. Sie ist auch keine Prognose über den Preis des nativen Vermögenswerts oder über die künftige Verbreitung des Systems. Warum die Durchsetzung außerhalb der Frage bleibt, führt der Abschnitt zur Forschungsfrage aus.

1.6 Aufbau der Arbeit

Die Antwort auf die Forschungsfrage baut sich über die folgenden sechs Kapitel auf, und jedes setzt an dem an, was das vorige erarbeitet hat. Zuerst entsteht der Maßstab, dann wird er an die Gegenwart und an die Zukunft angelegt, zuletzt werden beide Befunde zusammengeführt. Der Leser hat damit die Abfolge der folgenden Kapitel vor sich, die die nächsten Absätze im Einzelnen bezeichnen.

Die beiden ersten Kapitel stellen den Maßstab her. Kapitel 2, Theoretischer Rahmen und Methodik, klärt zunächst, was eine Infrastruktur zu einer fundamentalen macht, und entwickelt aus der Klärung den Bewertungsrahmen, die zwölf Kriterien. Kapitel 3, Infrastruktur-Kontextualisierung, hält die bereits hergeleiteten Kriterien gegen sieben etablierte Infrastrukturen, prüft an ihnen, ob die Kriterien der Konfrontation mit tatsächlicher Infrastruktur standhalten, und legt offen, was das Verfahren nicht leisten kann. Am Ende dieser beiden Kapitel steht ein geprüftes Instrument, das auf Ethereum angewendet werden kann.

Die beiden folgenden Kapitel wenden es an, zweimal auf denselben Gegenstand zu verschiedenen Zeitpunkten. Kapitel 4, IST-Bewertung, beschreibt das heutige Ethereum zusammenhängend und bewertet es dann entlang der drei Dimensionen des Bewertungsrahmens, der strukturellen Fundierung, der qualitativen Tragfähigkeit sowie der Resilienz und Souveränität, und gelangt zu einem Gesamturteil für die Gegenwart. Kapitel 5, Der Zielzustand, legt dasselbe Instrument an das Ethereum an, das unter vollständiger Umsetzung seiner Roadmap entstünde, und gelangt ebenso zu einem Gesamturteil. Beide Kapitel arbeiten mit demselben Maßstab, sodass ihre Befunde sich unmittelbar vergleichen lassen.

Die letzten beiden Kapitel führen zusammen und blicken voraus. Kapitel 6, Delta, Grenzen und Gesamturteil, stellt die beiden Befunde nebeneinander, untersucht die Differenz zwischen dem heutigen und dem künftigen Zustand, prüft, ob und welche Grenzen dem System über beide Zeitpunkte hinweg ge-

setzt bleiben, und prüft den Bewertungsrahmen auf das, was kein Kriterium erfasst. In diesem letzten Schritt wendet die Arbeit ihren eigenen Maßstab gegen sich selbst und macht sichtbar, wo er an seine Grenze stößt. Am Ende dieses Kapitels wird die Forschungsfrage beantwortet. Kapitel 7, Implikationen, tritt aus der bewertenden Rolle der vorigen Kapitel heraus und denkt die Antwort weiter, zu ihren Konsequenzen für jene, die auf dem System aufbauen, ihm vertrauen oder es regulieren, und zu einem Ausblick, dessen Ton sich öffnet. Der Ausblick nimmt die Zeit des Schreibens und der Recherche noch einmal in den Blick. So kehrt die Arbeit am Schluss dorthin zurück, wo das Vorwort begann, zur Stimme dessen, der die Frage gestellt hat.

Am Ende steht die Antwort auf die Frage, ob Ethereums Architektur die Anforderungen einer fundamentalen digitalen Infrastruktur erfüllt. Wie sie ausfällt, entscheiden die Kapitel, die zu ihr führen.

Kapitel 2

Theoretischer Rahmen und Methodik

Dieses Kapitel legt das theoretische und methodische Fundament der Arbeit dar. Abschnitt 2.1 verortet die Forschungsfrage in der Infrastrukturtheorie. Abschnitt 2.2 begründet, warum ein eigener Bewertungsrahmen entwickelt werden muss, dokumentiert die Forschungslücke und grenzt gegen bestehende Ansätze ab. Abschnitt 2.3 präsentiert den Bewertungsrahmen vollständig, von der Bewertungslogik über die zwölf Kriterien bis zu den Scope-Grenzen. Die Arbeit verfolgt dabei ein doppeltes Ziel: Sie liefert ein begründetes Urteil zur Forschungsfrage und dokumentiert gleichzeitig Evidenz und Schlussfolgerungen so transparent, dass der Leser zu einem eigenständigen, möglicherweise abweichenden Urteil gelangen kann.

2.1 Was ist Infrastruktur?

Die Forschungsfrage dieser Arbeit lautet, ob Ethereums Architektur die Anforderungen erfüllt, die an eine fundamentale digitale Infrastruktur zu stellen sind. Bevor diese Frage beantwortet werden kann, muss geklärt werden, was der Begriff Infrastruktur in einem akademischen Kontext bedeutet. Im politischen und medialen Sprachgebrauch ist der Begriff inflationär geworden: Breitbandnetze werden als digitale Infrastruktur bezeichnet, Bildungssysteme als gesellschaftliche Infrastruktur, Ladestationen als Ladeinfrastruktur, und in der Kryptoindustrie firmiert jedes Protokoll mit mehr als einer Handvoll Nutzern als Infrastruktur. Die Alltagsverwendung folgt einer impliziten Heuristik, nach der jedes System, das wichtig erscheint und von vielen genutzt wird, den Titel Infrastruktur verdient. Für eine akademische Bewertung reicht diese Heuristik nicht aus, weil sie keine Trennlinie zwischen Infrastruktur und Nicht-Infrastruktur zieht und damit die Forschungsfrage unbeantwortbar macht. Die folgenden theoretischen Perspektiven liefern die begriffliche Schärfe, die eine solche Trennlinie ermöglicht.

Die ökonomische Definition

Brett Frischmann hat 2012 in *Infrastructure: The Social Value of Shared Resources* eine grundlegende ökonomische Infrastrukturdefinition vorgelegt.[6] Seine zentrale Einsicht verschiebt den analytischen Fokus: Infrastruktur definiert sich durch das, was sie ermöglicht, nicht durch das, was sie ist. Ob ein System physisch oder digital, groß oder klein, teuer oder günstig ist, sagt nach Frischmann nichts darüber aus, ob es Infrastruktur ist. Entscheidend sind drei funktionale Kriterien. Das erste Kriterium ist Nicht-Rivalität im Konsum bis zu einer Kapazitätsschwelle: Die Nutzung durch einen Akteur schließt die gleichzeitige Nutzung durch andere nicht aus, solange das System nicht an seine Kapazitätsgrenze stößt. Das zweite Kriterium betrifft die Nachfragestruktur: Die Nachfrage nach dem System wird primär von produktiven Aktivitäten getrieben, die das System als Input benötigen, wobei der gesellschaftliche Gesamtnutzen den individuellen Nutzen übersteigt. Das dritte Kriterium ist Input-Charakter: Das System dient als Produktionsfaktor für weiterführende Aktivitäten und ist kein Endprodukt.

Das Straßennetz veranschaulicht die drei Kriterien. Es ist nicht-rival, solange kein Stau herrscht, denn die Fahrt eines Nutzers schließt die Fahrt eines anderen nicht aus, bis die Kapazitätsgrenze der Straße erreicht ist. Es generiert produktive Nachfrage, weil Handel, Arbeitsmobilität und gesellschaftliche Teilhabe auf ei-

[6] Frischmann, Brett M. (2012): *Infrastructure: The Social Value of Shared Resources*. Oxford University Press.

nem funktionierenden Straßennetz aufbauen und der gesellschaftliche Gesamtnutzen den individuellen Fahrnutzen übersteigt. Es hat Input-Charakter, weil ohne Straßen weder ein Logistiksektor noch ein flächendeckender Einzelhandel noch ein Arbeitsmarkt mit Pendlerbewegungen existieren könnte. Frischmanns drei Kriterien beschreiben damit eine spezifische ökonomische Rolle: Infrastruktur ist eine Ermöglichungsstruktur, deren Wert sich in den Aktivitäten realisiert, die sie ermöglicht.

Aus der Einsicht zieht Frischmann eine ordnungspolitische Konsequenz, die für den Gegenstand dieser Arbeit unmittelbar relevant ist. Weil Infrastruktur ihren Wert durch Ermöglichung erzeugt und der Wert mit der Breite der Nutzung steigt, ist Commons-Management, also nicht-diskriminierender offener Zugang, in vielen Fällen ökonomisch effizienter als die Einschränkung des Zugangs durch private Eigentumsrechte.[7] Ethereums Permissionless-Design, das jedem Akteur die Nutzung des Netzwerks ohne Genehmigung eines Gatekeepers ermöglicht, ist eine technische Implementierung genau dieses Arguments. Der Zusammenhang zwischen Frischmanns Infrastrukturtheorie und Blockchain-Systemen ist dabei kein Analogieschluss dieser Arbeit: James Grimmelmann und A. Jason Windawi haben 2023 im *William & Mary Law Review*, einem angesehenen amerikanischen Law Review, gezeigt, dass Blockchains Frischmanns Infrastrukturkriterien erfüllen und gleichzeitig als Semicommons funktionieren, also als Systeme mit verschränkter privater und gemeinsamer Ressourcennutzung.[8][9] Die vorliegende Arbeit baut auf der akademisch etablierten Verbindung auf.

---

[7] Frischmanns Argument baut auf dem von Elinor Ostrom (1990) empirisch belegten Befund auf, dass Gemeinschaften geteilte Ressourcen erfolgreich selbst verwalten können, ohne Privatisierung oder staatliche Kontrolle. Ostroms acht Designprinzipien für nachhaltige Commons-Governance sind auf Ethereums Governance-Modell anwendbar; eine systematische Anwendung auf Blockchain-Systeme haben Rozas et al. (2021) vorgenommen. — Ostrom, Elinor (1990): *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press. — Rozas, David / Tenorio-Fornés, Antonio / Díaz-Molina, Silvia / Hassan, Samer (2021): When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance. *SAGE Open*, 11(1), S. 1–14. DOI: 10.1177/21582440211002526.

[8] Grimmelmann, James / Windawi, A. Jason (2023): Blockchains as Infrastructure and Semicommons. *William & Mary Law Review*, 64(4), S. 1097–1129.

[9] Vgl. auch Dimitropoulos, Georgios (2020): The Law of Blockchain. *Washington Law Review*, 95(3), S. 1117–1200, der Blockchain als „infrastructural commons" konzipiert.

Die soziologische Erweiterung

Frischmanns Definition ist ökonomisch und funktioniert für Systeme, deren Wertschöpfung messbar ist. Susan Leigh Star hat 1999 in *The Ethnography of Infrastructure* eine Perspektive eingeführt, die über die ökonomische Funktionsbestimmung hinausgeht.[10] Ihre zentrale Einsicht lautet: Infrastruktur ist relational. Sie entsteht nicht durch objektive Eigenschaften eines Systems, sondern in Relation zu organisierten Praktiken. Was für den Ingenieur, der das Glasfasernetz wartet, ein Arbeitsobjekt ist, ist für den Nutzer, der über das Netz eine Videokonferenz führt, unsichtbare Infrastruktur. Was für den Bewohner eines Industrielandes selbstverständliche Infrastruktur ist, kann für den Bewohner eines anderen Landes ein unerreichbares Gut sein. Star hat eine weitere Eigenschaft identifiziert, die zum Standardrepertoire der Infrastrukturforschung gehört: Infrastruktur wird sichtbar beim Zusammenbruch. Solange sie funktioniert, ist sie unsichtbar. Niemand denkt an das Stromnetz, bis der Strom ausfällt, und niemand denkt an das Domain Name System, bis eine Website nicht mehr erreichbar ist.

Stars Perspektive verändert die Forschungsfrage dieser Arbeit auf eine Weise, die den gesamten Bewertungsrahmen prägt. Wenn Infrastruktur relational ist, dann lässt sich die Frage, ob Ethereum Infrastruktur ist, nicht binär beantworten, weil die Antwort davon abhängt, für wen und in welchem Anwendungskontext sie gestellt wird. Für einen DeFi-Entwickler, dessen gesamte Geschäftslogik auf Ethereum-Smart-Contracts aufbaut, ist Ethereum bereits heute Infrastruktur im Sinne Stars, denn das System ist für seine organisierte Praxis unsichtbare Voraussetzung. Für einen Nutzer, der eine einzelne Transaktion tätigt, ist es eher ein Werkzeug. Genau diese Kontextabhängigkeit operationalisiert das Meta-Muster, das die gesamte Bewertungslogik dieser Arbeit prägt: Die Ausprägung muss zum Anspruch passen. Der Bewertungsrahmen bewertet nicht, ob Ethereum Infrastruktur in einem absoluten Sinne ist, sondern ob es die Anforderungen erfüllt, die an eine fundamentale digitale Infrastruktur zu stellen sind, also kontextbezogen und anspruchskalibriert.

---

[10] Star, Susan Leigh (1999): The Ethnography of Infrastructure. *American Behavioral Scientist*, 43(3), S. 377–391.

Digitale Infrastruktur als eigenständige Kategorie

Die bisherige Theorie beschreibt überwiegend physische Infrastruktur, und die Übertragung auf digitale Systeme erfordert eine eigenständige konzeptionelle Grundlage. Ole Hanseth und Kalle Lyytinen haben 2010 Informationsinfrastrukturen als geteilte, offene, heterogene und evolvierende soziotechnische Systeme definiert und zwei fundamentale Designprobleme identifiziert, die digitale von physischer Infrastruktur unterscheiden.[11] Das Bootstrap-Problem beschreibt die Herausforderung, dass eine Infrastruktur frühen Nutzern sofort nützlich sein muss, um überhaupt die Dynamik zu gewinnen, die spätere Netzwerkeffekte ermöglicht. Das Adaptabilitätsproblem beschreibt die Herausforderung, dass lokale Designentscheidungen unbegrenztes Wachstum und funktionale Unsicherheit berücksichtigen müssen, weil die zukünftigen Nutzungsformen der Infrastruktur zum Zeitpunkt des Designs nicht vorhersehbar sind. Tilson, Lyytinen und Sørensen haben im selben Jahr argumentiert, dass digitale Infrastruktur eine eigene analytische Kategorie darstellt, mit eigenen Paradoxien, insbesondere der Spannung zwischen Offenheit und Kontrolle, und eigenen Forschungsfragen, die sich aus der Verschränkung von technischen und institutionellen Dynamiken ergeben.[12]

Beide Probleme manifestieren sich im Gegenstand dieser Arbeit. Ethereum musste 2015, finanziert durch einen Crowdsale von 18,3 Millionen US-Dollar, mit einem konkreten Anwendungsfall starten, der frühen Nutzern sofort nützlich war: der Möglichkeit, Smart Contracts bereitzustellen und auszuführen. Die EVM, Ethereums virtuelle Maschine, lieferte vom ersten Tag an ein programmierbares Ausführungsumfeld, das über reine Zahlungstransaktionen hinausging und damit die Grundlage für die Netzwerkeffekte schuf, die das System heute tragen. Das Adaptabilitätsproblem manifestiert sich in der Roadmap-Komplexität, die Kapitel 5 dieser Arbeit im Detail beschreibt: Das System muss sich weiterentwickeln, um den wachsenden Anforderungen an Skalierung, Datenverfügbarkeit und Nutzerzugang gerecht zu werden, ohne die bestehende Nutzerbasis und die auf dem System aufbauenden Anwendungen zu brechen.

---

[11] Hanseth, Ole / Lyytinen, Kalle (2010): Design Theory for Dynamic Complexity in Information Infrastructures: The Case of Building Internet. *Journal of Information Technology*, 25(1), S. 1–19.

[12] Tilson, David / Lyytinen, Kalle / Sørensen, Carsten (2010): Research Commentary — Digital Infrastructures: The Missing IS Research Agenda. *Information Systems Research*, 21(4), S. 748–759.

Der begriffliche Boden der Bewertungskriterien

Die drei Perspektiven definieren zusammen den analytischen Rahmen, in dem die Forschungsfrage steht. Frischmann liefert die ökonomische Grundlage: Infrastruktur ist eine Ermöglichungsstruktur, deren offener Zugang sich ökonomisch begründen lässt. Star liefert die soziologische Vertiefung: Infrastruktur ist relational und kontextabhängig, was eine binäre Beantwortung der Forschungsfrage ausschließt und eine anspruchskalibrierte Bewertung erfordert. Hanseth und Lyytinen liefern die informationstechnische Spezifizierung: Digitale Infrastruktur unterliegt eigenen Designproblemen, die bei der Bewertung eines konkreten Systems berücksichtigt werden müssen. Die Frage, ob Ethereum fundamentale digitale Infrastruktur ist, lässt sich vor dem Hintergrund als eine Frage stellen, die akademisch bearbeitbar ist: Sie fragt, ob ein konkretes System die Eigenschaften aufweist, die reale Infrastrukturen teilen. Die drei Perspektiven liefern damit den begrifflichen Boden, aus dem die Bewertungskriterien analytisch gewonnen werden. Was fundamentale digitale Infrastruktur konstitutiv auszeichnet, bestimmt sich aus dem Zusammenspiel der ökonomischen, der relationalen und der informationstechnischen Bestimmung des Infrastrukturbegriffs. Kapitel 3 prüft die so hergeleiteten Kriterien anschließend an sieben realen Infrastrukturen. Die Theorie liefert den Rahmen und die Herleitung, die sieben Referenzsysteme liefern den empirischen Prüfstein.

Für eine deutschsprachige Arbeit ist ergänzend die Tradition der großen technischen Systeme relevant. Renate Mayntz hat 1993 große technische Systeme als Komponenten funktionsspezifischer Infrastruktursysteme konzipiert und die Spannung zwischen Steuerung und Selbstorganisation als zentrales Forschungsproblem identifiziert.[13] Die Spannung beschreibt einen Grundkonflikt, der in jeder Infrastruktur angelegt ist: Je größer und komplexer das System, desto schwieriger wird zentrale Steuerung, und desto stärker wird die Eigendynamik des Systems. Ethereums Governance-Modell, das dezentral und ohne formale Steuerungsinstanz operiert und auf dem Prinzip des Rough Consensus beruht, ist ein Extremfall der Spannung. Es gibt keine zentrale Instanz, die Protokolländerungen anordnen kann. Jede Änderung muss von einer Mehrheit der Node-Betreiber freiwillig übernommen werden. Die Frage, ob dieses Modell die Anforderungen an adaptive Governance erfüllt, die an fundamentale Infrastruktur zu stellen sind, ist eine der zwölf Bewertungsdimensionen des Bewertungsrahmens dieser Arbeit.

[13] Mayntz, Renate (1993): Große technische Systeme und ihre gesellschaftstheoretische Bedeutung. *Kölner Zeitschrift für Soziologie und Sozialpsychologie*, 45(1), S. 97–108.

Eine institutionenökonomische Perspektive ergänzt den Rahmen. Sinclair Davidson, Primavera De Filippi und Jason Potts haben 2018 argumentiert, dass Blockchain eine institutionelle Innovation darstellt, die Oliver Williamsons Governance-Framework über die Dichotomie von Märkten und Hierarchien hinaus erweitert.[14] Ethereum kann in dieser Perspektive als ein System gelesen werden, das eine dritte Governance-Form realisiert: protokollbasierte Koordination durch algorithmische Regeln, die weder marktlich verhandelt noch hierarchisch angeordnet werden, sondern durch den Konsens der Netzwerkteilnehmer entstehen.

2.2 Warum ein eigener Bewertungsrahmen?

Die Forschungslücke

Die im vorigen Abschnitt dargestellte Infrastrukturtheorie bietet einen ausgereiften begrifflichen Apparat, um die Frage nach Infrastruktureignung zu stellen. Für Blockchain-Systeme im Allgemeinen und Ethereum im Speziellen ist dieser Apparat bislang nicht systematisch angewandt worden. Svein Ølnes und Arild Jansen haben 2018 und 2021 die relationale Infrastrukturdefinition von Star und Ruhleder sowie die Informationsinfrastruktur-Theorie von Hanseth und Lyytinen auf Blockchain allgemein übertragen und gezeigt, dass Blockchain-Systeme als Informationsinfrastrukturen konzipiert werden können.[15][16] Ihre Arbeiten identifizieren Eigenschaften, die Blockchain mit den in der IS-Forschung beschriebenen Informationsinfrastrukturen teilt, etwa die Offenheit und die Heterogenität der Nutzer, und schließen daraus, dass das Vokabular der Infrastrukturforschung auf Blockchain anwendbar ist. Die Arbeiten beschreiben Blockchain als Infrastruktur. Ob ein konkretes System die Anforderungen fundamentaler Infrastruktur erfüllt, prüfen sie nicht: Es fehlen operationalisierte Kriterien, Schwellenwerte und ein Bewertungsmechanismus. Kelsie Nabben hat 2023 Web3 als self-infrastructuring analysiert, also als einen Prozess, in dem die Community die Infrastruktur, die sie nutzt, selbst hervorbringt und fortlaufend ver-

[14] Davidson, Sinclair / De Filippi, Primavera / Potts, Jason (2018): Blockchains and the Economic Institutions of Capitalism. *Journal of Institutional Economics*, 14(4), S. 639–658. DOI: 10.1017/S1744137417000200.

[15] Ølnes, Svein / Jansen, Arild (2018): Blockchain Technology as Infrastructure in Public Sector: An Analytical Framework. In: *Proceedings of the 19th Annual International Conference on Digital Government Research (dg.o '18)*. ACM, S. 1–10. DOI: 10.1145/3209281.3209293.

[16] Ølnes, Svein / Jansen, Arild (2021): Blockchain Technology as Information Infrastructure in the Public Sector. In: Reddick, C.G. / Rodríguez-Bolívar, M.P. / Scholl, H.J. (Hrsg.): *Blockchain and the Public Sector*. Public Administration and Information Technology, Bd. 36. Springer, Cham, S. 19–46. DOI: 10.1007/978-3-030-55746-1_2.

ändert.[17] Ihre Analyse arbeitet mit dem Vokabular der Infrastructure Studies und liefert Einsichten in die Entstehungsdynamik dezentraler Infrastruktur, zielt aber auf die Prozessbeschreibung, nicht auf die Eignungsbewertung. Paul Dylan-Ennis, Donncha Kavanagh und Luis Araujo haben 2023 Ethereum als soziotechnisches Projekt mit drei Imaginaries untersucht, drei Vorstellungswelten, die die Ethereum-Community antreiben: Ethereum als Weltcomputer, als dezentrale Finanzinfrastruktur und als Koordinationsprotokoll.[18] Ihre soziologische Analyse gibt Aufschluss über die Selbstbeschreibung und die inneren Spannungen der Community. Eine Bewertung der Architektur oder der Infrastruktureignung anhand überprüfbarer Kriterien leistet sie nicht.

Die Lücke, die diese Arbeit füllt, ist damit spezifisch: Es existiert keine rahmenbasierte Bewertung, die operationalisierte Kriterien definiert, transparente Schwellenwerte setzt und ein reproduzierbares Bewertungsverfahren anwendet, um zu prüfen, ob Ethereum die Anforderungen einer fundamentalen Infrastruktur erfüllt. Die genannten Arbeiten steuern Vorarbeiten bei, auf denen diese Arbeit aufbaut, aber keine von ihnen beantwortet die Forschungsfrage.

Abgrenzung gegen bestehende Blockchain-Bewertungsansätze

Der Bedarf an einem eigenständigen Bewertungsrahmen wird deutlicher, wenn man die bestehenden Bewertungsansätze aus der Blockchain-Literatur betrachtet. Was die Ansätze verbindet, ist eine gemeinsame Stoßrichtung: Sie messen Dezentralisierung oder organisationale Eignung, aber sie bewerten keine Infrastruktureigenschaften im infrastrukturtheoretischen Sinne.

Balaji Srinivasan und Leland Lee haben 2017 den Nakamoto-Koeffizienten vorgeschlagen, der den Dezentralisierungsgrad eines Systems als die minimale Anzahl von Akteuren misst, die zusammenwirken müssten, um das System zu kompromittieren.[19] Der Koeffizient erfasst eine wichtige Eigenschaft, sagt aber nichts über Infrastruktureignung aus: SWIFT, das globale Finanznachrichtensystem, hat einen Nakamoto-Koeffizienten nahe eins, weil es von einer einzigen Organisation betrieben wird, und ist dennoch fundamentale Infrastruktur des internationalen Zahlungsverkehrs. Adem Efe Gencer und Kollegen haben 2018 eine empirische Dezentralisierungsmessung über Mining-Verteilung und Netzwerktopologie vorgelegt, die den operativen Dezentralisierungsgrad quanti-

[17] Nabben, Kelsie (2023): Web3 as 'Self-Infrastructuring': The Challenge Is How. *Big Data & Society*, 10(1). DOI: 10.1177/20539517231159002.

[18] Dylan-Ennis, Paul / Kavanagh, Donncha / Araujo, Luis (2023): The Dynamic Imaginaries of the Ethereum Project. *Economy and Society*, 52(1), S. 87–109. DOI: 10.1080/03085147.2022.2131280.

[19] Srinivasan, Balaji S. / Lee, Leland (2017): Quantifying Decentralization. Preprint/Blogpost. URL: https://news.earn.com/quantifying-decentralization-e39db233c28e.

fiziert, aber weder Governance-Dimensionen noch institutionelle Einbettung erfasst.[20] Die jüngste Systematisierung des Forschungsstrangs, eine 2025 publizierte SoK-Studie (Systematization of Knowledge) zur Messung von Blockchain-Dezentralisierung, inventarisiert alle existierenden Dezentralisierungsmetriken und macht damit sichtbar, dass der gesamte Forschungsstrang auf Dezentralisierungsmessung ausgerichtet ist.[21] Die Frage, ob ein System die Anforderungen an Infrastruktur erfüllt, wird von keiner der Metriken behandelt.

Neben der Dezentralisierungsmessung existieren Ansätze, die Blockchain-Eignung aus organisationaler Perspektive bewerten. Spencer-Hicken und Kollegen haben 2023 ein Blockchain Feasibility Assessment für Organisationen entwickelt, das bewertet, ob ein Unternehmen Blockchain-Technologie einsetzen sollte. Es trifft damit eine Übernahmeentscheidung und bewertet keine Infrastruktureignung.[22] Jensen und Kollegen haben 2021 die Governance-Dezentralisierung von DeFi-Protokollen untersucht, die auf der Anwendungsschicht operieren, nicht auf der Basisschicht, die diese Arbeit bewertet.[23] Pincheira und Kollegen haben 2023 die Infrastrukturkosten von Blockchain-Systemen analysiert, wobei sie den Begriff Infrastruktur im IT-technischen Sinne verwenden, als Oberbegriff für Server, Speicher und Netzwerkressourcen, nicht im gesellschaftlichen Sinne einer Ermöglichungsstruktur nach Frischmann.[24]

Die Konsequenz aus der Bestandsaufnahme ist eindeutig: Die bestehenden Ansätze fragen, wie dezentral ein System ist oder ob Blockchain für eine bestimmte Organisation geeignet ist. Die Forschungsfrage dieser Arbeit lautet, ob ein System die Anforderungen erfüllt, die an fundamentale Infrastruktur zu stellen sind. Diese Arbeit beantwortet die Frage mittels eines Bewertungsrahmens, der Infrastruktureigenschaften operationalisiert, gestützt auf die Infrastrukturtheorie und validiert an realen Infrastrukturen. Ein Bewertungsrahmen, der aus der Blockchain-Literatur stammt und Dezentralisierungsmetriken aggregiert, kann die Forschungsfrage nicht beantworten, weil er die falsche Eigenschaft misst.

---

[20] Gencer, Adem Efe et al. (2018): Decentralization in Bitcoin and Ethereum Networks. In: *Financial Cryptography and Data Security*. Springer, S. 439–457.

[21] Ovezik, Christina / Karakostas, Dimitris / Milad, Mary / Kiayias, Aggelos / Woods, Daniel W. (2025): SoK: Measuring Blockchain Decentralization. arXiv:2501.18279. Auch publiziert in: Fischlin, M. / Moonsamy, V. (Hrsg.): *Applied Cryptography and Network Security (ACNS 2025)*. Lecture Notes in Computer Science, Bd. 15825. Springer, Cham. DOI: 10.1007/978-3-031-95761-1_7.

[22] Spencer-Hicken, Scott et al. (2023): Blockchain Feasibility Assessment: A Quantitative Approach. *Frontiers in Blockchain*, 6. DOI: 10.3389/fbloc.2023.1155125.

[23] Jensen, Johannes R. / von Wachter, Victor / Ross, Omri (2021): How Decentralized is the Governance of Blockchain-based Finance: Empirical Evidence from four Governance Token Distributions. In: *Proceedings of the 29th European Conference on Information Systems (ECIS 2021)*.

[24] Pincheira, Miguel et al. (2023): An Infrastructure Cost and Benefits Evaluation Framework for Blockchain-Based Applications. *Systems*, 11(4), 184. DOI: 10.3390/systems11040184.

Die Methodik der Konstruktion des Bewertungsrahmens

Die Arbeit validiert ihren Bewertungsrahmen an sieben Referenzinfrastrukturen: Stromnetz, Internet (TCP/IP), Straßennetz, SWIFT, GPS, Cloud-Infrastruktur und Rechtssystem. Die sieben Fälle wurden gewählt, weil sie fünf Infrastrukturtypen abdecken: physisch (Stromnetz, Straßennetz), digital-offen (Internet/TCP-IP), digital-geschlossen (SWIFT, GPS), hybrid (Cloud-Infrastruktur) und institutionell (Rechtssystem). Diese Heterogenität repräsentiert die Breite des Infrastrukturbegriffs und stärkt die Validierungskraft der Auswahl, weil ein Kriterium, das sich in derart unterschiedlichen Systemen wiederfindet, mit höherer Plausibilität als konstitutiv für Infrastruktur gelten kann.

Der analytische Ansatz wurde bewusst gewählt, weil es keinen etablierten Bewertungsrahmen für die Bewertung kryptographischer Infrastruktur gibt. Bestehende Bewertungsansätze aus der Telekommunikation oder der Energiewirtschaft sind auf institutionelle Infrastruktur zugeschnitten, die von zentralen Organisationen betrieben und in regulatorische Rahmenbedingungen eingebettet ist, sodass ihre Übertragung auf ein permissionless System ohne zentrale Betreiberorganisation nach Einschätzung der Arbeit kategoriale Fehlannahmen erzeugen kann. Die Arbeit entwickelt ihren Bewertungsrahmen deshalb eigenständig, und zwar analytisch-deduktiv. Sie zerlegt den Begriff der fundamentalen digitalen Infrastruktur, wie ihn der theoretische Rahmen des vorigen Abschnitts bestimmt, in die konstitutiven Eigenschaften, die ein System aufweisen muss, um dem Anspruch zu genügen. Sie operationalisiert jede dieser Eigenschaften als überprüfbares Kriterium mit eigener Definition, eigenen Indikatoren und eigenen Schwellenwerten.

Das Verfahren folgt der Conceptual Framework Analysis, die Yosef Jabareen beschrieben hat. Diese qualitative Methode zur Framework-Konstruktion führt in systematischen Phasen von der Identifikation der relevanten begrifflichen und theoretischen Quellen über die Extraktion der tragenden Konzepte bis zu ihrer Integration in ein kohärentes Instrument.[25] Der Prüfstein eines so konstruierten Bewertungsrahmens ist nicht seine Herkunft aus einer Fallmenge, sondern seine innere Kohärenz, die Vollständigkeit seiner Dimensionen und seine analytische Produktivität, also die Frage, ob er die Unterscheidungen trifft, auf die es bei der Bewertung ankommt. Jedes der zwölf Kriterien trägt sich über seine eigene begriffliche Herleitung, und keines beansprucht Geltung aus der Häufigkeit, mit der eine Eigenschaft in einer Stichprobe realer Systeme auftritt.

[25] Jabareen, Yosef (2009): Building a Conceptual Framework: Philosophy, Definitions, and Procedure. *International Journal of Qualitative Methods*, 8(4), S. 49–62.

Weil ein analytisch hergeleiteter Bewertungsrahmen Gefahr läuft, an der Realität etablierter Infrastruktur vorbeizukonstruieren, validiert Kapitel 3 die zwölf Kriterien. Es prüft sie an sieben strukturell heterogenen Referenzinfrastrukturen und fragt, ob die deduktiv gewonnenen Anforderungen der Konfrontation mit Systemen standhalten, die sich historisch als fundamentale Infrastruktur etabliert haben. Diese Prüfung ist keine nachträgliche Illustration, sondern der empirische Härtetest des Bewertungsrahmens, dessen Ergebnisse in Kapitel 3 vollständig dokumentiert werden.

2.3 Der Bewertungsrahmen

Der Bewertungsrahmen ist das Instrument, mit dem die Forschungsfrage beantwortet wird.

2.3.1 Bewertungslogik

Drei Grundprinzipien bestimmen die Architektur des Bewertungsrahmens. Das erste Prinzip ist die konditionale Struktur der Bewertung. Die Forschungsfrage ist konditional formuliert: Sie fragt, ob die Architektur den Anspruch einlöst, den sie erhebt. Das Ergebnis ist ein Spektrum, das von „Geeignet“ über „Geeignet mit Bedingungen“ und „Geeignet unter erheblichen Bedingungen“ bis zu „Bedingt geeignet“ und „Nicht geeignet“ reicht. Jede Kategorie ist definiert, und die Zuordnung zu einer Kategorie folgt aus expliziten Regeln, die im Bewertungsmechanismus (M3-Kaskade) festgelegt sind.

Das zweite Prinzip ist das in Abschnitt 2.1 eingeführte Meta-Muster, dass die Ausprägung zum Anspruch passen muss. Es bestätigt sich in der Validierung an den sieben Referenzinfrastrukturen in Kapitel 3. GPS bietet maximale Inklusivität, denn jeder Empfänger weltweit kann das Signal nutzen, aber keine Neutralität, denn das System steht unter unilateraler Kontrolle der US-Regierung, die das Signal selektiv abschalten oder drosseln kann. SWIFT bietet globale Koordination im Finanznachrichtenverkehr, aber keinen offenen Zugang und keine Zensurresistenz, denn Staaten können einzelne Teilnehmer vom System ausschließen. Beide Systeme sind fundamentale Infrastruktur, obwohl keines von ihnen alle denkbaren Infrastruktureigenschaften in maximaler Ausprägung erfüllt. Das Meta-Muster verhindert den Fehlschluss, dass Ethereum jedes Kriterium in maximaler Ausprägung erfüllen muss, um als Infrastruktur zu gelten. Zugleich verhindert es den umgekehrten Fehlschluss, dass jede beliebige Ausprägung akzeptabel ist: Die Ausprägung muss zum spezifischen Anspruch passen, und der Anspruch, den Ethereum erhebt, ist der einer neutralen, permissionless, zensur-

resistenten Infrastruktur.

Das dritte Prinzip ist eine bewusste Designentscheidung: Die Bewertung ist hierarchisch-regelbasiert, nicht additiv. Die Arbeit verwendet kein gewichtetes Scoring-Modell, bei dem jedes Kriterium einen Prozentwert erhält und die Gesamtbewertung aus der Summe der gewichteten Einzelwerte folgt. Stattdessen operiert eine regelbasierte Hierarchie, in der Kritische Bedingungen als Schwelle fungieren: Wenn eine Kritische Bedingung nicht auf dem erforderlichen Niveau erfüllt ist, begrenzt das die bestmögliche Gesamtbewertung, unabhängig davon, wie gut die übrigen Kriterien abschneiden. In einem additiven Modell könnte ein System, das bei der Neutralität, einer Kritischen Bedingung, auf der Stufe „Offen" steht, aber bei allen anderen elf Kriterien die Stufe „Erfüllt" erreicht, trotzdem ein gutes Gesamtergebnis erzielen. Das widerspricht der Infrastrukturlogik: Ein System, das nicht neutral zugänglich ist, kann den Anspruch einer fundamentalen Infrastruktur nicht einlösen, unabhängig von seiner Leistung in anderen Dimensionen. Die Hierarchie bildet diese Logik ab. Sie tauscht Akkumulationssensitivität, also die Fähigkeit, viele kleine Einschränkungen zu einem schlechteren Gesamtergebnis zu aggregieren, gegen Reproduzierbarkeit und Transparenz: Ein zweiter Forscher, der dasselbe Material bewertet, kommt zum selben Ergebnis, weil die Regeln explizit sind und keine impliziten Gewichtungsentscheidungen erfordern.

2.3.2 Die Drei-Ebenen-Logik

Jedes der zwölf Kriterien wird auf drei Ebenen geprüft. Die Protokollebene fragt, was die Architektur ermöglicht. Die operative Ebene fragt, was davon tatsächlich realisiert ist. Die Infrastrukturebene fragt, ob das Zusammenspiel aus architektonischer Möglichkeit und operativer Realität den Infrastrukturanspruch einlöst. Diese Drei-Ebenen-Logik ist das zentrale Analysewerkzeug der gesamten Arbeit. Sie verhindert, dass die Bewertung bei der Architektur stehen bleibt und die operative Realität ignoriert, was zu einer Überbewertung führen würde, weil jedes gut entworfene Protokoll auf der Architekturebene die richtigen Eigenschaften aufweist. Sie schließt umgekehrt aus, dass die operative Realität ohne Berücksichtigung des architektonischen Potenzials bewertet wird, was zu einer Unterbewertung führen würde, weil operative Defizite durch Protokolländerungen behebbar sein können. Die Infrastrukturebene synthetisiert beide Perspektiven und erzwingt die Frage, die für den Infrastrukturanspruch entscheidend ist: Reicht das, was architektonisch möglich und operativ realisiert ist, für den Anspruch aus?

Ein Beispiel macht die drei Ebenen greifbar. Zensurresistenz, eines der Kriterien der Kategorie Kritische Bedingungen, operiert auf allen drei Ebenen mit unterschiedlichen Befunden. Auf der Protokollebene ermöglicht Ethereums Architektur, dass jede valide Transaktion in einen Block aufgenommen werden kann: Das Protokoll selbst enthält keinen Mechanismus, der Transaktionen nach Inhalt oder Absender diskriminiert. Auf der operativen Ebene zeigt sich eine abweichende Realität: Der Großteil der Blöcke wird von wenigen Buildern produziert, die theoretisch Transaktionen ausschließen könnten, und ein beträchtlicher Anteil der Blöcke wird unter Berücksichtigung von OFAC-Sanktionslisten gebaut. Auf der Infrastrukturebene stellt sich die entscheidende Frage: Reicht die protokollseitige Möglichkeit der Inklusion aus, oder muss die operative Zensurresistenz gegeben sein, damit das System den Anspruch einer neutralen Infrastruktur einlöst? Die Antwort, die Kapitel 4 im Detail begründet, hängt davon ab, ob die operative Diskrepanz den Infrastrukturanspruch untergräbt oder ob Mitigationsmechanismen, etwa protokollseitige Inclusion Lists (FOCIL), die Lücke zwischen Protokolldesign und operativer Realität schließen können. Die abschließende Bewertung folgt dem Prinzip des schwächsten Glieds: Die Ebene mit dem niedrigsten Erfüllungsgrad bestimmt die Gesamtbewertung des Kriteriums.

2.3.3 Die drei Bausteine des Bewertungsrahmens

Der Bewertungsrahmen besteht aus drei ineinandergreifenden Bausteinen: der Implementierungsstatus-Taxonomie (M1), den Schwellenwerten für die zwölf Kriterien (M2) sowie der Kriterien-Hierarchie und dem Bewertungsmechanismus (M3-Kaskade).

Implementierungsstatus-Taxonomie (M1)

Die Taxonomie klassifiziert alle Ethereum-Features nach ihrer Umsetzungsreife in fünf Stufen. Features mit dem Status IMPL (implementiert) sind auf dem Mainnet aktiv und produktiv genutzt, seit mindestens drei Monaten stabil und ohne kritische Bugs. Features mit dem Status DEPL (in Deployment) sind in Client-Releases implementiert und auf Testnets aktiv, mit einem angekündigten Mainnet-Datum. Features mit dem Status PLAN (geplant) haben ein akzeptiertes EIP, befinden sich im Status Review oder Last Call, sind in der offiziellen Roadmap und haben einen geschätzten Zeithorizont von weniger als 24 Monaten. Features mit dem Status RES (Research) sind in Roadmap-Dokumenten erwähnt und Gegenstand aktiver Forschung, aber ohne finale Spezifikation. Features mit dem Status DEP (Deprioritized) sind explizit zurückgestellt oder verworfen.

Die Grenze zwischen DEPL und PLAN ist die zentrale epistemische Trennlinie der Arbeit. IMPL und DEPL werden als vorhanden oder gesichert behandelt, weil ihre Umsetzung operativ belegt oder unmittelbar bevorstehend ist. PLAN und RES werden als bedingt behandelt, mit expliziter Unsicherheitskennzeichnung, weil ihre Realisierung von zukünftigen Governance-Entscheidungen, technischer Machbarkeit und Community-Konsens abhängt. Alles unterhalb von DEPL ist Projektion, und die Taxonomie weist den Grad der Projektion aus. Fünf Stufen wurden gewählt, weil sie die relevanten epistemischen Abstufungen abbilden, ohne unnötige Granularität zu erzeugen: Drei Stufen (implementiert, geplant, nicht geplant) würden die Differenz zwischen einem Feature in Testnet-Deployment und einem Feature in früher Forschungsphase einebnen, die für die Belastbarkeit der Bewertung entscheidend ist. Die Taxonomie erzeugt ein Gewissheitsgefälle, das die gesamte Arbeit bestimmt und in der integrierten Belastbarkeitsbewertung in Abschnitt 6.1 nach dem Reifegrad der tragenden Features operationalisiert wird.

Schwellenwerte: Zwölf Kriterien in drei Kategorien (M2)

Die zwölf Kriterien gliedern sich in drei Kategorien, die in der Hierarchie des Bewertungsrahmens unterschiedliche Rollen spielen. Jedes Kriterium wird auf einer vierstufigen Skala bewertet. „Erfüllt" bedeutet, dass die Anforderung vollständig umgesetzt ist und keine strukturellen Einschränkungen bestehen. „Erfüllt mit Einschränkung" bedeutet, dass die Anforderung grundsätzlich erfüllt ist, mit identifizierten Einschränkungen, die den Anspruch nicht grundlegend untergraben. „Bedingt erfüllt" bedeutet, dass die Erfüllung von Bedingungen abhängt, die noch nicht gesichert sind, für die aber ein erkennbarer Pfad besteht. „Offen" bedeutet, dass die Anforderung nicht erfüllt ist und kein operativer Pfad zur Erfüllung existiert. Die Kriterienbewertung ergibt sich aus der argumentativen Synthese der Indikatoren entlang der Drei-Ebenen-Logik. Die Indikatoren liefern die Evidenzbasis, aber die Bewertung folgt keiner mechanischen Zählregel, weil die Indikatoren eines Kriteriums unterschiedliches Gewicht für den Infrastrukturanspruch haben. Eine Zählregel, die etwa drei von vier Indikatoren auf „Erfüllt" als hinreichend für ein „Erfüllt" des Gesamtkriteriums werten würde, behandelt alle Indikatoren als gleichwertig, was sachlich nicht haltbar ist. Die argumentative Synthese erzwingt stattdessen eine strukturierte Begründung, die in jeder Einzelbewertung transparent dokumentiert wird. Der Leser kann die Evidenz und die Schlussfolgerung unabhängig beurteilen. Verändert sich ein Indikator zwischen zwei Bewertungszeitpunkten nicht, bleibt seine Stufe erhalten. Ein unveränderter Indikator kann nicht unter seine im Ausgangszustand erreichte Stufe absteigen.

Die folgenden Absätze stellen die zwölf Kriterien in der Reihenfolge ihrer hierarchischen Funktion vor. Zuerst kommen die Kritischen Bedingungen, die das Fundament des Infrastrukturanspruchs bilden und deren Nicht-Erfüllung die bestmögliche Gesamtbewertung begrenzt. Dann folgen die Strukturellen Bedingungen, die die Tragfähigkeit des Systems bestimmen. Schließlich kommen die Qualitativen Kriterien, die den Grad der Eignung innerhalb der erreichten Kategorie differenzieren.

Sicherheits- und Vertrauenslast (I.2) operiert auf zwei Dimensionen. Die erste Dimension fragt, ob Angriffe auf Ethereum ökonomisch undurchführbar sind. Die ökonomische Sicherheit wird über die Kosten einer 34-Prozent-Attacke gemessen, für die die Schwelle bei über 30 Milliarden US-Dollar für die Stufe „Erfüllt" liegt, abgeleitet aus der CoinMetrics-Studie „Breaking BFT" von 2024. Die 34-Prozent-Schwelle ergibt sich direkt aus der Blocking Minority des Casper-FFG-Konsensalgorithmus: Ein Angreifer, der 34 Prozent des gestakten ETH

kontrolliert, kann die Finalisierung blockieren. Die zweite Dimension fragt, wie viel Restvertrauen in Dritte der Nutzer aufbringen muss, um das System sicher zu nutzen. Diese Dimension ist komplementär zu Kriterium II.3 (Unabhängige Verifizierbarkeit): Während II.3 fragt, ob die Möglichkeit zur Verifikation existiert, fragt I.2, wie viel Restvertrauen trotz dieser Möglichkeit bleibt. Die Antworten können auseinanderfallen, weil ein System, das Verifikation ermöglicht, dennoch eine hohe Vertrauenslast erzeugen kann, wenn die Mehrheit der Nutzer über zentralisierte Intermediäre wie RPC-Anbieter auf das System zugreift.

Minimale tragfähige Garantien (I.4) fragt, ob Ethereum ein Mindestset an Garantien bietet, die auch unter Stress aufrechterhalten werden. Dazu zählen Finality, also die Irreversibilität finalisierter Transaktionen, Liveness, also die Fähigkeit, unter Stress weiter Blöcke zu produzieren, ein Degradation Mode für den Fall eines Validatoren-Ausfalls und Zensurresistenz unter Angriff, die über einen Querverweis zu Kriterium II.1 mitbewertet wird. Die Time-to-Finality-Schwelle von unter 15 Minuten für „Erfüllt" leitet sich direkt aus der Beacon-Chain-Spezifikation ab, die zwei Epochs mit je 32 Slots à 12 Sekunden, also rund 12,8 Minuten, für die Finalisierung vorsieht.

Neutralität und Zensurresistenz (II.1) ist das Kriterium mit dem größten Indikator-Set im Bewertungsrahmen. Sieben Indikatoren prüfen Neutralität auf zwei Ebenen: auf der Transaktionsebene, ob einzelne Transaktionen durch Builder, Relays oder Regulierung zensiert oder verzögert werden, und auf der Systemebene, ob ein Staat oder eine Akteursgruppe Ethereum als Ganzes instrumentalisieren kann. Die OFAC-Compliance-Rate der Blöcke, die Builder-Konzentration, die Existenz eines protokollseitigen Zensurresistenzmechanismus, die maximale Zensur-Verzögerung, die geopolitische Jurisdiktions-Diversität der Validatoren, der Marktanteil des größten Liquid-Staking-Providers und die kumulierte Konzentration der drei größten Staking-Anbieter, unabhängig davon, ob sie als Liquid-Staking-Protokoll oder als verwahrender Dienst auftreten, werden einzeln gemessen und in der Drei-Ebenen-Logik synthetisiert. Die 50-Prozent-Schwelle für OFAC-konforme Blöcke als Grenze zur Stufe „Erfüllt" geht auf die Watershed-Analyse von Uri Klarman zurück. Die 33-Prozent- und 66-Prozent-Schwellen für die Staking-Konzentration leiten sich aus der Blocking Minority und der Supermajority des Casper-FFG-Konsensalgorithmus ab.

Funktionale Unersetzbarkeit (I.1) zielt auf die Verankerungstiefe, gemessen an Netzwerkeffekten, Liquiditätskonzentration und Ökosystem-Bindung. Sie fragt ausdrücklich nicht nach Substituierbarkeit durch alternative Systeme, weil die Arbeit Ethereum isoliert gegen seinen eigenen Anspruch prüft, nicht gegen Konkurrenten. Drei Indikatoren prüfen sie: die Dominanz im DeFi Total Va-

lue Locked über alle Layer-1-Systeme, den Anteil an der globalen Stablecoin-Emission und die Größe des Entwickler-Ökosystems gemessen an öffentlicher Repository-Aktivität. Die Schwellen sind so gesetzt, dass eine Dominanz von über 50 Prozent die Stufe „Erfüllt" erreicht und ein Absinken unter 30 Prozent die Stufe „Offen" auslöst. Der dritte Indikator, das Entwickler-Ökosystem, ist transparent-normativ fundiert, weil die Datenquelle, der Electric Capital Developer Report, öffentliche Repository-Aktivität als Proxy für Entwickler-Netzwerkeffekte misst, eine Off-Chain-Metrik mit höherer Messunschärfe als die on-chain verifizierbaren TVL- und Stablecoin-Daten.

Koordinationsfunktion (I.3) fragt, ob Ethereum eine Koordinationsleistung bereitstellt, die ohne das System nicht oder nur mit signifikant höherem Aufwand erbracht werden könnte. Der Kriterienname und das übergreifende Muster aus der Infrastruktur-Kontextualisierung orientieren sich an der Funktion realer Infrastrukturen: Stromnetze koordinieren Angebot und Nachfrage, SWIFT koordiniert Finanznachrichten zwischen Banken, das Internet koordiniert Paketrouting zwischen Netzwerken. Drei Indikatoren operationalisieren diese Frage. Der erste ist der Koordinations-Scope, der die Breite der Koordinationsleistung misst, von reiner Settlement-Funktion bis zu Settlement, Execution, Verification und Data Availability. Der zweite ist die Layer-2-Settlement-Abhängigkeit, die misst, wie viele Layer-2-Systeme Ethereum als Koordinationspunkt nutzen. Der dritte ist die Cross-Layer-2-Composability, die die Kohärenz der Koordination erfasst, weil Ethereums stärkste Koordinationseigenschaft, die atomare Composability innerhalb einer Transaktion, auf Layer-2-Ebene verloren geht und damit die Koordinationsleistung fragmentiert.

Langfristige Stabilität (III.1) fragt, ob Ethereum über Dekaden hinweg operieren kann, ohne dass inhärente Designentscheidungen das System destabilisieren. Dieses Kriterium hat innerhalb der Strukturellen Bedingungen eine Sonderstellung als kritischste Langfrist-Bedingung, weil ohne Lösung für State Growth und Client Diversity die langfristige Tragfähigkeit nicht gewährleistet ist. Die fünf Indikatoren messen die Client-Diversität der Execution-Schicht, die Client-Diversität der Consensus-Schicht, die Existenz einer State-Growth-Mitigation-Lösung, die Stabilität der letzten fünf Protokoll-Upgrades und die Konzentration der zehn größten Validatoren. Die Grenze zur Stufe „Erfüllt" bildet die 33-Prozent-Schwelle der Blocking Minority aus Casper FFG.

Die Qualitativen Kriterien differenzieren den Grad der Eignung innerhalb der erreichten Kategorie. Sie entscheiden über das Wie, nicht über das Ob.

Offene Generativität (II.2) fragt, ob jeder permissionless auf Ethereum bauen und innovieren kann, ob also neue Anwendungen, Protokolle und Geschäftsmo-

delle ohne Gatekeeper auf dem System aufbauen können. Die drei Indikatoren messen Permissionless Deployment (kann jeder ohne Genehmigung bereitstellen?), atomare Composability (können Smart Contracts innerhalb einer Transaktion miteinander interagieren?) und Open-Source-Tooling (sind die wichtigsten Entwicklungswerkzeuge quelloffen?). Die Schwelle zwischen „Erfüllt" und „Erfüllt mit Einschränkung" liegt bei dokumentierten Gas-Limitationen und Cross-Layer-2-Einschränkungen, die die Composability fragmentieren.

Unabhängige Verifizierbarkeit (II.3) fragt, ob die Korrektheit von Smart Contracts und Protokollzustand ohne Vertrauen in Dritte überprüft werden kann. Dieses Kriterium bildet die Angebotsseite zur Vertrauenslast (I.2), deren Komplementarität dort erläutert wurde. Die Indikatoren messen die Verfügbarkeit formaler Verifikationstools, die Existenz einer formalen EVM-Spezifikation und die Verbreitung von Sicherheitsaudits als Standard vor der Veröffentlichung von DeFi-Protokollen.

Niedrigschwellige Inklusivität (II.4) fragt, ob die Teilnahme an Ethereum als Nutzer, Entwickler, Validator oder Verifizierer ohne prohibitive Barrieren möglich ist. Mit fünf Indikatoren führt dieses Kriterium neben der Langfristigen Stabilität (III.1) das zweitgrößte Indikator-Set im Bewertungsrahmen, weil Inklusivität an der Schnittstelle mehrerer Barrierentypen operiert: die Hardwareanforderungen für den Betrieb eines Full Node, die Hardwareanforderungen für den Betrieb eines Validators, der Staking-Zugang unterhalb der 32-ETH-Schwelle, die Layer-2-Transaktionskosten im Vergleich zu traditionellen Transaktionskosten und die Nutzbarkeit ohne kryptographisches Vorwissen. Der letzte Indikator ist an den Implementierungsstatus von Account Abstraction (EIP-7702) gebunden und misst die Komplexitätsbarriere: Kann ein Nutzer, der Online-Banking und App-Stores bedienen kann, aber noch nie mit Kryptowährungen interagiert hat, Ethereum nutzen? Die Fundierung dieses Indikators ist transparent-normativ, was bedeutet, dass der Leser seine Aussagekraft anders gewichten darf.

Adaptive Governance (III.2) fragt, ob Ethereum sich an veränderte Anforderungen anpassen kann, ohne dass der Anpassungsprozess selbst das System destabilisiert. Die drei Indikatoren messen die Funktionalität des EIP-Prozesses als dokumentierten Governance-Mechanismus, die Hotfix-Fähigkeit bei kritischen Bugs innerhalb von 48 bis 72 Stunden und die Fähigkeit, kontroverse Entscheidungen ohne Chain-Split zu lösen, was seit dem DAO-Fork von 2016 empirisch belegt ist.

Souveräne Portabilität (III.3) fragt, ob Ethereum frei von proprietären Abhängigkeiten ist, die einen Vendor-Lock-in erzeugen könnten. Die Indikatoren prüfen, ob die vollständige Blockchain-Historie exportiert werden kann, ob das

System vollständig Open Source mit mehreren unabhängigen Clients ist und ob Assets ohne Vertrauen in einzelne Bridges zwischen den Schichten bewegt werden können. Die Schwelle zwischen „Erfüllt“ und „Erfüllt mit Einschränkung“ liegt bei praktischen Hürden des Datenexports und bei Trust-Annahmen im Bridge-Design.

Hardware-Agnostik (III.4) fragt, ob Ethereum auf heterogener Hardware betrieben werden kann, ohne dass spezifische Hardware-Anforderungen die Teilnahme einschränken. Die drei Indikatoren messen Cloud-Unabhängigkeit (kein einzelner Provider über 50 Prozent), geographische Verteilung (Nodes über mindestens zehn Länder mit jeweils über einem Prozent) und Architektur-Support (alle großen Clients auf x86 und ARM). Dieses Kriterium nimmt unter den zwölf eine Sonderstellung ein. Keines der sieben Referenzsysteme weist das spezifische Risiko einer Cloud-Konzentration in der Form auf, wie es bei Ethereum existiert: Das Stromnetz und das Straßennetz sind physisch verteilt. Das Internet ist architektonisch dezentral. SWIFT und GPS operieren auf proprietärer Infrastruktur. Ethereum hingegen läuft auf Consumer-Hardware und Cloud-Servern, und eine Konzentration der Node-Infrastruktur auf wenige Cloud-Provider erzeugt eine physische Abhängigkeit, die die Dezentralisierung auf der logischen Schicht unterläuft. Das Kriterium ist anspruchsspezifisch motiviert: Es existiert, weil der Gegenstand es erfordert, und es ist funktional eine Voraussetzung für mehrere andere Kriterien, weil Client-Diversity (III.1) Hardware-Unabhängigkeit voraussetzt und Validator-Betrieb auf Consumer-Hardware möglich bleiben muss, um die Inklusivität (II.4) und die Jurisdiktions-Diversität (II.1) zu sichern. Die Arbeit markiert dieses Kriterium transparent als Sonderfall, dessen Berechtigung sich aus architektonischen Anforderungen des Gegenstands ergibt, die in keiner der sieben Referenzinfrastrukturen ein Analogon haben.

Kriterien-Hierarchie und Bewertungsmechanismus (M3-Kaskade)

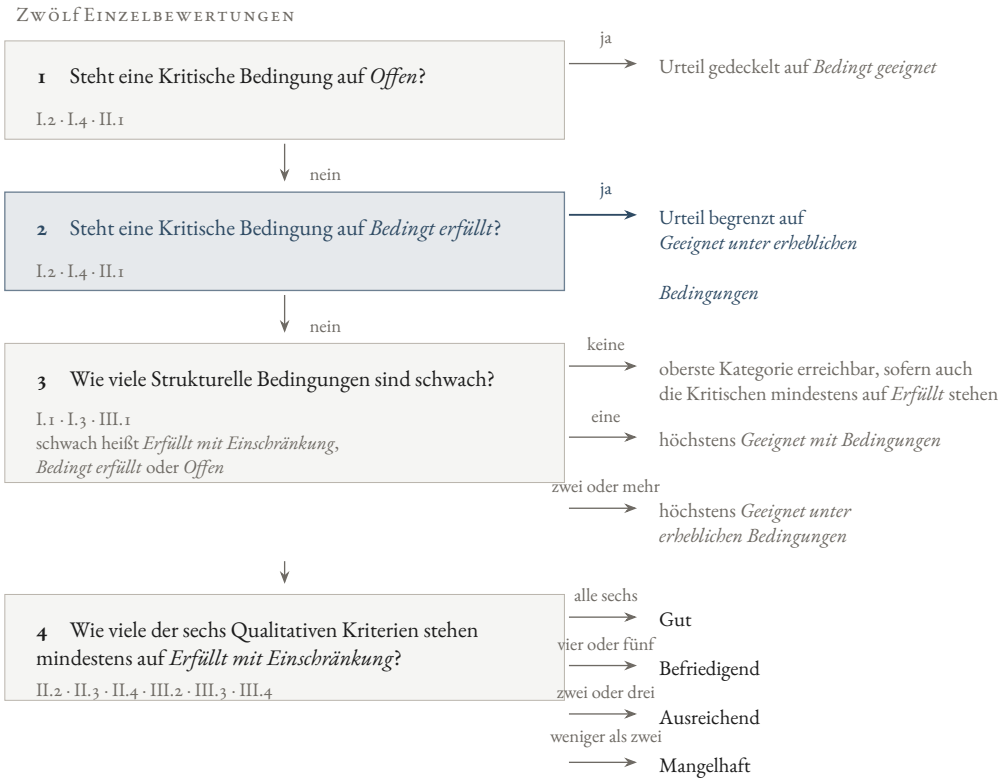
Die M3-Kaskade überführt die zwölf Einzelbewertungen in ein Gesamturteil. Die zwölf Kriterien sind in drei hierarchische Stufen gegliedert, die die Bewertungslogik bestimmen. Auf der ersten Stufe stehen die drei Kritischen Bedingungen (I.2, I.4, II.1), die das Fundament des Infrastrukturanspruchs bilden. Auf der zweiten Stufe stehen die drei Strukturellen Bedingungen (I.1, I.3, III.1), die die Tragfähigkeit des Systems bestimmen. Auf der dritten Stufe stehen die sechs Qualitativen Kriterien (II.2, II.3, II.4, III.2, III.3, III.4), die den Grad der Eignung differenzieren.

Die Kaskade prüft in einer expliziten Reihenfolge von fünf Schritten. Im ersten Schritt wird geprüft, ob mindestens eine Kritische Bedingung auf der Stufe „Offen" steht. Wenn ja, ist das Gesamturteil auf „Bedingt geeignet" gedeckelt, unabhängig von allen anderen Bewertungen. Im zweiten Schritt wird geprüft, ob mindestens eine Kritische Bedingung auf „Bedingt erfüllt" steht. Wenn ja, ist das Gesamturteil auf „Geeignet unter erheblichen Bedingungen" begrenzt. Im dritten Schritt werden die Strukturellen Bedingungen nach der Zahl ihrer schwachen Ausprägungen geprüft. Als schwach gilt jede Bedingung auf „Erfüllt mit Einschränkung", „Bedingt erfüllt" oder „Offen". Steht keine der drei Strukturellen schwach, ist die oberste Kategorie erreichbar, sofern auch die Kritischen mindestens auf „Erfüllt" stehen. Steht genau eine schwach, ist das Urteil auf höchstens „Geeignet mit Bedingungen" begrenzt. Stehen zwei oder mehr schwach, ist es auf höchstens „Geeignet unter erheblichen Bedingungen" begrenzt. Die Deckelungsprüfungen der ersten drei Schritte gehen den Positivdefinitionen der Kategorien vor: Greift eine Deckelung, bestimmt sie die höchstmögliche Kategorie, und die Positivdefinition ordnet das Urteil innerhalb dieser Obergrenze zu. Im vierten Schritt bestimmen die Qualitativen Kriterien den Grad innerhalb der erreichten Eignungskategorie, nach einer Grad-Skala von Gut (alle sechs qualitativen Kriterien mindestens auf „Erfüllt mit Einschränkung") über Befriedigend (vier oder fünf) und Ausreichend (zwei oder drei) bis Mangelhaft (weniger als zwei). Im fünften Schritt wird das Gesamturteil formuliert. Identifizierte Spannungen zwischen Kriterien gehen in die Kaskade ein, indem zu jeder Spannung der Mitigationspfad mit seinem Implementierungsstatus nach der M1-Taxonomie erfasst wird und der so bestimmte Erfüllungsgrad des betroffenen Kriteriums in den zuständigen Schritt einfließt.

Die Kaskadenregel im zweiten Schritt wurde während der Anwendung des Bewertungsrahmens ergänzt. In der ursprünglichen Fassung sah die Kaskade nur zwei Zustände für kritische Bedingungen vor: „Offen" als Deckelungsschwel-

le und alle Stufen darüber als passierbar. Die Anwendung des Bewertungsrahmens auf den IST-Zustand identifizierte eine Situation, die die binäre Unterscheidung nicht abbildete. Eine Kritische Bedingung auf „Bedingt erfüllt“ ist qualitativ ein anderer Zustand als eine auf „Erfüllt mit Einschränkung“, weil die Kerneigenschaft des Infrastrukturanspruchs noch nicht auf dem erforderlichen Niveau protokollseitig gesichert ist. Die Hierarchie definiert Kritische Bedingungen als Fundament des Infrastrukturanspruchs. Ein Fundament auf „Bedingt erfüllt“ bedeutet, dass der Pfad zur Erfüllung erkennbar, aber nicht gesichert ist, während ein Fundament auf „Erfüllt mit Einschränkung“ bedeutet, dass die Eigenschaft grundsätzlich gegeben ist, mit dokumentierten Einschränkungen. Die Kaskade muss diesen Unterschied abbilden, und die Ergänzung tut dies durch eine eigenständige Urteilskategorie. Die Ergänzung ist generisch formuliert: Sie gilt für jede Anwendung des Bewertungsrahmens, in der eine Kritische Bedingung auf „Bedingt erfüllt“ steht, unabhängig davon, welches Kriterium betroffen ist und welches System bewertet wird.

Die Kaskade erzeugt fünf mögliche Urteilskategorien, deren Definitionen klären, was eine Kategorie bedeutet und was sie ausschließt. Der Grad wird für jede erreichte Kategorie durch die Qualitativen Kriterien bestimmt. Er differenziert die Eignung innerhalb der erreichten Kategorie, ohne die Kategorie selbst zu verschieben. „Geeignet“ bedeutet, dass alle Kritischen und Strukturellen Bedingungen auf mindestens „Erfüllt“ stehen. Es bedeutet ausdrücklich nicht operative Einsatzreife, globale Skalierung oder Vollständigkeit, weil diese Faktoren Markt- und Übernahmedynamiken beschreiben, keine Infrastruktur-Eigenschaften. „Geeignet mit Bedingungen“ bedeutet, dass mindestens eine Kritische Bedingung oder genau eine Strukturelle Bedingung eine Einschränkung aufweist, solange keine Deckelungsregel einer höheren Stufe greift. Die Einschränkung qualifiziert den Anspruch, ohne ihn fundamental zu untergraben. „Geeignet unter erheblichen Bedingungen“ bedeutet, dass mindestens eine Kritische Bedingung auf „Bedingt erfüllt“ steht: Die Kerneigenschaft des Infrastrukturanspruchs ist noch nicht auf dem erforderlichen Niveau gesichert, und die Eignung ist an benannte, überprüfbare Bedingungen geknüpft. „Bedingt geeignet“ bedeutet, dass mindestens eine Kritische Bedingung auf „Offen“ steht und eine fundamentale Anforderung verfehlt wird, für die jedoch ein erkennbarer Pfad zur Erfüllung besteht. „Nicht geeignet“ bedeutet, dass fundamentale Anforderungen ohne erkennbaren Pfad zur Erfüllung verfehlt werden.



Der markierte Weg ist der des IST-Zustands. II.1 steht auf *Bedingt erfüllt*, deshalb greift Schritt 2. Schritt 3 greift ebenfalls, weil alle drei Strukturellen Bedingungen auf *Erfüllt mit Einschränkung* stehen und damit als schwach zählen.

Abbildung 2.1 Die M3-Kaskade. Die Reihenfolge, in der die zwölf Einzelbewertungen zu einem Gesamturteil zusammenlaufen.

2.3.4 Scope und Grenzen

Der Bewertungsrahmen operiert innerhalb expliziter Grenzen, die seine Aussagekraft definieren und seine Anwendbarkeit abgrenzen.

Die erste Grenze ist die Oracle-Grenze. Der Bewertungsrahmen bewertet den on-chain Zustand vollständig, also alle Eigenschaften, die protokollintern messbar sind. Was außerhalb des Protokolls liegt, kann der Bewertungsrahmen konzeptionell nicht bewerten. Die Qualität der Daten, die ins System gelangen, ist ein zentrales Beispiel: Ein Smart Contract kann die Logik einer Versicherungsauszahlung korrekt ausführen, aber wenn der Dateninput, der das auslösende Ereignis meldet, manipuliert ist, nützt die korrekte Ausführung nichts. Die regulatorische Umgebung, in der Ethereum operiert, und die gesellschaftliche Akzeptanz, die über die tatsächliche Nutzung als Infrastruktur entscheidet, sind weitere Variablen, die nicht protokollintern messbar sind und damit außerhalb des Bewertungsbereichs liegen. Die Oracle-Grenze ist eine Beschränkung zugunsten methodischer Sauberkeit: Der Bewertungsrahmen bewertet, was er bewerten kann, und dokumentiert, was er nicht bewerten kann.

Die zweite Grenze ist die Applikationsschicht-Trennlinie. Anwendungen, die auf Ethereum aufbauen, werden nur behandelt, soweit sie die Infrastruktur selbst beeinflussen. Die Trennlinie folgt einer Frage: Beeinflusst die Anwendung die Infrastruktureignung? Ein Liquid-Staking-Anbieter, dessen Marktanteil die Konsensschwellen des Protokolls berührt, ist relevant, weil seine Konzentration die Neutralität der Infrastruktur beeinflusst. Ein NFT-Marktplatz ist es nicht. Die Trennlinie wird dort angewandt, wo ein Befund über ihre Lage entscheidet, etwa an der Oracle-Grenze in Kapitel 4.

Die dritte Grenze ist die IST/SOLL-Zweiteilung. Die Arbeit bewertet zwei Zeitebenen mit demselben Bewertungsrahmen. Der IST-Zustand beschreibt, was Ethereum im ersten Quartal 2026 ist, und steht auf operativer Evidenz, also Features mit dem Taxonomie-Status IMPL. Features mit dem Status DEPL gehen ein, soweit sie das laufende System bereits prägen, tragen aber keine Bewertung allein. Der SOLL-Zustand beschreibt, was Ethereum unter Annahme vollständiger Roadmap-Umsetzung werden kann, und steht auf architektonischer Kohärenz mit abgestufter Implementierungsreife, also Features mit dem Status PLAN oder RES. Die Zweiteilung ist eine methodische Entscheidung: Ethereum ist ein evolvierendes System, dessen heutige Eigenschaften von den Eigenschaften abweichen, die die Roadmap in Aussicht stellt. Ohne die Zweiteilung müsste die Arbeit entweder den IST-Zustand bewerten und die Roadmap ignorieren, was die Dynamik des Systems ausblenden würde, oder den SOLL-Zu-

stand als gegeben annehmen, was die epistemische Unsicherheit verbergen würde. Die Zweiteilung erlaubt dem Leser, zu unterscheiden, was heute operativ belegt ist und was die Roadmap in Aussicht stellt, und die Belastbarkeit dieses Vorhabens anhand der Taxonomie-Stufen einzuschätzen. Sie zeigt, dass der Sprung zwischen dem IST- und dem SOLL-Zustand an konkrete Implementierungen gebunden ist, deren Belastbarkeit Kapitel 6 eigens analysiert.

Infrastruktureignung ist eine multidimensionale Eigenschaft, die sich einer Reduktion auf eine einzelne Kennzahl entzieht. Die Arbeit hat deshalb einen qualitativen Ansatz gewählt. Eine quantitative Bewertung würde Gewichtungen zwischen den Kriterien erfordern, die entweder willkürlich gesetzt oder aus einer größeren Stichprobe statistisch abgeleitet werden müssten. Beides ist für den Gegenstand nicht möglich: Willkürliche Gewichtungen würden eine Scheinpräzision erzeugen, die die tatsächliche Unsicherheit verbirgt, und eine statistische Ableitung scheitert daran, dass die Grundgesamtheit kryptographischer Infrastruktursysteme zu klein für statistische Verfahren ist. Die Vollständigkeit der zwölf Kriterien wird in Abschnitt 6.3 reflektiert, wo vier Eigenschaften identifiziert werden, die der Bewertungsrahmen nicht messen kann: Permissionless Composability, kryptographische Systemzustandsverifikation, dezentrale Selbstentwicklungsfähigkeit und Privacy als architektonische Infrastruktureigenschaft. Diese vier dokumentierten Grenzen des Bewertungsrahmens markieren die Stelle, an der die Validierung am Referenzmaterial an ihre Grenze stößt und der Gegenstand Eigenschaften aufweist, die keine der sieben Infrastrukturen in vergleichbarer Form zeigt.

Dass die Kriterienbewertung auf argumentativer Synthese beruht und keiner Zählregel folgt, wurde im Abschnitt zur Bewertungslogik begründet. Die methodische Begründung für dieses Vorgehen liegt in der Natur qualitativer Anwendung des Bewertungsrahmens: Die Stärke einer regelbasierten, aber interpretativen Bewertung liegt in der theoriegeleiteten Abwägung der Indikatoren, nicht in ihrer mechanischen Aggregation zu einem Punktwert. Die Transparenz des Verfahrens ermöglicht dem Leser, jede Einzelbewertung anhand der dokumentierten Evidenz und der begründeten Schlussfolgerung unabhängig nachzuvollziehen und, falls gewünscht, zu einem abweichenden Urteil zu gelangen. Dieses doppelte Ziel, das in der Kapiteleinleitung eingeführt wurde, ist eine methodische Stärke, die einen häufigen Kritikpunkt an qualitativer Forschung entschärft: Die Arbeit ist auch dann nützlich, wenn der Leser dem Urteil nicht zustimmt, weil sie die Grundlage für ein eigenständiges Urteil liefert.

Eine letzte methodische Grenze ist der Survivorship Bias in der Validierungsbasis: Die sieben Referenzinfrastrukturen sind anerkannte Systeme, gescheiterte

sind nicht enthalten, und die Validierung stützt deshalb nur die Lesart der zwölf Kriterien als notwendige Bedingungen. Abschnitt 3.3 führt diese Grenze aus.

Kapitel 3 dokumentiert die Validierung der zwölf Kriterien und die methodischen Grenzen dieses Vorgehens. Die vollständigen Einzelanalysen der sieben Infrastrukturen stehen in Abschnitt 3.1, die Konsolidierung und die Validierungsergebnisse in Abschnitt 3.2.

Kapitel 3

Infrastruktur-Kontextualisierung: Validierung der Bewertungskriterien an sieben Referenzinfrastrukturen

Kapitel 2 hat den theoretischen Rahmen dieser Arbeit dargelegt und den Bewertungsrahmen mit seinen zwölf Kriterien analytisch aus dem Begriff der fundamentalen digitalen Infrastruktur hergeleitet. Ein deduktiv konstruierter Bewertungsrahmen muss sich jedoch daran bewähren, dass seine Anforderungen nicht an der Wirklichkeit etablierter Infrastruktur vorbeigehen. Diese Bewährung leistet das vorliegende Kapitel. Es konfrontiert die zwölf Kriterien mit sieben strukturell heterogenen Referenzinfrastrukturen und prüft, ob die analytisch gewonnenen Anforderungen dort Halt finden, ob sie zwischen den Systemen zu unterscheiden vermögen und wo ein Kriterium in den Referenzsystemen kein Gegenstück besitzt. Die Prüfung ist damit Validierung, nicht Ursprung. Sie testet die Kriterien, statt sie zu erzeugen.

Die Auswahl der sieben Referenzinfrastrukturen und ihre Zuordnung zu fünf Infrastrukturtypen wurde in Kapitel 2 typologisch begründet, die Einzelbegründungen folgen hier. Die Auswahl folgte zwei Leitprinzipien: Jeder Infrastrukturtyp sollte mit mindestens einem System vertreten sein, und die gewählten Systeme sollten hinreichend dokumentiert sein, um eine quellengestützte Analyse zu ermöglichen. Innerhalb der physischen Infrastruktur wurde das Stromnetz gewählt, weil es als reguliertes natürliches Monopol der Paradigmenfall öffentlicher Infrastruktur ist, und das Straßennetz, weil es mit dem Gemeingebrauch eine rechtlich einzigartige Form des offenen Zugangs aufweist. Das Internet steht als digital-offene Infrastruktur aufgrund seiner protokollbasierten Architektur und seiner generativen Kapazität ohne Alternative. SWIFT und GPS wurden als digital-geschlossene Systeme gewählt, weil sie trotz globaler Verbreitung fundamentale Beschränkungen in Kontrolle und Zugang aufweisen und damit als Gegenbeispiele zur offenen Architektur fungieren. Cloud-Infrastruktur vertritt den hybriden Typ, weil sie faktische Infrastrukturbedeutung oh-

ne öffentlich-rechtlichen Status besitzt. Das Rechtssystem schließlich wurde als einzige nicht-technische Infrastruktur aufgenommen, weil die Frage nach Koordination und Durchsetzung ohne eine institutionelle Referenz unvollständig bliebe.

An jede der sieben Infrastrukturen werden drei Leitfragen gestellt: Was ist die Kernfunktion des Systems und warum ist sie gesellschaftlich relevant, welche Eigenschaften ermöglichen die Funktion, und was geschieht, wenn das System versagt oder manipuliert wird? Die Antworten erlauben es, jedes der zwölf Kriterien an der konkreten Ausprägung des jeweiligen Systems zu prüfen. Dieses Kapitel führt die Prüfung in drei Schritten. Es charakterisiert die sieben Infrastrukturen kompakt entlang der Leitfragen. Es hält die zwölf Kriterien gegen die Systeme und zeigt, in welcher Form und mit welcher Varianz jede Anforderung dort auftritt. Aus der Konfrontation zieht es die Bilanz für die Tragfähigkeit des Bewertungsrahmens.

3.1 Die sieben Referenzinfrastrukturen

3.1.1 Stromnetz

Das Stromnetz ist die physische Infrastruktur für die Übertragung und Verteilung elektrischer Energie von Erzeugungsanlagen zu Endverbrauchern. In Deutschland wird das Übertragungsnetz von vier Betreibern unter Aufsicht der Bundesnetzagentur betrieben, und die Transportschicht weist die Eigenschaften eines natürlichen Monopols auf: Hohe versunkene Kosten und Skaleneffekte machen den parallelen Aufbau eines zweiten Netzes physisch und ökonomisch unsinnig.[26] Die Kernfunktion des Stromnetzes, die permanente Bereitstellung elektrischer Energie für alle nachgelagerten Sektoren, ist dabei nicht durch ein alternatives System substituierbar. Kein anderer Infrastruktursektor funktioniert ohne Strom: Telekommunikation, Wasserversorgung, Verkehrssysteme, Gesundheitswesen und Finanzmärkte sind elektrisch abhängig, was das Stromnetz zu einer Meta-Infrastruktur macht, deren Ausfall kaskadierende Effekte über den eigenen Sektor hinaus erzeugt.[27]

Die infrastrukturellen Eigenschaften des Stromnetzes werden durch zwei Prinzipien geprägt. Die Schichtentrennung durch Unbundling, die Europa seit

[26] Europäische Richtlinie (EU) 2019/944 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt (Nachfolgerin der Richtlinien 96/92/EG, 2003/54/EG und 2009/72/EG). Das Unbundling-Prinzip wurde erstmals in Richtlinie 96/92/EG von 1996 eingeführt.

[27] Fraunhofer IEE: Systemsicherheit und Netzstabilität, 2023.

1996 schrittweise durchgesetzt hat, trennt Erzeugung, Transport und Vertrieb strukturell voneinander und stellt sicher, dass jeder Erzeuger einspeisen kann, ohne das Netz besitzen oder betreiben zu müssen.[28] Das Netz ist dadurch quellenneutral: Ob Strom aus einem Atomkraftwerk, einer Windanlage oder einer Solaranlage stammt, ist für die Transportschicht irrelevant. Die Regulierung durch die Bundesnetzagentur, die Netzentgelte, Investitionen und Systemstabilität überwacht, ist konstitutiv für das Funktionieren des Netzes, weil die Monopoleigenschaft der Transportschicht ohne externe Kontrolle in Diskriminierung oder Übervorteilung kippen würde.[29] Im Normalbetrieb ist das System außerordentlich stabil: Die durchschnittliche Ausfallzeit in Deutschland beträgt 10 bis 15 Minuten pro Jahr, einer der weltweit besten Werte.[30]

Die infrastrukturspezifische Beobachtung des Stromnetzes betrifft die physikalisch erzwungene Echtzeit-Koordination ohne Fehlermarge. Elektrische Energie lässt sich im Netz nicht speichern. Erzeugung und Verbrauch müssen in jedem Moment exakt im Gleichgewicht stehen, gemessen an der Netzfrequenz von 50 Hz in Europa. Abweichungen erzeugen ab einem bestimmten Schwellenwert Kaskadenversagen, weil das System keinen graduellen Qualitätsverlust kennt. Beim Blackout im Nordosten der USA und Kanada 2003 führte ein einzelner nicht zurückgeschnittener Baum zu einem Kaskadenversagen, das 55 Millionen Menschen betraf und einen wirtschaftlichen Schaden von geschätzten 4 bis 10 Milliarden US-Dollar verursachte.[31] Kein anderes der sieben untersuchten Systeme weist diese Null-Toleranz für Desynchronisation auf. Das Internet transportiert Pakete asynchron und toleriert Latenzschwankungen. Das Straßennetz organisiert sich dezentral und absorbiert lokale Störungen durch Ausweichrouten. Das Stromnetz dagegen operiert permanent an der Grenze seiner physikalischen Toleranz, und die Gesellschaft bemerkt diese Eigenschaft erst, wenn die Grenze überschritten wird. Diese Beobachtung illustriert Stars Einsicht von der Sichtbarkeit beim Zusammenbruch.[32]

---

[28] Europäische Richtlinie (EU) 2019/944, a.a.O.
[29] Bundesnetzagentur: Bericht zur Eigenkapitalverzinsung, 2024. https://www.bundesnetzagentur.de
[30] Bundesnetzagentur: SAIDI-Wert Deutschland, Monitoringbericht 2024.
[31] U.S.-Canada Power System Outage Task Force: Final Report on the August 14, 2003 Blackout, 2004.
[32] Star, Susan Leigh (1999): The Ethnography of Infrastructure. *American Behavioral Scientist*, 43(3), S. 377–391.

3.1.2 Internet (TCP/IP)

Das Internet ist ein globales Netzwerk von rund 70.000 autonomen Systemen, die über das gemeinsame Protokoll TCP/IP kommunizieren.[33] Es umfasst die physische Transportschicht aus Glasfaser, Kupfer und Funktechnik, die logische Schicht der Protokolle (TCP/IP, BGP, DNS) und die Anwendungsschicht (HTTP, SMTP und ihre Nachfolger). Die Kernfunktion besteht in der herstellerunabhängigen, technologieneutralen Vernetzung: TCP/IP abstrahiert die physische Transportschicht, sodass es für die Anwendungsebene irrelevant ist, ob Daten über Glasfaser, Kupfer oder Funk übertragen werden. Vor TCP/IP war Netzwerkkommunikation durch proprietäre, zueinander inkompatible Systeme dominiert. Das offene Protokoll ersetzte diese Monopole durch einen frei verfügbaren Standard, den jeder implementieren kann.

Die herausragenden Infrastruktureigenschaften des Internets liegen in der Kombination aus offener Protokollarchitektur und dezentraler Governance. Das Internet hat keinen Eigentümer und keinen zentralen Regulator. Stattdessen entwickelt die IETF technische Standards auf Basis von „rough consensus and running code", während ICANN das Domain Name System und die IP-Adressvergabe verwaltet.[34] 98 Prozent des internationalen Datenverkehrs fließen durch über 500 Unterwasser-Glasfaserkabelsysteme mit einer Gesamtlänge von 1,5 Millionen Kilometern, wobei die Resilienz geographisch ungleich verteilt ist: Europa und Nordamerika verfügen über massive Redundanz, während Inselstaaten durch einen einzigen Kabelbruch abgeschnitten werden können.[35][36] Im Ausfallverhalten zeigt das Internet ein fundamental anderes Muster als das Stromnetz: Es verliert typischerweise graduell an Leistung, gewinnt Latenz und verliert Bandbreite, während BGP automatisch alternative Routen berechnet.[37]

Was das Internet von den anderen Infrastrukturen unterscheidet, ist das End-to-End-Prinzip als architektonische Entscheidung, die Permissionless Innovation ermöglicht hat. Saltzer, Reed und Clark haben es 1984 formuliert: Die Intelligenz sitzt an den Endpunkten, das Netz selbst ist in dem Sinne „dumm", dass es Pakete transportiert, ohne zu wissen oder zu entscheiden, was sie enthalten.[38] Wer eine neue Anwendung bauen wollte, brauchte keine Genehmigung eines Netzbetreibers. Van Schewick hat 2010 gezeigt, dass diese Architekturei-

[33] APNIC: BGP Routing Table Analysis, 2024.
[34] IANA Functions Stewardship Transition, 2016. https://www.icann.org
[35] TeleGeography: Submarine Cable Map, 2025. https://www.submarinecablemap.com
[36] Internet Society: Submarine Cable Resilience Report, 2015.
[37] Kentik: Red Sea Cable Disruptions Impact Analysis, 2024–2025.
[38] Saltzer, Jerome H. / Reed, David P. / Clark, David D. (1984): End-to-End Arguments in System Design. *ACM Transactions on Computer Systems*, 2(4), S. 277–288.

genschaft direkte ökonomische Konsequenzen hatte. Das End-to-End-Prinzip senkte die Innovationsbarrieren auf nahezu null und ermöglichte die Entstehung von World Wide Web, E-Commerce, Cloud Computing und Social Media, ohne dass eine zentrale Instanz solche Entwicklungen hätte freischalten oder auch nur vorhersehen müssen.[39] Keine andere der untersuchten Infrastrukturen weist diese architektonisch verankerte Erlaubnisfreiheit in vergleichbarer Form auf: Das Stromnetz qualifiziert Einspeiser technisch, SWIFT bindet Zugang an Compliance, und selbst das Straßennetz kennt mit der Sondernutzungsgenehmigung eine Zugangsbeschränkung jenseits des Gemeingebrauchs.

3.1.3 Straßennetz

Das Straßennetz umfasst in Deutschland mehr als 830.000 Kilometer Verkehrswege, von Autobahnen über Bundes- und Landesstraßen bis zu kommunalen Gemeindestraßen, und ist die physisch umfangreichste von Menschen geschaffene Infrastruktur.[40] Seine Kernfunktion liegt in der flächendeckenden Erschließung: Es erreicht jeden Ort, jedes Gebäude, jede Siedlung. Weder Schiene noch Wasser- noch Luftwege leisten diese universelle Anbindung. Die letzte Meile jeder Transportkette ist fast immer eine Straße. Die ökonomische Bedeutung dieser Erschließung ist empirisch belegt: Aschauer hat für öffentliches Kapital, und darunter besonders für Verkehrswege, eine positive Output-Elastizität geschätzt und damit den Beitrag der Infrastruktur zur gesamtwirtschaftlichen Produktivität sichtbar gemacht.[41]

Die infrastrukturellen Eigenschaften des Straßennetzes sind durch die Kombination aus öffentlicher Bereitstellung und dezentralem Betrieb geprägt. Die Bereitstellung und Unterhaltung der Verkehrsinfrastruktur ist im deutschen Recht Daseinsvorsorge und damit unmittelbare Aufgabe der öffentlichen Hand, vertikal verteilt auf Bund, Länder und Kommunen.[42] Anders als beim Stromnetz mit seinen Leitwarten oder beim Internet mit seinem BGP-Routing hat das Straßennetz keine zentrale Betriebssteuerung: Jeder Verkehrsteilnehmer navigiert eigenständig, und die Koordination übernehmen dezentrale Regeln und physische Infrastruktur wie Ampeln und Beschilderung. Im Ausfallverhalten ähnelt das Straßennetz dem Internet: Lokale Ausfälle werden typischerweise durch Alternativrouten absorbiert, ohne dass das Gesamtsystem zusammenbricht, wie der Ein-

[39] Van Schewick, Barbara (2010): *Internet Architecture and Innovation*. MIT Press.
[40] Bundesministerium für Digitales und Verkehr: Verkehr in Zahlen, 2024.
[41] Aschauer, David Alan (1989): Is Public Expenditure Productive? *Journal of Monetary Economics*, 23(2), S. 177–200.
[42] Bundesfernstraßengesetz (FStrG) §§ 3 und 5; Straßengesetze der Länder.

sturz der I-35W-Brücke in Minneapolis 2007 exemplarisch gezeigt hat, der zu lokalen Verkehrsumleitungen führte, nicht zu einem systemischen Zusammenbruch des Straßennetzes.[43] Die eigentliche Bedrohung des Straßennetzes liegt im schleichenden Verfall durch Unterinvestition. Er entfaltet sich über Jahrzehnte, und die OECD beziffert die globale Infrastruktur-Finanzierungslücke auf circa eine Billion US-Dollar jährlich.[44]

Die einzigartige Eigenschaft des Straßennetzes liegt im Gemeingebrauch als Rechtsform des offenen Zugangs. Das deutsche Straßenrecht kennt den Gemeingebrauch als die widmungsgemäße, typischerweise unentgeltliche und gleichberechtigte Nutzung durch alle im Rahmen der Verkehrsregeln.[45] Der Zugang zur Straße ist ein subjektiv-öffentliches Recht, das aus der Widmung folgt und nur durch deren Änderung entzogen werden kann. Diese Konstruktion unterscheidet sich grundlegend von allen anderen Zugangsformen in der Stichprobe: Das Stromnetz bietet regulierten Zugang, der an technische Voraussetzungen und vertragliche Beziehungen gebunden ist. Das Internet erfordert einen Anschlussvertrag mit einem Provider. SWIFT beschränkt den Zugang auf zugelassene Finanzinstitutionen. Der Gemeingebrauch ist eine der ältesten Formen institutionell gesicherter Inklusivität, und er definiert den Zugang zur Infrastruktur weder technisch noch ökonomisch, sondern juristisch als Grundrecht. Frischmanns Argument, dass offener Zugang zu Infrastruktur ökonomisch effizient sein kann, findet im Gemeingebrauch seine längst etablierte rechtliche Entsprechung.[46]

3.1.4 SWIFT

SWIFT (Society for Worldwide Interbank Financial Telecommunication) ist ein Messaging-Netzwerk für standardisierte Kommunikation zwischen Finanzinstitutionen. Es überträgt Zahlungsanweisungen, Wertpapiertransaktionen und Treasury-Operationen, bewegt selbst jedoch kein Geld. Die eigentliche Wertübertragung übernehmen Korrespondenzbanken und Zahlungssysteme wie T2 in Europa oder Fedwire in den USA. Rund 11.000 Finanzinstitutionen in 212 Ländern und Territorien sind angeschlossen, bei einem geschätzten täglichen Transaktionsvolumen von circa 5 Billionen US-Dollar.[47] Die Kernfunktion von SWIFT liegt in der Standardisierung und Übermittlung von Finanznachrichten, und die Quasi-Monopolstellung beruht auf dem Netzwerkeffekt universel-

[43] National Transportation Safety Board: Collapse of I-35W Highway Bridge, Minneapolis, Minnesota, August 1, 2007. Highway Accident Report NTSB/HAR-08/03, 2008.
[44] OECD: Global Infrastructure Outlook, Infrastruktur-Finanzierungslücke, 2023.
[45] Bundesfernstraßengesetz (FStrG) §7, a.a.O.
[46] Vgl. Frischmann 2012.
[47] SWIFT: Annual Review 2024. https://www.swift.com

ler Übernahme: Chinas CIPS verarbeitete 2023 nur 6,6 Millionen Transaktionen gegenüber SWIFTs circa 11 Milliarden jährlich, obwohl es als politische Alternative konzipiert wurde.[48]

SWIFT ist als belgische Genossenschaft im Eigentum seiner Mitgliedsbanken organisiert, beaufsichtigt durch G10-Zentralbanken mit der belgischen Nationalbank als Lead Overseer. Der Zugang ist *permissioned by design*: Nur zugelassene Finanzinstitutionen können teilnehmen, Privatpersonen haben keinen direkten Zugang, und AML-, KYC- und CTF-Compliance sind Pflichtvoraussetzungen. Das eigentliche Settlement läuft über bilaterale Korrespondenzbeziehungen, eine föderierte Architektur aus unabhängigen Zahlungssystemen in verschiedenen Jurisdiktionen. Die Vertrauenskette ist für den Endnutzer lang und intransparent: Ob eine Überweisung korrekt abgewickelt wurde, kann der Endnutzer nicht selbst verifizieren, und Cross-Border-Zahlungen dauern 1 bis 3 Tage bei gestapelten Gebühren und intransparenten Zwischenständen.

Bei SWIFT zeigt sich eine Eigenschaft, die in keinem anderen System der Stichprobe in dieser Form auftritt: die Kombination aus Netzwerkeffekt als Monopolbasis und geopolitischer Instrumentalisierbarkeit. Die Alternativlosigkeit des Systems beruht auf dem Netzwerkeffekt-Lock-in, obwohl das SWIFT-Protokoll technisch replizierbar wäre. Praktisch jede Finanzsoftware weltweit verarbeitet SWIFT-Formate, und die von SWIFT etablierten Nachrichtenstandards (MT-Nachrichten, ISO 20022) haben ein Eigenleben entwickelt, das über das Netzwerk hinausreicht. Die geopolitische Dimension zeigt sich in den Sanktionsabkopplungen: 2012 wurden iranische Banken auf EU-Beschluss vom Netzwerk getrennt, 2022 russische Banken nach der Ukraine-Invasion.[49] Diese Instrumentalisierung offenbart eine Spannung, die für die Infrastrukturfrage zentral ist: SWIFT beansprucht Neutralität als Messaging-Infrastruktur, gibt diese Neutralität aber unter geopolitischem Druck selektiv auf. Die Kontrolle durch G10- und EU-Zentralbanken bedeutet de facto westliche Kontrolle über das globale Finanzmessaging. Die direkte Konsequenz ist das Fragmentierungsrisiko: Die Existenz von CIPS (China) und SPFS (Russland) als Alternativsystemen zeigt, dass eine Infrastruktur, deren Neutralität als selektiv wahrgenommen wird, Souveränitätsreaktionen auslöst und damit ihre universelle Geltung verliert.

[48] People's Bank of China: CIPS Annual Report, 2023.
[49] EU-Verordnung (EU) 2022/328 zum Ausschluss russischer Banken von SWIFT, 2022.

3.1.5 GPS

Das Global Positioning System besteht aus 31 Satelliten in sechs Orbitalebenen, die die Erde in 20.200 Kilometer Höhe umkreisen und permanent Positions- und Zeitsignale senden.[50] GPS liefert drei Funktionen (Position, Navigation und Timing) und wurde 1978 vom US-Verteidigungsministerium als militärisches System gestartet. Die zivile Nutzung begann 1983 als Reaktion auf den Abschuss der Korean Air Lines Maschine 007 und wurde 2000 durch die Abschaltung der absichtlichen Signaldegradation (Selective Availability) unter Präsident Clinton auf volle zivile Genauigkeit erweitert.[51][52] Die gesamte zivile GPS-Infrastruktur, auf die heute Finanztransaktionen, Mobilfunknetze, Stromnetze und Präzisionslandwirtschaft als Zeitreferenz angewiesen sind, ist ein unbeabsichtigtes Nebenprodukt einer militärischen Investition.

Ein fundamentaler Designunterschied prägt die infrastrukturellen Eigenschaften von GPS: Satelliten senden Signale, empfangen aber keine von Nutzern. Es gibt keine Interaktion, keine Registrierung, keine Authentifizierung. Das System skaliert perfekt, weil die Kapazität unabhängig von der Nutzerzahl ist, ob ein oder acht Milliarden Empfänger. Gleichzeitig bedeutet diese Architektur, dass zivile GPS-Signale nicht authentifiziert sind: Der Empfänger kann nicht kryptographisch beweisen, dass das empfangene Signal echt ist, und Spoofing ist möglich und dokumentiert. Nur der militärische M-Code bietet kryptographische Authentifizierung, was ein Zwei-Klassen-System auf derselben physischen Infrastruktur erzeugt: zivile Empfänger mit 5 bis 10 Meter Genauigkeit ohne Spoofing-Schutz, militärische Empfänger mit rund 1 Meter Genauigkeit und Verschlüsselung.[53]

GPS weist eine Eigenschaft auf, die die maximale Asymmetrie in der Stichprobe erzeugt: die Read-only-Architektur unter unilateraler Kontrolle. Jeder kann empfangen, niemand kann senden, einer kontrolliert. GPS wird vollständig vom US Department of Defense betrieben und durch die US Space Force operiert. Der kostenlose Zugang ist eine politische Entscheidung, die jederzeit revidiert werden könnte, und die US-Regierung behält sich explizit das Recht vor, GPS in Krisengebieten lokal zu stören. Die geopolitische Konsequenz dieser Asymmetrie ist die Duplikation: Die Europäische Union entwickelte Galileo als expli-

[50] GPS.gov: Space Segment, U.S. Government. https://www.gps.gov/systems/gps/space/

[51] Presidential Statement on the Use of GPS for Civilian Aviation Safety, September 1983, als Reaktion auf den Abschuss von KAL 007.

[52] Presidential Decision Directive (Clinton), Mai 2000: Abschaltung von Selective Availability.

[53] RAND Corporation: GPS Vulnerabilities and Alternative PNT Capabilities, 2020.

zite Souveränitätsmaßnahme, Russland betreibt GLONASS, China BeiDou.[54] Die RAND Corporation identifiziert GPS aufgrund der sektorübergreifenden Abhängigkeit als „attractive target for adversaries".[55] GPS zeigt damit eine Eigenschaft, die für die Forschungsfrage unmittelbar relevant ist: Eine Infrastruktur, die von der gesamten Welt genutzt wird, aber der souveränen Kontrolle eines einzelnen Staates unterliegt, provoziert Duplikation, die den universellen Charakter der Infrastruktur fragmentiert.

3.1.6 Cloud-Infrastruktur

Cloud-Infrastruktur stellt Compute, Storage und Networking als Service bereit. Drei Anbieter kontrollieren 63 Prozent des globalen Marktes, der 400 Milliarden US-Dollar jährlich übersteigt: AWS mit 30 Prozent, Azure mit 20 Prozent und Google Cloud mit 13 Prozent.[56] Finanzplattformen, Gesundheitssysteme, Regierungsdienste, KI-Anwendungen und Kommunikationsdienste laufen auf dieser Infrastruktur. Cloud erfordert massive Kapitalinvestitionen in globale Rechenzentren, Unterseekabel und proprietäre Hardware, was Markteintrittsbarrieren erzeugt, die für neue Wettbewerber kaum zu überwinden sind. Kunden, die ihre Anwendungen tief in anbieterspezifische Dienste integrieren, sind durch Vendor Lock-in gebunden, der aus der Ökosystemtiefe entsteht, weil die technische Integration weit über formale Vertragsbindung hinausgeht.

Die infrastrukturellen Eigenschaften der Cloud sind durch eine Spannung geprägt, die in der Stichprobe einzigartig ist. Die Skaleneffekte der großen Anbieter ermöglichen niedrigere Preise, breitere Dienste und schnellere Innovation, erzeugen aber gleichzeitig Single Points of Failure. Beim US-East-1-Vorfall im Dezember 2021 verursachte ein Netzwerkfehler kaskadierende Ausfälle bei DynamoDB, S3 und weiteren AWS-Diensten und demonstrierte, dass ein einzelner Fehler bei einem Anbieter in einer Region globale Auswirkungen haben kann.[57] Cloud-Anbieter sind privatwirtschaftliche Unternehmen ohne Infrastrukturregulierung. Es gibt keine Bundesnetzagentur für Cloud, keine Widmung, keinen Gemeingebrauchsanspruch. AWS, Azure und GCP können Kunden ablehnen, Dienste kündigen und Preise ändern. Die Verifikation der Infrastrukturintegrität ist für den Nutzer nicht unabhängig möglich: Ob die zugrunde liegende Infrastruktur korrekt funktioniert, wird durch SLAs und anbietereigene Status-Dash-

[54] European Space Agency (ESA): Why Europe Needs Galileo. https://www.esa.int/Applications/Satellite_navigation/Galileo/Why_Galileo

[55] RAND Corporation, a.a.O.

[56] Synergy Research Group: Cloud Infrastructure Market Share, Q3 2025.

[57] AWS: Summary of the AWS Service Event in the Northern Virginia (US-EAST-1) Region, Dezember 2021. https://aws.amazon.com/message/12721/

boards kommuniziert, nicht durch unabhängige Prüfmechanismen.

Die infrastrukturspezifische Beobachtung der Cloud ist die Diskrepanz zwischen De-facto-Infrastrukturbedeutung und fehlendem öffentlich-rechtlichen Status. AWS, Azure und GCP sind faktisch Infrastruktur, auf der ein erheblicher Teil der digitalen Wirtschaft läuft, aber sie haben keinen Infrastrukturstatus, keine Gemeinwohlverpflichtung, und ihre AGB können sich jederzeit ändern. Diese Diskrepanz hat regulatorische Reaktionen ausgelöst: Die EU erkennt mit dem Data Act und dem Digital Markets Act zunehmend die systemische Bedeutung der Cloud-Anbieter an und regelt mit Portabilitätsanforderungen die Datensouveränität.[58] Die genannte Marktkonzentration liegt in den Händen dreier US-Unternehmen. Europa versucht mit Initiativen wie Gaia-X eine souveräne Alternative zu schaffen.[59] Die Parallele zur GPS-Situation (US-Kontrolle provoziert europäische Souveränitätsantwort) ist direkt. Der historische Vergleich liegt nahe: Die Situation der Cloud ähnelt dem Zustand des Stromnetzes vor dem Unbundling, als die Transportschicht noch in den Händen integrierter Unternehmen lag und die regulatorische Trennung von Netz und Nutzung noch nicht vollzogen war.

[58] Europäische Kommission: Data Act (Verordnung (EU) 2023/2854), 2023; Digital Markets Act (Verordnung (EU) 2022/1925), 2022.

[59] Gaia-X European Association for Data and Cloud. https://gaia-x.eu

3.1.7 Rechtssystem

Das Rechtssystem umfasst die Gesamtheit von Gesetzen, Gerichten, Registern und Durchsetzungsmechanismen, die verbindliche Vereinbarungen zwischen Parteien ermöglichen. Es ist die einzige Infrastruktur in der Stichprobe, die institutioneller und nicht technischer Natur ist. Seine Kernfunktion löst das Grundproblem menschlicher Kooperation: Wie können Fremde verbindliche Vereinbarungen treffen? Avner Greif hat gezeigt, dass vor der Entwicklung institutionellen Rechts Transaktionen nur innerhalb von Clan-, Familien- oder ethnischen Netzwerken funktionierten, weil reputationsbasierte Durchsetzung nicht über kleine Gruppen hinaus skaliert.[60] Erst das staatlich durchgesetzte Vertragsrecht ermöglicht Kooperation zwischen Millionen Fremden. Die Effektivität dieser Infrastruktur zeigt sich daran, wie selten Gerichte tatsächlich in Anspruch genommen werden: Verträge funktionieren „im Schatten des Rechts", wie Mnookin und Kornhauser formuliert haben, weil die bloße Existenz der Durchsetzungsmöglichkeit genügt, um kooperatives Verhalten zu stabilisieren.[61]

Das Rechtssystem verwaltet den Zustand der realen Welt durch Register: Wer besitzt welches Grundstück, welche Firma existiert mit welcher Haftung, welche Vereinbarung gilt. Die Registerfunktion ist das institutionelle Äquivalent zu dem, was technische Systeme als State verwalten, wie Hodgson in seiner institutionenökonomischen Analyse des Kapitalismus herausgearbeitet hat.[62] Die Verifikation ist institutionell: Gerichtsverfahren sind grundsätzlich öffentlich, Urteile werden veröffentlicht und sind anfechtbar durch Berufung und Revision. Der Zugang zum Rechtssystem ist formell universell, faktisch aber ungleich verteilt. Die sogenannte Justice Gap, die Diskrepanz zwischen formellem Zugangsrecht und faktischer Zugänglichkeit, ist in allen Ländern dokumentiert.[63] Global existieren circa 200 Rechtssysteme mit unterschiedlichen Traditionen, die nicht interoperabel sind. Es gibt kein universelles Protokoll, das zwischen Jurisdiktionen automatisch vermittelt, und Cross-Border-Verträge müssen klären, welches Recht Anwendung findet.

Das Rechtssystem unterscheidet sich von allen anderen Infrastrukturen durch die institutionelle Durchsetzung mittels des Gewaltmonopols des Staates.

---

[60] Greif, Avner (1994): Cultural Beliefs and the Organization of Society. *Journal of Political Economy*, 102(5), S. 912–950.

[61] Mnookin, Robert H. / Kornhauser, Lewis (1979): Bargaining in the Shadow of the Law: The Case of Divorce. *Yale Law Journal*, 88(5), S. 950–997.

[62] Hodgson, Geoffrey M. (2016): *Conceptualizing Capitalism: Institutions, Evolution, Future*. University of Chicago Press.

[63] OECD / Open Society Foundations (2019): *Legal Needs Surveys and Access to Justice*. OECD Publishing, Paris. DOI: 10.1787/g2g9a36c-en.

Keine andere Infrastruktur in der Stichprobe verfügt über physische Durchsetzungsmacht: Das Stromnetz kann Strom abstellen, das Internet kann Pakete blockieren, SWIFT kann Teilnehmer ausschließen, aber keines dieser Systeme kann aktiv in die Realität eingreifen. Das Rechtssystem kann es, und diese Eigenschaft macht es zur Meta-Infrastruktur, innerhalb derer alle anderen operieren: Das Stromnetz braucht Konzessionsverträge, das Internet braucht Eigentumsrechte an Kabeln, SWIFT braucht Bankenregulierung, Cloud-Anbieter brauchen die Durchsetzbarkeit ihrer AGB. Die Frage, was Durchsetzung in einem System ohne Gewaltmonopol bedeutet, ist eine der offenen Fragen, die Ethereums Infrastrukturanspruch aufwirft und die der Bewertungsrahmen über die Koordinationsfunktion (I.3) aufgreift. Das Rechtssystem „fällt" nicht aus wie ein Stromnetz. Es erodiert durch Korruption, politische Einflussnahme, Unterfinanzierung und Vertrauensverlust, wie zahlreiche historische und gegenwärtige Beispiele belegen.[64] Ökonomische Entwicklung korreliert direkt mit der Qualität rechtsstaatlicher Institutionen, was die infrastrukturelle Bedeutung des Systems empirisch unterstreicht.

3.2 Die zwölf Kriterien im Spiegel der Referenzinfrastrukturen

Die zwölf Kriterien ordnen sich in drei Dimensionen, die zugleich die Prüfung strukturieren. Die Strukturelle Fundierung (I) fragt, ob ein System die tragenden Voraussetzungen einer Infrastruktur mitbringt. Die Qualitative Tragfähigkeit (II) fragt, ob es sie neutral, offen, überprüfbar und zugänglich einlöst. Die Resilienz und Souveränität (III) fragt, ob es unter Druck und über die Zeit Bestand hat. Innerhalb jeder Dimension verortet eine Ziffer das einzelne Kriterium, sodass die Neutralität und Zensurresistenz als erstes Kriterium der Dimension II die Kennung II.1 trägt. Die folgende Prüfung hält jedes Kriterium gegen die sieben Systeme und fragt doppelt: ob die geforderte Eigenschaft in etablierter Infrastruktur Halt findet und mit welcher Varianz sie auftritt. Gerade die Bandbreite belegt, dass ein Kriterium eine reale Unterscheidung trifft und keine einzelne Systemform zur Norm erhebt.

Die Funktionale Unersetzbarkeit (I.1) findet in allen sieben Systemen Halt, in bemerkenswert unterschiedlicher Begründung. Jede Infrastruktur erbringt eine Funktion, die kein alternatives System vergleichbar leisten kann, doch der Grund der Unersetzbarkeit variiert. Er ist physikalisch beim natürlichen Monopol der

[64] Vgl. Greif 1994, der zeigt, dass der Rückfall in clanbasierte Koordination eine direkte Folge schwacher Rechtsinstitutionen ist.

Stromtransportschicht, ökonomisch bei SWIFTs Netzwerkeffekt, institutionell bei der flächendeckenden Präsenz des Straßennetzes und souverän beim Gewaltmonopol des Rechtssystems. Das Internet verdankt seine Unersetzbarkeit der universellen Protokolladoption: TCP/IP ist als Standard so durchgesetzt, dass ein alternatives Protokoll technisch denkbar, praktisch aber nicht einführbar wäre. GPS bleibt als Timing-Referenz ohne funktionales Äquivalent, weil Galileo, BeiDou und GLONASS die Funktion zwar replizieren, GPS wegen der installierten Basis aber nur partiell ersetzen (vgl. 3.1.5). Cloud-Infrastruktur schließlich ist auf der Ebene der Skaleneffekte unersetzbar, die zugleich Qualität und Machtkonzentration erzeugen. Diese Bandbreite bestätigt eine strukturelle Verankerung, die viele Formen annimmt.

Die Sicherheits- und Vertrauenslast (I.2) und die Unabhängige Verifizierbarkeit (II.3) prüfen sich an derselben Frage: worauf das Vertrauen der Nutzer in das korrekte Funktionieren beruht. Die Referenzsysteme zeigen, warum der Bewertungsrahmen hier zwei Kriterien führt, wo eine oberflächliche Betrachtung eines erwartete. Die eine Anforderung fragt nach der Nachfrageseite, der Vertrauenslast des Nutzers, die andere nach der Angebotsseite, den Prüfmöglichkeiten der Infrastruktur, und beide können auseinanderfallen. Das Internet zeigt die Spaltung am deutlichsten: Mit TLS bietet es kryptographische Verifikation, die Angebotsseite wäre erfüllt, doch die Vertrauenskette hängt an zentralisierten Certificate Authorities, denen der Endnutzer vertrauen muss. Bei SWIFT und Cloud fehlt die Verifikationsmöglichkeit ganz, sodass beide Anforderungen zusammen negativ ausfallen. Das Stromnetz liefert die dritte Konstellation, in der die Verifikation lokal am geeichten Zähler möglich, auf Systemebene aber dem Betreiber vorbehalten bleibt. Dass Angebots- und Nachfrageseite beim Internet auseinandertreten und bei SWIFT zusammenfallen, ist der eigentliche Prüfbefund: Er belegt, dass die Trennung der beiden Kriterien keine begriffliche Verdopplung ist, sondern eine Unterscheidung, die reale Systeme erzwingen. Die Angebotsseite der Unabhängigen Verifizierbarkeit wird in der qualitativen Dimension gesondert geprüft, weil sie an einer eigenen Voraussetzung hängt, der Transparenz der Betriebsparameter.

Die Koordinationsfunktion (I.3) findet in allen sieben Systemen Halt, weil jede Infrastruktur eine Koordinationsleistung erbringt, die ohne sie nicht oder nur mit erheblich höherem Aufwand möglich wäre. Auch hier reicht das Spektrum weit. Es spannt sich von der physikalisch erzwungenen Echtzeit-Koordination beim Stromnetz, wo Erzeugung und Verbrauch sekündlich im Gleichgewicht bleiben, über die dezentrale Selbstorganisation beim Straßennetz bis zur institutionellen Durchsetzung beim Rechtssystem, das verbindliche Vereinbarun-

gen zwischen Fremden ermöglicht. Das Internet koordiniert Paketrouting zwischen 70.000 autonomen Systemen über BGP. SWIFT vermittelt Finanznachrichten zwischen 11.000 Institutionen in 212 Ländern und Territorien über standardisierte Formate. GPS liefert Timing-Signale als Zeitreferenz für Finanztransaktionen, Mobilfunk und Stromnetze. Cloud-Infrastruktur steuert die Allokation von Compute-, Storage- und Netzwerkressourcen über globale Rechenzentren. Die Art der Koordination hängt vom Infrastrukturtyp ab, die Anforderung selbst ist übergreifend: Ohne Koordinationsleistung besteht kein Infrastrukturanspruch.

Die Minimalen Tragfähigen Garantien (I.4), die eine Infrastruktur auch unter Stress aufrechterhalten muss, prüfen sich am Ausfallverhalten der sieben Systeme. Die Anforderung findet in sechs von ihnen Halt, das Rechtssystem bildet die Ausnahme, die den Zuschnitt des Kriteriums präzisiert. Die Prüfung zeigt drei distinkte Ausfallmuster. Das erste ist das Kaskadenversagen, bei dem ein lokaler Fehler sich durch das System fortpflanzt, wie der Blackout von 2003 beim Stromnetz (vgl. 3.1.1). Das zweite ist die graduelle Degradation, bei der das System Leistung verliert, aber funktionsfähig bleibt. Das Internet verliert bei Kabelbrüchen Bandbreite und gewinnt Latenz, während BGP automatisch umroutet. Das Straßennetz absorbiert lokale Ausfälle durch Alternativrouten, kennt mit Stau und Überlastung aber einen Schwellenwert, ab dem die Degradation den Infrastrukturanspruch gefährdet, weil die Koordinationsleistung zusammenbricht. Das dritte ist die redundante Stabilität mit lokaler Verwundbarkeit bei GPS: 31 Satelliten kompensieren Einzelausfälle, doch die extreme Signalschwäche aus 20.200 Kilometer Höhe macht das System gegenüber bodenbasierten Störern verwundbar. Das Rechtssystem erklärt, warum die Anforderung nur in sechs Systemen greift: Es fällt nicht technisch aus, sondern erodiert über Dekaden durch Korruption, Unterfinanzierung und Vertrauensverlust, ein Muster ohne Analogon in den technischen Infrastrukturen. Diese Ausnahme bestätigt, dass eine Infrastruktur, die bei Stress in den Totalausfall statt in kontrollierte Degradation übergeht, den Anspruch nicht einlöst.

Die Neutralität und Zensurresistenz (II.1) findet in sechs der sieben Systeme Halt, mit GPS als aufschlussreichem Gegenbeispiel. Die Prüfung ergibt zwei Befunde, deren zweiter der eigentliche ist. Der erste betrifft die Quelle der Neutralität, die nicht an eine Entstehungsform gebunden ist: Beim Internet folgt sie architektonisch aus dem End-to-End-Prinzip, das allerdings regulatorisch gegen die Interessen der Netzbetreiber durchgesetzt werden muss, beim Straßennetz ist sie juristisch im Gemeingebrauch verankert. Der zweite und wichtigere Befund ist, dass Neutralität auf zwei Ebenen auseinanderfallen kann, und ihn belegt SWIFT

am klarsten (vgl. 3.1.4): Auf der Transaktionsebene ist es neutral, weil jede Nachricht technisch gleichbehandelt wird, unter geopolitischem Druck gibt es diese Neutralität auf der Systemebene aber auf, sobald Staaten einzelne Teilnehmer ausschließen. GPS liefert das Gegenbeispiel: Im Empfang bleibt es neutral, weil jeder dasselbe Signal erhält, doch es steht unter unilateraler staatlicher Kontrolle, die es selektiv drosseln kann. Dass selbst die architektonische Neutralität des Internets physisch aushebelbar bleibt, hat die Netzabschaltung in Iran im September 2022 gezeigt. Die Prüfung darf deshalb nicht bei der Architektur stehen bleiben, sondern muss die operative Kontrollierbarkeit und beide Ebenen der Neutralität zugleich bewerten.[65]

Die Offene Generativität (II.2) bezeichnet die Fähigkeit einer Infrastruktur, unvorhergesehene Innovation ohne Genehmigung eines Gatekeepers zu tragen. Ihre begriffliche Herkunft liegt im End-to-End-Prinzip und der Permissionless-Innovation-Linie, die der theoretische Rahmen bereits führt. Am ausgeprägtesten findet die Prüfung sie im Internet, dessen Architektur die Innovationsbarriere auf nahezu null senkte und World Wide Web, E-Commerce und Cloud Computing ermöglichte, ohne dass eine zentrale Instanz sie hätte freischalten müssen. Das Straßennetz erzeugt ökonomische Generativität, weil der offene Zugang wirtschaftliche Aktivitäten ermöglicht, die ohne die Infrastruktur nicht existierten. GPS hat als unbeabsichtigtes Nebenprodukt militärischer Investitionen ein globales Ökosystem von Empfängern und Anwendungen hervorgebracht, weil die Signale kostenfrei empfangbar und die Spezifikationen offen sind. Und selbst SWIFTs Nachrichtenformate sind zu einem Industriestandard geworden, der über das Netzwerk hinausreicht. Dass die Eigenschaft nur in vier Systemen ausgeprägt auftritt, ist kein Mangel des Kriteriums, sondern bestätigt, dass Generativität eine unterscheidende Anforderung ist, die etablierte Infrastruktur in sehr unterschiedlichem Maß erfüllt.

Die Unabhängige Verifizierbarkeit (II.3), deren komplementäres Verhältnis zur Sicherheits- und Vertrauenslast die strukturelle Prüfung bereits gezeigt hat, hängt auf ihrer Angebotsseite eng an der Transparenz der Betriebsparameter. Diese tritt in allen sieben Systemen auf, ist aber kein binärer Zustand, sondern ein Spektrum, dessen Ausprägung mit dem Governance-Modell korreliert. Regulierte Infrastrukturen sind zur Transparenz verpflichtet: Beim Stromnetz sind Netzentgelte, Betriebskennzahlen und Investitionspläne regulatorisch offengelegt, beim Straßennetz Zustand und Investitionsvolumen öffentlich einsehbar.

[65] NetBlocks: Internet Shutdown in Iran during Mahsa Amini Protests, September 2022. https://netblocks.org/reports/internet-disrupted-in-iran-amid-mahsa-amini-protests-X8qVE8Ap

Offene Infrastrukturen sind architektonisch transparent, weil die Protokollspezifikationen des Internets vollständig dokumentiert sind und jeder die Routing-Tabellen von BGP einsehen kann. Geschlossene Infrastrukturen sind operativ intransparent, weil SWIFT nur aggregierte Transaktionsstatistiken kommuniziert und Cloud-Anbieter zwar SLAs und Status-Dashboards veröffentlichen, die zugrunde liegende Infrastruktur aber proprietär halten. GPS ist ein Sonderfall: Seine Signalspezifikationen sind öffentlich, sodass jeder Empfängerhersteller sie implementieren kann, während die Kontrollentscheidungen, wann und wo das Signal gedrosselt wird, unter der Hoheit des US-Verteidigungsministeriums bleiben. Diese Transparenz ist eine Voraussetzung der unabhängigen Verifizierbarkeit. Ihre Varianz bestätigt, dass die Angebotsseite des Vertrauens erst dort greift, wo die Betriebsparameter überhaupt einsehbar sind.

Die Niedrigschwellige Inklusivität (II.4) findet in allen sieben Systemen Halt, doch das Kriterium misst gerade den Ort auf einem Spektrum von maximaler Inklusivität bis zu maximaler Exklusivität. GPS steht am inklusivsten Ende, mit einem Zugang, der read-only, ohne Account, kostenlos und anonym ist. Das Straßennetz bietet mit dem Gemeingebrauch einen rechtlich gesicherten offenen Zugang, das Internet ist offen, setzt aber einen Anschlussvertrag mit einem Provider voraus. Das Stromnetz bietet regulierten Zugang, der an technische Voraussetzungen und vertragliche Beziehungen gebunden ist, das Rechtssystem ist formell universell, faktisch aber einkommensabhängig, und SWIFT steht am exklusivsten Ende, permissioned, compliance-gebunden und ohne Individualzugang. Die Anforderung wird damit nicht binär erfüllt oder verfehlt, sondern verlangt eine Verortung. Für ein bewertetes System lautet die Frage, ob die verbleibenden Zugangsschwellen mit dem Anspruch vereinbar sind, den es erhebt.

Die Langfristige Stabilität (III.1) über Dekaden findet in allen sieben Systemen Halt, und die Prüfung zeigt, dass jede Infrastruktur einem eigenen Langfristrisiko ausgesetzt ist, das ihre gegenwärtige Funktion nicht beeinträchtigt, aber ihre Zukunft bestimmt. Die Risiken fallen in deutlich verschiedene Kategorien, was der eigentliche Befund ist. Das Stromnetz trägt ein systemimmanentes Risiko, den Umbau von zentral-unidirektional zu dezentral-bidirektional, dessen Bewältigung ohne Stabilitätsverlust das zentrale Problem der Energiewende ist. GPS trägt ein fremdbestimmtes Risiko, weil sein Fortbestand von den Budgetprioritäten eines einzelnen Staates für die Satelliten-Erneuerung abhängt. SWIFT steht vor dem Fragmentierungsrisiko durch CIPS und SPFS, das die universelle Konnektivität erodieren könnte. Das Rechtssystem zeigt, dass Tragfähigkeit über technische Robustheit hinaus institutionelle Stabilität erfordert, weil demokratische Erosion die Funktionsfähigkeit von innen aushöhlen kann. Die

Varianz über diese Kategorien bestätigt, dass das Kriterium nach der spezifischen Langfristbedrohung des bewerteten Systems fragen muss und nicht nach einem einheitlichen Maß.

Die Adaptive Governance (III.2) findet in allen sieben Systemen Halt, und die Prüfung zeigt einen für das Kriterium konstitutiven Befund: Kein System zeigt dasselbe Governance-Modell. Das Spektrum reicht vom staatlichen Monopol des Rechtssystems über das regulierte private Monopol des Stromnetzes, die öffentliche Daseinsvorsorge des Straßennetzes, den Multistakeholder-Konsens des Internets, die genossenschaftliche Governance unter staatlicher Aufsicht bei SWIFT und die unilaterale Staatskontrolle bei GPS bis zum unregulierten Oligopol der Cloud. Diese Heterogenität ist der eigentliche Prüfbefund: Sie zeigt, dass kein bestimmtes Modell für Infrastruktur erforderlich ist, und deshalb fragt das Kriterium nicht nach dem Modell, sondern nach der Fähigkeit zur Anpassung, ohne dass der Anpassungsprozess das System destabilisiert. Dass das Stromnetz sich durch die Energiewende transformiert (vgl. III.1) und das Internet den Übergang der IANA-Funktionen vom US-Handelsministerium zu einer unabhängigen Multistakeholder-Organisation vollzogen hat, belegt diese Anpassungsfähigkeit in zwei sehr unterschiedlichen Governance-Formen.

Die Souveräne Portabilität (III.3) findet in fünf der sieben Systeme eine Entsprechung, wobei die Ausprägung erheblich variiert. Die Prüfung zeigt, dass Portabilität mehrschichtig zu fassen ist, weil ein System auf einer Schicht frei und auf einer anderen eingesperrt sein kann. Das Internet markiert das portable Ende des Spektrums, weil TCP/IP-Implementierungen herstellerunabhängig sind und ein Providerwechsel keine Anpassung der aufbauenden Anwendungen erfordert. Das Rechtssystem markiert das andere Ende, weil ein Jurisdiktionswechsel die vollständige Neuverhandlung der rechtlichen Grundlage verlangt, da die rund 200 Rechtssysteme nicht interoperabel sind. Die Schichtabhängigkeit tritt bei GPS am klarsten hervor: Auf der Empfängerseite ist es maximal portabel, weil standardisierte Signale jeder Empfänger verarbeitet, auf der Kontrollseite gar nicht, weil ein Anbieterwechsel mangels Alternative ausscheidet. SWIFT und Cloud zeigen schließlich, wie Netzwerkeffekte und Ökosystemtiefe einen Lock-in erzeugen, der den Wechsel nicht verbietet, aber prohibitiv verteuert. Diese Bandbreite bestätigt, dass das Kriterium die Abwesenheit proprietärer Abhängigkeit auf mehreren Schichten zugleich prüfen muss.

Die Hardware-Agnostik (III.4) ist das eine der zwölf Kriterien, das in den Referenzinfrastrukturen kein Gegenstück findet, und diese Abwesenheit ist selbst der Befund. Keines der sieben Systeme ist ein permissionless-dezentrales Netzwerk, dessen Dezentralisierung auf der logischen Schicht durch eine Hardware-

Monokultur auf der physischen Schicht unterlaufen werden könnte. Das Risiko, das dieses Kriterium erfasst, entsteht deshalb erst mit Ethereums Systemklasse. Seine Herleitung stützt sich daher nicht auf die Referenzsysteme, sondern auf den Begriff dezentraler digitaler Infrastruktur selbst. Die Prüfung bestätigt gerade durch das Fehlen eines Gegenstücks, dass etablierte Infrastruktur dieses spezifische Risiko nicht kennt, während es für ein System mit Ethereums Architektur konstitutiv ist.

Die Prüfung zeigt schließlich eine Eigenschaft, die bewusst kein Kriterium wird. Fünf der sieben Systeme fungieren als Meta-Infrastruktur, deren Ausfall über den eigenen Sektor hinaus kaskadiert: Strom bildet die physische Grundschicht, das Internet die digitale, die Straße die intermodale Verbindungsschicht, GPS die Timing-Grundschicht und das Recht die institutionelle Grundschicht. Dieser Status ist jedoch eine emergente Eigenschaft, die ein System durch Übernahme und Abhängigkeitsbildung erwirbt und auf die es nicht ausgelegt werden kann. Er gehört deshalb nicht in ein Bewertungsraster, das prüft, welche konstitutiven Eigenschaften ein System als Infrastruktur auszeichnen. Die Beobachtung wird hier festgehalten, ohne den Anspruch, die Bewertung zu tragen.

Das übergreifende Ergebnis bestätigt das Meta-Muster, das Kapitel 2 als zweites Grundprinzip der Bewertungslogik eingeführt hat: Die Ausprägung muss zum Anspruch passen. Keine der sieben Infrastrukturen erfüllt alle Anforderungen in maximaler Ausprägung, und dieser Befund verhindert den Fehlschluss, dass ein System jedes Kriterium maximal erfüllen muss, um als Infrastruktur zu gelten. Für ein System, das den Anspruch einer neutralen, permissionless, zensurresistenten Infrastruktur erhebt, sind die Anforderungen an Neutralität, Zugang und Zensurresistenz höher als für ein System ohne diesen Anspruch. Zehn der zwölf Kriterien finden in etablierter Infrastruktur Halt, in unterschiedlicher Form und mit einer Varianz, die ihre Unterscheidungskraft belegt. Das zwölfte erweist sich als anspruchsspezifische Anforderung, die gerade dort greift, wo die Referenzsysteme kein Gegenstück bieten.

		Strom	Internet	Straße	SWIFT	GPS	Cloud	Recht	Gesamtaussage
I.1	Funktionale Unersetzbarkeit	●	●	●	●	●	●	●	7 von 7
I.2	Sicherheits- und Vertrauenslast	◌	◌		○		○		ohne Gesamtaussage
I.3	Koordinationsfunktion	●	●	●	●	●	●	●	7 von 7
I.4	Minimale tragfähige Garantien	●	●	●	●	●	●	○	6 von 7
II.1	Neutralität und Zensurresistenz	●	●	●	◌	○	●	●	6 von 7
II.2	Offene Generativität	○	●	●	●	●	○	○	4 von 7
II.3	Unabhängige Verifizierbarkeit	●	●	●	○	◌	○	●	7 von 7, Spektrum
II.4	Niedrigschwellige Inklusivität	◌	●	●	○	●	●	◌	7 von 7, Spektrum
III.1	Langfristige Stabilität	●	●	●	●	●	●	●	7 von 7
III.2	Adaptive Governance	●	●	●	●	●	●	●	7 von 7
III.3	Souveräne Portabilität		●		◌	◌	◌	○	5 von 7, Spektrum
III.4	Hardware-Agnostik	○	○	○	○	○	○	○	kein Gegenstück

● findet Halt
◌ gespalten oder auf einem Spektrum verortet
○ findet keinen Halt
⋯ der Text trifft keine Aussage

Abbildung 3.1 Die zwölf Kriterien im Spiegel der sieben Referenzinfrastrukturen. Wo der Text zu einem System nichts sagt, bleibt die Zelle leer. Der Zusatz Spektrum bedeutet, dass die Gesamtaussage alle verorteten Systeme zählt, auch die am gegenläufigen Ende.

3.3 Methodische Grenzen und Positionierung

Die dokumentierte Herleitung und Validierung der Bewertungskriterien unterliegt vier Grenzen, die transparent benannt werden müssen.

Die erste Grenze ist der Survivorship Bias in der Validierungsbasis. Die sieben Referenzinfrastrukturen sind Systeme, die sich historisch als fundamentale Infrastruktur etabliert haben, während gescheiterte oder verdrängte Infrastrukturen, etwa proprietäre Netzwerkprotokolle, die von TCP/IP verdrängt wurden, oder Telex als vormals globales Kommunikationssystem, nicht enthalten sind. Die Konsequenz ist spezifisch: Die Validierung kann bestätigen, dass die Kriterien Eigenschaften erfassen, die alle erfolgreichen Referenzinfrastrukturen teilen, und sie stützt damit die Lesart der Kriterien als notwendige Bedingungen der Infrastruktureignung. Ob ihre Erfüllung hinreichend für die tatsächliche Etablierung als Infrastruktur ist, kann die Prüfung nicht beantworten, weil die Validierungsbasis keine gescheiterten Systeme enthält, an denen sich hinreichende Bedingungen ablesen ließen.

Die zweite Grenze betrifft die theoretische Prägung der Kriterienherleitung. Die Kriterien wurden aus dem Begriff der fundamentalen digitalen Infrastruktur deduziert, und die Herleitung war durch die Forschungsfrage geleitet, weil der Begriff selbst mit Blick auf ein kryptographisches, dezentrales System entfaltet wurde, sodass Eigenschaften wie Neutralität, Zensurresistenz, unabhängige Verifizierbarkeit und Herstellerunabhängigkeit stärker ins Gewicht fielen als Eigenschaften, die den Anspruch nicht berühren. Die Prägung ist normaler Bestandteil begriffsgeleiteter Konstruktion des Bewertungsrahmens und kein Mangel, aber sie muss offengelegt werden, weil sie die Frage aufwirft, welche Eigenschaften nicht als Kriterien formuliert wurden und warum. Traditionelle Infrastruktureigenschaften wie die regulatorische Einbettung in staatliche Aufsichtsstrukturen, die Existenz institutioneller Wartungsorganisationen oder Universaldienstpflichten prägen die etablierten Referenzinfrastrukturen, ohne in allen durchgängig aufzutreten. Sie wurden nicht als Kriterien formuliert, und die Entscheidung folgt einem angebbaren Unterscheidungskriterium und nicht dem Zuschnitt des Gegenstands, mit Ausnahme der Hardware-Agnostik, die unter der vierten Grenze eigens ausgewiesen wird. Konstitutiv ist eine Eigenschaft, wenn ihre Abwesenheit das System daran hindern würde, seine Infrastrukturfunktion überhaupt zu erbringen, während betriebsmodellspezifisch eine Eigenschaft ist, die beschreibt, wie eine bestimmte historische Klasse von Infrastruktur organisiert und reguliert wird, ohne dass die Funktion selbst an ihr hängt. Nach diesem Kriterium ist die regulatorische Aufsicht betriebsmodellspezifisch, weil

das Internet in seiner Protokollarchitektur seine Koordinationsfunktion ohne eine zentrale Aufsichtsbehörde erbringt, während die adaptive Governance konstitutiv ist, weil ein System, das sich nicht an veränderte Anforderungen anpassen kann, seine Funktion über die Zeit verliert. Die Anwendung des Kriteriums bleibt eine Forscherentscheidung, die hier transparent dokumentiert wird und dem Leser die Grundlage für ein eigenständiges Urteil gibt.

Die dritte Grenze betrifft die Reichweite der Validierung. Sieben Referenzsysteme prüfen die Kriterien nicht statistisch, sondern exemplarisch. Ihre Aussagekraft beruht nicht auf einer Fallzahl, sondern auf ihrer Heterogenität: Ein Kriterium, das sich an physischen, digitalen, hybriden und institutionellen Infrastrukturen zugleich bewährt, ist stärker geprüft als eines, das nur an einem Infrastrukturtyp geprüft würde, weil die strukturelle Verschiedenheit der Systeme die Chance erhöht, ein untragfähiges Kriterium an mindestens einem von ihnen scheitern zu sehen. Die Validierung erhebt deshalb keinen Anspruch auf Vollständigkeit, und weitere Infrastrukturen wie das Domain Name System, das Schienennetz oder die Telekommunikationsinfrastruktur könnten die Prüfung schärfen oder ergänzen, ohne dass ihr Fehlen die Tragfähigkeit der geprüften Kriterien in Frage stellt.

Die vierte Grenze betrifft die Positionierung des Bewertungsrahmens als Instrument. Die zwölf Kriterien erheben nicht den Anspruch, eine vollständige Theorie fundamentaler Infrastruktur zu formulieren. Sie operationalisieren Eigenschaften, die aus dem Begriff fundamentaler digitaler Infrastruktur analytisch hergeleitet und an den Referenzsystemen geprüft wurden, ergänzt um gegenstandsspezifische Anforderungen wie die Hardware-Agnostik, deren Relevanz sich aus dem Anspruch des bewerteten Systems ergibt. Der Bewertungsrahmen ist für den spezifischen Zweck konstruiert, die Forschungsfrage dieser Arbeit zu beantworten, und seine Anwendbarkeit auf andere Systeme oder andere Forschungsfragen wäre eine eigenständige methodische Frage, die diese Arbeit nicht behandelt. Die Kriterien sind anspruchskalibriert: Eine Infrastruktur mit einem anderen Anspruchsprofil als dem Ethereums, etwa eine rein nationale, regulierte Infrastruktur, würde andere oder weniger Kriterien erfordern.

Die zwölf Bewertungskriterien sind an sieben Referenzinfrastrukturen geprüft, ihre Validierung ist dokumentiert und ihre Grenzen sind benannt. Kapitel 4 wendet die Kriterien auf den IST-Zustand von Ethereum an, auf die Architektur, die operative Realität und die Frage, ob das Zusammenspiel aus beidem den Infrastrukturanspruch einlöst, den das System erhebt.

Kapitel 4

IST-Bewertung: Ethereum im operativen Zustand Q1 2026

Die vorangegangenen Kapitel haben den theoretischen Rahmen dargelegt und die empirische Grundlage geschaffen, auf der die Bewertung des konkreten Gegenstands aufbauen kann. Kapitel 2 hat den Bewertungsrahmen mit seinen zwölf Kriterien in drei Hierarchiestufen vorgestellt, die Bewertungslogik mit ihrer vierstufigen Skala und der M3-Kaskade dokumentiert und die Scope-Grenzen der Untersuchung definiert. Kapitel 3 hat die zwölf Kriterien, die Kapitel 2 analytisch aus dem Infrastrukturbegriff hergeleitet hat, an sieben strukturell unterschiedlichen Referenzinfrastrukturen validiert. Sie kommen nun zur Anwendung. Die Kriterien, geordnet in Kritische Bedingungen, Strukturelle Bedingungen und Qualitative Kriterien, bilden das Raster, durch das der Gegenstand betrachtet wird. Der Leser verfügt damit über das Instrumentarium, aber noch nicht über den Gegenstand: Ethereum als System ist bislang nur in Bezug auf die Forschungsfrage benannt, nicht beschrieben worden.

Dieses Kapitel schließt diese Lücke in zwei Schritten. Die Abschnitte 4.1 bis 4.6 beschreiben Ethereums Architektur, den Transaktionslebenszyklus, die Sicherheitsökonomie, das Skalierungsmodell, die Governance-Strukturen und die institutionelle Einbettung des Systems im operativen Zustand des ersten Quartals 2026. Diese Beschreibung ist keine Aufzählung technischer Merkmale, sondern der Versuch, das System als zusammenhängendes Ganzes verständlich zu machen, in dem jede Komponente ihre Funktion aus dem Zusammenspiel mit anderen Komponenten bezieht. Die Abschnitte 4.7 bis 4.10 wenden die zwölf Kriterien auf diesen beschriebenen Gegenstand an, bewerten jedes Kriterium einzeln auf der vierstufigen Skala, synthetisieren die Einzelbewertungen zu einem dimensionsbasierten Profil und formulieren das M3-Gesamturteil zum IST-Zustand.

Der Scope-Hinweis aus Kapitel 2 gilt unverändert: Der IST-Zustand umfasst Features, die auf dem Ethereum-Mainnet implementiert und operativ sind (Status IMPL) oder die nach der Taxonomie aus Abschnitt 2.2 den Status DEPL tragen. Features mit Status PLAN oder RES werden in Kapitel 5 bewertet, das den SOLL-Zustand der Ethereum-Roadmap analysiert. Der Stichtag für alle Netzwerkdaten ist der 27. März 2026, sofern nicht anders angegeben. Am Ende dieses Kapitels wird der Leser ein vollständiges Systembild, eine begründete Bewertung jedes einzelnen Kriteriums und ein IST-Profil haben, das die Stärken und die Einschränkungen des Systems gleichermaßen sichtbar macht.

Neben diesem sachlichen Scope tritt ein zeitlicher Vorbehalt, der für die Lektüre der folgenden Abschnitte ebenso konstitutiv ist. Sämtliche quantitativen Kennzahlen dieses Kapitels bilden den Stand des ersten Quartals 2026 ab, erhoben zum genannten Stichtag, und sie sind als Momentaufnahmen einer lebenden Infrastruktur zu verstehen, deren Marktanteile, Validatorenzahlen und Wertaggregate sich fortlaufend verschieben. Die zugrunde liegende Architektur und die aus ihr abgeleiteten strukturellen Befunde besitzen demgegenüber eine erheblich größere Beständigkeit, sodass im weiteren Verlauf nicht der exakte Betrag einer einzelnen Zahl die Argumentation trägt, sondern die Größenordnung und die Richtung, die sie markiert. Eine spätere Fortschreibung dieser Werte würde mithin die empirische Grundlage aktualisieren, ohne die Logik der Bewertung zu berühren.

4.1 Architektonische Grundlagen

Historische Einordnung und Entwicklungspfad

Ethereum wurde am 30. Juli 2015 als öffentliches Netzwerk gestartet, finanziert durch einen Crowdsale im Jahr 2014, und unterschied sich von Beginn an durch eine zentrale Designentscheidung von der damals dominierenden Blockchain-Technologie Bitcoin: Es war nicht als Zahlungssystem konzipiert, sondern als programmierbare Plattform, auf der beliebiger Code ausgeführt werden konnte.[66] Das Whitepaper, das Vitalik Buterin 2014 veröffentlichte, beschrieb ein System, in dem Smart Contracts als selbstausführende Programme auf einer gemeinsamen Zustandsdatenbank operieren, die von einem dezentralen Netzwerk gleichberechtigter Nodes gepflegt wird. Die technische Spezifikation dieses Sys-

[66] Buterin, Vitalik (2014): A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum Whitepaper. URL: https://ethereum.org/en/whitepaper/

tems legte Gavin Wood im selben Jahr im Yellow Paper vor, das die Ethereum Virtual Machine formal definierte und bis heute, in seiner aktuellen Berlin-Version von 2024, als Referenzdokument für die Protokollmechanik dient.[67]

In den ersten sieben Jahren operierte Ethereum unter einem Proof-of-Work-Konsensmechanismus, bei dem Miner durch den Einsatz von Rechenleistung um das Recht konkurrierten, neue Blöcke zu produzieren. Am 15. September 2022 vollzog das Netzwerk mit dem sogenannten Merge den Übergang zu Proof of Stake, einem Konsensmechanismus, bei dem Validatoren durch das Hinterlegen von Kapital die Berechtigung zur Blockproduktion erwerben. Die fundamentale Idee hinter Proof of Stake ist, Netzwerksicherheit durch ökonomischen Einsatz statt durch Rechenleistung herzustellen: Validatoren hinterlegen Kapital als Sicherheit und riskieren dessen Verlust bei Fehlverhalten, sodass das ökonomische Risiko den Energieaufwand als Sicherheitsmechanismus ersetzt. Die Konsequenz ist ein System, in dem die Sicherheit proportional zum gebundenen Kapital steigt, nicht proportional zum Stromverbrauch, und in dem die Kosten eines Angriffs direkt in der Höhe des zu riskierenden Kapitals messbar werden. Der Merge war ein technisches Ereignis von erheblicher Komplexität, weil ein laufendes System mit einem Gesamtwert von über hundert Milliarden US-Dollar im Betrieb umgestellt wurde, ohne dass eine einzige Transaktion verloren ging oder das Netzwerk pausierte, und reduzierte den Energieverbrauch des Netzwerks um 99,95 Prozent.[68] Die Beacon Chain, die das Proof-of-Stake-System implementiert, war bereits am 1. Dezember 2020 gestartet und hatte über 21 Monate parallel zum bestehenden Proof-of-Work-System operiert, bevor beide Schichten zusammengeführt wurden. Der Merge war nicht der erste kritische Moment in der Geschichte des Netzwerks: Im Juni 2016, kaum ein Jahr nach dem Start, wurde die erste dezentrale autonome Organisation auf Ethereum, die schlicht als The DAO bekannt wurde, durch eine Schwachstelle im Smart-Contract-Code exploitet, wobei circa 60 Millionen US-Dollar an ETH abgezogen wurden. Die Ethereum-Community entschied sich für einen Hard Fork, der die Transaktion rückgängig machte, eine Entscheidung, die das Netzwerk in Ethereum und Ethereum Classic spaltete und eine Grundsatzdebatte über die Unveränderbarkeit von Blockchain-Transaktionen auslöste. Für den Gegenstand dieser Arbeit ist der DAO-Fork aus zwei Gründen relevant: Er zeigt, dass Ethereums Commu-

[67] Wood, Gavin (2014/2024): Ethereum: A Secure Decentralised Generalised Transaction Ledger (Yellow Paper). Aktuelle Version: Berlin Version, 2024.

[68] Ethereum Foundation Blog (2022): The Merge. URL: https://blog.ethereum.org/2022/09/15/the-merge. Für den Energieverbrauchsvergleich vgl. Digiconomist: Ethereum Energy Consumption Index. Cambridge Centre for Alternative Finance (2022): Cambridge Blockchain Network Sustainability Index.

nity in einer existenziellen Krise handlungsfähig war, und er markiert den historischen Moment, nach dem die Community faktisch entschied, dass eine soziale Intervention in den Zustand des Systems möglich ist, auch wenn sie seither nie wiederholt wurde.

Seit dem Merge hat Ethereum vier Protokoll-Upgrades durchlaufen, deren Kadenz die Weiterentwicklungsfähigkeit des Systems illustriert. Shapella im April 2023 ermöglichte erstmals die Entnahme von gestaktem ETH, das bis dahin seit dem Start der Beacon Chain im Dezember 2020 eingefroren war, und beseitigte damit ein Risiko, das Staker über zwei Jahre lang getragen hatten. Dencun im März 2024 führte Blob-Transactions ein, eine neue Transaktionsform, die Layer-2-Rollups ermöglicht, Daten zu einem Bruchteil der bisherigen Kosten auf der Basisschicht zu verankern, und eröffnete damit die architektonische Grundlage für die Rollup-zentrische Skalierungsstrategie, die Abschnitt 4.4 beschreibt. Pectra am 7. Mai 2025 erhöhte die maximale Effective Balance pro Validator von 32 auf 2.048 ETH, reduzierte die Deposit-Finalisierung von zwölf Stunden auf rund 13 Minuten und führte mit EIP-7702 die erste protokollnative Form von Account Abstraction ein. Fusaka am 3. Dezember 2025 implementierte PeerDAS, ein Peer-to-Peer-basiertes Data Availability Sampling, das die Bandbreitenanforderungen an Validatoren um rund 85 Prozent reduziert und die Kapazität für Blob-Daten erweitert. Jedes dieser Upgrades wurde als Hard Fork durchgeführt, bei dem alle Node-Betreiber ihre Software aktualisieren mussten, um im Netzwerk zu verbleiben.

Die Zwei-Client-Architektur

Das Ethereum-Netzwerk besteht aus 14.339 Nodes, die über das öffentliche Internet verteilt sind und gemeinsam den Zustand des Systems pflegen.[69] Nicht jeder Node ist ein Validator: Ein Validator ist ein Node, dessen Betreiber mindestens 32 ETH als Sicherheit hinterlegt hat und dadurch das Recht erwirbt, am Konsensprozess teilzunehmen, Blöcke vorzuschlagen und Attestationen abzugeben. Die 964.768 aktiven Validatoren, die Abschnitt 4.3 im Detail beschreibt, bilden eine Teilmenge des Netzwerks. Die übrigen Nodes validieren Transaktionen und pflegen den Systemzustand, ohne direkt am Konsens teilzunehmen. Der Begriff Node bezeichnet einen Rechner, der die Ethereum-Protokollsoftware ausführt und mit anderen Nodes kommuniziert, um Transaktionen zu verbreiten,

[69] Etherscan: Ethereum Node Tracker. URL: https://etherscan.io/nodetracker (abgerufen am 27.03.2026). Für die Ethereum Foundation Dokumentation der Client-Architektur vgl. https://ethereum.org/en/developers/docs/nodes-and-clients/

Blöcke zu validieren und den aktuellen Systemzustand zu synchronisieren. Jeder Node betreibt gleichzeitig zwei Software-Komponenten: einen Consensus Layer Client, der den Proof-of-Stake-Konsens verwaltet, Validator-Zuweisungen koordiniert und über das libP2P-Netzwerkprotokoll mit anderen Consensus-Clients kommuniziert, und einen Execution Layer Client, der Smart Contracts ausführt, den Zustand der Konten und Verträge pflegt und über das DevP2P-Protokoll Transaktionen propagiert. Beide Clients sind über die Engine API verbunden, eine interne Schnittstelle auf Port 8551, die durch JWT-Token authentifiziert wird und über die der Consensus Client den Execution Client anweist, welche Blöcke auszuführen und welche Zustandsänderungen zu übernehmen sind. Der Consensus Client entscheidet, welcher Block kanonisch ist. Der Execution Client führt die Transaktionen in diesem Block aus und gibt die Ergebnisse zur Verifikation zurück.

Die Architektur sieht vor, dass für jede der beiden Schichten mehrere unabhängige Client-Implementierungen existieren. Fünf Consensus Layer Clients stehen zur Verfügung: Lighthouse, in Rust geschrieben und von Sigma Prime entwickelt, Prysm in Go von Prysmatic Labs, Teku in Java von ConsenSys, Nimbus in Nim von der Status-Organisation und Lodestar in TypeScript von ChainSafe. Ebenso fünf Execution Layer Clients: Geth in Go, der am längsten etablierte und am umfangreichsten getestete Client, Nethermind in C#, Besu in Java mit Fokus auf Enterprise-Anforderungen, Erigon in Go mit optimierter Speichereffizienz und Reth in Rust als jüngste Implementierung mit einer modernen Codebasis. Alle zehn Implementierungen sind Open Source, in unterschiedlichen Programmiersprachen geschrieben und von unabhängigen Teams entwickelt. Diese Multi-Client-Philosophie ist keine organisatorische Präferenz, sondern eine Kern-Sicherheitseigenschaft des Systems: Ein Bug in einer Software-Implementierung kann das Netzwerk nur dann gefährden, wenn der betroffene Client mehr als ein Drittel des Netzwerks bedient, weil ab dieser Schwelle die Finalisierung von Blöcken blockiert werden kann.

Der Dezember-2025-Vorfall bei Fusaka liefert eine empirische Validierung dieses Designprinzips. Ein Bug im Consensus Client Prysm führte dazu, dass die Netzwerk-Partizipation auf 75 Prozent fiel, doch die Finalisierung blieb ununterbrochen, weil Prysms Marktanteil zu diesem Zeitpunkt bei 22 Prozent lag.[70] Wäre derselbe Bug Anfang 2022 aufgetreten, als Prysm noch 68 Prozent des Netzwerks bediente, hätte die Partizipation unter die kritische Zwei-Drittel-Schwel-

[70] Cointelegraph (2025): Ethereum sees 25% validation drop post-Fusaka as Prysm bug affects network participation. Dezember 2025. Für historische Client-Marktanteile vgl. clientdiversity.org.

le fallen und die Finalisierung zum Stillstand bringen können. Die Client-Diversität wirkt als strukturelle Fehlerisolierung, deren Schutzwirkung von der tatsächlichen Verteilung der Marktanteile abhängt. Die Geschichte des Netzwerks zeigt, dass diese Verteilung das Ergebnis aktiver Community-Arbeit ist, getrieben durch Aufklärungskampagnen, wirtschaftliche Anreize und die wiederholte öffentliche Thematisierung der Gefahren einer Supermajority-Konzentration, und kein automatischer Gleichgewichtszustand.

Die geographische und infrastrukturelle Verteilung der Nodes liefert Kontextdaten, die für die spätere Bewertung relevant sind. 39 Prozent der Nodes befinden sich in den USA, 14,5 Prozent in Deutschland und 14 Prozent in China, was eine Konzentration auf den nordamerikanischen, europäischen und ostasiatischen Raum zeigt, die Jurisdiktionsrisiken für das System erzeugt. Von den gehosteten Execution Layer Nodes laufen 59 Prozent auf drei Cloud-Providern: AWS mit 35,5 Prozent, Hetzner mit 13,8 Prozent und OVHcloud mit 9,7 Prozent.[71] Dieser Wert ist seit 2022 rückläufig, als die Cloud-Konzentration noch höher lag, bleibt aber ein relevanter Faktor für die Frage, wie unabhängig das Netzwerk von einzelnen Infrastrukturanbietern operieren kann. Ein koordinierter Ausfall oder eine regulatorische Maßnahme gegen diese drei Provider würde die Mehrzahl der gehosteten Nodes betreffen, auch wenn das Netzwerk weiter operieren würde, solange die Gesamtzahl der aktiven Nodes über der für Konsens erforderlichen Schwelle bleibt.

[71] Ethernodes: Ethereum Node Distribution. URL: https://ethernodes.org (abgerufen Anfang 2026). Die Cloud-Prozentsätze beziehen sich auf gehostete EL-Nodes, nicht auf die Gesamtheit aller Nodes, da ein Teil der Nodes auf privater Hardware betrieben wird.

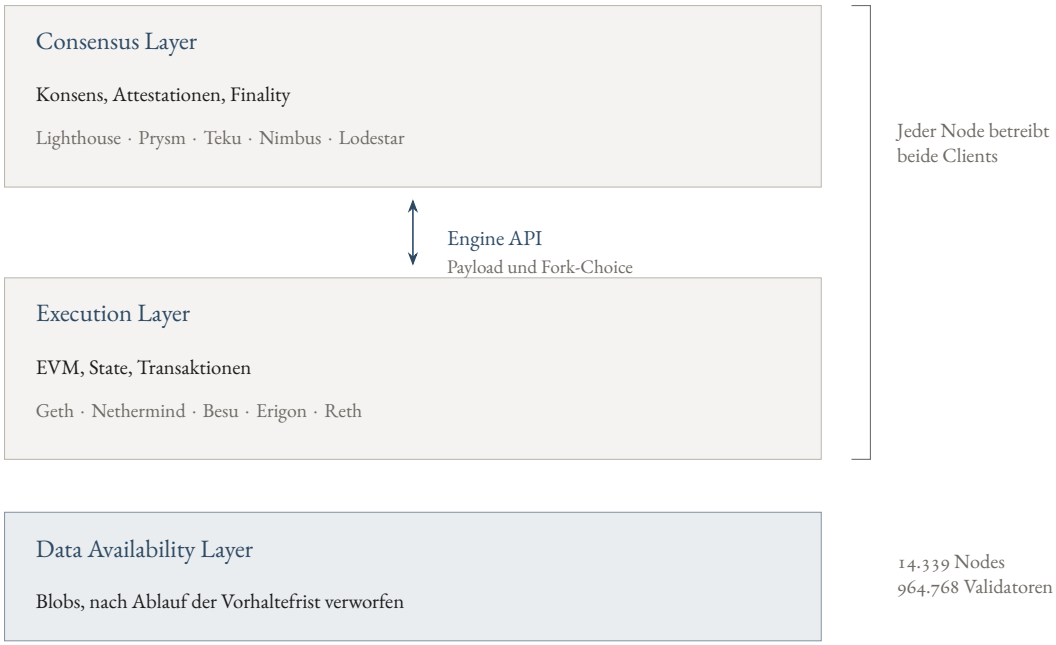


Abbildung 4.1 Ethereums Schichtenmodell. Consensus Layer und Execution Layer, verbunden über die Engine API, dazu die Schicht der Datenverfügbarkeit.

Die EVM als programmierbare Ausführungsumgebung

Was Ethereum von einer reinen Zahlungskette wie Bitcoin unterscheidet, ist die Ethereum Virtual Machine. Die EVM ist eine deterministische 256-Bit-Stack-Maschine: Jeder Node im Netzwerk führt denselben Code mit denselben Eingaben aus und kommt zwingend zum selben Ergebnis.[72] Die 256-Bit-Wortgröße wurde gewählt, um Keccak-256-Hashing und die secp256k1-Kryptographie, die Ethereum für Signaturen verwendet, in einzelnen Operationen verarbeiten zu können. Der Stack hält maximal 1.024 Elemente, und ein Call-Depth-Limit verhindert unendliche Rekursion. Diese Determinismus-Eigenschaft ist konstitutiv für das Funktionieren des Systems, weil sie die Grundlage dafür bildet, dass alle Nodes über den korrekten Zustand übereinstimmen können, ohne sich untereinander darüber abstimmen zu müssen, welches Ergebnis einer Berechnung richtig ist. Die Übereinstimmung ergibt sich aus der Tatsache, dass identische Inputs auf einer identischen Maschine identische Outputs erzeugen müssen.

Die EVM operiert mit einem dreistufigen Speichermodell, das die Zuständigkeiten nach Persistenz und Kosten trennt. Der Stack ist eine volatile Datenstruktur nach dem Last-In-First-Out-Prinzip, die als Arbeitsspeicher für die unmittel-

[72] Wood, Gavin (2014/2024): Ethereum: A Secure Decentralised Generalised Transaction Ledger (Yellow Paper). Aktuelle Version: Berlin Version, 2024.

baren Operanden der Opcodes dient und nach dem Ende eines Funktionsaufrufs gelöscht wird. Der Memory ist ein volatiler, byte-adressierbarer Speicherbereich, der innerhalb einer Transaktion als temporärer Arbeitsbereich dient und dessen Kosten quadratisch mit der Größe wachsen, eine Designentscheidung, die exzessiven Speicherverbrauch ökonomisch bestraft. Der Storage schließlich ist der persistente Speicher, dessen Inhalte im Merkle Patricia Trie verankert sind und über Transaktionen hinweg erhalten bleiben. Storage-Operationen sind die teuersten im gesamten Opcode-Set, weil jeder geschriebene Wert von allen Nodes auf unbestimmte Zeit gespeichert werden muss. Diese Kostenstaffelung ist eine ökonomische Übersetzung der technischen Realität: Was das Netzwerk dauerhaft belastet, kostet mehr als das, was nur temporär existiert.

Smart Contracts sind Programme, die auf der EVM ausgeführt werden. Sie werden als Bytecode, einer maschinennahen Repräsentation des Programmcodes, auf dem Netzwerk deployt und sind danach unveränderbar: Der Code kann nicht mehr modifiziert werden, und die Regeln, die der Code implementiert, gelten so lange das Netzwerk existiert. Die Unveränderbarkeit ist eine Konsequenz der Datenstruktur, in der der Code gespeichert wird: Der Code-Hash eines Contract Accounts ist Teil des Zustandstrie und wird durch den Konsensmechanismus geschützt wie jeder andere Zustandseintrag. In der Praxis existieren Upgradeability Patterns, bei denen ein Proxy-Contract Aufrufe an eine austauschbare Implementierung weiterleitet, aber diese Patterns operieren auf der Anwendungsschicht und ändern nicht den deployten Bytecode selbst. Das Deployment ist permissionless, die einzige Voraussetzung sind Gas-Gebühren, die an das Netzwerk gezahlt werden. Jeder Akteur kann Code deployen, ohne eine Genehmigung einholen zu müssen, und jeder andere Akteur kann diesen Code aufrufen, solange er die Gebühren trägt. Die Ausführungsarchitektur ist sequentiell: Alle Transaktionen innerhalb eines Blocks werden strikt in Reihenfolge abgearbeitet, eine Transaktion nach der anderen, ohne Parallelisierung. Diese Eigenschaft ist eine bewusste Designentscheidung zugunsten des Determinismus, weil parallele Ausführung Konflikte bei gleichzeitigen Zugriffen auf denselben Speicherbereich erzeugen kann, die den Determinismus gefährden würden. Der Preis dieser Entscheidung ist ein begrenzter Durchsatz auf der Basisschicht: Bei einer Slotzeit von 12 Sekunden und dem aktuellen Gas Limit von 60.000.000 verarbeitet Ethereum auf Layer 1 durchschnittlich 15 bis 30 Transaktionen pro Sekunde bei gemischter Transaktionskomplexität, mit einem theoretischen Maximum von 238 Transaktionen pro Sekunde für einfache ETH-Transfers und einem praktischen Durchsatz am unteren Rand dieses Bereichs für komplexe DeFi-Interaktionen. Diese Kapazitätsgrenzen sind

der architektonische Grund für die Rollup-zentrische Skalierungsstrategie, die Ethereum seit 2020 verfolgt: Die Basisschicht priorisiert Sicherheit und Dezentralisierung, während Layer-2-Systeme den Durchsatz vervielfachen, indem sie Transaktionen außerhalb der Basisschicht ausführen und die Ergebnisse auf Layer 1 verankern.

Ethereum operiert als vollständig transparentes System: Jede Transaktion, jeder Kontostand und jeder Smart-Contract-Zustand ist für jeden Netzwerkteilnehmer einsehbar. Es gibt keine nativen Privacy-Mechanismen auf Protokollebene, weder Sender noch Empfänger noch Transaktionsbetrag sind verschleiert. Diese Transparenz ist eine Konsequenz der Verifikationsarchitektur, die erfordert, dass alle Nodes denselben Zustand nachvollziehen können, und sie erzeugt eine Eigenschaft, die für manche Anwendungsfälle eine Stärke ist, vor allem Auditierbarkeit und Nachvollziehbarkeit, und für andere eine fundamentale Einschränkung, insbesondere für institutionelle Akteure mit Datenschutzanforderungen und Nutzer mit Privatsphärebedürfnis.

Innerhalb eines Blocks ermöglicht die EVM eine Eigenschaft, die in traditionellen Finanzsystemen kein Äquivalent hat: atomare Composability. Beliebig viele Smart-Contract-Interaktionen können innerhalb einer einzigen Transaktion verkettet werden, und die gesamte Kette wird entweder vollständig ausgeführt oder vollständig zurückgesetzt, ohne Teilzustände zu hinterlassen. Flash Loans illustrieren diese Eigenschaft: Ein Nutzer kann in einer einzigen Transaktion Millionen US-Dollar leihen, die geliehenen Mittel für eine Arbitrage-Operation zwischen dezentralen Börsen einsetzen und den Kredit in derselben Transaktion zurückzahlen, ohne Sicherheiten hinterlegen zu müssen und ohne dass ein Intermediär die Transaktion genehmigt. Wenn die Rückzahlung am Ende der Transaktion nicht gelingt, wird die gesamte Transaktion rückgängig gemacht, als hätte sie nie stattgefunden. Diese Eigenschaft ist eine emergente Konsequenz der sequentiellen Ausführungsarchitektur und der atomaren Zustandsänderungen der EVM, und sie bildet die Grundlage für das Ökosystem der Decentralized Finance. Decentralized Finance, abgekürzt DeFi, bezeichnet das Ökosystem dezentraler Finanzprotokolle, die als Smart Contracts auf Ethereum operieren und Finanzdienstleistungen wie Kreditvergabe, Handel, Derivate und Vermögensverwaltung ohne institutionelle Intermediäre ermöglichen. In diesem Ökosystem bauen Protokolle aufeinander auf, ohne bilaterale Vereinbarungen treffen zu müssen, weil die Kompatibilität auf der Ebene der gemeinsamen Ausführungsumgebung hergestellt wird. Ein Lending-Protokoll kann die Liquiditätspools eines dezentralen Börsenprotokolls als Preisquelle nutzen, ein Derivate-Protokoll kann Positionen in einem Lending-Protokoll als Sicherheit akzeptie-

ren, und ein Yield-Aggregator kann alle drei in einer einzigen Transaktion orchestrieren. Die Composability erzeugt Netzwerkeffekte auf der Protokollebene: Jeder neue Smart Contract, der auf bestehenden Protokollen aufbaut, erhöht den Nutzen aller beteiligten Protokolle, weil er neue Kombinationsmöglichkeiten eröffnet. Die Kehrseite dieser Vernetzung sind systemische Risiken, weil ein Fehler oder ein ökonomischer Exploit in einem zentralen Protokoll durch die Composability-Ketten kaskadierende Effekte auf abhängige Protokolle erzeugen kann, wie mehrere DeFi-Exploits in den Jahren 2020 bis 2023 gezeigt haben.

Die Determinismus-Eigenschaft der EVM ermöglicht eine weitere infrastrukturell relevante Praxis: die formale Verifikation und das systematische Auditing von Smart Contracts. Werkzeuge wie Certora Prover, Slither, Echidna und Mythril erlauben die automatisierte Prüfung von Smart-Contract-Code auf Sicherheitslücken und logische Fehler, und für Tier-1-DeFi-Protokolle ist ein unabhängiges Audit durch spezialisierte Sicherheitsfirmen vor dem Deployment Branchenstandard. Die EVM-Spezifikation selbst ist formalisiert: Das Yellow Paper definiert die Semantik, und KEVM bietet eine maschinenverifizierte Formalisierung, was die Grundlage für maschinelle Verifikation schafft und für die spätere Bewertung der unabhängigen Verifizierbarkeit (II.3) eine relevante Voraussetzung darstellt.

Account Abstraction

Ethereum kennt historisch zwei Typen von Accounts. Externally Owned Accounts werden durch einen einzelnen kryptographischen Schlüssel kontrolliert, den der Nutzer selbst verwahrt: eine Zeichenfolge aus 64 hexadezimalen Zeichen, deren Verlust den unwiederbringlichen Verlust aller Vermögenswerte auf dem zugehörigen Account bedeutet. Contract Accounts werden durch Code kontrolliert, der auf der EVM läuft und dessen Verhalten durch die Programmlogik determiniert ist. Diese Trennung erzeugte in der Praxis erhebliche Nutzbarkeitsbarrieren: Das Management der Seed Phrase, einer menschenlesbaren Repräsentation des privaten Schlüssels, wurde zur zentralen Herausforderung für Endnutzer. Jede Transaktion erforderte die Zahlung von Gas in ETH, auch wenn der Nutzer nur andere Token besaß und kein ETH hielt. Komplexere Zugangsmuster wie Mehrsignaturen, zeitlich begrenzte Berechtigungen oder automatisierte Transaktionsfreigaben waren nur über Umwege auf der Anwendungsschicht implementierbar.

EIP-7702, das mit dem Pectra-Upgrade am 7. Mai 2025 auf dem Mainnet aktiviert wurde, adressiert diese Einschränkungen auf der Protokollebene, indem es Standard-Accounts erlaubt, temporär die Logik eines Smart Contracts zu über-

nehmen. Im operativen Betrieb bedeutet das: Ein Nutzer kann seinen Account so konfigurieren, dass Session Keys vergeben werden, die einer Anwendung für einen begrenzten Zeitraum begrenzte Transaktionsrechte einräumen, ohne den Hauptschlüssel preiszugeben. Social Recovery wird implementierbar, bei der ein Nutzer seinen Zugang über ein Netzwerk vertrauenswürdiger Kontakte wiederherstellen kann, wenn der Hauptschlüssel verloren geht. Gas Sponsoring wird möglich, bei dem ein Wallet-Anbieter oder eine Anwendung die Transaktionskosten für den Nutzer übernimmt, sodass Nutzer Transaktionen ausführen können, ohne selbst ETH zu besitzen. Die Bedeutung dieser Funktionen für den Infrastrukturanspruch des Systems ist direkt: Ein System, das von seinen Nutzern verlangt, kryptographische Schlüssel fehlerfrei zu verwalten, Gasgebühren in einer spezifischen Währung vorzuhalten und bei jedem Fehler den irreversiblen Verlust von Vermögenswerten zu riskieren, stellt Zugangsanforderungen, die für eine fundamentale Infrastruktur mit breiter Nutzerbasis zu hoch sind. Account Abstraction senkt diese Anforderungen auf ein Niveau, das der Nutzererfahrung traditioneller Finanzdienstleistungen näherkommt, ohne die Selbstverwahrungseigenschaft aufzugeben, die Ethereum von zentralisierten Systemen unterscheidet. Der EIP ist deployt und auf dem Mainnet aktiv, die Integration in die großen Wallet-Anwendungen wie MetaMask und Coinbase Wallet befindet sich in der Umsetzung. Die Übernahmedynamik der Smart-Account-Funktionalität lässt sich bereits am älteren ERC-4337-Standard ablesen, der dieselbe Funktionalität ohne Protokolländerung auf der Anwendungsschicht implementiert: Über 25,5 Millionen Smart Accounts und 132 Millionen UserOperations dokumentieren die Nachfrage nach programmierbaren Accounts.[73]

State als Zustandsdatenbank

Alles, was Ethereum als System speichert, liegt in einer Datenstruktur namens Merkle Patricia Trie. Diese Struktur besteht aus vier verschachtelten Tries: dem World State Trie, der alle Accounts mit ihren Kontoständen, Nonces und Verweisen auf den jeweiligen Code und Speicher enthält, dem Account Storage Trie, der den persistenten Speicher jedes einzelnen Smart Contracts abbildet und als Subtrie im World State Trie referenziert wird, sowie dem Transactions Trie und dem Receipts Trie, die Transaktionsdaten und Ausführungsergebnisse pro Block speichern. Die Trie-Struktur ermöglicht kryptographische Verifizierbarkeit: Der World State Root, ein 32-Byte-Hash, der den gesamten Zustand des Systems zu-

[73] Dune Analytics: ERC-4337 Account Abstraction Dashboard (abgerufen am 27.03.2026). Für EIP-7702 vgl. Ethereum Foundation: Pectra Upgrade Specification.

sammenfasst, wird im Header jedes Blocks verankert, und ein Merkle Proof kann mit logarithmischem Aufwand belegen, dass ein bestimmter Zustandseintrag im Trie vorhanden ist oder fehlt, ohne den gesamten Trie durchsuchen zu müssen.

Der State umfasst in der komprimierten Speicherform der Clients 150 bis 200 GB, die gesamte Größe eines Full Node beträgt 1.579 GB, wobei die Differenz aus historischen Blockdaten, Transaktions-Receipts und der Chain-History besteht.[74] Die Hardware-Anforderungen für den Betrieb eines Full Node umfassen derzeit mindestens 2 TB SSD-Speicher, 16 GB RAM und eine stabile Internetverbindung mit mindestens 25 Megabit pro Sekunde, Anforderungen, die zwar für professionelle Betreiber trivial sind, aber die Einstiegshürde für Solo-Betreiber und insbesondere für Nutzer in Regionen mit begrenzter Infrastruktur erhöhen. Jeder neue Smart Contract, jedes neue Wallet, jeder neue Token-Transfer akkumuliert Zustandsdaten, die permanent gespeichert werden müssen, weil Ethereum keinen nativen Mechanismus für das Ablaufen oder Löschen ungenutzter Zustandseinträge kennt. Ein Smart Contract, der 2016 deployt wurde und seit Jahren nicht mehr aufgerufen wird, belegt denselben Speicherplatz wie ein Contract, der tausende Transaktionen pro Tag verarbeitet, weil das Protokoll nicht zwischen aktiven und inaktiven Zustandseinträgen unterscheidet. Das permanente Wachstum des State ist das zentrale Langzeitproblem der Ethereum-Architektur: Steigende Hardware-Anforderungen erhöhen die Einstiegshürde für neue Node-Betreiber, verlängern die Synchronisationszeiten für Nodes, die dem Netzwerk beitreten wollen, und konzentrieren den Betrieb von Nodes zunehmend bei professionellen Anbietern mit entsprechender Infrastruktur. Die geplanten Lösungen, insbesondere die Migration von der Merkle-Patricia-Trie-Struktur zu Verkle Trees, die effizientere Zustandsbeweise ermöglichen, und die Einführung von History Expiry, die historische Zustandsdaten nach einer definierten Frist aus der Pflichtvorhaltung der Nodes entlässt, haben den Status PLAN und werden in Kapitel 5 bewertet.

[74] Etherscan / YCharts: Ethereum Chain Data Size (abgerufen am 27.03.2026). Der Wert von 1.579 GB bezieht sich auf die Full-Node-Größe; der State Trie umfasst in komprimierter Client-Speicherung 150 bis 200 GB. Kapitel 5 misst demgegenüber den unkomprimierten Gesamt-State (rund 430 GiB), sodass beide Angaben dieselbe Ressource in unterschiedlicher Messdefinition beziffern.

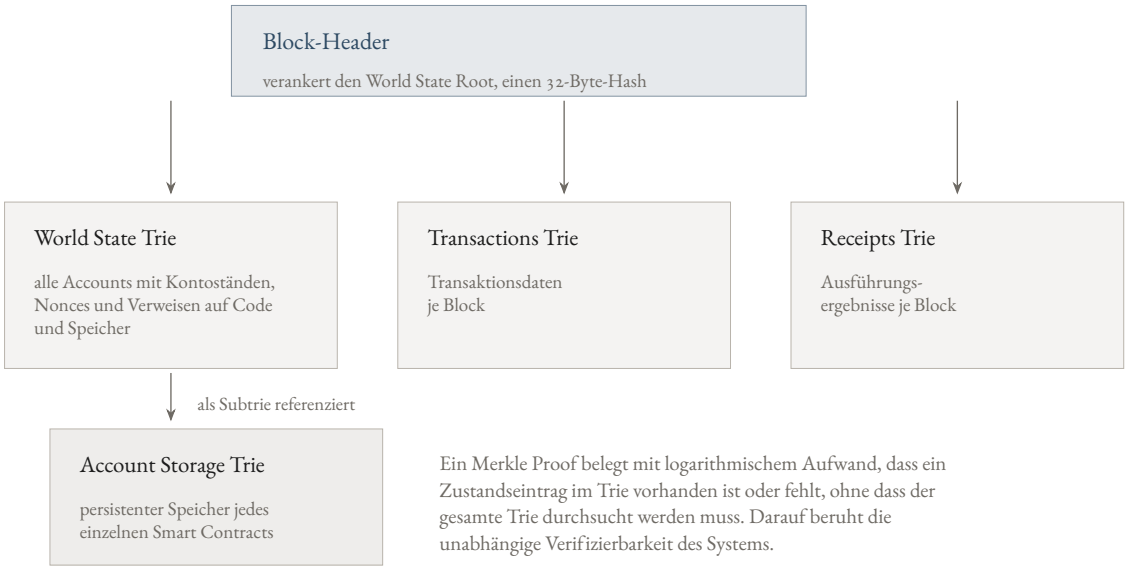


Abbildung 4.2 Die Merkle Patricia Trie. Vier verschachtelte Tries und der World State Root, der sie im Block-Header verankert.

4.2 Der Transaktionslebenszyklus

Eine einzelne Transaktion durchquert auf ihrem Weg von der Erstellung bis zur Finalisierung das gesamte System. An jeder Station dieses Weges offenbart sich eine Komponente der Architektur, die im Zusammenspiel mit den anderen die Eigenschaften des Systems bestimmt. Der folgende Abschnitt verfolgt diesen Weg und erklärt an jeder Station die beteiligten Mechanismen, ihre Designlogik und die Spannungen, die sie erzeugen.

Erstellung und Gas

Der Lebenszyklus einer Transaktion beginnt beim Nutzer, der eine signierte Nachricht erstellt, die den gewünschten Zustandsübergang beschreibt: einen Transfer von ETH an eine andere Adresse, einen Aufruf einer Funktion eines Smart Contracts oder das Deployment eines neuen Contracts auf dem Netzwerk. Die Signatur erfolgt über den ECDSA-Algorithmus auf der secp256k1-Kurve, die auch Bitcoin verwendet, und beweist kryptographisch, dass der Absender über den privaten Schlüssel des sendenden Accounts verfügt, ohne diesen Schlüssel preiszugeben. Die Transaktion enthält neben der Signatur die Zieladresse, den zu transferierenden Wert, die Eingabedaten für den Smart-Contract-Aufruf, eine sequentielle Nonce, die Doppelausführungen verhindert, und die Parameter für die Gebührenberechnung.

Jede Operation auf der EVM verbraucht eine definierte Menge Gas, die Maßeinheit für Rechenkosten im Ethereum-Netzwerk. Die Kostenstruktur spiegelt die tatsächliche Belastung wider, die eine Operation für das Netzwerk erzeugt: Eine einfache Addition kostet 3 Gas, ein Keccak-256-Hash 36 Gas, das Laden eines Speicherwerts aus dem persistenten Storage bei erstmaligem Zugriff 2.100 Gas und ein Schreibvorgang in den persistenten Speicher, der einen leeren Slot füllt, 22.100 Gas. Speicheroperationen sind die teuersten, weil sie den permanent wachsenden State vergrößern und damit eine Belastung erzeugen, die alle künftigen Node-Betreiber tragen müssen. Das Gas Limit pro Block, die Obergrenze der gesamten Rechenleistung, die ein Block verbrauchen darf, liegt bei 60.000.000 und wurde im Laufe des Jahres 2025 durch Validator-Signaling ohne Hard Fork von zuvor 30.000.000 verdoppelt.[75] Das Signaling-Verfahren, bei dem Validatoren in ihren Blöcken ein präferiertes Gas Limit angeben und der tatsächliche Wert sich graduell dem gewichteten Durchschnitt annähert, illustriert einen Governance-Mechanismus, der Kapazitätsänderungen ohne formale Protokolländerungen ermöglicht.

Das Gebührenmodell EIP-1559, das seit August 2021 aktiv ist, teilt die Transaktionsgebühr in zwei Komponenten auf und ersetzt das frühere Auktionsmodell, bei dem Nutzer Gebote abgeben mussten, ohne die aktuelle Marktsituation zuverlässig einschätzen zu können.[76] Die Base Fee wird algorithmisch bestimmt

[75] Etherscan: Ethereum Average Gas Limit Chart. URL: https://etherscan.io/chart/gaslimit (abgerufen am 27.03.2026). Die Erhöhung erfolgte durch graduelles Validator-Signaling im Lauf des Jahres 2025, ohne dass ein Protokoll-Upgrade erforderlich war.

[76] Buterin, Vitalik / Conner, Eric / Dudley, Rick / Slipper, Matthew / Norden, Ian / Bakhta, Abdelhamid (2019): EIP-1559: Fee market change for ETH 1.0 chain. Ethereum Improvement Proposal. Aktiviert im London-Upgrade, August 2021. Vgl. Ethereum Foundation Blog für die technische Dokumentation.

und passt sich dynamisch an die Blockauslastung an: Wenn der vorangegangene Block mehr als die Hälfte seines Gas Limits verbraucht hat, steigt die Base Fee um bis zu 12,5 Prozent. Liegt die Auslastung darunter, sinkt sie um denselben maximalen Faktor. Dieser Mechanismus erzeugt eine vorhersagbare Gebührendynamik, weil ein Nutzer aus dem aktuellen Block die Base Fee des nächsten Blocks mit hoher Genauigkeit ableiten kann. Die Base Fee wird verbrannt, das heißt die entsprechende Menge ETH wird permanent aus dem Umlauf genommen. Die Priority Fee wird vom Nutzer frei gewählt und fließt an den Proposer des Blocks als Anreiz für die bevorzugte Inklusion der Transaktion. In Perioden niedriger Netzwerkauslastung bewegt sich die Base Fee im Bereich von 1 bis 2 Gwei, also einer Milliardstel ETH. In Perioden hoher Auslastung kann sie auf 20 bis 50 Gwei und darüber steigen.

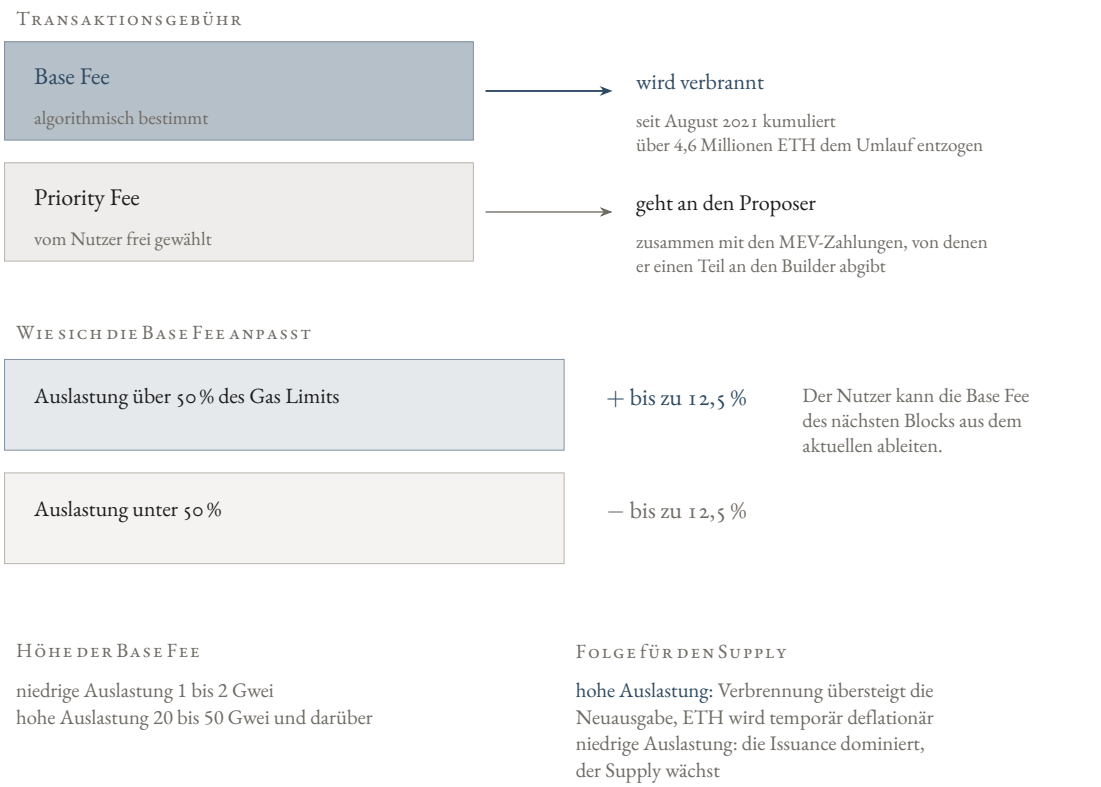
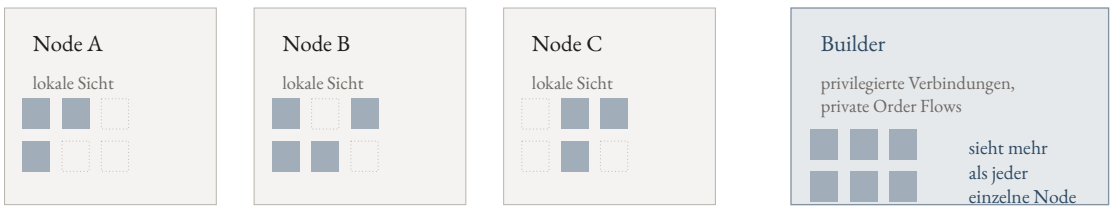


Abbildung 4.3 Der Gebührenmarkt nach EIP-1559. Base Fee und Priority Fee, ihre Ziele und die Regel, nach der sich die Base Fee anpasst.

Propagation im Peer-to-Peer-Netzwerk

Die signierte Transaktion wird über das Peer-to-Peer-Netzwerk an die Nodes des Ethereum-Netzwerks verbreitet. Der Execution Layer nutzt das DevP2P-Protokoll für die Transaktionspropagation, ein Gossip-basiertes Verfahren, bei dem jeder Node empfangene Transaktionen an eine Auswahl seiner verbundenen Peers weiterleitet, die sie wiederum an ihre Peers weiterleiten, bis die Transaktion das gesamte Netzwerk durchdrungen hat. Der Consensus Layer nutzt libP2P, ein modulareres Netzwerkprotokoll, das auch Topic-basiertes Publish-Subscribe unterstützt und für die Verbreitung von Blöcken, Attestationen und Sync-Committee-Nachrichten verwendet wird. Die Trennung der Netzwerkprotokolle zwischen den beiden Layern spiegelt die architektonische Trennung der Clients wider und ermöglicht es, die Kommunikationsmuster jeder Schicht unabhängig zu optimieren.

Es gibt keinen einzelnen zentralen Mempool, in dem alle ausstehenden Transaktionen gesammelt und geordnet werden, sondern jeder Node pflegt eine lokale Sicht auf die Transaktionen, die er von seinen Peers empfangen hat. Diese dezentrale Mempool-Architektur bedeutet, dass verschiedene Nodes zu jedem Zeitpunkt unterschiedliche Transaktionsmengen sehen können, abhängig von der Netzwerktopologie, den Propagationszeiten und den individuellen Filterregeln der Nodes. Die Heterogenität der Mempool-Sichten ist eine direkte Konsequenz der dezentralen Architektur und erzeugt eine informationelle Asymmetrie, die für das MEV-Phänomen konstitutiv ist: Builder, die über privilegierte Verbindungen zu mehr Nodes verfügen oder private Order Flows empfangen, haben eine vollständigere Sicht auf die ausstehenden Transaktionen als durchschnittliche Nodes und können daraus einen ökonomischen Vorteil ziehen. Die Transaktion wartet im lokalen Mempool eines oder mehrerer Nodes auf die Inklusion in einen Block, wobei die Wartezeit von der Gebührenbereitschaft des Nutzers und der aktuellen Auslastung des Netzwerks abhängt.



Es gibt keinen zentralen Mempool

Jeder Node pflegt eine eigene Sicht auf die ausstehenden Transaktionen. Welche er kennt, hängt von der Netzwerktopologie, den Propagationszeiten und seinen Filterregeln ab. Aus dieser Ungleichheit der Sichten entsteht die informationelle Asymmetrie, die für das MEV-Phänomen konstitutiv ist.

Abbildung 4.4 Die Mempool-Sichten. Jeder Node kennt eine andere Teilmenge der ausstehenden Transak-

tionen.

Block Building und MEV

Wer entscheidet, welche Transaktionen in welcher Reihenfolge in einen Block aufgenommen werden, und warum ist diese Reihenfolge ökonomisch relevant? Die Antwort auf diese Frage erschließt eine Dimension des Systems, die weder im Whitepaper noch in der ursprünglichen Protokollspezifikation vorgesehen war und die sich erst mit dem Wachstum der dezentralen Finanzmärkte als eigenständiges Phänomen herausgebildet hat. Spezialisierte Block Builder sammeln Transaktionen aus öffentlichen Mempools und privaten Order Flows, die ihnen direkt von Suchagenten und Handelsprotokollen zugesendet werden, und konstruieren Blöcke, die für die Extraktion von Maximal Extractable Value optimiert sind.[77]

MEV entsteht aus der Tatsache, dass die Reihenfolge von Transaktionen innerhalb eines Blocks den wirtschaftlichen Ausgang beeinflusst. Ein Builder kann Arbitrage-Transaktionen zwischen dezentralen Börsen platzieren, die Preisdifferenzen zwischen Märkten ausnutzen, indem sie auf einer Börse günstig kaufen und auf einer anderen teurer verkaufen, und diese Transaktion in dem Moment in den Block einfügen, in dem die Preisdifferenz am größten ist. Liquidationen in Lending-Protokollen, die fällig werden, wenn der Wert der hinterlegten Sicherheiten unter eine definierte Schwelle fällt, bieten ebenfalls Extraktionsmöglichkeiten, weil der Liquidator eine Prämie erhält. Sandwich-Attacks konstruieren ein Szenario, in dem eine große Nutzer-Transaktion zwischen zwei Builder-Transaktionen eingebettet wird: Die erste kauft vor dem Nutzer und treibt den Preis nach oben, der Nutzer kauft zum höheren Preis, und die zweite Transaktion verkauft nach dem Nutzer zum gestiegenen Preis. Die ökonomische Analyse dieses Phänomens durch Daian und Kollegen im Jahr 2020, die den Begriff Miner Extractable Value prägten, zeigte, dass die Reihenfolgeabhängigkeit der Transaktionsverarbeitung einen strukturellen Anreiz für die Manipulation der Blockzusammensetzung erzeugt, der das Konsensprotokoll destabilisieren kann.

Die kumulative MEV-Extraktion seit dem Merge wird auf 1,5 bis 2 Milliarden US-Dollar geschätzt, wobei circa 93 Prozent dieser Werte als Gebote an die Validatoren fließen, die den jeweiligen Block vorgeschlagen haben.[78] Für den einzel-

[77] Daian, Philip / Goldfeder, Steven / Kell, Tyler / Li, Yunqi / Zhao, Xueyuan / Bentov, Iddo / Breidenbach, Lorenz / Juels, Ari (2020): Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. In: *IEEE Symposium on Security and Privacy (S&P)*, 2020. DOI: 10.1109/SP40000.2020.00040.

[78] Flashbots: MEV-Explore und MEV-Boost Dashboard (abgerufen am 27.03.2026). Die Schätzung der kumula-

nen Nutzer manifestiert sich MEV als versteckte Kostenkomponente jenseits der Gas-Gebühren: Ein Swap auf einer dezentralen Börse kann durch Sandwich-Attacks einen schlechteren Ausführungspreis erfahren, ohne dass der Nutzer dies unmittelbar bemerkt. Die ökonomische Forschung hat gezeigt, dass MEV eine strukturelle Eigenschaft des Systems ist, die sich aus der Reihenfolgeabhängigkeit der Transaktionsverarbeitung ergibt und ohne architektonische Änderungen an der Blockproduktions-Pipeline nicht eliminiert werden kann.

Die Marktstruktur der Blockproduktion per 27. März 2026 zeigt eine erhebliche Konzentration: Titan Builder kontrolliert 51,2 Prozent der Blöcke, BuilderNet, ein dezentrales Multi-Operator-Netzwerk, das Flashbots, Beaverbuild und Nethermind im Dezember 2024 gestartet haben, baut 25,7 Prozent, und Quasar baut 16,4 Prozent.[79] BuilderNet repräsentiert den Versuch, die Konzentrationstendenzen des Builder-Markts durch eine kollaborative Architektur zu durchbrechen: Mehrere unabhängige Operatoren tragen Transaktionen bei und teilen sich den Gewinn, anstatt gegeneinander zu konkurrieren, was die Bündelungsvorteile einzelner großer Builder reduzieren soll. Trotz dieser Innovation kontrollieren drei Builder-Adressen 93,3 Prozent der Ethereum-Blockproduktion. Der Herfindahl-Hirschman-Index dieser Marktstruktur liegt bei 3.554, ein Wert, der die Schwelle von 2.500 deutlich überschreitet, ab der das US-Justizministerium einen Markt als hochkonzentriert einstuft. Die Blockproduktion, der kritischste operative Pfad des Systems, weist damit eine Konzentration auf, die in deutlichem Kontrast zur dezentralen Architektur des Konsensprotokolls steht, wo 964.768 unabhängige Validatoren die Blöcke validieren. Die Ursache dieser Konzentration liegt in den Skaleneffekten des Block Building: Ein Builder mit mehr privaten Order Flows kann profitablere Blöcke konstruieren, höhere Gebote an Proposer zahlen und damit seine Marktposition ausbauen, ein Mechanismus, der zur natürlichen Konzentration tendiert und dem Marktmuster der Cloud-Infrastruktur ähnelt, die Kapitel 3 als Referenz analysiert hat.

---

tiven MEV-Extraktion basiert auf den über MEV-Boost dokumentierten Proposer-Zahlungen seit dem Merge. Vgl. Daian et al. (2020), a.a.O., für die theoretische Grundlage.

[79] relayscan.io: Builder und Relay-Marktanteile (abgerufen am 27.03.2026). Die OFAC-Compliance-Daten stammen aus MEV Watch und relayscan.io.

Proposer-Builder Separation

Die Architekturantwort auf die Frage, wie Blockproduktion von Blockvalidierung getrennt werden kann, ist Proposer-Builder Separation. Builder senden fertige Blöcke mit Geboten an Relays, Off-Chain-Intermediäre wie Ultra Sound Relay, Titan Relay oder BloXroute, die als vertrauenswürdige Vermittler zwischen Buildern und Validatoren fungieren. Die Relays prüfen die Validität der Blöcke und die Korrektheit der Gebote, bevor sie diese an Validatoren weiterleiten, und verhindern damit, dass ein Builder einen ungültigen Block einreicht und der Proposer seinen Slot verliert. Der für den jeweiligen Slot ausgewählte Proposer, ein Validator aus dem Netzwerk, wählt blind das höchste Gebot und schlägt den zugehörigen Block vor, ohne dessen Inhalt zu kennen. Die Blindheit des Proposers ist eine Designentscheidung, die verhindern soll, dass der Proposer die Transaktionsreihenfolge nachträglich manipuliert oder selbst MEV extrahiert. 90 Prozent der Blöcke nutzen MEV-Boost, die Sidecar-Software, die Validatoren mit diesem Builder-Marktplatz verbindet.

Diese Architektur hat eine direkte Konsequenz für den Infrastrukturanspruch des Systems: Die Blockproduktions-Pipeline, der kritischste Pfad vom Moment der Blockzusammensetzung bis zur Vorlage beim Konsensprotokoll, hängt von Off-Chain-Intermediären ab, die nicht durch Protokollregeln diszipliniert werden, sondern auf der Basis von Reputation und ökonomischem Eigeninteresse operieren. Ein Relay, das ausfällt oder manipuliert wird, kann Blöcke zurückhalten oder selektiv weiterleiten, ohne dass das Protokoll eine Korrekturmöglichkeit bietet. Die kryptographischen und ökonomischen Sicherheitsgarantien, die das Konsensprotokoll bietet, erstrecken sich nicht auf die Relay-Schicht. ePBS (EIP-7732), die geplante protokollnative Lösung, die Proposer-Builder Separation in das Konsensprotokoll einbetten und die Relay-Abhängigkeit beseitigen soll, hat den Status PLAN und ist für das Glamsterdam-Upgrade in der zweiten Jahreshälfte 2026 vorgesehen.

Die Frage der Zensurresistenz auf der Blockproduktionsebene lässt sich an konkreten Daten ablesen. 15 Prozent der Blöcke laufen über Relays, die explizit OFAC-konform operieren und Transaktionen von sanktionierten Adressen ausschließen: Flashbots Boost mit 3,8 Prozent und BloXroute Regulated mit 11,4 Prozent.[80] Der größte Builder Titan betreibt explizit keine Zensur. Die historische Entwicklung zeigt einen markanten Rückgang: Im November 2022, wenige Monate nach dem Merge, liefen 79 Prozent der Blöcke über OFAC-kon-

[80] relayscan.io: Builder und Relay-Marktanteile (abgerufen am 27.03.2026). Die OFAC-Compliance-Daten stammen aus MEV Watch und relayscan.io.

forme Relays, ein Wert, der in der Community erhebliche Besorgnis auslöste, weil er bedeutete, dass eine staatliche Sanktionsliste die Transaktionsverarbeitung eines permissionless Systems de facto kontrollierte. Der Rückgang auf 15 Prozent erfolgte ohne protokolläre Intervention, getrieben durch Marktdynamik: durch die wachsende Dominanz nicht-zensierender Builder und Relays, durch die ökonomische Attraktivität der Verarbeitung aller Transaktionen, da zensierende Builder auf die Gebühreneinnahmen der ausgeschlossenen Transaktionen verzichten müssen, und durch den Community-Druck auf zensierende Relays. Die Trajektorie von 79 auf 15 Prozent innerhalb von drei Jahren ist ein empirisches Datum von erheblicher Bedeutung für die Infrastrukturbewertung: Sie zeigt, dass das System ohne formale Governance-Intervention einen Zustand der faktischen Zensurresistenz hergestellt hat, aber sie zeigt auch, dass diese Zensurresistenz auf Marktdynamik beruht, nicht auf einer protokollären Garantie, und damit reversibel ist, wenn sich die Marktbedingungen oder das regulatorische Umfeld ändern. Die maximale Verzögerung, die eine sanktionierte Transaktion im aktuellen Zustand erfahren kann, beschränkt sich auf wenige Blöcke, weil innerhalb dieses Zeitraums mit hoher Wahrscheinlichkeit ein nicht-zensierender Builder an der Reihe ist. FOCIL (EIP-7805), ein Validator-Komitee-basiertes Inclusion-List-System, bei dem ein Komitee von Validatoren Transaktionen benennt, die in den nächsten Block aufgenommen werden müssen, soll diese emergente Zensurresistenz durch eine protokolläre Garantie ersetzen und hat den Status PLAN.

Abbildung 4.5 Proposer-Builder Separation. Der Weg eines Blocks vom Builder über den Relay zum Proposer, der blind das höchste Gebot wählt.

Konsens und Finality

Der für einen Slot ausgewählte Proposer schlägt den Block dem Netzwerk vor, und die 964.768 aktiven Validatoren attestieren über das Gasper-Protokoll, ob sie den Block als gültig anerkennen.[81] Gasper ist eine Kombination aus zwei komplementären Mechanismen, die akademisch in zwei getrennten Arbeiten formalisiert wurden und im operativen Betrieb als Einheit funktionieren.[82]

Casper FFG, das Friendly Finality Gadget, ist ein Byzantine Fault Tolerant Finalization-Protokoll, das ökonomische Finalität herstellt. Das Ethereum-Netzwerk ist in Epochs von je 32 Slots unterteilt, wobei jeder Slot 12 Sekunden dauert und jede Epoch damit 6,4 Minuten umfasst. Am Ende jeder Epoch steht ein Checkpoint, und die Validatoren attestieren über Paare von Checkpoints: den Source-Checkpoint, der der zuletzt justified Checkpoint ist, und den Target-Checkpoint, der den aktuellen Epoch-Boundary-Block bezeichnet. Wenn Validatoren, die zusammen mehr als zwei Drittel des gesamten gestakten ETH repräsentieren, einen Supermajority Link zwischen Source und Target attestieren, wird der Target-Checkpoint als justified markiert. Wenn der darauffolgende Checkpoint ebenfalls justified wird und dabei auf den vorherigen als Source verweist, wird der vorherige Checkpoint finalisiert. Diese Zwei-Epoch-Kaskade erklärt die Finalisierungszeit von 12,8 Minuten: 64 Slots à 12 Sekunden. Die Zwei-Drittel-Schwelle leitet sich aus der Theorie der byzantinischen Fehlertoleranz ab: Wenn zwei Drittel der Validatoren für zwei konfligierende Checkpoints stimmen, muss mindestens ein Drittel doppelt abgestimmt haben und ist damit slashbar, was den wirtschaftlichen Preis eines Angriffs definiert. Ein finalisierter Block ist kryptographisch-ökonomisch irreversibel, weil eine Reversion erfordern würde, dass mehr als ein Drittel des gesamten gestakten ETH geslasht wird, ein Betrag, der bei aktuellem Preisniveau in der Größenordnung von 26 Milliarden US-Dollar liegt.

LMD-GHOST, Latest Message Driven Greedy Heaviest Observed SubTree, handhabt die komplementäre Aufgabe der Echtzeit-Blockauswahl zwischen den Finalisierungspunkten. Ausgehend vom letzten finalisierten Checkpoint folgt der Algorithmus bei jeder Gabelung der Kette dem Subtree, der das meiste Stake-Gewicht akkumuliert hat, wobei nur die jeweils neueste Attestation jedes Valida-

[81] beaconcha.in: Ethereum Beacon Chain Explorer (abgerufen am 27.03.2026). Die Zahl 964.768 reflektiert den Post-Pectra-Konsolidierungseffekt durch EIP-7251; vor der Konsolidierung lag die Validator-Anzahl bei rund 1,07 Millionen.

[82] Buterin, Vitalik / Griffith, Virgil (2019): Casper the Friendly Finality Gadget. arXiv:1710.09437. Für die kombinierte Gasper-Spezifikation vgl. Buterin, Vitalik / Hernandez, Diego / Kamphefner, Thor / Pham, Khiem / Qiao, Zhi / Ryan, Danny / Sin, Juhyeok / Wang, Ying / Zhang, Yan X (2020): Combining GHOST and Casper. arXiv:2003.03052.

tors gezählt wird. Die Beschränkung auf die neueste Nachricht verhindert, dass ein Angreifer alte Attestationen akkumuliert, um einen alternativen Kettenverlauf aufzubauen, und der gierige Traversierungsalgorithmus stellt sicher, dass das Netzwerk dem Pfad folgt, den die Mehrheit des Stake-Gewichts unterstützt.

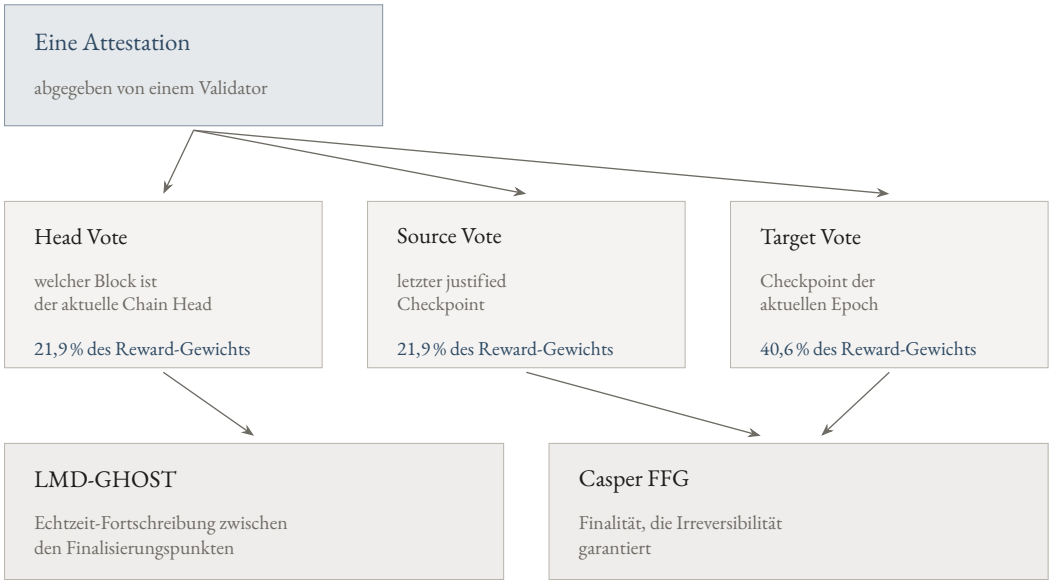
Die operative Bewältigung von fast einer Million gleichzeitig attestierender Validatoren erfordert eine Infrastruktur, die den Kommunikationsaufwand beherrschbar macht. In jeder Epoch werden die aktiven Validatoren pseudorandomisiert auf Committees verteilt, die durch einen RANDAO-basierten Shuffle-Algorithmus eine Epoch im Voraus zugewiesen werden. Jeder Slot kann bis zu 64 Committees enthalten, und jedes Committee umfasst je nach Gesamtzahl der Validatoren zwischen 128 und rund 2.000 Validatoren. Innerhalb eines Committees aggregieren designierte Aggregatoren die Einzelattestationen ihrer Mitglieder und publizieren sie über das globale Subnet. Die BLS-Signatur-Aggregation auf der BLS12-381-Kurve ermöglicht es, hunderte individuelle Signaturen zu einer einzigen 96-Byte-Aggregatsignatur zusammenzufassen, die mit konstantem Aufwand verifiziert werden kann. Ohne diese kryptographische Kompression wäre die Verarbeitung von fast einer Million Attestationen pro Epoch rechnerisch nicht darstellbar. Die optimale Inklusion einer Attestation, also die Aufnahme in den unmittelbar folgenden Block mit einem Delay von einem Slot, maximiert die Rewards des Validators. Eine verzögerte Inklusion reduziert die Belohnung progressiv.

Jede Attestation, die ein Validator abgibt, enthält drei simultane Votes: den Head Vote, der angibt, welchen Block der Validator als aktuellen Chain Head ansieht und der in den LMD-GHOST-Algorithmus eingeht, den Source Vote, der den letzten justified Checkpoint benennt und in Casper FFG eingeht, sowie den Target Vote, der den Checkpoint der aktuellen Epoch benennt und ebenfalls für Casper FFG relevant ist. Die Verschränkung beider Mechanismen in einer einzigen Nachricht ist die zentrale Architekturentscheidung des Gasper-Protokolls: Casper FFG liefert die Finalität, die Irreversibilität garantiert, und LMD-GHOST liefert die Echtzeit-Fortschreibung, die sicherstellt, dass das Netzwerk zwischen den Finalisierungspunkten weiterarbeiten kann, ohne auf den nächsten Checkpoint warten zu müssen.

Die empirische Bilanz des Konsensmechanismus seit dem Merge ist bemerkenswert stabil. Von 287.000 produzierten Epochs wurden 13 nicht finalisiert, eine Finality-Rate von über 99,99 Prozent.[83] Alle 13 nicht-finalisierten Epochs

[83] beaconcha.in: Epoch Finality Statistics. Die 13 nicht-finalisierten Epochs traten am 11. und 12. Mai 2023 auf. Vgl. Etherscan Blog (2023): Battle-Testing Ethereum's Finality.

traten im Mai 2023 bei zwei Vorfällen innerhalb von 24 Stunden auf, die durch Bugs in den Consensus Clients Prysm und Teku beim Handling alter Attestationen ausgelöst wurden. Der Mai-2023-Vorfall war gleichzeitig der erste und bislang einzige Mainnet-Test des Inactivity Leak, eines automatischen Degradation Mode, der aktiviert wird, wenn die Finalisierung für mehr als vier Epochs, also 25,6 Minuten, ausbleibt. Im Inactivity Leak werden die regulären Attestation-Rewards suspendiert, und inaktive Validatoren verlieren progressiv Stake, wobei die Strafen quadratisch mit der Dauer der Inaktivität skalieren: Ein Validator, der vollständig offline ist, verliert circa 40 Prozent seines Stake während des Leaks, während ein Validator, der zu 90 Prozent online bleibt, nur 0,4 Prozent verliert. Der Mechanismus zielt darauf ab, die Finalisierung wiederherzustellen, indem der Stake inaktiver Validatoren so weit reduziert wird, dass die verbleibenden aktiven Validatoren wieder die Zwei-Drittel-Schwelle erreichen. Die Selbstheilung im Mai 2023 dauerte 96 Minuten, ohne dass ein externer Eingriff erforderlich war, und die kumulierten Strafzahlungen betrugen circa 28 ETH. Das System zeigte damit unter Stress genau das Verhalten, das die Protokollspezifikation vorsah.



Die Verschränkung beider Mechanismen in einer einzigen Nachricht ist die zentrale Architekturentscheidung des Gasper-Protokolls. Die übrigen Anteile des Reward-Gewichts entfallen auf die Blockproduktion mit 12,5 % und das Sync Committee mit 3,1 %.

Abbildung 4.6 Die Attestation. Drei Votes in einer Nachricht, die in zwei verschiedene Konsensmechanismen eingehen.

Settlement und State-Aktualisierung

Nach der Finalisierung ist die Transaktion irreversibel in den Zustand des Netzwerks eingeschrieben, und kein Akteur, unabhängig von seiner wirtschaftlichen oder politischen Macht, kann diese Einschreibung rückgängig machen, ohne die ökonomischen Kosten einer 34-Prozent-Attacke zu tragen. Die Gebührenverteilung folgt dem EIP-1559-Mechanismus: Die Base Fee wird verbrannt, und kumulativ sind seit der Einführung im August 2021 über 4,6 Millionen ETH dem Umlauf entzogen worden, was die monetäre Dynamik des Gesamtsystems beeinflusst, die Abschnitt 4.3 analysiert. Die Verbrennungsmechanik erzeugt eine direkte Verbindung zwischen Netzwerkaktivität und Supply-Dynamik: In Perioden hoher Auslastung übersteigt die Verbrennung die Neuausgabe, und ETH wird temporär deflationär. In Perioden niedriger Auslastung dominiert die Issuance, und der Supply wächst. Die Priority Fee und eventuelle MEV-Zahlungen fließen an den Proposer des Blocks, der einen Teil der MEV-Zahlungen mit dem Builder teilt, der den Block konstruiert hat, entsprechend dem Gebot, das im PBS-Prozess abgegeben wurde. Die State Transition Function wendet die durch die Transaktion ausgelösten Änderungen, etwa veränderte Kontostände, aktualisierte Storage-Werte, neu angelegte Accounts oder emittierte Event-Logs, auf den World State Trie an und berechnet einen neuen State Root, der im Header des Blocks verankert wird und fortan als kryptographischer Anker für den gesamten Systemzustand dient.

Systemeigenschaften des Lebenszyklus

Der Weg einer Transaktion durch das System legt vier Architektur-Eigenschaften frei, die für die Bewertung in den späteren Abschnitten dieses Kapitels zentral sind. Die Modularität der Architektur, manifestiert in der Trennung von Consensus und Execution Layer, in der Multi-Client-Philosophie und in der Schichtenarchitektur, ermöglicht Fehlerisolierung und unabhängige Weiterentwicklung einzelner Komponenten, erzeugt dabei aber Komplexität in der Abstimmung zwischen den Schichten. Die ökonomisch verankerte Sicherheit, implementiert durch das Staking-System und die Slashing-Mechanismen, erzeugt Angriffskosten, die das System schützen, die aber an den Marktwert von ETH gekoppelt sind und damit mit dem Ökosystem schwanken. Die Off-Chain-Abhängigkeit der Blockproduktion, sichtbar in der Relay-basierten PBS-Architektur und der Builder-Konzentration, erzeugt eine strukturelle Verwundbarkeit im kritischsten Pfad des Systems, die durch die aktuelle Architektur nicht protokollseitig adressiert wird. Die kryptographisch erzwungene Finality, hergestellt durch Casper FFG, bietet eine Irreversibilitätsgarantie, die stärker ist als die probabilistischen Garantien von Proof-of-Work-Systemen, aber mit einer Finalisierungszeit von 12,8 Minuten langsamer als die Sofortfinalität zentralisierter Systeme. Jedes dieser vier Merkmale trägt Stärken und Einschränkungen gleichermaßen.

4.3 Die Sicherheitsökonomie

Warum staken 964.768 Validatoren ihr Kapital in einem System, das dieses Kapital bei Fehlverhalten konfiszieren kann, und was passiert, wenn sie aufhören es zu tun? Die ökonomische Logik hinter diesem Einsatz trägt die Sicherheitsarchitektur des Systems und legt zugleich die Spannungen offen, die diese Architektur langfristig unter Druck setzen.

Ökonomische Anreize und Konsolidierung

Validatoren erhalten Belohnungen für korrektes Verhalten im Konsensprotokoll, aufgeteilt auf zwei Quellen: die Protokoll-Issuance, also neu geschaffene ETH, die das Protokoll an korrekt attestierende Validatoren verteilt, und MEV-Rewards, die aus der Blockproduktions-Pipeline an den Proposer eines Blocks fließen. Die Reward-Struktur des Protokolls gewichtet verschiedene Formen korrekten Verhaltens: Der korrekte Target Vote, der die Casper-FFG-Finalisierung unterstützt, erhält 40,6 Prozent des Gesamtgewichts, der Source Vote und der Head Vote erhalten jeweils 21,9 Prozent, die Teilnahme am Sync Committee 3,1 Prozent und die Blockproduktion 12,5 Prozent. Die Issuance skaliert invers mit der Quadratwurzel des gesamten gestakten ETH, was bedeutet, dass die Rendite pro Validator sinkt, je mehr Kapital im System gestakt wird. Die effektive Staking-Rate liegt bei circa 2,6 Prozent, gesunken von circa 13 Prozent, als der Staking-Anteil noch niedrig war.[84] Zwischen 30 und 31 Prozent des ETH Total Supply von 120.693.582 ETH sind gestakt, ein Volumen, das die ökonomische Verankerung des Konsensmechanismus widerspiegelt, aber zugleich die sinkende Rendite erklärt: Je mehr ETH gestakt wird, desto weniger erhält jeder einzelne Validator.

Das Pectra-Upgrade im Mai 2025 löste eine strukturelle Verschiebung in der Validator-Landschaft aus. EIP-7251 erhöhte die maximale Effective Balance pro Validator von 32 auf 2.048 ETH, und große Staking-Anbieter nutzten diese Möglichkeit, um viele einzelne 32-ETH-Validatoren in wenige High-Balance-Validatoren zu konsolidieren.[85] Die Gesamtzahl der aktiven Validatoren sank daraufhin von 1,07 Millionen auf 964.768, ohne dass sich die Menge des gestakten ETH veränderte. Dieselbe ökonomische Sicherheit wird seither von weniger, aber größeren Validatoren getragen, was die Netzwerklast reduziert, weil weniger Attestationen pro Epoch verarbeitet werden müssen, aber eine Verschiebung in der Machtverteilung erzeugt, die bei der Analyse der Staking-Konzentration relevant wird. Die Konsolidierung ist kein Vertrauensverlust, sondern eine architektonische Rationalisierung, deren Langzeiteffekte auf die Machtverteilung im Netzwerk erst in den kommenden Jahren vollständig sichtbar werden.

---

[84] CoinDesk (18. Februar 2026): Ethereum Staking Rate Reaches 30.8% of Total Supply. Die effektive APR-Angabe von circa 2,6 Prozent reflektiert den Rückgang, der durch die steigende Validator-Basis bei inverser Quadratwurzel-Skalierung der Issuance entsteht.

[85] beaconcha.in: Ethereum Beacon Chain Explorer (abgerufen am 27.03.2026). Die Zahl 964.768 reflektiert den Post-Pectra-Konsolidierungseffekt durch EIP-7251; vor der Konsolidierung lag die Validator-Anzahl bei rund 1,07 Millionen.

Angriffsökonomie und Slashing

Die zentrale Sicherheitsschwelle des Systems ist die 34-Prozent-Blocking-Minority, die sich direkt aus dem Casper-FFG-Konsensmechanismus ableitet: Ein Angreifer, der mehr als ein Drittel des gestakten ETH kontrolliert, kann die Finalisierung blockieren, indem er seine Attestationen verweigert oder widersprüchlich abgibt, und ein Angreifer mit mehr als zwei Dritteln könnte theoretisch eine widersprüchliche Kette finalisieren.[86] Bei einem gestakten Volumen von 30 bis 31 Prozent des Total Supply und einem ETH-Preis, der am Stichtag Ende März 2026 bei rund 2.100 US-Dollar liegt, beträgt die statische Kapitalanforderung für einen Blocking-Angriff rund 26 Milliarden US-Dollar, und der Angreifer riskiert dabei den vollständigen Verlust seines Einsatzes durch Slashing. Um diese Zahl einzuordnen: Der Angriff erforderte den Erwerb von mehr als 12 Millionen ETH auf einem Markt, der bereits bei Käufen im Bereich von hunderttausenden ETH signifikante Preisbewegungen zeigt, was die tatsächlichen Kosten eines Angriffs weit über den statischen Berechnungswert treiben würde. Die ökonomische Sicherheit ist damit eine Funktion des Stake-Volumens, des ETH-Preises und der Marktliquidität, die eine schrittlose Akkumulation der erforderlichen Position in der Praxis verhindert.

Slashing ist der ökonomische Bestrafungsmechanismus, der das Konsensprotokoll vor zwei spezifischen Angriffsformen schützt. Equivocation liegt vor, wenn ein Validator für denselben Slot zwei verschiedene Blöcke vorschlägt oder für dieselbe Target-Epoch zwei verschiedene Attestationen abgibt. Surround Voting liegt vor, wenn ein Validator eine Attestation abgibt, deren Source-Target-Range eine seiner früheren Attestationen umschließt, ein Verhalten, das auf den Versuch hindeuten kann, eine alternative Kette zu unterstützen. Die Strafstruktur skaliert mit Korrelation: Die initiale Strafe für einen einzelnen geslashten Validator ist gering und beträgt circa ein Viertausendstel der Effective Balance, aber je mehr Validatoren innerhalb desselben 36-Tage-Fensters geslasht werden, desto höher fällt die Korrelationsstrafe am 18. Tag des Exit-Zeitraums aus, bis zum vollständigen Verlust des Stake bei einem koordinierten Angriff, an dem ein Drittel oder mehr der Validatoren beteiligt ist. Diese Korrelationsskalierung ist eine spieltheoretische Designentscheidung: Ein einzelner Validator, der durch einen Konfigurationsfehler doppelt signiert, wird milde bestraft, weil das Fehlverhalten vermutlich nicht böswillig ist. Eine koordinierte Gruppe, die gleichzeitig ge-

[86] Buterin, Vitalik / Griffith, Virgil (2019): Casper the Friendly Finality Gadget. arXiv:1710.09437. Für die kombinierte Gasper-Spezifikation vgl. Buterin, Vitalik / Hernandez, Diego / Kamphefner, Thor / Pham, Khiem / Qiao, Zhi / Ryan, Danny / Sin, Juhyeok / Wang, Ying / Zhang, Yan X (2020): Combining GHOST and Casper. arXiv:2003.03052.

slasht wird, erfährt eine Strafe, die den Angriff ökonomisch vernichtend macht.

Die empirische Bilanz des Slashing-Mechanismus bestätigt ein System, das durch Abschreckung wirkt. In über fünf Jahren Beacon Chain, seit dem 1. Dezember 2020, wurden 525 Validatoren geslasht, bei über 2,2 Millionen jemals erstellten, eine Quote von 0,024 Prozent.[87] Das größte Einzelevent betraf 75 Validatoren des Anbieters Staked Anfang Februar 2021 und ging auf eine deaktivierte Slashing-Schutzdatenbank zurück, die Doppelsignaturen ermöglichte. Das jüngste größere Ereignis betraf 39 bis 40 Validatoren im September 2025 durch Infrastrukturprobleme bei SSV Network und Ankr, ein Vorfall, der auf fehlerhafte Konfiguration der Distributed-Validator-Infrastruktur zurückging. Die überwältigende Mehrheit der Slashing-Events geht auf operationelle Fehler zurück, insbesondere auf den parallelen Betrieb identischer Validator-Keys auf mehreren Nodes, ein Fehler, der beim Failover oder bei der Migration zwischen Server-Umgebungen auftreten kann. Böswillige Angriffe sind in der gesamten Slashing-Historie nicht dokumentiert. Die Parallele zum Rechtssystem, das Kapitel 3 als institutionelle Referenzinfrastruktur analysiert hat, ist instruktiv: Beide Systeme erbringen ihre Koordinationsleistung im Schatten der Sanktion, deren Wirksamkeit gerade darin besteht, dass sie selten vollstreckt werden muss. Die Existenz der Strafe, nicht ihre Anwendung, erzeugt die Verhaltenskonformität, die das System stabilisiert.

Staking-Verteilung

Die Verteilung des gestakten ETH über verschiedene Staking-Kategorien zeigt eine Landschaft, in der die Zugangswege zum System unterschiedlich strukturiert sind und unterschiedliche Implikationen für die Dezentralisierung des Netzwerks tragen. Liquid Staking dominiert mit 31,1 Prozent des gestakten ETH: Nutzer delegieren ihr ETH an ein Protokoll wie Lido, Rocket Pool oder ether.fi und erhalten im Gegenzug einen handelbaren Token, der den gestakten Anteil repräsentiert und auf dezentralen Finanzmärkten als Sicherheit, Liquiditätsbereitstellung oder Handelsinstrument eingesetzt werden kann. Die Liquid-Staking-Tokens, insbesondere Lidos stETH, sind tief in das DeFi-Ökosystem integriert: Sie dienen als Sicherheit in Lending-Protokollen, als Liquidität in dezentralen Börsen und als Basiswert für weitere Derivate. Diese Integration erzeugt einen ökonomischen Vorteil für Liquid Staking gegenüber Solo-Staking, weil der Nutzer parallel Staking-Rendite bezieht und sein Kapital in DeFi-Anwendungen ein-

[87] beaconcha.in: Slashing Statistics (abgerufen am 27.03.2026). Vgl. Migalabs / CryptoSlate (11. September 2025) für die Analyse des SSV Network/Ankr Slashing-Events.

setzt, ein Phänomen, das als Rehypothekierung bekannt ist und das die natürliche Tendenz zur Konzentration des gestakten ETH bei Liquid-Staking-Anbietern erklärt. Zugleich erzeugt die Integration systemische Risiken: Ein Depeg-Event, bei dem der Liquid-Staking-Token seinen Wechselkurs zum zugrunde liegenden ETH verliert, kann kaskadierende Liquidationen in den DeFi-Protokollen auslösen, die den Token als Sicherheit akzeptieren. Staking über zentralisierte Börsen macht 24 Prozent aus, wobei Coinbase und Binance die größten Anbieter sind. Diese Form des Staking delegiert die Validator-Kontrolle an Unternehmen, die direkt nationaler Regulierung unterliegen und im Fall regulatorischen Drucks gezwungen sein können, bestimmte Transaktionen zu zensieren oder Staking-Dienste einzuschränken. Staking Pools, die Einlagen unterhalb der 32-ETH-Schwelle bündeln, ohne einen handelbaren Token auszugeben, halten 16 Prozent. Solo-Staker, also Individuen, die eigenständig einen Validator betreiben und damit die dezentralste Form der Netzwerksicherung darstellen, halten weniger als 1 Prozent des gestakten ETH, ein Wert, der die Wirkung der ökonomischen Einstiegsbarriere widerspiegelt: Die Mindesteinlage von 32 ETH entspricht beim Stichtagskurs rund 67.000 US-Dollar, ein Betrag, der für die Mehrheit potentieller Teilnehmer prohibitiv ist. Die vier Kategorien decken rund 72 Prozent des gestakten ETH ab.

Lido, das größte Liquid-Staking-Protokoll, hält 22,8 bis 23 Prozent des gestakten ETH, ein Anteil, der von 32 Prozent im Jahr 2023 rückläufig ist.[88] Der Rückgang resultiert aus dem Zusammenwirken dreier Faktoren: Die sinkende Staking-Rendite, die von rund 5 Prozent im Jahr 2023 auf 2,6 Prozent im ersten Quartal 2026 gefallen ist, macht Lidos Angebot gegenüber alternativen Kapitalverwendungen weniger attraktiv, insbesondere in einem Marktumfeld, in dem traditionelle Zinsprodukte vergleichbare Renditen bieten. Die wachsende Konkurrenz durch jüngere Protokolle wie ether.fi, die mit differenzierten Produktangeboten wie Native Restaking Marktanteile gewinnen, und durch Staking-Angebote zentralisierter Börsen, die für ihre bestehende Nutzerbasis niedrigschwellig zugänglich sind, erodiert Lidos Dominanz. Der Community-Druck, der Lidos Marktanteil als systemisches Konzentrationsrisiko thematisierte und öffentlich dazu aufrief, Stake zu diversifizieren, trug ebenfalls zum Rückgang bei. Die Lido DAO lehnte 2022 per Governance-Abstimmung eine formale Selbstbeschränkung auf 22 Prozent ab, die von Mitgliedern der Ethereum-Community vorgeschlagen worden war, integrierte aber als strukturelle Gegenmaßnahme Distribu-

[88] Dune Analytics / CCN (5. März 2026): Lido Staking Market Share. Der Rückgang von 32 Prozent (2023) auf 22,8 bis 23 Prozent reflektiert relative Marktdynamik, nicht notwendigerweise einen Rückgang der absoluten Staking-Menge bei Lido.

ted Validator Technology, die den Betrieb der einzelnen Validatoren über mehrere unabhängige Operatoren verteilt, sodass kein einzelner Operator die Kontrolle über einen signifikanten Anteil der Lido-Validatoren hat. 547.968 ETH laufen auf DVT, ein Wachstum von 57 Prozent gegenüber dem Vorquartal.[89] Lido liegt mit seinem aktuellen Anteil unter der kritischen 33-Prozent-Schwelle, ab der ein einzelner Staking-Anbieter die Finalisierung blockieren könnte.

Die kumulierte Staking-Konzentration der drei größten Anbieter, Lido, Coinbase und Binance, liegt bei 40 bis 45 Prozent des gestakten ETH, während kein einzelner dieser Anbieter die 33-Prozent-Blocking-Minority-Schwelle erreicht. Die Konzentration ist hoch genug, um bei einer hypothetischen koordinierten Aktion dieser drei Anbieter die Finalisierung potentiell zu blockieren, aber niedrig genug, dass kein einzelner Anbieter allein die kritischen Schwellen erreicht. Die Frage, ob eine solche Koordination realistisch ist, hängt von Faktoren ab, die über die reine Staking-Verteilung hinausgehen: regulatorischer Druck, der mehrere Anbieter parallel trifft, könnte eine faktische Koordination erzwingen, ohne dass die Anbieter dies beabsichtigen. Ein konkretes Szenario wäre eine regulatorische Anordnung an US-basierte Staking-Anbieter, die Validierung bestimmter Transaktionstypen einzustellen. Coinbase und andere US-regulierte Anbieter wären gezwungen zu kooperieren, und die Frage, ob ihr kumulierter Stake die Blocking-Minority erreicht, würde aus einer theoretischen zu einer praktischen Frage werden. Die DVT-Integration bei Lido und die Diversifizierung des Builder-Markts durch BuilderNet sind Gegenmaßnahmen, die dieses Risiko mindern, aber die strukturelle Spannung zwischen regulatorischer Erreichbarkeit und dezentralem Anspruch bleibt bestehen.

Drei Spannungen der Sicherheitsökonomie

Die erste Spannung betrifft die inflationäre Dynamik des Gesamtsystems. ETH ist im operativen Zustand Q1 2026 leicht inflationär, mit einer jährlichen Supply-Änderung von circa 0,5 Prozent. Die Mechanik hinter dieser Dynamik lässt sich präzise benennen: Die L2-Migration hat mehr Transaktionsaktivität von der Basisschicht absorbiert, als die Blob-Gebühren an Verbrennungsvolumen zurückführen. Layer-2-Rollups, die in Abschnitt 4.4 beschrieben werden, zahlen für Blob-Space auf Layer 1, aber die Blob-Gebühren sind nahe null, weil die Blob-Kapazität nach den Dencun- und Fusaka-Erweiterungen die aktuelle Nachfrage übersteigt. Vor der Einführung von Blob-Transactions zahlten Rollups für Call-

[89] Lido DAO: Tokenholder Update (26. Februar 2026). DVT-Adoption und QoQ-Wachstum. Für den Governance-Entscheid zur Selbstbeschränkung vgl. Lido DAO Snapshot Vote, Juni 2022.

data auf Layer 1, was zu substanziellen Base-Fee-Beiträgen führte. Nach Dencun fielen die L2-Kosten um 80 bis 95 Prozent, und mit ihnen fiel der Beitrag der L2-Aktivität zur ETH-Verbrennung. Parallel dazu ist die direkte L1-Transaktionsaktivität und damit die Base-Fee-Verbrennung gesunken, weil Nutzer und Anwendungen zunehmend auf Layer-2-Systeme migrieren, die niedrigere Gebühren und höheren Durchsatz bieten. Die Spannung liegt in der Zirkularität: Die L2-Skalierung, die Ethereum als Infrastruktur stärkt, indem sie die Nutzerbasis erweitert, die Gebühren senkt und die Kapazität des Gesamtsystems vervielfacht, schwächt zugleich den ökonomischen Mechanismus, der die Verbrennung von ETH antreibt und damit die L1-Sicherheit langfristig mitfinanzieren soll. Ob diese Spannung strukturell ist oder eine Übergangsphase darstellt, die sich mit wachsender L2-Nachfrage auflöst, wenn die Blob-Kapazität wieder an ihre Grenzen stößt, ist eine offene Frage.

Die zweite Spannung betrifft das prozyklische Risiko der Sicherheitsarchitektur. Die Angriffskosten in der Größenordnung von 26 Milliarden US-Dollar sind eine Funktion des ETH-Preises, und der ETH-Preis ist eine Marktgröße, die mit dem Krypto-Gesamtmarkt und den makroökonomischen Bedingungen schwankt. Im Krypto-Winter 2022 fiel der ETH-Preis um über 80 Prozent, und proportional fielen die ökonomischen Angriffskosten. Das System überlebte diesen Stresstest empirisch: Kein Angriff wurde versucht, die Validator-Zahlen stiegen trotz fallender Renditen weiter, und das Konsensprotokoll operierte durchgehend im Normalbetrieb. Die Sicherheitsgarantie ist aber keine physische Konstante wie die Tragfähigkeit einer Brücke, sondern eine marktabhängige Größe, die in dem Moment am schwächsten ist, in dem das Ökosystem unter dem größten Stress steht und ein Angriff die größte Wirkung entfalten würde. Die systematische Analyse dieses prozyklischen Risikos, einschließlich der Szenarien, in denen die Angriffskosten unter kritische Schwellen fallen könnten, und der Mechanismen, die ein solches Szenario abmildern oder verschärfen.

Die dritte Spannung betrifft die langfristige Finanzierung der Netzwerksicherheit und wird im Ethereum-Ökosystem unter dem Begriff Security Budget Sustainability diskutiert. Wenn Layer-2-Systeme den Großteil der Transaktionsaktivität absorbieren und die L1-Fee-Revenue dauerhaft auf niedrigem Niveau verbleibt, stellt sich die Frage, ob die Sicherheit des Netzwerks progressiv durch Neuausgabe von ETH finanziert werden muss, was die Inflation dauerhaft erhöht und den deflationären Mechanismus von EIP-1559 unterläuft. Die Alternative wäre, dass L2-Rollups über steigende Blob-Nachfrage langfristig substanzielle Fee-Revenue an die Basisschicht zurückführen, ein Szenario, das die aktuelle Blob-Kapazitätsausweitung durch PeerDAS mittelfristig unwahrscheinlich

macht, weil die Kapazität schneller wächst als die Nachfrage. Eine dritte Möglichkeit, die in der Community zunehmend diskutiert wird, ist die Reduktion der Issuance selbst: Wenn 30 bis 31 Prozent des Supply bereits gestakt sind und die Sicherheit damit auf einem Niveau liegt, das bei weitem ausreicht, um selbst staatlich finanzierte Angriffe ökonomisch unsinnig zu machen, könnte die Issuance reduziert werden, ohne die Sicherheit substanziell zu gefährden. Die Issuance-Reform-Debatte im Ethereum-Ökosystem ist aktiv und ungelöst: Mehrere Vorschläge zur Anpassung der Issuance-Kurve sind in Diskussion, darunter Modelle, die die Issuance an eine Ziel-Staking-Rate koppeln und die Ausgabe progressiv senken, wenn der Staking-Anteil einen definierten Schwellenwert übersteigt, sowie Modelle, die eine absolute Obergrenze für die Issuance einführen. Keiner dieser Vorschläge hat den Status eines formalen EIP erreicht, und die Debatte ist politisch aufgeladen, weil jede Issuance-Änderung die Interessen der Staking-Anbieter, der ETH-Halter und der Node-Betreiber unterschiedlich betrifft. Die Frage, ob Ethereums Sicherheitsökonomie in einem Gleichgewicht operiert, das über Dekaden tragfähig ist, oder ob strukturelle Anpassungen erforderlich sind, die das Verhältnis zwischen Issuance, Fee-Revenue und Sicherheitsbudget neu kalibrieren, ist eine der offenen Fragen, die das IST-Urteil im Bewertungsabschnitt dieses Kapitels adressieren wird.

4.4 Die Skalierungsarchitektur

Die Sicherheitsökonomie hat gezeigt, wie das System finanziert und geschützt wird. Die nächste architektonische Frage betrifft die Kapazität: ob die Basisschicht den Transaktionsbedarf eines Systems bedienen kann, das den Anspruch erhebt, als fundamentale Infrastruktur für globale Koordination zu dienen.

Das in Abschnitt 4.2 beschriebene Gas Limit von 60.000.000 pro Block begrenzt die Transaktionskapazität der Basisschicht auf 15 bis 30 Transaktionen pro Sekunde für komplexe Operationen. Die sequentielle Ausführungsarchitektur der EVM, die Abschnitt 4.1 als bewusste Designentscheidung zugunsten des Determinismus erläutert hat, schließt eine Parallelisierung auf der Basisschicht im aktuellen Zustand aus. Um diese Zahlen einzuordnen: Visa verarbeitet in Spitzenzeiten über 65.000 Transaktionen pro Sekunde, und selbst die durchschnittliche Last des globalen Zahlungsverkehrs übersteigt Ethereums L1-Kapazität um mehrere Größenordnungen. Die Begrenzung ist dabei kein temporärer Engpass, der durch Hardware-Verbesserungen aufgelöst werden könnte, sondern eine Konsequenz des fundamentalen Designs, das jedem Node zumutet, jede Transaktion nachzuvollziehen, um den Systemzustand unabhängig zu verifizieren. Der nächste geplante Kapazitätssprung auf 200.000.000 Gas mit paralleler Transaktionsverarbeitung (EIP-7928) ist für das Glamsterdam-Upgrade in der zweiten Jahreshälfte 2026 vorgesehen, hat aber den Status PLAN und wird in Kapitel 5 bewertet. Die Frage, die sich aus dieser Limitation ergibt, ist architektonischer Natur: Wenn die Basisschicht nur wenige Dutzend Transaktionen pro Sekunde verarbeiten kann, wie soll das System Millionen von Nutzern bedienen?

Die rollup-zentrische Strategie

Die Antwort, die das Ethereum-Ökosystem seit Oktober 2020 verfolgt, ist eine Arbeitsteilung zwischen Schichten. Vitalik Buterins Blogpost „A rollup-centric ethereum roadmap“ formulierte die strategische Weichenstellung: Die Basisschicht konzentriert sich auf zwei Funktionen, Settlement und Datenverfügbarkeit, während eigenständige Layer-2-Systeme die Transaktionsausführung übernehmen.[90] Diese Entscheidung war das Ergebnis eines mehrjährigen Forschungsprozesses, in dem alternative Skalierungsansätze wie Sharding der Execution-Schicht und Plasma-Chains untersucht und verworfen wurden, weil sie entweder die Composability der Basisschicht zerstört oder unlösbare Probleme bei der Datenverfügbarkeit erzeugt hätten. Die rollup-zentrische Strategie vereint die Er-

[90] Buterin, Vitalik (2020): A rollup-centric ethereum roadmap. Blogpost, Oktober 2020. URL: https://vitalik.eth.limo/general/2020/10/08/rollup.html

kenntnisse beider Forschungsstränge: Sharding löste 2019 das Problem des Data Availability Sampling, und Rollups benötigten genau die hohe Datenbandbreite auf der Basisschicht, die ein Sharding-Design bereitstellen konnte.

Die Arbeitsteilung lässt sich an einer Analogie zum Stromnetz verdeutlichen, das Kapitel 3 als Referenzinfrastruktur analysiert hat: Das Hochspannungsnetz transportiert Energie zuverlässig über große Distanzen und stellt die Spannung bereit, auf der das gesamte System aufbaut, aber es muss nicht jede Steckdose direkt erreichen. Die Verteilnetze übernehmen die letzte Meile zum Endverbraucher. Ethereum als Basisschicht stellt in dieser Analogie die Spannung bereit, also die Sicherheitsgarantie und die Datenverfügbarkeit, auf die Layer-2-Systeme aufbauen, während die Layer-2-Systeme die Transaktionen verarbeiten, mit denen die Endnutzer interagieren. Die Analogie hat Grenzen: Verteilnetze im Stromsystem sind reguliert, interoperabel und untereinander koordiniert, Eigenschaften, die Ethereums L2-Ökosystem im aktuellen Zustand nur eingeschränkt aufweist.

Die Verschiebung verändert Ethereums operative Rolle grundlegend. Von einer Plattform, auf der Nutzer direkt Transaktionen ausführen, wird das System zu einer Infrastrukturschicht, die Sicherheit und Datenverfügbarkeit für darauf aufbauende Systeme bereitstellt. Diese Transformation ist in der Geschichte der digitalen Infrastruktur nicht ohne Vorläufer: Das Internet hat eine ähnliche Schichtentrennung vollzogen, als die Transportprotokolle (TCP/IP) und die Anwendungsschicht (HTTP, SMTP, DNS) sich funktional ausdifferenzierten, wobei die Transportschicht für den Endnutzer unsichtbar wurde. In der Praxis bedeutet das: Ein Nutzer, der auf Arbitrum oder Base eine Transaktion ausführt, interagiert mit dem Layer-2-System, und die Basisschicht tritt nur als Anker in Erscheinung, der die Korrektheit des Layer-2-Zustands garantiert. Ob diese Rollenverschiebung den Infrastrukturanspruch stärkt, weil sie Ethereum als Settlement-Schicht positioniert, die zahlreiche aufbauende Systeme trägt, oder schwächt, weil sie die direkte Nutzererfahrung an Intermediäre delegiert, ist eine Bewertungsfrage, die Abschnitt 4.8 adressiert.

Datenverfügbarkeit als Vorbedingung

Bevor die Mechanik der Rollups beschrieben werden kann, muss ein Konzept geklärt werden, das die gesamte Skalierungsarchitektur trägt: Datenverfügbarkeit. Das Problem ist präzise formulierbar: Wenn ein Layer-2-System Transaktionen außerhalb der Basisschicht ausführt, muss sichergestellt sein, dass die Transaktionsdaten für unabhängige Prüfer zugänglich sind, damit diese den Zustand des Rollups verifizieren oder einen Betrug nachweisen können. Ohne garantierte Datenverfügbarkeit könnte ein Rollup-Betreiber Transaktionen unterschlagen oder Zustände fälschen, ohne dass dies nachweisbar wäre, weil die Daten, die den Betrug belegen würden, nicht abrufbar sind. Die Basisschicht übernimmt diese Garantie: Sie speichert die Transaktionsdaten temporär in Form von Blobs, sodass jeder Prüfer innerhalb eines definierten Zeitfensters darauf zugreifen kann. Die Datenverfügbarkeitsgarantie ist damit die architektonische Voraussetzung dafür, dass Layer-2-Systeme die Sicherheitseigenschaften der Basisschicht erben können, und sie markiert die Trennlinie zwischen echten Rollups, die Ethereum-Blobs nutzen, und alternativen Konstruktionen wie Validiums, die ihre Daten außerhalb der Basisschicht speichern und damit schwächere Garantien bieten.

Blobs, eingeführt durch EIP-4844 im Dencun-Upgrade vom März 2024, sind 128 KB große temporäre Datenpakete, die circa 18 Tage auf Beacon Nodes vorgehalten und danach automatisch gelöscht werden.[91] Die temporäre Speicherung ist eine bewusste Designentscheidung: Die Daten müssen lange genug verfügbar sein, damit ein Fraud Proof innerhalb der Challenge-Period eingereicht werden kann, aber sie müssen nicht permanent gespeichert werden, weil das den State-Wachstum der Basisschicht beschleunigen würde. Die Blobs operieren in einem eigenen Gebührenmarkt, getrennt vom Execution-Gas, sodass Layer-2-Daten nicht mit regulären EVM-Transaktionen um Blockspace konkurrieren. Die Blob-Kapazität liegt nach den Blob-Parameter-Only-Forks des Fusaka-Upgrades bei einem Target von 14 und einem Maximum von 21 Blobs pro Block, und PeerDAS ermöglicht die weitere Erweiterung auf deutlich höhere Blob-Zahlen durch Peer-basiertes Data Availability Sampling. Die Kostenreduktion seit Einführung der Blobs war erheblich: Die Transaktionskosten auf führenden Layer-2-Systemen fielen nach Dencun um 80 bis 95 Prozent, was das Transaktionsvolumen auf Systemen wie Base um über 200 Prozent ansteigen ließ. Im operativen Betrieb bedeutet das: Eine einfache Token-Transaktion auf Arbitrum, Base oder Optimism kostet im Median weniger als 0,01 US-Dollar, ein Niveau, das

[91] EIP-4844: Shard Blob Transactions. Ethereum Improvement Proposal, aktiviert im Dencun-Upgrade, März 2024. Für die Kostenreduktionsdaten vgl. L2BEAT: Transaction Costs Dashboard (abgerufen am 27.03.2026).

unter den Gebühren einer Kreditkartentransaktion oder einer Banküberweisung liegt und den Zugang zum System für Nutzer in Regionen mit niedrigem Einkommen ökonomisch erschließt. Nach Pectra sanken die Blob-bezogenen Kosten um weitere 51 Prozent. Im aktuellen Zustand übersteigt die Blob-Kapazität die Nachfrage, und die Blob-Gebühren bewegen sich nahe dem Minimum, eine Tatsache, die in Abschnitt 4.3 als Treiber der inflationären Dynamik identifiziert wurde.

Alternative Datenverfügbarkeitslösungen wie Celestia, EigenDA und Avail bieten höheren Durchsatz zu niedrigeren Kosten, operieren aber mit eigenen Validatorensets und Sicherheitsmodellen, die schwächere Garantien bieten als die Ethereum-Basisschicht. Celestia nutzt ein eigenes Proof-of-Stake-System mit einem Nakamoto-Koeffizienten von 6, was bedeutet, dass sechs Akteure ausreichen würden, um das System zu kompromittieren. Ethereums 964.768 Validatoren sind demgegenüber eine Rohzahl, die die tatsächliche Dezentralität überzeichnet, weil ein erheblicher Teil von wenigen großen Betreibern geführt wird. Ein Nakamoto-Koeffizient und eine Validatorenzahl messen verschiedene Größen und lassen sich nicht unmittelbar vergleichen. EigenDA basiert auf einem Restaking-Modell, bei dem Ethereum-Validatoren zusätzliche Sicherheitsleistungen erbringen, operiert aber mit einem Data Availability Committee, das die Daten nicht öffentlich verifizierbar macht. Layer-2-Systeme, die diese alternativen DA-Lösungen nutzen, verlieren die Sicherheitsgarantien von Ethereum und werden in der Klassifizierung von L2BEAT als Validiums oder Optimiums eingestuft, eine Unterscheidung, die signalisiert, dass die volle Sicherheitsvererbung nur bei der Nutzung von Ethereum-Blobs als Datenverfügbarkeitsschicht gegeben ist. Alle fünf führenden Layer-2-Systeme nach Total Value Secured, Arbitrum One, Base, OP Mainnet, Starknet und zkSync Era, nutzen Ethereum-Blobs als primäre Datenverfügbarkeitsschicht, was die Präferenz für die stärkeren Sicherheitsgarantien der Basisschicht reflektiert, selbst wenn günstigere Alternativen verfügbar sind.

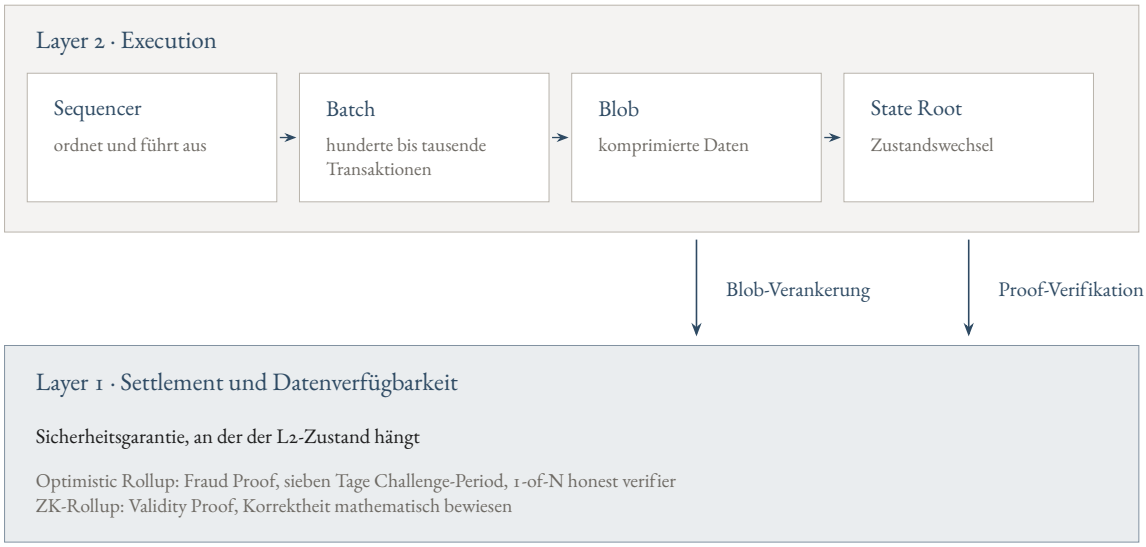
Wie ein Rollup funktioniert

Ein Rollup delegiert die Transaktionsausführung an ein eigenständiges System, verankert aber die Ergebnisse und die Transaktionsdaten auf der Basisschicht, um deren Sicherheitsgarantien zu erben. Der operative Ablauf folgt einem wiederkehrenden Muster: Ein Sequencer, ein spezialisierter Betreiber, der das Layer-2-System steuert, sammelt Transaktionen der L2-Nutzer aus dem lokalen Mempool des L2, führt sie auf der L2-Ausführungsumgebung aus, bündelt die Ergebnisse zu Batches und postet komprimierte Daten als Blobs auf Layer 1. Der Sequencer bestimmt die Reihenfolge der Transaktionen auf dem L2, veröffentlicht den resultierenden Zustandswechsel als State Root auf der Basisschicht und ist damit der Akteur, der die Schnittstelle zwischen den beiden Schichten kontrolliert. Die Komprimierung ist erheblich: Hunderte bis tausende L2-Transaktionen werden in einen einzigen Blob gepackt, und die L2-Nutzer zahlen nur einen Bruchteil der L1-Kosten, weil die Kosten der Blob-Verankerung auf alle Transaktionen im Batch verteilt werden.

Die Transaktionsbestätigung auf dem L2 erfolgt in zwei Stufen mit unterschiedlichen Sicherheitseigenschaften. Die erste Stufe ist die Sequencer-Bestätigung, die innerhalb von Sekunden oder Sub-Sekunden erfolgt und dem Nutzer signalisiert, dass seine Transaktion in die L2-Kette aufgenommen wurde. Diese Bestätigung beruht auf dem Vertrauen in den Sequencer und hat keine Finalitätsgarantie: Der Sequencer könnte die Transaktion theoretisch rückgängig machen, solange sie noch nicht auf Layer 1 verankert ist. Die zweite Stufe ist die L1-Finalisierung, die eintritt, wenn der Batch auf Layer 1 gepostet und durch den Konsensmechanismus finalisiert wurde, zuzüglich der Verifikationsperiode, die bei Optimistic Rollups sieben Tage und bei ZK-Rollups die Proof-Generierungszeit umfasst. Erst nach dieser zweiten Stufe erbt die Transaktion die vollen Sicherheitsgarantien der Basisschicht.

Die Verifikation der State Roots folgt einem von zwei Ansätzen, deren Unterschied in der Beweislast liegt. Optimistic Rollups gehen davon aus, dass die eingereichten Zustände korrekt sind, und gewähren eine siebentägige Challenge-Period, in der jeder Teilnehmer einen Fraud Proof einreichen kann, der eine fehlerhafte Zustandsbehauptung widerlegt. Die Sicherheit dieses Modells beruht auf der 1-of-N honest verifier assumption: Es genügt, dass ein einziger ehrlicher Prüfer innerhalb der Frist den Betrug nachweist, und das System bleibt sicher, solange diese Bedingung erfüllt ist. Der Preis ist die siebentägige Verzögerung bei nativen Withdrawals von L2 zu L1, die für viele Anwendungsfälle zu lang ist und den Einsatz von Liquiditäts-Bridges erzwingt, die eigene Trust-Annahmen ein-

führen. ZK-Rollups verfolgen den umgekehrten Ansatz: Sie beweisen die Korrektheit des eingereichten Zustands mathematisch vor dessen Akzeptanz durch einen Validity Proof, den ein Verifier-Contract auf Layer 1 in konstanter Zeit prüft, unabhängig davon, wie viele Transaktionen der Batch enthält. Withdrawals können nach Verifizierung des Proofs sofort finalisiert werden, aber die Erzeugung der Proofs ist rechenintensiv und erzeugt Kosten, die an die L2-Nutzer weitergegeben werden. Arbitrum One, Base und OP Mainnet sind Optimistic Rollups. Starknet und zkSync Era sind ZK-basiert, wobei die Grenzen zunehmend verschwimmen, weil Projekte wie BOB optimistische Execution mit ZK-Proofs on demand kombinieren.



Zwei Bestätigungsstufen: der Sequencer bestätigt in Sekunden ohne Finalitätsgarantie, die vollen Garantien der Basisschicht erbt die Transaktion erst mit der L1-Finalisierung.

Abbildung 4.7 Die rollup-zentrische Architektur. Layer 1 trägt Settlement und Datenverfügbarkeit, die Rollups die Ausführung.

Das L2-Ökosystem im operativen Zustand

Alle führenden Layer-2-Systeme operieren mit zentralisierten Sequencern, eine Tatsache, die dem Dezentralisierungsanspruch des Gesamtsystems widerspricht und die wichtigste Einschränkung des aktuellen Skalierungsmodells darstellt. Die Sequencer-Kontrolle liegt bei den jeweiligen Entwicklerteams: Offchain Labs betreibt den Arbitrum-Sequencer, Coinbase den Base-Sequencer, die Optimism Foundation den OP-Mainnet-Sequencer, StarkWare die drei Starknet-Sequencer. Diese Zentralisierung erzeugt ein dreifaches Risikoprofil: Der Sequencer bildet einen Single Point of Failure für die Liveness des L2, weil sein Ausfall den gesamten Betrieb des Systems unterbricht. Er kann Transaktionen willkürlich ausschließen oder verzögern, weil er die alleinige Entscheidung über die Transaktionsinklusion trifft. Sein Monopol auf die Transaktionsreihenfolge ermöglicht MEV-Extraktion auf der L2-Ebene. Dokumentierte Sequencer-Ausfälle, darunter 78 Minuten bei Arbitrum im Dezember 2023, 33 Minuten bei Base im August 2025 und über fünf Stunden bei Starknet im September 2025, illustrieren das Liveness-Risiko in der Praxis. Der Linea-Vorfall vom Juni 2024, bei dem das Entwicklerteam den Sequencer bewusst stoppte und Angreifer-Adressen nach einem Exploit zensierte, illustriert das Zensurrisiko und zeigt, dass die Fähigkeit zur Zensur nicht nur theoretisch besteht, sondern im Ernstfall tatsächlich ausgeübt wird, wenn auch mit der Begründung, Schaden vom Ökosystem abzuwenden. Die MEV-Dynamik auf Layer-2-Systemen unterscheidet sich fundamental von der auf Layer 1: Zentralisierte Sequencer operieren mit privaten Mempools, was klassische Mempool-basierte Sandwich-Attacks verhindert, aber die Sequencer-Betreiber verfügen über ein Monopol auf die Transaktionsreihenfolge, das sie ökonomisch nutzen können. Base generierte im August 2025 allein rund 70 Prozent aller Rollup-Profite durch Sequencer-Gebühren, ein Volumen, das die ökonomischen Anreize gegen eine Dezentralisierung der Sequencer-Ebene verdeutlicht.

Das L2BEAT-Stage-Framework misst den Dezentralisierungsgrad der Rollups auf einer dreistufigen Skala.[92] Stage 0 erfordert Selbstidentifikation als Rollup, Datenverfügbarkeit auf L1 und Open-Source-Software. Stage 1 verlangt ein funktionierendes Proof-System, einen Security Council mit mindestens acht Teilnehmern, von denen mindestens die Hälfte extern ist, und eine 75-Prozent-Schwelle für Eingriffe des Councils. Stage 2 erfordert ein permissi-

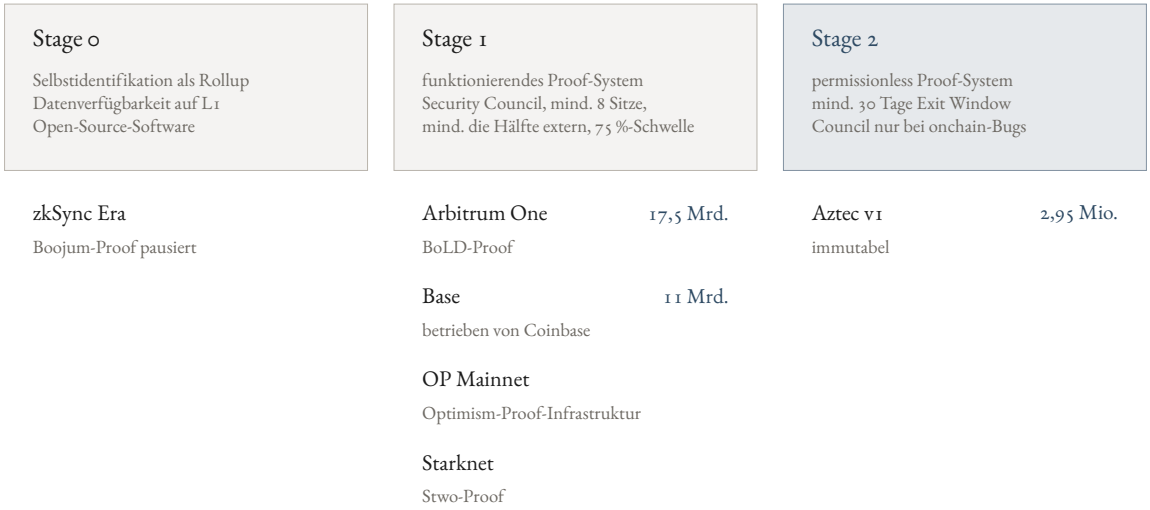
[92] L2BEAT: Stages Framework und Risk Analysis. URL: https://l2beat.com/scaling/summary (abgerufen am 27.03.2026). Die Stage-Klassifizierung folgt dem im Juni 2023 eingeführten Framework, das Dezentralisierung und Vertrauensminimierung misst. Für Vitalik Buterins Analyse der Stage-Übergänge vgl. Buterin, Vitalik (2025): Stages as a framework for evaluating rollup maturity. Blogpost.

onless Proof-System, mindestens 30 Tage Exit Window bei allen Upgrades und eine Beschränkung des Security Council auf onchain-nachweisbare Bugs. Arbitrum One (Stage 1, Total Value Secured 17,5 Milliarden US-Dollar) verfügt über das BoLD-Proof-System und einen öffentlich besetzten Security Council. Base (Stage 1, 11 Milliarden US-Dollar), betrieben von Coinbase, und OP Mainnet (Stage 1) teilen die Optimism-Proof-Infrastruktur. Starknet hat mit dem Stwo-Proof-System Stage 1 erreicht. zkSync Era verbleibt bei Stage 0, weil sein Boojum-Proof-System pausiert wurde. Stage 2, die vollständige Dezentralisierung, existiert nur bei immutablen Projekten mit minimalem Transaktionsvolumen wie Aztec v1 mit einem TVL von 2,95 Millionen US-Dollar. Die Distanz zwischen dem aktuellen Stage-1-Status der führenden Rollups und dem Stage-2-Ziel ist erheblich: Sie erfordert 30-Tage-Exit-Windows statt der aktuellen null bis 17 Tage, die Beschränkung des Security Council auf onchain-nachweisbare Bugs und ein permissionless Proof-System, das ohne privilegierte Akteure operiert. Die kombinierte Transaktionskapazität aller aktiven L2-Systeme übersteigt 10.000 Transaktionen pro Sekunde und hat damit die L1-Kapazität um mehr als zwei Größenordnungen erweitert, wobei rund 65 Prozent aller neuen Smart Contracts inzwischen direkt auf L2-Systemen deployt werden statt auf der Basisschicht.

Forced Inclusion, ein Mechanismus, der es Nutzern erlaubt, Transaktionen unter Umgehung des Sequencers direkt an Layer 1 zu senden und damit sicherzustellen, dass ihre Transaktion auch bei Sequencer-Zensur verarbeitet wird, existiert bei Arbitrum mit einer maximalen Verzögerung von 24 Stunden und bei Optimism mit 12 Stunden, fehlt aber bei Starknet. Neuere Forschung hat das „Hand-off Problem“ identifiziert, bei dem der Sequencer Forced-Inclusion-Transaktionen in der Queue sieht und sie durch State-Manipulation zum Scheitern bringen kann, eine Einschränkung, die den Zensurschutz des Mechanismus in der Praxis reduziert. Die Exit Windows, also die Zeitfenster, die Nutzern nach einem Upgrade-Vorschlag zum Abzug ihrer Mittel bleiben, variieren drastisch: 17 Tage bei Arbitrum, aber null Tage bei Base und OP Mainnet, was bedeutet, dass ein Upgrade ohne Vorankündigung die Regeln ändern kann, unter denen die Nutzer operieren. Ein Exit Window von null Tagen bedeutet, dass der Security Council ein Upgrade aktivieren kann, das die Regeln des Systems ändert, ohne den Nutzern eine Frist zum Abzug ihrer Mittel zu gewähren.

Die Dezentralisierung der Sequencer-Ebene wird über zwei Ansätze verfolgt, die sich in ihrem architektonischen Ambitionsgrad unterscheiden. Shared Sequencing, bei dem mehrere Rollups ein dezentrales Sequencer-Netzwerk teilen, verspricht verbesserte Zensurresistenz und die Möglichkeit, Cross-Rollup-Atomizität herzustellen, hat aber mit der Einstellung des Astria-Projekts im Jahr

2025 einen Rückschlag erlitten, der die technische und ökonomische Fragilität dieses Ansatzes offenlegte. Based Rollups, ein Konzept, das 2023 vorgestellt wurde, verfolgen einen radikaleren Ansatz: Die Ethereum-Validatoren selbst übernehmen das Transaction Ordering, was die Dezentralisierung maximiert, weil die gesamte Validator-Basis der Basisschicht als Sequencer fungiert. Taiko ist das einzige produktive Based Rollup, und der Ansatz erzeugt einen Trade-off zwischen Dezentralisierung und Nutzererfahrung, weil die Blockzeiten des Based Rollup an die 12-Sekunden-Slotzeit der Basisschicht gebunden sind, während zentralisierte Sequencer Sub-Sekunden-Bestätigungen liefern können.



Gesichert ist der Wert dort, wo die Dezentralisierung unvollständig bleibt. Stage 2 erreicht bislang nur ein immutables Projekt mit einem Bruchteil des Werts, den Arbitrum One trägt. Für OP Mainnet und Starknet nennt der Text keinen Wert.

Abbildung 4.8 Das L2BEAT-Stage-Framework. Die Anforderungen der drei Stufen und die Rollups, die sie erreichen, mit dem gesicherten Wert.

Gebrochene Cross-L2-Composability

Die atomare Composability, die Abschnitt 4.1 als emergente Eigenschaft der EVM beschrieben hat, existiert auf der Layer-2-Ebene nicht. Über 50 aktive Layer-2-Systeme operieren mit isoliertem State, und eine Transaktion auf Arbitrum kann nicht atomar mit einer Transaktion auf Base interagieren, obwohl beide Systeme auf derselben Basisschicht settlen. Die Isolation ergibt sich zwingend aus der Architektur: Jedes L2 führt seine Transaktionen in einer eigenen Ausführungsumgebung aus, pflegt seinen eigenen State und postet seine eigenen Batches auf Layer 1, ohne dass die Basisschicht eine Koordination zwischen den L2-States erzwingt. Cross-L2-Transfers erfordern Bridges, spezialisierte Protokolle, die Assets auf einer Chain sperren und auf einer anderen freigeben, und die eigene Trust-Annahmen einführen, die über die Sicherheitsgarantien der Basisschicht hinausgehen. Die Sicherheitsbilanz dieser Bridges ist problematisch: Der kumulative Schaden durch Bridge-Hacks übersteigt 2,8 Milliarden US-Dollar. Der größte Krypto-Diebstahl der Geschichte, der Bybit-Hack vom Februar 2025 mit 1,5 Milliarden US-Dollar, betraf allerdings die Wallet-Infrastruktur einer Börse und keine Bridge.[93] Die Angriffsvektoren sind vielfältig: kompromittierte Multisig-Wallets, fehlerhafte Smart-Contract-Logik, manipulierte Oracles und Social-Engineering-Angriffe auf die Betreiber der Bridge-Infrastruktur. Die Alternative zu Bridges sind die nativen Withdrawal-Mechanismen der Rollups, die bei Optimistic Rollups eine siebentägige Wartezeit erfordern und damit für die meisten Anwendungsfälle zu langsam sind.

Die praktischen Konsequenzen der Fragmentierung betreffen Nutzer und Protokollentwickler gleichermaßen. Ein Nutzer, der seine Assets von Arbitrum nach Base bewegen möchte, muss entweder eine Bridge nutzen und dabei Gebühren, Slippage und ein Sicherheitsrisiko in Kauf nehmen, oder den nativen Withdrawal-Weg über Layer 1 wählen und eine Woche warten. Die Liquidität, die auf der Basisschicht konzentriert war und die atomare Composability des DeFi-Ökosystems ermöglichte, verteilt sich über dutzende isolierte Systeme, was die Effizienz der Märkte reduziert und die Spreads erhöht. Protokollentwickler müssen entscheiden, auf welchem L2 sie deployen, und wenn sie auf mehreren L2s präsent sein wollen, müssen sie separate Deployments pflegen, die nicht miteinander interoperieren.

Die Superchain-Initiative, die 34 OP-Stack-basierte Chains unter einem ge-

[93] Für die kumulativen Bridge-Hack-Schäden vgl. DeFiLlama: Hacks Dashboard und Chainalysis: Crypto Crime Report 2025. Der Bybit-Hack vom Februar 2025 betraf eine Hot-Wallet-Infrastruktur und wird in der Branche als der größte Krypto-Diebstahl der Geschichte eingestuft.

meinsamen Interoperabilitätsstandard zusammenfasst und rund 66 Prozent des gesamten L2-TVL repräsentiert, hat mit dem SuperchainERC20-Standard Fortschritte bei der Intra-Stack-Fungibilität erzielt, also bei der nahtlosen Bewegung von Tokens zwischen Chains, die denselben Software-Stack verwenden. Cross-Stack-Atomizität, also die Möglichkeit atomarer Transaktionen zwischen einer OP-Stack-Chain und einer Arbitrum-Chain, existiert nicht und ist auch nicht absehbar. Die L2-Fragmentierung ist die zentrale architektonische Spannung des Skalierungsmodells: Die Kapazität des Gesamtsystems wächst durch jedes neue Layer-2-System, aber die Kohärenz des Ökosystems nimmt mit jedem isolierten State ab, die Liquidität verteilt sich über immer mehr Systeme, und die Nutzererfahrung wird durch die Notwendigkeit fragmentiert, Assets zwischen Systemen zu bewegen. Die Frage, ob Ethereum ein zusammenhängendes System ist oder eine Ansammlung lose gekoppelter Systeme, die eine gemeinsame Settlement-Schicht teilen, wird in der Bewertung der Koordinationsfunktion adressiert.

Stablecoin-Verankerung und Substitutionsrisiko

Ethereum dominiert die globale Stablecoin-Emission mit einem Marktanteil von 52 bis 54 Prozent, was einem Volumen von circa 166 Milliarden US-Dollar entspricht.[94] USDC, USDT und DAI werden primär auf Ethereum emittiert, und die DeFi-Integration dieser Stablecoins, insbesondere als Sicherheit in Lending-Protokollen, als Basisliquidität in dezentralen Börsen und als Reservemedium in Treasury-Strategien institutioneller Akteure, erzeugt eine Verankerungstiefe, die über die bloße Emission hinausgeht. Diese Verankerung muss jedoch gegen ein konkretes Substitutionsrisiko abgewogen werden: Seit Dezember 2025 liegt das USDC-Transaktionsvolumen auf Solana höher als auf Ethereum. Solana ist eine eigenständige Layer-1-Blockchain mit niedrigeren Gebühren und Sub-Sekunden-Transaktionszeiten, kein Ethereum-L2, und ihr wachsender Anteil am Stablecoin-Volumen zeigt, dass Transaktionsaktivität dorthin migriert, wo die Nutzererfahrung am günstigsten und schnellsten ist, unabhängig von der Verankerungstiefe der emittierenden Chain.

Die Differenzierung, die diese Arbeit beobachtet, liegt in der Unterscheidung zwischen Verankerungstiefe und Transaktionsvolumen: Die Emission, die institutionelle Collateral-Nutzung und die tiefe DeFi-Integration bleiben Ethereum-konzentriert, während das Transaktionsvolumen, insbesondere für Retail-Transfers und Zahlungsanwendungen, dem niedrigsten Gebührenpfad folgt. Ob die-

[94] CoinGecko / DefiLlama: Stablecoin Market Cap by Chain (abgerufen am 27.03.2026). Der Wert von 52 bis 54 Prozent bezieht sich auf den Anteil Ethereums am gesamten Stablecoin-Markt einschließlich L2-Emission.

se Differenzierung langfristig stabil ist oder ob eine anhaltende Volumenmigration die Verankerungstiefe erodiert, weil Emittenten ihre Primäremission dorthin verlagern, wo das Volumen liegt, ist eine offene Frage, die für die Bewertung der funktionalen Unersetzbarkeit relevant ist. Die Parallele zu SWIFTs Situation aus Kapitel 3 ist instruktiv: SWIFT dominiert den internationalen Zahlungsnachrichtenverkehr trotz technisch überlegener Alternativen wie CIPS, weil die installierte Basis und die institutionelle Integration eine Wechselbarriere erzeugen, die über die technische Funktionalität hinausgeht. Ethereum besitzt mit der DeFi-Integration und der Stablecoin-Emission eine analoge installierte Basis, aber die Wechselbarriere ist niedriger als bei SWIFT, weil Stablecoins auf mehreren Chains parallel existieren können und ein Emittent die Primäremission ohne koordinierten Systemwechsel verlagern kann. BNB Chain hält relevante Consumer-Marktanteile, operiert aber mit einem fundamental anderen Dezentralisierungskompromiss, der für die Infrastrukturbewertung eine andere Risikokategorie eröffnet, weil die Chain von einer einzelnen kommerziellen Entität kontrolliert wird.

Der GENIUS Act, am 18. Juli 2025 als erstes US-Bundesgesetz für Stablecoins unterzeichnet, reguliert Stablecoin-Emittenten hinsichtlich Reserveanforderungen, Transparenzpflichten und Lizenzierung, adressiert aber die Protokollschicht nicht.[95] Das Gesetz schafft regulatorische Klarheit auf der Anwendungsschicht, indem es definiert, welche Anforderungen ein Stablecoin-Emittent erfüllen muss, um legal in den USA zu operieren, und stabilisiert damit die Rahmenbedingungen für den größten Anwendungsfall, der auf Ethereums Infrastruktur aufbaut. Die Reserveanforderungen stellen sicher, dass jeder emittierte Stablecoin-Dollar durch qualifizierte Reserven gedeckt ist, und die Transparenzpflichten verlangen regelmäßige Berichte über die Zusammensetzung und den Umfang der Reserven. Für die Infrastrukturbewertung ist der GENIUS Act ein relevantes Datum, weil er zeigt, dass der regulatorische Rahmen sich auf die Anwendungsschicht konzentriert und die Protokollschicht unberührt lässt: Das Gesetz reguliert Circle und Tether als Emittenten, aber es reguliert weder Ethereum als Protokoll noch die Smart Contracts, die USDC und USDT auf der Basisschicht verwalten. Für DeFi insgesamt, also für die dezentralen Protokolle, die auf der Infrastruktur operieren und die keine identifizierbaren Emittenten haben, existiert kein vergleichbarer regulatorischer Rahmen, und die Frage, wie die dezentrale Finanzschicht reguliert werden wird, ob durch Anpassung bestehen-

[95] GENIUS Act: Guiding and Establishing National Innovation for U.S. Stablecoins Act. U.S. Congress (2025), unterzeichnet am 18. Juli 2025.

der Regulierungsinstrumente oder durch neue, an die dezentrale Architektur angepasste Rahmenwerke, bleibt offen.

Die beschriebene Arbeitsteilung, bei der die Basisschicht Settlement und Datenverfügbarkeit bereitstellt und Layer-2-Systeme die Execution übernehmen, wird seit Anfang 2026 durch eine strategische Verschiebung ergänzt. Vitalik Buterin formulierte in einem Blogpost die Zielsetzung, die Basisschicht selbst auf ein Vielfaches ihrer aktuellen Kapazität zu skalieren, durch parallele Transaktionsverarbeitung (EIP-7928), ein Gas Limit von 200.000.000 und langfristig eine tausendfache Kapazitätssteigerung. Diese Verschiebung, die in der Community als L1-first Pivot diskutiert wird, verändert Ethereums Positionierung: von einer reinen Settlement-Schicht, auf der Endnutzer nur indirekt über L2s Transaktionen ausführen, zu einem System, das auch auf der Basisschicht direkte Nutzung in größerem Umfang ermöglichen soll. Die Features, die diese Verschiebung umsetzen sollen, haben den Status PLAN und werden in Kapitel 5 bewertet.

4.5 Governance und Systemevolution

Wie entwickelt sich ein System ohne zentrale Autorität weiter? Die vorangegangenen Abschnitte haben Ethereums Architektur als technisches System beschrieben. Dieser Abschnitt beschreibt die Prozesse, durch die dieses System verändert wird, die Akteure, die diese Veränderungen tragen, und die Spannungen, die aus dem Zusammenspiel von dezentralem Anspruch und operativer Realität entstehen.

Der EIP-Prozess

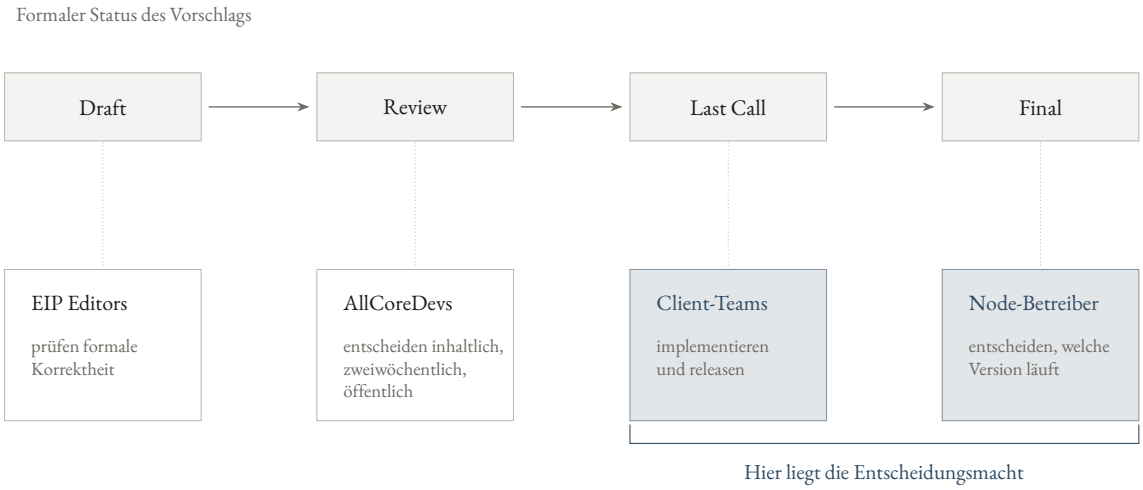
Ethereum Improvement Proposals sind der formale Standardisierungsmechanismus für Protokolländerungen, inspiriert von Pythons PEP-System und Bitcoins BIPs.[96] Der Prozess folgt einer definierten Sequenz: Ein Vorschlag wird als Draft eingereicht, wobei jeder Akteur unabhängig von seiner institutionellen Zugehörigkeit einen Vorschlag einreichen kann. Der Draft durchläuft ein Review, in dem technische Korrektheit, Spezifikationsvollständigkeit und Kompatibilität mit bestehenden Protokollelementen geprüft werden, erreicht den Status Last Call, in dem die Community eine finale Einspruchsfrist erhält, und wird bei Akzeptanz als Final markiert. Im Jahr 2025 wurden 230 EIPs eingereicht, von denen 37 akzeptiert wurden, eine Akzeptanzrate von 16 Prozent, die die Selektivi-

[96] EIP-1: EIP Purpose and Guidelines. URL: https://eips.ethereum.org/EIPS/eip-1. Für die EIP-Statistik 2025 vgl. Ethereum Magicians Forum und EIPs.ethereum.org (abgerufen am 27.03.2026).

tät des Prozesses reflektiert und zeigt, dass die Mehrheit der Vorschläge entweder technisch unausgereift, redundant oder zu kontrovers für eine Aufnahme ist. EIP Editors prüfen die formale Korrektheit und Vollständigkeit der Vorschläge. Inhaltliche Entscheidungen über die Aufnahme eines EIP in ein konkretes Upgrade fallen in den AllCoreDevs-Calls, zweiwöchentlichen Videokonferenzen der Client-Entwicklerteams, die öffentlich gestreamt, aufgezeichnet und protokolliert werden. Die Aufzeichnungen sind ein wesentliches Transparenzmerkmal des Prozesses: Jeder Interessierte kann nachvollziehen, welche Argumente für und gegen die Aufnahme eines EIP vorgebracht wurden und wer welche Position vertreten hat.

Das Verfahren ist transparent, dokumentiert und selektiv, operiert aber ohne formale Autorität: Kein Gremium kann eine Entscheidung erzwingen, kein Abstimmungsmechanismus kann eine Mehrheit binden, und kein institutionelles Mandat legitimiert die Entscheidungsträger jenseits ihrer technischen Kompetenz und ihres Commitments zum Ökosystem. Die Entscheidungsmacht liegt bei den Client-Teams, die die Software releasen, und bei den Node-Betreibern, die entscheiden, welche Version sie betreiben. Ein Upgrade, das von den Client-Teams implementiert, aber von einer signifikanten Minderheit der Node-Betreiber abgelehnt wird, würde zu einer Kettenspaltung führen, ein Risiko, das als disziplinierendes Element wirkt und den Konsensdruck im Vorfeld der Entscheidung erhöht. Ethereum hat bewusst keine On-Chain-Governance implementiert, also keine Token-Voting-Mechanismen, die Protokolländerungen durch Abstimmung der Token-Halter legitimieren würden. Das Entscheidungsprinzip folgt dem Modell, das das Internet aus Kapitel 3 geprägt hat: Rough Consensus and Running Code, eine Formulierung der Internet Engineering Task Force, die formale Abstimmungen durch iterative technische Konsensfindung ersetzt.[97] Das einzige Governance-Instrument, das Validatoren direkt ausüben, ist das Gas-Limit-Signaling, durch das die Verdopplung des Limits von 30.000.000 auf 60.000.000 ohne Hard Fork erfolgte, wie Abschnitt 4.2 beschrieben hat.

[97] Die Formulierung „Rough Consensus and Running Code“ geht auf David Clark zurück, der sie 1992 auf einem IETF-Meeting prägte. Vgl. RFC 7282: On Consensus and Humming in the IETF. Internet Engineering Task Force, 2014.



Kein Gremium kann eine Entscheidung erzwingen, kein Abstimmungsmechanismus bindet eine Mehrheit. Ethereum hat bewusst keine On-Chain-Governance. 2025 wurden über 230 EIPs eingereicht, 37 akzeptiert.

Abbildung 4.9 Der Ethereum-Governance-Prozess. Der formale Status eines Vorschlags und die Instanzen, bei denen die Entscheidung tatsächlich liegt.

Die Ethereum Foundation und dezentrale Finanzierung

Die Ethereum Foundation, gegründet 2014 als Schweizer Stiftung, ist die älteste und finanziell bedeutendste Organisation im Ethereum-Ökosystem. Ihr Treasury wird auf 850 bis 950 Millionen US-Dollar geschätzt, wovon 70.000 ETH gestakt und circa 5.800 ETH in DeFi-Vaults angelegt sind.[98] Die Stiftung finanziert Forschung, Entwicklung, Bildung und Community-Initiativen, hat aber bewusst keine Protokollkontrolle: Sie kann keine Protokolländerungen anordnen, keine Upgrades erzwingen und keine Transaktionen zensieren. Die „Subtraction"-Philosophie, die der aktuelle Führungskreis der Stiftung vertritt, sieht vor, dass sich die EF progressiv aus operativen Funktionen zurückzieht und ihre Rolle auf die Bereiche beschränkt, die das Ökosystem aus eigener Kraft nicht finanzieren kann, insbesondere langfristige Grundlagenforschung, formale Verifikation und die Koordination der Client-Entwicklung.

Die Einschränkungen dieser Struktur sind erkennbar und werden innerhalb des Ökosystems offen diskutiert. Die Stiftung wird von einem Board kontrolliert, das keiner protokollären Rechenschaftspflicht unterliegt. Ihre Entscheidungen über Mittelvergabe, Personalpolitik und strategische Prioritäten sind freiwillige Transparenzakte, die der jährliche Report dokumentiert, aber keine protokollpflichtigen Offenlegungen, die durch Governance-Mechanismen erzwun-

[98] Ethereum Foundation: Report 2024. URL: https://ethereum.foundation/report-2024.pdf. Für aktuelle Treasury-Schätzungen vgl. Arkham Intelligence: Ethereum Foundation Wallet Tracking (abgerufen am 18.03.2026). Die Angabe von $850 bis $950 Mio. ist eine Schätzung auf Basis der veröffentlichten Bestände und der Marktentwicklung seit dem letzten Report.

gen werden könnten. Die Frage, wer die Forschungsagenda setzt und welche Projekte finanziert werden, hat direkte Auswirkungen auf die Richtung der Protokollentwicklung, auch wenn die Stiftung formal keine Entscheidungsgewalt über Protokolländerungen besitzt. Die Konzentration einer substanziellen Treasury in einer einzigen Organisation erzeugt ein Zentralisierungsrisiko, das mit dem dezentralen Anspruch des Protokolls in Spannung steht, insbesondere weil die Stiftung durch ihre Finanzierungsentscheidungen die Richtung der Protokollentwicklung faktisch mitbestimmt. Im Jahr 2024 und 2025 hat die EF mehrfach interne Umstrukturierungen vorgenommen, die Diskussionen über die Governance der Stiftung selbst ausgelöst haben, ein Zeichen dafür, dass die Spannung zwischen zentralisierter Organisationsstruktur und dezentralem Ökosystem auch innerhalb der Institution wahrgenommen wird. Protocol Guild, ein kollektives Finanzierungsinstrument für Core-Entwickler mit über 190 Mitgliedern, hat seit seiner Gründung mehr als 50 Millionen US-Dollar aus freiwilligen Spenden des Ökosystems erhalten und stellt einen dezentralen Gegenpol zur EF-Finanzierung dar.[99] Das Instrument verteilt die empfangenen Mittel zeitgewichtet an die Mitglieder, die aktiv an der Protokollentwicklung arbeiten, und schafft damit einen Anreiz für langfristiges Engagement, der unabhängig von der Ethereum Foundation operiert. Die Finanzierung durch Protocol Guild ist aber weder protokollär verankert noch langfristig planbar, sondern abhängig von der fortgesetzten Spendenbereitschaft eines Ökosystems, das aus ökonomischem Eigeninteresse handelt, und keine vertragliche Verpflichtung zur Fortführung eingegangen ist. Das Gesamtbild der Protokollfinanzierung zeigt eine mehrstufige Struktur: Die Ethereum Foundation als größter Einzelförderer, Protocol Guild als kollektiver Mechanismus, einzelne Unternehmen wie ConsenSys und Paradigm, die Client-Teams finanzieren, und Grant-Programme verschiedener L2-Ökosysteme die spezifische Entwicklungsarbeit unterstützen. Die Abhängigkeit der Protokollentwicklung von freiwilliger Finanzierung, die weder durch Protokollgebühren noch durch institutionelle Pflichten gesichert ist, unterscheidet Ethereum von den Referenzinfrastrukturen aus Kapitel 3, die durchgehend über regulierte Gebührenmodelle, steuerfinanzierte Haushalte oder institutionelle Mitgliedsbeiträge verfügen.

[99] Protocol Guild: Documentation and Membership. URL: https://protocol-guild.readthedocs.io (abgerufen am 27.03.2026).

Upgrades als Risiko und Beweis

Der in Abschnitt 4.1 dokumentierte DAO-Fork von 2016 bleibt der einzige Fall, in dem die Community einen Zustandseingriff vornahm, und er wurde seither nie wiederholt. Die vier Post-Merge-Upgrades, Shapella, Dencun, Pectra und Fusaka, verliefen alle ohne Kettenspaltung, was die Reifung des Governance-Prozesses empirisch belegt: Die Community hat vier komplexe Protokolländerungen koordiniert, implementiert und aktiviert, ohne dass das Netzwerk gespalten oder unterbrochen wurde. Die Upgrade-Kadenz von ungefähr einem Major Fork pro Jahr seit dem Merge zeigt ein System, das sich aktiv weiterentwickelt, und jedes Upgrade hat substanzielle Verbesserungen eingeführt, von Staking-Withdrawals über Blob-Transactions bis zu Account Abstraction.

Die Komplexitätsakkumulation ist dabei ein steigendes Risiko: Pectra bündelte 11 EIPs in einem einzigen Release, die Interaktionen zwischen diesen EIPs mussten über fünf Consensus- und fünf Execution-Client-Implementierungen hinweg korrekt implementiert werden, und der in Abschnitt 4.1 beschriebene Prysm-Bug bei Fusaka war eine direkte Folge der Interaktion zwischen neuen Protokollelementen und bestehenden Client-Implementierungen. Die Koordinationskosten steigen mit der Zahl der beteiligten Teams und der Komplexität der Änderungen: Jeder EIP muss in zehn unabhängigen Implementierungen korrekt umgesetzt werden, die Interaktionen zwischen den EIPs innerhalb eines Upgrades müssen über alle zehn Implementierungen konsistent sein, und die Testphase auf den Testnetzwerken muss genügend Edge Cases abdecken, um Mainnet-Fehler zu vermeiden. Die Ethereum-Community diskutiert aktiv, ob die aktuelle Bündelungsstrategie, bei der viele EIPs in einem Release zusammengefasst werden, durch kleinere, häufigere Upgrades ersetzt werden sollte, um das Fehlerrisiko pro Release zu reduzieren. Die Frage, ob das Governance-Modell, das auf Rough Consensus und freiwilliger Kooperation beruht, in der Lage ist, die wachsende Komplexität langfristig zu bewältigen, ohne entweder die Upgrade-Kadenz zu verlangsamen oder die Fehlerrate zu erhöhen, ist offen und wird in der Bewertung der Langfristigen Stabilität adressiert.

Die Fähigkeit des Governance-Systems, auf akute Sicherheitsvorfälle zu reagieren, hat historische Präzedenzfälle jenseits des DAO-Forks. Im September 2016 erzwang eine gezielte Denial-of-Service-Attacke auf den Geth-Client zwei Emergency-Hard-Forks innerhalb weniger Wochen, Tangerine Whistle und Spurious Dragon, eine außergewöhnlich schnelle Reaktion, die die Handlungsfähigkeit des Governance-Systems in akuten Krisen belegte. Die Grenze dieser Handlungsfähigkeit liegt im Fehlen eines Pause-Mechanismus: Wenn ein kritischer

Bug auf Protokollebene deployt ist, kann niemand das Netzwerk anhalten. Die einzige Antwort ist ein Emergency-Hard-Fork, der die Koordination aller Client-Teams erfordert und Wochen in Anspruch nehmen kann. Für ein System, das Vermögenswerte in dreistelliger Milliardenhöhe sichert, ist das eine relevante Einschränkung, die in der Bewertung der Adaptive Governance berücksichtigt wird.

4.6 Emergente Eigenschaften: Was die Architektur ermöglicht

Die Abschnitte 4.1 bis 4.5 haben Ethereums Architektur als System aus Komponenten beschrieben: EVM, Konsensprotokoll, Sicherheitsökonomie, Skalierungsarchitektur und Governance. Jede dieser Komponenten hat spezifische Stärken und Einschränkungen, die in den jeweiligen Abschnitten benannt wurden. Die Eigenschaften, die den Infrastrukturanspruch begründen, lassen sich jedoch in keiner einzelnen Komponente lokalisieren. Sie emergieren aus dem Zusammenspiel der Architekturelemente und erzeugen Fähigkeiten, die über die Summe der Einzelkomponenten hinausgehen. Die Analogie zur Infrastrukturtheorie aus Kapitel 2 ist direkt: Stars relationale Perspektive hat gezeigt, dass Infrastruktur in Relation zu organisierten Praktiken entsteht, und die folgenden fünf Eigenschaften beschreiben genau diese Relationen, also die Fähigkeiten, die das System für seine Nutzer erzeugt und die den Infrastrukturanspruch empirisch begründen. Fünf solcher Eigenschaften lassen sich benennen, die jeweils aus der Interaktion spezifischer Komponenten entstehen und deren infrastrukturelle Relevanz sich aus dem theoretischen Rahmen von Kapitel 2 erschließt.

Die erste emergente Eigenschaft ist Permissionless Deployment. Aus dem Zusammenspiel der EVM als offener Ausführungsumgebung, dem permissionless Zugang zum Netzwerk und dem Gas-Markt als einziger Zugangsvoraussetzung entsteht ein System, in dem jeder Akteur Code deployen kann, ohne eine Genehmigung einholen zu müssen. Frischmanns Argument, dass offener Zugang zu Infrastruktur ökonomisch effizienter ist als die Einschränkung durch private Eigentumsrechte, weil der gesellschaftliche Gesamtnutzen mit der Breite der Nutzung steigt, findet hier eine technische Implementierung.[100] Die Parallele zum End-to-End-Prinzip des Internets, das Kapitel 3 als architektonische Grundlage der Innovationsfähigkeit des Netzes beschrieben hat, ist direkt: Van Schewick hat gezeigt, dass das End-to-End-Prinzip die Entstehung von World Wide Web, E-Commerce und Cloud Computing ermöglichte, indem es die Innovationsbar-

[100] Vgl. Frischmann 2012 sowie die Darstellung in Kapitel 2, Abschnitt 2.1.

rieren an den Rändern des Netzes senkte.[101] Die EVM erzeugt eine analoge Dynamik für programmierbare Finanzlogik und dezentrale Anwendungen, und die Breite der auf Ethereum aufbauenden Aktivitäten illustriert die generative Kapazität des offenen Zugangs. Die 31.869 aktiven Entwickler, die der Electric Capital Developer Report für September 2025 dokumentiert, arbeiten an Protokollen, die Finanzmärkte, Identitätssysteme, Supply-Chain-Tracking, dezentrale Governance und digitale Kunst umfassen, und jedes dieser Anwendungsfelder entstand aus der Initiative einzelner Akteure, die die Infrastruktur nutzten, ohne eine Genehmigung einzuholen.[102] Das DeFi Total Value Locked von circa 100 Milliarden US-Dollar auf Ethereum L1 und L2 zusammen quantifiziert den ökonomischen Umfang der produktiven Aktivitäten, die auf dieser Infrastruktur aufbauen. Die Einschränkung liegt in den Gas-Kosten, die auf Layer 1 für viele Anwendungen prohibitiv sind und das Deployment faktisch auf Layer-2-Systeme verlagern, wo die Infrastruktureigenschaften, insbesondere die Dezentralisierung und die Composability, eingeschränkt sind.

Die zweite emergente Eigenschaft ist atomare Composability. Aus dem Zusammenspiel der EVM mit dem gemeinsamen State und der sequentiellen Blockausführung entsteht die Möglichkeit, beliebig viele Protokollinteraktionen in einer einzigen Transaktion zu verketten, wie Abschnitt 4.1 an Flash Loans illustriert hat. Die infrastrukturelle Implikation reicht über den technischen Mechanismus hinaus: Protokolle können aufeinander aufbauen, ohne bilaterale Vereinbarungen treffen zu müssen, weil die Kompatibilität auf der Ebene der gemeinsamen Ausführungsumgebung hergestellt wird. Ein Entwickler, der ein neues DeFi-Protokoll erstellt, kann die Liquiditätspools von Uniswap, die Lending-Märkte von Aave und die Stablecoin-Logik von MakerDAO in seine eigene Anwendung integrieren, ohne dass eine Vertragsbeziehung zu einem dieser Protokolle besteht, ohne dass eine Genehmigung eingeholt werden muss und ohne dass die Betreiber der genutzten Protokolle von der Integration erfahren müssen. DeFi als Ökosystem, dessen ökonomischen Umfang der vorige Absatz beziffert hat, ist das Ergebnis dieser Eigenschaft, eine emergente Schicht produktiver Aktivitäten, die auf der Infrastruktur aufbaut, ohne von ihr geplant oder antizipiert worden zu sein. Das ist Frischmanns Konzept des Input-Charakters von Infrastruktur in seiner präzisesten Form: Die Infrastruktur schafft den Ermögli-

[101] Van Schewick, Barbara (2010): Internet Architecture and Innovation. MIT Press. Vgl. die Referenz in Kapitel 3, Abschnitt 3.1.2.

[102] Electric Capital: Developer Report, September 2025. Die Zahl von 31.869 aktiven Entwicklern umfasst öffentliche Repository-Aktivität im Ethereum-Ökosystem. DefiLlama: Ethereum DeFi TVL (abgerufen am 27.03.2026).

chungsraum, und die produktiven Aktivitäten der Nutzer schaffen den Wert, der die Infrastruktur rechtfertigt. Die Stärke der Composability liegt in ihrer Permissionlessness, die Schwäche in ihren Grenzen: Auf Layer-2-Ebene ist diese Composability gebrochen, wie Abschnitt 4.4 dokumentiert hat, und die Fragmentierung über mehr als 50 isolierte Systeme untergräbt die Eigenschaft, die das Ökosystem hervorgebracht hat.

Die dritte emergente Eigenschaft ist die unabhängige Verifizierbarkeit des Systemzustands. Aus dem Zusammenspiel der Multi-Client-Architektur, des Merkle Patricia Trie und des Peer-to-Peer-Netzwerks entsteht die Möglichkeit, den gesamten Systemzustand ohne Vertrauen in einen Intermediär zu überprüfen. Technisch ist diese Verifikation auf Consumer-Hardware mit einer 2-TB-NVMe-SSD und 16 bis 32 GB RAM möglich, bei Gesamtkosten von 500 bis 1.500 US-Dollar. Ein Nutzer, der einen Full Node betreibt, kann jede Transaktion, jeden Kontostand und jeden Smart-Contract-Zustand unabhängig verifizieren, ohne einer externen Quelle vertrauen zu müssen, weil sein Node alle Blöcke seit dem Genesis-Block nachvollzogen und jeden Zustandsübergang eigenständig berechnet hat. Operativ nutzen circa 70 Prozent der Nutzer RPC-Provider wie Infura und Alchemy, die als zentralisierte Vermittler zwischen Nutzer und Netzwerk fungieren und deren Ausfall den Nutzerzugang unterbricht, ohne dass das Protokoll selbst betroffen ist. Der Infura-Ausfall im November 2020, bei dem MetaMask und zahlreiche dezentrale Anwendungen für Stunden nicht erreichbar waren, obwohl das Ethereum-Protokoll durchgehend operierte, illustrierte die Diskrepanz zwischen der protokollären Dezentralisierung und der operativen Zentralisierung auf der Zugangsschicht. Dezentrale RPC-Alternativen wie Pocket Network und dRPC existieren, erreichen aber nur einen einstelligen Prozentteil des Marktanteils, weil institutionelle Nutzer die Service-Level-Agreements und die Latenzstabilität zentralisierter Anbieter bevorzugen. Die Möglichkeit zur unabhängigen Verifikation ist gegeben, ihre Nutzung ist Opt-in mit ökonomischen und technischen Barrieren. Das unterscheidet Ethereum von traditionellen Systemen, in denen die Zustandskorrektheit von institutioneller Autorität behauptet wird, etwa von Banken, Clearing-Häusern oder Zentralregistern, und in denen der Nutzer keine technische Möglichkeit hat, die Behauptung eigenständig zu prüfen.

Die vierte emergente Eigenschaft ist kryptographisches Eigentum. Aus dem Zusammenspiel von Private Keys, Smart Contracts und der in Abschnitt 4.2 beschriebenen Settlement-Finality entsteht eine Form von Eigentumskontrolle, die durch kryptographische Beweise ausgeübt wird, ohne dass eine Institution sie gewähren muss. Ein Nutzer, der seinen Private Key kontrolliert, hat unbedingte

Kontrolle über seine Assets auf Protokollebene, ohne dass eine Bank, eine Börse oder eine Behörde diese Kontrolle erteilen oder entziehen kann. Die Unbedingtheit dieser Kontrolle ist eine direkte Konsequenz der kryptographischen Architektur: Der Private Key ist die einzige Information, die benötigt wird, um eine gültige Transaktion zu signieren, und keine Instanz im System kann eine korrekt signierte Transaktion blockieren, solange der Nutzer Gas-Gebühren bezahlt und die Transaktion die Protokollregeln einhält. Selbstverwahrung ist der Default, die Delegation an einen Intermediär wie eine zentralisierte Börse eine bewusste Entscheidung des Nutzers, die jederzeit reversibel ist. Die Kehrseite dieser Eigenschaft ist ihre Unversöhnlichkeit: Schlüsselverlust ist irreversibel, weil keine Instanz einen neuen Schlüssel ausstellen oder den Zugang wiederherstellen kann, und die in Abschnitt 4.1 beschriebene Account Abstraction adressiert diese Barriere erst teilweise, weil die Wallet-Integration noch in der Umsetzung ist und die Mehrzahl der Nutzer weiterhin mit klassischen Externally Owned Accounts operiert. Die empirische Realität zeigt ein Spannungsfeld: Ein wachsender Anteil des ETH-Bestands wird auf zentralisierten Börsen verwahrt, deren Nutzer die Selbstverwahrungseigenschaft faktisch aufgeben, sei es aus Bequemlichkeit, sei es aus Unkenntnis der Alternative. Die protokolläre Möglichkeit zur Selbstverwahrung und ihre tatsächliche Nutzung klaffen auseinander, eine Diskrepanz, die für die Bewertung der Sicherheitslast relevant ist.

Die fünfte emergente Eigenschaft ist programmierbare Verbindlichkeit. Aus dem Zusammenspiel von Smart Contracts, der kryptographisch erzwungenen Finality und dem Slashing-Mechanismus entsteht eine Durchsetzungsschicht für Vereinbarungen, die ohne externe Instanz operiert. Grimmelmann und Windawi haben gezeigt, dass Blockchains als Semicommons funktionieren, nach der in Kapitel 2 gesetzten Definition als Systeme also, in denen private und gemeinsame Ressourcennutzung verschränkt sind und in denen die Regeln durch den Code durchgesetzt werden.[103] Smart Contracts erzwingen Vereinbarungen automatisch: Ein Lending-Protokoll liquidiert eine unterbesicherte Position ohne Gerichtsbeschluss, sobald der Wert der hinterlegten Sicherheiten unter die im Code definierte Schwelle fällt. Ein dezentrales Börsenprotokoll führt einen Swap exakt zu den Konditionen aus, die der Algorithmus vorgibt, ohne Gegenparteirisiko. Das Slashing-System, das Abschnitt 4.3 beschrieben hat, bestraft Fehlverhalten von Validatoren ohne Behörde und ohne physisches Gewaltmonopol. Die Durchsetzung ist algorithmisch und deterministisch: Wenn die definierten Bedingungen eintreten, wird die vorgesehene Konsequenz ausgeführt,

[103] Vgl. Grimmelmann/Windawi 2023, S. 1097–1129, sowie die Darstellung in Kapitel 2, Abschnitt 2.1.

unabhängig davon, ob die betroffene Partei einverstanden ist oder ob eine Instanz die Durchsetzung anordnet. Diese Eigenschaft ersetzt nicht das Rechtssystem, das Kapitel 3 als institutionelle Meta-Infrastruktur beschrieben hat, aber sie erzeugt eine komplementäre Durchsetzungsschicht für Fälle, in denen institutionelle Durchsetzung zu langsam, zu teuer, jurisdiktionsübergreifend nicht verfügbar oder für den spezifischen Anwendungsfall nicht vorgesehen ist. Die praktische Relevanz dieser Eigenschaft zeigt sich in der DeFi-Nutzung: Lending-Protokolle mit einem kumulierten Volumen von Milliarden US-Dollar operieren ohne eine einzige gerichtliche Vereinbarung zwischen den Parteien, und die Sicherheit der Vereinbarung beruht auf der Korrektheit des Codes und der Finalität der Basisschicht. Die Grenze dieser Eigenschaft liegt in der Ausdrucksfähigkeit des Codes: Was der Smart Contract nicht abbilden kann, insbesondere Streitigkeiten über Absichten, Interpretationen, fahrlässiges Verhalten und außervertragliche Ansprüche, bleibt auf institutionelle Durchsetzung angewiesen, und die Schnittstelle zwischen Code-basierter und institutioneller Durchsetzung ist rechtlich weitgehend ungeklärt.

DeFi-Protokolle nutzen für Preisinformationen externe Datenquellen, sogenannte Oracles, die außerhalb des Ethereum-Protokolls operieren. Oracle-Netzwerke wie Chainlink liefern Preisfeeds von externen Märkten an Smart Contracts und erzeugen damit eine zusätzliche Vertrauensschicht, die nicht durch das Konsensprotokoll abgesichert ist. Der Bewertungsrahmen schließt die Oracle-Schicht durch die in Kapitel 2 definierte Oracle-Grenze bewusst von der Bewertung aus, weil Oracles Anwendungsschicht-Komponenten sind, nicht Infrastrukturschicht.

Diese fünf Eigenschaften begründen den Infrastrukturanspruch, den die folgenden Abschnitte prüfen. Die Bewertung fragt, ob die aktuelle Ausprägung dieser Eigenschaften dem Anspruch einer fundamentalen digitalen Infrastruktur genügt, denn die Existenz einer Eigenschaft und die Angemessenheit ihrer Ausprägung sind zwei verschiedene Fragen, und die Antwort auf die zweite erfordert die systematische Prüfung gegen die zwölf Kriterien. Ein System kann Permissionless Deployment ermöglichen und trotzdem an der Zugangsschwelle scheitern, wenn die Gas-Kosten den Zugang faktisch beschränken. Es kann Trustless Verification anbieten und trotzdem eine hohe Vertrauenslast erzeugen, wenn die Mehrheit der Nutzer über zentralisierte Intermediäre zugreift. Es kann programmierbare Verbindlichkeit herstellen und trotzdem die Anforderungen an Koordination verfehlen, wenn die L2-Fragmentierung die Kohärenz des Systems untergräbt. Die Bewertung muss diese Spannungen zwischen Möglichkeit und Realität systematisch erfassen, und genau dafür wurden die zwölf Kriterien

konzipiert.

Vier Eigenschaften, von denen zwei in diesem Abschnitt beschrieben wurden, lassen sich mit den Indikatoren des Bewertungsrahmens nicht vollständig operationalisieren. Die permissionless Composability, die Fähigkeit, beliebige Protokoll-Kombinationen ohne Genehmigung zu schaffen und atomar auszuführen, verlangte eine formale Modellierung der Interaktionsmöglichkeiten zwischen Smart Contracts. Die kryptographische Systemzustandsverifikation, die Möglichkeit jedes Nutzers, den gesamten Netzwerkzustand unabhängig zu prüfen, verlangte eine empirische Erhebung der tatsächlichen Verifikationspraxis. Die dezentrale Selbstentwicklungsfähigkeit, die Kapazität des Systems, sich ohne zentrale Autorität weiterzuentwickeln, verlangte über die hier dokumentierte Prozessbeschreibung hinaus eine langfristige institutionelle Analyse. Die Privacy schließlich ist auf Protokollebene nicht verankert, was Anwendungsfälle mit Vertraulichkeitsbedarf einschränkt, insbesondere institutionelle Akteure mit regulatorischen Datenschutzanforderungen. Diese vier Dimensionen erscheinen in der Synthese (Abschnitt 6.3) als Forschungsagenda, weil sie für eine vollständige Infrastrukturbewertung relevant sind, aber mit den Methoden und Indikatoren dieser Arbeit nicht hinreichend operationalisiert werden können.

4.7 Dimension I: Strukturelle Fundierung

Die vorangegangenen Abschnitte haben Ethereum als zusammenhängendes System beschrieben: seine Architektur, den Transaktionslebenszyklus, die Sicherheitsökonomie, das Skalierungsmodell, die Governance-Strukturen und die institutionelle Einbettung. Die Bewertung, die nun folgt, wendet die zwölf Kriterien des Bewertungsrahmens auf diesen beschriebenen Gegenstand an. Sie referenziert die Architektur, sie erzählt sie nicht nach. Jedes Kriterium wird auf der vierstufigen Skala bewertet, und jede Bewertung macht die Drei-Ebenen-Logik im Argumentationsfluss erkennbar: Was ermöglicht das Protokoll, was davon ist operativ realisiert, und reicht das Zusammenspiel für den Infrastrukturanspruch.

Die erste Dimension prüft, ob Ethereum die strukturellen Voraussetzungen mitbringt, die eine fundamentale Infrastruktur tragen. Vier Kriterien operationalisieren diese Frage. Zwei davon, Sicherheits- und Vertrauenslast (I.2) und Minimale tragfähige Garantien (I.4), sind als Kritische Bedingungen verankert, was bedeutet, dass ein Befund auf „Offen" bei einer der beiden das Gesamturteil über die M3-Kaskade auf „Bedingt geeignet" deckeln würde, unabhängig von der Leistung in allen übrigen Kriterien. Zwei der drei Kritischen Bedingungen des gesamten Bewertungsrahmens liegen damit in dieser Dimension.

I.1 Funktionale Unersetzbarkeit

Die erste Frage an ein System, das den Infrastrukturanspruch erhebt, ist die nach seiner Verankerung: Ist Ethereum strukturell so positioniert, dass es als Schelling Point für dezentrale Koordination fungiert, als der Punkt also, auf den Akteure ohne explizite Abstimmung konvergieren?

Das Protokoll produziert diese Verankerung nicht durch technische Sperrmechanismen. Es gibt kein erzwungenes Vendor-Commitment, keine exklusive API und keinen proprietären Netzwerkstack. Die in Abschnitt 4.1 beschriebene offene Architektur schafft die Voraussetzungen für Netzwerkeffekte, erzwingt sie aber nicht. In Frischmanns Infrastrukturterminologie ist Ethereum damit ein System, das seine Unersetzbarkeit durch die Breite und Tiefe der produktiven Aktivitäten herstellt, die auf ihm aufbauen, nicht durch die Zugangsschranke, die es errichtet.[104] Die Implikation ist direkt: Ein erzwungener Lock-in wäre mit dem Neutralitätsanspruch unvereinbar, und emergente Verankerung ist die einzige Form, die mit dem Anspruch einer globalen und neutralen Infrastruktur

[104] Vgl. Frischmann 2012, S. 61–96, zur Abgrenzung von Infrastruktur als Ermöglichungsstruktur, deren Wert sich in den Aktivitäten realisiert, die sie ermöglicht.

kompatibel bleibt. Die Cloud-Infrastruktur, eine der Referenzinfrastrukturen aus Kapitel 3, illustriert das Muster: AWS ist trotz fehlenden Vendor-Lock-ins de facto unersetzbar, weil die Akkumulation von Tooling, Integrationen und Fachkompetenz Wechselkosten erzeugt, die kein technischer Sperrmechanismus erreichen würde.

Die Nutzungsrealität zeigt eine Verankerung, die in drei Dimensionen über den Schwellenwert hinausreicht. Die in Abschnitt 4.6 dokumentierte DeFi-TVL-Dominanz beläuft sich auf rund 100 Milliarden US-Dollar unter Ethereum-Sicherheit und repräsentiert konsistent über 60 Prozent des gesamten On-Chain-gesicherten DeFi-Kapitals, wobei die Konzentration innerhalb des L2-Ökosystems einer Power-Law-Verteilung folgt: Base hält rund 46,6 Prozent des L2-DeFi-TVL, Arbitrum rund 30,9 Prozent, und die übrigen mehr als 48 L2s teilen sich weniger als 25 Prozent. Diese Konzentration auf Ethereum-native Systeme ist Ausdruck von Liquiditätsnetzwerkeffekten, weil DeFi-Protokolle auf eine Liquiditätstiefe zugreifen, die auf keiner anderen Plattform in vergleichbarer Form verfügbar ist. Die Stablecoin-Emission auf Ethereum beträgt rund 166 Milliarden US-Dollar und macht 52 bis 54 Prozent des Gesamtmarkts aus, wobei die drei größten Stablecoins USDC, USDT und DAI ihre tiefste DeFi-Integration auf Ethereum haben.[105] Die strategische Bedeutung dieser Verankerung wird durch den GENIUS Act (18. Juli 2025) als erstes US-Bundesgesetz für Stablecoins verstärkt, der den regulatorischen Rahmen schafft, innerhalb dessen die Stablecoin-Emission operiert, und der die institutionelle Legitimation der auf Ethereum emittierten Dollar-Derivate erhöht. Das Developer-Ökosystem umfasst 31.869 aktive Entwickler (Stand September 2025), den historischen Höchstwert und über 70 Prozent aller Blockchain-Entwickler.[106] Die Entwickler-Verankerung ist die stabilste der drei Dimensionen, weil die Ethereum-spezifische Toolchain hohe Wechselkosten erzeugt: Ein Entwickler, der zwei Jahre in EVM, Solidity und Foundry investiert hat, wird nicht ohne erheblichen Produktivitätsverlust auf eine andere Plattform wechseln, und diese Trägheit ist eine strukturelle Barriere, die nicht von Marktzyklen abhängt.

Die Schock-Resilienz dieser Verankerung ist empirisch belegt. Im Marktzyklus 2022 kollabierte der DeFi-TVL absolut um über 75 Prozent, doch Ethereums relative Dominanzposition blieb erhalten, was darauf hindeutet, dass die Verankerung über den Preismechanismus hinausgeht und durch Netzwerkeffek-

[105] Daten zur Stablecoin-Marktkapitalisierung auf Ethereum: DefiLlama, Stablecoins Dashboard, abgerufen Anfang 2026.

[106] Electric Capital (2025): Developer Report, September 2025. Die Methodik zählt aktive Entwickler als Personen, die in den letzten 30 Tagen Code zu einem Ethereum-bezogenen Open-Source-Repository beigetragen haben.

te aus Liquidität, Composability und Toolchain gehalten wird. Einschränkungen sind gleichwohl dokumentiert. Die in Abschnitt 4.4 beschriebene Stablecoin-Volumenmigration auf Solana zeigt, dass Ethereum zwar die primäre Issuance-Plattform bleibt, aber Transaktionsvolumen zunehmend auf andere Netzwerke verlagert wird. Die L2-Autonomie, die sich in eigenständigen Treasuries (Arbitrum DAO über 3,5 Milliarden US-Dollar), proprietären Geschäftsmodellen (Base als Coinbase-Produkt) und eigenen Governance-Strukturen manifestiert, bedeutet, dass die technische Anbindung an Ethereum bei wachsender organisatorischer Unabhängigkeit besteht. Der Multi-Chain-Drift institutioneller Akteure, den BlackRock BUIDL mit seinem Deployment auf sieben Chains seit März 2025 exemplarisch zeigt, relativiert die Exklusivität der Ethereum-Verankerung.

In Frischmanns Terminologie ist der Schelling-Point-Charakter eine Ermöglichungsfunktion: Die Verankerung erzeugt ihren Wert dadurch, dass sie produktive Aktivitäten ermöglicht, und die Breite dieser Aktivitäten konstituiert die Unersetzbarkeit. Die Verankerung ist emergent und damit prinzipiell reversibel, auch wenn die historische Evidenz erhebliche Beharrungskraft dokumentiert. Die Reversibilität ist dabei nicht nur theoretisch: Die L2-Autonomie zeigt, dass Ökosystem-Akteure ihre Ethereum-Abhängigkeit aktiv zu reduzieren versuchen. Funktionale Unersetzbarkeit steht damit auf: Erfüllt mit Einschränkung. Die Verankerung überschreitet alle quantitativen Schwellenwerte und hat einen Stresstest bestanden, aber die Emergenz der Verankerung, die L2-Autonomie und der Multi-Chain-Drift qualifizieren den Befund.

Die Verankerung zeigt, dass Ethereum als Gravitationszentrum funktioniert. Die nächste Frage folgt zwingend: Ist dieses Gravitationszentrum auch sicher?

I.2 Sicherheits- und Vertrauenslast

Dieses Kriterium ist als Kritische Bedingung im Bewertungsrahmen verankert: Ein Befund auf „Offen" würde das Gesamturteil auf „Bedingt geeignet" deckeln. Die Prüfung operiert auf zwei Dimensionen, der ökonomischen Sicherheit und der Restvertrauenslast, die in einem komplementären Verhältnis zueinander stehen: Die eine fragt, ob Angriffe undurchführbar sind, die andere, wie viel Vertrauen der Nutzer trotz dieser Sicherheit aufbringen muss.

Die Casper-FFG-Architektur, deren Mechanik Abschnitt 4.2 beschrieben hat, verankert ökonomische Sicherheit mathematisch zwingend: Validatoren, die doppelt signieren oder widersprüchliche Checkpoints attestieren, verlieren ihren Stake durch Slashing, wobei die drei kritischen Schwellenwerte der BFT-Mathematik, 33 Prozent als Blocking Minority, 51 Prozent für Reorgs vor Finality und 66 Prozent als Supermajority, im Protokoll implementiert und nicht deaktivierbar sind.[107] Parallel verankert das Protokoll die technische Möglichkeit trustlosen Zugangs: Full Nodes verifizieren die gesamte Chain-Historie unabhängig, und Merkle-Patricia-Trie-Strukturen ermöglichen kryptographische Zustandsverifizierung mit logarithmischer Effizienz.

Die Daten zum operativen Sicherheitsprofil sind stark. Bei 964.768 aktiven Validatoren und rund 30 Prozent des ETH Total Supply von 120.693.582 ETH im Staking belaufen sich die statischen Kosten einer 34-Prozent-Attacke auf rund 26 Milliarden US-Dollar, berechnet aus rund 34 Prozent der 35,8 Millionen gestakten ETH multipliziert mit dem ETH-Preis am Stichtag von rund 2.100 US-Dollar. Dieser Wert liegt in der Größenordnung des Schwellenwerts von über 30 Milliarden US-Dollar, unterschreitet ihn beim Kursniveau des Stichtags jedoch, sodass die ökonomische Sicherheit ihre Wirkung über die erzwungene Slashing-Mechanik, die Größenordnung des Angriffs und die Marktilliquidität entfaltet und nicht allein über die statische Schwelle. Die Berechnung folgt der BFT-Logik: Ein Angreifer müsste rund ein Drittel des gestakten ETH kontrollieren und wäre bei einem Finalitäts-Angriff zwingend Slashing ausgesetzt, wodurch der kontrollierte Stake vollständig verloren ginge, unabhängig davon, ob der Angriff erfolgreich ist. Die Slashing-Bilanz von 525 Validatoren seit Genesis, dokumentiert in Abschnitt 4.3, belegt, dass der Mechanismus operativ funktioniert und das Abschreckungssignal wirkt, wobei die geringe Zahl bei knapp einer Million Validatoren zeigt, dass rationale Akteure

[107] Buterin, Vitalik / Griffith, Virgil (2019): Casper the Friendly Finality Gadget. arXiv:1710.09437. Die BFT-Schwellenwerte sind in der Beacon-Chain-Spezifikation implementiert und seit dem Merge (September 2022) operativ.

das Slashing-Risiko vermeiden. Im Bewertungsfenster der letzten 24 Monate ist kein Finalitätsverlust über vier Epochs aufgetreten, und die Finality-Rate liegt bei über 99,99 Prozent: Von rund 287.000 Epochs seit dem Merge wurden lediglich 13 nicht finalisiert, alle im Mai 2023, und seit diesem Zeitpunkt ist kein einziger Ausfall aufgetreten.[108]

Die prozyklische Einschränkung verdient eine differenzierte Einordnung, weil sie die Natur der Sicherheitsgarantie selbst betrifft. Die Attack Cost ist eine Funktion des ETH-Preises, der in einem zirkulären Abhängigkeitsverhältnis zum DeFi-Ökosystem steht: Ein sinkender Preis schwächt die Sicherheitsgarantie gerade dann, wenn sie am meisten benötigt wird, und im Stressszenario verstärkt sich dieser Effekt, weil Roadmap-Komplexität Bugs produzieren kann, Bugs das Vertrauen senken, sinkendes Vertrauen den ETH-Preis drückt und ein sinkender Preis die Attack Cost weiter senkt. Im 2022-Marktzyklus fiel der ETH-Preis um über 80 Prozent, was die Attack Cost proportional senkte, aber das System überlebte empirisch ohne Sicherheitsvorfall, was die Belastbarkeit auch unter ungünstigen Bedingungen dokumentiert. Diese Marktpreisabhängigkeit unterscheidet Ethereum von traditionellen Infrastrukturen: Die physische Sicherheit eines Stromnetzes sinkt nicht mit dem Strompreis, und die institutionelle Sicherheit von SWIFT hängt nicht von der Bewertung seiner Mitgliedsbanken ab. Die aktuelle Attack Cost in der Größenordnung von 26 Milliarden US-Dollar übertrifft konventionelle Sicherheitsgarantien allerdings in einem qualitativen Punkt: Slashing ist mechanisch erzwungen und hängt weder von Strafverfolgung noch von institutioneller Kontrolle ab.

Die Restvertrauenslast zeigt eine Diskrepanz zwischen Protokollanspruch und Nutzungsrealität, die in ihrer kumulierenden Wirkung erfasst werden muss. Trustloser Zugang ist technisch möglich: Ein Full Node auf Consumer-Hardware, wie in Abschnitt 4.6 dokumentiert, ermöglicht unabhängige Verifikation ohne Intermediär, und das Protokoll erzwingt keinen Intermediär. Die operative Realität hat jedoch eine Schichtung von Vertrauensabhängigkeiten erzeugt, bei der jede Schicht eine Abhängigkeit hinzufügt, die der Infrastrukturanspruch eigentlich ausschließt, und bei der die Kumulierung der Schichten eine Vertrauenslast erzeugt, die sich qualitativ von der Einzelbetrachtung unterscheidet.

Wallets wie MetaMask operieren als Closed-Source-Komponenten mit unilateralen Update-Mechanismen, und der Nutzer vertraut dem Wallet-Anbieter, die korrekte Transaktion zu konstruieren und den richtigen RPC-Endpunkt

[108] Finality-Daten: beaconcha.in, 27. März 2026. Die 13 nicht finalisierten Epochs im Mai 2023 waren die Folge zweier aufeinanderfolgender Attestation-Handling-Bugs in Prysm und Teku.

zu nutzen. Auf der nächsten Schicht dominieren Infura und Alchemy rund 70 Prozent des RPC-Traffics, wobei der Infura-Ausfall im November 2020 empirisch belegte, dass die systemische Abhängigkeit operativ manifest ist: Ethereum war für die Mehrheit der Nutzer temporär nicht zugänglich, obwohl das Protokoll durchgehend operierte. Darüber liegt die L2-Sequencer-Schicht: 91,5 Prozent des L2-TVL operieren auf Stage-1-Rollups mit Security-Council-Multisigs und zentralisierten Sequencern, wobei der Linea-Vorfall im Juni 2024, bei dem das Team den Sequencer bewusst stoppte und Angreifer-Adressen zensierte, die Zensur-Möglichkeit dieser Architektur demonstrierte. Auf der äußersten Schicht erfordern Cross-L2-Transfers Trust-basierte Bridges mit kumulativen Hack-Schäden von über 2,8 Milliarden US-Dollar oder siebentägige Challenge-Perioden, wobei die Exit-Window-Bedingungen drastisch variieren: Base hat ein Exit-Window von null Tagen, Arbitrum One von 17 Tagen. Die Kumulierung dieser vier Schichten bedeutet, dass ein typischer Nutzer, der über MetaMask auf einen L2-DeFi-Service zugreift, vier Vertrauensschichten durchläuft, von denen keine durch das Ethereum-Protokoll selbst abgesichert ist.

Die Konsequenz dieser Schichtung ist präzise formulierbar: Die kryptographische Vertrauenslosigkeit, die Ethereum als Infrastruktur beansprucht, gilt im IST-Zustand primär für einen kleinen Nutzerkreis aus Full-Node-Betreibern, On-Chain-Protokollen und L1-Nutzern mit direktem Protokollzugang. Für den Massennutzer und für den Großteil des L2-Kapitals ist Ethereum eine Infrastruktur mit institutionellen Trust-Schichten. Der qualitative Unterschied zu traditionellen Systemen bleibt bestehen, weil der Opt-out jederzeit möglich ist: Jeder Nutzer kann einen Full Node betreiben und die gesamte Kette selbst verifizieren, und dieses Recht ist protokollär verankert. Quantitativ nutzen diesen Opt-out wenige, und die Barrieren dafür, Hardware, Betrieb, Wartung, technisches Wissen, sind real. Sicherheits- und Vertrauenslast steht damit auf: Erfüllt mit Einschränkung. Die ökonomische Sicherheitsdimension erfüllt alle technischen Indikatoren. Die Restvertrauens-Dimension dokumentiert eine operative Diskrepanz zwischen Protokollmöglichkeit und Nutzungsrealität, die den Anspruch qualifiziert, ohne ihn fundamental zu untergraben.

Die ökonomische Sicherheit ist gegeben. Die nächste Frage lautet: Wofür ist dieses System sicher? Ein sicheres System ohne Koordinationsleistung wäre ein Tresor ohne Inhalt.

I.3 Koordinationsfunktion

Dieses Kriterium prüft nach der in Kapitel 2 gesetzten Definition, ob Ethereum eine Koordinationsleistung bereitstellt, die ohne das System nicht oder nur mit signifikant höherem Aufwand erbracht werden könnte. Die Referenzinfrastrukturen aus Kapitel 3 zeigen das Muster: Stromnetze koordinieren Angebot und Nachfrage in Echtzeit, SWIFT koordiniert Finanznachrichten zwischen über 11.000 Banken, das Internet koordiniert Paketrouting zwischen autonomen Netzwerken. Die Frage ist, ob Ethereum eine vergleichbare Koordinationsleistung erbringt, und wenn ja, welcher Art sie ist.

Das Protokoll implementiert drei der vier in Abschnitt 4.2 und 4.4 beschriebenen Koordinationsprimitive operativ: Settlement als finalisierte, irreversible Transaktionsverarbeitung nach rund 12,8 Minuten, Execution als deterministische Smart-Contract-Ausführung in der EVM mit atomarer Composability, und Data Availability als KZG-Commitment-basierte Blob-Verfügbarkeit für L2-Rollups seit Dencun (März 2024). Das vierte Primitiv, die protokollseitige Verifikation beliebiger Off-Chain-Berechnungen, getragen von der zkEVM-Verifikation und exponiert über die EXECUTE-Precompile der Native Rollups (EIP-8079), befindet sich im Status RES und ist damit nicht Teil der IST-Bewertung. Drei von vier Primitiven im Status IMPL belegen einen Koordinations-Scope, der den Schwellenwert für „Erfüllt mit Einschränkung“ überschreitet.

Die Absolutzahlen verdienen eine Einordnung, die über den internen Blockchain-Vergleich hinausgeht. Rund 100 Milliarden US-Dollar sind in einem permissionlosen System ohne institutionellen Treuhänder koordiniert, und dieses Volumen wird rund um die Uhr, 365 Tage im Jahr, ohne Wartungsfenster und ohne Feiertagskalender abgewickelt. Fedwire, das größte US-Settlement-System, settelt rund 4 Billionen US-Dollar täglich, operiert aber mit institutionellem Träger (Federal Reserve), geographischer Einschränkung (US-Dollar-Raum) und Zugangsbeschränkung (Federal-Reserve-Mitgliedschaft erforderlich). Ethereums Volumen ist mit Fedwire nicht gleichzusetzen, weil die Systeme unterschiedliche Funktionen erfüllen und unterschiedliche Nutzerbasen bedienen, aber die Koordinationseigenschaft, permissionless, global, ohne Intermediär, ist strukturell verschieden und durch Hochskalierung eines traditionellen Systems nicht replizierbar: Kein institutionelles Settlement-System kann permissionless operieren, weil die institutionelle Trägerschaft die Zugangskontrolle impliziert. Die atomare Composability, die Abschnitt 4.1 beschrieben hat, ermöglicht Flash-Loan-basierte Operationen in einem einzelnen Block, die in traditionellen Systemen mehrtägige Settlement-Latenz erfordern würden, und

die Stablecoin-Emission von rund 166 Milliarden US-Dollar auf Ethereum zeigt, dass die Koordinationsleistung bereits institutionelle Akteure einbezieht, die Dollar-denominierte Werte auf der Ethereum-Infrastruktur emittieren.[109]

Die L2-Settlement-Abhängigkeit belegt die operative Reichweite. Alle Top-5-Rollups nach TVL, Arbitrum One, OP Mainnet, Base, zkSync Era und Starknet, settlen auf Ethereum und nutzen Blob-Transactions für Data Availability, wobei Hybridausnahmen wie Arbitrum Nova oder Mantle keinen signifikanten TVL-Anteil halten. Diese Bindung ist technisch, weil keine Alternative vergleichbare Sicherheitsgarantien zu vergleichbaren Kosten bietet. Die DA-Entscheidungen illustrieren die Abhängigkeit: Alle führenden Rollups nutzen Ethereum-Blobs als primäre DA-Quelle, und das in Abschnitt 4.4 beschriebene Fusaka-Upgrade (Dezember 2025) hat mit PeerDAS die Blob-Kapazität weiter erhöht, was die ökonomische Attraktivität der Ethereum-DA gegenüber alternativen DA-Lösungen verstärkt. Die gesamte Blockproduktions-Pipeline operiert über MEV-Boost, wobei die in Abschnitt 4.2 beschriebene Proposer-Builder-Separation die Koordination zwischen Validatoren und Buildern über Off-Chain-Relays organisiert, die selbst keine protokolläre Verantwortlichkeit tragen und auf Reputation und ökonomischem Eigeninteresse basieren. Die Relay-Abhängigkeit ist Teil der Koordinationsarchitektur und damit für I.3 relevant: Das System koordiniert die Blockproduktion über eine Schicht, die außerhalb des Protokolls liegt.

Die Cross-L2-Composability ist allerdings die qualitative Einschränkung, die den Gesamtbefund bestimmt. Ethereums stärkste Koordinationseigenschaft, die atomare Composability, ist auf L2-Ebene strukturell nicht vorhanden: Jedes L2 verarbeitet Transaktionen in eigenen, asynchronen Zustandsräumen, und Cross-L2-Transfers erfordern Trust-basierte Bridges oder mehrtägige Challenge-Perioden. Die Superchain mit ihren 34 OP-Chains hat Fortschritte in der intra-Stack-Interoperabilität erzielt, wobei SuperchainERC20 Cross-Chain-Token-Transfers innerhalb des OP-Stacks ermöglicht, aber atomare Composability über Stack-Grenzen, etwa zwischen OP Mainnet und Arbitrum, bleibt nicht gegeben. Monatliche Bridge-Volumina von rund 11,2 Milliarden US-Dollar zeigen das Ausmaß des Koordinationsbedarfs, der über Intermediäre abgewickelt wird, und Bridge-Hack-Schäden von über 2,8 Milliarden US-Dollar dokumentieren die Kosten dieser Intermediation. Die Liveness-Risiken zentralisierter Sequencer verstärken das Bild: Arbitrum erlebte im Dezember 2023 einen 78-minütigen

[109] Zum Vergleich der Settlement-Geschwindigkeiten: SWIFT-Settlement dauert 1–3 Tage, ACH 2–3 Tage, SEPA-Überweisungen typisch 1 Werktag. Ethereums 12,8-Minuten-Finalität und die atomare Composability ermöglichen Koordinationsmuster, die in diesen Systemen strukturell unmöglich sind.

Ausfall, Base im August 2025 einen 33-minütigen, jeweils verursacht durch Single Points of Failure in der Sequencer-Infrastruktur.

Gemessen am Infrastrukturanspruch ergibt sich eine Zweischichtigkeit der Koordination, die für die Bewertung entscheidend ist. Für L1-Nutzer ist die Koordination trustless und protokollär garantiert: Settlement ist irreversibel, Execution ist deterministisch, und die Interaktion erfordert keinen Intermediär. Für L2-Nutzer, die die Mehrheit der tatsächlichen Aktivität ausmachen, ist die Koordination durch zentralisierte Sequencer, Relay-Abhängigkeit und Bridge-Trust eingeschränkt. Eine Infrastruktur, die universelle Koordination ohne institutionelles Vertrauen beansprucht, aber den Großteil ihrer Koordinationsleistung über institutionelle Intermediäre abwickelt, weist eine Anspruchs-Diskrepanz auf. Die Diskrepanz ist qualitativ verschieden von traditionellen Infrastrukturen: SWIFT koordiniert durchgehend über institutionelle Intermediäre und beansprucht keine Vertrauenslosigkeit, während Ethereum den Anspruch erhebt und auf L1 einlöst, ihn aber auf L2 relativiert. Der Befund für Koordinationsfunktion lautet: Erfüllt mit Einschränkung. Die Koordinationsleistung ist real, quantitativ substanziell und qualitativ einzigartig, aber die L2-Fragmentierung untergräbt die Kohärenz der Koordination, die das System als Infrastruktur bieten muss.

Die Koordination ist real und einzigartig. Die entscheidende Anschlussfrage lautet, ob sie auch unter Stress hält, denn ein System, das unter normalen Bedingungen koordiniert, aber bei Störungen ausfällt, ist keine Infrastruktur.

I.4 Minimale tragfähige Garantien

Dieses Kriterium ist die zweite Kritische Bedingung in dieser Dimension und fragt, ob Ethereum ein Mindestset an Garantien bietet, die auch unter Stress aufrechterhalten werden. Das Kriterium hat eine besondere Funktion im Bewertungsrahmen, weil es die Belastbarkeit des Systems unter widrigen Bedingungen prüft, die für den Infrastrukturanspruch konstitutiv ist: Jede der sieben Referenzinfrastrukturen aus Kapitel 3 musste Stresssituationen absorbieren, vom Stromnetz-Blackout über DNS-Angriffe bis zu SWIFT-Sanktionen, und die Frage, ob das System degradiert oder kollabiert, ist für die Infrastruktureignung entscheidend. Vier Garantien stehen zur Prüfung: Finality, Liveness, Degradation Mode und Zensurresistenz unter Angriff.

Die Time-to-Finality beträgt 12,8 Minuten, berechnet aus zwei Epochs mit je 32 Slots à 12 Sekunden, und liegt damit unter dem Schwellenwert von 15 Minuten.[110] Dieser Wert ist protokollmathematisch verankert und seit dem Merge konsistent. Für ein System, das den Infrastrukturanspruch erhebt, ist die Qualität dieser Finalität entscheidend: SWIFT-Settlement dauert ein bis drei Tage, ACH zwei bis drei Tage, SEPA-Überweisungen typischerweise einen Werktag. Die 12,8-Minuten-Finalität ist qualitativ überlegen, weil sie von kryptographischer Irreversibilität getragen wird, die keiner institutionellen Abwicklung bedarf. Die Liveness ist durch eine Finality-Rate von über 99,99 Prozent belegt, wobei seit Mai 2023 kein einziger Ausfall aufgetreten ist. Der Dezember-2025-Vorfall, bei dem ein Prysm-Bug die Netzwerk-Partizipation temporär auf 75 Prozent senkte, hat empirisch belegt, dass die verbesserte Client-Diversität als Sicherheitspuffer funktioniert: Wäre derselbe Bug 2022 aufgetreten, als Prysms Anteil bei rund 68 Prozent lag, hätte die Partizipation unter die 67-Prozent-Schwelle fallen können. Die Tatsache, dass das System diesen Bug absorbierte, ohne dass ein Nutzer eine Auswirkung bemerkte, illustriert die Robustheit der Finality-Garantie.

Der Degradation Mode ist die Eigenschaft, die Ethereum von allen in Kapitel 3 analysierten Referenzinfrastrukturen abhebt, und er verdient eine Einordnung, die über die technische Beschreibung in Abschnitt 4.2 hinausgeht. Der dort beschriebene Inactivity Leak wurde im Mai 2023 auf dem Mainnet getestet, als zwei aufeinanderfolgende Finalitätsverluste die Netzwerk-Partizipation unter die Zwei-Drittel-Schwelle drückten. Das Protokoll reagierte automatisch: Inaktive Validatoren verloren progressiv Stake, bis die verbleibenden aktiven Validatoren wieder über zwei Drittel des Sets repräsentierten, und die Selbsthei-

[110] Die Beacon-Chain-Spezifikation definiert eine Epoch als 32 Slots à 12 Sekunden. Finality erfordert die Justification und Finalization zweier aufeinanderfolgender Checkpoints durch über zwei Drittel des Validator-Sets.

lung erfolgte nach rund 96 Minuten, ohne manuellen Eingriff, ohne Koordination außerhalb des Protokolls und ohne Unterbrechung der Block-Produktion. Die infrastrukturelle Bedeutung dieses Mechanismus lässt sich durch den Vergleich mit den Referenzinfrastrukturen schärfen: Bei einem Ausfall eines Teils des DNS-Root-Server-Netzwerks muss koordiniert werden, typischerweise durch manuelle Eskalation zwischen den Betreibern der Root-Server. Bei einem Ausfall von SWIFT-Knoten greifen institutionelle Notfallprozesse. Bei einem partiellen Stromausfall erfordert die Wiederherstellung physische Intervention durch Netzbetreiber. In jedem dieser Fälle hängt die Wiederherstellung von externer Koordination ab, die ihrerseits Kommunikationsinfrastruktur, organisatorische Strukturen und menschliche Entscheidungsprozesse voraussetzt. Ethereums Inactivity Leak benötigt nichts davon. Das Protokoll führt das System autonom zur Funktionsfähigkeit zurück, und der Mainnet-Beweis macht diesen Befund belastbar.[111]

Die vierte Garantie, Zensurresistenz unter koordiniertem Angriff, erreicht nicht das Niveau der ersten drei. Es gibt keinen Protokollmechanismus, der einen Block-Proposer oder Builder zwingt, eine spezifische valide Transaktion aufzunehmen. FOCIL (EIP-7805), das diese Lücke schließen würde, befindet sich im Status PLAN. Die OFAC-Compliance-Rate, die bei Kriterium II.1 vollständig analysiert wird, liegt bei rund 15 Prozent und damit deutlich unter dem 50-Prozent-Schwellenwert, aber diese Leistung beruht auf Marktdynamik, nicht auf einer protokollären Garantie, was bedeutet, dass sie unter veränderten Marktbedingungen reversibel ist.[112] Die in Abschnitt 4.2 dokumentierte Builder-Konzentration, die bei Kriterium II.1 als Hauptthema die vollständige Analyse erhält, bedeutet für I.4, dass die Zensurresistenz emergent ist und nicht protokollär garantiert. Dieser Einzelindikator steht auf „Bedingt erfüllt", weil der Pfad zur protokollären Absicherung erkennbar ist, aber im IST nicht gesichert.

Die Aggregation der vier Garantien ergibt ein Bild, das die Stärken des Systems präzise verortet: Drei Garantien stehen auf „Erfüllt", eine auf „Bedingt erfüllt". Die drei erfüllten Garantien decken den Kern des Mindestsets ab, wobei Finality und Liveness die Basisfunktion sichern und der Degradation Mode eine Eigenschaft bereitstellt, die über das hinausgeht, was die Referenzinfrastrukturen aus Kapitel 3 bieten. Die bedingte Garantie betrifft die Zensurresistenz un-

[111] Die technischen Details des Mai-2023-Inactivity-Leak-Ereignisses sind in Abschnitt 4.2 dokumentiert. Die Bewertung hier bezieht sich auf die infrastrukturelle Bedeutung: automatisierte Selbstheilung ohne externe Koordination.

[112] OFAC-Compliance-Daten: MEV Watch / relayscan.io, 27. März 2026. Die historische Trajektorie vom 79-Prozent-Peak dokumentiert die marktgetriebene Normalisierung.

ter koordiniertem Angriff, die funktional gegeben ist, solange die Marktbedingungen günstig bleiben, aber nicht durch das Protokoll gegen ungünstige Bedingungen abgesichert wird. Das stärkere der beiden möglichen Labels ist gerechtfertigt, weil die drei erfüllten Garantien den Kern bilden und die vierte einen klaren Schließungspfad aufweist. Minimale tragfähige Garantien steht auf: Erfüllt mit Einschränkung. Drei von vier Garantien sind protokollär verankert und operativ bewiesen. Die vierte ist funktional gegeben, aber nicht durch das Protokoll abgesichert.

Synthese Dimension I

Das Bewertungsprofil der ersten Dimension zeigt ein konsistentes Muster: Alle vier Kriterien stehen auf „Erfüllt mit Einschränkung". Die Homogenität ist bemerkenswert, weil kein Kriterium darunter fällt und keines „Erfüllt" ohne Qualifizierung erreicht. Funktionale Unersetzbarkeit (I.1) ist durch starke, aber emergente und damit reversible Verankerung gekennzeichnet. Sicherheits- und Vertrauenslast (I.2) dokumentiert eine robuste ökonomische Sicherheit bei gleichzeitiger operativer Restvertrauenslast durch den vierschichtigen Trust-Stack. Koordinationsfunktion (I.3) belegt eine quantitativ und qualitativ einzigartige Koordinationsleistung, die durch die L2-Fragmentierung und die Relay-Abhängigkeit eingeschränkt wird. Minimale tragfähige Garantien (I.4) zeigt drei starke und eine bedingte Garantie, wobei der Degradation Mode die herausragende Einzeleigenschaft der gesamten IST-Bewertung darstellt.

Die beiden Kritischen Bedingungen, I.2 und I.4, stehen auf „Erfüllt mit Einschränkung". In der Kaskadenlogik aus Kapitel 2 bedeutet das: Die Kerneigenschaft ist grundsätzlich gegeben, mit dokumentierten Limitationen, und dieser Zustand ist passierbar für die nächste Kaskadenstufe. Diese beiden Kritischen Bedingungen begrenzen das Gesamturteil nicht nach unten. Das Muster, das die gesamte Dimension charakterisiert, lässt sich auf einen Satz bringen: Die architektonische Grundlage ist tragfähig, die Einschränkungen liegen durchgehend in der Diskrepanz zwischen dem, was das Protokoll ermöglicht, und dem, was die operative Realität davon einlöst. Vier Einschränkungen sind Ausprägungen desselben Grundmusters. Der vierschichtige Trust-Stack reduziert die kryptographische Vertrauenslosigkeit für den Massennutzer auf eine institutionelle Vertrauensabhängigkeit. Die fragmentierte L2-Composability beschränkt die stärkste Koordinationseigenschaft des Systems auf die Basisschicht. Die emergente Zensurresistenz hängt von Marktdynamik ab, statt vom Protokoll garantiert zu werden. Die reversible Verankerung schließlich beruht auf Netzwerkeffekten, nicht auf technischer Bindung. Die Frage, ob der Weg von der Möglichkeit zur Realität

durch die Roadmap gesichert ist, gehört in die SOLL-Bewertung des folgenden Kapitels.

Die strukturelle Fundierung ist gegeben. Die nächste Dimension prüft die qualitative Eignung des Systems für den Infrastrukturanspruch, und dort liegt der schärfste Einzelbefund der gesamten IST-Bewertung.

4.8 Dimension II: Qualitative Tragfähigkeit

Die zweite Dimension prüft, ob Ethereum die qualitativen Eigenschaften aufweist, die den Infrastrukturanspruch inhaltlich tragen. Vier Kriterien stehen zur Bewertung: Neutralität und Zensurresistenz (II.1) als einzige Kritische Bedingung dieser Dimension und dritte und letzte des gesamten Bewertungsrahmens, gefolgt von Offener Generativität (II.2), Unabhängiger Verifizierbarkeit (II.3) und Niedrigschwelliger Inklusivität (II.4). Die Asymmetrie zwischen der Kritischen Bedingung, die den schärfsten Einzelbefund der gesamten IST-Bewertung trägt, und den drei Qualitativen Kriterien, die ein konsistentes Profil ohne fundamentale Defizite aufweisen, prägt das Gesamtbild.

II.1 Neutralität und Zensurresistenz

Von den zwölf Kriterien des Bewertungsrahmens ist dieses das Kriterium mit dem schärfsten Befund im IST-Zustand. Es ist als Kritische Bedingung verankert und enthält den einzigen Indikator, der auf der Stufe „Offen“ steht. Die Prüfungsfrage lautet: Operiert Ethereum neutral gegenüber allen Nutzern, und kann jede valide Transaktion inkludiert werden?

Das Protokoll verankert Neutralität durch Permissionless Participation ohne Zulassung durch eine zentrale Autorität, inhaltsneutrale Blockvalidierung durch Casper FFG und Fork-Choice-Neutralität ohne Whitelist oder Blacklist. Was das Protokoll nicht verankert, ist eine Inklusions-Obligation: Kein Mechanismus zwingt einen Block-Proposer oder Builder, eine spezifische valide Transaktion aufzunehmen. Diese Lücke, beschrieben in Abschnitt 4.2, ist die protokolläre Grundlage der Zensur-Anfälligkeit.

Sieben Indikatoren operationalisieren die Prüfungsfrage, und ihre Bewertung ergibt ein heterogenes Bild, das die Spannung zwischen operativer Leistung und struktureller Absicherung schärfer zeigt als bei jedem anderen Kriterium. Die OFAC-Compliance-Rate von rund 15 Prozent der Blöcke liegt deutlich unter dem 50-Prozent-Schwellenwert und dokumentiert eine positive Trajektorie vom 79-Prozent-Peak im November 2022, wobei die Normalisierung ohne protokolläre Intervention durch Marktdynamik erfolgte: Non-OFAC-com-

pliant Builder gewannen Marktanteile, weil sie keine Einschränkungen beim Transaktions-Screening hatten und dadurch profitablere Blöcke bauen konnten. Der Van-Loon-v.-Treasury-Entscheid im November 2024 und das OFAC-Delisting von Tornado Cash im März 2025 haben den regulatorischen Druck reduziert.[113] Selbst beim 79-Prozent-Peak erlebten sanktionierte Transaktionen nur inkrementelle Verzögerungen von wenigen Blöcken, keine permanente Exklusion. Die maximale Zensur-Verzögerung liegt operativ bei wenigen Blöcken, weil rund 85 Prozent der Builder-Slots von non-OFAC-compliant Akteuren gebaut werden. Die Leistung ist allerdings emergent und nicht protokollär garantiert, was bedeutet, dass sie unter veränderten Marktbedingungen reversibel ist.

Der strukturelle Defektbefund liegt in der Builder-Konzentration. Titan mit 51,2 Prozent, BuilderNet mit 25,7 Prozent und Quasar mit 16,4 Prozent kontrollieren zusammen 93,3 Prozent aller Blöcke bei einem Herfindahl-Hirschman-Index von rund 3.554, der die DOJ-Schwelle für hochkonzentrierte Märkte von 2.500 deutlich überschreitet.[114] Diese Konzentration ist kein Zufall, wie Daian und Kollegen 2020 gezeigt haben: Builder, die die effizientesten MEV-Extraktionsstrategien implementieren, gewinnen systematisch den Wettbewerb um die profitabelsten Blöcke, was eine sich selbst verstärkende Konzentrationsdynamik erzeugt.[115] Titan allein produziert über die Hälfte aller Ethereum-Blöcke. Falls Titan und BuilderNet koordinieren, kontrollieren sie 76,9 Prozent der Blockproduktion, hinreichend für De-facto-Zensur des Großteils aller MEV-Boost-Blöcke. Die Schutzfaktoren gegen diese Koordination sind ökonomischer Natur: Zensur reduziert Builder-Revenue, und Proposer können lokal bauen, allerdings mit 2,66- bis 5,57-fach geringerem Ertrag. Diese Schutzfaktoren sind real, aber sie sind Marktanreize, keine Protokollgarantien, und die Erfahrung des 79-Prozent-OFAC-Peaks zeigt, dass regulatorischer Druck ökonomische Anreize übersteuern kann. Dieser Indikator steht auf „Offen" und ist der einzige Offen-Befund der gesamten IST-Bewertung.

FOCIL (EIP-7805) ist der spezifizierte Lösungsansatz, der Proposer protokollär zur Übernahme von Transaktionen aus einer dezentral zusammengestellten Inclusion List verpflichten würde: Ein zufällig ausgewähltes Validator-Komitee von 16 Validatoren stellt die Liste zusammen, und der Proposer des nächsten Blocks ist protokollär verpflichtet, diese Transaktionen zu inkludieren, sofern sie

[113] Van Loon v. Department of the Treasury, 5th Circuit Court of Appeals, November 2024: Immutable Smart Contracts sind kein „Property" im Sinne des IEEPA. OFAC-Delisting von Tornado Cash: 21. März 2025.

[114] Builder-Marktanteile: relayscan.io, 27. März 2026. HHI berechnet als Summe der quadrierten Marktanteile. Die DOJ Horizontal Merger Guidelines von 2010 definieren einen HHI über 2.500 als hochkonzentrierten Markt.

[115] Daian, Philip et al. (2020): Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. In: *IEEE Symposium on Security and Privacy*, S. 910–927.

valide und profitabel sind. Der Mechanismus würde die emergente Marktleistung in eine protokolläre Garantie transformieren. Der Status PLAN mit klarer Timeline belegt einen erkennbaren Pfad, aber kein im IST gesichertes Ergebnis, weil Governance-Entscheidungen und technische Machbarkeit noch ausstehen. Die geopolitische Jurisdiktions-Diversität zeigt eine gemäßigte Konzentration: Rund 39 Prozent der Nodes operieren in den USA und rund 53 Prozent in zwei Ländern, wobei die Infrastruktur-Kontextualisierung aus Kapitel 3 das Muster perspektiviert: SWIFT wurde geopolitisch instrumentalisiert, GPS steht unter unilateraler US-Kontrolle, und Cloud-Infrastruktur unterliegt der Jurisdiktion des Betreiberlandes. Ethereums Situation ist nicht mit der unilateralen Kontrolle von GPS vergleichbar, aber die Risikoimplikation ist real, weil institutionelles Staking über US-regulierte Entitäten die jurisdiktionelle Exposition verstärkt.[116] Die Cloud-Konzentration von rund 59 Prozent gehosteter Execution-Layer-Nodes auf drei Providern, wobei AWS allein 35,5 Prozent beherbergt, vergrößert die US-Jurisdiktionsexposition über die reine Node-Geographie hinaus.

Die Staking-Konzentrationsindikatoren liegen in akzeptablen Bereichen. Lido hält 22,8 bis 23 Prozent des gestakten ETH, deutlich unter der 33-Prozent-Blocking-Minority-Schwelle und rückläufig von rund 32 Prozent im Jahr 2023, wobei die DVT-Integration von 547.968 ETH mit einem Quartalszuwachs von 57 Prozent das Single-Point-of-Failure-Risiko im Operator-Set reduziert.[117] Die kumulierte Top-3-Staking-Anbieter-Konzentration liegt bei 40 bis 45 Prozent und überschreitet die 33-Prozent-Blocking-Minority-Schwelle allein als koordinierte Summe, während kein einzelner Anbieter sie erreicht.

Das Gesamtbild ist durch eine Asymmetrie gekennzeichnet. Die Transaktionsebene ist operativ gut, die LST-Indikatoren liegen im akzeptablen Bereich, aber die Builder-Konzentration als einzelner Offen-Indikator bildet einen strukturellen Defektbefund. Die Zensurresistenz des Systems resultiert aus Marktdynamik, nicht aus Protokolldesign, und für ein System, das beansprucht, dass jede valide Transaktion inkludiert werden kann, ist die Abhängigkeit von drei kommerziellen Entitäten eine strukturelle Lücke, die sich durch Verweis auf die positive OFAC-Trajektorie nicht schließen lässt: Die OFAC-Normalisierung zeigt, dass der Markt unter günstigen Bedingungen Zensurresistenz produziert, aber die Builder-Konzentration zeigt, dass die Struktur des Marktes die Voraussetzungen für diese Leistung untergräbt. Die Gesamtbewertung des Kriteriums ist

[116] Node-Verteilungsdaten: Ethernodes, Anfang 2026. Cloud-Konzentrationsschätzung: circa 59 Prozent gehosteter EL-Nodes auf AWS (35,5%), Hetzner (13,8%) und OVHcloud (9,7%).

[117] Lido Tokenholder-Update, 26. Februar 2026: 547.968 ETH auf DVT (Distributed Validator Technology), +57 Prozent QoQ.

dennoch nicht „Offen“, weil die Aggregation aller sieben Indikatoren zeigt, dass die Transaktionsebene funktioniert, der regulatorische Druck nachlässt, die LST-Konzentration rückläufig ist und ein klarer Pfad zur protokollären Absicherung existiert. Neutralität und Zensurresistenz steht auf: Bedingt erfüllt. Die Erfüllung hängt von Bedingungen ab, die im IST-Zustand nicht gesichert sind, insbesondere der Implementierung von FOCIL oder eines funktional äquivalenten Mechanismus. Das ist der schwächste Einzelbefund der gesamten IST-Bewertung und der einzige, bei dem eine Kritische Bedingung unterhalb von „Erfüllt mit Einschränkung“ steht.

Die Neutralitätslücke ist dokumentiert. Ausgerechnet die nächste Eigenschaft, die offene Generativität, ist die stärkste des Systems. Die Spannung zwischen der kritischsten Schwäche und der größten Stärke in derselben Dimension zeigt ein System, das maximale Offenheit produziert, die Neutralität dieser Offenheit aber nicht protokollär absichert.

II.2 Offene Generativität

Die Architektur, die Abschnitt 4.1 beschrieben hat, implementiert Permissionless Deployment vollständig: Jede Ethereum-Adresse kann Smart Contracts deployen, ohne Whitelist, Genehmigungspflicht oder Registrierungsanforderung, und die EVM als quasi-Turing-vollständige Maschine schließt keine Kategorie von Anwendungslogik auf Protokollebene aus. Die atomare Composability ermöglicht Interaktionsmuster wie Flash Loans, die in keinem traditionellen System ein Äquivalent haben: Ein Nutzer kann in einer einzigen Transaktion Millionen US-Dollar leihen, für Arbitrage einsetzen und zurückzahlen, ohne Sicherheiten und ohne Intermediär, und wenn die Rückzahlung scheitert, wird die gesamte Transaktion rückgängig gemacht. Die ERC-Standard-Familie hat sich als emergenter Interoperabilitätsmechanismus ohne zentrale Autorität etabliert, wobei Standards wie ERC-20, ERC-721 und ERC-4626 die Schnittstellen zwischen Protokollen definieren, ohne dass eine zentrale Instanz sie vorschreibt. Das Zusammenspiel dieser drei Eigenschaften, permissionless Zugang, atomare Interaktion und emergente Standards, erzeugt die Generativität, die das DeFi-Ökosystem hervorgebracht hat: Protokolle bauen aufeinander auf, ohne bilaterale Vereinbarungen treffen zu müssen, weil die Kompatibilität auf der Ebene der gemeinsamen Ausführungsumgebung hergestellt wird.

Die Praxis bestätigt die Protokolleigenschaft. Permissionless Deployment ist vollständig realisiert, rund 65 Prozent aller neuen Smart Contracts werden direkt auf L2s deployt, und im Jahr 2025 wurden 230 EIPs eingereicht, von denen 37 akzeptiert wurden, was dokumentiert, dass der Innovationsprozess selbst permis-

sionless ist: Jeder kann Standards vorschlagen, und die Akzeptanz folgt einem Community-getriebenen Prozess ohne zentralen Gatekeeper. Die einzige faktische Deployment-Beschränkung auf L1 ist das Gas Limit von 60.000.000, das in der Praxis kein Hindernis für die Mehrheit der Anwendungslogiken darstellt, da selbst komplexe Smart-Contract-Deployments das Block-Gas-Limit nicht ausschöpfen.

Die Toolchain verdient eine eigenständige Einordnung, weil sie für die Generativität eine Qualitätsdimension eröffnet, die über das Permissionless Deployment hinausgeht. Die gesamte Kern-Entwicklungsinfrastruktur steht unter liberalen Open-Source-Lizenzen (MIT, Apache 2.0): Foundry als Test- und Deployment-Framework, Hardhat als Build-Umgebung, Ethers.js als JavaScript-Bibliothek für die Blockchain-Interaktion, Slither und Echidna als Sicherheits-Tools. Kein einzelner Anbieter kontrolliert die Toolchain oder kann den Zugang einschränken, und die Werkzeuge werden von unabhängigen Teams gewartet, was die Resilienz der Entwicklungsinfrastruktur gegen den Ausfall eines einzelnen Anbieters sichert. Das ist für die Generativität relevant, weil ein Entwickler nicht nur die Möglichkeit benötigt, Code auf dem Netzwerk auszuführen, sondern auch frei verfügbare Werkzeuge, um diesen Code zu schreiben, zu testen und zu verifizieren. Van Schewick hat für das Internet gezeigt, dass offene Werkzeuge und offene Protokolle zusammen die Innovationsdynamik erzeugen, weil sie die Innovationsbarriere von der Infrastrukturschicht an die Ränder des Netzwerks verlagern. Für Ethereum gilt dasselbe Muster auf der Smart-Contract-Schicht, wo jeder Entwickler mit Zugang zu Open-Source-Tools innovieren kann, ohne die Erlaubnis des Protokollbetreibers einzuholen.[118]

Die Einschränkung liegt in der L2-Fragmentierung, und sie trifft die Eigenschaft, die Ethereums Generativität hervorgebracht hat. Die in Abschnitt 4.4 dokumentierte Composability-Fragmentierung bedeutet, dass ein Entwickler, der Liquidität über mehrere L2s hinweg benötigt, die atomare Composability von L1 nicht nutzen kann und auf Bridge-Mechanismen mit Trust-Annahmen angewiesen ist. Flash Loans, das paradigmatische Beispiel für die generative Kraft der atomaren Composability, funktionieren nur innerhalb eines einzelnen Blocks auf einer einzelnen Chain und sind über L2-Grenzen hinweg strukturell unmöglich. Die reichste Composability-Eigenschaft ist auf der Schicht verfügbar, auf der nur ein kleiner Teil der Transaktionsaktivität stattfindet, während die L2-Schicht, auf der die meiste Aktivität stattfindet, eigene, interne Composability-

[118] Vgl. van Schewick, Barbara (2010): *Internet Architecture and Innovation*. MIT Press. Van Schewicks Argument, dass die End-to-End-Architektur des Internets Innovation an den Rändern ermöglicht, ist auf Ethereums permissionless Smart-Contract-Layer übertragbar.

Muster entwickelt, die nicht über Stack-Grenzen interagieren. Für den Generativitätsanspruch ist das eine reale Einschränkung, weil die Netzwerkeffekte, die aus der Composability entstehen, durch die Fragmentierung abgeschwächt werden: Jedes L2-Ökosystem entwickelt eigene Liquiditätspools, eigene DeFi-Protokolle und eigene Nutzergruppen, und die Verbindung zwischen ihnen erfordert Intermediäre, die Trust-Annahmen einführen. Offene Generativität steht auf: Erfüllt mit Einschränkung. Das Permissionless-Deployment-Modell und die offene Toolchain bilden die strukturell stärkste Eigenschaft des Systems. Die L2-Composability-Fragmentierung ist die dokumentierte Einschränkung.

Wenn das System generativ ist, wenn also auf ihm gebaut werden kann, stellt sich die Komplementärfrage: Kann man das Ergebnis auch prüfen?

II.3 Unabhängige Verifizierbarkeit

Die Angebotsseite der Verifikation bildet das Komplement zur Restvertrauenslast (I.2): Während I.2 fragt, wie viel Vertrauen trotz Verifikationsmöglichkeit bleibt, fragt dieses Kriterium, ob die Möglichkeit zur Verifikation überhaupt existiert.

Die deterministische EVM, beschrieben in Abschnitt 4.1, garantiert, dass jeder Full Node bei identischem Input den identischen Zustand berechnet. Merkle-Proof-Verifizierbarkeit ermöglicht die kryptographische Überprüfung einzelner Zustandseinträge, ohne den gesamten Zustand nachzuvollziehen, was für Light Clients und ressourcenbeschränkte Verifizierer relevant ist. Die EVM-Spezifikation ist über das Yellow Paper formal definiert und durch KEVM maschinenverifiziert, was eine Grundlage für maschinelle Verifikation schafft, die in traditionellen Finanzsystemen kein Äquivalent hat: Die Korrektheit einer SWIFT-Transaktion wird institutionell behauptet und durch bilaterale Abstimmung zwischen Sender- und Empfängerbank bestätigt, während die Korrektheit einer Ethereum-Transaktion mathematisch nachgewiesen werden kann, indem jeder Full Node die Zustandsänderung unabhängig berechnet.[119] Full-Node-Verifikation ohne Dritte ist technisch möglich, und das Protokoll erfordert keinen Intermediär für die Zustandsverifikation, was auf der Angebotsseite eine starke Grundlage schafft.

Die operative Evidenz ist substanziell. Mindestens sechs produktiv genutzte Verifikations-Tools überschreiten den Schwellenwert: Certora Prover für formale Verifikation von Invarianten, Foundry/Forge für Fuzz-Testing und Property-

[119] Das Yellow Paper (Wood 2014/2024) definiert die EVM-Semantik formal. KEVM (Hildenbrandt et al. 2018) bietet eine in K-Framework maschinenverifizierte Formalisierung.

Based Testing, Echidna als Fuzzer, Mythril für symbolische Analyse, Slither für statische Analyse und KEVM als maschinenverifizierte Referenzimplementierung. Die EVM-Spezifikation ist substanziell, weist aber dokumentierte Lücken bei Pre-Compiles und einen Lag bei der Formalisierung rezenter EIPs auf, was bedeutet, dass neuere Protokollfeatures zeitweise weniger vollständig spezifiziert sind als ältere. Die Audit-Kultur ist für Tier-1-DeFi-Protokolle Standard, wobei Protokolle wie Aave, Compound und Uniswap regelmäßig mehrere unabhängige Audits durch spezialisierte Firmen wie Trail of Bits, OpenZeppelin und Spearbit durchlaufen, bevor neue Versionen deployt werden. Die Universalität der Praxis bleibt allerdings begrenzt, weil Permissionless Deployment bedeutet, dass jeder unauditierte Contracts deployen kann, und der Long-Tail der Protokolle weder die Ressourcen noch den Anreiz für umfassende Audits hat. Die Lazarus-Group-Angriffe von 2025 mit Schäden von 2,02 Milliarden US-Dollar belegen, dass auch auditierte Systeme über Angriffsvektoren wie Private Key Compromise und Oracle Manipulation verwundbar bleiben, was den Stellenwert von Audits als notwendige, aber nicht hinreichende Sicherheitsbedingung unterstreicht.[120]

Die Verifikation von Layer-2-Zuständen fügt eine Komplexitätsschicht hinzu, die über die L1-Verifikation hinausgeht, weil ein System, das kryptographische Verifizierbarkeit als Kerneigenschaft beansprucht, dieses Versprechen auf allen Schichten einlösen muss. Bei Optimistic Rollups ist der Zustand nach Ablauf der siebentägigen Challenge-Period finalisiert, wobei die Sicherheit auf der Annahme beruht, dass mindestens ein ehrlicher Prüfer innerhalb der Frist einen Fraud Proof einreicht. Dieses Verifikationsmodell ist permissionless, jeder kann einen Fraud Proof einreichen, setzt aber voraus, dass der Prüfer den L2-Zustand vollständig nachvollziehen kann, was spezialisierte Infrastruktur und technisches Wissen erfordert. Bei ZK-Rollups ist die Verifikation sofort und mathematisch: Ein On-Chain-STARK- oder SNARK-Proof kann von jedem L1-Node überprüft werden. Die Erstellung und das Verständnis dieser Proofs setzen allerdings Kryptographie-Expertise voraus, die erheblich über Standard-EVM-Verifikation hinausgeht, von STARK-Mathematik über SNARK-Trusted-Setup-Annahmen bis zu ZK-Circuit-Logik, und die Zahl der Akteure, die diese Verifikation unabhängig durchführen können, ist klein. Native Rollups (EIP-8079, Status RES) würden die Verifikation auf die Basisschicht zurückführen und damit vereinheitlichen, indem die EVM selbst als Verifikationsumgebung für Off-Chain-Be-

[120] Lazarus-Group-Daten: Chainalysis-Report, Februar 2026. Die Angriffe erfolgten hauptsächlich durch Private Key Compromise und Cross-Chain Message Spoofing an auditierten Protokollen.

rechnungen dient, sind aber nicht Teil der IST-Bewertung. Die wachsende L2-Verifikationskomplexität ist eine Einschränkung, die den Befund von II.3 auf der operativen Ebene mitbestimmt.

Die RPC-Konzentration von 70 Prozent über zwei Provider, die bei I.2 als Restvertrauens-Indikator bewertet wird, zeigt, dass die Mehrheit der Nutzer die verfügbare Verifikationsmöglichkeit nicht nutzt. Das ist kein II.3-Problem im engeren Sinne, weil II.3 die Angebotsseite fragt, aber die infrastrukturelle Implikation ist real: Ein System, das sich auf kryptographische Verifizierbarkeit beruft, muss sicherstellen, dass Verifizierung praktisch zugänglich bleibt, und die wachsenden Anforderungen an Full-Node-Hardware (Abschnitt 4.1 dokumentiert 1.579 Gigabyte Full-Node-Größe mit steigender Tendenz) könnten die Angebotsseite mittelfristig einschränken, wenn die Verifikation zunehmend spezialisierte Hardware erfordert. Die Bewertung für Unabhängige Verifizierbarkeit ergibt: Erfüllt mit Einschränkung. Das Verifikationsangebot ist protokollär verankert und toolseitig substanziell, aber die L2-Verifikationskomplexität steigt, Spezifikationslücken bestehen, die Audit-Kultur ist nicht universal, und die praktische Zugänglichkeit der Verifikation wird durch steigende Hardware-Anforderungen und die L2-Schichtung langfristig herausgefordert.

Wenn gebaut und geprüft werden kann, bleibt die Abschlussfrage der qualitativen Dimension: Kann auch teilgenommen werden?

II.4 Niedrigschwellige Inklusivität

Dieses Kriterium hat mit fünf Indikatoren das zweitgrößte Indikator-Set im Bewertungsrahmen, weil Inklusivität an der Schnittstelle mehrerer Barrierentypen operiert: Hardware, Kapital, Kosten, Wissen.

Die Full-Node-Hardware-Anforderungen liegen im Consumer-Bereich, mit Kosten von 500 bis 1.500 US-Dollar für ein Setup aus NVMe-SSD, 16 bis 32 Gigabyte RAM und breitbandiger Internetverbindung. Das liegt oberhalb von Standard-Consumer-Hardware, weil ein typischer Laptop mit 512 Gigabyte SSD nicht ausreicht, aber unterhalb von Datacenter-Grade-Hardware, wobei ressourceneffiziente Clients wie Nimbus den Betrieb auf einem Raspberry Pi 5 ermöglichen. Die in Abschnitt 4.1 dokumentierte State-Growth-Problematik ist die zentrale Langzeitbedrohung: Bei einer Full-Node-Größe von 1.579 Gigabyte und einem wöchentlichen Wachstum von circa 14 Gigabyte steigen die Anforderungen progressiv, und Projektionen für ein Gas-Target von 200 Millionen ergeben 5 Terabyte bis 2028 und 9 Terabyte bis 2030. Die Bandbreitenanforderungen von mindestens 25 Megabit pro Sekunde schließen Haushaltsnetzwerke in Regionen mit schlechter Infrastruktur aus, was den globalen Inklusivitätsanspruch einschränkt.

Die 32-ETH-Mindesteinlage für Solo-Staking ist das Defizit, das die gesamte Inklusivitätsbewertung prägt, und es verdient eine Einordnung, die über den reinen Datenpunkt hinausgeht. Zum Kursniveau des ersten Quartals 2026 entsprechen 32 ETH beim Stichtagskurs rund 67.000 US-Dollar, und Solo-Staking ist auf unter ein Prozent des Staking-Gesamtvolumens geschrumpft.[121] Die Hardware-Barriere für den Validator-Betrieb ist gering, aber die ökonomische Barriere schließt die breite Mehrheit der potenziellen Teilnehmer aus. Die Konsequenz ist eine Nutzungsverteilung, in der Liquid Staking 31,1 Prozent des gestakten ETH hält (Lido dominant), CEX Staking 24 Prozent, Staking Pools 16 Prozent und Solo-Staker unter einem Prozent. Die vier Kategorien decken rund 72 Prozent des gestakten ETH ab. Diese Verteilung bedeutet, dass die dezentrale Validator-Kontrolle, die der Infrastrukturanspruch einer permissionlosen Infrastruktur erfordert, de facto bei institutionellen Entitäten konzentriert ist, während der breite Nutzerkreis über delegierte Modelle teilnimmt.

Dieses Defizit ist das einzige in der gesamten IST-Bewertung, für das die Roadmap keinen operativen Pfad enthält. EIP-7251 (MaxEB, Pectra) hat die maximale Effective Balance auf 2.048 ETH erhöht, zielt aber auf die Effizienz

[121] L2BEAT dokumentiert die Verteilung der Staking-Methoden. Solo-Staker unter einem Prozent: Schätzung auf Basis von Dune Analytics, Q1 2026.

großer Staker, nicht auf die Zugangsschwelle. Rainbow Staking, das verschiedene Staking-Typen mit unterschiedlichen Kapitalanforderungen ermöglichen würde, befindet sich im Status RES ohne Implementierungscommitment. Bei anderen Einschränkungen der IST-Bewertung markiert ein Feature im Status PLAN oder DEPL den Schließungspfad: FOCIL für die Zensurresistenz und EIP-4444 für die State-Growth-Mitigation. Die 32-ETH-Barriere und die L2-Verifikations-Lücke teilen die Eigenschaft, dass ihr einziger benannter Ansatz auf RES ohne Implementierungscommitment steht, Rainbow Staking im einen und die Rückführung der Verifikation auf die Basisschicht über Native Rollups im anderen Fall. Anders als die L2-Verifikations-Lücke, hinter der mit den Native Rollups ein aktives Forschungsprogramm samt Draft-EIP steht, verfügt die 32-ETH-Barriere über kein solches Programm, und dieser Unterschied qualifiziert das Defizit in besonderer Weise. Liquid Staking über Anbieter wie Lido, Rocket Pool oder Coinbase löst den Zugang zur Staking-Rendite ab Beträgen von 0,01 ETH, aber der Nutzer delegiert damit die Validator-Verantwortung an Dritte und gewinnt Rendite, nicht Kontrolle. Der ökonomische Zugang ist inklusiv. Der Zugang zur dezentralen Validator-Kontrolle bleibt hinter der Barriere.

Die L2-Transaktionskosten dokumentieren die stärkste Verbesserung gegenüber früheren Zuständen des Systems. Die Median-Kosten auf den führenden L2s liegen nach EIP-4844 (Dencun, März 2024) und dem Pectra-Upgrade unter 0,01 US-Dollar pro Transaktion, was den Referenzwert von Kreditkartengebühren (zwei bis drei Prozent) und Banküberweisungen (0,50 bis 5,00 US-Dollar) um Größenordnungen unterschreitet. Vor Dencun lagen die Optimism-Gebühren bei rund 1,00 US-Dollar pro Transaktion. Die Prozentangaben in Abschnitt 4.4 beziehen sich auf andere Erhebungszeiträume und Systemkörbe und lassen sich mit diesem Wertepaar nicht zu einer Kette verrechnen. Die Reduktion ist eine direkte Konsequenz der Blob-Architektur, die Abschnitt 4.4 beschrieben hat. Ein Nutzer in Subsahara-Afrika oder Südostasien kann mit unter einem Cent pro Transaktion am globalen Finanzsystem teilnehmen, was substanzielle Inklusivität für die transaktionale Nutzung darstellt. L1-Transaktionen bleiben teuer, typischerweise 2 bis 15 US-Dollar für komplexe DeFi-Operationen in Hochlastphasen, aber da die meiste Aktivität auf L2s migriert ist, ist die L1-Gebührenproblematik für typische Nutzungsszenarien kein kritisches Inklusivitätsproblem.

Die Nutzbarkeit ohne kryptographisches Vorwissen hat sich durch EIP-7702 (Pectra, Mai 2025) substanziell verbessert. Account Abstraction ermöglicht Session Keys, Social Recovery und Gas Sponsoring auf Protokollebene: Ein Nutzer kann seinen Account so konfigurieren, dass einer Anwendung begrenzte

Transaktionsrechte eingeräumt werden, ein verlorener Schlüssel über vertrauenswürdige Kontakte wiederherstellbar ist, und Transaktionskosten von Wallet-Anbietern übernommen werden können, sodass Nutzer ohne eigene ETH-Bestände interagieren können. Der EIP ist deployt, aber die Integration in die großen Wallet-Anwendungen befindet sich in der Umsetzung, und der typische Nutzer trifft noch auf Seed-Phrases und Gas-Management als primäre Interaktionsmuster. Die Adoptionsdynamik über den älteren ERC-4337-Standard, dokumentiert durch über 25,5 Millionen Smart Accounts und 132 Millionen UserOperations, zeigt die Nachfrage nach programmierbaren Accounts. Die UX-Transformation ist allerdings nicht abgeschlossen, und die Übergangsphase, in der das alte Modell (EOA mit Seed Phrase) und das neue Modell (Smart Account mit Social Recovery) koexistieren, erzeugt für den typischen Nutzer eher mehr als weniger Komplexität, weil die Wallet-Anbieter beide Paradigmen parallel bedienen müssen und die Onboarding-Erfahrung fragmentiert bleibt.

Das Profil der fünf Indikatoren zeigt keinen Befund unterhalb von „Erfüllt mit Einschränkung“, wobei die L2-Transaktionskosten als einziger Indikator auf „Erfüllt“ stehen. Die 32-ETH-Barriere als einziges IST-Defizit ohne Roadmap-Antwort ist die gewichtigste Einschränkung. Niedrigschwellige Inklusivität steht auf: Erfüllt mit Einschränkung. Die Teilnahme ist für die transaktionale Nutzung auf L2 substanziell inklusiv, für den Full-Node-Betrieb im Consumer-Bereich möglich aber durch steigende State-Größe gefährdet, und für Solo-Staking durch die 32-ETH-Barriere prohibitiv eingeschränkt.

	Kriterium	Hierarchiestufe	IST-Bewertung
I.1	Funktionale Unersetzbarkeit	Strukturell	Erfüllt mit Einschränkung
I.2	Sicherheits- und Vertrauenslast	Kritisch	Erfüllt mit Einschränkung
I.3	Koordinationsfunktion	Strukturell	Erfüllt mit Einschränkung
I.4	Minimale tragfähige Garantien	Kritisch	Erfüllt mit Einschränkung
II.1	Neutralität und Zensurresistenz	Kritisch	Bedingt erfüllt
II.2	Offene Generativität	Qualitativ	Erfüllt mit Einschränkung
II.3	Unabhängige Verifizierbarkeit	Qualitativ	Erfüllt mit Einschränkung
II.4	Niedrigschwellige Inklusivität	Qualitativ	Erfüllt mit Einschränkung

Sieben der acht Kriterien tragen dasselbe Label. II.1 ist der einzige Ausreißer und zugleich kritisch in der Kaskade.

Abbildung 4.10 IST-Bewertungsprofil Dimension I und II — die acht Einzelbewertungen mit Hierarchie-

stufe und Bewertungslabel

Synthese Dimension II

Das Bewertungsprofil der zweiten Dimension zeigt eine ausgeprägte Asymmetrie. Die Kritische Bedingung (II.1) steht auf „Bedingt erfüllt", die drei Qualitativen Kriterien (II.2, II.3, II.4) stehen konsistent auf „Erfüllt mit Einschränkung". Der schwächste Befund der gesamten IST-Bewertung liegt in dieser Dimension, getrieben durch den Offen-Indikator der Builder-Konzentration. Die Dimension enthält sowohl die kritischste Schwachstelle des Systems, die fehlende protokolläre Neutralitätsgarantie, als auch eine seiner strukturell stärksten Eigenschaften, die offene Generativität. Die Spannung zwischen beiden Befunden ist kein Widerspruch: Sie zeigt ein System, das maximale Offenheit produziert, die Neutralität dieser Offenheit aber operativ der Marktdynamik überlässt.

Die drei Qualitativen Kriterien zeigen keine fundamentalen Defizite, und ihre Einschränkungen folgen dem Grundmuster der gesamten IST-Bewertung: Die Protokollebene liefert die richtigen Eigenschaften, die operative Ebene realisiert sie unvollständig. Offene Generativität (II.2) verbindet Permissionless Deployment mit einer offenen Toolchain, eingeschränkt durch die L2-Composability-Fragmentierung, die ausgerechnet die Eigenschaft untergräbt, die das DeFi-Ökosystem hervorgebracht hat. Unabhängige Verifizierbarkeit (II.3) ist protokollär verankert und toolseitig ausgebaut, mit der wachsenden L2-Verifikationskomplexität und den Spezifikationslücken als dokumentierten Einschränkungen. Niedrigschwellige Inklusivität (II.4) hat sich durch Blob-Transactions und Account Abstraction substanziell verbessert, wobei die 32-ETH-Barriere als das einzige IST-Defizit ohne Roadmap-Pfad den Zugang zur dezentralen Validator-Kontrolle blockiert, während der transaktionale Zugang substanzielle Inklusivität bietet.

II.1 als Kritische Bedingung trägt ein Gewicht, das über das Gewicht der Qualitativen Kriterien hinausgeht. „Bedingt erfüllt" bei einer Kritischen Bedingung ist qualitativ ein anderer Zustand als „Erfüllt mit Einschränkung", weil die Kerneigenschaft des Infrastrukturanspruchs, die protokolläre Neutralitätsgarantie, noch nicht auf dem erforderlichen Niveau gesichert ist. Der Pfad zur Sicherung ist erkennbar, weil FOCIL als spezifizierter Mechanismus existiert, aber er ist im IST nicht gesichert, weil Governance-Entscheidungen, technische Machbarkeit und Community-Konsens noch ausstehen. Der Befund ist jedoch nicht „Offen", was bedeutet, dass die Kaskade diesen Zustand anders behandelt als ein fundamentales Verfehlen. Welche Kaskadenstufe dieser Befund auslöst und wie er mit den Befunden der dritten Dimension interagiert, wird in der Gesamtsyn-

these (4.10) ausgeführt.

4.9 Dimension III: Resilienz und Souveränität

Die ersten beiden Dimensionen haben geprüft, ob das System die strukturellen und qualitativen Voraussetzungen einer fundamentalen Infrastruktur mitbringt. Ihre Bewertung bildet ein Profil, das sieben von acht Kriterien auf „Erfüllt mit Einschränkung“ und eines, die Neutralität und Zensurresistenz, auf „Bedingt erfüllt“ setzt. Die dritte Dimension verschiebt den Zeithorizont: Weg von der Frage, ob Ethereum heute geeignet ist, hin zur Frage, ob es geeignet bleiben kann, stabil über Jahrzehnte, anpassungsfähig ohne Destabilisierung, frei von proprietären Abhängigkeiten und auf generischer Hardware betreibbar. Vier Kriterien operationalisieren diese Frage, eine Strukturelle Bedingung (III.1) und drei Qualitative Kriterien (III.2, III.3, III.4), wobei III.4 ein anspruchsspezifischer Sonderfall ist, der ohne korrespondierendes Muster aus der Infrastrukturanalyse in Kapitel 3 existiert. Keine Kritische Bedingung liegt in dieser Dimension, was bedeutet, dass ihre Ergebnisse das Gesamturteil nicht nach unten deckeln können und stattdessen innerhalb der Eignungsstufe differenzieren, die durch die Kritischen Bedingungen bestimmt wird.

III.1 Langfristige Stabilität

Langfristige Stabilität ist die einzige Strukturelle Bedingung dieser Dimension und fragt, ob Ethereum über Dekaden stabil operieren kann, ökonomisch nachhaltig, technisch wartbar, ohne Akkumulation systemischer Risiken, die die Weiterführung in Frage stellen. Das Kriterium hat eine Sonderstellung, weil es die Spannung zwischen der bemerkenswerten Kurzzeitstabilität des Systems und den identifizierbaren Langzeitvektoren sichtbar machen muss, die diese Stabilität unterlaufen könnten.

Der Protokoll-Upgrade-Track-Record ist der stärkste Indikator. Seit dem Merge hat Ethereum vier erfolgreiche Hard Forks abgeschlossen, von Shapella über Dencun und Pectra bis zu Fusaka, bei einer Kadenz von circa sechs bis zwölf Monaten. Keiner dieser Forks hat einen Chain-Split erzeugt. Für ein globales, dezentrales Protokoll ohne zentrale Release-Authority ist diese Konsistenz bemerkenswert, weil jeder Fork die Koordination über zehn unabhängige Client-Teams erfordert. Die Kehrseite dieser Kadenz ist die Komplexitätsakkumulation: Pectra bündelte elf EIPs in einem einzigen Release, den komplexesten Single-Release-Scope in der Ethereum-Geschichte, und der Dezember-2025-Prysm-Bug bei Fusaka war eine direkte Folge dieser Komplexität. Ein Bug im Prysm-

Client senkte die Netzwerk-Partizipation temporär auf rund 75 Prozent, ohne die Finalität zu unterbrechen, weil die übrigen Clients weiterliefen. Die Backward Compatibility ist über die gesamte Laufzeit gewahrt: Contracts von 2017 laufen unverändert, wobei die einzige systematische Ausnahme Gas-Repricing-EIPs sind, die historisch Contract-Funktionalität gebrochen haben, weil manche Contracts Gas-Kosten hardcoded annahmen.

Das State Growth ist der kritische Langzeitfaktor, der die Stabilität des Systems bedroht, und seine Bedeutung reicht über III.1 hinaus, weil es die Bewertungen von II.4 (Inklusivität) und III.4 (Hardware-Agnostik) direkt beeinflusst. Die in Abschnitt 4.1 dokumentierte Full-Node-Größe von 1.579 Gigabyte wächst mit circa 14 Gigabyte pro Woche, eine Rate, die den Full Node samt History misst und deshalb über der Wachstumsrate des State allein liegt, und das Protokoll hat keinen nativen Mechanismus, der dieses Wachstum begrenzt. Jeder deployte Contract, jedes neue Wallet, jeder gespeicherte Storage-Slot akkumuliert permanent auf allen Full Nodes, ohne dass inaktive Einträge verfallen oder komprimiert werden. Die Projektionen aus Abschnitt 4.8 zeigen die Trajektorie. Bei einem Gas-Target von 200 Millionen, das die Glamsterdam-Phase der Roadmap als Ziel definiert, erreicht die Full-Node-Größe 5 Terabyte bis 2028 und 9 Terabyte bis 2030.[122] Diese Projektion ist keine pessimistische Annahme, sondern eine lineare Extrapolation dokumentierter Wachstumsraten unter Berücksichtigung der geplanten Gas-Limit-Erhöhung. Wenn Full-Node-Betrieb auf Datacenter-Hardware beschränkt wird, verliert Ethereum die physische Dezentralisierungsgrundlage, die die in II.4 bewertete Inklusivität und die in III.4 bewertete Hardware-Agnostik voraussetzen. Der Ethereum-Kernentwickler-Konsens klassifiziert State Growth als das dringlichste ungelöste skalierungsbedingte Zentralisierungsrisiko. Verkle Trees (EIP-6800, Status RES, Stagnant) und History Expiry (EIP-4444, Phase 1 DEPL seit Juli 2025, Phase 2 PLAN) adressieren Teile des Problems, wobei Verkle Trees Stateless Clients ermöglichen, die den State nicht lokal speichern müssen, und History Expiry die Speicheranforderungen für historische Daten reduziert. State Expiry selbst, das Konzept, inaktive Zustandseinträge nach einer definierten Periode verfallen zu lassen, befindet sich im Status RES ohne Implementierungscommitment und ist konzeptuell hochkomplex, weil die Abgrenzung zwischen aktivem und inaktivem State, die Proof-Generierung für verfallenen State und die Backward-Compatibility-Implikationen offene Forschungsfragen sind.[123]

[122] Projektionen basierend auf dokumentierten Wachstumsraten und dem geplanten Gas-Target von 200 Millionen. Vgl. Abschnitt 4.8 für die Datengrundlage und die Szenario-Analyse.

[123] Verkle Trees: EIP-6800, Status RES, Stagnant. History Expiry: EIP-4444, Phase 1 DEPL seit Juli 2025, Phase 2

Die ökonomische Nachhaltigkeit stellt die zweite Langzeitfrage. Das in Abschnitt 4.3 beschriebene Issuance-Modell erzeugt eine leichte Inflation von circa 0,5 Prozent jährlich, wobei die EIP-1559-Basisfee-Verbrennung unter hoher Auslastung einen deflationären Gegenpart liefert. Die L2-Migration hat dieses Gleichgewicht verschoben: Wenn L2s den Großteil der Transaktionsaktivität absorbieren, sinkt die L1-Fee-Revenue, und damit verringert sich der deflationäre Gegenpart zur Issuance. Langfristig ist die Frage, ob die L1-Fee-Revenue als Settlement-Layer für L2s ausreicht, um das Sicherheitsbudget zu finanzieren, das die ökonomische Sicherheit aus I.2 trägt. Die Issuance-Reform-Debatte, die Abschnitt 4.3 als aktiv und ungelöst dokumentiert hat, adressiert genau diese Frage, hat aber im IST-Zustand keinen Lösungspfad produziert: Kein Feature im Status PLAN oder DEPL adressiert die langfristige Sicherheitsbudget-Frage. Die Debatte selbst ist ein Governance-Testfall, weil die Interessen der Staker (höhere Rendite) und die Interessen des Netzwerks (nachhaltige Sicherheit) in einem Spannungsverhältnis stehen, das der informelle Konsensprozess bislang nicht aufgelöst hat.

Die Post-Quantum-Migration bildet die dritte Langzeitfrage. Die kryptographischen Grundlagen des Systems, ECDSA für Account-Signaturen, BLS12-381 für Validator-Attestationen und KZG-Commitments für Data Availability, müssen langfristig auf quantenresistente Algorithmen umgestellt werden, weil ein kryptographisch relevanter Quantencomputer Private Keys aus Public Keys ableiten könnte. Die Migration befindet sich im Status RES, wobei über zehn Client-Teams Devnets für Post-Quantum-Kryptographie koordinieren, und sie ist konstitutiv für die Dauerhaftigkeit der kryptographischen Garantien, auf denen die in I.2 und I.4 bewertete Sicherheit beruht. Im IST-Zeithorizont ist das Risiko nicht akut, weil kryptographisch relevante Quantencomputer nach aktuellem Forschungsstand nicht im Fünf- bis Zehn-Jahres-Horizont operativ werden, aber als Langzeitfrage gehört die Migration in die Stabilitätsbewertung, weil sie die Grundlagen des Sicherheitsmodells betrifft.

Die Differenzierung nach Zeithorizont ist für die Bewertung entscheidend und spiegelt ein Muster, das auch die Referenzinfrastrukturen aus Kapitel 3 zeigen: Jede Infrastruktur hat Langzeitrisiken, die ihre aktuelle Funktionsfähigkeit nicht beeinträchtigen, aber ihre Zukunft bestimmen. Kurz- bis mittelfristig, auf einem Horizont von fünf bis zehn Jahren, ist Ethereum stabil: Der Upgrade-Track-Record ist konsistent, die ökonomische Sicherheit liegt in der Größenordnung von 26 Milliarden US-Dollar, und die Validator-Infrastruktur ist in-

PLAN. State Expiry: RES, ohne Implementierungscommitment.

takt. Langfristig, auf einem Horizont von zwanzig Jahren und darüber, bedrohen das State-Growth-Problem, die offene Issuance-Frage und die ausstehende Post-Quantum-Migration die Tragfähigkeit des Systems. Das State Growth ist dabei das strukturell schwerere Problem, weil es physische Hardware-Anforderungen betrifft, die sich nicht durch ökonomische Anreize lösen lassen, während die Issuance-Frage ein Governance-Problem ist, das prinzipiell durch eine Protokolländerung adressierbar wäre, und die Post-Quantum-Migration eine technische Herausforderung, die den gesamten Blockchain-Sektor betrifft und für die Ethereum durch Account Abstraction einen Migrationspfad vorbereitet hat. Langfristige Stabilität steht damit auf: Erfüllt mit Einschränkung. Die Kurz- und Mittelfriststabilität ist operativ belegt, die Langfriststabilität hängt von Entwicklungen ab, die im IST nicht gesichert sind.

Das System ist langfristig stabil, aber kann es sich auch weiterentwickeln? Stabilität ohne Anpassungsfähigkeit wäre Stagnation, und die Roadmap-Komplexität, die Abschnitt 4.5 beschrieben hat, erfordert ein Governance-System, das liefern kann.

III.2 Adaptive Governance

Dieses Kriterium stellt die Komplementärfrage zu III.1: Kann Ethereum auf technische Anforderungen, Sicherheitslücken und veränderte Nutzerbedürfnisse reagieren, ohne dass der Anpassungsprozess selbst das System destabilisiert? Die Spannung zwischen Stabilität und Adaptivität ist in jeder Infrastruktur angelegt, wie Mayntz 1993 für große technische Systeme gezeigt hat, aber in einem dezentralen System ohne formale Steuerungsinstanz nimmt sie eine besondere Form an: Es gibt kein Gremium, das Änderungen anordnen kann, und keinen Abstimmungsmechanismus, der binden könnte.[124]

Der EIP-Prozess ist transparent, selektiv und öffentlich: Von 230 eingereichten EIPs im Jahr 2025 wurden 37 akzeptiert, eine Akzeptanzrate von 16 Prozent, die eine selektive Entscheidungskultur dokumentiert, bei der die Mehrheit der Vorschläge den Qualitätsfilter des Prozesses nicht passiert. Die ACD-Calls (All Core Devs) operieren als zweiwöchentliche Koordinationsinstanz, öffentlich gestreamt und protokolliert, in der Vertreter aller Client-Teams den Inhalt und das Timing der Hard Forks abstimmen. Die Transparenz dieses Prozesses ist für ein System mit dem Infrastrukturanspruch relevant, weil sie es jedem Beobach-

[124] Vgl. Mayntz 1993, S. 97–108. Die Spannung zwischen Steuerung und Selbstorganisation, die Mayntz als zentrales Forschungsproblem identifiziert, manifestiert sich in Ethereums informellem Governance-Modell als Spannung zwischen Rough Consensus und formaler Autorität.

ter ermöglicht, die Governance-Entscheidungen nachzuvollziehen, und weil sie die Machtausübung einzelner Akteure sichtbar macht. Der Prozess funktioniert, aber ohne formale Autorität: Die Entscheidung liegt letztlich bei den Client-Teams, die Software releasen, und bei der Node-Betreiber-Community, die entscheidet, welche Version sie betreibt. Das ist Governance durch Rough Consensus, ein Prinzip, das die IETF-Parallele aus Kapitel 3 aufgreift: Entscheidungen werden getroffen, wenn kein wesentlicher Widerstand mehr besteht, und die IETF hat gezeigt, dass dieses Modell für die Governance eines globalen Protokollstandards funktionieren kann, wobei der TCP/IP-Stack über Jahrzehnte ohne formale Abstimmungsmechanismen weiterentwickelt wurde.

Der Hard-Fork-Track-Record belegt die operative Leistungsfähigkeit. Alle Post-Merge-Forks wurden ohne Chain-Split durchgeführt, und die historische Emergency-Governance-Fähigkeit, die Abschnitt 4.5 mit den September-2016-DoS-Emergency-Forks Tangerine Whistle und Spurious Dragon dokumentiert hat, zeigt, dass das System auch unter akutem Druck handlungsfähig ist. Der Dezember-2025-Prysm-Bug erforderte keinen Emergency-Fork, weil die verbesserte Client-Diversität den Bug absorbierte, was die strukturelle Governance-Resilienz dokumentiert: Die beste Governance-Reaktion ist die, die nicht gebraucht wird, weil das System den Schock autonom verarbeitet. Die Grenze liegt im fehlenden Pause-Mechanismus: Bei einem Zero-Day-Konsens-Bug im Protokoll dauert die Reaktion Wochen, weil sie die Koordination aller Client-Teams und einen Emergency-Fork erfordert, und für ein System, das über 100 Milliarden US-Dollar sichert, ist diese Reaktionszeit eine Einschränkung.

Die Ethereum Foundation als Governance-Akteur ist eine dokumentierte Zentralisierungsspannung, die für den Infrastrukturanspruch eines dezentralen Systems relevant ist. Board-kontrolliert, ohne protokolläre Rechenschaftspflicht und mit einem Treasury von geschätzten 850 bis 950 Millionen US-Dollar ist die EF der einflussreichste Einzelakteur im Ökosystem, weil sie die Finanzierung der meisten Core-Developer-Teams beeinflusst und durch die Beschäftigung der Geth-Entwickler direkt den dominantesten Execution-Layer-Client kontrolliert.[125] Die Subtraction-Philosophie, die die EF als Leitbild formuliert hat, zielt darauf ab, die eigene Rolle systematisch zu reduzieren, und das Protocol Guild mit über 190 Mitgliedern und mehr als 50 Millionen US-Dollar an empfangenen Mitteln ist eine dezentrale Alternative zur EF-Finanzierung, die die Abhängigkeit des Ökosystems von einer einzelnen Organisation verringert. Beide Mecha-

[125] Protocol Guild: 190+ Mitglieder, >$50 Mio. empfangen (Stand Januar 2026). EF-Treasury-Schätzung: $850–950 Mio. auf Basis des Ethereum Foundation Report 2024 und der ETH-Marktentwicklung.

nismen sind allerdings nicht protokollär verankert: Weder die EF noch das Protocol Guild haben eine protokollseitige Garantie, die ihre Finanzierung oder ihre Governance-Rolle absichert, und die Nachhaltigkeit des Protocol Guild hängt von der Zahlungsbereitschaft des Ökosystems ab, die in Abschwungphasen sinken kann.

Die Issuance-Reform-Debatte ist der aktive Testfall für die Governance-Fähigkeit bei kontroversen Entscheidungen, und ihr Ausgang wird zeigen, ob der informelle Konsensprozess auch dann funktioniert, wenn die ökonomischen Interessen der Governance-Teilnehmer direkt tangiert sind. Die Frage, ob und wie die ETH-Issuance angepasst werden soll, berührt direkte ökonomische Interessen der Staker, die rund 30 bis 31 Prozent des ETH Supply kontrollieren und von einer höheren Rendite profitieren, und steht in einem Spannungsverhältnis zur langfristigen Sicherheitsnachhaltigkeit, die von einer nachhaltigen Issuance-Politik abhängt. Die Debatte hat im IST-Zustand keinen Konsens produziert, was sowohl die Schwierigkeit der Entscheidung als auch die Grenzen des informellen Governance-Modells bei Verteilungskonflikten dokumentiert. Der Befund für Adaptive Governance lautet: Erfüllt mit Einschränkung. Das Governance-System ist operativ stark und hat einen Track Record, den kein vergleichbares dezentrales System vorweisen kann, aber die Informalität bietet keine mechanischen Garantien für Extremkonflikte, und die EF-Zentralisierung steht in Spannung zum dezentralen Anspruch.

Das System kann sich weiterentwickeln. Die nächste Frage prüft, ob es dabei neue Abhängigkeiten erzeugt: Ist die Offenheit, die II.2 als stärkste Eigenschaft des Systems identifiziert hat, auch auf der Infrastrukturschicht realisiert?

III.3 Souveräne Portabilität

Dieses Kriterium fragt, ob Ethereum frei von proprietären Abhängigkeiten ist, die einzelne Akteure in unkontrollierbare Kontrollpositionen bringen. Die Antwort fällt unterschiedlich aus, je nachdem, welche Schicht des Systems betrachtet wird.

Die Protokollschicht ist vollständig Open Source und proprietätsfrei, und das unterscheidet Ethereum fundamental von allen sieben Referenzinfrastrukturen in Kapitel 3. Alle zehn Clients, fünf auf dem Execution Layer und fünf auf dem Consensus Layer, stehen unter liberalen Lizenzen, von LGPL-3.0 für Geth über Apache 2.0 für Besu bis zu MIT für zahlreiche Tools. Die Spezifikationen, vom Yellow Paper über die Execution Layer Specs bis zu den Consensus Specs, sind öffentlich dokumentiert und frei verfügbar. Es gibt kein Ethereum-Inc., das IP-Rechte hält, und die Ethereum Foundation als Schweizer Stiftung besitzt das Protokoll nicht und kann es nicht legal kontrollieren. SWIFT ist eine belgische Genossenschaft unter Mitglieder-Governance, GPS steht unter dem US-Verteidigungsministerium, Cloud-Infrastruktur ist proprietär: Keine dieser Referenzinfrastrukturen erreicht die Proprietätsfreiheit, die Ethereums Protokollschicht aufweist. Der EVM-Standard selbst ist als De-facto-Standard ohne proprietäre Kontrolle in das breitere Blockchain-Ökosystem diffundiert: Der OP Stack, Arbitrum, zkSync, Polygon und BNB Chain haben die EVM als Ausführungsumgebung übernommen, was eine Standardisierungsdynamik erzeugt, die den Wechsel zwischen EVM-kompatiblen Systemen erleichtert und die Portabilität auf der Anwendungsschicht stärkt.

Die Multi-Client-Architektur verstärkt diesen Befund. Die historische Geth-Dominanz, die 2020 bis 2023 bei über 70 Prozent des Execution Layers lag, ist das dokumentierte Klumpenrisiko dieser Dimension, weil Geth-Bugs bei einem Marktanteil über der 33-Prozent-Blocking-Minority Konsens-Spaltung verursachen könnten. Die IST-Situation zeigt eine deutliche Verbesserung: Geth ist auf circa 42 Prozent gesunken, Nethermind hält rund 24 Prozent, Besu rund 16 Prozent, und kein Consensus-Layer-Client überschreitet 34 Prozent.[126] Die Tatsache, dass Nutzer zwischen fünf EL- und fünf CL-Clients frei wählen und kombinieren können, ist eine Portabilitätseigenschaft, die in zentralisierten Systemen kein Äquivalent hat: Ein SWIFT-Teilnehmer kann die SWIFT-Software nicht durch eine Alternative ersetzen, ein Ethereum-Node-Betreiber kann

[126] Client-Diversitäts-Daten: clientdiversity.org / supermajority.info, Stand Anfang 2026. Execution-Layer-Verteilung: Geth rund 42 Prozent, Nethermind rund 24 Prozent, Besu rund 16 Prozent, Erigon rund 11 Prozent, Reth rund 7 Prozent.

zwischen 25 Client-Kombinationen wählen. Die kryptographischen Standards, ECDSA, BLS12-381, Keccak-256 und KZG-Commitments, sind offene Standards ohne proprietäre Bindung, wobei die Quantenresistenz ein Langzeitrisiko darstellt, das im IST-Zeithorizont nicht akut ist, weil kryptographisch relevante Quantencomputer nach aktuellem Forschungsstand nicht im Fünf- bis Zehn-Jahres-Horizont operativ werden.

Die operative Infrastrukturschicht zeigt ein anderes Bild. Die in I.2 dokumentierte RPC-Konzentration von 70 Prozent über Infura und Alchemy, die proprietäre SaaS-Services sind, erzeugt eine De-facto-Abhängigkeit auf der Zugriffsschicht, die für die Mehrheit der Nutzer und Entwickler den operativen Standard darstellt. Dezentrale Alternativen wie dRPC und Pocket Network existieren, haben aber geringe Verbreitung, weil institutionelle Nutzer die SLAs der etablierten Provider bevorzugen. Die L2-Proliferation hat neue Soft-Lock-ins geschaffen, die auf einer Schicht operieren, die das Ethereum-Protokoll selbst nicht kontrolliert: Der OP Stack ist Apache-2.0-lizenziert, aber die Optimism Foundation fungiert als De-facto-Standard-Setzer. zkSync und Starknet nutzen teilweise proprietäre Prover-Technologien, und ein Protokoll, das auf Arbitrum deployt und Arbitrum-spezifische Features wie Stylus oder spezifische Precompiles nutzt, ist nicht ohne Weiteres auf einen anderen Stack migrierbar. Diese neue Schicht von Abhängigkeiten qualifiziert den Proprietätsfreiheits-Anspruch auf der Nutzungsebene, ohne die Proprietätsfreiheit der Basisschicht zu beeinträchtigen.[127]

Souveräne Portabilität steht auf: Erfüllt mit Einschränkung. Die Protokollschicht ist proprietätsfrei in einem Ausmaß, das keine der Referenzinfrastrukturen erreicht. Die operative Schicht zeigt Konzentrationen und L2-Lock-ins, die den Anspruch auf der Nutzungsebene qualifizieren.

Die Software-Souveränität ist gegeben. Die letzte Frage betrifft die Hardware: Kann das System auf generischer, handelsüblicher Hardware betrieben werden?

[127] Zur L2-Lock-in-Problematik: OP Stack (Apache 2.0, Optimism Foundation), Arbitrum Nitro (MIT, Offchain Labs-Governance), zkSync Era und Starknet (teilweise proprietäre Prover). Die Fragmentierung erzeugt eine neue Schicht von Soft-Lock-ins, die auf der Basisschicht nicht existiert.

III.4 Hardware-Agnostik

Dieses Kriterium hat eine Sonderstellung im Bewertungsrahmen, weil es ohne korrespondierendes Muster aus der Infrastrukturanalyse in Kapitel 3 existiert, wie die in Kapitel 2 gesetzte Definition festhält: Keines der sieben Referenzsysteme weist das spezifische Risiko einer Cloud-Konzentration in der Form auf, wie es bei Ethereum existiert. Das Kriterium prüft, ob die Hardware-Unabhängigkeit, die Proof of Stake architektonisch ermöglicht, operativ realisiert ist.

Die Architektur ist stark. Der in Abschnitt 4.1 beschriebene Übergang von Proof of Work zu Proof of Stake hat die ASIC-Abhängigkeit eliminiert und den Energiebedarf um 99,95 Prozent reduziert, was eine fundamentale Veränderung der Hardware-Anforderungen darstellt: Proof of Work erforderte spezialisierte ASICs oder Hochleistungs-GPUs, die einen eigenen industriellen Sektor mit Lieferkettenabhängigkeiten, Stromkosten-Arbitrage und Hardware-Obsoleszenzzyklen erzeugten, während Proof of Stake auf generische CPU-Rechenkapazität und SSD-Speicher angewiesen ist. Ein Validator-Node benötigt rund 100 Watt, was Consumer-Energie-kompatibel ist und den Betrieb auf Solarenergie oder unterbrechungsfreier Stromversorgung in Regionen mit instabiler Infrastruktur ermöglicht. Alle zehn Clients laufen nativ auf ARM-64 und x86-64-Architekturen, wobei Nimbus explizit für Low-Power-ARM-Devices optimiert ist. Das Protokoll hat keine Hardware-Präferenz: Ein Validator auf Consumer-Hardware hat dasselbe Stimmgewicht wie ein Validator auf einem Datacenter-Server, weil die Abstimmung key-pair-basiert ist und nicht von der Rechenleistung abhängt. Diese strukturelle Eigenschaft ist eine Post-Merge-Errungenschaft, die Ethereum von ASIC-abhängigen Systemen wie Bitcoin fundamental unterscheidet und die Voraussetzung für die physische Dezentralisierung schafft, die der Infrastrukturanspruch erfordert.

Die Cloud-Konzentration konterkariert diese Protokolleigenschaft. Rund 59 Prozent der gehosteten Execution-Layer-Nodes laufen auf drei Cloud-Providern, wobei AWS 35,5 Prozent, Hetzner 13,8 Prozent und OVHcloud 9,7 Prozent halten. Der Trend ist rückläufig seit 2022, was eine positive Entwicklung dokumentiert, aber die Konzentration bleibt substanziell: Wenn AWS, Hetzner und OVHcloud koordiniert abschalten oder regulatorisch abgekoppelt werden, fällt eine Mehrheit der gehosteten Node-Infrastruktur aus. Der AWS-Outage im Oktober 2025 hat gezeigt, dass das Netzwerk den Ausfall einer AWS-Region absorbieren konnte, ohne Finalität zu verlieren, was die Robustheit dokumentiert, aber der Korridor zwischen normalem Betrieb und Finalitätsverlust wurde kurzfristig enger. Home-Staking, also der Betrieb auf eigener Hardware,

liegt bei unter 15 Prozent des gestakten ETH und schließt die Solo-Staker aus Abschnitt 4.3 als kleinere Teilmenge ein, was bedeutet, dass der Großteil der Validator-Infrastruktur physisch auf kommerziellen Cloud-Servern liegt und die Dezentralisierung, die das Protokoll auf der logischen Schicht ermöglicht, auf der physischen Schicht durch kommerzielle Abhängigkeiten untergraben wird.[128]

Die geographische Verteilung verstärkt das Bild: 39 Prozent der Nodes operieren in den USA, 14,5 Prozent in Deutschland, 14 Prozent in China, und rund 53 Prozent in zwei Ländern. Jenseits dieser drei Länder verteilt sich der übrige Node-Anteil auf zahlreiche weitere Jurisdiktionen, von denen mehr als zehn, darunter Singapur, Kanada, Japan, Australien, die Niederlande und die Schweiz, jeweils über ein Prozent der Nodes halten. Der geographische Indikator des Kriteriums, mindestens zehn Länder mit jeweils über einem Prozent, ist damit erfüllt. Die Cloud-Konzentration multipliziert die Jurisdiktions-Exposition, weil US-basierte Provider wie AWS die Exposition über die reine Node-Geographie hinaus vergrößern. Für ein System, das beansprucht, geopolitische Instrumentalisierung zu widerstehen, ist die Kombination aus geographischer und infrastruktureller Konzentration eine Einschränkung, die bei II.1 in der Jurisdiktions-Dimension und hier in der Hardware-Dimension sichtbar wird.

Der größte Einzelprovider AWS trägt mit 35,5 Prozent unterhalb des Schwellenwerts für „Offen“ von über 50 Prozent auf einem einzelnen Provider, während sich das Aggregat von 59 Prozent auf drei Provider verteilt, und der rückläufige Trend seit 2022 dokumentiert eine positive Entwicklung. Hardware-Agnostik steht auf: Erfüllt mit Einschränkung. Die protokolläre Hardware-Agnostik ist vollständig realisiert, ohne ASIC-Abhängigkeit, ARM-kompatibel und Consumer-Energie-tauglich, aber die operative Cloud-Konzentration auf drei Providern erzeugt eine physische Abhängigkeit, die die Dezentralisierung auf der logischen Schicht unterläuft, und der geringe Home-Staking-Anteil von unter 15 Prozent zeigt, dass die architektonische Möglichkeit des Consumer-Hardware-Betriebs von der Mehrheit der Validatoren nicht genutzt wird.

[128] Cloud-Konzentrationsschätzung: Ethernodes, Anfang 2026. Die 59 Prozent beziehen sich auf gehostete EL-Nodes; der Home-Staking-Anteil unter 15 Prozent ist eine Schätzung auf Basis der Node- und Cloud-Verteilung aus Abschnitt 4.1.

Synthese Dimension III

Das Bewertungsprofil der dritten Dimension zeigt ein konsistentes Muster: Alle vier Kriterien stehen auf „Erfüllt mit Einschränkung", identisch zu Dimension I. Das Muster ist allerdings anders gelagert. Die drei Dimensionen bilden ein Triptychon der Diskrepanz: Dimension I zeigt den Abstand zwischen Protokollversprechen und operativer Einlösung im Hier und Jetzt, Dimension II die Spannung zwischen maximaler Offenheit und fehlender Neutralitätsgarantie, und Dimension III den Abstand zwischen gegenwärtiger Funktionsfähigkeit und langfristiger Tragfähigkeit. Jede Facette hat eigene Adressierungspfade, und die Gesamtsynthese wird zeigen, welche dieser Facetten das Gesamturteil bestimmt. Das State Growth, die offene Issuance-Frage und die Post-Quantum-Migration sind keine akuten Probleme, die den heutigen Betrieb gefährden, sondern Langzeitvektoren, die sich über Jahre entfalten und die strukturelle Tragfähigkeit des Systems mittelfristig herausfordern. Die Governance ist operativ stark, hat einen Track Record, den kein vergleichbares dezentrales System vorweisen kann, aber die Informalität bietet keine mechanischen Garantien für den Fall, dass der soziale Konsens bricht. Die Proprietätsfreiheit ist auf der Protokollschicht stärker als bei jeder Referenzinfrastruktur, wird aber auf der operativen Schicht durch RPC-Konzentration und L2-Lock-ins qualifiziert. Die Hardware-Agnostik ist architektonisch vollständig realisiert, wird aber durch Cloud-Deployment-Muster konterkariert, die eine physische Abhängigkeit erzeugen, die das Protokolldesign ausschließt.

Die Strukturelle Bedingung III.1 steht auf „Erfüllt mit Einschränkung" und zählt damit im dritten Kaskadenschritt als schwach: Die Langfriststabilität ist grundsätzlich gegeben, mit dokumentierten Risiken, die den Anspruch qualifizieren, ohne die Tragfähigkeit im bewerteten IST-Zeitraum zu untergraben. Keine Kritische Bedingung liegt in dieser Dimension, doch III.1 geht als schwache Strukturelle Bedingung in den dritten Kaskadenschritt ein und trägt dort zur Deckelung bei, während die Eignungsstufe durch die sechs Qualitativen Kriterien differenziert wird. Alle zwölf Kriterien sind bewertet, und das vollständige Profil liegt vor. Die Gesamtsynthese führt die Einzelbefunde zum IST-Profil zusammen und formuliert das Gesamturteil über die M3-Kaskade.

4.10 Gesamtsynthese und IST-Urteil

Die zwölf Einzelbewertungen der Abschnitte 4.7 bis 4.9 ergeben ein Profil, das in seiner Konsistenz ebenso aufschlussreich ist wie in seiner einzigen Abweichung. Kein Kriterium erreicht „Erfüllt“ ohne Qualifizierung, was bedeutet, dass das System in keiner Dimension die Anforderungen vollständig und ohne strukturelle Einschränkungen erfüllt, und was zugleich zeigt, dass die Infrastrukturanforderungen, die Kapitel 2 hergeleitet und Kapitel 3 an sieben Referenzinfrastrukturen validiert hat, für den Gegenstand anspruchsvoll kalibriert sind. Elf der zwölf Kriterien stehen auf „Erfüllt mit Einschränkung“, was bedeutet, dass die jeweilige Anforderung grundsätzlich erfüllt ist, mit identifizierten Limitationen, die den Anspruch qualifizieren, aber nicht fundamental untergraben. Eines, Neutralität und Zensurresistenz (II.1), steht auf „Bedingt erfüllt“, was bedeutet, dass die Erfüllung von Bedingungen abhängt, die im IST-Zustand nicht gesichert sind, insbesondere der Implementierung eines protokollären Mechanismus zur Erzwingung der Transaktionsinklusion. Keines steht auf „Offen“, was bedeutet, dass kein Kriterium eine fundamentale Anforderung verfehlt, für die kein operativer Pfad erkennbar wäre. Das numerische Profil 0-11-1-0 zeigt ein System, das die Infrastrukturanforderungen in der Breite adressiert, bei dem aber die operative Realität die protokollären Möglichkeiten noch nicht vollständig einlöst.

0 – 11 – 1 – 0 keinmal Erfüllt, elfmal Erfüllt mit Einschränkung, einmal Bedingt erfüllt, keinmal Offen

Abbildung 4.11 IST-Profil aller zwölf Kriterien — Bewertungslabel nach Hierarchiestufe und Dimension

Die in Kapitel 2 definierte M3-Kaskade bestimmt das Gesamturteil anhand der hierarchischen Stufung der Kriterien. Die drei Kritischen Bedingungen bilden die erste Prüfungsstufe. Sicherheits- und Vertrauenslast (I.2) steht auf „Erfüllt mit Einschränkung“: Die ökonomische Sicherheit trägt über die mechanisch er-

zwungene Slashing-Sanktion und die Größenordnung eines Angriffs, dessen statische Kapitalanforderung am Stichtag bei rund 26 Milliarden US-Dollar liegt und dessen tatsächliche Kosten die Marktilliquidität weit darüber treibt. Die Einschränkung liegt in der Marktpreisabhängigkeit dieser Sicherheit und in der operativen Restvertrauenslast des vierschichtigen Trust-Stacks, die den Anspruch qualifizieren, ohne ihn fundamental zu untergraben. Minimale tragfähige Garantien (I.4) steht ebenfalls auf „Erfüllt mit Einschränkung“: Drei von vier Garantien sind protokollär verankert und operativ bewiesen, wobei der Degradation Mode eine Eigenschaft ohne Äquivalent in den Referenzinfrastrukturen darstellt, und die vierte Garantie, die Zensurresistenz unter Angriff, funktional gegeben, aber nicht protokollär abgesichert ist. Beide Kritischen Bedingungen passieren die Kaskadenschwelle: Die Kerneigenschaften Sicherheit und Garantien sind grundsätzlich gegeben. Neutralität und Zensurresistenz (II.1) passiert die Schwelle nicht uneingeschränkt. Die Builder-Konzentration von 93,3 Prozent bei drei Akteuren markiert einen strukturellen Defekt, und kein Protokollmechanismus erzwingt die Transaktionsinklusion. Die Zensurresistenz des Systems ist eine emergente Marktleistung, keine protokolläre Garantie, und für eine Infrastruktur, die Neutralität als Kernanspruch erhebt, ist diese Abhängigkeit eine Bedingung, die im IST nicht eingelöst ist. Der Befund ist „Bedingt erfüllt“, nicht „Offen“, was bedeutet, dass der Pfad zur Erfüllung erkennbar ist, die Erfüllung aber von der Implementierung von FOCIL oder eines funktional äquivalenten Mechanismus abhängt. Keine Kritische Bedingung steht auf „Offen“, was das Gesamturteil von „Bedingt geeignet“ abhebt. Eine Kritische Bedingung steht auf „Bedingt erfüllt“, was die Kaskade auf die Stufe „Geeignet unter erheblichen Bedingungen“ setzt.[129]

Die drei Strukturellen Bedingungen bilden die zweite Prüfungsstufe. Funktionale Unersetzbarkeit (I.1), Koordinationsfunktion (I.3) und Langfristige Stabilität (III.1) stehen alle auf „Erfüllt mit Einschränkung“. Die strukturelle Grundlage ist tragfähig: Ethereum fungiert als Gravitationszentrum für dezentrale Koordination mit einer TVL-Dominanz von über 60 Prozent und einer Developer-Verankerung von über 70 Prozent aller Blockchain-Entwickler. Es erbringt eine quantitativ und qualitativ einzigartige Koordinationsleistung, die rund 100 Milliarden US-Dollar permissionless koordiniert, und es ist kurz- bis mittelfristig stabil, mit einem konsistenten Upgrade-Track-Record und einer

[129] Die Kaskadenlogik im zweiten Schritt wurde in Kapitel 2 als methodische Ergänzung eingeordnet: „Bedingt erfüllt“ bei einer Kritischen Bedingung ist qualitativ ein anderer Zustand als „Erfüllt mit Einschränkung“, weil die Kerneigenschaft des Infrastrukturanspruchs noch nicht auf dem erforderlichen Niveau gesichert ist. Vgl. Abschnitt 2.3 zur Definition der Urteilskategorien und der M3-Kaskadenlogik.

Finality-Rate von über 99,99 Prozent. Die Einschränkungen, die emergente Verankerung, die L2-Fragmentierung und die Langzeitrisiken aus State Growth und Issuance, qualifizieren die Tragfähigkeit, ohne sie fundamental zu untergraben. Keine Strukturelle Bedingung steht auf „Bedingt erfüllt" oder „Offen", doch alle drei stehen auf „Erfüllt mit Einschränkung" und gelten damit als schwach, sodass der dritte Kaskadenschritt dieselbe Deckelung setzt wie der zweite.

Die sechs Qualitativen Kriterien differenzieren den Grad innerhalb der erreichten Eignungsstufe. Alle sechs, Offene Generativität (II.2), Unabhängige Verifizierbarkeit (II.3), Niedrigschwellige Inklusivität (II.4), Adaptive Governance (III.2), Souveräne Portabilität (III.3) und Hardware-Agnostik (III.4), stehen auf „Erfüllt mit Einschränkung". Die Grad-Skala aus Kapitel 2 definiert den Grad als „Gut", wenn alle sechs Qualitativen Kriterien mindestens auf „Erfüllt mit Einschränkung" stehen, was hier der Fall ist. Die Einschränkungen verteilen sich über verschiedene Dimensionen und zeigen keine Häufung in einem einzelnen Problembereich: L2-Composability-Fragmentierung und L2-Verifikationskomplexität betreffen die Skalierungsarchitektur, die 32-ETH-Solo-Staking-Barriere als einziges Defizit ohne Roadmap-Pfad betrifft die Zugangsschwelle, informelle Governance ohne mechanische Garantien betrifft die Anpassungsfähigkeit, operative RPC-Konzentration und L2-Lock-ins betreffen die Proprietätsfreiheit, und Cloud-Deployment-Muster betreffen die physische Dezentralisierung. Kein einzelnes Qualitatives Kriterium zeigt einen fundamentalen Ausfall, und die Breite der Einschränkungen bestätigt das Grundmuster: Die Einschränkungen sind operativer Natur, nicht protokollärer.

Das Gesamturteil lautet: **Geeignet unter erheblichen Bedingungen, Grad Gut.** Kapitel 2 hat diese Kategorie definiert als einen Zustand, in dem mindestens eine Kritische Bedingung auf „Bedingt erfüllt" steht und die Eignung an benannte, überprüfbare Bedingungen geknüpft ist, wobei die Kerneigenschaft des Infrastrukturanspruchs noch nicht auf dem erforderlichen Niveau protokollseitig gesichert ist, der Pfad zur Sicherung aber erkennbar bleibt.[130] Die zentrale Bedingung, die das Label bestimmt, ist die Implementierung von FOCIL (EIP-7805) oder eines funktional äquivalenten Mechanismus, der die Zensurresistenz von einer emergenten Marktleistung in eine protokolläre Garantie transformiert. Solange die Transaktionsinklusion von der Marktstruktur der Builder abhängt und nicht vom Protokoll erzwungen wird, bleibt die Neutralitätsgarantie, die der Infrastrukturanspruch erhebt, operativ eingelöst, aber strukturell ungesichert.

[130] Vgl. Abschnitt 2.3.3 zur Definition der fünf Urteilskategorien und der M3-Kaskadenlogik. „Geeignet unter erheblichen Bedingungen" ist die mittlere Kategorie des Spektrums und wurde in Kapitel 2 generisch definiert, unabhängig davon, welches Kriterium betroffen ist und welches System bewertet wird.

Das Urteil „Geeignet unter erheblichen Bedingungen“ bedeutet ausdrücklich nicht „Bedingt geeignet“: Es gibt keinen „Offen“-Befund, der eine fundamentale Anforderung verfehlt, und der Pfad zur Einlösung der zentralen Bedingung ist erkennbar und spezifiziert.

Ein Muster durchzieht alle zwölf Bewertungen, und es lässt sich in einem Satz formulieren: Die Diskrepanz zwischen dem, was das Protokoll ermöglicht, und dem, was die operative Realität einlöst, ist das Grundmuster des IST-Zustands. Ethereum bietet auf Protokollebene die Voraussetzungen einer fundamentalen Infrastruktur, von der ökonomischen Sicherheit über die offene Generativität bis zur kryptographischen Verifizierbarkeit, von der atomaren Koordination bis zur automatisierten Selbstheilung. Die operative Nutzungsrealität hat diese Möglichkeiten nicht vollständig realisiert: Der Trust-Stack erzeugt institutionelle Abhängigkeiten, die L2-Fragmentierung untergräbt die Composability, die Builder-Konzentration gefährdet die Neutralität, der State Growth bedroht die langfristige Dezentralisierung, und die Governance operiert ohne mechanische Garantien für Extremkonflikte. Jede der drei Dimensionen zeigt eine eigene Facette dieser Diskrepanz: Dimension I dokumentiert die Spannung zwischen Protokollmöglichkeit und operativer Nutzung, Dimension II die Asymmetrie zwischen der stärksten Eigenschaft (offene Generativität) und der kritischsten Schwachstelle (fehlende Neutralitätsgarantie), und Dimension III die Spannung zwischen Kurzfriststabilität und Langzeitrisiken. Das Profil 0-1 1-1-0 ist die numerische Verdichtung dieser dreifachen Diskrepanz. Die Stärke des Systems liegt in der Tatsache, dass das Protokoll die richtigen Eigenschaften verankert. Die Einschränkung liegt darin, dass die operative Schicht, der Trust-Stack, die L2-Architektur, die Builder-Ökonomie und die Cloud-Infrastruktur, diese Verankerung noch nicht in der Breite einlöst.

Das IST-Urteil definiert die Ausgangslage für die SOLL-Bewertung. Kapitel 5 wird prüfen, ob die Ethereum-Roadmap die identifizierten Einschränkungen adressiert und ob das SOLL-Profil das Gesamturteil verschieben kann. Die Frage ist dabei nicht, ob Ethereum als Infrastruktur geeignet ist, denn das IST-Urteil bestätigt die grundsätzliche Eignung unter Bedingungen, sondern ob die Roadmap die Bedingungen einlösen kann, an die die Eignung geknüpft ist. Der Abstand zwischen „Geeignet unter erheblichen Bedingungen“ und der nächsthöheren Stufe „Geeignet mit Bedingungen“ wird primär durch die kaskadenbestimmende Bedingung definiert: die Transformation der emergenten Zensurresistenz in eine protokolläre Garantie durch FOCIL. Die elf Einschränkungen auf „Erfüllt mit Einschränkung“, vom Trust-Stack über die L2-Fragmentierung und das State Growth bis zur Cloud-Konzentration, bestimmen nicht das Gesamturteil,

sondern den Reifegrad innerhalb der erreichten Eignungsstufe, und die SOLL-Bewertung wird prüfen, welche dieser Einschränkungen durch Roadmap-Features adressierbar sind. Die Roadmap beansprucht, die kaskadenbestimmende Bedingung durch FOCIL zu adressieren, die L2-Composability durch Native Rollups und Based Sequencing zu schließen, das State Growth durch Verkle Trees und History Expiry zu mitigieren, und den Trust-Stack durch Native Rollups und dezentrale Alternativen zu reduzieren. Die SOLL-Bewertung wird prüfen, ob die Features, die diese Abstände schließen sollen, den epistemischen Anforderungen der Taxonomie genügen: PLAN-Features mit klarer Timeline und EIP-Akzeptanz oder RES-Features in früher Forschungsphase. Ob die Roadmap die Bedingungen belastbar einlöst, ist Gegenstand der SOLL-Bewertung.

Kapitel 5

Der Zielzustand: Darstellung und Bewertung der vollständigen Roadmap

5.1 Strategischer Pivot

5.1-A Der strategische Pivot

Kapitel 4 hat das Ethereum im momentanen IST-Zustand des ersten Quartals 2026 dargestellt, erklärt und gegen die vorgestellten Kriterien in Kapitel 2 geprüft. Daraufhin ist die Arbeit zu einem qualifizierten Urteil gelangt, wonach sich das System als fundamentale digitale Infrastruktur eignet, allerdings unter erheblichen Bedingungen. Mit Kapitel 5 wendet die Arbeit den Blick und beschreibt, wie Ethereum aussähe, wenn die Roadmap über einen Horizont von zehn und mehr Jahren vollständig umgesetzt wäre. Das Protokoll wird von hier an als fertig gedachtes System dargestellt und behandelt, dessen Eigenschaften aus dem Zusammenwirken der geplanten Umbauten hervorgehen, wobei der Gegenstand durchgehend der Zielzustand bleibt und nicht der jeweilige Entwicklungsstand einzelner Bausteine.

Der Wechsel verschiebt neben dem Zeitpunkt der Betrachtung auch die Logik, nach der das System gelesen wird. Kapitel 4 hat jedes Kriterium gegen gemessene Zustände geprüft (Validator-Verteilungen, Client-Anteile und Gebührenverläufe etc.) während Kapitel 5 ein Systemdesign liest, dessen Bestandteile als Spezifikationen, Prototypen und Forschungslinien vorliegen und hier zu dem Bild zusammengesetzt werden. Die Darstellung nimmt die Bestandteile in dem Endzustand, den ihre Spezifikationen und Forschungsentwürfe beschreiben, und hält die Frage nach Wahrscheinlichkeit und Reihenfolge ihrer Umsetzung aus der Systemdarstellung heraus. Die folgenden Abschnitte zeigen ein Ethereum, dessen Basisschicht ihre eigene Ausführung in Größenordnungen

trüge, die heute den Rollups vorbehalten sind, dessen Konsens in Sekunden statt in Minuten finalisierte und dessen Garantien sich über angeschlossene Layer hinweg ausdehnen. Bevor die Abschnitte 5.2 bis 5.6 dieses System Schicht für Schicht entfalten, braucht der Zielzustand allerdings seinen Rahmen, denn die Vielzahl der Umbauten wird erst dann als zusammenhängendes Programm lesbar, wenn die strategische Prämisse benannt ist, aus der sie hervorgehen.

Die hier dargelegte Prämisse nimmt ihren Ausgangspunkt im Jahr 2025. Über jenes Jahr hat die Layer 1 ihre Ausführungskapazität deutlich erweitert, während die Rollups, denen die Skalierung der Plattform in der bisherigen Architektur zugedacht war, weiterhin von je einem einzelnen Sequencer geordnet werden, der die Aufnahme und die Reihenfolge der Transaktionen allein bestimmt. Aus der Spannung zwischen beiden Beobachtungen ist die strategische Neuorientierung hervorgegangen, deren Ergebnis das vorliegende Kapitel zeigt. Der dargestellte Zielzustand basiert auf einer grundlegend veränderten Systemarchitektur. Layer 1 erweitert die eigene Ausführungskapazität künftig wieder selbst. Rollups dienen dabei als integrierte, spezialisierte Ausführungsumgebungen (z. B. für Privacy), die komplexe Anwendungen verarbeiten und deren Daten final auf Layer 1 absichern.

Abgelöst wurde mit der Neuorientierung die rollup-zentrische Roadmap, der Ethereum seit 2020 gefolgt war. In ihr blieb die Layer 1 eine bewusst schlanke Schicht für Konsens, Settlement und Datenverfügbarkeit, deren Ausführungskapazität absichtlich begrenzt war, während die Verarbeitung der Transaktionen an die Rollups ausgelagert wurde. Die Arbeitsteilung setzte eine doppelte Annahme voraus, wonach die Rollups die Sicherheitsgarantien der Layer 1 erben, weil sie ihre Daten und Beweise dort verankern und sich zugleich mit der Zeit aus der Kontrolle ihrer Betreiber lösen würden. Wie weit das reale System jener Annahme im ersten Quartal 2026 entsprach, hat Kapitel 4 im Einzelnen erhoben.

Zwei Befunde erzwingen die Revision

Zwei empirische Befunde mit je eigenem Gewicht erzwangen die Revision. Der erste betrifft das Auslagerungsversprechen selbst: Die Dezentralisierung der führenden Rollups verlief erheblich langsamer, als die Roadmap unterstellt hatte. Das zeigt sich daran, dass die großen Netzwerke weiterhin von zentralisierten Sequencern ihrer jeweiligen Betreiber geordnet werden, dass erhebliche Werte hinter den Multisignatur-Schlüsseln von Security Councils liegen und dass die organisatorische Bindung der Betreiber an Ethereum loser ausfällt als die technische Anbindung ihrer Systeme.

Der zweite Befund trägt die Last in umgekehrter Richtung, denn die Layer 1 hat erwiesen, dass sie ihre eigene Ausführung erweitern kann. Über das Jahr 2025 verdoppelte sich das Gas Limit von 30 auf 60 Millionen, ohne dass sich das Protokoll ändern musste, weil die Anpassung über das blockweise Voting der Validatoren lief und allein durch sozialen Konsens koordiniert wurde.[131] Die Wirkung reichte bis in einzelne Anwendungsprojekte hinein, etwa beim Ethereum Name Service, der sein geplantes eigenes Rollup zugunsten der günstiger gewordenen Layer 1 aufgab.[132] Erwiesen ist damit ein Pfad und noch kein Zustand. Bei 60 Millionen Gas verarbeitet die Layer 1 15 bis 30 Transaktionen pro Sekunde. Die Aussage, die Basisschicht skaliere selbst, ist als volle Eigenschaft im heutigen System nicht eingelöst. Der Befund belegt die Richtung der Erweiterung, noch nicht ihre Größenordnung.

Beide Befunde führte Vitalik Buterin am 3. Februar 2026 in einem Beitrag auf X zusammen, in dem er die Abkehr von der bisherigen Strategie aussprach.[133] Er benannte zwei Tatsachen. Die Dezentralisierung der zweiten Schicht sei weit langsamer und mühsamer verlaufen als ursprünglich erwartet, und die Layer 1 skaliere inzwischen selbst. Daraus zog er den Schluss, die ursprüngliche Vision der Rollups als ausgelagerter Skalierungsschicht ergebe keinen Sinn mehr und verlange einen neuen Pfad. Der Beitrag artikuliert die Neuorientierung und begründet sie aus den beiden Befunden, er lässt jedoch offen, welche Gestalt das Verhältnis der Schichten künftig annimmt. Diese Offenheit schließt das neue Modell.

---

[131] Gas-Limit-Verdopplung von 30 auf 60 Millionen über das Jahr 2025, koordiniert über das blockweise Validator-Voting (Anpassung um rund 0,1 Prozent pro Block) ohne Protokolländerung, das Default Target ist in EIP-7935 formalisiert. Datenbasis: Ethereum Foundation, vgl. die Datengrundlage in Abschnitt 5.2.

[132] Einstellung des geplanten ENS-eigenen Rollups Namechain zugunsten der Layer 1, begründet mit einer rund 99-prozentigen Senkung der Registrierungskosten auf der Layer 1. ENS-Blog (nick.eth), 6. Februar 2026, Sekundärberichterstattung: CoinDesk, The Block.

[133] Vitalik Buterin, X-Beitrag vom 3. Februar 2026 (Pivot-Artikulation mit den zwei Tatsachen der zu langsamen L2-Dezentralisierung und der selbst skalierenden Layer 1 sowie der Folgerung, die ursprüngliche Vision ergebe keinen Sinn mehr und ein neuer Pfad sei nötig). Sekundäranker: CoinDesk, Decrypt.

Das neue Modell: zwei Richtungen

Das neue Modell hat zwei Richtungen, deren erste die Layer 1 selbst betrifft. Sie nimmt die Skalierung ihrer eigenen Ausführung wieder auf. Sie beruht dabei auf einem gestaffelten Pfad weiterer Gas-Limit-Erhöhungen und auf einer enshrined zkEVM, unter der Validatoren Blöcke allein über Gültigkeitsbeweise prüfen. Die Last der Verifikation wäre von der Kapazität des Systems entkoppelt, sodass die Kapazität wachsen könnte, ohne die Anforderungen an die Teilnahme am Konsens mitwachsen zu lassen. Die Abstimmung der Validatoren, die die Verdopplung von 2025 trug, wäre darin nur der Anfang, denn die späteren Erweiterungen blieben an die Beweisarchitektur gebunden. Welche Stufen der Pfad durchläuft und auf welcher Architektur die Beweise beruhen, entwickelt Abschnitt 5.2.

Die zweite Richtung bestimmt das Verhältnis zu den Rollups neu. An die Stelle einer homogenen Skalierungsschicht tritt ein Spektrum, das sich entlang zweier Dimensionen ordnet. Der Bindungsgrad reicht von der vollen Konvergenz an die Layer 1 bis zur souveränen Chain mit minimaler Bindung. Die Differenzierung beschreibt, worüber ein Rollup seine Existenz begründet, über Privacy-fokussierte Ausführungsumgebungen, anwendungsspezifische Effizienz, niedrige Latenz statt bloßen Durchsatzes oder extreme Skalierung jenseits der Kapazität der Layer 1. Die Vorstellung einer einheitlichen Rolle der Rollups entfällt in dem Spektrum. Jedes Netz positioniert sich entlang beider Dimensionen und trägt die Folgen seiner Position. Am äußeren Ende steht die souveräne Chain, die mit eigener Datenverfügbarkeit und eigenem Konsens volle Gestaltungsfreiheit gewinnt und zugleich außerhalb der Garantien Ethereums operiert. Innerhalb des Spektrums liegt die Wahl des Vertrauensniveaus bei den Nutzern und Anwendungen selbst, als Redline für die Anbindung an Ethereums Garantien gilt Stage 1, jener Reifegrad, ab dem ein funktionierendes Beweissystem die Eingriffsrechte des Betreibers auf den Notfall beschränkt. Den Mechanismus der vollen Konvergenz soll die native-Rollup-Precompile bereitstellen, über die ein konvergiertes Rollup die Ausführungslogik der Layer 1 unmittelbar nutzen und jedes Protokoll-Upgrade automatisch übernehmen würde, eine Konstruktion, deren Substanz Abschnitt 5.6 entwickelt. Die Privacy-Richtung gewinnt im Schlussteil von Abschnitt 5.1 eigene Gestalt.

Ihre dimensionale Gestalt gewinnt die neue Strategie in fünf Zielbildern, die das Forschungsumfeld als North Stars führt und die Justin Drake im Februar 2026 in der Strawmap bündelte. Die Strawmap ist ein Koordinationsdokument ohne formalen Governance-Status, das die Richtung der Arbeit belegt, ohne einen verbindlichen Zielhorizont zu setzen. Buterin ordnete sie öffentlich als wich-

tige Orientierung ein.[134] Die fünf Zielbilder spannen die Dimensionen des Zielzustands auf, von der Ausführung über die Daten bis zu Konsens, Kryptographie und Privatsphäre. Fast L1 bezeichnet die Konzentration der Finalität, die von heute rund 13 Minuten in den Sekundenbereich sänke und im realisierten Zielzustand über eine Drei-Slot-Finalität bei rund 36 Sekunden läge, deren konsensusseitige Substanz der spätere Verlauf des Kapitels entwickelt. Gigagas L1 benennt die Zielmarke von rund 10.000 Transaktionen pro Sekunde auf der Layer 1, die über den gestaffelten Ausbaupfad der Ausführung langfristig erreichbar würde und deren Stufen ebenfalls in Abschnitt 5.2 stehen. Teragas L2 bezeichnet die Entkopplung des Durchsatzes der zweiten Schicht von der Layer 1 über Data Availability Sampling, deren Mechanik der Datenteil von Abschnitt 5.2 entwickelt. Post-Quantum L1 beschreibt den Endzustand einer vollständig hash-basierten Kryptographie, dessen Substanz der folgende Abschnitt und Abschnitt 5.3 entwickeln, und Private L1 benennt native shielded ETH Transfers auf Protokollebene als langfristige Richtung, deren Substanz ebenjener Schlussteil von Abschnitt 5.1 behandelt.

In der Summe beschreibt der SOLL-Zustand des Kapitels eine Arbeitsteilung, in der die Layer 1 die Ausführung wieder selbst trägt und die Rollups ihren Platz über Bindungsgrad und Differenzierung selbst wählen. Die Garantien der Basisschicht reichen über die Konvergenz dorthin, wo die angeschlossenen Netze sie beziehen wollen. Dass der Anspruch der Neuorientierung über das Protokoll hinausreicht, dokumentieren die Rückbindung der Ethereum Foundation an Cypherpunk-Prinzipien unter dem Titel DeFipunk, der Aufbau des dAI-Departments für die Ökonomie autonomer KI-Agenten samt dem Standard ERC-8004 für Trustless Agents und Buterins Neujahrs-Einordnung Ethereums als zivilisatorischer Infrastruktur.[135] Ob ein Programm solcher Spannweite sich realisieren lässt, hängt an einer Designphilosophie, die die Komplexität des Protokolls selbst zum Gegenstand macht und die der folgende Abschnitt entwickelt.

[134] Justin Drake, Strawmap (strawmap.org), veröffentlicht im Februar 2026, ausdrücklich als Strawman und Roadmap ohne formalen Governance-Status benannt, Koordinationsinstrument für Forscher und Client-Teams.

[135] Vitalik Buterin, Neujahrs-Beitrag vom 1. Januar 2026 (Rahmung Ethereums als Civilisational Infrastructure), Beleg für die Anspruchsebene der Ökosystem-Signale.

5.1-B Lean Ethereum als Designphilosophie

Mit jedem Jahr seiner Entwicklung ist das Protokoll schwerer zu überblicken geworden. Was als überschaubarer Satz von Regeln begann, ist zu einem Geflecht aus Spezifikationen, Client-Implementierungen und kryptographischen Verfahren angewachsen, dessen Wartung Spezialwissen verlangt und dessen Auditierung mit dem Umfang des Codes teurer wird. Der Kreis derer, die das System in seiner Gänze noch überblicken, ist über die Jahre kleiner geworden, und jede neue Fähigkeit, die das Protokoll gewinnt, fügt ihm eine weitere Schicht aus Code und Angriffsfläche hinzu. Die neue Strategie, die Abschnitt 5.1-A umrissen hat, vergrößert das Geflecht weiter, und die Roadmap bindet seine Beherrschbarkeit an eine Designphilosophie, die die Komplexität des Protokolls selbst zum Gegenstand macht.

Lean Ethereum heißt das Programm der Vereinfachung, und es beruht auf der Annahme, dass Sicherheit und Dauer eines Protokolls mit jeder vermeidbaren Komponente sinken, die ein Angreifer studieren und ein Entwickler missverstehen kann. Die Ethereum Foundation hat die akkumulierte Komplexität seit etwa 2024 als eigene Belastung benannt, sichtbar in der Code-Komplexität der Clients ebenso wie in der Erschöpfung des EIP-Konsens-Prozesses.[136] Der Konsens-Prozess kann pro Hard Fork nur eine kleine Auswahl konkurrierender Vorschläge klären und spielt jede zusätzliche Funktion gegen die nächste aus. Die Glieder des Programms reichen von der Reduktion des Client-Codes über die Umstellung auf SSZ als einheitliches Serialisierungsformat bis zu einem formal verifizierten Consensus-Client und hash-basierten Primitiven. Hinzu treten eine neue Execution-Umgebung in Gestalt der leanVM und die RISC-V-Linie als deren Fundament.[137]

Aus den Prinzipien dieser Vereinfachung ginge die Post-Quantum-Resistenz als integrale Eigenschaft hervor. Die Migration aus den heute deployten Komponenten bildete dann allein das Übergangsproblem. Der eigentliche Konstruktionsaufwand liegt anderswo. Hash-basierte Primitiven stehen standardmäßig an der Stelle zahlentheoretischer Verfahren, von Poseidon über leanXMSS bis zu den STARKs, deren Sicherheit allein auf der Kollisionsresistenz von Hashfunktionen beruht. Die ECDLP-abhängigen Komponenten, von der BLS-Aggregation über Pedersen Commitments und IPA bis zu KZG, weichen hash-basierten Alternativen, womit die Angriffsfläche für einen hinreichend großen

[136] EF-Komplexitätsdiagnose: Vitalik Buterin, „Possible futures of the Ethereum protocol“ (Blog-Serie ab Oktober 2024, insbesondere „The Purge“), fortgeschrieben in der Post-Quantum-Roadmap vom 26. Februar 2026.

[137] leanVM und RISC-V: Verweis auf Abschnitt 5.2-E für die Substanz.

Quantencomputer entfällt. Formale Verifizierbarkeit auf allen Ebenen träte hinzu und machte die Korrektheit beweisbar und nicht bloß empirisch vertraut. Lean Ethereum erscheint so als kryptographische Vereinfachung mit emergenter Post-Quantum-Resistenz. Sie folgt strukturell aus der Architektur jenseits 2029.

Auf der Consensus-Schicht nähme der Lean-Ethereum-Endzustand die Gestalt der Beam Chain an, inzwischen Lean Consensus genannt, einer vollständigen Neugestaltung der bestehenden Beacon Chain, die fünf Jahre Betriebserfahrung aufnähme und deren Aufgabe übernähme, ohne deren kryptographisches Fundament zu erben. Hash-basierte Validator-Signaturen aus der leanXMSS-Linie träten an die Stelle der BLS-Signaturen, konstruktiv Post-Quantum-resistent. An die Stelle der algebraischen BLS-Aggregation träte eine hash-basierte Aggregation, die viele gültige Signaturen über hash-native Beweisverfahren wie STARKs und hash-basierte SNARKs zu einem einzigen prüfbaren Beweis verdichtete.[138] Die Post-Quantum-Sicherheit beruhte dabei allein auf der Härte der Hashfunktion. Die Beam Chain wäre formal verifiziert und ihre Korrektheit mathematisch bewiesen. Wo die Finalität berührt wird, steht eine Drei-Slot-Finalität von rund 36 Sekunden als Zielzustand, der die heutige Finalität nach mehreren Minuten ablöste, mit Verweis auf Abschnitt 5.5 für die Mechanik. Methodisch bleibt die Beam Chain ein Forschungsgegenstand ohne Fork-Termin. Sie hängt von bereits deployten Voraussetzungen ab, unter denen die mit Pectra eingeführte höhere maximale Effective Balance (MaxEB) die hash-basierte Aggregation erleichtert.[139]

leanVM auf der Ausführungsumgebung und Beam Chain auf der Consensus-Schicht teilten die gleichen drei Eigenschaften, hash-basierte Primitiven, formale Verifizierbarkeit und konstruktive Post-Quantum-Resistenz. Die Lean-Ethereum-Designphilosophie nähme auf beiden Schichten als integrale Konsequenz die gleiche Gestalt an, deren Execution-Substanz Abschnitt 5.2-E entfaltet und deren operative Konsens-Migration Abschnitt 5.5 beschreibt. Der hier gezeigte Endzustand ist ein Designzustand und gilt unter denselben Bedingungen für beide Schichten.

Die Designphilosophie benennt die Richtung der Roadmap und setzt dafür keine Termine. leanVM und Beam Chain liegen jenseits des Horizonts von 2029, ohne in finaler Form spezifiziert zu sein. Konkrete Forschungsarbeiten und ein EF-interner Konsens tragen sie, der die Bauteile benennt, ohne ihre endgültige Verzahnung schon festzulegen. Die Verzahnung mit der RISC-V-Linie bleibt in

[138] Beam Chain: Justin Drake, Beam Chain (Devcon SEA 2024), ethresear.ch-Follow-ups; Vitalik Buterin, Post-Quantum-Roadmap (Februar 2026).

[139] leanXMSS-Linie, Beam Chain als RES, MaxEB (EIP-7251, DEPL, Pectra).

den Primärquellen offen und wird die kommenden Spezifikationsrunden beschäftigen. Ob die Designphilosophie trägt, entscheidet sich über die Protokollarchitektur hinaus an den operativen Bedingungen ihrer Implementierung, an Governance, Client-Diversität und Privacy, die der folgende Abschnitt entwickelt.

5.1-C Die operative Erwartung

Die operative Ebene ist der Ort, an dem ein technisch stimmiges Protokoll-Design noch scheitern kann, weil ein Ökosystem es über Jahre tragen, pflegen und gegen Erosion verteidigen muss. Ein korrekt spezifiziertes Protokoll zerfiele, wenn die Client-Basis monokulturell würde, die Weiterentwicklung am Engagement einzelner Personen hinge oder eine angekündigte Eigenschaft nie den Weg ins Protokoll fände. Allen drei Bedingungen, die der vorliegende Abschnitt entwickelt, ist gemeinsam, dass das Design sie voraussetzt, ohne sie selbst garantieren zu können. Die erste ist eine planbare Governance, die zweite eine aktiv gepflegte Client-Diversität, die dritte eine Privacy, die vom Ausnahmefall zum Default wird. Die letzte dieser Bedingungen zeigt zugleich, wo das Bewertungsrahmen an eine eigene Grenze stößt.

Planbare Governance

Das Governance-Zielbild ist eine planbare, institutionalisierte Protokoll-Entwicklung, die als verstetigter Prozess unabhängig von der jeweiligen Führung liefe. Ihr sichtbarster Anker ist die angestrebte Sechsmonats-Fork-Kadenz, zwei Hard Forks pro Jahr in einem Rhythmus, auf den das Ökosystem sich Jahre im Voraus einstellt und der bis 2029 reicht.[140] Für ein Infrastruktursystem zählt weniger die Geschwindigkeit der Änderung als ihre Vorhersehbarkeit, weil abhängige Systeme ihre eigene Entwicklung an den bekannten Fork-Fenstern festmachen. Der Rhythmus legt die Termine fest, ohne die Inhalte zu fixieren, weshalb sich der Takt halten lässt, auch wenn einzelne Features in einen späteren Fork rücken. Erst die Verstetigung über mehrere Jahre macht aus einem Releaseplan eine institutionelle Erwartung, die nicht mehr von der Tagesform einzelner Akteure abhängt.

Was die Entwicklung gegen den Wechsel einzelner Personen robust macht, ist die Verankerung in einem dokumentierten Prozess, der jeden Vorschlag unabhängig von seinem Urheber durch die gleichen Stufen führt. Ein benannter tech-

[140] Zur Fork-Kadenz Strawmap (Justin Drake, Februar 2026), zwei Hard Forks pro Jahr im Sechsmonats-Rhythmus bis 2029.

nischer Ansprechpartner begleitet einen Vorschlag von der Einreichung bis zur möglichen Aufnahme in einen Fork. Pro Upgrade und Layer wählt der Prozess ein Headliner-Feature, während die übrigen Vorschläge bis zu einer Frist gesammelt und als Batch bewertet werden.[141]

Der Stand jedes Vorschlags ist öffentlich nachvollziehbar in gestaffelten Stufen von der ersten Erwägung bis zur festen Einplanung, was die Koordination von der internen Kenntnis einzelner Beteiligter löst. Für ein System, auf dem andere aufbauen, ist eine lesbare Pipeline selbst eine Leistung, weil abhängige Teams den Reifegrad einer geplanten Änderung einschätzen können, ohne an internen Gesprächen teilzunehmen. Der Prozess macht den Fortgang eines Vorschlags damit von seinem dokumentierten Stand abhängig und nicht von der Aufmerksamkeit einer bestimmten Leitung. Ein Wechsel an der Spitze unterbricht den Takt deshalb nicht. Die Reorganisation der Protokollarbeit in drei Tracks im Februar 2026 richtete den Prozess an wenigen klaren Prioritäten aus, statt ihn an einer wachsenden Featureliste zu orientieren. Als zweiter Beleg planbarer Langfrist-Koordination tritt die Strawmap hinzu, die über die einzelne fork-weise Abstimmung hinausreicht.[142]

Gepflegte Client-Diversität

Client-Diversität bleibt eine aktiv gepflegte Eigenschaft des Ökosystems und kein Selbstläufer, weil die Marktdynamik zu einer Standardimplementierung drängt, deren Verbreitung das Netzwerk an einen einzelnen Code bindet. Die Pflege verlangt fortlaufende Anreize für Minderheits-Clients, weil die bequeme Wahl der verbreitetsten Implementierung die Konzentration sonst von selbst verstärkt. Das Zielbild wäre eine Verteilung der Execution- und Consensus-Layer-Clients, in der keine einzelne Implementierung die 33-Prozent-Schwelle überschritte. Oberhalb der Schwelle könnte ein Bug in einem einzigen Client die Finalität des Netzwerks gefährden. Unterhalb der Schwelle fängt die Diversität der übrigen Clients den Fehler eines einzelnen auf, sodass ein Implementierungsfehler lokal bleibt und nicht zum Konsensausfall des gesamten Netzwerks eskaliert.[143] Als langfristige Vereinfachung träte die leanVM-Harmonisierung hinzu,

[141] Zu den institutionellen Trägern EF, „Protocol Priorities Update for 2026" (18. Februar 2026), das eine planbare Lieferung als Anspruch benennt. Der Fork-Prozess wählt pro Upgrade und Layer einen Headliner und bewertet die übrigen Vorschläge als Batch im All-Core-Developers-Prozess mit Statusführung über Forkcast. Das Protocol Support Team stellt mit dem EIP-Champions-Handbuch einen dokumentierten Pfad für jeden Vorschlag bereit (EF-Blog, Checkpoint April 2026).

[142] Strawmap (Februar 2026) hier in ihrer Governance-Funktion als abgestimmte Mehrjahres-Planung über die fork-weise Abstimmung hinaus. Die North-Star-Quelle erscheint in 5.1-A.

[143] Zur 33-Prozent-Schwelle und zur Staking-Konzentration gilt, dass der größte LST-Anbieter im Zielzustand bei rund 23 Prozent verbliebe und kein einzelner Client die Blocking-Minority-Schwelle überschreiten sollte. Die

die Client-Übereinstimmung aus einer formalen Spezifikation ableiten würde, deren drei Dimensionen Abschnitt 5.2-E entfaltet.[144]

Privacy als Grenze und Zielbild

Das Zwölf-Kriterien-Rahmen der Arbeit erfasst die Privacy nicht und markiert damit eine Grenze des Bewertungsinstruments selbst, deren Reflexion Abschnitt 6.3 trägt. Die Grenze entsteht daraus, dass die zwölf Kriterien deduktiv aus einem Infrastrukturbegriff entfaltet wurden, der Vertraulichkeit nicht als konstitutiv führte, und dass die Verifikation an Systemen ohne eigenen Vertraulichkeitsanspruch keinen Anlass zur Korrektur bot. Das Instrument kann die Transparenz des heutigen Zustands beschreiben, hält aber kein Kriterium bereit, das eine Bewegung zur Vertraulichkeit als Fortschritt oder Rückschritt registrierte. Selbst ein protokollnativer Shielded Pool löste die Ende-zu-Ende-Privacy nicht allein, weil die Verschlüsselung des Mempools, die Anonymität auf der Netzwerkebene und die Gestaltung der Wallet-UX außerhalb des Protokolls liegen.[145] Protokoll-Privacy wäre eine notwendige Grundlage, ohne für sich genommen die Vertraulichkeit der gesamten Interaktion zu sichern.

Als Zielbild im Horizont jenseits eines Jahrzehnts würde Privacy-by-Default die heutige Ordnung umkehren. Gegenwärtig sind alle Transfers öffentlich, und Vertraulichkeit ist Sache einzelner Anwendungen und der Rollups. Das Protokoll stellt sie nicht bereit. Wer heute Vertraulichkeit sucht, muss sie aktiv herstellen und wird schon durch den Wechsel in einen geschützten Pfad sichtbar, während ein Default diese Last auf die Offenlegung verschöbe. Solange Vertraulichkeit auf einzelne Anwendungen verteilt bleibt, zerfällt sie in kleine und schwache Anonymitätsmengen, in denen sich die Teilnehmer kaum verbergen. Der Strawmap-North-Star Private L1 setzte native shielded ETH Transfers ins Protokoll und verstünde Vertraulichkeit als Default des Protokolls.[146] Der Horizont reicht über die North-Star-Marke um 2028 hinaus, bis Privacy als architektonische Eigenschaft der Infrastruktur gälte und über die heutige Bindung an einzelne Anwendungen hinauswüchse. Vertraulichkeit ist dann eine verlässliche Grundeigenschaft, auf der jede Anwendung aufsetzt, statt ein Zusatzdienst ein-

Stateless Clients tragen den Status RES, die Validator-Konsolidierung erfolgt über MaxEB (EIP-7251, DEPL).

[144] leanVM als Zielzustand der Ausführungsumgebung (RES, Horizont jenseits 2029). Die drei leanVM-Dimensionen und die formale Spezifikation entfaltet 5.2-E.

[145] Zur Pre-Inclusion-Privacy als eigene Schicht neben dem Shielded Pool Encrypted Mempool (EIP-8105/LUCID, RES) als Beleg, dass Protokoll-Privacy die Ende-zu-Ende-Privacy nicht allein löst. Die Reflexion des Bewertungsrahmens trägt Abschnitt 6.3.

[146] Strawmap-North-Star Private L1 (Februar 2026), native shielded ETH Transfers auf Protokollebene, Privacy als Default statt als Opt-in (RES).

zelner Anbieter zu bleiben.

EIP-8182 konkretisiert die Richtung mit einem protokollverwalteten Shielded Pool und einer ZK-Verifikation als Protokoll-Feature, sodass private Transfers an jede gewöhnliche Adresse möglich würden, ohne ein eigenes Privacy-Adressformat zu verlangen.[147] Der Pool läge als System-Contract an fester Adresse, ohne privilegierten Schlüssel und ohne Anhaltemechanismus, sodass keine Instanz die Vertraulichkeit nachträglich aufheben oder den Verkehr unterbrechen könnte. Der Kern liegt im vereinheitlichten Anonymitäts-Set, weil jede integrierende Wallet denselben gemeinsamen Pool speiste und die Anonymität damit aus einem einzigen Pool entstünde. Mit jeder Wallet, die den gemeinsamen Pool nutzt, wächst die Anonymitätsmenge, sodass die Vertraulichkeit mit der Verbreitung der Integration zunimmt. Der Vorschlag ist für Hegotá eingebracht und befindet sich im Status eines Entwurfs in der PFI-Review, der Proposed-for-Inclusion-Stufe des ACD-Prozesses, deren Aufnahme nicht gesichert ist. Buterins Aufruf von 2025 nach einer nativen Shielded-Balance, aus der der Versand standardmäßig erfolgt, trägt die Logik eines solchen Defaults.[148] Beide ruhen auf kurvenbasierter ZK-Kryptographie und gehören damit in einen anderen Horizont als der hash-basierte Post-Quantum-Endzustand, den der vorige Abschnitt umrissen hat.

Die folgenden Abschnitte prüfen die einzelnen Richtungen des Zielzustands der Reihe nach. Abschnitt 5.2 behandelt die Skalierung der Execution, 5.3 die Verifikation und den Zugang, 5.4 das State-Management, 5.5 die Neutralität und 5.6 die Architektur der Layer 2. Jeder Abschnitt nimmt eine der Richtungen auf, die der Rahmen benannt hat, und prüft, wie weit das Design sie im Zielzustand trägt.

5.2 Execution-Skalierung

[147] EIP-8182 „Private ETH and ERC-20 Transfers“ (Tom Lehman, Mai 2026), protokollverwalteter Shielded Pool mit ZK-Verifikation, für Hegotá eingebracht und in der PFI-Review, Aufnahme nicht gesichert. Die Verifikation ist kurvenbasiert (Groth16 über BN254) und nicht post-quantum.

[148] Vitalik Buterin, Aufruf zu nativer Wallet-Privacy mit standardmäßig aktivem Versand aus dem geschützten Guthaben (April 2025).

5.2-A Die Abhängigkeitskette: Parallelisierung, Entkopplung, Konvergenz

Jede Kapazitätserhöhung jenseits von 100 Millionen Gas erzwingt eine Entscheidung, die das heutige Protokoll nicht anbietet: höherer Durchsatz oder breitere Verifikationsbasis. Bei 60 Millionen Gas verarbeitet Ethereum zwischen 15 und 30 Transaktionen pro Sekunde, abhängig von der Transaktionskomplexität.[149] Für eine Infrastruktur, die Finanzsysteme, Lieferketten und institutionelle Settlements tragen soll, ist das eine strukturelle Begrenzung: Visa verarbeitet im Durchschnitt über 8.000 Transaktionen pro Sekunde, bei einer getesteten Spitzenkapazität von 65.000 TPS.[150]

Der Vergleich über Transaktionsanzahlen unterschätzt allerdings die Leistungsklasse, in der Ethereum bereits operiert. Eine einzige Ethereum-Transaktion kann Werte von mehreren hundert Millionen US-Dollar mit programmierbarer Finalität settlen und verbraucht dabei dieselben 21.000 Gas wie ein Transfer von 0,01 ETH. In der für institutionelles Settlement relevanten Dimension des Wertdurchsatzes pro Zeiteinheit bewegt sich Ethereum L1 bereits in der Größenordnung globaler Zahlungsinfrastruktur.[151] Die strukturelle Begrenzung betrifft damit die Zahl gleichzeitiger Operationen, die L1 tragen kann, und die Breite der Anwendungsfälle jenseits hochvolumiger Einzeltransaktionen.

Der exponentielle Skalierungspfad, den EIP-9698 als Zielmarke formuliert, soll diese Begrenzung aufheben, indem er die L1-Kapazität über vier Jahre um den Faktor 100 steigert (Verzehnfachung alle zwei Jahre über zwei Zyklen).[152] Eine solche Steigerung würde Ethereum aus der Nische spezialisierter Krypto-Anwendungen in die Reichweite globaler Infrastrukturlasten bringen, voraus-

[149] Bei einem Gas Limit von 60M verarbeitet Ethereum je nach Transaktionskomplexität 15–30 TPS. Einfache ETH-Transfers verbrauchen 21.000 Gas (rund 2.800 TPS theoretisch), komplexe DeFi-Transaktionen 200.000–500.000 Gas (rund 12–30 TPS effektiv).

[150] Visa: 257,5 Milliarden processed transactions im Fiskaljahr 2025 (Visa Q4 2025 Earnings Release, endend 30. September 2025), entsprechend einem Durchschnitt von circa 8.165 TPS. Die häufig zitierten 65.000 TPS beziehen sich auf die getestete VisaNet-Netzkapazität, nicht auf den realen Spitzenwert. Der Vergleich dient der Größenordnung; Visa und Ethereum sind architektonisch nicht direkt vergleichbar.

[151] Stablecoin-Transfervolumen auf Ethereum: über 8 Billionen US-Dollar im vierten Quartal 2025 (Token Terminal, Januar 2026). Der Bot-Anteil von circa 70 Prozent umfasst Arbitrage, Paymaster-Transaktionen und andere automatisierte Transfers über alle Chains; der Ethereum-spezifische Anteil kann davon abweichen (CEX.io, Stablecoin Report Q3 2025). Die Brutto-Zahl enthält keine nativen ETH-Transfers und DeFi-Settlements. Visa im Fiskaljahr 2025: 17 Billionen US-Dollar bei 329 Milliarden Transaktionen (Visa Annual Report, endend September 2025). Die Zahl weicht von den 257,5 Milliarden in der vorigen Note ab, weil beide Berichte unterschiedliche Transaktionsbegriffe führen. Die Metriken sind methodisch nicht direkt kommensurabel, weil Ethereum Wertbewegungen zwischen Adressen misst, während Visa Kauftransaktionen erfasst.

[152] EIP-9698 (Draft, Autor: Dankrad Feist, April 2025) formuliert einen exponentiellen Gas-Limit-Pfad mit dem Ziel einer 100-fachen Kapazitätssteigerung über vier Jahre (Verzehnfachung alle 164.250 Epochen, zwei Zyklen, G0 = 50M ab Epoch 369017 / circa 1. Juni 2025, Endwert circa 5 Milliarden Gas). Der EIP ändert keine Konsensregeln, sondern nur das Voting-Default-Verhalten der Clients; er ist backward-kompatibel.

gesetzt, die Dezentralisierung der Verifikation bleibt gewahrt. Genau hier liegt die Spannung: Drei Features müssen den Trade-off zwischen Kapazität und Dezentralisierung architektonisch aufbrechen, bevor die Erweiterung sicher voranschreiten kann. Sie setzen an unterschiedlichen Engpässen an, bilden jedoch eine gerichtete Abhängigkeitskette, deren gemeinsame infrastrukturelle Voraussetzung Enshrined Proposer-Builder Separation ist.

Parallelisierung als Gatekeeper

Die sequentielle Verifikation aller Transaktionen durch jeden Node wird bei steigendem Gas Limit zum zeitlichen Engpass. Im heutigen Modell prüft ein Validator jede Transaktion nacheinander, wobei die Reihenfolge zwingend ist, solange der Node nicht feststellen kann, welche Transaktionen um dieselben Storage Slots konkurrieren. Bei einem Gas Limit unter 100 Millionen bleibt die Verifikationszeit innerhalb des 12-Sekunden-Slots handhabbar.[153] Bei höheren Werten wächst sie linear, bis der Slot nicht mehr ausreicht. Block Access Lists (EIP-7928, SFI Glamsterdam, also Scheduled for Inclusion) lösen dieses Zeitproblem durch ein neues Feld im Block Header: Der Builder deklariert bei der Block-Konstruktion sämtliche State-Zugriffe jeder Transaktion, einschließlich der Post-Execution-Werte.[154] Empfangende Nodes können daraufhin Festplattenzugriffe und Transaktionsvalidierung parallelisieren, weil die Abhängigkeiten zwischen Transaktionen vorab bekannt sind.[155] Der zusätzliche Datenaufwand bleibt mit durchschnittlich 70 KiB pro Block bei einem Gas Limit von 60 Millionen unterhalb der maximalen Calldata-Größe und belastet das Protokoll nicht durch ein neues Datenproblem.[156]

BALs sind damit keine Optimierung, sondern der Gatekeeper der gesamten L1-Execution-Skalierung. Ohne sie kann das Gas Limit nicht sicher über 100 bis 150 Millionen angehoben werden, weil die sequentielle Verifikationszeit den Slot sprengen würde. Der Governance-Status untermauert die Realisierbarkeit: SFI für Glamsterdam, drei Client-Teams (Besu, Geth, Nethermind) mit laufenden Prototyp-Implementierungen.[154] Die Parallelisierung löst jedoch ausschließlich das Zeitproblem auf der Verifikationsseite. Das Kostenproblem

[153] Bei einem Gas Limit von 36M beträgt die durchschnittliche Validierungszeit ca. 400ms. Bei 60M steigt sie auf ca. 1–2 Sekunden. Ab circa 100M nähert sich die Validierungszeit der Slot-Grenze, bei der neue Voraussetzungen (BALs, ePBS) erforderlich werden. Quelle: EF Research, Execution Layer Performance Benchmarks, 2025.

[154] EIP-7928. Autoren: Toni Wahrstätter, Dankrad Feist, Francesco D'Amato, Jochem Brouwer, Ignacio Hagopian. Status: Draft seit März 2025, SFI für Glamsterdam. Prototyp-Implementierungen: Besu, Geth, Nethermind.

[155] BALs ermöglichen neben parallelen Disk Reads und Transaction Validation auch parallele State Root Computation sowie Executionless State Updates in ePBS-Kontexten.

[156] Die durchschnittliche BAL-Größe beträgt ca. 35 KiB pro Block bei 36M Gas und ca. 70 KiB bei 60M Gas (EIP-7928, Overhead Analysis). Im Worst Case bleibt sie unterhalb der maximalen Calldata-Größe.

bleibt bestehen: Jeder Node vollzieht trotz paralleler Abarbeitung weiterhin jede Transaktion vollständig nach. Die Hardware-Anforderungen an die Validatoren wachsen mit dem Gas Limit linear mit, und diese lineare Kopplung hat keine Obergrenze. Ab einem bestimmten Schwellenwert werden die Anforderungen so hoch, dass nur noch professionell betriebene Nodes mithalten können, was die Verifikationsbasis aushöhlt. Genau diese Erosion muss ein zweiter Mechanismus verhindern. BALs entfalten dabei eine zweite Wirkung, die über die Validator-Seite hinausgeht: Der Abhängigkeitsgraph, den sie bereitstellen, ist zugleich die Voraussetzung für parallele Witness-Generierung in der zkEVM-Proving-Pipeline.[157] Da 60 bis 80 Prozent der Transaktionen in einem Block disjunkte Storage Slots nutzen, können Prover die Ausführung über unabhängige Transaktionscluster parallelisieren und die Proof-Generierung auf mehrere Maschinen verteilen.[155] Ohne den vorab bekannten Abhängigkeitsgraphen bliebe die serielle Witness-Erzeugung die Engstelle, die die zkEVM-Skalierung bei hohen Gas Limits begrenzt.

Entkopplung durch kryptographische Verifikation

Die lineare Kopplung zwischen Kapazität und Hardware-Anforderungen lässt sich quantifizieren. Bei einem Gas Limit von 60 Millionen benötigt die vollständige Verifikation eines Blocks ein bis zwei Sekunden.[158] Bei 600 Millionen wären es zehn bis zwanzig Sekunden bei sequentieller Verarbeitung. Selbst mit der durch BALs ermöglichten Parallelisierung erreicht die Verifikationszeit in diesem Bereich die Grenze des 12-Sekunden-Slots. Bei 5.000 Millionen, dem projizierten Endpunkt des EIP-9698-Pfads, wäre die Verifikation innerhalb eines 12-Sekunden-Slots unmöglich.[159] Die Konsequenz ist eindeutig: Jede Erhöhung der Netzwerkkapazität steigert zugleich die Mindestanforderungen an die Hardware der Validatoren. Das steht in direktem Konflikt mit dem Dezentralisierungsziel, weil die Teilnahme an der Verifikation mit jeder Kapazitätsstufe teurer wird. Die zkEVM (EIP-8025, aktive EF-Roadmap seit Januar 2026) bricht diese Kopplung,

[157] In einem ZK-Kontext ist der Latenz-Engpass häufig die serielle Ausführung zur Witness-Generierung. BALs liefern den deterministischen Dependency Graph, der parallele Execution und Sharding der Proof-Generierung ermöglicht. Vgl. HackMD, „A Deep Dive into EIP-7928 and Block-Level Access Lists“, Januar 2026.

[158] Validierungszeiten: 60M Gas ≈ 1–2s, 600M ≈ 10–20s. Bei 5.000M wäre die Validierung innerhalb eines 12-Sekunden-Slots nicht mehr möglich. EF Research, L1-zkEVM Roadmap, 26.01.2026.

[159] EIP-9698 (Draft, Autor: Dankrad Feist, April 2025) projiziert eine Verzehnfachung alle 164.250 Epochen (ca. zwei Jahre) über zwei Zyklen, also eine Gesamtsteigerung um Faktor 100 innerhalb von vier Jahren, beginnend bei G0 = 50M ab Epoch 369017 (circa 1. Juni 2025). Projizierter Pfad: 50M (Juni 2025) → circa 500M (Mitte 2027) → circa 5.000M (Mitte 2029). Der EIP ändert keine Konsensregeln, sondern nur das Voting-Default-Verhalten der Clients; er ist backward-kompatibel. Die Projektion beschreibt den maximal möglichen Pfad bei kontinuierlichem Validator-Voting, nicht den operativ erwarteten Verlauf.

indem sie die Art der Verifikation grundlegend verändert.[160]

Der Paradigmenwechsel besteht darin, die universelle Re-Execution durch kryptographische Proof-Verifikation zu ersetzen. Statt dass jeder Validator jede Transaktion nachrechnet, erzeugt ein spezialisierter Prover einen Zero-Knowledge-Proof, der die korrekte Ausführung aller Transaktionen mathematisch beweist.[160] Der Prover ist dabei eine eigenständige Rolle, die das EIP-8025-Design von Proposer und Builder trennt: Der Proposer schlägt den Block vor, der Builder konstruiert ihn, und der Prover liefert den kryptographischen Beweis der korrekten Ausführung. Validatoren verifizieren den Proof in Millisekunden, unabhängig davon, wie viele Transaktionen der Block enthält. Ein Block mit 60 Millionen Gas und ein Block mit 5.000 Millionen Gas erzeugen für den Verifizierer denselben Aufwand. Das entscheidende Designprinzip ist die Optionalität: Nodes können jederzeit auf vollständige Re-Execution zurückfallen, wenn sie dem Proof nicht vertrauen.[161] Die Proving-Latenz sank zwischen Juli und Dezember 2025 von 16 Minuten auf 16 Sekunden, bei einer 45-fachen Kostenreduktion.[162] Diese Schwelle hat architektonische Bedeutung: Erstmals wird es realistisch, einen Block innerhalb eines einzigen Slots zu beweisen, sodass ein Validator auf handelsüblicher Hardware einen Block verifiziert, ohne ihn selbst auszuführen. Das ändert die Verifikationsarchitektur des Netzwerks.

Die Sicherheitsfrage als offene Reibungsstelle

Die Proving-Geschwindigkeit ist gelöst. Die mathematische Absicherung steht aus. Schnelle Proving-Zeiten beruhen auf STARK-basierten Beweisverfahren, die sich auf unbewiesene kryptographische Annahmen stützen, vor allem zur Kollisionsresistenz bestimmter Hash-Funktionen und zur Sicherheit der Fiat-Shamir-Transformation, die interaktive Beweissysteme in nicht-interaktive umwandelt.[163] Arbeiten aus dem Umfeld der EF-Forschungsgruppe und unabhängiger Kryptographen haben im Laufe des Jahres 2025 begonnen, einzelne dieser Annahmen formal zu hinterfragen.[163] Sollten sie fallen, wären die betroffenen

[160] EIP-8025. Autoren: Alex Stokes, Justin Drake, Ethereum Foundation Research. Paradigma: Optional Execution Proofs. Die EF publizierte am 26. Januar 2026 eine Implementation Roadmap mit sechs Sub-Themes.

[161] Die Optionalität erfordert keinen Hard Fork und ist rückwärtskompatibel. EIP-8025 definiert einen neuartigen Governance-Status: protokollseitig integriert, aber ohne Erzwingung der Nutzung.

[162] EF Blog, 18.12.2025: Performance-Sprint abgeschlossen. Proving-Latenz von 16 Minuten auf 16 Sekunden, 45-fache Kostenreduktion. Zielmarke: 99 Prozent aller Mainnet-Blöcke in unter 10 Sekunden beweisbar, auf Hardware im Bereich von 100.000 US-Dollar, vollständig Open-Source, bei 128-bit Security.

[163] STARK-basierte Proof-Systeme stützen sich u.a. auf Conjectures zur Kollisionsresistenz spezifischer Hash-Funktionen und zur Sicherheit der Fiat-Shamir-Heuristik. Im Laufe des Jahres 2025 haben sowohl EF-interne Arbeiten als auch unabhängige kryptographische Forschungsgruppen begonnen, die formale Belastbarkeit dieser Annahmen systematisch zu untersuchen. Quelle: EF zkEVM Team, L1-zkEVM Roadmap, 26.01.2026.

Proof-Systeme mathematisch ungesichert, und die 128-Bit-Sicherheit, die das Protokoll als Ziel setzt, wäre mit den aktuellen Verfahren nicht erreichbar. Die Ethereum Foundation reagiert mit gestuften Meilensteinen: beweisbare 100-Bit-Sicherheit bis Glamsterdam, 128 Bit bis Ende 2026.[164]

Für den Skalierungspfad folgt daraus zweierlei. Sollten die Proving-Zeiten bei mathematisch abgesicherter Security um den Faktor drei bis fünf steigen, verschiebt sich die Entkopplung zeitlich nach hinten. Single-Slot-Proving wäre dann erst mit der nächsten Generation von Proving-Hardware oder optimierten Proof-Systemen erreichbar, was den vollständigen Skalierungspfad um ein bis zwei Jahre verzögern könnte. Die Sicherheit des Netzwerks ist davon nicht betroffen, weil die Optionalität als Rückfallebene greift: Solange die kryptographische Absicherung aussteht, verifizieren Nodes durch vollständige Re-Execution. Die Frage der unbewiesenen Annahmen ist damit ein Zeitplan-Risiko für die Entkopplung.

Eine zweite Absicherungsschicht reduziert das verbleibende Risiko weiter. Das vorgeschlagene 3-of-5-Threshold-Modell sieht vor, dass fünf unabhängige Client-Implementierungen jeweils eigene Proofs generieren. Ein Block gilt als valide, wenn drei davon verifiziert sind.[165] Ein kryptographischer Fehler in einem einzelnen Proof-System kompromittiert das Netzwerk nicht, solange die übrigen Implementierungen intakt bleiben. Client Diversity, die im IST-Zustand eine Best Practice ohne protokolläre Erzwingung darstellt, wird durch dieses Modell zu einer kryptographischen Sicherheitsgarantie.

Warum das Building spezialisiert bleibt

Die zkEVM entkoppelt die Verifikation vom Gas Limit. Der State bleibt an die Kapazität gebunden. Block Builder müssen den vollständigen State weiterhin vorhalten, der mit steigender Kapazität wächst.[166] Die Architektur trennt damit bewusst drei Rollen. Verifikation wird demokratisiert, weil die Proof-Verifikation unabhängig von der Blockgröße ist und auf ressourcenschwacher Hardware funktioniert. Building bleibt die Rolle spezialisierter Betreiber, weil ein Block-

[164] EF-Meilensteine: 100-bit provable Security bis Glamsterdam (Ziel Q2 2026, laut EF Checkpoint #9 von April 2026 jedoch erst in der zweiten Jahreshälfte 2026 erwartet), 128-bit bis Ende 2026. Quelle: EF Blog, „Shipping an L1 zkEVM #2: The Security Foundations", 18. Dezember 2025.

[165] 3-of-5-Threshold-Mechanik: Attesters akzeptieren einen Block als valide, wenn drei von fünf unabhängigen Proofs verschiedener Client-Implementierungen verifiziert sind. EF zkEVM Team, 2026.

[166] Die zkEVM verschiebt den Dezentralisierungsengpass von „Execution Layer Client betreiben" zu „vollständigen State vorhalten." Die Soundness der zkEVM ist kryptographisch durch die ZK-Proof-Verifikation garantiert; das 1-of-N-Modell in EIP-8025 bezieht sich auf die Liveness: Ein einziger ehrlicher Prover genügt, damit die Proving-Pipeline nicht stillsteht. Die ökonomische Absicherung dieses Mindestbetriebs, also die Anreize für eine tragfähige Anzahl aktiver Prover, bleibt als Koordinationsaufgabe offen.

Builder den vollständigen State (Stand Q1 2026 rund 430 GiB) im schnellen Zugriff halten muss und diese Last mit jeder Gas-Limit-Erhöhung wächst. Proving etabliert sich als dritte Rolle auf einer eigenen Hardware-Basis: spezialisierte GPU-Cluster mit hoher Energielast, ohne State-Vorhalten, mit eigenen Marktbedingungen und Konzentrationsrisiken.[167] Abschnitt 5.3 führt beide Dimensionen aus: Stateless Clients zeigen die Demokratisierung der Verifikation. Die kryptographische Infrastruktur-Ebene behandelt dort die Hardware- und Marktbedingungen der Prover-Rolle.

ePBS als Konvergenzpunkt

Die zkEVM löst das Kostenproblem der Verifikation, erzeugt dabei aber eine neue Anforderung: Die Proof-Generierung benötigt Zeit, die das aktuelle Slot-Design nicht hergibt. Ohne strukturelle Änderung verbleibt dem Prover nach Block-Propagation und Attestation ein Fenster von lediglich ein bis zwei Sekunden, was für Real-Time-Proving bei praxisrelevanten Gas Limits nicht ausreicht.[168] Enshrined Proposer-Builder Separation (EIP-7732) löst diesen Engpass durch eine Reorganisation des Slot-Ablaufs.[169] ePBS trennt die Block-Verifikation in zwei Phasen: Consensus-Verifikation in Slot N und Execution-Verifikation in Slot N+1. Dadurch entsteht ein Proving-Fenster von sechs bis neun Sekunden, in dem der Prover den kryptographischen Beweis fertigstellen kann, bevor die Attestation des Folge-Slots beginnt.

Dieselbe Trennung von Proposer und Builder ist zugleich die Voraussetzung für BALs. Der Builder erstellt die Block Access List parallel zur Proposer-Selektion. Ohne die protokollseitige Formalisierung dieser Rollentrennung ist der Ablauf nicht sicher implementierbar.[170] Zwei Features mit grundsätzlich verschiedenen Funktionen, Parallelisierung bei BALs und Entkopplung bei der zkEVM, münden in denselben infrastrukturellen Mechanismus. Diese Konvergenz ist eine Konsequenz des Architekturwechsels: Sobald das Protokoll Block-Konstruktion und Block-Verifikation formal trennt, werden beide Skalierungspfade gleichzeitig möglich.

Das Nadelöhr ist governance-seitig geklärt. ePBS hat den Status SFI für Glamsterdam, alle fünf Consensus-Layer-Clients befinden sich in aktiver Ent-

[167] EF Blog, 18.12.2025: Zielmarke für Proving-Hardware im Bereich circa 100.000 US-Dollar (vgl. Fußnote 32).

[168] Ohne ePBS beträgt das Proving Window ca. 1–2 Sekunden. ePBS erweitert es durch Block Pipelining auf 6–9 Sekunden. Vgl. EIP-8025 / EF L1-zkEVM Roadmap, 26.01.2026.

[169] EIP-7732 (Enshrined PBS). Status: SFI Glamsterdam (Aktivierung 2026, Q3/Q4 realistischer als H1 nach EF Checkpoint 9, April 2026). CL-Headliner seit August 2025.

[170] BALs erfordern ePBS für Block Pipelining; die zkEVM erfordert ePBS für das Proving Window (Slot N+1). Beide Abhängigkeiten sind in der EF-Roadmap dokumentiert.

wicklung, das erste generalisierte Devnet wurde im April 2026 gestartet.[171] ePBS entfaltet über die hier beschriebene Kapazitätsfunktion hinaus eine zweite Wirkung: die Beseitigung des Relay-Chokepoints und ihre Konsequenzen für die Zensurresistenz. Abschnitt 5.5 behandelt sie.

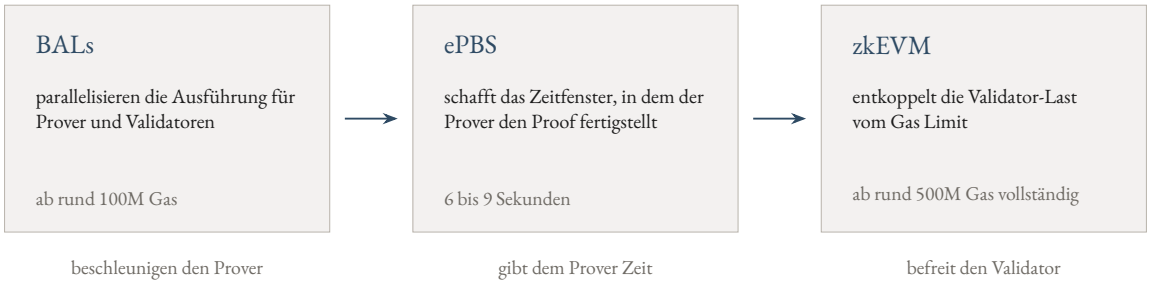


Abbildung 5.2-A.1 Die Abhängigkeitskette der L1-Execution-Skalierung. BALs parallelisieren die Ausführung für Prover und Validatoren (ab rund 100M Gas). ePBS schafft das Zeitfenster, in dem der Prover den Proof fertigstellen kann (6–9 Sekunden). Die zkEVM entkoppelt die Validator-Last vom Gas Limit (ab rund 500M Gas vollständig). Die Kette ist gerichtet: BALs beschleunigen den Prover → ePBS gibt dem Prover Zeit → zkEVM befreit den Validator. Gestaffelte Gas-Schwellen: <100M (Validator-Voting), 100–150M (BALs + ePBS), 150–500M (Gas Repricings), 500–1.000M (zkEVM), >1.000M (offene Voraussetzungen Proving-Ökonomie und State).

Das Zusammenspiel der drei Features

Die drei Features bilden eine gerichtete Abhängigkeitskette, in der jedes Glied das nächste ermöglicht. BALs liefern den Dependency Graph, der parallele Witness-Generierung und verteiltes Proving erst ermöglicht. ePBS reorganisiert den Slot-Ablauf so, dass der Prover das resultierende Zeitfenster von sechs bis neun Sekunden nutzen kann. Die zkEVM überführt das Ergebnis dieser Kette in eine konstante Verifikationszeit für Validatoren, unabhängig vom Gas Limit. Entfällt eines der drei Glieder, bricht die Skalierung an einer anderen Stelle: Ohne BALs wird die Proof-Erzeugung zur Engstelle, ohne ePBS fehlt dem Prover das Zeitfenster, ohne zkEVM wächst die Validator-Last linear mit der Kapazität.[172]

Der Governance-Status staffelt die Implementierung entlang dieser Kette. BALs und ePBS sind als SFI-Headliner für Glamsterdam bestätigt und schaffen die infrastrukturelle Grundlage, auf der die zkEVM aufsetzen kann. Die zkEVM selbst folgt einer aktiven EF-Roadmap mit gestuften Sicherheitsmeilensteinen, deren vollständige Umsetzung die kryptographische Absicherung zur Voraussetzung hat. Die vollständige hundertfache Skalierung hängt an Voraussetzungen

[171] ePBS-Entwicklungsstand: Prysm (aktive Entwicklung), Lighthouse (Rebasing devnet4), Teku (Tests auf Dev Branch), Lodestar (FOCIL-Prototype auf ePBS Branch), Nimbus (in Progress). epbs-devnet-0 in Vorbereitung.

[172] Zeitliche Staffelung: BALs + ePBS (SFI Glamsterdam, H2 2026) → zkEVM (aktive EF-Roadmap seit Januar 2026, Draft EIP-8025, kein Fork-Termin; gestufte Sicherheitsmeilensteine bis Ende 2026) → Gas Limit >1.000M (abhängig von State-Lösung und weiteren Voraussetzungen).

jenseits der Execution-Skalierung, die in Abschnitt 5.3 und 5.4 behandelt werden. Was die Kette als Ganzes leistet, könnte keines der Features allein erreichen: eine Kapazitätserweiterung, die die Dezentralisierung der Verifikation architektonisch absichert, indem sie die Rollen von Builder, Prover und Validator formal trennt und jeder Rolle die Skalierungsvoraussetzungen zuweist, die ihrer Funktion entsprechen.

5.2-B Der gestaffelte Skalierungspfad

Damit Ethereum die in Kapitel 3 operationalisierten Kriterien der Funktionalen Unersetzbarkeit und Koordinationsfunktion auf der Ebene globaler Infrastruktur einlöst, muss seine L1-Kapazität das heutige Niveau von 15 bis 30 Transaktionen pro Sekunde bei 60 Millionen Gas deutlich überschreiten. Die in 5.2-A dargestellte Rollentrennung ist die architektonische Antwort auf diese Anforderung. Der gestaffelte Skalierungspfad entlang dieser Rollentrennung beginnt jedoch bereits vor ihrer Formalisierung. Das Gas Limit verdoppelte sich von 30 auf 60 Millionen zwischen Februar und November 2025, also in rund zehn Monaten, ohne dass sich das Protokoll ändern musste.[173] Diese Verdopplung zeigt, dass Ethereum seine L1-Kapazität erweitern kann, ohne die Dezentralisierung der Verifikation zu opfern. Die Frage für die Infrastrukturbewertung ist, wie belastbar die Voraussetzungen jeder weiteren Stufe abgesichert sind[174] und welche neuen Engpässe jede Stufe erzeugt. Der Skalierungspfad gliedert sich in fünf Schwellen, wobei jede Schwelle eine spezifische technische Grenze offenlegt, die erst adressiert werden muss, bevor die nächste Stufe erreichbar wird.

---

[173] Gas Limit: 30M (bis Februar 2025) → 36M (Februar 2025) → 45M (Mitte 2025) → 60M (November 2025). Ausgelöst durch Vitalik Buterins öffentliche Befürwortung im November 2024. Kein Consensus Change, kein Fork, keine Protokolländerung; der Fusaka-Hard-Fork (3. Dezember 2025) standardisierte den bereits erreichten 60M-Wert via EIP-7935 als Client-Default. Vgl. EIP-9698 (Informational), Autor: Dankrad Feist. Validator-Voting: dezentraler Abstimmungsprozess, bei dem jeder Block Proposer das Gas Limit um circa 0,1 Prozent anpassen kann; Konsens entsteht durch Konvergenz.

[174] Die in diesem Abschnitt genannten Schwellenwerte (circa 100M, 150–500M, 500–1.000M, >1.000M) sind aus Client-Benchmarks der Execution-Layer-Teams, EF-Kommunikation und öffentlichen Forschungsdokumenten abgeleitete Größenordnungen. Sie markieren Bereiche, in denen spezifische Engpässe bindend werden, und sind keine festen Protokollgrenzen. Die exakten Übergänge können je nach Client-Implementierung und Transaktionsmix variieren.

Der operative Beweis

Die Verdopplung des Gas Limits von 30 auf 60 Millionen (vgl. Abschnitt 5.1-A) erweiterte die L1-Transaktionskapazität um den Faktor zwei.[173] Im Validator-Voting konvergierten die Validatoren innerhalb weniger Monate auf den neuen Zielwert, wobei jeder Block Proposer das Limit um circa 0,1 Prozent pro Block anpassen kann. Der Fusaka-Hard-Fork im Dezember 2025 verankerte zwei flankierende Schutzmaßnahmen. Das Gas Limit Default Target (EIP-7935, DEPL) formalisiert den voreingestellten Zielwert für die Client-Software. Der Transaction Gas Cap (EIP-7825, DEPL) begrenzt den maximalen Gas-Verbrauch einer Einzeltransaktion auf 16,78 Millionen.[175] Blob-Parameter-Optimierungen hoben das Blob-Target schrittweise auf 14 und das Maximum auf 21 an.[176]

Derselbe Mechanismus, der die Verdopplung auf 60 Millionen getragen hat, kann das Limit bis circa 100 Millionen weitertreiben, weil die sequentielle Verifikationszeit in diesem Bereich innerhalb des 12-Sekunden-Slots handhabbar bleibt.[153] Erst oberhalb dieser Schwelle erzwingt die wachsende Verifikationszeit neue protokolläre Voraussetzungen. In der Praxis wirken drei Mechanismen als sequentielle Schwellen, die das Gas Limit an die tatsächliche Protokollreife koppeln. Wenn Blöcke die Verarbeitungskapazität der Validatoren überschreiten, steigen verpasste Attestations und die damit verbundenen Reward-Verluste, ein selbstkorrigierender ökonomischer Anreiz, der das Limit an die operative Realität bindet. Client-Teams und die Ethereum Foundation beziehen öffentlich Position zu den Voraussetzungen jeder Erhöhungsstufe, wie Buterins Befürwortung der Verdopplung im November 2024 belegt.[173] Große Staking-Operatoren erhöhen ihre Targets erst, wenn die eigene Infrastruktur die neuen Anforderungen trägt. Die Verdopplung von 30 auf 60 Millionen war entsprechend kein emergenter Prozess: Die EF hatte die Voraussetzungen kommuniziert, die Client-Teams hatten die Execution optimiert, die Hardware war bereit. Die reale Dynamik ist sequentiell: Features werden deployt, ihre operative Stabilität wird bestätigt, und erst dann ermöglicht das Validator-Voting die nächste Kapazitätsstufe.

---

[175] EIP-7935 (Gas Limit Default Target, DEPL) formalisiert den Zielwert für Validator-Voting. EIP-7825 (Transaction Gas Cap, DEPL, Fusaka) setzt ein Maximum von 16,78M Gas pro Einzeltransaktion als DoS-Schutz.

[176] Fusaka (Dezember 2025, DEPL) umfasst das DoS-Hardening als Voraussetzung für aggressive Gas-Limit-Erhöhungen. Blob-Parameter-Optimierungen: BPO1 (9. Dezember 2025, Blob Target 10 / Max 15), BPO2 (7. Januar 2026, Target 14 / Max 21).

Vom Validator-Voting zum Hard Fork

Ab 100 Millionen Gas stößt die sequentielle Verifikation an eine zeitliche Grenze, die das heutige Protokoll nicht auflösen kann: Die Verifikationszeit wächst linear mit dem Gas Limit und überschreitet den 12-Sekunden-Slot, sobald der Node nicht mehr feststellen kann, welche Transaktionen unabhängig voneinander verarbeitbar sind. BALs und ePBS, deren Mechanismen 5.2-A dargestellt hat, adressieren genau diesen Engpass. BALs entlasten die Verifikationszeit durch parallele Verarbeitung, ePBS schafft das erweiterte Propagation-Fenster für größere Blöcke. Beide setzen protokolläre Änderungen voraus, die nur ein koordinierter Hard Fork liefern kann.[177] Der Übergang von autonomem Voting zu koordinierter Fork-Entwicklung folgt aus der Komplexität der nächsten Stufe: BALs verändern den Block Header, ePBS reorganisiert den Slot in zwei Phasen, und beide setzen voraus, dass alle Clients die neuen Strukturen gleichzeitig übernehmen. Ethereums Fork-Kadenz zeigt die Tragfähigkeit dieser Koordination: Dencun (März 2024), Pectra (Mai 2025), Fusaka (Dezember 2025) und Glamsterdam (erwartet 2026) folgen in einem zunehmend kürzeren Rhythmus, der sich von jährlich auf zweimal jährlich beschleunigt hat und den Skalierungspfad kontinuierlich strukturiert. Beide Features haben SFI-Status. Die Implementierungen laufen in drei Execution-Layer-Clients für BALs und fünf Consensus-Layer-Clients für ePBS. Der nächste Schritt ist damit spezifikationsreif und in fortgeschrittener Implementierungsarbeit, wobei die ePBS-Entwicklung sich laut EF-Checkpoint 9 (April 2026) als komplexer erweist als ursprünglich erwartet.[178] Tomasz K. Stańczak, damaliger EF-Co-Executive Director, hat die gestaffelten Schwellen im Dezember 2025 präzisiert: zunächst 100 Millionen Gas nach Glamsterdam, 200 Millionen Gas nach voll betriebsbereitem ePBS, langfristig eine L1-Zielmarke von circa 10.000 Transaktionen pro Sekunde.[179] Die Soldøgn-Konsensbildung der Core-Developer vom 2. Mai 2026 hat diese Etappenwerte als operative Orientierung bekräftigt.[180]

[177] BALs (EIP-7928) und ePBS (EIP-7732): beide SFI Glamsterdam (H2 2026). BALs adressieren die Validierungszeit (parallele Transaktionsverarbeitung), ePBS das Propagation-Fenster (erweiterte Verteilungszeit größerer Blöcke). Hard Fork: koordiniertes Protokoll-Upgrade, bei dem alle Nodes gleichzeitig auf neue Regeln umstellen.

[178] BALs: Prototyp-Implementierungen in Besu, Geth und Nethermind (vgl. Fußnote 24); BAL-Devnets machen laut EF Checkpoint #9 (April 2026) stetigen Fortschritt. ePBS: alle fünf CL-Clients in aktiver Entwicklung (vgl. Fußnote 41); derselbe Checkpoint stuft die ePBS-Implementierung als komplexer als ursprünglich erwartet ein, weil die Zwei-Parteien-Koordination zwischen Proposer und Builder jeden Teil des Stacks berührt. Status beider Features: SFI gemäß EF Checkpoint #9 (April 2026).

[179] Stańczak-Präzisierung, öffentliche Kommunikation des EF-Direktionsteams, Dezember 2025. Die Werte sind autorisiert, nicht spekulativ. Sie markieren die erste Etappe eines gestaffelten Pfads, dessen SOLL-Zielzustand (Faktor 100 über vier Jahre nach EIP-9698, siehe Fußnote 22) weit jenseits dieser Schwellen liegt.

[180] Soldøgn-Konsens der Core Developers vom 2. Mai 2026: Bekräftigung der 100-Millionen-Schwelle nach Glamsterdam und der 200-Millionen-Schwelle nach vollständig operationalem ePBS als verbindliche operative Orien-

Die Schwelle bei 150 bis 500 Millionen Gas erzeugt einen zweiten Engpass: Die Gas-Kosten einzelner EVM-Operationen spiegeln nicht mehr die tatsächlichen Hardware-Kosten wider, sodass ein Angreifer mit geringem Gas-Aufwand überproportional teure Operationen erzwingen kann. Die Gas Repricings (EIP-7904 und EIP-8038, Meta-EIP 8007, CFI Glamsterdam, also Considered for Inclusion) rekalibrieren die Kosten an aktuelle Hardware-Realitäten.[181] Diese Art der Rekalibrierung ist etablierte Governance-Praxis: EIP-1884 (Istanbul, 2019) und EIP-2929 (Berlin, 2021) haben in früheren Forks bereits Gas-Kosten an veränderte Hardware und geänderte Angriffsprofile angepasst.[182] Die Details und die DoS-Risiken, die die aktuelle Rekalibrierung adressieren muss, behandelt Abschnitt 5.2-C.

Bis zu der Schwelle ist der Skalierungspfad governance-verankert und operativ vorbereitet: Jede Voraussetzung hat einen SFI- oder CFI-Status und einen benannten Fork. Die erste knappe Verzehnfachung der L1-Kapazität, von 60 auf circa 500 Millionen Gas, bewegt sich im Bereich erprobter Governance-Mechanismen. Parallel zum Execution-Engpass erzeugt der Skalierungspfad ab der Schwelle jedoch ein korreliertes State-Wachstum, dessen Tragfähigkeit Abschnitt 5.4 quantifiziert und das die Bewertung der ersten Verzehnfachung unter einen Vorbehalt stellt, der hier nicht aufgelöst wird.

Die zweite Verzehnfachung: Aktive Forschung, offene Spezifikation

Ab circa 500 Millionen Gas tritt der Skalierungspfad in ein Stadium, in dem die Voraussetzungen aktiv erforscht, aber noch nicht spezifikationsreif sind. Der spezifische Engpass liegt in der vollständigen Re-Execution: Ab circa 600 Millionen Gas überschreitet die Verifikationszeit selbst mit paralleler Verarbeitung den Slot, sodass die in 5.2-A dargestellte zkEVM zur zwingenden Voraussetzung wird, um Verifikation und Kapazität zu entkoppeln. Die zkEVM hat einen Draft EIP (EIP-8025), eine publizierte EF-Roadmap und ein dediziertes Forschungsteam, aber keinen Fork-Termin.[183] Ein Feature ohne Fork-Termin ist in diesem Entwicklungsstadium der erwartbare Zustand: BALs und ePBS hatten ebenfalls keinen, bevor sie spezifikationsreif wurden und den SFI-Status erhielten. Die verbleiben-

tierung. Der Konsens markiert die Übergangsphase zwischen Fusaka und Glamsterdam.

[181] Gas Repricings: EIP-7904, EIP-8038; Meta-EIP 8007. Alle CFI Glamsterdam. Rekalibrierung der Gas-Kosten an aktuelle Hardware-Realitäten, unabhängig von Verkle-spezifischen Gas-Änderungen.

[182] EIP-1884 (Istanbul, Dezember 2019) erhöhte Gas-Kosten für SLOAD und BALANCE an geänderte State-Zugriffszeiten. EIP-2929 (Berlin, April 2021) führte differenzierte Gas-Kosten für kalte und warme Storage-Zugriffe ein. Beide adressierten DoS-Vektoren, die durch Diskrepanzen zwischen Gas-Kosten und realen Ausführungskosten entstanden.

[183] EIP-8025 (zkEVM). Status: Draft EIP, aktive EF-Roadmap seit Januar 2026 mit sechs Sub-Themes und gestuften Meilensteinen (vgl. Fußnoten 10, 14). Kein Fork-Termin.

de Unsicherheit liegt im genauen Zeitpunkt der protokollären Integration. Die in 5.2-A dargestellte Conjectures-Problematik wirkt als Zeitplan-Risiko, das den Pfad verzögern kann. Sollten die kryptographischen Annahmen der STARK-basierten Verfahren sich als nicht haltbar erweisen, wäre die Verzögerung substanzieller als die in 5.2-A veranschlagten ein bis zwei Jahre. Die sequentielle Logik des Pfads begrenzt dieses Risiko: Das Gas Limit wird 500 Millionen nicht erreichen, bevor BALs, ePBS und Gas Repricings deployt sind, und die zkEVM hat bis dahin mehrere Jahre Entwicklungszeit.

Bei 600 bis 800 Millionen Gas wird verteiltes Proving zur Voraussetzung, weil ein einzelner Prover das ePBS-Fenster nicht mehr einhalten kann.[184] Die ökonomische Koordination eines solchen Proving-Netzwerks hat weder einen EIP noch eine Roadmap. Der Vergleich mit der Builder-Ökonomie liefert ein Gegenmodell. MEV-Auktionen, Builder-APIs und die gesamte PBS-Infrastruktur entstanden organisch, als die ökonomischen Anreize vorhanden waren, ohne dass ein EIP sie vorher spezifiziert hätte.[185] Die Analogie hat allerdings eine strukturelle Grenze: MEV-Extraktion ist ein Wertentnahme-Spiel mit endogenen Profitquellen, während Proving primär eine Infrastrukturleistung ist, deren Vergütung aus Protokoll-Subventionen oder Priority Fees alimentiert werden muss. Die Analogie setzt voraus, dass die Proving-Ökonomie vergleichbare Anreize generiert, was von der protokollären Verankerung der zkEVM und dem Transaktionsvolumen auf dieser Kapazitätsstufe abhängt. Execution Tickets (RES), die für das Building diskutiert werden, könnten perspektivisch die Koordination von Building und Proving ins Protokoll verlagern. Die Proving-Ökonomie ist ein zukünftiges Koordinationsproblem, dessen Schwierigkeit sich an einer realen Analogie messen, aber nicht vorhersagen lässt.

>1.000 Millionen Gas als Projektion

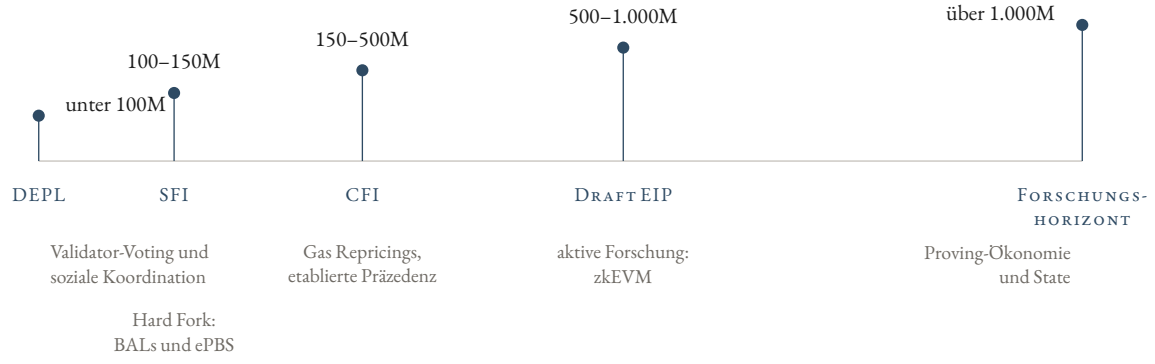
Oberhalb von 1.000 Millionen Gas liegt der Bereich, für den die Roadmap keine konkreten Antworten bereithält. Die Soundness der zkEVM ist kryptographisch durch die ZK-Proof-Verifikation garantiert. Das 1-of-N-Modell sichert die Liveness, solange mindestens ein ehrlicher Prover aktiv ist. Die ökonomische

[184] Bei circa 600 bis 800M Gas überschreitet die Proof-Erzeugungszeit das ePBS-Fenster eines einzelnen Provers. Verteiltes Proving wird zur Voraussetzung. Die Soundness der zkEVM ist kryptographisch durch die ZK-Proof-Verifikation selbst garantiert; fehlerhafte Blöcke können keinen gültigen Proof erzeugen. Das 1-of-N-Modell in EIP-8025 bezieht sich auf die Liveness: Ein einziger ehrlicher Prover genügt, damit die Proving-Pipeline nicht stillsteht. Die ökonomische Koordination dieses Mindestbetriebs wird vom Modell nicht adressiert und ist Gegenstand der Forschung.

[185] MEV-Boost (Flashbots, September 2022) etablierte den Builder-Markt ohne protokolläre Spezifikation. Die gesamte PBS-Infrastruktur, einschließlich Builder-APIs und Relay-Netzwerk, entstand organisch als Antwort auf ökonomische Anreize.

Absicherung dieses Mindestbetriebs, also die Anreize für eine tragfähige Anzahl aktiver Prover, bleibt als Koordinationsaufgabe offen.[184] Die State-Problematik, die bereits ab circa 500 Millionen Gas als wachsender Engpass wirkt und bei dieser Schwelle zum binär limitierenden Faktor wird, ist Gegenstand von Abschnitt 5.4.[186]

Entscheidend für die Infrastrukturbewertung ist die Einordnung der Schwellen in operative Größenordnungen. Bei 60 Millionen Gas pro Block und 12-Sekunden-Slots verarbeitet Ethereum circa 5 Millionen Gas pro Sekunde. Bei 500 Millionen Gas pro Block wären es circa 42 Millionen Gas pro Sekunde, genug für rund 2.000 einfache ETH-Transfers oder rund 200 Uniswap-Swaps pro Sekunde. Die tatsächliche Kapazität hängt vom Transaktionsmix ab. Die Größenordnung verdeutlicht den Sprung von einer Nische spezialisierter Krypto-Anwendungen in eine Leistungsklasse, in der institutionelle Settlement-Lasten auf L1 operieren könnten. Bei 1.000 Millionen Gas verdoppeln sich die Werte nochmals. Die erste knappe Verzehnfachung, die diese Arbeit als governance-verankert und operativ vorbereitet bewertet, adressiert die in Kapitel 2 formulierten Infrastrukturanforderungen. Die zweite bewegt sich auf einem Forschungs-Zeitplan, deren Reifegrad der Position in der Pipeline entspricht. Jenseits davon beginnt offenes Terrain, das den infrastrukturellen Kapazitätsbedarf des relevanten Planungshorizonts nicht betrifft.



Der zunehmende Abstand ist die Aussage. Die Skalierung wird nicht gleichmäßig schwerer, sondern sprunghaft.

Abbildung 5.2-B.1 Der Skalierungspfad als sequentielle Pipeline. Fünf Schwellen mit zunehmendem Reifegrad-Abstand: <100M (DEPL, Validator-Voting + soziale Koordination), 100–150M (SFI, Hard Fork: BALs + ePBS), 150–500M (CFI, Gas Repricings, etablierte Präzedenz), 500–1.000M (Draft EIP, aktive Forschung: zkEVM), >1.000M (Forschungshorizont: Proving-Ökonomie + State). Pro Schwelle: Governance-Status, Engpass-Typ, De-facto-Schwellen und sequentielle Abhängigkeiten.

[186] Die State-Problematik bei steigendem Gas Limit wird in Abschnitt 5.4 quantifiziert und analysiert. Tiered State als vorgeschlagene Lösung hat den Status RES.

Der Pfad als Governance-Leistung

Jede Schwelle des Skalierungspfads erzeugt einen spezifischen Engpass, den die jeweils nächste Protokolländerung adressiert: die sequentielle Verifikationszeit bis 100 Millionen, die Slot-Überlastung bis 150 Millionen, die DoS-Anfälligkeit fehlkalibrierter Gas-Kosten bis 500 Millionen, die lineare Kopplung zwischen Kapazität und Verifikationsaufwand bis 1.000 Millionen. Die sequentielle Dynamik des Pfads, in der Features deployt werden, bevor das Gas Limit die nächste Stufe erreicht, ist die eigentliche Governance-Leistung. Die praktischen Mechanismen, die diesen Rhythmus sichern, sind wirksam, auch wenn sie nicht protokollär formalisiert sind: ökonomische Anreize über verpasste Attestations, öffentliche Positionierung der EF zu jeder Erhöhungsstufe und die Infrastrukturbereitschaft der Staking-Operatoren. Sollte eine Stufe sich verzögern, blockiert der Pfad an dieser Stelle, weil das Validator-Voting die nächste Schwelle erst freigibt, wenn die operative Realität sie trägt. Die Schwelle bei 150 bis 500 Millionen Gas hängt an einer Rekalibrierung der Gas-Kosten, die bisher nur als Voraussetzung erwähnt wurde. Was genau diese Rekalibrierung umfasst und welche DoS-Risiken sie adressieren muss, klärt der folgende Abschnitt.

5.2-C Die Neukalibrierung des Preissystems

Die Rekalibrierung, die den Skalierungspfad bis 500 Millionen Gas trägt, korrigiert eine Abweichung zwischen den Gas-Preisen und den realen Hardware-Kosten. Gas ist das Preissystem, mit dem das Protokoll jede Operation gegen die Belastung der Validator-Hardware verrechnet. Die Kalibrierung muss so gewählt sein, dass selbst der teuerste konstruierbare Block innerhalb des 12-Sekunden-Slots vollständig verifiziert werden kann. Gelingt das nicht, verpasst der ehrliche Validator seine Abstimmung darüber, welcher Block in die Kette aufgenommen wird, und verliert einen Teil der mit dem Slot verbundenen Belohnung. Die heutigen Gas-Preise stammen aus der Frühzeit von Ethereum. Rechenoperationen sind seitdem deutlich billiger auszuführen geworden, weil die Prozessorleistung stark gewachsen ist. Der Zugriff auf gespeicherte Daten ist demgegenüber teurer geworden. Der State-Speicher der Blockchain ist auf rund 430 GiB angewachsen, sodass das Auffinden einzelner Einträge entsprechend länger dauert.[187] Die

[187] State-Größe Ethereum: rund 430 GiB per Q1 2026, mit Bandbreite 410–450 GiB je nach Client-Implementierung und Compression-Modus. Quellen: Maria Silva (ethresear.ch/t/23476, November 2025) misst 340 GiB im Mai 2025 (uncompressed, Geth-Node, dedicated to state); Vitalik Buterin (ethresear.ch/t/24052, Februar 2026) gibt das aktuelle Wachstum mit rund 100 GB pro Jahr an. Die Q1-2026-Schätzung folgt aus dem Mai-2025-Ausgangswert plus zweistufigem Wachstum: rund 73 GiB pro Jahr bei 36 Millionen Gas Limit (bis Juni 2025), rund 124 GiB pro Jahr bei 60 Millionen Gas Limit (ab Dezember 2025). Die Rechenleistung pro Prozessor ist seit der ursprünglichen Gas-Kalibrierung durch die Hardware-Entwicklung stark gewachsen, während die Zugriffszeit auf den State durch dessen

Gas-Preise beider Operationsklassen blieben dabei unverändert, sodass ein Teil der Rechenoperationen heute gemessen an der gewachsenen Prozessorleistung überbepreist ist, während andere Rechenoperationen sowie die Speicherzugriffe gemessen an ihrer tatsächlichen Hardware-Last unterbepreist bleiben.

Bei 60 Millionen Gas pro Block ist diese Abweichung zu klein, um die Validator-Kapazität spürbar zu beanspruchen. Ab 150 bis 500 Millionen Gas wird sie zum praktischen Problem. Ein Angreifer kann auf dieser Stufe mit niedrigem Gas-Budget Blöcke konstruieren, die eine deutlich höhere Hardware-Last bei den Validatoren erzeugen, als er selbst bezahlt. Bei größerer Blockgröße passen mehr unterbepreiste Operationen gleichzeitig in einen Block, sodass die Hardware-Last kumulativ über die Slot-Grenze hinauswachsen kann. Ein gestaffelter Kapazitätspfad stellt damit eine Anforderung an das Preissystem. Die relativen Preise müssen der realen Hardware-Last so nahe kommen, dass ein Angreifer mit wenig Gas keine übergroße Validator-Last mehr erzeugen kann.

Die Glamsterdam-Repricings heben die Gas-Kosten dreier systematisch unterbepreister Operationsklassen an: Rechenoperationen, State-Zugriffe und State-Erzeugung. Die Compute Gas Cost Increase (EIP-7904, CFI Glamsterdam) hebt die Kosten von 13 unterbepreisten Rechenoperationen und Precompiles an, deren tatsächliche Ausführung langsamer ist als ihre aktuelle Bepreisung widerspiegelt. Kryptographische Precompiles wie POINT_EVALUATION steigen dabei von 50.000 auf 89.363 Gas, arithmetische Grundoperationen wie DIV von 5 auf 15 Gas.[188] Die State-Access Gas Cost Increase (EIP-8038, CFI Glamsterdam) hebt die Kosten unterbepreister State-Zugriffe an. Eine Lese-Operation wie EXTCODESIZE, die zwei Datenbank-Reads auf den aktuellen State-Bestand auslöst, wird in dieser Richtung neu kalibriert.[189] Als dritte Korrektur hebt die State Creation Gas Cost Increase (EIP-8037, SFI Glamsterdam) die Kosten für das Anlegen neuer Storage-Slots und Accounts an. Die langfristigen

Wachstum strukturell gestiegen ist. Die Asymmetrie zwischen Compute, State und Data wird in Abschnitt 5.4 als eigenständiges Problem behandelt.

[188] EIP-7904 (Compute Gas Cost Increase). Status: PLAN, CFI Glamsterdam. Hebt die Gas-Kosten von 13 unterbepreisten Compute-Operationen und Precompiles an, deren tatsächliche Ausführung auf Validator-Hardware langsamer ist als ihre aktuelle Bepreisung reflektiert. Beispielhafte Anhebungen: DIV 5 auf 15 Gas, MOD 5 auf 12 Gas, SDIV 5 auf 20 Gas, KECCAK256 30 auf 45 Gas, BLAKE2F 0 auf 170 Gas, BLS12_G1ADD 375 auf 643 Gas, ECADD 150 auf 314 Gas, POINT_EVALUATION 50.000 auf 89.363 Gas. Die Anhebung unterbepreister Operationen ist Voraussetzung für die vorgesehene Blocklimit-Erhöhung, weil bottleneck-bildende Operationen erst nach der Anhebung nicht mehr die Kapazität bei größeren Blöcken limitieren. POINT_EVALUATION (KZG-Commitment-Verifikation), BLS12_G1ADD und ECADD sind strukturell Bestandteile der on-chain Precompile-Schicht, deren systematische Einordnung Abschnitt 5.3 in der Behandlung der kryptographischen Infrastruktur-Ebene ausführt. Quelle: EIP-7904 Originaltext.

[189] EIP-8038 (State-Access Gas Cost Increase). Status: PLAN/Draft, CFI Glamsterdam. Anhebung der Kosten unterbepreister State-Zugriffe. Belegbeispiel: Operationen mit zwei Datenbank-Reads pro Aufruf, deren I/O-Kosten die aktuellen Gas-Preise bei der heutigen State-Größe nicht mehr reflektieren.

Auswirkungen neuer State-Einträge auf die Gesamtgröße des State waren in der ursprünglichen Kalibrierung nicht eingepreist.[190] Die Frage, warum das State-Wachstum trotz der Anpassung ein ungelöstes strukturelles Problem bleibt, behandelt Abschnitt 5.4. Die drei Korrekturen treffen Anwendungsklassen in unterschiedlicher Intensität: Protokolle mit hoher Dichte kryptographischer Operationen oder State-erzeugender Deployments tragen stärkere Kostenanhebungen als Protokolle mit leichtgewichtigen Transaktionsprofilen. Abschnitt 5.5 behandelt die Neutralitäts-Implikationen der differenziellen Wirkung.

Reduce Intrinsic Transaction Gas (EIP-2780, CFI Glamsterdam) senkt als flankierender Baustein die festen 21.000 Gas Intrinsic Costs, die jede Standardtransaktion unabhängig von ihrem Inhalt trägt.[191] Meta-EIP 8007 führt alle zum Repricing-Paket gehörenden EIPs zentral zusammen und erlaubt dem Ökosystem damit einen Überblick darüber, welche Korrekturen zusammengehören. Die inhaltliche Abstimmung zwischen den Einzel-EIPs leisten die Glamsterdam-Repricings-Calls der Ethereum-Kernentwickler.[192]

Zwei bereits in Fusaka aktive Mechanismen begrenzen den Spielraum, den ein Angreifer pro Transaktion und pro Fork ausnutzen kann. Der Transaction Gas Cap (vgl. Abschnitt 5.2-B) wirkt in der Rekalibrierung als Randbedingung. Bei einer Blockgröße von 500 Millionen Gas kann selbst die teuerste zulässige Transaktion damit nur 3,4 Prozent des Blocks belegen. Ein Angreifer müsste folglich viele Transaktionen kombinieren, um einen Block über den Slot zu treiben, was seine Angriffskosten deutlich erhöht. Das Gas Limit Default Target formalisiert den Zielwert, an dem sich die Gas-Limit-Stimmabgabe der Validatoren orientiert. Validatoren können das Gas-Limit pro Block geringfügig erhöhen oder senken. Das Default Target gibt ihnen den gemeinsamen Referenzwert, an dem sich die Einzelentscheidungen koordinieren. Die Korrekturen und die flankierenden Mechanismen adressieren die Preis-Hardware-Abweichung auf drei Ebenen: Die Repricings kalibrieren den Preis pro Operation, der Transaction Gas Cap begrenzt die Wirkung pro Transaktion, das Gas Limit Default Target koor-

[190] EIP-8037 (State Creation Gas Cost Increase). Status: PLAN, SFI Glamsterdam. Hebt die Gas-Kosten für das Anlegen neuer Storage-Slots und Accounts an. In der ursprünglichen Gas-Kalibrierung waren die langfristigen Auswirkungen neuer State-Einträge auf die Gesamtgröße des State nicht angemessen eingepreist. Quelle: Meta-EIP 7773 (Glamsterdam Meta-EIP) und EIP-8037 Originaltext.

[191] EIP-2780 (Reduce Intrinsic Transaction Gas). Status: PLAN, CFI Glamsterdam. Senkt die fixen 21.000 Gas Intrinsic Costs einer Standardtransaktion. Flankierender Baustein neben EIP-7904, EIP-8038 und EIP-8037. Quelle: Meta-EIP 7773 (Glamsterdam Meta-EIP).

[192] Meta-EIP 8007. Der EIP-Text deklariert sich selbst als „purely informational" und erklärt explizit, keine aktive Rolle im Governance-Prozess zu übernehmen. Das Meta-EIP führt die Einzel-EIPs des Repricing-Pakets zentral zusammen; die inhaltliche Koordination erfolgt in den Glamsterdam-Repricings-Calls der Ethereum-Kernentwickler.

diniert die Anpassung pro Fork.

Die Reibung jeder Rekalibrierung

Die Rekalibrierung des Preissystems folgt in Ethereum einer eingeübten Praxis, deren Reibungsstelle strukturell zum Modus gehört. Die Istanbul-Rekalibrierung von Dezember 2019 hat die Gas-Kosten einer Trias von State-Zugriffs-Opcodes an veränderte State-Zugriffszeiten angepasst.[193] Der Effekt lässt sich an SLOAD ablesen, dessen Kosten von 200 auf 800 Gas angehoben wurden, um die gewachsene I/O-Last zu tragen. Rund 680 deployte Aragon-Contracts wurden nach dieser Anpassung funktionsuntauglich, weil ihre interne Transfer-Logik implizit auf den alten Gas-Kosten beruhte. ETH-Deposits von anderen Smart Contracts an Aragon-Organisationen vor Version 0.8 konnten nach dem Fork nicht mehr abgerufen werden. Die Betroffenheit reichte über Aragon hinaus zu Kyber, Gods Unchained und verschiedenen OpenZeppelin-Proxies. Das ist eine strukturelle Kosten-Kategorie der Rekalibrierung: Jede Preisanhebung auf unterbepreiste Operationen trifft Contracts, die dieselbe Annahme tragen. Für das gegenwärtige Glamsterdam-Paket folgt daraus, dass auch die dortigen Preisanhebungen solche Contracts treffen werden. Diese Reibung ist der Preis jeder Rekalibrierung des Preissystems. Der Berlin-Hard-Fork bestätigte die Logik 16 Monate später mit einer erneuten Kalibrierung der State-Zugriffe, die als zweite große Anpassung innerhalb dieses Zeitraums folgte.[194] Die Fork-Kadenz ist seitdem kürzer geworden: 14 Monate zwischen Dencun und Pectra, 7 Monate zwischen Pectra und Fusaka, rund sechs Monate angestrebt zwischen Fusaka und Glamsterdam.[195] Die halbjährliche Kadenz ist das erklärte Ziel. Die Governance reagiert iterativ, das Ökosystem absorbiert die Kosten der Anpassung in denjenigen Contracts, die auf der alten Kalibrierung gebaut wurden.

[193] EIP-1884 (Istanbul, 8. Dezember 2019). Rekalibrierung der Gas-Kosten einer Trias von State-Zugriffs-Opcodes (u. a. SLOAD, BALANCE, EXTCODEHASH) an veränderte State-Zugriffszeiten. SLOAD von 200 auf 800 Gas. Breaking-Wirkung: Rund 680 Aragon-Contracts (nach Aragon-CTO Jorge Izquierdo) wurden funktionsuntauglich, weil ihre interne Transfer-Logik implizit auf den alten Gas-Kosten basierte; ETH-Deposits von anderen Smart Contracts an pre-0.8-Aragon-Organisationen konnten nach dem Fork nicht mehr abgerufen werden (Aragon Help Desk). Betroffenheit auch bei Kyber, Gods Unchained und OpenZeppelin AdminUpgradeability-Proxies. Quellen: EIP-1884 Originaltext, Aragon Help Desk, Coindesk.

[194] EIP-2929 (Berlin, 15. April 2021). Einführung eines differenzierten Kostenmodells für State-Zugriffe, das den erstmaligen von wiederholten Zugriffen preislich trennt. Zweite große Rekalibrierung 16 Monate nach EIP-1884. Quelle: EIP-2929 Originaltext.

[195] Fork-Kadenz: Dencun (März 2024) → Pectra (Mai 2025), 14 Monate; Pectra → Fusaka (Dezember 2025), 7 Monate; Fusaka → Glamsterdam, rund sechs Monate angestrebt. Die Sechsmonats-Kadenz ist das erklärte Ziel der Ethereum-Kernentwickler; laut EF Checkpoint 9 (April 2026) erweist sich ePBS jedoch als komplexer als ursprünglich erwartet, sodass eine Aktivierung in Q3 oder Q4 2026 realistischer ist als H1. Die Kadenz-Disziplin ist eine Strukturaussage über die Governance-Reife (Kriterium III.2), nicht über den Zeithorizont des SOLL-Zielbilds, das weit über diesen Fork hinausreicht.

Auf mehreren Ebenen gleichzeitig adressieren die Bausteine der Korrektur die Preisseite der Schwelle zwischen 150 und 500 Millionen Gas. Im Zusammenspiel der Elemente korrigiert die Compute-Anhebung das Verhältnis zwischen Opcode-Kosten und Hardware-Last. Die State-Access-Anhebung entzieht einem Angreifer die Möglichkeit, mit wenig Gas überproportionale I/O-Last zu erzeugen, während die State-Creation-Anhebung die Erzeugung neuer State-Einträge an deren langfristige Kosten bindet. Der Transaction Gas Cap hält die Wirkung einer Einzeltransaktion bei den oben genannten 3,4 Prozent des Blocks. Das Default Target verankert den Pfad governance-seitig, indem es den Zielwert formalisiert, an dem sich die Koordination aller nachfolgenden Anpassungen orientiert. Ein weiterer Glamsterdam-Baustein verschiebt die strukturelle Grenze der Contract-Größe: EIP-7954 (Max Contract Size Increase, CFI Glamsterdam) hebt das aktuelle 24-KB-Limit pro Contract auf 64 KB an und entlastet damit größere zkVM-Verifizierer und komplexere DeFi-Architekturen.[196] Die Preis-Absicherung tritt damit neben die in 5.2-A dargestellten Parallelisierungs- und Verifikations-Mechanismen. Diese Elemente adressieren gemeinsam die in der Roadmap vorgesehene erste knappe Verzehnfachung der Kapazität.

Was die Rekalibrierung nicht löst

Die Absicherung bleibt innerhalb einer strukturellen Grenze, die Glamsterdam verschiebt, aber nicht aufhebt. Die PLAN-Korrekturen operieren innerhalb eines Preissystems, in dem Rechenzeit, Speicherzugriffe und Bandbreite in einem gemeinsamen Gas-Budget zusammengeführt werden. Eine Preisverschiebung auf einer Seite wirkt damit weiterhin auf die anderen Seiten zurück. Zwei Features im RES-Status zielen auf eine strukturelle Umgestaltung dieses Systems. EIP-8011 (Multidimensional Gas Metering, RES/DFI Glamsterdam, also Declined for Inclusion) schlägt vor, das eindimensionale Gas-Budget durch getrennte Zähler für mehrere Ressourcen-Kategorien zu ersetzen, die der EIP-Autor als Block-Ausführungszeit, Block-Netzwerk-Zeit, kurzfristigen Speicher und langfristigen Storage bündelt. Jede Ressourcen-Kategorie bekommt damit ihr eigenes Gas-Budget, sodass eine Preisverschiebung auf einer Seite die anderen Seiten nicht mehr verzerrt.[197] EIP-8057 (Inter-Block Temporal Locality Gas Discounts,

[196] EIP-7954 (Max Contract Size Increase). Status: CFI Glamsterdam. Hebt das EIP-170-Limit von 24.576 Byte (24 KB) auf 65.536 Byte (64 KB) pro Contract an und entlastet damit Anwendungen, deren Bytecode an die alte Schwelle stößt: insbesondere zkVM-Verifizierer, komplexere DeFi-Architekturen mit eingebetteten Bibliotheken und Solidity-Compiler-Output ohne aggressive Optimierung. Die Anhebung steht im Kontext der Gigagas-Skalierung, weil größere Block-Kapazität auch komplexere Einzeltransaktionen tragen können soll.

[197] EIP-8011 (Multidimensional Gas Metering). Status: RES/DFI Glamsterdam (per EIP-7773 von der Glamsterdam-Inclusion-Liste deklassifiziert, weiter im Forschungsstatus). Konzeptionelle Weiterentwicklung,

RES/DFI Glamsterdam) verfolgt eine andere Richtung und rabattiert Gas-Kosten für Zugriffe auf State-Einträge, die innerhalb eines Fensters der letzten 32 Blöcke bereits berührt wurden. Die Idee stützt sich auf empirische Cache-Beobachtungen: Kürzlich berührte Einträge liegen wahrscheinlich noch im Client-Cache und verursachen beim erneuten Zugriff geringere tatsächliche Kosten als kalte Einträge.[198] Beide Optionen tragen EIP-Nummern, sind aber keinem Fork zugeordnet und haben noch keinen Fork-Termin. Sie markieren Forschungsrichtungen, die die Preisseite über die punktuellen Korrekturen der PLAN-Bausteine hinaus strukturell weiterentwickeln sollen.

Die Reichweite der gesamten Preis-Absicherung bleibt damit in zweifacher Hinsicht begrenzt. Erstens kalibriert das Glamsterdam-Paket die Preise auf die Schwelle zwischen 150 und 500 Millionen Gas. Höhere Schwellen werden weitere Rekalibrierungen erzeugen, die der eingeübte Governance-Modus tragen kann, die aber nicht in diesem Fork mitgeliefert werden. Zweitens adressiert die Korrektur die Preisseite, nicht das State-Wachstum selbst. Die strukturelle Asymmetrie zwischen der Verarbeitungs-, der Daten- und der Speicher-Ressource bleibt damit bestehen. Die Daten-Ressource behandelt Abschnitt 5.2-D, das State-Wachstum behandelt Abschnitt 5.4.

Damit zielt die Roadmap darauf ab, das Preissystem zu einer adaptiven Schicht des Protokolls zu entwickeln, die sich an der Hardware-Realität der Netzwerkressourcen ausrichtet. Die Korrekturen im PLAN-Status sollen die Abweichung zwischen Preis und Hardware-Last innerhalb des bestehenden eindimensionalen Gas-Budgets adressieren. Die Forschungsrichtungen im RES-Status, namentlich das mehrdimensionale Gas-Metering und die zeitlich-lokale Rabattierung kürzlich berührter State-Einträge, zielen auf eine strukturelle Umgestaltung des Preissystems selbst, deren konkrete Implementierung offen bleibt. Das Ziel ist, dass das Netzwerk seine Ressourcen so bepreist, wie sie die Hardware tatsächlich belasten, und diese Bepreisung entlang der gestaffelten Kapazitätsstufen nachjustiert.

---

die das eindimensionale Gas-Budget durch getrennte Zähler für mehrere Ressourcen-Kategorien ersetzt. Der EIP spezifiziert sechs technische Dimensionen (compute, access, size, memory, state, history) und clustert sie im Rationale-Abschnitt in vier konzeptuelle Ressourcen-Kategorien: Block-Ausführungszeit, Block-Netzwerk-Zeit, kurzfristiger Speicher und langfristiger Storage. Die Darstellung im Haupttext folgt dieser vierer-Clusterung.

[198] EIP-8057 (Inter-Block Temporal Locality Gas Discounts). Status: RES/DFI Glamsterdam (per EIP-7773 von der Glamsterdam-Inclusion-Liste deklassifiziert, weiter im Forschungsstatus). Konzeptionelle Option, die Gas-Kosten für Zugriffe auf State-Einträge rabattiert, die innerhalb eines rollierenden Fensters der letzten 32 Blöcke (rund sechs Minuten) bereits berührt wurden. Der Rabatt folgt einer smoothstep-Decay-Funktion, die mit zeitlichem Abstand zum letzten Zugriff abnimmt. Hintergrund: Kürzlich berührte Einträge liegen wahrscheinlich noch in Client-Caches und verursachen beim erneuten Zugriff geringere tatsächliche I/O-Kosten als kalte Einträge.

Die Preisseite der Ausführungs-Ressource wird in der Roadmap durch PLAN-Korrekturen und RES-Forschungsrichtungen adressiert. Das Protokoll skaliert jedoch nicht nur Verarbeitung. Die L2-Rollups veröffentlichen ihre Transaktionsdaten auf L1, sodass die Kapazität der zweiten Richtung zu einer eigenständigen Skalierungsaufgabe wird.

5.2-D Die Skalierung der Datenverfügbarkeit

Die Rekalibrierung des Preissystems aus Abschnitt 5.2-C kalibriert die Execution-Ressource. Die zweite Ressource, die der Skalierungspfad adressiert, folgt einer eigenen Logik. Für die Daten, die L2-Rollups auf L1 veröffentlichen, gelten nicht dieselben Engpässe wie für die Execution selbst. Vor Proto-Danksharding (EIP-4844, DEPL seit März 2024)[199] konkurrierten diese Daten um denselben Blockraum wie reguläre Transaktionen und bestimmten damit direkt den L2-Kostenaufwand. Proto-Danksharding hat diese Konkurrenz aufgelöst, indem es Blobs als separaten Datentyp mit eigenem Fee-Markt eingeführt hat.[200] Blob-Gas folgt einer eigenen EIP-1559-analogen Preisdynamik, die vom Execution-Gas entkoppelt ist. Damit ist die Datenverfügbarkeits-Last der L2-Rollups preislich von der L1-Execution-Last getrennt.

Vor Dencun zahlten die großen L2-Sequencer zusammen mehr als 15.000 ETH pro Monat für Calldata auf L1, eine Größenordnung von rund 34 Millionen US-Dollar.[201] Nach Dencun bewegen sich die Blob-Kosten bei normaler Auslastung nahe dem Minimum. Die Transaktionskosten auf den großen Optimistic Rollups sanken von durchschnittlich rund 0,35 US-Dollar vor Dencun auf unter 0,01 US-Dollar nach Dencun.[202] Das entspricht einer Reduktion um 95 bis 99 Prozent, mit Abweichungen je nach Rollup und Utilization. Für einen L2-Betreiber bedeutet das einen Wechsel des Kostenmodells:

[199] EIP-4844 „Shard Blob Transactions" wurde mit dem Dencun-Hard-Fork am 13. März 2024 auf Ethereum-Mainnet aktiviert. Quelle: eips.ethereum.org/EIPS/eip-4844.

[200] Technische Parameter gemäß EIP-4844 „Shard Blob Transactions": Blob-Größe 131.072 Bytes (128 KB) = 4.096 Field Elements × 32 Bytes auf dem BLS12-381 Scalar Field. Retention-Dauer 4.096 Epochen (≈ 18 Tage) im Consensus Layer, gemäß MIN_EPOCHS_FOR_BLOB_SIDECARS_REQUESTS. Nach Ablauf der Retention verbleiben nur die KZG Commitments auf die Blob-Inhalte permanent on-chain. Quelle: eips.ethereum.org/EIPS/eip-4844 (Final, aktiviert mit Dencun am 13. März 2024); Ethereum Consensus Specs, Deneb-Fork-Spezifikation.

[201] Aggregierte Pre-Dencun Calldata-Ausgaben der großen L2-Sequencer (insbesondere Arbitrum, Optimism, Base) auf L1, Größenordnung umgerechnet zu durchschnittlichem ETH-Kurs Q1/2024. Quelle: On-chain-Daten via Dune Analytics, L2BEAT (Stand März 2024).

[202] Arbitrum: Durchschnittliche Fee von ca. $0,37 vor Dencun auf $0,012 nach Dencun (-97%). Optimism: $0,32 → $0,009 (-97%). Base: $0,31 → $0,0005–0,001 (-96% bis -99%). Starknet: $6,80 → $0,02–0,04 (-99%). Der in den Haupttext gezogene Durchschnittswert von rund 0,35 US-Dollar vor Dencun und unter 0,01 US-Dollar nach Dencun ist eine Mittelung über die großen Optimistic Rollups; Werte variieren mit Blob-Auslastung und Rollup-spezifischer Compression. Quelle: L2BEAT, growthepie.xyz.

Die Datenverfügbarkeit war vor Dencun einer der größten Bilanzposten. Nach Dencun ist sie keine strukturelle Betriebslast mehr.

Diese Entkopplung birgt eine Schwachstelle am unteren Ende des Preiskorridors. Bei Unter-Target-Auslastung, wenn pro Block weniger Blobs eingereicht werden als der Zielwert vorsieht, konvergiert der Blob-Preis rapide gegen Null, weil die EIP-4844-Fee-Formel den Preis in jedem Block exponentiell reduziert. Die Datenverfügbarkeits-Ressource wird bei Niedrig-Auslastung damit faktisch kostenfrei, obwohl sie L1-Block-Space und Validator-Bandbreite beansprucht. Das Protokoll trägt die Ressource ökonomisch, ohne Gegeneinnahmen daraus zu ziehen. Der Blob-Fee-Anteil an den Validator-Einnahmen geht gegen Null, und das L1-Security-Budget schwächt sich entsprechend. Blob Fee Stabilization (EIP-7918, DEPL mit Fusaka)[203] koppelt die Mindest-Blob-Base-Fee an die Execution-Gas-Kosten, sodass der Preis einen Boden annimmt, der die Block-Space-Kosten der Blob-Einreichung widerspiegelt. Der Blob-Fee-Anteil am L1-Security-Budget bleibt damit auch bei Unter-Target-Auslastung erhalten. Die vollständige Security-Budget-Argumentation entfaltet Abschnitt 5.5. An dieser Stelle genügt, dass EIP-7918 die Daten-Ressource ökonomisch stabilisiert.

PeerDAS: Verifikation über Stichproben

Die Preis-Schicht ist ökonomisch kalibriert. Die zweite architektonische Schicht der Daten-Ressource setzt an der Verifikations-Seite an. Bis Fusaka lud jeder Full Node jeden Blob vollständig herunter, sodass die Validator-Bandbreite linear mit der Blob-Kapazität skalierte. Diesen Aufwand ersetzt PeerDAS (EIP-7594, DEPL mit Fusaka im Dezember 2025)[204] durch Data Availability Sampling, ein probabilistisches Verfahren. Jeder Node prüft nur einen kleinen Ausschnitt der Blob-Daten. Ein Angreifer, der Daten zurückhält, wird statistisch auffällig. Technisch werden die Blobs horizontal via Reed-Solomon-Codierung erweitert, und die erweiterte Matrix wird in 128 Column Subnets aufgeteilt. Jeder Node lädt deterministisch nur die ihm zugewiesenen rund 12,5 Prozent der Daten.[205] Die

[203] EIP-7918 „Blob base fee bounded by execution cost". Eingeführt mit dem Fusaka-Hard-Fork. Koppelt den Mindest-Blob-Base-Fee an die Execution-Gas-Kosten, um Konvergenz des Blob-Preises bei niedriger Blob-Auslastung gegen das absolute Minimum von 1 Wei (10^{-18} ETH) zu vermeiden. Die EIP-4844-Fee-Formel reduziert den Blob-Preis bei Unter-Target-Auslastung in jedem Block exponentiell gemäß BLOB_BASE_FEE_UPDATE_FRACTION = 3.338.477. Quelle: eips.ethereum.org/EIPS/eip-7918, eips.ethereum.org/EIPS/eip-4844.

[204] EIP-7594 „PeerDAS — Peer Data Availability Sampling". Mit dem Fusaka-Hard-Fork im Dezember 2025 auf Mainnet aktiviert, mit Implementierung in allen sechs Consensus-Layer-Clients (Prysm, Lighthouse, Teku, Nimbus, Lodestar, Grandine). Quelle: eips.ethereum.org/EIPS/eip-7594, ethereum.org Forkcast.

[205] PeerDAS-Parameter: 128 Column Subnets in der erweiterten Blob-Matrix; deterministische Zuweisung eines Subsets pro Node basierend auf Node-ID; durchschnittliche Download-Last entspricht ca. 1/8 = 12,5 Prozent der Total Blob Data. Quelle: EIP-7594, CL-Specs.

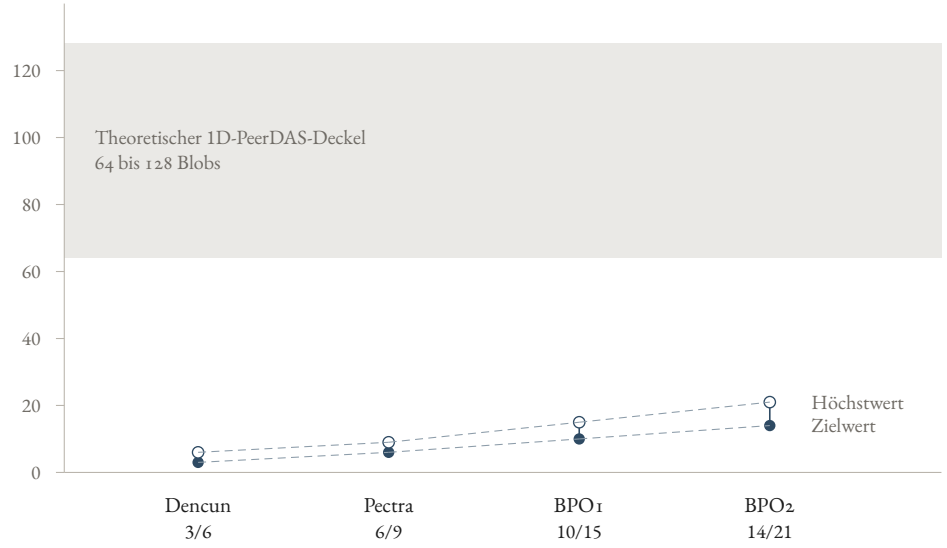
Architektur folgt demselben Prinzip wie die zkEVM auf der Execution-Seite: Wo die zkEVM die Re-Execution durch Proof-Verifikation ersetzt, ersetzt PeerDAS die vollständige Datenvorhaltung durch Sampling-Verifikation. Beide Mechanismen entkoppeln die Ressourcenanforderung pro Node von der Gesamtlast des Netzwerks.

Die Kapazitätswirkung dieser Entkopplung lässt sich am Blob-Parameter-Pfad der letzten Hard Forks ablesen. Seit Dencun ist die Blob-Kapazität in mehreren Schritten erhöht worden. Der aktuelle Stand nach BPO2 liegt bei Target 14 und Maximum 21 Blobs pro Block.[206] Das theoretische 1D-Maximum der PeerDAS-Architektur liegt bei 64 bis 128 Blobs und damit bei einem Vielfachen des aktuellen Stands.[207] Bei einer Rollup-spezifischen Compression von einigen hundert bis wenigen tausend L2-Transaktionen pro Blob erreicht der aktuelle Stand die Größenordnung einiger tausend L2-TPS, während das 1D-Maximum mehrere zehntausend erreicht.[208] Der Mechanismus, der diese Erhöhungen ermöglicht, sind Blob-Parameter-Only-Forks: isolierte Parameter-Änderungen, die ausschließlich Blob-Kapazitätsparameter berühren, ohne einen koordinierten Hard Fork zu erfordern. Die bisherigen BPO-Runden zeigen die Implementierungsreife der PeerDAS-Mechanik unter produktiver Last. Die Blob-Kapazität kann damit unabhängig vom allgemeinen Fork-Kalender erweitert werden, solange die Netzwerk-Stabilität die nächste Stufe trägt. Einen solchen Governance-Modus kennt die Ausführungs-Ressource mit ihren Hard-Fork-Abhängigkeiten nicht. Die operative Bewährung unter adversarialen Bedingungen wird sich an den kommenden Blob-Erhöhungen erweisen, konkret an der Netzwerk-Stabilität bei höheren Blob-Counts und am Sync-Verhalten bei Column-Subnet-Ungleichverteilung.

[206] Blob-Parameter im Zeitverlauf: Dencun (März 2024): Target 3 / Max 6. Pectra (Mai 2025): Target 6 / Max 9. Fusaka + BPO1 (Dezember 2025): Target 10 / Max 15. Fusaka + BPO2 (Januar 2026): Target 14 / Max 21. Quelle: ethereum.org Forkcast, EF-Blog „Fusaka BPO Schedule".

[207] Das theoretische 1D-PeerDAS-Maximum von 64–128 Blobs pro Block ist aus den Bandbreite- und Networking-Parametern der 1D-Sampling-Architektur abgeleitet. Quelle: ethresear.ch „PeerDAS Capacity Analysis", EF-Research-Blog.

[208] Blob-Compression-Werte variieren zwischen Rollups und mit der jeweiligen Transaktions-Zusammensetzung: Arbitrum und Optimism berichten Compression-Werte in der Größenordnung mehrerer hundert Transaktionen pro Blob, hochoptimierte Rollups (Starknet, zkSync) nähern sich vierstelligen Werten. Bei einem Slot-Intervall von 12 Sekunden und einem Blob-Target von 14 ergibt sich für Compression-Werte zwischen 500 und 2.000 L2-Transaktionen pro Blob eine aggregierte L2-TPS-Kapazität in der Größenordnung einiger tausend; am 1D-Deckel (64–128 Blobs) entsprechend mehrere zehntausend. Die Werte sind Größenordnungen, keine präzisen Projektionen; die tragende Aussage ist die Entkopplung der L2-Kapazität vom L1-Gas-Limit. Quelle: L2BEAT Blob-Compression-Daten, growthepie.xyz, Ethereum Foundation Research.



Der Abstand zwischen dem erreichten Wert und dem Deckel trägt die Aussage.

Abbildung 5.2-D.1 Blob-Parameter-Pfad — Dencun (3/6) → Pectra (6/9) → BPO1 (10/15) → BPO2 (14/21), mit theoretischem 1D-PeerDAS-Deckel bei 64–128 Blobs

Jenseits des 1D-Maximums liegt der Langfristpfad der Daten-Ressource in einer zweidimensionalen Erweiterung derselben Architektur. Full Danksharding (RES, keine Fork-Zuordnung) erweitert PeerDAS von eindimensionalem auf zweidimensionales Sampling, indem zur horizontalen Reed-Solomon-Erweiterung eine vertikale hinzutritt. Die Rekonstruierbarkeit der Daten skaliert damit quadratisch statt linear, und ein Node erfasst die Blob-Vollständigkeit aus einem deutlich kleineren Sample-Anteil. In dieser Matrix laden Nodes einzelne Cells (Matrix-Zellen) statt ganzer Columns (Spalten), sodass die Datenmenge pro Node bei wachsender Blob-Zahl konstant bleibt. Die Validator-Anforderungen werden vom Skalierungsziel strukturell entkoppelt.[209] Die Kapazitätsprojektion liegt bei 64 Blobs Target und 256 Maximum, entsprechend rund 32 MB Datendurchsatz pro Slot.[210] Die technische Voraussetzung ist eine effiziente bivariate Polynomial Interpolation, die die vollständige Matrix aus einem Teilausschnitt der Samples rekonstruiert. Diese Rekonstruktion ist mathematisch seit längerem definiert. Offen ist die produktionsreife Implementierung, weil die Rechenlast pro Rekonstruktion derzeit die Hardware-Budgets der Prover- und Validator-Infrastruktur überschreitet.[211] Full Danksharding hängt damit an ei-

[209] Full Danksharding erweitert die Reed-Solomon-Codierung von einer rein horizontalen (Row Extension) auf eine zweidimensionale Struktur (Row + Column Extension). Nodes samplen Cells statt Columns; die Sampling-Bandbreite pro Node wird damit vom Blob Count entkoppelt und nähert sich einem konstanten Wert. Quelle: Vitalik Buterin, „Proto-Danksharding FAQ“ und „Dankrad Feist on 2D DAS“ (notes.ethereum.org).

[210] Full-Danksharding-Zielspezifikation: 64 Blobs Target / 256 Blobs Maximum pro Slot, entsprechend ca. 32 MB Datendurchsatz pro Slot. Quelle: ethereum.org „Danksharding Roadmap“, Dankrad Feist Research Notes.

[211] Die bivariate Polynomial Interpolation für die 2D-Matrix-Rekonstruktion ist in algorithmischen Varianten implementiert, insbesondere als FFT-basierte Verfahren und GPU-beschleunigte Reed-Solomon-Encoder. Die offene Frage ist die produktionsreife Effizienz unter den Latenz- und Hardware-Budgets einer Slot-synchronen

nem Engineering-Engpass, dessen Lösung erwartbar, aber nicht terminiert ist. Unter dem L1-first-Pivot ist der Pfad nicht kritisch, solange PeerDAS die absehbare L2-Entwicklung trägt. Beschleunigte Adoption durch institutionelle Rollups, ENS Namechain oder Based Sequencing kann die Grundannahme überholen.

Neben der Engineering-Dimension birgt der Endzustand eine kryptographische Migrations-Frage. Die KZG-Commitments, die heute Blob-Korrektheit ohne vollen Download garantieren, ruhen auf Paarungen elliptischer Kurven, die ein hinreichend großer Quantenrechner mittels Shors Algorithmus brechen würde. Die Roadmap sieht daher den Übergang auf STARK- oder gitterbasierte Commitments vor. Das Problem liegt darin, dass STARKs die mathematische Linearitäts-Eigenschaft (Homomorphie) von KZG nicht besitzen. Da die Linearität jedoch die mathematische Grundlage für das zweidimensionale Data Availability Sampling (die effiziente Verifikation von Datenstrukturen über Teil-Stichproben) bildet, hinterlässt der Wechsel ein bislang ungelöstes Folgeproblem in der Skalierungs-Architektur.[212]

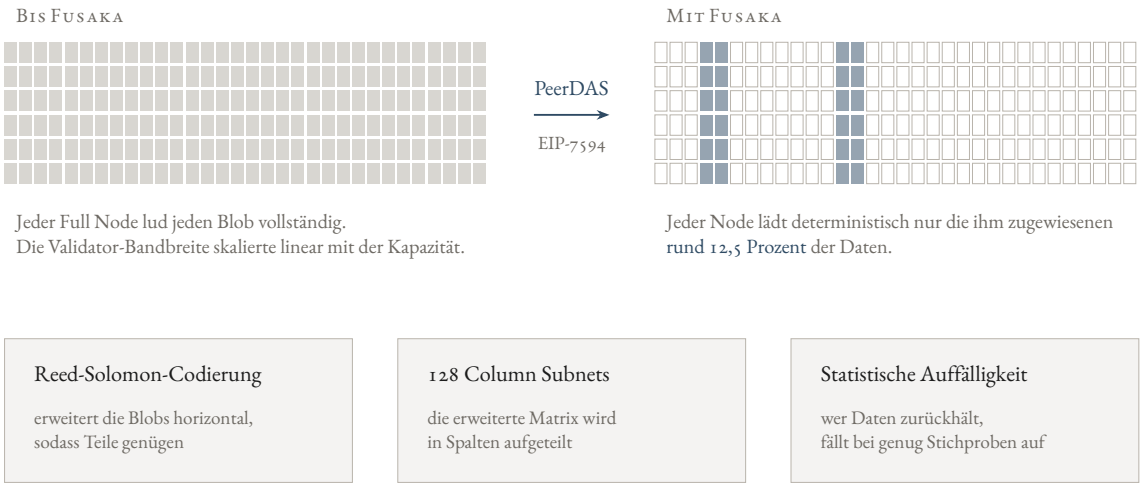


Abbildung 5.2-D.2 PeerDAS. Aus vollständiger Datenvorhaltung wird eine deterministisch zugewiesene Stichprobe.

Prover- und Validator-Infrastruktur. Quelle: EF-Research-Publikationen zu 2D-DAS-Algorithmen, Dankrad Feist Research Notes (notes.ethereum.org).

[212] KZG-Quantum-Vulnerabilität und Migrations-Kandidaten: Vitalik Buterin, „Possible Futures of the Ethereum Protocol — Post-Quantum Roadmap“ (26. Februar 2026); ethereum.org/roadmap/future-proofing/quantum-resistance/. Der Linearitäts-Trade-off zwischen KZG- und STARK-Commitments für das zweidimensionale Daten-Sampling ist in Vitaliks Roadmap explizit gemacht.

State: die Richtung ohne Durchbruch

Während die Daten-Ressource einen gestuften Ausbau erlaubt, stellt sich mit den beiden Durchbruchsmechanismen auf Execution- und Daten-Seite eine Frage, die über die Daten-Ressource hinausreicht. Die drei Skalierungsressourcen des Protokolls, Execution, Data und State, stehen auf drei verschiedenen Reifestufen, die aus der Architektur folgen. Die Ausführungs-Ressource hat mit der zkEVM einen identifizierten Durchbruchsmechanismus, dessen Governance-Pfad und Gas-Schwellen-Zuordnung 5.2-A und 5.2-B entfaltet haben. Für die Daten-Ressource liefert PeerDAS einen deployten Durchbruchsmechanismus und Full Danksharding eine Langfristoption. Die Speicher-Ressource hat hingegen keinen vergleichbaren Durchbruchsmechanismus, der mit diesen beiden in einer Reifestufe stünde.

Die Durchbrüche in den ersten beiden Richtungen treiben das Wachstum der dritten. Jede zusätzliche Execution-Kapazität kann State erzeugen, jede zusätzliche Daten-Kapazität ermöglicht L2-Aktivität, deren Settlement auf L1 wiederum State produziert. Mit jeder Skalierungsstufe verschärft sich die Asymmetrie: Was in frühen Roadmap-Formulierungen als langfristiges Risiko erschien, wird unter dem L1-Gas-Limit-Pfad zum mittelfristigen Engpass.

Die Rollentrennung aus 5.2-A löst Verifikation und Proving, nicht aber das Building selbst. Die zkEVM entkoppelt den Validator von der Gas-Kapazität, PeerDAS zusätzlich von der Blob-Bandbreite. Das verteilte Proving entkoppelt den Prover vom Block-Volumen. ePBS trennt den Proposer vom Building und eliminiert zugleich den Relay-Chokepoint (vgl. Abschnitt 5.5). Die Rolle des Block Builders bleibt an den State gebunden. Ein Builder muss den vollständigen State vorhalten, um einen gültigen Block zu konstruieren. Mit jeder Kapazitätsstufe wächst seine State-Synchronisationslast. Damit steigt die Einstiegshürde für das Block Building mit jeder Kapazitätsstufe, auch wenn die Verifikations- und Proving-Hürden fallen. Die Dezentralisierung der Verifikation ist damit architektonisch getragen. Die Dezentralisierung des Building bleibt an die ungelöste State-Ressource gebunden. Abschnitt 5.4 untersucht diese State-Bindung als tiefsten ungelösten Engpass der Roadmap.

Die Ausführungs-Ressource steht damit mit einer architektonischen Kette, einem gestaffelten Pfad und der perspektivischen Entkopplung durch die zkEVM. Die Daten-Ressource steht mit einem deployten Sampling-Mechanismus und einem zweidimensionalen Langfristpfad. State bleibt die offene Dimension und ist der Gegenstand von Abschnitt 5.4. Die Blob-Kapazität der Daten-Ressource entfaltet zugleich eine Wirkung jenseits des L2-Kostenmodells. Sie ist

die L1-Voraussetzung dafür, dass Rollups ihre Sicherheitsgarantien von institutioneller auf kryptographische Basis umstellen können. Abschnitt 5.6 behandelt die Umstellung als eigene architektonische Frage. Bis hierher reichen der Designzustand und das Zusammenspiel der Features, das die Roadmap für die Kapazitätserweiterung in den beiden skalierenden Richtungen vorsieht. Jenseits des Designzustands zeichnet sich eine Weiterentwicklung ab, die nicht die Kapazität der Execution-Schicht, sondern ihre Ausführungsumgebung selbst neu entwirft.

5.2-E Post-Designzustand: RISC-V, leanVM und die EIP-invariante Rollentrennung

Die Ausführungsumgebung, deren Weiterentwicklung der vorangegangene Abschnitt markiert hat, ist die Ethereum Virtual Machine: die Laufzeitumgebung, in der alle bisher beschriebenen Skalierungsmechanismen ablaufen. Die zkEVM, die 5.2-A eingeführt hat, beweist die korrekte Ausführung dieser bestehenden Maschine mit ihren historisch gewachsenen Opcodes und State-Übergängen. Eine tiefergehende Weiterentwicklung ersetzt nicht einzelne Mechanismen, sondern die Instruction Set Architecture selbst: den Grundkatalog der Befehle, den die Laufzeitumgebung interpretiert und ausführt. Jeder Smart-Contract-Code wird letztlich in diese Befehle übersetzt. Buterins Vorschlag vom Mai 2025 skizziert diese Richtung: die EVM langfristig durch eine RISC-V-basierte oder ähnlich ZK-native Ausführungsumgebung zu ergänzen oder abzulösen.[213]

RISC-V und der Proving-Vorteil

RISC-V (RES, explorativ, keine Governance-Verankerung) steht für Reduced Instruction Set Computing, fünfte Generation. Die Philosophie hinter dem Reduced Instruction Set ist eine minimalistische Grundentscheidung der Rechnerarchitektur: wenige, einfache Befehle, die jeweils nur einen Rechenschritt ausführen, während komplexe Makro-Befehle intern in viele Teilschritte zerfallen. RISC-V ist die offene Standardisierung der Architektur, 2010 an der UC Berkeley entwickelt und seitdem unter einer lizenzfreien Spezifikation verfügbar. Für Ethereum ist weder der akademische Ursprung noch die Lizenzfreiheit der entscheidende Punkt. Entscheidend ist, was die Einfachheit der Instruktionen für ZK-Proving bedeutet: Jeder RISC-V-Befehl führt nur einen einzigen Rechenschritt aus, ohne versteckte interne Komplexität, und lässt sich deshalb mit wenigen mathematischen Gleichungen abbilden. Ein ZK-Circuit-Constraint ist ei-

[213] Vitalik Buterin, „A simplified version of the EVM: Long-term L1 execution layer proposal with RISC-V", Ethereum Magicians Forum, Mai 2025. Der Vorschlag trägt keinen EIP-Status und keinen Fork-Termin; er ist als Forschungsrichtung publiziert, nicht als Implementierungsplan.

ne solche Gleichung, die die korrekte Ausführung einer Instruktion erzwingt: Sie legt fest, welche Werte vor und nach der Instruktion gelten müssen, damit die Rechnung als gültig bewiesen werden kann. Jede Instruktion wird durch eine Menge solcher Gleichungen dargestellt. Ein RISC-V-Befehl operiert auf einer kleinen Zahl von Registern, den schnellen internen Speicherzellen einer CPU, und führt darauf eine einzige Rechenoperation aus: Addition, Multiplikation, Vergleich, Shift. Seitenwirkungen, ein mitveränderter Stack-Zustand, ein mitwachsender Speicher und eine Buchhaltung über den Ressourcen-Verbrauch fehlen ihm. Ein EVM-Opcode dagegen führt meist mehrere solcher Grundoperationen intern zusammen und trägt zusätzlich eine Gas-Buchhaltung, einen wachsenden Memory-Bereich und Stack-Operationen mit sich. All das muss in der ZK-Verifikation mitabgebildet werden. Daraus folgt die Größenordnungs-Differenz: Ein RISC-V-Befehl wird typischerweise mit einstelligen bis niedrig zweistelligen Gleichungen belegt, eine EVM-Opcode-Ausführung mit einigen hundert bis tausend. Die daraus abgeleitete Performance-Verbesserung für Smart Contract Execution in ZK-Provern liegt laut Buterins Vorschlag bei Faktor 100 oder mehr. Die praktische Konsequenz: Der Proving-Aufwand, der heute signifikante Latenz- und Kostenschranken setzt, würde auf Niveaus sinken, die für Realtime-Proving innerhalb eines Slot-Fensters ausreichen.[214] Die Zahl ist eine Projektion aus dem Vorschlag. Gemessen wurde sie an keinem laufenden System.

Die Roadmap erwartet drei Konsequenzen aus diesem Architekturwechsel, die auf verschiedenen Ebenen Zugänglichkeit und Beweisbarkeit erhöhen. Die erste Ebene ist die Proving-Ökonomie. Als direkte Konsequenz der Constraint-Zahlen aus dem vorangegangenen Absatz ist heute eine spezialisierte Proving-Infrastruktur nötig: Ein EVM-Block enthält Millionen Opcode-Ausführungen, die in Summe mehrere Milliarden Constraints erzeugen. Ein Beweissystem, das diese Menge in akzeptabler Zeit verarbeiten muss, braucht massiv parallele Hardware, typischerweise GPU-Cluster oder spezialisierte ASICs. Mit einer RISC-V-basierten Ausführungsumgebung verliert die Infrastruktur ihre strukturelle Notwendigkeit: Die Constraints pro Instruktion sinken um ein bis zwei Größenordnungen, der Gesamtaufwand wird auf handelsüblicher Hardware bewältigbar, der Prover-Markt öffnet sich für eine breitere Akteursbasis. Die zweite Ebene ist die Developer-Generativität. Weltweit gibt es zwischen 70.000 und 80.000

[214] ebd. Die 100×-Projektion bezieht sich auf die Proving-Performance in ZK-Provern, nicht auf native Execution-Performance. Die Zahl ist Richtwert aus der Primärquelle, kein Messwert eines laufenden Systems; die Ableitung gründet auf der Constraints-Reduktion pro Instruktion. Die im Haupttext genannte Konsequenzebene (Latenz- und Kostenschranken, Realtime-Proving innerhalb eines Slot-Fensters) ist qualitative Einordnung auf Basis der Proving-Entwicklung 2024/2025; konkrete Zeit-Anker zur Gegenüberstellung EVM-Proving-Latenz vs. RISC-V-Proving-Latenz sind in Vitaliks Proposal nicht quantifiziert.

Entwickler mit Solidity-Erfahrung. Rust, C und Go zusammen sind die Systemsprachen, aus denen Linux-Kernel, Browser-Engines, Cloud-Infrastruktur, Datenbanken und Betriebssysteme entstehen. Smart Contracts wären für denselben Developer-Pool schreibbar, aus dem auch die Infrastrukturen kommen. Die Spezial-Community um Solidity bliebe dabei bestehen, würde aber um eine Größenordnung erweitert. Damit wäre die Smart-Contract-Entwicklung keine Spezialdisziplin mehr mit eigener Sprache und eigener Community, sie würde zu einer Domäne der allgemeinen Software-Entwicklung. Die dritte Ebene ist die formale Verifikation. Die RISC-V Sail-Spezifikation ist eine vollständige, akademisch geprüfte formale Beschreibung der Ausführungsumgebung, während die EVM nur über teilweise formalisierte Semantiken einzelner Komponenten verfügt: Runtime-Verification-Modelle für einzelne Opcodes, K-Framework-Formalisierungen ausgewählter Teilmengen, aber keine einheitliche formale Grundlage. Einfachere Ausführungsumgebungen mit klarer spezifizierten Befehlssätzen erlauben schnellere formale Verifikation ihrer Implementierung: den mathematischen Nachweis, dass die konkrete Software genau das tut, was die Spezifikation vorgibt. Dieser Nachweis ist für Ethereum operativ relevant, weil die EVM-Spezifikation von mehreren unabhängigen Client-Implementierungen getragen wird: Softwares in verschiedenen Programmiersprachen, etwa Geth in Go, Nethermind in C#, Besu in Java, Reth in Rust. Jede der Implementierungen muss sich exakt gleich verhalten, damit das Netzwerk Konsens findet. Heute sichern umfangreiche Tests und der Mainnet-Betrieb die Übereinstimmung ab. Eine formal verifizierbare Ausführungsumgebung würde es erlauben, die Übereinstimmung mathematisch zu beweisen. Consensus-Bugs durch abweichende Client-Interpretationen wären damit strukturell ausschließbar, wo Tests und Betrieb sie heute nur unwahrscheinlich machen.[215]

Der Horizont der Potenziale liegt in der Post-Strawmap-Periode nach 2029. RISC-V steht ohne Governance-Verankerung, ohne EIP und ohne Fork-Termin. Zeitlich liegt der Vorschlag hinter der zkEVM: Erst wenn diese deployt und stabilisiert ist, wird die Frage einer RISC-V-basierten Weiterentwicklung operativ.

---

[215] Zur Sail-basierten formalen Spezifikation siehe RISC-V International, „The RISC-V Instruction Set Manual, Volume I: Unprivileged ISA“, mit begleitender Sail-Modellierung. Zu teilweisen EVM-Semantik-Formalisierungen vgl. Runtime Verification (EVM-as-Automaton) und die K-Framework-Modellierungen einzelner Opcodes. Zur Einordnung in die Lean-Ethereum-Philosophie vgl. Vitalik Buterin, „Possible futures of the Ethereum protocol“, Februar 2026.

leanVM als Endzustand der Ausführung

Die EVM steht in einem größeren Protokoll-Gefüge, dessen akkumulierte Komplexität die Ethereum Foundation seit etwa 2024 als eigene Belastung identifiziert. Diese Belastung trifft die EVM unmittelbar.[216] Buterin und andere haben wiederholt benannt, dass die größte strukturelle Aufgabe der nächsten Jahre nicht die weitere Erweiterung ist, sondern die systematische Vereinfachung: weniger Code, klarere Semantiken, formal spezifizierte Komponenten, die ihre Implementierungen beweisbar einhalten.[217] Lean Ethereum ist das Programm, das diese Vereinfachung trägt, und Abschnitt 5.1-B entfaltet es als Gesamtrahmen. Innerhalb dieses Programms markiert leanVM (RES, Horizont jenseits 2029) den postulierten Endzustand der Ausführungsumgebung mit drei definierten Eigenschaften. Die genaue Verzahnung mit der RISC-V-Linie bleibt in den Primärquellen offen.

leanVM definiert sich über drei Dimensionen, die im Zusammenspiel das Vertrauensmodell des Protokolls verändern. Die erste Dimension sind harmonisierte Client-Implementierungen. Client-Diversität ist im heutigen Ethereum eine aktive Ökosystem-Anstrengung, erkämpft über separate Teams, unterschiedliche Programmiersprachen und jahrelange Spezifikations-Koordination. Bugs in einzelnen Clients müssen deshalb durch die Diversität anderer Clients aufgefangen werden. Die leanVM-Architektur würde Client-Diversität aus einer formalen Spezifikation ableiten. Eine formale Spezifikation ist ein Dokument, das jede Instruktion in einer mathematischen Sprache exakt festlegt, ohne Spielraum für Interpretation durch Implementierer. Verschiedene Teams bauen weiterhin verschiedene Implementierungen, in verschiedenen Sprachen, mit verschiedenen Optimierungen, aber ihre Semantik, also ihr Input-Output-Verhalten, wäre mathematisch beweisbar identisch mit der Spezifikation. Das Risiko eines Consensus-Splits durch abweichende Interpretation entfällt. Die zweite Dimension ist die formale Verifizierbarkeit. Die heutige EVM ist empirisch stabil, ihre Korrektheit wird durch jahrelangen Betrieb, umfangreiche Tests und Bug-Bounties belegt, nicht durch mathematischen Beweis. Ein formal verifizierter

[216] Justin Drake (Ethereum Foundation) charakterisiert den ACD-Prozess (All Core Devs) als belastend für die Entwickler-Community: Pro Hard Fork werden typischerweise drei bis fünf EIPs klärungsfähig, während zehn bis dreißig Vorschläge konkurrieren. Lean Ethereum versteht sich nach Drakes Darstellung als Governance-Batching-Strategie, die längere R&D-Phasen mit anschließend gebündelten EIP-Paketen verbindet. Quelle: Bankless-Interview „Ethereum Beast Mode — Scaling L1 to 10k and Beyond", 12. November 2025.

[217] Die Komplexitätsdiagnose ist prominent in Vitalik Buterin, „Possible futures of the Ethereum protocol", sechsteilige Blog-Serie ab Oktober 2024, insbesondere die Teile „The Purge" und die Beiträge zur Lean-Ethereum-Vision. Sie wird fortgeschrieben in Vitaliks Post-Quantum-Roadmap vom 26. Februar 2026 und in Lean-Ethereum-Forschungsbeiträgen auf ethresear.ch in den Jahren 2025 und 2026.

Endzustand würde Implementierungs-Korrektheit aus Spezifikations-Beweisen ableiten. Ganze Bug-Klassen wären in der Folge architektonisch ausgeschlossen. Die dritte Dimension ist die ZK-Nativität. Die EVM verwendet Primitiven, die auf klassischer CPU-Hardware effizient sind: KECCAK256-Hashing für State-Tree-Zugriffe, 256-Bit-Integer-Arithmetik für die meisten Berechnungen, Gas-Accounting für Ressourcen-Kontrolle. All das ist für CPU-Ausführung optimal gewählt, in ZK-Circuits aber teuer: KECCAK256 erzeugt allein pro Hash-Operation tausende Constraints, Gas-Accounting wird mit jeder Instruktion mitgeführt. Die leanVM würde von Anfang an Primitiven wählen, die sich in ZK-Circuits günstig darstellen lassen. Hash-basierte Funktionen wie Poseidon erzeugen in ZK-Circuits um Größenordnungen weniger Constraints als KECCAK256. Die Feld-Arithmetik arbeitet in der algebraischen Struktur des Proof-Systems statt in 256-Bit-Integer-Operationen. Die Datenstrukturen kommen ohne laufende Buchhaltung aus. Damit entfallen die Kosten der nachträglichen ZK-Anpassung, die heute einen großen Teil der Proving-Gesamtkosten ausmachen. Im Zusammenspiel verschieben diese drei Dimensionen das Vertrauensmodell: weg von empirisch etablierter Stabilität, hin zu mathematisch abgesicherter Korrektheit der Laufzeitumgebung. Die Roadmap postuliert den Endzustand, ohne eine konkrete Spezifikation vorzulegen.

Was leanVM für die EVM ist, ist Beam Chain für die Beacon Chain. Justin Drake hat auf der Devcon SEA 2024 den Consensus-Layer-Endzustand skizziert, der seitdem auf ethresear.ch und in Buterins Roadmap vom Februar 2026 weiterentwickelt wird: hash-basierte Kryptographie statt gewachsene Komplexität, Post-Quantum-Sicherheit als Design-Prinzip und formale Verifizierbarkeit auf allen Ebenen.[218] Die substanzielle Entfaltung trägt Abschnitt 5.1-B. Beide Endzustände liegen jenseits 2029 und stehen für dieselbe Designphilosophie der Vereinfachung auf ein formal beherrschbares Minimum.

Während leanVM und Beam Chain noch ausstehen, zeigt sich die Richtung der Entwicklung bereits im aktuellen Governance-Prozess. Zwei EVM-Erweiterungen, die auf den ersten Blick als technische Verbesserungen erscheinen, stehen unter dem Vorbehalt, dass eine langfristige RISC-V-Ablösung sie redundant machen würde. EOF (EVM Object Format, RES, Status offen) hätte die EVM-Bytecode-Struktur durch Code Validation, Static Jumps und Funktionsgrenzen reformiert. Im April 2025 wurde der Vorschlag aus Fusaka entfernt, aus mehreren Gründen, darunter der zunehmend fragliche langfristige Nutzen unter

[218] Justin Drake, „Beam Chain“, Vortrag Devcon SEA 2024; Follow-up-Diskussionen auf ethresear.ch ab Ende 2024; Vitalik Buterin, Roadmap-Update Februar 2026.

RISC-V-Perspektive.[219] EVMMAX (RES) würde bestimmte kryptographische Grundoperationen wie elliptische-Kurven-Multiplikation und modulare Exponentiation deutlich effizienter in der EVM verfügbar machen, was Smart Contracts mit Signatur-Verifikation oder ZK-Beweis-Verifikation günstiger ausführbar macht. Auch der Ansatz steht jedoch unter demselben RISC-V-Redundanz-Vorbehalt. Der Post-Designzustand prägt bereits die Priorisierung heutiger EIPs.

Ethereums Antwort: Rollentrennung

Andere Blockchain-Architekturen haben andere Antworten auf die Skalierungs-Frage gewählt. Eine Richtung erhöht die Hardware-Anforderungen an die Validator-Rolle und akzeptiert dadurch eine höhere Zugangsschwelle zur Netzwerk-Teilnahme. Eine andere reduziert die Zahl der Validatoren und konzentriert die Konsens-Findung auf wenige Akteure. Solana und Monad sind prominente Vertreter der ersten Richtung, BNB Chain der zweiten.[220] Ethereums Antwort ist eine dritte: Rollentrennung. Die Skalierung um den Faktor 100, die Abschnitt 5.2 entfaltet hat, wird erst dadurch möglich, dass keine einzelne Rolle sie allein leisten muss. Der Kern dieser Rollentrennung, so wie 5.2-A sie protokollär verankert hat, lässt sich in drei parallelen Sätzen fassen. Der Validator verifiziert, ohne nachzurechnen. Der Builder konstruiert, ohne zu validieren. Der Prover beweist, ohne Blöcke vorzuschlagen. Damit bildet er eine eigenständige Infrastruktur-Schicht aus, deren Entfaltung Abschnitt 5.3-A′ übernimmt. Keine dieser Rollen könnte die Skalierung allein tragen. Erst ihr Zusammenspiel erzeugt Kapazitätswachstum, ohne dass die Dezentralisierung einer einzelnen Rolle unter die Hardware-Schwelle fällt. Entscheidend ist dabei die Lastverteilung: Builder und Prover dürfen kapitalintensiv werden, weil ihre Outputs von jedem Validator mit minimaler Hardware verifiziert werden. Validator und Proposer bleiben auf Consumer-Hardware, weil sie allein Beweise prüfen. Diese Rollentrennung ist das EIP-invariante Prinzip, das Abschnitt 5.2 als Ganzes zusammenhält.[221]

[219] Fusaka Interop Testing Call, 28. April 2025. Neben der RISC-V-Redundanz-Perspektive wurden in der ACDE-Diskussion auch die Komplexitätskosten der Doppel-Maintenance von Legacy-EVM und EOF sowie der fehlende Application-Layer-Konsens als Gründe dokumentiert. Vgl. EIP-7692 (Meta-EIP, Status stagnant); die Einzel-EIPs (u. a. EIP-3540, EIP-3670, EIP-4200, EIP-4750, EIP-5450) blieben im Draft-Status.

[220] Solana operiert mit etwa 1.000 Validatoren, von denen nach Angabe von Justin Drake (Ethereum Foundation) mehr als die Hälfte in zwei Rechenzentren konzentriert sind, die wenige Dutzend Kilometer voneinander entfernt liegen. Monad operiert mit etwa 100 Validatoren. BNB Chain operiert seit 2024 mit 41 aktiven Validatoren in einer Zwei-Tier-Struktur, vormals 21. Quelle: Bankless-Interview „Ethereum Beast Mode — Scaling L1 to 10k and Beyond", 12. November 2025.

[221] Die Zusammenführung der vier Rollen (Validator, Builder, Proposer, Prover) als EIP-invariantes Prinzip ist eine analytische Synthese der in 5.2-A protokollär verankerten Einzelmechanismen: EIP-7732 (ePBS) für die Proposer/Builder-Trennung, EIP-7928 (BALs) für die Builder-Parallelisierung, EIP-8025 (zkEVM) für die

Die Grenze des Prinzips hat 5.2-D bereits markiert, und die Rollentrennung reicht, so weit sie trägt, bis zum Proposing (vgl. Abschnitt 5.2-D). Das hat eine strukturelle Konsequenz, die über die Kapazitäts-Frage hinausweist. Während Verifikation und Proving durch die Architekturen aus 5.2-A bis 5.2-D architektonisch demokratisierbar werden, bleibt das Block Building an die State-Vorhaltung gebunden, und damit an Hardware-Anforderungen, die mit jeder Skalierungsstufe wachsen. Die Teilnahme-Architektur des Systems wird dadurch asymmetrisch: Wer verifiziert, braucht weniger. Wer baut, braucht mehr.

Die Skalierung erzeugt damit eine Frage, die über die Kapazität hinausgeht: Damit stehen zwei Fragen offen: die nach der Verifizierbarkeit des skalierten Systems und die nach der Teilnahme daran. Die Antwort liegt in der Architektur der Verifikation, in der kryptographischen Basis, die sie trägt, und in der Zugangsschwelle, die sie setzt.

5.3 Verifikation und Zugang

Validieren heißt: Berechnungen tatsächlich nachrechnen. Ein Validator, der einen Block validiert, führt die Transaktionen des Blocks selbst aus, mit derselben EVM-Logik, denselben Gas-Kosten, denselben State-Übergängen, denen der Block-Builder bei der Konstruktion gefolgt ist. Verifizieren bedeutet etwas Allgemeineres: prüfen, ob ein Block korrekt ist, ohne notwendigerweise selbst zu rechnen. In Ethereums historischer Architektur fielen beide Begriffe zusammen, weil das Protokoll keine andere Form der Verifikation kannte als die Re-Execution durch jeden einzelnen Verifizierer. Wer einen Block prüfen wollte, brauchte deshalb die Hardware, die das Nachrechnen trug, und diese Hardware wuchs mit dem Gas Limit mit.

Die zkEVM bricht diese Identität auf. Sie ersetzt Re-Execution durch die Verifikation eines kryptographischen Beweises, dessen Aufwand unabhängig von der Blockgröße bleibt. Damit wird Verifikation auch dort möglich, wo der Verifizierer die Berechnungen weder nachvollziehen will noch kann. Eine zweite Kopplung bleibt jedoch bestehen. Auch eine zk-basierte Verifikation braucht den State als Eingabe. Der Beweis bestätigt: Wenn der Anfangs-State X war und die Transaktionen Y angewendet wurden, ist der End-State Z. Wer aber nicht weiß, dass der Anfangs-State X war, kann die Aussage des Beweises nicht in die Welt einbetten. Der Verifizierer braucht Zugang zu den State-Werten, die der

Prover-Rolle und die Entkopplung des Validators von der Gas-Kapazität. Der Dreisatz als rhetorische Verdichtung findet sich in dieser Form nicht in den Primärquellen; er ist analytische Kondensation des Verfassers.

Block liest und schreibt. Solange er den vollständigen State lokal halten muss, um an diese Werte zu kommen, hängt seine Teilnahme an der Speicherkapazität, die der State beansprucht. Diese zweite Kopplung ist Gegenstand von Abschnitt 5.3.

Der Abschnitt entwickelt die Antwort in drei Schritten. Zuerst verkleinert eine neue State-Datenstruktur die Datenmenge, die ein Verifizierer überhaupt braucht. Dann sichern post-quantum-resiliente Verfahren die kryptographische Basis, auf der diese Verkleinerung beruht. Schließlich senkt eine flexiblere Account-Schicht die Zugangsschwelle, ab der ein gewöhnlicher Akteur das System tatsächlich nutzen kann. Die Reihenfolge ist zwingend. Die kryptographische Basis schützt erst eine reduzierte Datenmenge. Die Reduktion wird erst durch eine langfristig stabile kryptographische Basis verlässlich. Über die Zugangsschwelle entscheidet, ob die ermöglichte Verifikation jemand nutzt, der außerhalb professioneller Infrastruktur steht. Der erste Schritt beginnt bei der Datenstruktur, in der Ethereum seinen State hält.

5.3-A Die neue State-Datenstruktur

Ethereums State umfasst alle Account-Stände, Contract-Storage-Werte und Bytecodes des Netzwerks. Das Protokoll speichert diese Werte als Baum mit mehreren hundert Millionen Blättern. Jedes Blatt enthält einen konkreten Wert, etwa den Token-Stand eines Accounts oder einen einzelnen Storage-Slot eines Smart Contracts. Die Wurzel dieses Baumes ist die State Root, eine kryptographische Zusammenfassung aller Blätter. Der Block Header trägt diese State Root. Wer einen einzelnen Wert prüfen will, etwa den Token-Stand eines bestimmten Accounts, braucht nicht den ganzen Baum. Er braucht einen Witness: einen Beweispfad von dem entsprechenden Blatt bis zur State Root. Ein Verifizierer, der den Witness gegen die State Root prüft, kann die Korrektheit des Werts feststellen, ohne die anderen Blätter zu kennen.

Die Größe eines Witness hängt von zwei Eigenschaften der Tree-Struktur ab. Erstens vom Branching Factor, der Zahl der Kinder, die jeder Knoten im Baum hat. Bei einem Baum mit Branching Factor 16 hat jeder Knoten 16 Kinder, und der Pfad von der Wurzel bis zum Blatt muss an jeder Verzweigung alle 15 Geschwister-Knoten mitführen, sonst lässt sich die Knoten-Berechnung beim Verifizieren nicht reproduzieren. Zweitens vom Commitment Scheme: dem Verfahren, das aus den Werten eines Knotens den kryptographischen Anker des Knotens bildet. Das Commitment Scheme bestimmt, in welcher Form die Geschwister-Knoten überhaupt mitgeführt werden müssen.

Ethereums heutige Datenstruktur, die Merkle Patricia Trie (MPT), hat einen

Branching Factor von 16 und nutzt Keccak-256-Hashes als Commitment Scheme. Die durchschnittliche Witness-Größe pro Account-Zugriff liegt bei rund drei Kilobyte, im schlechtesten Fall bei rund neun.[222] Verkle Trees (EIP-6800, RES, Stagnant) verändern beide Eigenschaften. Sie erhöhen den Branching Factor auf 256 und ersetzen die Keccak-Hashes durch Pedersen Commitments mit Inner Product Arguments. Pedersen Commitments fassen viele State-Werte zu einem einzigen kurzen Anker zusammen. Wer einen einzelnen Wert prüfen will, kann das gegen den Anker tun, ohne die anderen Werte zu kennen oder mitliefern zu müssen. Konkret operieren die Commitments auf der Bandersnatch-Kurve, einer elliptischen Kurve über dem BLS12-381-Skalarfeld. Inner Product Arguments erzeugen einen einzigen kompakten Beweis für den Pfad zur State Root, statt alle Geschwister-Knoten einzeln aufzuzählen. Damit hängt die Witness-Größe nicht mehr von der Tiefe oder Breite des Baums ab. Die durchschnittliche Witness-Größe pro Account-Zugriff sinkt auf rund 200 Byte, der Block Witness im schlechtesten Fall von etwa 18 Megabyte auf rund 1,2 Megabyte. Das entspricht einer Reduktion um den Faktor fünfzehn bis fünfundvierzig.[223]

Die Witness-Reduktion entkoppelt den Verifikations-Aufwand vom State-Volumen. Was ein Verifizierer prüfen muss, hängt nicht mehr von der Größe des State-Trees ab, sondern bleibt für jeden einzelnen Wert auf den kompakten Pfad zur State Root begrenzt. Welche Hardware-Konsequenzen ein Stateless Client daraus zieht, behandelt der nächste Abschnitt. Verkle Trees spielen jenseits der Verifikations-Funktion eine doppelte Rolle. Sie sind die State-Datenstruktur, auf der spätere architektonische Verfeinerungen aufbauen, und sie sind die Witness-Form, die Native Rollups für ihre EXECUTE-Precompile brauchen, weil MPT-Witnesses für den Zweck prohibitiv groß wären.

Verkle ist deployment-fähig. Kaustinen-7 läuft seit Ende 2024 als dediziertes Verkle-Testnet in Multi-Client-Konfiguration, mit Geth, Nethermind, Besu und EthJS auf der Execution-Seite und Lighthouse, Lodestar und Teku auf der Consensus-Seite.[224] Reth und Prysm fehlen, das sind Lücken im Multi-Client-Bild, aber keine Sperren des Pfades. EIP-7612 und EIP-7748 stellen benannte

[222] Witness-Größen für die Merkle Patricia Trie: durchschnittlich rund 3 KB pro Account-Zugriff, im Worst Case bis rund 9 KB; Block Witness im Worst Case bis ca. 18 MB. Vgl. Ethereum Foundation Research, Verge Documentation; sowie EIP-6800, Rationale-Sektion.

[223] Witness-Größen für Verkle Trees: durchschnittlich rund 200 Byte pro Account-Zugriff, Block Witness im Worst Case ca. 1,2 MB. Die Reduktion um den Faktor 15–45× bezieht sich auf den Vergleich avg-zu-avg bzw. worst-zu-worst zwischen MPT und Verkle. Quellen: EIP-6800; EF Verkle Tree Documentation, Stand Februar 2026.

[224] Implementierungsstatus Kaustinen-7 per Februar 2026: Geth (Work in Progress), Nethermind (Stateless Client komplett), Besu (Java Libraries und Bonsai Interface), EthJS (Implementation aktiv); auf Consensus-Seite Lighthouse, Lodestar, Teku. Reth und Prysm ohne Verkle-Implementierung; Erigon implementiert, aber nicht auf Testnet aktiv. Quelle: EF Verkle Implementation Tracker.

Migrationsstrategien mit gemessenen Benchmarks bereit. Wenn die Governance den Headliner-Slot zuteilt, kann Verkle in einem der nächsten Forks aktiviert werden. Dieser Pfad steht allerdings still: Verkle trägt die Kennzeichnung Stagnant, weil die Ethereum Foundation die langfristige Richtung auf Binary Trees priorisiert hat und die Deployment-Reife bislang in keine Fork-Zuteilung gemündet ist.

Verkle oder Binary: die Quantenfrage

Diese Implementierungsreife verdeckt jedoch eine kryptographische Schwäche, die unter klassischer Hardware nicht ins Gewicht fällt. Pedersen Commitments und Inner Product Arguments stützen sich auf das ECDLP über der Bandersnatch-Kurve. Das ECDLP lautet: Gegeben seien ein Punkt P und ein Punkt Q auf der Kurve. Gesucht ist die Zahl k, sodass Q gleich k mal P ist. Klassische Computer können diese Zahl bei den verwendeten Kurven-Größen nicht in praktikabler Zeit finden. Ein ausreichend leistungsfähiger Quantencomputer kann sie mit Shors Algorithmus direkt berechnen, in einer Laufzeit, die polynomiell mit der Schlüssellänge wächst statt exponentiell. Damit fällt das ECDLP, und mit ihm fallen Pedersen Commitments und IPA. Ein Forschungspapier aus dem Dagstuhl-Umfeld hält fest, dass Verkle Trees nicht sicher gegen Quantencomputer sind, und das Design dynamischer Vector Commitments, die zugleich asymptotisch optimal, praktisch effizient und post-quantum-resilient wären, bleibt eine offene Forschungsfrage.[225] Buterin charakterisiert Verkle vor diesem Hintergrund als Übergangslösung, die Zeit verschafft, bis STARK-basierte und verwandte Verfahren reif sind.[226]

Binary Trees (EIP-9257, RES) ersetzen Bandersnatch und IPA durch STARK-kompatible Hash-Funktionen. Hash-Funktionen lassen sich durch Shors Algorithmus nicht beschleunigen. Die effektive Sicherheit halbiert sich höchstens unter Grovers Algorithmus, was sich durch hinreichend lange Hashes kompensieren lässt. Der Implementierungsstand liegt jedoch deutlich zurück. Es gibt kein Multi-Client-Testnet auf dem Niveau von Kaustinen-7 und keine Migration-EIPs auf vergleichbarem Reifegrad. Schätzungen aus dem Forschungsumfeld kalkulieren, dass ein Wechsel zu Binary Trees den Verifikations-

[225] Boneh, Bünz, Fisch et al., Dagstuhl-Reports zu Vector Commitments und Post-Quantum-Sicherheit; vgl. auch Nomos Research, „Verkle Trees and Quantum Resistance", 2024. Paraphrasiert: Verkle Trees sind nicht post-quantum-sicher, und die Konstruktion dynamischer Vector Commitments mit zugleich asymptotisch optimalem, praktisch effizientem und post-quantum-resilientem Verhalten bleibt offen.

[226] Vitalik Buterin, „Possible futures of the Ethereum protocol — The Verge", 2024; Roadmap-Update vom Februar 2026. Verkle wird darin als Übergangstechnologie charakterisiert, deren Funktion darin besteht, Statelessness frühzeitig zu ermöglichen, während STARK-basierte und post-quantum-sichere Verfahren noch reifen.

und L2-Garantie-Strang um zwölf bis achtzehn Monate verschieben würde.[227]

Das EF Protocol Priorities Update vom 18. Februar 2026 nennt erstmals „a move to binary trees and statelessness" als langfristige Richtung. Damit markiert die Ethereum Foundation eine strategische Priorisierung gegenüber Verkle. Guillaume Ballet, einer der EIP-6800-Autoren, charakterisiert Binary Trees in der Folge als „a serious alternative".[228] Zwei Szenarien sind damit offen. Im einen Szenario wird Verkle als Brückenlösung deployt, mit langfristiger Architektur auf Binary-Trees-Basis. Im anderen Szenario revidiert die Roadmap die Verkle-Deployment-Entscheidung zugunsten eines direkten Binary-Pfads. Die Spannung dieser Entscheidung lässt sich konkret benennen. Verkle ist heute deployment-fähig, trägt aber die langfristige Stabilität nicht, weil seine kryptographische Basis vor Quantencomputern fällt. Binary Trees tragen die langfristige Stabilität, sind aber heute nicht deployment-fähig, weil ihre Implementierung dem Verkle-Pfad zwölf bis achtzehn Monate hinterherhinkt. Die Roadmap entscheidet damit über das Verhältnis zwischen kurzfristiger Verfügbarkeit und langfristiger Robustheit. Diese Entscheidung fügt sich in das Lean-Ethereum-Programm ein, das Post-Quantum-Sicherheit als Designprinzip versteht.

Die Migration ohne Downtime

Der Migrationspfad zur neuen State-Datenstruktur ist als Bundle dreier EIPs konzipiert, das gegenüber der Verkle-vs.-Binary-Wahl weitgehend invariant bleibt. EIP-7612 (Overlay Tree, RES, ohne Fork-Zuordnung) löst das Problem des State-Wechsels ohne Mainnet-Downtime. Bei Fork-Aktivierung schaltet das Protokoll den neuen Tree als Overlay parallel zur bestehenden MPT, und die MPT wird schreibgeschützt eingefroren. Alle State Writes laufen ab diesem Zeitpunkt in den neuen Tree. Reads suchen zuerst dort, fallen bei Bedarf auf die MPT zurück und migrieren den gefundenen Wert beim nächsten Write. Der Big-Bang-Wechsel, der einen Offline-Zeitraum von rund einem Monat erfordert hätte, wurde verworfen.[229]

EIP-7748 (State Conversion, RES, ohne Fork-Zuordnung) regelt die Hintergrund-Migration. Pro Block konvertiert das Protokoll eine feste Anzahl

[227] Schätzwert aus dem EF-Forschungsumfeld; siehe ethresear.ch-Diskussion zu Binary Trees vs. Verkle Trees, Februar 2026. Die Spanne von zwölf bis achtzehn Monaten ist eine konsolidierte Einschätzung mehrerer Beiträge, kein offiziell quantifizierter Roadmap-Aufschlag, und sollte als Größenordnung gelesen werden.

[228] Ethereum Foundation, Protocol Priorities Update, 18. Februar 2026. Guillaume Ballet, ethresear.ch-Beitrag zu Binary Trees als ernsthafter Alternative zu Verkle, Februar 2026.

[229] EIP-7612 (Verkle State Transition via an Overlay Tree). Autoren: Guillaume Ballet, Ansgar Dietrichs, Tanishq Jasoria, Gajinder Singh, Ignacio Hagopian. Die verworfene Big-Bang-Migration hätte bei Mainnet-State-Größe rund einen Monat Offline-Konversion erfordert.

Key-Values von der MPT in den neuen Tree. Benchmarks auf einem AMD Ryzen 7 5800U messen rund 300 Millisekunden für 10.000 Keys pro Block, woraus eine Gesamtkonversion von etwa fünfzehn Tagen folgt. Die Migration ist vorübergehend, aber planbar.[230] EIP-4762 (Statelessness Gas Cost Changes, RES, ohne Fork-Zuordnung) bildet die neuen Zugriffskosten im Gas-Schedule ab. Pro Code-Chunk und pro Storage-Slot kostet ein Zugriff 200 Gas, mit Adjacent-Storage-Optimierung für aufeinanderfolgende Slots derselben 256er-Gruppe. Die durchschnittliche Gas-Erhöhung liegt bei sechs bis zwölf Prozent.[231]

Die drei EIPs lösen die Migration als eigenständiges Problem. Welches Commitment-Schema verwendet wird, entscheidet die Tree-Wahl, während das Migrations-Bundle bestimmt, wie der Wechsel verwaltbar bleibt. Beide Fragen sind separat lösbar. Die Komplexität dieses Wechsel-Verfahrens ist erheblich. Guillaume Ballet hat die Verkle-Migration „on the scale of the Merge if not worse in terms of complexity" genannt.[232] Diese Komplexität liegt in der Implementierung der Migration.

Die State-Datenstruktur ist der erste Schritt der Verifikations-Architektur, die Abschnitt 5.3 entwickelt. Sie senkt die Datenmenge, die ein Verifizierer braucht, vom vollständigen State auf einzelne Witnesses. Welche Datenstruktur Ethereum konkret deployt, Verkle oder Binary, entscheidet über die langfristige kryptographische Robustheit. Die architektonische Logik der Reduktion bleibt davon unberührt. Pedersen Commitments, Inner Product Arguments und die Bandersnatch-Kurve sind keine Sonderausstattung der State-Migration. Sie gehören zu einer breiteren Schicht spezialisierter kryptographischer Bausteine, die das Protokoll oberhalb der EVM bereitstellt. Diese Schicht entfaltet der nächste Abschnitt.

5.3-A′ Die Erweiterungs-Schicht oberhalb der EVM

Es gibt im Ethereum-Protokoll Operationen, die kryptographisch teuer sind: Beweise erzeugen, Signaturen verifizieren, Blob-Daten gegen Commitments prüfen, demnächst auch quantenresistente Signaturen aggregieren. In der EVM können sie nicht effizient laufen, weil die EVM keinen Befehl für eine 256-Bit-Modular-Multiplikation oder eine elliptische-Kurven-Punktaddition kennt. Sie

[230] EIP-7748 (State Conversion to Verkle Tree). Benchmark: 10.000 Keys pro Block in rund 300 ms auf AMD Ryzen 7 5800U; bei einer 12-Sekunden-Slot-Cadence ergibt sich eine Gesamtkonversion in ca. 15 Tagen.

[231] EIP-4762 (Statelessness Gas Cost Changes). Code-Chunk-Access (31 Bytes) und Storage-Slot-Access kosten jeweils 200 Gas; die Adjacent-Storage-Optimierung reduziert die Folgekosten innerhalb derselben 256er-Slot-Gruppe. Durchschnittliche Gas-Erhöhung: sechs bis zwölf Prozent (EIP-4762 Impact-Analyse).

[232] Guillaume Ballet (Ethereum Foundation), zitiert in der ACDE-Diskussion zur Verkle-Migration; vgl. All Core Devs Call Notes, 2024–2025.

müsste solche Operationen aus tausenden Grundbausteinen aufbauen, deren Gas-Kosten sich addieren. Eine native Implementierung in der Client-Software derselben Operation kommt dagegen in Mikrosekunden aus, da die CPU einen direkten Befehl für die Multiplikation breiter Zahlen kennt. Genau diesen Engpass zwischen EVM-Geschwindigkeit und nativer Geschwindigkeit adressiert die Erweiterungs-Schicht. Precompiles und Prover führen teure Operationen außerhalb der EVM aus und binden ihre Korrektheit über kryptographische Beweise oder Konsens-Garantien an die EVM zurück. Auf ihr ruhen vier Funktionen des Zielbilds: die zkEVM-Verifikation, die Post-Quantum-Migration der Signaturen, die Native L1 Privacy und die Verifikation des reduzierten State aus 5.3-A. Wo 5.3-A zwei alternative Tree-Optionen diskutiert, entfaltet 5.3-A′ zwei zusammenwirkende Bausteine der Erweiterungs-Schicht für die rechnerische Arbeit auf der reduzierten Datenmenge. Der Begriff Erweiterungs-Schicht ist eine analytische Setzung dieser Arbeit und keine etablierte Bezeichnung der Quellen. Die Primärquellen diskutieren die on-chain Precompiles und die off-chain Prover-Pipeline überwiegend getrennt, hier werden sie zusammengefasst, da sie eine gemeinsame architektonische Funktion erfüllen.

Die Erweiterungs-Schicht besteht aus zwei Teilen: die on-chain Precompiles und die off-chain Prover-Pipeline. Off-chain heißt hier: außerhalb des Konsens-Protokolls, sodass der Prover nicht in den Slot-Zyklus eingebunden ist und seine Beweise erst nach ihrer Erzeugung in das Protokoll einfließen. Die On-chain Precompiles erweitern die EVM um Operationen, die sie selbst nicht effizient leisten kann, etwa die Verifikation einer BLS-Signatur oder eines KZG-Commitments. Die off-chain Prover-Pipeline erzeugt für jeden Block einen kryptographischen Beweis seiner korrekten Ausführung. Ein Verifizierer kann diesen Beweis on-chain prüfen, ohne die gesamte Block-Ausführung wiederholen zu müssen. Beide verfolgen dasselbe Ziel: teure Operationen aus der EVM-Bytecode-Ausführung herauszuziehen. Precompiles tun das für einzelne kryptographische Operationen, die Prover-Pipeline für die gesamte Block-Ausführung. Die Verifikation eines Prover-Beweises auf der on-chain Seite verwendet ihrerseits Precompiles als kryptographische Bausteine. Die beiden Bausteine sind unterschiedlich weit gereift. Heute sind die Precompiles im Mainnet aktiv, während die Prover-Pipeline im Designzustand der Roadmap noch nicht durch Hard Fork verankert ist. Der Prover als Akteur folgt aus der Rollentrennung aus 5.2: Wer die Blöcke beweisen soll, ist ein anderer als wer sie baut, vorschlägt oder validiert.

Die Precompiles sind heute in einer ersten Stufe etabliert und wachsen über zukünftige Hard Forks weiter. Drei Operationen sind aktuell aktiv und decken die kryptographischen Klassen ab, die die EVM nach dem heutigen Stand

braucht. BLS-Signaturen tragen die Validator-Aggregation der Beacon Chain (EIP-2537, IMPL Pectra). KZG-Commitment-Verifikation prüft die Blob-Daten der Rollups (EIP-4844, IMPL Cancun). secp256r1-Verifikation öffnet die Passkey-Authentifizierung der Accounts (EIP-7951, IMPL Pectra). In der Roadmap angelegt sind zwei weitere Bausteine. EVMMAX (EIP-6690, RES) beschleunigt die modulare Arithmetik, mit dem RISC-V-Vorbehalt aus 5.2-E. Eine geplante Familie von Post-Quantum-Precompiles (RES, ETH2030-Linie) umfasst die gitterbasierten Operationen und STARK-Verifikations-Bausteine.

Die Akkumulation der Schicht verläuft asymmetrisch zwischen Protokoll und Anwendung. Hard Forks aktivieren neue Precompiles diskret, in scharfen Sprüngen alle sechs bis neun Monate. Die Anwendung in Smart Contracts diffundiert dagegen kontinuierlich über Jahre. Eine Precompile kann jahrelang im Protokoll existieren, bevor sie in den meistgenutzten Verträgen ankommt. Das ist die normale Geschwindigkeit, mit der sich Smart-Contract-Adoption entwickelt. Die Erweiterungs-Schicht entsteht damit als langsame Konzentration über mehrere Hard-Fork-Zyklen.

Der Prover als neuer Akteur

Die Prover-Pipeline bringt einen neuen ökonomischen Akteur ins Protokoll, dessen Hardware-Anforderungen oberhalb des Validator-Niveaus und unterhalb des Rechenzentrums-Niveaus liegen. Das EF-Profil für Realtime Proving fixiert die Schwelle über zwei Werte: eine Kapitalausstattung von höchstens 100.000 US-Dollar und eine Leistungsaufnahme von höchstens 10 Kilowatt, jeweils für ein vor Ort betriebenes Setup.[233] Die Spanne liegt oberhalb des Validator-Setups, dessen Investitionskosten im niedrigen vierstelligen Bereich angesiedelt sind. Sie liegt unterhalb eines Hyperscaler-Rechenzentrums, dessen Investitionen in den siebenstelligen Bereich reichen. Der Prover gehört damit weder in die Validator-Klasse noch in die Rechenzentrums-Klasse, sondern bildet eine eigene ökonomische Schicht zwischen beiden. Die Schwelle ist nicht statisch, denn die zkVM-Teams haben ihre GPU-Anforderung in den letzten Monaten um etwa drei Viertel reduziert. Damit verlagern sich die Investitionskosten in den Bereich tat-

[233] EF-Profil für Realtime Proving: Ethereum Foundation Blog, „Shipping an L1 zkEVM #1: Realtime Proving", 10. Juli 2025 (Sophia Gold). Die Spezifikation umfasst neben den im Fließtext genannten zwei konstitutiven Werten drei weitere Parameter: eine Latenz-Anforderung von höchstens zehn Sekunden für 99 Prozent der Mainnet-Blöcke, eine Beweis-Sicherheit von mindestens 128 Bit und eine Proof-Größe von höchstens 300 KiB ohne Trusted Setups. Sämtliche Werte gelten als Mindestanforderung für Realtime-Proving im Produktivbetrieb.

sächlicher Heim-Prover-Setups.[234] Zwei Punkte trennen die Prover-Pipeline heute noch vom Designzustand: die Realtime-Proving-Schwelle und die ökonomische Architektur der Prover-Bezahlung. 99 Prozent der Mainnet-Blöcke sollen in zehn Sekunden bewiesen sein, doch die Mainnet-Realität liegt heute noch oberhalb der Soll-Spanne. Bei der Bezahlung legt die Roadmap weder eine Vergütung im Protokoll noch eine vollständige Lösung außerhalb des Protokolls fest. Abschnitt 5.5-B greift das Defizit unter dem Aspekt der MEV- und Builder-Ökonomie auf.

Um den Chokepoint einer einzelnen zkVM-Implementierung zu vermeiden, verankert EIP-8025 (zkEVM Optional Execution Proofs, aktive EF-Roadmap) eine Akzeptanz-Schwelle. Drei Beweise aus fünf verschiedenen zkVM-Implementierungen müssen für einen Block vorliegen, bevor er in der vollen Sicherheits-Stufe gilt.[235] Die Schwelle zielt auf Software-Diversität in der zkVM-Implementierung, während die Akteurs-Diversität der Prover davon unberührt bleibt. Ein einzelner Prover kann seine Beweise mit drei verschiedenen Implementierungen erzeugen und damit die Schwelle erfüllen. Entscheidend ist nicht die Marktkonzentration der Prover, sondern die Vielfalt der Software wie SP1, RISC Zero, Pico Prism oder Zisk. Damit überträgt sich die Logik der heutigen Client-Diversität auf die Prover-Pipeline, ohne in die Marktstruktur der Prover einzugreifen. Ein Bug in einer einzelnen zkVM verfälscht den Konsens nicht, sofern die Mehrheit der unabhängigen Proofs ihn nicht reproduziert. Die Liveness bleibt unberührt, da im 1-aus-N-Modell ein einzelner ehrlicher Prover für die Beweis-Generierung genügt. Auch hier bleiben zwei Punkte offen: der Reifegrad der zkVM-Implementierungen und die Hard-Fork-Aktivierung von EIP-8025 selbst. Die EF-Sicherheits-Meilensteine für 2026 sehen drei Stufen vor, in denen die Sicherheits- und Performance-Anforderungen schrittweise verschärft werden. Die volle 3-aus-5-Tragfähigkeit hängt an der letzten Stufe.[236] EIP-8025 bleibt bis zur Hard-Fork-Aktivierung Architektur-Aussage und greift in der heutigen Konsensus-Regel nicht.

---

[234] Hardware-Trajektorie der RTP-Kohorte: Ethproofs 2025/2026 (HackMD, 6. Dezember 2025, Will Corcoran). Pico Prism reduziert seine Anforderung von 64 auf 16 RTX-5090-GPUs für 99-Prozent-Proving in unter zwölf Sekunden, was die GPU-Kosten von etwa 128.000 US-Dollar auf rund 32.000 US-Dollar senkt. Die Drei-Viertel-Reduktion ist nicht für alle Implementierungen der RTP-Kohorte repräsentativ, sondern zeigt die obere Grenze des bisher erreichten Implementierungs-Fortschritts.

[235] EIP-8025 und 3-aus-5-Multi-Prover-Mechanik: verankert im EIP-8025-Design (zkEVM Optional Execution Proofs) und in der Ethereum-Magicians-Diskussion zur L1-zkEVM-Roadmap (26. Januar 2026, Kevaundray Wedderburn, EF zkEVM-Team) als Diversitäts-Architektur entwickelt.

[236] Drei Sicherheits-Meilensteine 2026 (Februar, Mai, Dezember): Ethereum Foundation Blog, „Shipping an L1 zkEVM #2: Security Foundations" (18. Dezember 2025). Die im Verlauf der drei Meilensteine erzielte Verbesserung der Proof-Latenz wird in den EF-Daten als Reduktion von 16 Minuten auf 16 Sekunden geführt, was einer 45-fachen Kostenreduktion entspricht.

Viele Beweise, ein Master-Beweis

Die Erweiterungs-Schicht enthält eine Aggregations-Mechanik, die viele einzelne Beweise zu einem Master-Beweis zusammenfasst. STARK-Beweise haben dafür eine rekursive Eigenschaft: Ein übergeordneter Beweis verpackt die Verifikator-Logik mehrerer untergeordneter Beweise in sich. Der Verifikations-Aufwand des Master-Beweises bleibt damit annähernd unabhängig von ihrer Zahl. Auf der Mempool-Ebene tritt eine zweite Aggregations-Stufe hinzu, wo das Protokoll die Signaturen mehrerer Transaktionen in einem 500-Millisekunden-Takt sammelt und zu einem einzigen Aggregations-Proof zusammenfasst.[237] Auf der Mechanik beruht zuerst die Post-Quantum-Migration der Signaturen, da ihre unaggregierten Verifikationskosten andernfalls das Transaktions-Budget sprengen würden. Die Roadmap-Quantifizierung nennt die Spanne von ECDSA bis STARK: 3.000 Gas für eine klassische ECDSA-Signatur, 200.000 Gas für eine unaggregierte hash-basierte Einzelsignatur, 10 Millionen Gas für einen STARK ohne Aggregation. In der Aggregations-Charge kehren die amortisierten Pro-Signatur-Kosten in das Transaktions-Budget zurück.[238] Validation Frames (EIP-8141, PLAN, CFI Hegotá Non-Headliner) bringen das Aggregations-Vehikel in das Transaktions-Format und machen es für alle Anwendungsklassen verfügbar, die solche ZK-Wrappers benötigen. Neben der PQ-Migration ruhen drei weitere Anwendungsklassen auf derselben Mechanik: Native Privacy-Wrappers, Data-Availability-Sampling-Proofs und Application-Layer-ZK-Beweise externer Protokolle. Die Architektur ist im Designzustand vollständig beschrieben, hängt für die on-chain Verifikation der aggregierten quantenresistenten Beweise aber an der noch nicht aktivierten PQ-Precompile-Familie.

Die Erweiterungs-Schicht folgt einer Glue-and-Coprocessor-Architektur, in der die EVM Daten und Aufrufe koordiniert und Precompiles wie Prover die teuren Operationen übernehmen. Das Bild aus der Hardware-Ebene ist die Beziehung zwischen CPU und GPU. Die EVM verhält sich wie eine universelle CPU: Sie kann jede Operation ausführen, ist aber für teure spezielle Aufgaben nicht optimal. Precompiles und Prover verhalten sich wie spezialisierte Chips, die jene Operationen schnell ausführen, die in der EVM langsam wären. Buterin hat das

[237] 500-Millisekunden-Tick als Mempool-Aggregations-Takt: Vitalik Buterin, „Possible Futures of the Ethereum Protocol — Post-Quantum Roadmap“, 26. Februar 2026. Die Quelle nennt den Tick als Design-Anker, ohne die genaue Verzahnung mit den Hard Forks zu spezifizieren.

[238] Gas-Kostenspanne ECDSA / unaggregierte hash-basierte Signatur / STARK ohne Aggregation: Vitalik Buterin, PQ-Roadmap, ebd. Die amortisierten Pro-Signatur-Kosten in der Aggregation werden in der Quelle qualitativ als „near-zero long-term“ beschrieben, ohne eine konkrete Per-Signatur-Quantifizierung zu nennen.

Schema 2024 an einer EVM-Trace empirisch belegt. Von den 46.924 Gas einer einfachen ENS-Hash-Aktualisierung entfielen rund 73 Prozent auf eine kleine Zahl strukturierter teurer Operationen wie Storage-Reads, -Writes, Logging und Kryptographie.[239] Aus dem Muster lässt sich die Richtung der Roadmap-Entwicklung ablesen. Die Effizienz-Arbeit verlagert sich nach außen: zu Precompile-Erweiterungen für teure Kryptographie und zur Prover-Pipeline für teure Verifikation. Ein tieferer Opcode-Umbau der EVM selbst unterbleibt. Die Rückstellung von EOF aus Fusaka folgt der Verschiebung, da ein EVM-internes Bytecode-Format-Refactoring weniger Wirkung erwarten lässt als die parallele Entwicklung der Koprozessoren.

Damit ist die Erweiterungs-Schicht als architektonische Grundlage beschrieben, auf dem die Post-Quantum-Migration aus 5.3-D und die Native-L1-Privacy-Aussage aus 5.1-C ruhen. Die PQ-Migration selbst ist ein Querschnitts-Phänomen mit vier Schwachstellenklassen, die Abschnitt 5.3-D einzeln entfaltet. Für den unmittelbar folgenden Abschnitt 5.3-B liefert sie eine zentrale Voraussetzung. 5.3-A hat gezeigt, wie das Protokoll die Daten-Menge eines Blocks reduziert: Witnesses auf Verkle- oder Binary-Basis ersetzen den State-Tree-Pfad durch einen kompakten Beweis-Pfad. 5.3-A′ hat gezeigt, wie das Protokoll die Rechen-Menge eines Blocks reduziert: STARK-Beweise ersetzen die Re-Execution des Blocks durch eine konstante Verifikation. Beide Reduktionen wirken zusammen, und ihre gemeinsame Konsequenz ist eine architektonische Verschiebung. Wer einen Block validieren will, muss weder den gesamten State herunterladen noch die gesamte Block-Ausführung wiederholen. Er prüft einen kompakten Witness und verifiziert einen kurzen Beweis. Genau dies ist die Voraussetzung der Stateless Verification, deren Hardware-Konsequenz Abschnitt 5.3-B entfaltet. Die Erweiterungs-Schicht trägt damit nicht nur die kryptographische Substanz der späten Roadmap-Funktionen, sondern auch die rechnerische Voraussetzung der Stateless Clients aus 5.3-B.

5.3-B Die Hardware-Konsequenz der Stateless Verification

Ein Stateless Client verifiziert Blöcke, ohne den State lokal zu halten oder die Block-Ausführung zu wiederholen, und damit wird die Verifikation aus einer Server-Aufgabe zu einer Funktion, die auf Consumer-Hardware läuft. Die Voraussetzung dafür liefern die beiden Reduktionen der vorangehenden Abschnitte:

[239] Glue-and-Coprocessor-Architektur und EVM-Trace: Vitalik Buterin, „Glue and Coprocessor Architectures“, September 2024. Die Trace bezieht sich auf eine Transaktion zur Aktualisierung des IPFS-Hashes des Blog-ENS-Eintrags. Die 73-Prozent-Marke umfasst die EVM-Ausführung allein, mit Basiskosten erweitert ergibt sich ein Anteil von rund 85 Prozent.

Die Witness-Reduktion entkoppelt die Verifikation von der lokalen State-Speicherung, die Beweis-Verifikation entkoppelt sie von der Re-Execution. Damit fällt der Faktor weg, der die heutige Vollverifikation hardwareseitig dominiert, denn die Pflicht zur lokalen State-Speicherung hat die Hardware-Last der Execution gegenüber der leichten Konsens-Verifikation erst erzeugt. Der Stateless Client kennt diese Hardware-Last nicht mehr, weil er den State pro Block als Witness empfängt und die Korrektheit gegen die State Root prüft, ohne den Pfad der Berechnung lokal nachzuvollziehen.

Das resultierende Hardware-Profil verschiebt die Anforderungen eines Verifizierungs-Node um drei bis vier Größenordnungen. Jeder der vier Hardware-Faktoren leitet sich aus einer der beiden Reduktionen ab, deren technische Mechanik in den vorangehenden Abschnitten dargestellt wurde. Die Storage-Anforderung sinkt von 2 bis 4 Terabyte auf unter 100 Megabyte, eine Reduktion um den Faktor 20.000 bis 40.000.[240] Der Arbeitsspeicher sinkt von 16 bis 64 Gigabyte auf unter 1 Gigabyte, um den Faktor 16 bis 64. Die Rechenanforderung sinkt von 4 bis 8 CPU-Kernen auf einen einzelnen Kern, weil eine Beweis-Verifikation mit konstanter Kostengröße die lineare Re-Execution ersetzt. Stunden bis Tage beansprucht heute die initiale Synchronisation, also der Aufbau der lokalen State-Datenbank aus dem Netzwerk, und sie bildet die größte Einstiegshürde für neue Node-Betreiber. Sie kollabiert auf Sekunden, sofern der Client keinen historischen State mehr aufbaut. Die Hardware-Klasse verlagert sich damit von der professionellen Server-Konfiguration auf das Spektrum der Consumer-Geräte: Smartphone, Browser-Tab, Raspberry Pi und Home-Server.

[240] Hardware-Reduktion durch Stateless Clients: Storage von 2–4 TB auf unter 100 MB (Faktor 20.000–40.000), RAM von 16–64 GB auf unter 1 GB (Faktor 16–64), CPU von 4–8 Cores auf 1 Core, Sync-Zeit von Stunden/Tagen auf Sekunden. Die Reduktionsfaktoren beziehen sich auf die Übergangs-Spanne zwischen heutigem Full-Node-Profil und projiziertem Stateless-Profil unter Verkle- oder Binary-Tree-Migration. Sie setzen voraus, dass der Client keinen historischen State mehr lokal aufbaut und den State pro Block als Witness empfängt.

Nur eine von drei Rollen

Die Reduktion betrifft jedoch nur eine der drei Rollen, die das Protokoll auf der Hardware-Seite trägt. Der Verifizierer im engeren Sinne folgt dem Profil des vorigen Absatzes und betreibt seine Node auf Consumer-Hardware, da er weder Blöcke produziert noch Transaktionen ordnet. Der Validator, der im Designzustand als zkAttester Beweise verifiziert, sinkt in seiner Compute-Anforderung auf das gleiche Profil. Er behält jedoch eine Hardware-Dimension, die sich der Reduktion entzieht: die Bandbreite, also die Netzwerkanbindung für die Block-Propagation. Sie skaliert linear mit dem Gas Limit, denn die Block-Größe selbst skaliert. Bei einem hypothetischen Limit von 5.000M Gas wachsen die Blöcke auf eine Größenordnung von 100 bis 500 Megabyte pro Slot.[241] Eine solche Größenordnung verlangt eine Netzwerkanbindung, die heutige Heim-Anschlüsse jenseits der Spitzenklasse überfordert. Die heutige Validator-Empfehlung liegt bei rund 25 Megabit pro Sekunde, eine Anbindung, die der Skalierungspfad in den Bereich mehrerer Gigabit verschiebt. Die Compute-Anforderung ist damit vom Gas Limit entkoppelt, die Bandbreiten-Skalierung mit dem Gas Limit bleibt bestehen, und sie definiert die Hardware-Grenze des Designzustands für die Attestations-Rolle. Der Block Builder bleibt schließlich in der Rechenzentrums-Klasse. Er hält den vollständigen State, um MEV zu extrahieren und Block-Kandidaten parallel zu komponieren, und er konkurriert mit anderen Buildern in einem Latenz-Race im Millisekunden-Bereich. Die Wettbewerbs-Infrastruktur der Rolle wird heute auf rund 200.000 US-Dollar pro Monat veranschlagt.[242] Die naive Lesart, Stateless Clients senken die Hardware-Anforderungen pauschal, übersieht damit die strukturelle Differenzierung. Die Reduktion gilt für die Verifikations-Seite vollständig, für die Attestations-Seite mit offener Bandbreiten-Frage, für die Builder-Seite gar nicht.

[241] Bandbreiten-Skalierung mit Gas Limit: Bei einem hypothetischen Gas Limit von 5.000M wachsen die Blöcke auf eine Größenordnung von 100–500 MB pro Slot. Heutige Validator-Empfehlung: rund 25 Megabit pro Sekunde im Mainnet-Profil. Der Skalierungspfad verschiebt diese Anforderung in den Bereich mehrerer Gigabit. Die Bandbreiten-Anforderung ist die verbleibende Hardware-Skalierungsfrage für Validatoren, da die Compute-Last über zkEVM-Attestation entkoppelt ist, die Bandbreite jedoch linear mit der Block-Größe wächst.

[242] Builder-Latenz-Race und Infrastrukturkosten: Der Wettbewerb zwischen Buildern operiert in der späten Slot-Phase im Millisekunden-Bereich. Empirische Daten zeigen einen Peak der Winning Bids zwischen 2000 und 2500 Millisekunden in den Slot, mit fast vollständiger Reorg-Sicherheit für Bids vor 1500 Millisekunden und häufigen Orphan-Ereignissen für Bids nach 2500 Millisekunden. Die monatlichen Infrastrukturkosten für kompetitive Builder werden auf rund 200.000 US-Dollar veranschlagt, getrieben durch geographische Proximity zu Relays und Proposern, hochperformante Compute-Cluster und private Order-Flow-Akquisition. Die Hardware-Klasse der Builder-Rolle ist damit nicht durch eine einzelne Compute-Anforderung definiert. Sie entsteht aus der Kombination aus lokaler State-Speicherung, Compute-Kapazität, niedriger Netzwerk-Latenz und privater Order-Flow-Infrastruktur.

Heute beruht die Hardware-Schichtung der drei Rollen auf einer Out-of-Protocol-Konstruktion, die ePBS in den Designzustand verlagert. MEV-Boost übernimmt die Trennung zwischen Proposer- und Builder-Hardware als Out-of-Protocol-Sidecar und routet Stand Q1 2026 rund 96 Prozent aller Mainnet-Blöcke.[243] ePBS verlagert dieselbe Trennung ins Protokoll und macht sie zum verbindlichen Element des Slot-Ablaufs.[244] Die Hardware-Folge der Verlagerung ist die institutionelle Absicherung dessen, was die Architektur ohnehin verlangt. Die Proposer-Funktion bleibt auf das Consumer-Hardware-Profil tragbar, die Builder-Funktion bleibt in der Rechenzentrums-Klasse. Die Protokoll-Schrittfolge verankert die Trennung damit strukturell, wo sie heute von sozialem Druck und Marktkoordination abhängt. Damit verschiebt die institutionelle Verlagerung die Dezentralisierungs-Anforderung auf die Proposer-Schicht, während die Builder-Schicht als spezialisierter Markt operiert, deren Neutralität anderswo abgesichert wird.

Die Cloud-Konzentration bleibt

Mit dem reduzierten Verifizierungs-Profil verschiebt sich die Möglichkeit der Teilnahme vom Rechenzentrum auf die Home-Hardware, ohne dass damit die heutige Hyperscaler-Konzentration aufgelöst wäre. Im IST-Zustand betreiben rund 59 Prozent der gehosteten Execution-Layer-Nodes ihren Dienst auf den Infrastrukturen von AWS, Hetzner und OVHcloud.[245] Der M2-Schwellenwert von maximal 50 Prozent gilt für einen einzelnen Provider. Die 59 Prozent verteilen sich auf drei Anbieter und verfehlen ihn damit nicht. Die Roadmap enthält keinen Mechanismus, der die Konzentration direkt adressiert. Weder existie-

[243] MEV-Boost-Anteil im IST-Zustand: Rund 90 Prozent aller Mainnet-Blöcke werden per Q1 2026 durch die MEV-Boost-Sidecar geroutet, gegenüber 11 von 20 Blöcken beim Launch im September 2022. MEV-Boost übernimmt damit als Out-of-Protocol-Implementierung der Proposer-Builder-Separation die heutige Trennung zwischen Proposer-Hardware und Builder-Hardware ohne protokollarische Verankerung. Die Builder-Konzentration der drei größten Akteure liegt im selben Erhebungszeitraum bei rund 93 Prozent. Dieser Befund gehört methodisch zur Neutralitäts-Diskussion in 5.5 und wird hier nicht weiter ausgeführt.

[244] ePBS als institutionelle Trennung der Hardware-Klassen: Die ePBS-Mechanik (Trennung der Block-Validierung in zwei Slot-Phasen, Consensus-Validierung in Slot N und Execution-Validierung in Slot N+1, daraus resultierendes Proving-Fenster von 6–9 Sekunden) wurde in 5.2-A vollständig dargestellt. In 5.3-B erscheint sie als funktionale Resonanz nach R7d, mit Fokus auf der Hardware-Folge der Trennung: Proposer-Rolle (Consumer-Hardware-tauglich) und Builder-Rolle (Rechenzentrums-Klasse) werden auf Protokoll-Ebene strukturell separiert. Quellen: 5.2-A (ePBS als Konvergenzpunkt). Die Neutralitäts-Folgen der Trennung (Relay-Elimination, MEV-Internalisierung) werden in 5.5 aufgegriffen.

[245] Cloud-Konzentration im IST-Zustand: Rund 59 Prozent der Ethereum-Nodes werden auf den Infrastrukturen von AWS (rund 35,5 Prozent), Hetzner (rund 13,8 Prozent) und OVHcloud (rund 9,7 Prozent) betrieben. M1-Schwellenwert für III.4 Cloud-Unabhängigkeit: kein einzelner Cloud-Provider mehr als 50 Prozent. Die Datenbasis stammt aus den Ethernodes/Migalabs-Snapshots des IST-Erhebungszeitraums. Die exakte Provider-Verteilung schwankt zwischen Snapshots, die Größenordnung der Konzentration ist stabil. Die Roadmap enthält per Februar 2026 keine Maßnahme, die diese Konzentration direkt adressiert.

ren Protokoll-Penalties für Cloud-Deployment, noch verfügt das System über eine Anreizschicht, die geographisch verteilte Home-Nodes ökonomisch belohnt. Die Konzentration beruht auf operativen Vorteilen, die das Protokoll nicht beseitigen kann, weil sie außerhalb seiner Reichweite liegen. Dazu gehören die garantierte Uptime der Hyperscaler-SLAs, das automatisierte Monitoring der Validator-Infrastruktur, die niedrige Latenz zu den großen Builder-Nodes und die Bequemlichkeit eines Klick-Setups gegenüber dem manuellen Betrieb einer Home-Node. Stateless Clients senken die Hardware-Schwelle für Home-Staking auf ein Niveau, das technisch erreichbar ist. Sie übersetzen sich aber nicht automatisch in eine veränderte Betriebs-Verteilung, da die operativen Friktionen des Home-Betriebs unabhängig vom Hardware-Profil bestehen bleiben. Die Architektur liefert die Voraussetzung. Die operative Folge entscheidet sich außerhalb des Protokolls, in den Wahlen der Betreiber. Zur Hardware-Konsequenz gehört die Diagnose mit derselben Klarheit wie die Reduktionsfaktoren des Verifizierungs-Profils, weil sonst die Architektur-Aussage mit einer Betriebs-Aussage verwechselt würde, die sie nicht trägt.

Für die Hardware-Agnostik des Designzustands ergibt sich daraus eine asymmetrische Verbesserung. Auf der Verifikations-Seite wird das Spektrum der Hardware-Klassen, die einen Ethereum-Block kryptographisch prüfen können, radikal erweitert. Smartphone, Browser-Tab und eingebettete Systeme treten neben die professionelle Server-Klasse, und das Spektrum der akzeptablen Verifikations-Hardware ist im Designzustand nicht mehr durch das Gas Limit begrenzt. Auf der Betriebs-Seite bleibt die Konzentration der Node-Infrastruktur auf wenige Hyperscaler bestehen, da keine Protokoll-Maßnahme die operative Bequemlichkeit der Cloud gegen die Friktion des Home-Betriebs aufwiegt. Die Reichweite des Protokolls endet an der Grenze seines Mechanismus, und die Wahl der Betriebs-Umgebung bleibt eine Entscheidung der Akteure, die das Protokoll allenfalls erleichtert und nicht vorschreibt. Damit ist die Hardware-Voraussetzung für eine breitere Teilnahme geklärt. Die Frage, woher ein Stateless Client den Witness und den Beweis bezieht, ohne dass die gewonnene Vertrauenslosigkeit durch einen neuen zentralen Datenkanal wieder verlorengeht, trägt der nächste Abschnitt.

5.3-C Die Trustless RPC Architecture

Der Stateless Client aus 5.3-B kann Blöcke auf einem Smartphone kryptographisch verifizieren, weil er weder den State hält noch die Ausführung wiederholt. Was er aber nicht selbst produziert, sind Witness und Beweis pro Block, sodass er die Daten aus dem Netzwerk empfangen muss, und an der Empfangsseite hängt die Tragfähigkeit der gesamten Hardware-Demokratisierung. Der Bezugskanal ist heute der RPC-Endpunkt, ein Server, der eine Ethereum-Full-Node betreibt und Anfragen über das JSON-RPC-Protokoll entgegennimmt. Per Februar 2026 laufen rund neunzig Prozent des Ethereum-RPC-Verkehrs über drei Provider: Infura aus dem ConsenSys-Umfeld, das unabhängige Alchemy und QuickNode.[246] Wenn ein Wallet eine RPC-Antwort empfängt, verlässt es sich auf die Wahrhaftigkeit des Providers ohne eigene kryptographische Verifikation. Diese Vertrauensbeziehung lässt sich durch die kryptographische Verifikation des Stateless Client nicht auflösen. Der Client prüft die Daten zwar gegen Beweise, doch beides, Daten wie Beweise, stammt vom selben Provider, sodass ein manipulierter Provider beides intern konsistent fälschen könnte. Mit der Tragfähigkeit der Verifikation auf Consumer-Hardware verschiebt sich die Frage der Trustlosigkeit somit auf die Datenversorgung.

Die Trustless RPC Architecture ersetzt die zentrale Provider-Beziehung durch drei zusammenwirkende Out-of-Protocol-Komponenten, deren Verbund die Funktion eines RPC-Endpunkts mit kryptographischer Verifikation erfüllt. Die Ethereum Foundation hat den Verbund in ihren Protocol Priorities 2026 unter genau dem Namen Trustless RPC Architecture geführt.[247] Helios trägt die Verifikation auf dem Endgerät über eine kryptographische Prüfung der Beacon-Chain-Header. Das Portal Network übernimmt die dezentrale Verteilung der historischen und der Zustands-Daten, die der Client zur Verifikation benötigt. Die Witness-Verfügbarkeit aus der State-Tree-Architektur, deren Mechanik 5.3-A vollständig behandelt, liefert schließlich die kryptographischen Belege, gegen die geprüft wird. Die drei Komponenten tragen jeweils nur unter Voraussetzung

[246] RPC-Provider-Konzentration im IST-Zustand. Per Februar 2026 routen rund neunzig Prozent aller Ethereum-Interaktionen über drei bis vier kommerzielle Anbieter, dominant Infura (ConsenSys-Umfeld), Alchemy und QuickNode. Der konkrete Vertrauensvektor entsteht doppelt: Der Provider kann erstens die ausgelieferten Witnesses und State-Roots manipulieren, sodass der Client eine kryptographische Verifikation gegen einen kompromittierten Eingangsstand ausführt, und er kann zweitens die Sicht des Clients auf den Mempool und auf eingehende Transaktionen filtern. Quelle: EF Protocol Priorities 2026.

[247] Benennung der „Trustless RPC Architecture“. Die Konvergenz von Stateless Clients, Portal Network und Light Clients mündet in ein übergeordnetes Ziel, das die Ethereum Foundation in ihren Protocol Priorities 2026 als ‘Trustless RPC Architecture’ benennt. Der englische Eigenname wird in dieser Arbeit beibehalten, weil er in den Primärquellen als feststehende Bezeichnung verwendet wird und keine analytische Setzung dieser Arbeit ist.

der anderen. Helios verifiziert nur den Block-Header und braucht die Belege, die das Portal Network liefert. Das Portal Network transportiert nur die Daten, die durch die Witness-Struktur aus 5.3-A überhaupt übertragbar werden. Die Witnesses tragen nur, sofern Helios den Header-Stand kryptographisch verifiziert hat. Damit löst die Architektur die Frage, woher der Client seine Daten bezieht, ohne dass die Vertrauenslast neu zentralisiert wird.

Helios: Verifikation auf dem Gerät

Helios löst das Vertrauensproblem, indem die Echtheit der Daten lokal prüfbar wird und der Daten-Server selbst nicht vertrauenswürdig sein muss. Der Client lädt Light-Client-Updates von einem beliebigen Beacon-Chain-Endpunkt, und jedes Update enthält den signierten Block-Header zusammen mit der aggregierten Signatur des Sync Committee. Die Signatur wird lokal gegen die bekannte Committee-Mitgliedschaft geprüft, sodass die Echtheit unabhängig vom liefernden Server feststeht und die Vertrauensbeziehung sich vom Daten-Server auf die Verifikation im Endgerät verschiebt. Die in Rust geschriebene und zu WebAssembly kompilierte Implementierung benötigt für eine Erstsynchronisation etwa zwei Sekunden und liegt bei dreizehn Megabyte Binärgröße, womit Helios auf einem Smartphone, im Browser-Tab und auf Hardware der Raspberry-Pi-Klasse lauffähig ist, ohne dass eine eigene Blockchain-Speicherung nötig wäre.[248] Das Vertrauensmodell stützt sich auf die Annahme, dass mindestens zwei Drittel des Sync Committee ehrlich agieren, wobei das Komitee aus 512 Validatoren besteht, die alle 27 Stunden zufällig aus dem Gesamtbestand gezogen werden und die Beacon-Block-Header per BLS-Aggregation signieren.[249] Die Reichweite der Verifikation endet auf der Konsens-Schicht. Helios prüft, dass der Block-Header vom Sync Committee signiert ist. Was Helios nicht prüft, ist die Frage, ob die Transaktionen innerhalb des Blocks tatsächlich korrekt ausgeführt wurden, ob also die State-Transition aus den Eingaben nach Protokoll-Regeln folgt. Diese Execution-Korrektheit beruht im heutigen Helios auf der Annahme, dass die Validatoren ihre Pflicht erfüllen und kein manipuliertes Ergebnis signiert haben, al-

[248] Helios-Spezifikationen. Light Client aus der Forschungseinheit a16z crypto, in Rust implementiert mit Kompilation zu WebAssembly, lauffähig im Browser und auf mobilen Endgeräten. Initialsynchronisation in etwa zwei Sekunden, Binärgröße bei dreizehn Megabyte, keine lokalen Storage-Anforderungen. Multichain-Unterstützung für Ethereum Mainnet und für OP-Stack-basierte Layer 2. Status DEPL, produktiv seit 2024 und aktiv gepflegt.

[249] Sync-Committee-Mechanik. 512 Validatoren werden zufällig aus dem Gesamtbestand für eine Amtszeit von 256 Epochs (in etwa 27 Stunden) ausgewählt. Sie signieren jeden Beacon-Block-Header während ihrer Amtszeit. Die BLS-Aggregation ermöglicht eine effiziente Verifikation der zusammengefassten Signatur. Datenaufkommen für Helios in der Größenordnung von 25 Kilobyte pro Periode, Sicherheitsbudget der Sync-Committee-Verifikation 512 mal 32 ETH gleich 16.384 ETH.

so auf einer sozialen Annahme über die Validator-Ehrlichkeit ohne eigene kryptographische Garantie. Sie wird im Designzustand durch eine Kombination zweier Schichten geschlossen: Die Beweis-Pipeline aus 5.3-A′ liefert den Korrektheits-Beweis der State-Transition, die Stateless-Client-Architektur aus 5.3-B verifiziert ihn auf dem Endgerät. Die Implementierung ist seit 2024 produktiv im Einsatz.

Das Portal Network ergänzt die Verifikations-Schicht durch die dezentrale Distribution der historischen und Zustands-Daten, deren Notwendigkeit aus der mit EIP-4444 eingeführten History-Reduktion erwächst. EIP-4444 (DEPL seit Juli 2025) erlaubt Execution Clients, historische Daten älter als ein Jahr zu verwerfen, was den Full-Node-Betrieb auf einer Festplatte von zwei Terabyte ermöglicht.[250] Die strukturelle Konsequenz der Reduktion ist eine Verfügbarkeits-Lücke, weil kein einzelner Node die vollständige Historie mehr halten muss und das Netzwerk die Daten-Verantwortung vom Einzelnen auf das Kollektiv verschiebt. Das Portal Network verteilt die historischen und Zustands-Daten über ein dezentrales Peer-Netzwerk, in dem jeder Node einen Teil der Daten hält. Ein Discovery-System leitet Anfragen an die jeweils zuständigen Nodes. Vier Sub-Protokolle decken unterschiedliche Datenklassen ab. Das History Network trägt Block-Bodies und Receipts, das State Network die Konto-Daten und den Bytecode. Das Beacon Network liefert die Sync-Committee-Daten, auf denen Helios verifiziert, während ein Transaction-Gossip-Subnetz den Mempool-Zugang ohne lokalen State sicherstellt. Vier produktive Implementierungen (Trin, Fluffy, Ultralight, Shisui) sind Stand Februar 2026 operativ aktiv, mit client-übergreifender Interoperabilität, ohne dass das Portal Network als verbindlicher Teil des Konsens-Protokolls verankert wäre.[251] Die Daten-Verantwortung liegt somit bei einem verteilten Netzwerk außerhalb des Protokoll-Kerns.

Damit eine vollständig dezentrale Daten-Distribution auch bei steigendem Gas Limit trägt, hebt EIP-7975 (PLAN/CFI Glamsterdam) das eth-Wire-Protokoll auf eth/70 und führt die Paginierung der Block-Receipt-Listen ein, womit die Übertragungs-Grenze von zehn Mebibyte pro devp2p-Nachricht für die

[250] EIP-4444 (History Expiry Phase 1). Status DEPL seit 8. Juli 2025, alle fünf Execution Clients (Geth, Nethermind, Besu, Erigon, Reth) unterstützen Pre-Merge History Pruning. Reduziert den Storage-Bedarf um 300 bis 500 Gigabyte pro Node und ermöglicht den Full-Node-Betrieb auf einer Festplatte von zwei Terabyte. Phase 2 (Rolling Window für Post-Merge-Daten) ist als PLAN ausgewiesen, ohne Timeline.

[251] Portal Network. Status IMPL. Discovery via discv5 (UDP-basiertes Protokoll mit ENR-Records nach EIP-778). Die Inhaltsverteilung folgt einem Kademlia-inspirierten DHT mit XOR-Distanz-Metrik, in dem die Nodes jeweils diejenigen Inhalte vorhalten, deren IDs ihrer eigenen Node-ID am nächsten liegen. Vier produktive Implementierungen: Trin in Rust (Schwerpunkt History Network und State Network im Alpha-Stadium), Fluffy in Nim (History Network, Beacon Network und Portal-Bridge), Ultralight in TypeScript (Browser- und Mobil-Schwerpunkt, State Network in R&D), Shisui in Go (Ökosystem-Diversifizierung). Cross-Client-Interop-Tests via Hive-Framework, Netzwerk-Monitoring via GlaDOS. Per Februar 2026 nicht im Konsens-Protokoll als verbindliche Mainnet-Komponente verankert, aber Out-of-Protocol-operativ.

Architektur-Skalierung außer Kraft gesetzt wird. Das devp2p-Protokoll, auf dem die Peer-zu-Peer-Kommunikation der Execution Clients beruht, erlaubt heute Nachrichten bis zehn Mebibyte. Die Grenze ist bei steigendem Gas Limit nicht durchhaltbar, da die Block-Receipts mit der Transaktionszahl wachsen. Die rechnerische Schwelle für das Überschreiten der zehn Mebibyte liegt nach EIP-Text bei 83 Millionen Gas, die in den Erigon-Tests vom Januar 2026 dokumentierte praktische Schwelle bereits bei rund 75 Millionen Gas.[252] Wer historische Blöcke aus dem Netzwerk nachsynchronisiert, kann die zugehörigen Receipts nicht mehr in einer einzigen Nachricht übertragen, was die Synchronisation an einer reinen Übertragungs-Grenze scheitern lässt. EIP-7975 löst das Risiko, indem ein Node die Receipt-Liste eines Blocks in mehreren Teil-Anfragen abrufen kann, etwa die ersten hundert Receipts in einer Anfrage und die nächsten hundert in einer separaten, woraufhin das Wire-Protokoll die Teil-Übertragungen zu einer vollständigen Receipt-Liste zusammenfügt. Mit der Härtung wird die Skalierungs-Kapazität aus 5.2 im RPC-Pfad tatsächlich durchsetzbar, das heißt Gas-Schwellen oberhalb der heutigen 60 Millionen. Andernfalls würde sie an einem Übertragungs-Engpass kollabieren, lange bevor die Hardware-Reduktion aus 5.3-B ihre Wirkung entfaltet.

Verfügbar, aber nicht integriert

Die Trustless RPC Architecture steht heute technisch zur Verfügung. Ihre Wirkung auf die reale Vertrauenslast entscheidet sich an der Adoption durch Wallets und Frontends, Akteure, die das Protokoll nicht verpflichten kann. Per Februar 2026 integriert keine der drei marktdominanten Wallet-Lösungen, weder MetaMask noch Trust Wallet noch Ledger, Helios als Standard für trustlose Verifikation.[253] Die Infrastruktur ist verfügbar, die Integration in die Endnutzer-Software steht aus. Die Diagnose folgt einem Muster, das bereits die Hyperscaler-Konzentration in 5.3-B trug. Beide Phänomene berühren operative Schichten oberhalb des Protokolls. Das Protokoll kann sie erleichtern, ihre Besetzung aber nicht vor-

[252] EIP-7975 und der Übergang zu eth/70. Status PLAN/CFI Glamsterdam (per April 2026, Checkpoint 9). EIP-7975 hebt das eth-Wire-Protokoll von eth/69 auf eth/70 und führt die Paginierung der Block-Receipt-Listen als integralen Bestandteil des Protokoll-Updates ein; es existiert kein separater Networking-EIP für die Paginierung. Die rechnerische Schwelle für das Überschreiten der zehn-Mebibyte-Grenze pro devp2p-Nachricht liegt nach EIP-Text bei 83 Millionen Gas, die in den Erigon-Implementierungs-Tests vom Januar 2026 dokumentierte praktische Schwelle bereits bei rund 75 Millionen Gas. eth/69 war als Networking-Update für Fusaka (Dezember 2025) deployt; eth/70 ist mit Glamsterdam (H2 2026 wahrscheinlich) verbunden. Quellen: ethereum/EIPs Repository, EIP-7975-Spezifikation; erigontech/erigon Issue Januar 2026 zu Receipt-Größen oberhalb 75 Millionen Gas.

[253] Wallet-Adoption per Februar 2026. MetaMask, Trust Wallet und Ledger unterstützen die in Pectra deployten Account-Erweiterungen, integrieren aber keinen Light Client für die kryptographische Verifikation der RPC-Antworten als Standard-Verbindungsweg. Die Frontend-Adoption für die Light-Client-Verifikation ist ein Marktphänomen außerhalb des Protokoll-Designs und liegt nicht in der Reichweite der ACD-Governance.

schreiben. Sie unterscheiden sich in ihrem Gegenstand. Die Hyperscaler-Konzentration betrifft die Wahl der Betreiber-Infrastruktur durch die Validator-Operateure, die RPC-Provider-Diagnose die Wahl der Frontend-Integration durch die Wallet- und dApp-Entwickler.

Mit der Verteilung der Vertrauensfrage auf drei Out-of-Protocol-Komponenten und der Lösung der Skalierungs-Frage durch die Wire-Protokoll-Härtung beruht die Verifikations-Architektur des skalierten Netzwerks auf dem Endgerät vollständig kryptographisch. Die kryptographische Tragschicht von Helios stützt sich ihrerseits auf die BLS-Signaturen des Sync Committee, deren Sicherheit auf demselben ECDLP beruht, das in 5.3-A für die IPA-Commitments der Verkle Trees als nicht quantenresistent identifiziert wurde.[254] Die Verifikations-Architektur der Stateless Clients und die kryptographische Grundlage aus 5.3-A teilen damit dieselbe Annahme und stehen vor derselben Migrations-Anforderung. 5.3-D entfaltet die Post-Quantum-Roadmap als Migration, die beide Säulen der bisher gebauten Architektur betrifft.

5.3-D Die Post-Quantum-Migration der Verifikation

Die vorangegangenen Abschnitte haben gezeigt, wie ein Block sich auf gewöhnlicher Konsumer-Hardware verifizieren lässt, auf einem Handy oder Laptop, ohne lokalen State und ohne eigene Re-Execution. Getragen wird diese Verifikation von den Signaturen und Commitments, die der Block mitführt und deren Echtheit der Verifizierer nachrechnet. Die heutigen Signaturen beruhen auf der Kryptographie elliptischer Kurven, deren Sicherheit das Problem des diskreten Logarithmus trägt. Aus dem privaten Schlüssel lässt sich der zugehörige öffentliche Wert in Sekundenbruchteilen berechnen, während die umgekehrte Berechnung für klassische Rechner mit jeder zusätzlichen Stelle des Schlüssels exponentiell aufwändiger wird. Auf der Asymmetrie zwischen leichter Berechnung und praktisch unmöglicher Umkehrung beruht die Sicherheit jeder Signatur, die heute einen Block schützt.

Ein hinreichend großer Quantenrechner verschiebt die Grenze, an der die Umkehrung unmöglich wird. Shors Algorithmus bricht das ECDLP in polynomieller Zeit (vgl. Abschnitt 5.3-A). Gegen wachsende klassische Rechenkraft ge-

[254] BLS-Signaturen und IPA-Commitments unter der Discrete-Log-Annahme. BLS12-381, die paarungsfreundliche elliptische Kurve der Validator-Aggregation und Sync-Committee-Verifikation, beruht auf dem Discrete-Logarithm-Problem in Pairing-friendly Elliptic Curve Groups. Die IPA-Commitments der Verkle Trees beruhen auf Bandersnatch, einer nicht-paarungsfreundlichen Kurve, deren Sicherheit ebenfalls auf einem Discrete-Logarithm-Problem auf elliptischen Kurven ruht. Beide Annahmen gehören derselben kryptographischen Klasse an und sind durch Shor's Algorithmus auf einem ausreichend großen Quantenrechner in polynomialer Zeit angreifbar. Sie sind jedoch nicht identisch, weil BLS die Pairing-Eigenschaft nutzt und IPA nicht.

nügte bisher ein längerer Schlüssel, doch gegen eine polynomielle Laufzeit verfehlt dieses Mittel seine Wirkung, weil die Verdopplung der Länge den Aufwand des Angreifers nur moderat erhöht. Der Quantenrechner entwertet damit die Annahme selbst, auf der die Sicherheit der Verfahren steht, und der Bruch reicht über jedes einzelne von ihnen hinaus.

Nicht jede Form der Kryptographie beruht auf einer solchen algebraischen Struktur. Eine Hash-Funktion verbirgt kein lösbares Problem, ihre Sicherheit liegt allein darin, dass ein Angreifer alle möglichen Eingaben durchprobieren müsste. Grovers Algorithmus macht dieses Durchprobieren für einen Quantenrechner schneller, bleibt aber ein Durchprobieren, denn der Rechner sucht weiterhin, statt die Antwort auszurechnen. Eine schnellere Suche lässt sich abwehren, indem man den Suchraum vergrößert und die Ausgabe der Hash-Funktion verlängert. Genau hier liegt der Unterschied zu Shors Angriff auf die elliptischen Kurven, der die Antwort direkt berechnet und sich deshalb durch keinen größeren Suchraum abwehren lässt.[255]

Der Zielzustand der Verifikation ersetzt die angreifbaren Verfahren deshalb durch hash-basierte Kryptographie. Die späte Roadmap behandelt die Resistenz als Entwurfsprinzip und führt sie unter dem Namen Lean Ethereum (Abschnitt 5.1). Für die Verifikationsschicht, die Abschnitt 5.3 über die reduzierte Datenstruktur und die Trustless RPC Architecture aufgebaut hat, stellt der Übergang eine doppelte Frage. Zu prüfen bleibt, ob die Architektur unter ihm kryptographisch tragfähig bleibt und was eine verspätete Migration nach sich zöge.

Vier Schwachstellenklassen

Die Bedrohung reicht über die Verifikation hinaus, und die Roadmap gliedert sie in vier Schwachstellenklassen, die jeweils ein anderes Primitiv an einem anderen Ort im Protokoll betreffen. Die BLS-Signaturen des Konsens werden durch hash-basierte Signaturen mit STARK-Aggregation ersetzt, deren Substanz Abschnitt 5.5 entwickelt. Ebenso betroffen sind die KZG-Commitments der Data Availability, die aber einem eigenen Migrationspfad mit einem ungelösten Folgeproblem folgen, das Abschnitt 5.2-D behandelt. Die ECDSA-Signaturen, mit denen heute jedes Konto seine Transaktionen unterschreibt, gehen über ein Opt-

[255] Die Charakterisierung der beiden Algorithmen folgt Vitalik Buterin, „Possible Futures of the Ethereum Protocol — Post-Quantum Roadmap“, 26. Februar 2026, sowie der etablierten Post-Quantum-Kryptographie. Shors Algorithmus reduziert das Faktorisierungs- und das Discrete-Log-Problem auf polynomielle Laufzeit, weshalb längere Schlüssel keinen wirksamen Schutz bieten; Grovers Algorithmus liefert für die unstrukturierte Suche nur einen quadratischen Vorteil, der die effektive Hash-Sicherheit halbiert und durch eine Verdopplung der Ausgabelänge ausgeglichen wird. Die EF behandelt Post-Quantum-Sicherheit im Rahmen des Lean-Ethereum-Programms als Entwurfsprinzip; dessen Substanz trägt Abschnitt 5.1.

in-Vehikel auf hash-basierte Verfahren über. Abschnitt 5.3-E entfaltet die Mechanik. Die vierte Klasse, die Beweise der Anwendungsebene, beruht auf der Aggregations-Mechanik, die weiter unten als Scharnier wiederkehrt. Die Karte zeigt ein Querschnitts-Phänomen, deren Abschnitte je eine Klasse tragen.[256]

Von den vier Klassen ist die Verifikation am stärksten exponiert, weil sie ihre Vertrauenslosigkeit mit zwei Effizienz-Gewinnen erkauft hat, die beide auf der angreifbaren Klasse beruhen. Der erste ist der kompakte Witness aus 5.3-A, der den Beweis-Pfad zur State Root auf einen kurzen Beweis zusammenzieht und den Stateless Client erst auf Consumer-Hardware trägt. Der zweite ist die aggregierte Sync-Committee-Signatur aus 5.3-C, die Helios eine einzige Prüfung gegen das gesamte Komitee erlaubt, statt jede Signatur einzeln zu verifizieren. Beide ruhen auf demselben diskreten Logarithmus, der Witness über die Inner Product Arguments der Bandersnatch-Kurve, die Signatur über die Pairing-Eigenschaft von BLS12-381. Genau das, was das Smartphone zum Verifizierer macht, ist damit der quantenanfälligste Teil der Architektur.[257]

Der hash-basierte Ausweg ist robust gegen den Quantenangriff, für die Signaturen aber teuer. An die Stelle von BLS treten die hash-basierten Signaturen der leanXMSS-Linie (RES), deren Substanz Abschnitt 5.5 entfaltet. Eine einzelne solche Signatur verbraucht unaggregiert mehr als das Sechzigfache des Gases einer ECDSA-Signatur, und ihr Speicherbedarf liegt um Größenordnungen höher. Müsste das Protokoll jede Signatur einzeln prüfen, sobald hash-basierte Verfahren vom Ausnahmefall zur Regel werden, sprengten diese Kosten das Budget eines Blocks.[258]

Hier greift die Aggregations-Mechanik aus 5.3-A′ als Scharnier ein und macht den teuren Pfad wieder bezahlbar. Die Aggregation fasst die Beweise zusammen

[256] Vier Vulnerabilitätsklassen: Vitalik Buterin, PQ-Roadmap, ebd. Die vier Klassen umfassen die Consensus-BLS-Signaturen (Heimat 5.5), die KZG-Commitments der Data Availability (5.2-D), die ECDSA-Signaturen der Accounts (5.3-E) und die Application-Layer-Beweise. Die KZG-Migration ist insofern eigenständig, als der Umstieg auf STARK-basiertes Erasure Coding die homomorphe Eigenschaft der KZG-Commitments verliert und deshalb das eindimensionale Sampling maximiert, statt das zweidimensionale zu tragen; sie ist teils ungelöst und wird in 5.2-D als distinkte Migration mit eigenem offenem Problem geführt.

[257] Verkle-Commitments und Binary Trees: Die ECDLP-Verwundbarkeit der IPA-Commitments in Verkle wird getrennt von den vier Vulnerabilitätsklassen geführt, weshalb ihre Zusammenfassung mit den BLS-Signaturen des Sync Committee eine Setzung dieses Abschnitts ist; beide gehören derselben kryptographischen Klasse an, BLS12-381 über die Pairing-Eigenschaft (vgl. 5.3-C), die Bandersnatch-Kurve über das ECDLP (vgl. 5.3-A), ohne identisch zu sein. Den Wechsel auf Binary Trees rahmt die Ethereum Foundation primär als Skalierungsschritt und führt die Quantenresistenz als komplementären Effekt.

[258] Kostenspanne: Die Gas-Werte folgen der in 5.3-A′ getragenen Roadmap-Quantifizierung (Vitalik Buterin, PQ-Roadmap, ebd.): rund 3.000 Gas für eine klassische ECDSA-Signatur gegenüber rund 200.000 Gas für eine unaggregierte hash-basierte Einzelsignatur. Der erhöhte Speicherbedarf quantensicherer Signaturen (ML-DSA, SLH-DSA) liegt um ein bis drei Größenordnungen über dem einer ECDSA-Signatur (rund 2,4 bis 4,6 KB bei ML-DSA und 7,9 bis 49,9 KB bei SLH-DSA gegenüber 64 Byte).

(vgl. Abschnitt 5.3-A′), sodass die je Signatur prohibitiven Kosten in der Masse auf einen tragbaren Anteil je Block fallen. Dieselbe Mechanik, die die Beweise der Anwendungsebene trägt, macht damit auch die hash-basierten Konsens-Signaturen tragbar. Der hash-basierte State-Tree erreicht seine Quantenresistenz auf einem eigenen Weg, dem Wechsel auf Binary Trees, dessen Preis im größeren Witness liegt und den keine Signatur-Aggregation senkt. Die Mechanik ist im Designzustand vollständig beschrieben, hängt für die Verifikation der aggregierten Beweise aber an einer Familie von Precompiles, die noch nicht durch Hard Fork aktiviert ist.[259]

Exposition ist nicht Risiko

Maximale Exposition ist nicht maximales Risiko, denn was Ethereum über eine verspätete Migration hinwegträgt, ist die Bereitschaft des Konsens, ohne Finalität weiterzulaufen, und kein kryptographisches Verfahren. Der Inactivity Leak, der diese Bereitschaft erzwingt, ist ein seit Jahren auf Mainnet erprobter Mechanismus: Erreicht das Netzwerk keine Finalität mehr, verlieren die nicht-partizipierenden Validatoren schrittweise ihren Stake, bis die verbliebenen wieder zwei Drittel stellen. Gespannt wurde das Netz für den Fall offline gegangener Validatoren, und es fängt den Quantenfall mit ab, ohne je für ihn entworfen worden zu sein. Bricht ein Verfahren vor Abschluss der Migration, produziert die Kette weiter Blöcke, und die Finalität kehrt zurück, sobald zwei Drittel des Stake auf das neue Schema gewechselt sind, ein ökonomischer Vorgang ohne neue kryptographische Voraussetzung. So verliert das Netzwerk die Finalitätsgarantie, während die Kette weiterläuft, in Buterins Formulierung „keeps chugging along“.[260]

Der Designzustand zieht die Finalität drastisch zusammen, ohne den Mechanismus aufzugeben, der den Übergang absichert. Single-Slot-Finalität finalisiert einen Block im selben Slot, in dem er vorgeschlagen wird, behält den Inactivity Leak aber ausdrücklich bei.[261] Ihren Endzustand findet die Konsens-Schicht

[259] Reife der Aggregations-Mechanik: Die Mechanik ist nach 5.3-A′ im Designzustand vollständig beschrieben, für die On-Chain-Verifikation der aggregierten quantenresistenten Beweise aber an die dort behandelte, noch nicht durch Hard Fork aktivierte Familie von Post-Quantum-Precompiles gebunden. Status RES.

[260] Inactivity Leak und Tragfähigkeitsaussage: Der Inactivity Leak ist im IST-Zustand auf Mainnet erprobt und operativ (Status DEPL des Mechanismus); er reduziert den Stake nicht-partizipierender Validatoren schrittweise, bis die verbleibenden eine Zwei-Drittel-Mehrheit zurückgewinnen. Die Tragfähigkeitsaussage, dass die Kette ohne Finalitätsgarantie weiterläuft („keeps chugging along“), stammt aus Vitalik Buterins PQ-Roadmap und ist mehrfach belegt. Eine im selben Beitrag referenzierte Metaculus-Schätzung beziffert die Wahrscheinlichkeit kryptographisch relevanter Quantenrechner vor 2030 mit etwa 20 Prozent.

[261] Single Slot Finality und der Inactivity Leak: Im IST-Zustand greift der Leak, sobald die Beacon Chain länger als vier Epochen nicht finalisiert (MIN_EPOCHS_TO_INACTIVITY_PENALTY = 4), und reduziert das Gewicht inaktiver Validatoren, bis die aktiven wieder zwei Drittel des Stake stellen (ethereum.org, „Proof-of-stake rewards and penalties“; eth2book, Abschnitt 2.8.6). Single Slot Finality finalisiert einen Block im selben Slot, in dem er vorgeschlagen wird, behält den Inactivity Leak aber ausdrücklich als Rückfall-Mechanismus bei, der die Kette bei einem Ausfall von

in der Beam Chain, deren Substanz Abschnitt 5.5 entfaltet und die jenseits des laufenden Jahrzehnts liegt.[262] Die Reform des Leak für das migrierte Verfahren gehört zu diesem Horizont, während der Mechanismus, der den Übergang absichert, in seiner heutigen Form bereits auf Mainnet steht.

Die Verifikations-Architektur aus Abschnitt 5.3 beruht damit auf einer kryptographischen Basis, die exponiert, aber nicht unverteidigt ist. Witness und Sync-Committee-Signatur teilen die Quantenfragilität ihrer Discrete-Log-Fundamente, doch ihr hash-basierter Ersatz wird über die Aggregation bezahlbar, und die Tragfähigkeit des Übergangs liegt am Ende weniger in der Kryptographie als in einem Konsens, der ohne rechtzeitige Migration weiterläuft. Was die Account-Ebene zu diesem Bild beiträgt, die programmierbare Validierungslogik, über die ein Nutzer seine Authentifizierung von ECDSA auf ein quantenresistentes Verfahren umstellt, entfaltet der abschließende Abschnitt von 5.3.

5.3-E Account Abstraction und die Migration der Nutzer-Signatur

Die bisherigen Abschnitte dieses Kapitels haben gezeigt, wie das Netzwerk einen ganzen Block verifiziert, auf billiger Hardware, ohne zentrale Dienste und auch dann noch, wenn ein Quantenrechner die heutige Kryptographie bricht. Jede dieser Prüfungen beginnt jedoch eine Ebene tiefer, bei der einzelnen Transaktion, deren Gültigkeit das Protokoll an der Unterschrift des absendenden Kontos misst. Der letzte Abschnitt von 5.3 wendet sich der untersten Prüfung zu und damit dem Nutzer selbst, der sein Konto führt und seine Transaktionen unterschreibt. Ein Konto ist heute an ein einziges Geheimnis gebunden, einen privaten Schlüssel, den sein Besitzer verwahren muss. Wer eine Transaktion sendet, beweist seinen Besitz, indem er sie mit dem Schlüssel unterschreibt, und das Verfahren der Unterschrift, ECDSA, ist für jedes Konto dasselbe und fest im Protokoll verankert.

Diese Starrheit hat einen Preis, den jeder Nutzer trägt. Verliert er den Schlüssel, verliert er das Konto und alles darin, ohne Möglichkeit der Wiederherstellung, denn niemand außer ihm kann den Besitz beweisen. Er kann die Art seiner Unterschrift nicht wechseln, auch wenn ein sichereres Verfahren bereitstünde,

über einem Drittel der Validatoren weiterlaufen lässt (Vitalik Buterin, „Epochs and slots all the way down“, 30. Juni 2024; ethereum.org, „Single slot finality“). SSF trägt den Status RES; die genaue Adaptation des Leaks an die Slot-Finalität ist nicht spezifiziert.

[262] Beam Chain: vollständige Neugestaltung der Consensus-Schicht mit SNARK-basierter Aggregation und auf wenige Slots verkürzter Finalität, die Single Slot Finality und MaxEB absorbiert (Justin Drake, Devcon 2024; RES). Die Reform des Inactivity Leak für das post-quantum-migrierte Verfahren ist als Teilpunkt dieser Neugestaltung geführt; ihre Substanz und die konsens-seitige BLS-Migration trägt Abschnitt 5.5, der Konsens-Endzustand Abschnitt 5.1.

und er kann die Gebühr einer Transaktion nur in der Währung des Netzwerks bezahlen. Das Konto ist an einen einzigen Schlüssel und ein einziges Verfahren gebunden, und die feste Bindung ist die eigentliche Hürde für die breite Nutzung.

Account Abstraction löst die Bindung. Sie nimmt dem Protokoll die Vorschrift, wie ein Konto eine Transaktion gültig macht, und gibt sie dem Konto selbst, dessen Validierungsregel damit frei programmierbar wird. Auf der einen Verschiebung im Protokoll beruht alles Weitere: Die Wallets und Anwendungen, die auf ihr aufsetzen, können ein Konto per Fingerabdruck entsperren, es nach einem Verlust wiederherstellen oder seine Unterschrift auf ein quantensicheres Verfahren umstellen. Wie weit die Programmierbarkeit die Teilnahme an Ethereum für den gewöhnlichen Nutzer verändert, und wo die gewonnene Leichtigkeit ihren eigenen Preis hat, ist die Frage dieses Abschnitts.

Das Gerät wird zur Wallet

Für den gewöhnlichen Nutzer beginnt die Teilnahme im Zielzustand mit einer Geste, die er von seinem Telefon längst kennt. Er entsperrt sein Konto und bestätigt eine Transaktion über den Fingerabdruck oder einen Passkey, also über jenes Verfahren, mit dem sein Gerät schon heute Anmeldungen ohne Passwort absichert und dessen Schlüssel das gesicherte Element des Geräts nie verlässt. An die Stelle der Zeichenfolge, die der Besitzer eines Kontos bislang notieren und auf Jahre hinaus sicher verwahren musste und deren Verlust unwiderruflich war, tritt damit eine Authentifizierung, die der Nutzer aus dem alltäglichen Umgang mit seinem Gerät bereits beherrscht. Das Konto verlangt von ihm kein neues Wissen über Schlüssel und Verwahrung und fügt sich in eine Handhabung ein, die für ihn keiner Erklärung mehr bedarf. Das Gerät, das er ohnehin bei sich trägt, wird damit zur Wallet, und die gesonderte Installation einer spezialisierten Software, die im heutigen Zustand zwischen ihm und dem Netzwerk steht, entfällt. Der erste Kontakt mit Ethereum setzt damit nicht länger voraus, dass der Nutzer die Logik privater Schlüssel verstanden und ihre Sicherung eingeübt hat.

Verliert der Nutzer das Gerät, auf dem sein Schlüssel ruht, bleibt sein Konto erreichbar. Er hat es zuvor an mehrere Vertrauens-Instanzen seiner Wahl gebunden, an weitere Personen, eigene Zweitgeräte oder einen spezialisierten Dienst, von denen eine zuvor festgelegte Mehrheit genügt, um den Zugang gemeinsam wiederherzustellen, ohne dass eine von ihnen allein über das Guthaben verfügt. Die Gebühr einer Transaktion entrichtet er in einer beliebigen Währung seines Kontos oder gar nicht selbst, weil die Anwendung, die er nutzt, sie für ihn übernimmt, sodass der Erwerb der Netzwerk-Währung als Voraussetzung der ersten

Nutzung entfällt. Mehrere Handlungen, die das Protokoll heute als einzeln zu bestätigende Transaktionen behandelt, etwa die Freigabe eines Betrags und seine anschließende Verwendung, fasst sein Konto zu einer einzigen, atomaren Bestätigung zusammen, deren Teile gemeinsam gelingen oder gemeinsam unterbleiben. Erteilt er einer Anwendung einmal eine eng umrissene Vollmacht, etwa für wiederkehrende Zahlungen innerhalb eines von ihm gesetzten Rahmens, handelt sein Konto fortan in diesen Grenzen, ohne dass jede einzelne Handlung erneut seine Bestätigung verlangt. Die Summe der Annehmlichkeiten ergibt eine Teilnahme, die sich in ihrer Handhabung den gewohnten Diensten des offenen Internets annähert, ohne deren zentrale Verwahrung zu übernehmen.

Jede der Annehmlichkeiten beruht auf der einen Verschiebung, die das Protokoll vornimmt, und entsteht doch erst auf der Ebene über ihm. Das Protokoll gibt die feste Vorschrift auf, dass ein Konto seine Transaktion allein über eine ECDSA-Unterschrift gültig macht, und behandelt das Konto stattdessen als Smart Contract, dessen Logik zur Prüfung der Gültigkeit in seinem eigenen Code liegt. Bevor das Protokoll eine Transaktion dieses Kontos ausführt, übergibt es sie dessen Validierungsfunktion, und diese entscheidet nach frei gewählter Logik, ob die mitgelieferten Daten die Transaktion autorisieren. Diese Daten müssen keine ECDSA-Unterschrift mehr sein. Der Code des Kontos kann eine über den Fingerabdruck erzeugte Signatur prüfen, für eine Wiederherstellung das Zusammenwirken mehrerer Schlüssel verlangen oder die Gebühr einem Dritten zurechnen, und welche der Regeln gelten, bestimmt allein das Konto und nicht das Protokoll. Was der Nutzer als Erlebnis wahrnimmt, prägen deshalb die Wallets und Anwendungen, die den Code für ihn schreiben und pflegen, während das Protokoll allein die Freiheit verbürgt, in der sie es tun. Die Grenze zwischen dem, was Ethereum selbst leistet, und dem, was die Schicht darüber daraus macht, verläuft genau an der Stelle: Das Protokoll stellt die programmierbare Validierung bereit, und die Wallet macht daraus das für den Nutzer bedienbare Konto.[263]

[263] Der heute aktive Unterbau der Account Abstraction: ERC-4337 (Account Abstraction über einen separaten Mempool, DEPL seit März 2023) etabliert Smart-Contract-Konten mit programmierbarer Signaturprüfung, Gas-Sponsoring und Batching auf der Anwendungsebene; über 40 Millionen solcher Konten sind ausgerollt. EIP-7702 (DEPL mit Pectra, Mai 2025) hebt die programmierbare Validierung auf die Protokollebene, indem es einer bestehenden EOA erlaubt, temporär an Smart-Contract-Code zu delegieren; innerhalb der ersten Woche nach Aktivierung verzeichnete Mainnet über 11.000 Autorisierungen, mit Wallet-Unterstützung durch MetaMask, Trust Wallet, Ambire und Ledger. Die Passkey-Authentifizierung ruht auf der secp256r1-Precompile (EIP-7951, DEPL im Fusaka-Zyklus, Dezember 2025), die die von FIDO2/WebAuthn und der Apple Secure Enclave genutzte Kurve nativ verfügbar macht.

Der Preis der Leichtigkeit

Die gewonnene Leichtigkeit hat ihren Preis an derselben Naht, an der sie entsteht. Die Bindung der Wiederherstellung an Vertrauens-Instanzen gibt Sicherheit gegen den Verlust und schafft zugleich eine Abhängigkeit von deren Verfügbarkeit und Redlichkeit, deren Zusammenwirken den Zugang im Ernstfall überhaupt erst trägt. Die Übernahme der Gebühr durch einen Dritten verlangt dessen fortgesetzte Bereitschaft. Die Führung des Kontos über eine bestimmte Anwendung verlässt sich darauf, dass deren Validierungs-Code korrekt geschrieben ist und gepflegt bleibt. Die Bequemlichkeit verlagert damit einen Teil dessen, was der Nutzer im heutigen Zustand allein verantwortet, auf Anbieter, deren Auswahl er zwar selbst trifft, deren Verhalten er anschließend aber nur begrenzt kontrolliert. Wie weit die niedrige Einstiegshürde am Ende trägt, hängt davon ab, ob diese Schicht die gewonnene Komplexität verlässlich verbirgt, und dieser Teil der Antwort liegt außerhalb dessen, was das Protokoll selbst verbürgen kann.[264]

Der freiwillige Wechsel der Signatur

Dieselbe programmierbare Validierung, die das Konto leichter zu führen macht, erlaubt ihm einen weiteren und schwerer wiegenden Schritt, den Wechsel des Verfahrens, mit dem es seine Unterschrift bildet. Die ECDSA-Unterschrift, an die jedes Konto heute gebunden ist, beruht auf jener Kryptographie elliptischer Kurven, deren Sicherheit ein hinreichend großer Quantenrechner aufhebt, und sie ist damit die größte einzelne Quanten-Schwachstelle, die den Nutzer unmittelbar an seinem Eigentum trifft. Über ein eigenes Transaktions-Format, die Validation Frames, kann ein bestehendes Konto seine Unterschrift auf ein quantensicheres Verfahren umstellen, etwa auf eine hash- oder gitterbasierte Signatur, deren hier einzig wesentliche Eigenschaft ihr deutlich größerer Schlüssel ist.[265] Das Protokoll verbietet die alte Unterschrift dabei nicht. Es stellt die neue als freiwillige Möglichkeit daneben, sodass jedes Konto den Zeitpunkt seiner Migrati-

[264] Die Verlagerung auf die Anwendungsebene ist im Bewertungsrahmen der Arbeit angelegt: Das Kriterium II.4 führt die Netto-Inklusivität ausdrücklich als davon abhängig, ob Wallet-Anbieter und dApp-Entwickler die gewachsene konzeptuelle Komplexität für den Endnutzer abstrahieren, was außerhalb des Protokolls liegt. Das Ausmaß der heutigen Gebühren-Übernahme zeigt die ERC-4337-Adoption: 2024 entfielen rund 87 Prozent aller UserOperations auf von einem Paymaster gesponserte Transaktionen, bei einem gesponserten Gas-Volumen von etwa 3,4 Millionen US-Dollar.

[265] Frame Transactions (EIP-8141, PLAN, per Checkpoint #9 vom 10. April 2026 als CFI Hegotá Non-Headliner und Platzhalter-Commitment für native Account Abstraction geführt) bündeln in einem neuen Transaktions-Typ unter anderem die programmierbare Validierungslogik anstelle der festen ECDSA-Prüfung sowie die native Umstellung von ECDSA auf quantensichere Verfahren wie ML-DSA, SLH-DSA oder STARK-basierte Signaturen. Sie bauen auf der vollständigen nativen Account Abstraction (EIP-7701, PLAN) auf. Ein generischer Alternativpfad, der sekundäre Signaturverfahren protokollseitig zulässt, liegt in EIP-7932 (Secondary Signature Algorithms) vor.

on selbst wählt. Tragbar bleiben die je Unterschrift zunächst prohibitiven Kosten des quantensicheren Verfahrens allein durch die Aggregations-Mechanik aus 5.3-A′, die viele solcher Unterschriften zu einem Beweis zusammenfasst und ihren Prüfaufwand in der Masse auf einen geringen Anteil je Block senkt.[266] Der freiwillige Charakter dieser Umstellung ist derselbe, der den Zugang von Beginn an niedrigschwellig hält, weil das Konto auch hier selbst bestimmt, welche Validierungslogik es trägt.

Abschnitt 5.3 schließt damit den Bogen von der Prüfung eines ganzen Blocks auf gewöhnlicher Hardware bis zu der untersten Prüfung, an der das Protokoll die Unterschrift eines einzelnen Kontos misst, und sie zeigt auf jeder Stufe dieselbe Bewegung. Die reduzierte Datenstruktur verkleinerte den Beweis, den eine Prüfung benötigt, und die entlastete Hardware brachte diese Prüfung auf das Gerät des gewöhnlichen Nutzers. Von den zentralen Datendiensten löste sie die Trustless RPC Architecture, gegen den Quantenübergang sicherte die Post-Quantum-Migration ihre kryptographische Grundlage. Die unterste der Prüfungen, die der Nutzer-Signatur, legte die programmierbare Validierung schließlich in die Hand des Nutzers selbst. Auf jeder Stufe verbürgt das Protokoll eine tragfähige und quantensicher migrierbare Grundlage, während die Brauchbarkeit für den Nutzer erst auf der Schicht darüber entsteht, die das Fundament für den Menschen nutzbar macht.

Der freiwillige Wechsel der Nutzer-Signatur, mit dem der Abschnitt geschlossen hat, trägt jedoch eine Folge, die über die Verifikation hinausreicht. Ein quantensicherer Schlüssel wie der einer ML-DSA-Signatur ist um Größenordnungen größer als der heutige ECDSA-Schlüssel, und jedes Konto, das ihn übernimmt, hinterlegt den größeren Schlüssel dauerhaft im Zustand des Netzwerks.[267] Migrieren viele Konten, summieren sich die größeren Schlüssel zu einem spürbaren Anschwellen des State, das keine Signatur-Aggregation senkt, weil die Aggregation den Prüfaufwand der Unterschriften verkleinert und nicht die dauerhaft gespeicherte Datenmenge. Eben dieses Anschwellen des Zustands, das die Migrati-

[266] Die tragbaren Kosten der quantensicheren Unterschrift ruhen auf der in 5.3-A′ entfalteten Aggregations-Mechanik. Die Roadmap-Quantifizierung beziffert eine klassische ECDSA-Signatur mit rund 3.000 Gas und eine unaggregierte hash-basierte Einzelsignatur mit rund 200.000 Gas, deren amortisierter Pro-Signatur-Anteil in der Aggregations-Charge auf einen tragbaren Wert zurückfällt. Quelle: Vitalik Buterin, „Possible Futures of the Ethereum Protocol — Post-Quantum Roadmap“, 26. Februar 2026; vgl. 5.3-A′.

[267] Zur Schlüssel- und Signaturgröße und ihrer State-Folge: Quantensichere Verfahren (ML-DSA, SLH-DSA) erzeugen deutlich größere Signaturen, in der Größenordnung von 2,4 bis 4,6 Kilobyte bei ML-DSA und 7,9 bis 49,9 Kilobyte bei SLH-DSA gegenüber 64 Byte einer ECDSA-Signatur, sowie einen höheren State Bloat von etwa dem Neunundfünfzigfachen bei ML-DSA, der aus dem dauerhaft im Zustand hinterlegten öffentlichen Schlüssel des migrierten Kontos stammt. Tiered State und die State-Tree-Migration mildern die Storage-Folge, während die Bandbreiten-Frage eine offene Forschungsfrage bleibt.

on der Verifikation als ihre Nebenfolge erzeugt, ist der Gegenstand des folgenden Abschnitts.

5.4 State und Speicherpersistenz

5.4-A Warum State anders ist

Das Anschwellen des Zustands, auf das die Migration der Nutzer-Signatur am Ende des vorigen Abschnitts verwies, ist nur der jüngste Druck auf eine Ressource, deren Schwierigkeit tiefer reicht als jede einzelne ihrer Lasten. Der in 5.2-D formulierte strukturelle Befund, Execution hat einen Durchbruchsmechanismus, Data hat einen, State hat keinen, lässt eine zweite Ebene der Asymmetrie sichtbar werden: die Natur der Ressource selbst.[268] Execution und Data lassen sich delegieren: Die zkEVM verlagert die Verifikationslast auf einen Proof, PeerDAS die Datenverfügbarkeit auf ein Sampling-Verfahren (vgl. Abschnitt 5.2 und 5.2-D). Beide Mechanismen erlauben es einzelnen Nodes, nur einen Bruchteil der Gesamtarbeit zu leisten und trotzdem vollständig zu verifizieren. State erlaubt diese Delegation nicht. Ein Builder, der einen gültigen Block produzieren will, muss den vollständigen State vorhalten, jeden Account-Stand, jeden Storage Slot, jeden Contract-Bytecode. Ein niedrigeres Gas Limit verkleinert einzelne Blöcke. Der akkumulierte State bleibt davon unberührt. Buterin bringt diese Asymmetrie auf eine Formel: Für Execution gibt es die zkEVM, für Data gibt es PeerDAS, für State gibt es kein vergleichbares Instrument.[269]

Zwei Engpässe begrenzen die State-Skalierung, und nur einer davon ist prinzipiell lösbar. Der kurzfristige Engpass liegt in der Datenbankeffizienz: Heutige Client-Datenbanken sind nicht für Multi-Terabyte-States ausgelegt, und jede State-Schreiboperation erfordert logarithmisch wachsende Tree-Updates.[270] Neue Datenbank-Designs und Block Access Lists können diesen Engpass entschärfen. Der langfristige Engpass entzieht sich der Art von technischer Lösung. Das Synchronisieren eines State von mehreren Terabyte erfordert selbst bei perfekter Bandbreiteneffizienz signifikante Zeit, weil der gesamte State-Tree traver-

[268] Execution: zkEVM ermöglicht Faktor-1000-Skalierung (vgl. 5.2). Data: PeerDAS (DEPL) und perspektivisch Full Danksharding (RES) ermöglichen Faktor-500-Skalierung. State: kurzfristig Faktor 5–30 durch Datenbank-Optimierungen und Block Access Lists, langfristig kein vergleichbarer Mechanismus.

[269] Vitalik Buterin, „Hyper-scaling Ethereum state by creating new forms of state“, ethresear.ch/t/24052, 5. Februar 2026. Sinngemäße Wiedergabe der Formulierung.

[270] State Writes erfordern log(n) Tree-Updates mit jeweils log(n) Datenbank-Operationen. Sobald die State-Größe den verfügbaren RAM übersteigt, steigen die I/O-Kosten durch Zugriffe auf den Sekundärspeicher sprunghaft an.

siert und verifiziert werden muss. Mit jeder Verdopplung der State-Größe sinkt die Zahl der Akteure näherungsweise auf die Hälfte, die bereit und technisch in der Lage sind, den vollständigen State vorzuhalten. Kein Datenbank-Design kann den Zusammenhang auflösen, solange ein einzelner Builder den gesamten State lokal vorhalten muss.

Diese Synchronisierungsgrenze hat direkte Konsequenzen für die Dezentralisierung des Block Building. Wenn nur noch Betreiber mit Server-Hardware den State synchronisieren können, verengt sich der Kreis der Block Builder. Die Verengung trifft genau die Rolle des Block Builders, die der SOLL-Zustand durch die Trennung von Proposer und Builder protokollär verankert. Die Skalierungshierarchie offenbart damit eine Asymmetrie, die die Dezentralisierungsannahmen des Skalierungspfads oberhalb von 500 Millionen Gas unter Vorbehalt stellt.

Woraus der State besteht

Ethereums State umfasst Stand Q1 2026 rund 430 GiB, doch entscheidend für die Building-Frage ist die Zusammensetzung dieses Volumens.[271] 81,7 Prozent entfallen auf Contract Storage, wobei ERC-20-Token-Balances mit 27,2 Prozent und ERC-721-Daten mit 21,6 Prozent die größten Einzelkategorien bilden.[272] Der überwiegende Teil dieses States wird nicht aktiv genutzt: Rund 80 Prozent sind seit mehr als einem Jahr unberührt. 63 Prozent aller Storage Slots wurden nur ein einziges Mal beschrieben.[273] Mehr als die Hälfte aller Contracts besitzt überhaupt keine Storage Slots und belegt trotzdem Platz im State-Tree. Das Protokoll unterscheidet nicht zwischen aktivem und inaktivem State: Beide belegen denselben Speicher, erfordern dieselbe Synchronisation und erzeugen für jeden Builder dieselben Vorhaltekosten. Ein Builder, der einen gültigen Block produzieren will, synchronisiert den gesamten State, einschließlich der 80 Prozent, die seit Jahren niemand abgerufen hat. Bei konstantem Gas Limit von 60 Millionen wächst der State um rund 100 bis 125 GiB pro Jahr, was bis 2030 ein Volu-

[271] State-Größe rund 430 GiB per Q1 2026, mit Bandbreite 410–450 GiB je nach Client-Implementierung und Compression-Modus. Quellen: Maria Silva (ethresear.ch/t/23476, November 2025) misst 340 GiB im Mai 2025 (uncompressed, Geth-Node, dedicated to state); Vitalik Buterin (ethresear.ch/t/24052, Februar 2026) gibt das aktuelle Wachstum mit rund 100 GB pro Jahr an. Die Q1-2026-Schätzung folgt aus dem Mai-2025-Ausgangswert plus zweistufigem Wachstum gemäß Gas-Limit-Pipeline (36M bis Juni 2025, 45M Juli–November 2025, 60M ab Dezember 2025).

[272] Paradigm (2024): Contract Storage 81,7 Prozent, Accounts 14,1 Prozent, Bytecodes 4,3 Prozent. Innerhalb des Contract Storage: ERC-20-Token-Balances 27,2 Prozent, ERC-721-Daten 21,6 Prozent.

[273] Han / EF Research: rund 80 Prozent inaktiver State (>1 Jahr unberührt), 63 Prozent Single-Use Storage Slots, 54 Prozent Stateless Contracts (ohne Storage Slots), ≥7,4 Prozent dormanter State (aufgegebene Protokolle).

men von rund 830 bis 930 GiB ergibt.[274] Das bleibt innerhalb handelsüblicher 2-TB-SSDs. Doch die kritische Schwelle liegt früher: Empirische Stress-Tests der Bloatnet-Initiative identifizieren bei rund 650 GiB einen Performance-Cliff, an dem State-Access-Zeiten um 40 Prozent ansteigen und Sync-Zeiten sich exponentiell verlängern.[275] Nach dem Skalierungs-Modell von Maria Silva wird diese Schwelle bei konstantem Gas Limit bereits Mitte 2027 überschritten, nach linearer Fortschreibung der eigenen Wachstumsrate um den Jahreswechsel 2027/28. Die Roadmap sieht keine Konstanz vor.

Der in 5.2 dargestellte Gas-Limit-Pfad verändert die Rechnung von Grund auf. Der exponentielle Gas-Limit-Pfad nach EIP-9698 würde bei kontinuierlichem Validator-Voting das Limit bis Mitte 2027 auf 500 Millionen treiben. Bis Mitte 2029 stiege es auf fünf Milliarden. Operativ sind die tatsächlichen Schwellen abhängig von Feature-Reife und Client-Benchmarks, sodass die Zeitlinie sich um ein bis zwei Jahre verschieben kann.[276] Die Korrelation zwischen Gas Limit und State-Wachstum ist nicht linear: Ein historisch beobachteter Korrekturfaktor von etwa 1,5 dämpft den Effekt, weil nicht jedes zusätzliche Gas in State-Schreiboperationen fließt.[277] Selbst mit der Dämpfung erreicht der kumulative State ohne Gegenmaßnahmen rund 2,7 bis 7,0 TB bis 2030. Bereits 2028 überschreitet er in der konservativen Schätzung ein Terabyte, in der aggressiven fast zwei.[278] 2-TB-SSDs reichen ab dem Punkt für Block Builder nicht mehr aus. Block Builder bräuchten Server-Infrastruktur mit 8 bis 16 TB, wie sie heute in Rechenzentren üblich ist und in den Arbeitszimmern unabhängiger Block Builder fehlt.

---

[274] Wachstumsraten 100–125 GiB/Jahr bei 60M Gas Limit. Quellen: Vitalik Buterin (ethresear.ch/t/24052, Februar 2026) gibt rund 100 GB/Jahr; Maria Silvas Skalierungs-Modell (ethresear.ch/t/23476, November 2025) ergibt 124 GiB/Jahr (342 MiB/Tag mal 365 Tage). Die Bandbreite reflektiert Mess-Unterschiede zwischen Clients und Compression-Modi. Die historische Paradigm-Schätzung von 31–72 GiB/Jahr (März 2024, bei 30M Gas Limit) ist mit dem aktuellen 60M-Gas-Limit-Stand nicht mehr direkt vergleichbar.

[275] Bloatnet Initiative (cperezz.github.io/bloatnet-website), Carlos Pérez et al., 2025–2026. Empirische Stress-Tests an einem dedizierten Testnet identifizieren bei rund 650 GiB einen Performance-Cliff: State-Access-Zeiten steigen um etwa 40 Prozent, Memory-Konsum erhöht sich exponentiell, Sync-Zeiten verlängern sich substanziell. Maria Silvas Skalierungs-Modell (ethresear.ch/t/23476, November 2025) projiziert für Mitte 2027 in allen drei Gas-Limit-Szenarien (conservative 686 GiB, base 859 GiB, aggressive 1.080 GiB) ein Überschreiten dieser Schwelle.

[276] EIP-9698 definiert den exponentiellen Gas-Limit-Erhöhungspfad. Vgl. 5.2 für die vollständige Darstellung.

[277] Paradigm (2024): Historisch beobachteter Korrekturfaktor rund 1,5 zwischen Gas-Limit-Verdopplung und State-Growth-Steigerung, weil ein Teil des zusätzlichen Gas in Execution und reine Calldata fließt.

[278] Eigene Projektion auf Basis der aktualisierten Wachstumsraten (Fn. 7) und des EIP-9698-Pfads (vgl. 5.2). Die Projektion summiert das jährliche State-Wachstum über die EIP-9698-Steigerungsstufen, jeweils korrigiert um den in Fn. 10 beschriebenen Korrekturfaktor von rund 1,5 (Gas-Limit-Verdopplung erzeugt rund 1,5-faches State-Wachstum, nicht 2-faches). Ausgangspunkt ist die Q1-2026-State-Größe von rund 430 GiB (vgl. Fn. 4). Die konservative Schätzung (2,7 TB) legt die untere Wachstumsrate (100 GiB/Jahr bei 60M Gas, hochskaliert über EIP-9698) zugrunde, die obere Schätzung (7,0 TB) eine Wachstumsrate von 125 GiB/Jahr in derselben Skalierung. Hardware-Anforderung ab rund 2 TB: 8–16-TB-SSD (Server-Klasse).

Ein differenziertes State-Modell, das neue restriktivere State-Typen einführt und bestehenden State unangetastet lässt, könnte den permanenten State auf 1,2 bis 1,5 TB begrenzen.[279] Vor dem Weg dorthin steht eine Sackgasse, die zuerst verstanden werden muss.

History als gelöster Kontrast

History zeigt im Kontrast zu State, wie ein gelöstes Speicherproblem in der Praxis aussieht. History Expiry nach EIP-4444 (vgl. Abschnitt 5.3-C) ermöglicht allen fünf Execution Clients, historische Blöcke, Transaktionen und Receipts nach einem definierten Zeitraum zu löschen.[280] Die Einsparung beträgt 300 bis 500 GB pro Node, wodurch Full Nodes auf 2-TB-Disks wieder Reserve haben.[281] Vor dem Pruning benötigten sie über ein Terabyte. Archive Nodes in der Geth-Implementierung erreichten 15 bis 20 TB.[282] Das Portal Network archiviert die gelöschten Daten dezentral über drei unabhängige Clients, eine Architektur, die in 5.3-C als Baustein der vertrauensfreien Verifikationsinfrastruktur beschrieben wird.[283] Wer historische Daten benötigt, ruft sie aus dem Netzwerk ab. Rolling Window Expiry als nächste Phase erweitert dieses Modell auf fortlaufendes Pruning und ist im Governance-Prozess verankert.[284]

Der Kontrast zwischen History und State verschärft den Befund für die Gesamtarchitektur. History ließ sich delegieren: Historische Daten können geprunt und bei Bedarf aus dem Netzwerk abgerufen werden, weil kein laufender Prozess sie permanent vorhalten muss. State ist das genaue Gegenteil, er wird bei jedem Block gebraucht, von jedem Builder, vollständig. Das einzige Speicherproblem, das Ethereum bisher strukturell gelöst hat, war kein State-Problem. Einen direkten Lösungsversuch für State gab es: State Expiry sollte ungenutzten State nach einem definierten Zeitraum verfallen lassen. Der Versuch scheiterte an einem fundamentalen technischen Hindernis.

---

[279] Vitalik Buterin, „Hyper-scaling Ethereum state by creating new forms of state“, ethresear.ch/t/24052, 5. Februar 2026.

[280] EIP-4444: History Pruning für Pre-Merge-Daten. Alle fünf Execution Clients (Geth v1.16.0+, Nethermind v1.32.2+, Besu v25.7.0+, Erigon v3.0.12+, Reth v1.5.0+) unterstützen History Pruning seit Juli 2025.

[281] Pre-Merge Data Savings: 300–500 GB. Full Nodes nach Pruning auf 2-TB-Disk lauffähig.

[282] Archive Nodes (Erigon-optimiert): 3–3,5 TB vs. 15–20 TB (Geth).

[283] Portal Network: DHT-basiert, drei unabhängige Clients (Trin/Rust, Fluffy/Nim, Ultralight). Vgl. 5.3-C für die Rolle im Verifikationsstack.

[284] History Expiry Rolling Window (EIP-4444 Phase 2): PLAN-Status im Governance-Prozess.

5.4-B State Expiry und Tiered State

Das fundamentale Hindernis liegt in der Forderung nach Inexistenz-Beweisen.[285] Wenn ein Nutzer einen neuen State erzeugt, an einer Adresse oder einem Storage Slot, muss das Protokoll verifizieren, dass an dieser Stelle in Ethereums gesamter Geschichte nie zuvor etwas existierte, und nicht allein in der aktuellen Periode. Ohne State Expiry ist diese Prüfung trivial: Was nicht im aktuellen State-Tree steht, existiert nicht. Sobald das Protokoll State verfallen lässt, verliert diese Prüfung ihre Grundlage. Ein Slot, der leer erscheint, könnte einen verfallenen State enthalten, der jederzeit reaktivierbar wäre. Die Unterscheidung zwischen „nie belegt" und „einmal belegt, dann verfallen" erfordert einen historischen Beweis, den das Protokoll nicht effizient erbringen kann.

Für Accounts existiert ein partieller Lösungsansatz: CREATE3 würde Adressen an Erstellungsperioden binden, sodass eine Adresse nachweislich erst ab Jahr N existieren kann.[286] Für Storage Slots gibt es keine vergleichbare Absicherung: Ein ERC-20-Balance für Account X wird unter keccak256(..., X) gespeichert, einem Hash, der dem Protokoll opak ist.[287] Das Protokoll sieht einen Slot. Es sieht nicht, dass der Slot einen Token-Balance repräsentiert, der einem konkreten Nutzer gehört. State Expiry für Storage Slots ist daher nicht rückwärtskompatibel umsetzbar, ohne die ERC-20-Logik vollständig umzuschreiben. Sämtliche bestehenden Token-Contracts, deren Balances zusammen 27,2 Prozent des State ausmachen, sind zu migrieren.[288]

Im September 2025 zog Buterin die Konsequenz: State Expiry sei aufzugeben zugunsten von Partial State Nodes, die funktional ähnlich seien, ohne Consensus-Layer-Änderungen auskämen und deutlich flexibler seien.[289] Die Ethereum Foundation hielt im Dezember 2025 die konzeptionelle Option zwar offen, doch Workstream, Team und Diskussionspunkt in den All Core Developers Calls fehlen.[290] State Expiry ist faktisch aufgegeben.

---

[285] Das Problem der Inexistenz-Beweise wird in Vitalik Buterin, „Hyper-scaling Ethereum state by creating new forms of state", ethresear.ch/t/24052, 5. Februar 2026, als zentrales Hindernis identifiziert. Ergänzend: EF Research, State Expiry Design Space, 2024.

[286] CREATE3 (Address Period Mechanism): Adressen, die nachweislich erst ab einer bestimmten Periode erstellt werden können. Konzeptueller Ansatz ohne EIP-Finalisierung.

[287] ERC-20-Storage-Slots werden über keccak256(abi.encode(address, slot)) berechnet. Das Ergebnis ist dem Protokoll semantisch opak: Es sieht einen 256-Bit-Schlüssel, nicht dessen Bedeutung.

[288] Paradigm (2024): ERC-20-Token-Balances 27,2 Prozent des Contract Storage.

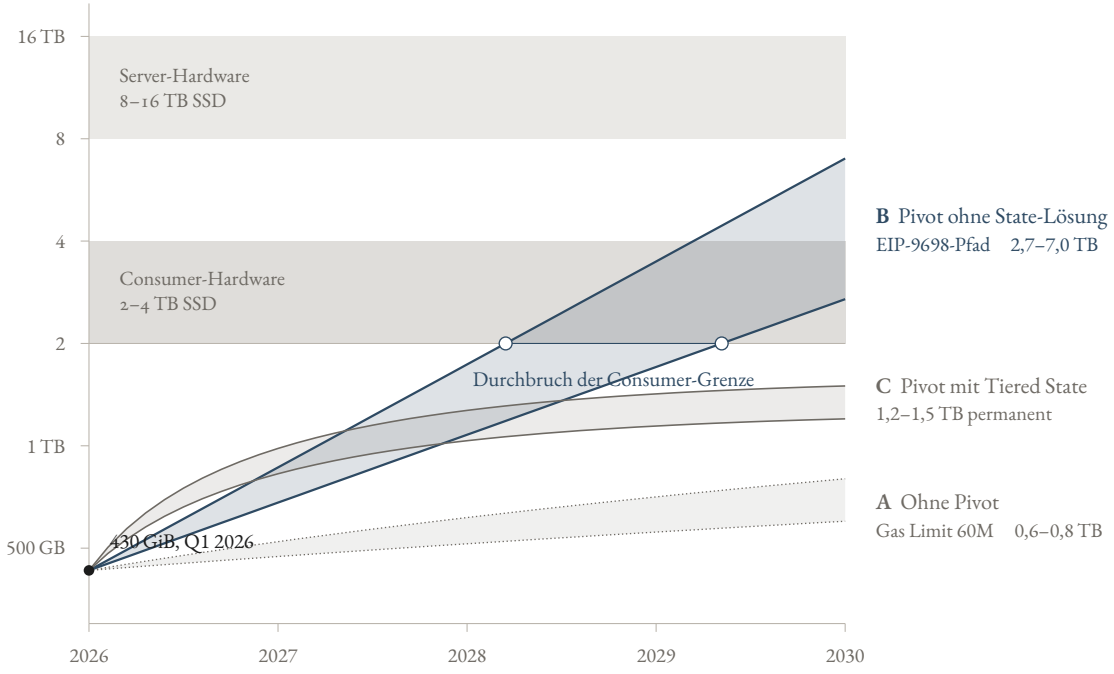
[289] Vitalik Buterin, 19. September 2025, sinngemäß: „Don't do state expiry, do partial state nodes." Partial State Nodes erfordern keine Consensus-Layer-Änderungen.

[290] EF Blog, Dezember 2025: State Expiry konzeptionell nicht ausgeschlossen, aber kein aktiver Workstream.

Tiered State: der umgekehrte Hebel

Das Scheitern von State Expiry erklärt, warum der einzige verbleibende Ansatz einen grundsätzlich anderen Weg wählt. State Expiry sollte ungenutzten State automatisch aus dem aktiven Datensatz entfernen. Genau das erwies sich als unmöglich, solange das Protokoll nicht zwischen aktivem und verfallbarem State unterscheiden kann. Tiered State (RES, ethresear.ch-Post Februar 2026) setzt am entgegengesetzten Punkt an: Bestehender State bleibt vollständig unangetastet. Stattdessen werden neue, billigere, aber restriktivere State-Typen eingeführt, die das künftige Wachstum kanalisieren.[279]

Die Architektur setzt auf zwei Extreme statt auf einen Mittelweg und stellt drei State-Typen nebeneinander. Permanenter State umfasst Accounts, Core Contracts und alle Daten, die bei jedem Block vollständig und ohne zusätzliche Abrufkosten verfügbar sein müssen. Temporary Storage wird zu jedem Periodenbeginn auf Null gesetzt, vorgesehen für kurzlebige Daten mit einem monatlichen Reset-Zyklus. UTXOs treiben dieses Prinzip auf die Spitze: Ihre Expiry Period ist Null, sie verfallen unmittelbar nach Verbrauch.[291] Bestehender Contract-Code, bestehende Balances, bestehende DeFi-Positionen bleiben im permanenten Tier. Die Wachstumsbegrenzung entsteht über die Anreizstruktur: Neue Anwendungen wählen die restriktiveren Typen, sobald permanente Persistenz nicht erforderlich ist. Eine Löschung bestehender Daten findet nicht statt.



[291] Ebd. Drei State-Typen: Permanent (Accounts, Core Contracts), Temporary Storage (monatlicher Reset), UTXOs (sofortiger Expiry). Vitaliks vierter Typ (Strong-Stateless Storage Tree) wurde im selben Post verworfen.

Abbildung 5.4-B.1 State-Wachstum-Szenarien. Drei Projektionen: (A) Ohne Pivot, konstantes Gas Limit 60M → 600–800 GB bis 2030. (B) Pivot ohne State-Lösung, EIP-9698-Pfad → 2,7–7,0 TB bis 2030. (C) Pivot mit Tiered State → 1,2–1,5 TB permanenter State bis 2030. Referenzlinien: Consumer-Hardware (2–4 TB SSD), Server-Hardware (8–16 TB SSD).

Die größten State-Verbraucher wären die ersten Kandidaten für die restriktiveren Tiers. ERC-20-Token-Balances beanspruchen 27,2 Prozent des aktuellen State, ERC-721-Daten weitere 21,6 Prozent.[292] Beide könnten dem UTXO- oder Temporary-Tier zugeordnet werden, individuelle DeFi-Positionen ebenfalls.

Die Frage „In welchem Tier speichere ich diese Daten?" existiert im heutigen Ethereum nicht. Sie würde zur zentralen Designentscheidung jedes neuen Contracts werden, vergleichbar mit der Wahl zwischen Calldata und Blob-Storage, die Proto-Danksharding für L2-Betreiber eingeführt hat. Die Calldata-Blob-Entscheidung betraf allerdings eine Handvoll Rollup-Teams. Die Tier-Entscheidung beträfe jeden Smart-Contract-Entwickler im Ökosystem. Kein Protokoll-Upgrade kann diese Umstellung erzwingen: Sie erfordert die freiwillige Übernahme neuer Token-Standards, die Anpassung bestehender Toolchains und die Koordination eines Ökosystems, das sich auf permanenten State als Standardannahme eingestellt hat.

Ein Pricing-Modell, das nicht existiert

Selbst wenn das Ökosystem diese Koordination leisten könnte, stünde Tiered State vor ungelösten technischen Abhängigkeiten. Das mehrstufige System setzt eine effiziente State-Tree-Struktur voraus, wie sie Verkle Trees (EIP-6800, RES, Stagnant) oder Binary Trees (EIP-9257, RES) liefern.[293] Diese State-Separation allein reicht nicht: Das System braucht separate Gas-Dimensionen für verschiedene Tiers, damit die ökonomischen Anreize die gewünschte Allokation erzeugen. Multidimensionales Gas (EIP-8011, RES/DFI Glamsterdam) und Inter-Block Temporal Locality Gas Discounts (EIP-8057, RES/DFI Glamsterdam) sind die technischen Voraussetzungen für diese Preisdifferenzierung, analog zum Blob-Pricing-Template, das EIP-4844 für Datenblobs etabliert hat.[294] Das Blob-Pricing baut auf einem funktionierenden EIP und einem deployten Mecha-

[292] Paradigm (2024): ERC-20 27,2 Prozent, ERC-721 21,6 Prozent des Contract Storage. Vgl. Fn. 5 in 5.4-A.

[293] Verkle Trees (EIP-6800, RES, Stagnant) oder Binary Trees (EIP-9257, RES) als Voraussetzung für die State-Separation im Tiered-State-Modell. Das EF Protocol Priorities Update vom 18. Februar 2026 signalisiert Binary Trees als langfristige Richtung; Verkle ist deployment-fähig, aber durch die Quantum-Anfälligkeit der Pedersen Commitments als Übergangslösung markiert. Vgl. 5.3-A für die vollständige Darstellung der Tree-Transition.

[294] EIP-4844 (Proto-Danksharding) führte mit der Dencun-Aktivierung im März 2024 separates Blob-Gas-Pricing ein und gilt nach Kapitel-2-Definition (über zwei Jahre stabil) als IMPL. Tiered State erfordert eine analoge Erweiterung auf State-Tiers. EIP-8011 (Multidimensional Gas Metering) und EIP-8057 (Inter-Block Temporal Locality Gas Discounts) waren beide für Glamsterdam als CFI gelistet und sind per EIP-7773 als RES/DFI Glamsterdam deklassifiziert worden; sie bleiben Forschungsrichtungen ohne Fork-Zuordnung.

nismus auf. Für State-Tiers existiert das Pricing-Modell bisher nur konzeptionell. EIP-Entwurf, Referenzimplementierung und Simulation der Marktdynamik zwischen den Tiers fehlen. Tiered State setzt Multidimensionales Gas voraus. Multidimensionales Gas setzt ein spezifiziertes Pricing-Modell voraus. Das Pricing-Modell existiert nicht.

Ein kleinerer Vorläufer dieser Pyramide unterstreicht die Distanz zwischen Konzept und Umsetzung. EIP-8032 (Size-Based Storage Pricing, RES/DFI Glamsterdam) hätte die Storage-Kosten an die tatsächliche Speicher-Größe gekoppelt und damit einen ersten Baustein der Storage-Repricing-Architektur geliefert, die Tiered State voraussetzt.[295] Der EIP war für die Glamsterdam-Inclusion-Liste vorgesehen und wurde per EIP-7773 zurückgestuft. Die argumentative Lage ist damit klar: Die Tiered-State-Architektur erfordert mehrere Repricings, und schon der kleinste vorgesehene Baustein hat den ersten Fork-Zyklus nicht erreicht.

Die ethresear.ch-Diskussion vom Februar 2026 zeigt, dass auch innerhalb der Research-Community kein Konsens besteht.[296] Der konservativste Einwand betrifft die Reihenfolge: Der Nutzer MicahZoltu im Ethereum-Magicians-Forum fordert, State-Expansion erst dann zuzulassen, wenn mindestens eine nutzerbetriebene RPC-Node den vollständigen State bedienen könne.[297] Diese Bedingung ist heute nicht erfüllt, zumal State-Expansion selbst ihre Erfüllung zusätzlich erschweren würde. Selbst wenn die Reihenfolge geklärt wäre, bliebe ein architektureller Trade-off: Verschiedene Tiers erzeugen unterschiedliche Zugriffsmuster, aus denen sich Rückschlüsse auf die Nutzung eines Contracts ziehen lassen. Der Nutzer igor53627 identifiziert darin ein Privacy-Risiko, das im aktuellen Ethereum nicht existiert.[298] Der radikalste Gegeneinwand stellt die Prämisse selbst in Frage: der Nutzer kladkogex argumentiert, dass Parallelisierung über Node-Cluster das State-Problem trivialisiere und ein mehrstufiges System daher unnötige Komplexität einführe.[299]

Diese Einwände treffen auf einen Vorschlag im frühesten denkbaren Entwicklungsstadium. Tiered State ist ein ethresear.ch-Post und steht weder als

[295] EIP-8032 (Size-Based Storage Gas Pricing, RES) skaliert die Storage-Kosten mit dem State-Footprint eines Contracts und verteuert damit größere State-Einträge. Der EIP war für die Glamsterdam-Inclusion-Liste vorgesehen und wurde per EIP-7773 in die Declined-for-Inclusion-Liste verschoben; eine Wieder-Aufnahme in Hegotá oder eine spätere Fork ist denkbar.

[296] ethresear.ch/t/24052, Diskussionsthread, Februar 2026. Reviewers u.a.: Guillaume Ballet, Marius van der Wijden, Justin Drake.

[297] MicahZoltu, Kommentar in ethresear.ch/t/24052, Februar 2026, sinngemäß.

[298] igor53627, Kommentar in ethresear.ch/t/24052, Februar 2026, sinngemäß.

[299] kladkogex, Kommentar in ethresear.ch/t/24052, Februar 2026. Argument: horizontale Skalierung über Node-Cluster als Alternative.

EIP-Draft noch auf der Tagesordnung der All Core Developers Calls. Forschungsteam, Fürsprecher im Client-Ökosystem und Fork-Zeitplan fehlen. Von den Features, die eine Kernressource adressieren, befindet sich keines in einem vergleichbar frühen Stadium. Tiered State ist zugleich das einzige Feature, das Aussicht auf eine langfristige Antwort auf die in 5.4-A beschriebene Skalierungshierarchie-Asymmetrie bietet.

5.4-C Der Timing-Widerspruch

Lösung und Problem bewegen sich damit auf grundsätzlich unterschiedlichen Zeitskalen. Der Gas-Limit-Pfad nach EIP-9698 treibt den State ab 2027 in Bereiche, in denen eine Managementlösung strukturell notwendig wird. Die einzige vorgeschlagene Lösung hat weder eine Spezifikation noch einen Zeitplan. Das Gas Limit hingegen hat beides.

Das Gas Limit wird durch Validator-Voting gesteuert, einen dezentralen Abstimmungsprozess, der schneller konvergieren kann als die koordinierte Entwicklung komplexer Protokolländerungen. Die jüngste Erhöhung illustriert diese Geschwindigkeitsdifferenz: Das Gas Limit verdoppelte sich innerhalb eines Jahres (vgl. Abschnitt 5.1-A), während Fusaka mit PeerDAS als Kernfeature denselben Zeitraum für Spezifikation, Implementierung und Deployment benötigte.[300] Der EIP-9698-Pfad sieht eine exponentielle Steigerung vor, die das Limit bis 2028 über 500 Millionen treiben würde. Validator-Voting kommt dafür ohne neue Spezifikation, ohne Client-Implementierung und ohne koordiniertes Hard-Fork-Deployment aus. Tiered State erfordert all das und hat mit keinem dieser Schritte begonnen.

Die Konsequenz ist ein zwölf bis vierundzwanzig Monate breites Fenster, in dem die L1-Kapazität die Infrastruktur für nachhaltige Nutzung überholt.[301] In dem Fenster steigt die Fragilität: Höhere Kapazität wird genutzt, der State wächst entsprechend, aber die Mechanismen zur Differenzierung und Begrenzung dieses Wachstums fehlen. ML-DSA, der führende Post-Quantum-Signaturkandidat (RES), verschärft den Druck weiter: Seine Signaturen und Public Keys sind gegenüber ECDSA um ein Vielfaches größer.[302] Wo die Daten im State gespei-

[300] Gas Limit 30M→60M: Zeitraum Februar bis November 2025, in vier Stufen über Validator-Voting (30M→36M→45M→60M). Fusaka: DEPL Dezember 2025. Vgl. 5.2-B für die vollständige Governance-Dynamik und EIP-7935 für den formalisierten Default.

[301] Abgeleitet aus dem EIP-9698-Pfad (Gas >500M bis 2027–2028) und dem frühestmöglichen Tiered-State-Deployment (kein EIP, keine Timeline). Die Bandbreite reflektiert die Unsicherheit beider Variablen.

[302] ML-DSA (NIST FIPS 204) erzeugt Signaturen in der Größenordnung von 2,4 bis 4,6 Kilobyte gegenüber 64 Byte bei ECDSA, also rund das 38- bis 72-Fache; der State Bloat liegt bei etwa dem Neunundfünfzigfachen, weil der quantensichere öffentliche Schlüssel dauerhaft im Zustand hinterlegt wird, etwa unter Native Account Abstraction. Vgl. 5.3-D und 5.3-E für die vollständige Darstellung der Post-Quantum-Migrationspfade.

chert werden, etwa in Smart-Contract-Wallets unter Native Account Abstraction, erhöht das den State-Druck, den die in 5.3-D und 5.3-E beschriebene Post-Quantum-Migration damit zusätzlich verschärft. Das Fenster schließt sich erst, wenn die Voraussetzungen nachgeliefert werden. Die Voraussetzungskette aus 5.4-B gilt unverändert, dazu die freiwillige Übernahme neuer Token-Standards durch das gesamte Ökosystem.

Die temporäre Zentralisierung in dem Fenster betrifft genau die Rolle, die der SOLL-Zustand durch die Trennung von Proposer und Builder protokollär verankert. Wenn der State auf zwei bis drei Terabyte anwächst, bevor eine Managementlösung greift, können nur noch Betreiber mit Server-Infrastruktur den vollständigen State synchronisieren.[303] Der Kreis der Block Builder verengt sich in dem Moment, in dem das Protokoll ihn durch ePBS gerade öffnen will. Die Verifikationsschicht, die durch Stateless Clients und zkEVM vom State-Wachstum entkoppelt wird, bleibt davon unberührt. ePBS akzeptiert professionelles Building als bewussten Trade-off und schützt die Dezentralisierung über den Proposer-Satz und FOCIL (EIP-7805, SFI Hegotá-Headliner). Der Timing-Widerspruch betrifft deshalb die Zensurresistenz: Ein Builder-Markt mit zwei bis drei dominanten Akteuren stellt die Frage, ob die Inclusion Lists, die FOCIL auf Proposer-Seite sicherstellt, dem Building-Bottleneck strukturell standhalten können.

SSZ als inkrementeller Kontrast

Die SSZ-Migration (EIP-6404, EIP-6466, EIP-6493, EIP-7807, alle DRAFT) zeigt im Kontrast, dass Protokollvereinfachung auf der State-Darstellungsebene möglich ist, wenn die Änderung inkrementell verläuft.[304] SSZ ersetzt die informell spezifizierte RLP-Serialisierung durch ein typisiertes, Merkle-prüfbares Format und verbessert damit die Interoperabilität zwischen Consensus Layer und Execution Layer. Der Consensus Layer nutzt SSZ seit Dezember 2020. Die EL-Migration ist ein mehrstufiges Projekt mit Zeithorizont 2025 bis 2026 und darüber hinaus.[305] SSZ löst nicht das State-Wachstum. Es reduziert die Komplexität der State-Darstellung, eliminiert RLP-Parsing als Fehlerquelle und ermöglicht

[303] Konservative Projektion basierend auf den Szenarien in 5.4-A. Vgl. Fn. 11 für die vollständige Bandbreite (2,6–6,9 TB).

[304] SSZ EL-Migration (EIP-6404, EIP-6466, EIP-6493, EIP-7807, alle im DRAFT-Status): überführt die Serialisierung der Execution-Schicht von RLP auf SSZ (Simple Serialize), ein typisiertes, Merkle-prüfbares Format für alle EL-Datenstrukturen.

[305] Der Consensus Layer nutzt SSZ seit Dezember 2020; die EL-Migration ist ein mehrstufiges Projekt mit Zeithorizont 2025 bis 2026 und darüber hinaus und gilt als Voraussetzung der Protokollvereinfachung und der leanVM-Vision (vgl. 5.1).

direkte Zustandsbeweise. Die Vereinfachung kommt voran, weil sie rückwärtskompatibel ist und keine bestehende Developer Experience verändert.

Der Kontrast zu Tiered State verschärft den Befund. Tiered State ist weder inkrementell noch rückwärtskompatibel im selben Sinne. Es führt eine neue Designentscheidung ein, die jeder Smart-Contract-Entwickler bei jedem neuen Contract treffen müsste. Hinzu kommt die offene Voraussetzungskette aus 5.4-B. Ethereum kann State vereinfachen. State skalieren ist eine qualitativ andere Herausforderung, die über Serialisierungsformate hinausgeht und in die Kernlogik des Ökosystems eingreift.

Das Zusammenspiel aus Tiered State, Multidimensionalem Gas und differenzierten Persistenz-Stufen würde erstmals ermöglichen, State-Kosten an tatsächliche Nutzungsmuster zu koppeln: permanente Daten zu höheren Kosten, temporäre zu niedrigeren, verbrauchbare zum günstigsten Tarif. Die ökonomische Logik entspräche dem Blob-Pricing-Template (vgl. Abschnitt 5.4-B), erweitert auf die Ressource, die das Protokoll bislang undifferenziert behandelt. Dieses Zusammenspiel ist die fragilste aller Systemkombinationen in Kapitel 5, weil ihre zentrale Komponente am Anfang ihrer Spezifikation steht. Die Fragilität liegt im Abstand zwischen Entwurf und Implementierung.

Die Aussicht von Tiered State liegt damit darin, dem State die architektonische Antwort zu geben, die das Wachstum einer Kernressource langfristig tragfähig macht und die bei der History durch das Pruning bereits eingelöst ist. Solange diese Antwort fehlt, bleibt State die Dimension, in der die Roadmap keine belastbare Lösung vorweisen kann.

Die Kapazität skaliert, die Verifikation ist demokratisiert. Die Neutralität des Systems unter dieser erweiterten Leistungsfähigkeit, insbesondere die Zensurresistenz bei konzentriertem Block Building, ist nicht gesichert: Ob die protokollären Garantien gegen Zensur und Diskriminierung halten, wenn die ökonomischen Anreize sich verschieben, beantwortet Abschnitt 5.5. Die offene Flanke des State geht in diese Analyse ein. Ein System, das seine Kapazität schneller erweitert als seine Schutzmechanismen, muss die Neutralität aktiv sichern.

5.5 Neutralität und Fairness

5.5-A Das dreisäulige Zensurresistenz-System

Bis hierher hat das Kapitel die Basisschicht von drei Seiten betrachtet, und jede hat einen Teil des Zielzustands freigelegt. Die Skalierung hat gezeigt, dass die Schicht weit mehr leisten kann als heute, weil sie die Last der Ausführung in einen Beweis verwandelt und die Vorhaltung aller Daten durch ein Stichprobenverfahren ersetzt, sodass ein einzelner Block ein Vielfaches seines heutigen Volumens trägt (Abschnitt 5.2). Die Verifikation hat gezeigt, dass diese gewachsene Schicht für jedermann prüfbar bleibt, auf gewöhnlicher Hardware, ohne zentrale Dienste, hinab bis zur Unterschrift des einzelnen Kontos (Abschnitt 5.3). Und das State-Management hat die Kehrseite freigelegt: State ist die eine Ressource ohne Durchbruchsmechanismus, der Engpass, an dem sich die Produktion der Blöcke auf wenige professionelle Builder verengt, während die Verifikation sich auf tausende gewöhnliche Geräte verteilt (Abschnitt 5.4). So steht am Ende ein System, das leistungsfähiger und zugleich allgemein prüfbar ist, dessen Produktion sich aber in wenigen Händen bündelt. Bis hierher ging es darum, was die Schicht leisten kann. Nun geht es darum, was sie ihren mächtigsten Akteuren erlaubt. Dieser Abschnitt prüft die Neutralität und die Fairness der konzentrierten Schicht: ihre Neutralität daran, ob ein einzelner mächtiger Produzent eine gültige Transaktion noch ausschließen oder einen bereits bestätigten Block nachträglich aus der Kette verdrängen kann, ihre Fairness daran, ob er den Wert des Blockbaus allein für sich abschöpft. Die Antwort des Zielzustands verlagert die Neutralität von der Redlichkeit der Betreiber auf die Regeln des Protokolls, das ihnen abverlangt, was es ihnen früher anvertraute. Die grundlegendste der drei Gefahren, gegen die das Protokoll die Neutralität so erzwingt, ist das Ausschließen einer gültigen Transaktion.

Das Ausschließen trifft auf eine Grenze, die dort beginnt, wo die Verifikation endet, denn es verschiebt die Frage der Neutralität von der Korrektheit eines Blocks auf seine Vollständigkeit. Die billige Verifikation, die der vorige Teil des Kapitels auf das Gerät des gewöhnlichen Nutzers gebracht hat, fängt zuverlässig den ungültigen Block, weil tausende Validatoren ihn nachrechnen und einen Fehler im Zustandsübergang sofort verwerfen. Sie fängt jedoch nicht den gültigen Block, der eine bestimmte Adresse einfach auslässt, denn ein vollständig korrekter Block kann eine missliebige Transaktion übergehen, ohne je eine Regel zu verletzen, die das Protokoll nachprüfen könnte. Die Verifikation sichert, dass ein Block nichts Falsches enthält, und sie sagt nichts darüber, ob er alles Gültige aufnimmt. Was die Aufnahme einer gültigen Transaktion gegen das Belieben des Produzenten erzwingt, ist die Schicht, die der vorliegende Abschnitt beschreibt.

Sie tritt neben die geprüfte Korrektheit als deren notwendige Ergänzung, weil ein konzentrierter Produzent die Lücke zwischen beiden ausnutzen könnte, die das Protokoll bislang offenlässt.

Drei Stellen der Zensur

Eine gültige Transaktion lässt sich an drei Stellen aus einem Block heraushalten, und der Zielzustand schließt jede davon durch einen eigenen Mechanismus. Die erste Stelle liegt noch vor der Kette, beim Off-Chain-Relay, über das heute der weit überwiegende Teil der Blöcke läuft und an dem sich Transaktionen nach äußeren Vorgaben wie den OFAC-Listen herausfiltern lassen, obgleich die Kette selbst keine solche Filterung kennt. Die Beseitigung des Relays leistet die Enshrined Proposer-Builder Separation, die den Builder seine Gebote unmittelbar und ohne vertrauenswürdigen Zwischenhändler an die Kette richten lässt und damit den einen Punkt entfernt, an dem eine Filterung außerhalb des Protokolls überhaupt ansetzen kann. Bliebe der Relay bestehen, so liefe jede protokollär verankerte Inklusionsregel ins Leere, weil sich ihre Wirkung am Zwischenhändler umgehen ließe, sodass die Trennung von Proposer und Builder, terminiert für die frühere der beiden kommenden Forks, weniger ein Baustein der Neutralität als deren Bedingung ist.[306] Die beiden übrigen Stellen liegen innerhalb des Protokolls, bei der Wahl des Proposers und bei der Sichtbarkeit des Transaktionsinhalts, und sie verlangen jeweils einen eigenen, nativ verankerten Mechanismus, den die folgenden Absätze entfalten.

Die zweite Stelle betrifft die Wahl, die der Proposer über den Inhalt seines Blocks trifft, und sie wird durch eine erzwungene Inklusionsliste geschlossen, die ihm vorschreibt, welche Transaktionen er aufnehmen muss. Diesen Zwang leisten die Fork-choice Enforced Inclusion Lists (FOCIL, EIP-7805), bei denen ein Komitee aus 16 zufällig bestimmten Validator-Includern zusammen mit dem Block-Proposer in jedem Slot anhand ihrer eigenen Mempool-Sicht eine Liste der aufzunehmenden Transaktionen erstellt, deren Umfang je Liste auf 8 KiB begrenzt bleibt. Die Garantie beruht auf einer 1-von-N-Annahme: Ein einziger ehrlicher Includer unter den 16 genügt, damit eine zu Unrecht ausgelassene Transaktion dennoch auf die Liste gelangt und der Proposer sie aufnehmen muss. Durchgesetzt wird die Liste über die Attester, die einem Block ihre Stimme verweigern,

[306] Enshrined Proposer-Builder Separation (EIP-7732, PLAN, SFI Glamsterdam-Headliner; Aktivierung H2 2026 nach EF Checkpoint #9, April 2026). Sie verankert die Rollentrennung im Protokoll und macht den Relay obsolet, indem der Builder signierte Gebote on-chain einreicht. Im IST-Zustand laufen rund 90 Prozent der Blöcke über vertrauenswürdige Relays; die OFAC-Compliance-Rate erreichte im November 2022 einen Spitzenwert von 79 Prozent und liegt zuletzt bei rund 15 Prozent. Die ausführliche Behandlung der Kapazitäts- und Konvergenzfunktion von ePBS steht in 5.2-A; hier zählt allein die Neutralitätsfunktion.

der gültige Listen-Transaktionen ohne den Grund fehlenden Platzes ausschließt, sodass die Missachtung der Liste den Block um seine Bestätigung bringt. Die maximale Verzögerung, mit der eine zunächst übergangene Transaktion dennoch in die Kette gelangt, sinkt von empirisch rund 29 auf 12 bis 24 Sekunden. Die Stärke der 1-von-N-Konstruktion zeigt sich am regulatorischen Druck, denn selbst wenn er die Mehrheit der Builder zur Konformität mit einer Sperrliste zwänge, erzwingt ein einziger nicht-konformer Includer die Aufnahme der betroffenen Transaktion. Unter den drei Mechanismen ist die erzwungene Inklusion der reifste, für die kommende Hegotá-Fork als deren einziger gesetzter Consensus-Headliner terminiert.[307] Eine formale Absicherung dieser erzwungenen Aufnahme gegen einen nachträglichen Reorg steht noch aus, sodass ihr Schutz vorerst auf den allgemeinen Finalitätsgarantien des Protokolls beruht und nicht auf einer eigens für sie gesetzten Regel.[308] Wie weit ein bereits bestätigter Block überhaupt noch durch einen solchen Reorg verdrängt werden kann, hängt an der Single-Slot-Finalität, der dieser Abschnitt sich später zuwendet.

Die dritte Stelle ist die Sichtbarkeit des Transaktionsinhalts selbst, denn was der Builder vor der Aufnahme lesen kann, kann er auch gezielt übergehen, und genau diese Information bleibt offen, nachdem die beiden ersten Mechanismen gegriffen haben. Die Sichtbarkeit hebt ein Verfahren auf, das den Inhalt jeder Transaktion bis zu ihrer Aufnahme in den Block verschlüsselt hält. Der Builder entscheidet damit über die Aufnahme, ohne den Inhalt zu kennen, und nicht zensieren kann, was er nicht sieht. Geführt wird es als Universal Enshrined Encrypted Mempool (EIP-8105). Erst nachdem die Reihenfolge der Transaktionen feststeht, wird ihr Inhalt entschlüsselt, sodass weder der Builder eine Auswahl nach Inhalt treffen noch ein Beobachter eine Order vorwegnehmen kann. Die Verschlüsselung schließt so eine zweite Lücke, weil mit dem verborgenen Inhalt auch das Front-Running und die Sandwich-Angriffe entfallen, die das Vorauslesen des öffentlichen Mempools heute erst ermöglicht. Der Entwurf aus dem Shutter-Umfeld und der unter dem Namen LUCID entwickelte Ansatz der EF-

[307] Fork-choice Enforced Inclusion Lists (EIP-7805, PLAN, SFI Hegotá-Headliner; finale ACD-Entscheidung am 23. Februar 2026, der einzige gesetzte Consensus-Headliner des Forks, Erwartung zweite Jahreshälfte 2026, bei Verzögerung von Glamsterdam ein Rutsch in Anfang 2027 möglich). Ein Komitee aus 16 zufällig gewählten Validator-Includern und dem Block-Proposer (17 Akteure) erstellt pro Slot Inklusions-Listen von je höchstens 8 KiB; die 1-von-N-Annahme verlangt nur einen ehrlichen Includer; Attester verweigern Blöcken, die gültige Listen-Transaktionen ohne Platzgrund auslassen, ihre Stimme; der maximale Inclusion Delay sinkt von empirisch rund 29 auf 12 bis 24 Sekunden. Autor: Thomas Thiery (EF Robust Incentives Group).

[308] Available Attestation (EIP-7942, RES, DFI Glamsterdam, per EIP-7773 in die Declined-for-Inclusion-Liste verschoben; Wieder-Aufnahme in Hegotá oder eine spätere Fork denkbar). Das Verfahren fügt den Validator-Attestations ein Availability-Voting hinzu, sodass die Kette nur Forks folgt, auf denen mindestens ein Drittel des Stakes die Datenverfügbarkeit attestiert, und macht tiefe Reorgs sowie Long-Range-Angriffe ohne erhebliche Validator-Kollusion praktisch unmöglich. Kritisch für I.4 (Schutz vor Finality-Rollbacks) und II.1.

Forschung konvergieren technisch auf dieselbe Threshold Encryption. Unter den drei Mechanismen ist der verschlüsselte Mempool der am wenigsten gereifte, für die Hegotá-Fork vorgeschlagen, doch ohne festen Platz in ihr, nachdem er sich als Headliner-Vorschlag gegen die erzwungene Inklusion nicht durchsetzen konnte.[309]

Die Garantie der erzwungenen Inklusion beruht auf eben jener Dezentralität, die der spätere Abschnitt 5.5-C als nicht gesichert markiert, denn die 1-von-N-Annahme und die durchsetzenden Attester tragen nur, solange das Validator-Set hinreichend vielfältig bleibt. Bei einem Anteil des größten Stakers von rund 23 Prozent hält die Annahme mit Abstand, und wie tragfähig die Voraussetzung auf Dauer ist, prüft der genannte Abschnitt.[310] Wie weit die erzwungene Inklusion über frühere Anläufe hinausreicht, zeigt der Kontrast zu den Original Inclusion Lists (EIP-7547), dem ersten und inzwischen verworfenen Versuch einer erzwungenen Inklusion, dessen starres Modell gerade jene Flexibilität vermissen ließ, die das spätere 1-von-N-Komitee gewährt.[311]

Was der Zielzustand der geprüften Korrektheit zur Seite stellt, ist mit den drei Mechanismen eine erzwungene Vollständigkeit, die das Protokoll dem Produzenten abverlangt, wo sie heute von seinem Wohlverhalten abhängt. Sie beantwortet die erste der drei Gefahren, die von der konzentrierten Produktion ausgehen, während das Abschöpfen des Werts und das nachträgliche Verdrängen bereits bestätigter Blöcke zwei späteren Abschnitten vorbehalten bleiben.

5.5-B Wertabschöpfung und die Entkopplung der Validatoren-Ökonomie

Derselbe konzentrierte Produzent, dessen Zensurmacht die drei Mechanismen des vorigen Abschnitts eingedämmt haben, erzielt aus den Blöcken, die er nun aufnehmen muss, weiterhin einen Gewinn, den keiner dieser Mechanismen erfasst. Die erzwungene Inklusion schreibt vor, welche Transaktionen in den Block gelangen, und sie lässt offen, in welcher Reihenfolge der Produzent sie anordnet,

[309] Universal Enshrined Encrypted Mempool (EIP-8105 bzw. LUCID, RES). Der Transaktionsinhalt bleibt bis zur Aufnahme verschlüsselt und wird erst nach festgelegter Reihenfolge entschlüsselt, womit zugleich Front-Running und Sandwich-Angriffe entfallen. Der für Hegotá vorgeschlagene Mechanismus erhielt keinen festen Fork-Slot und setzte sich als Headliner-Vorschlag nicht gegen FOCIL durch; der Shutter-Entwurf (EIP-8105) und der LUCID-Ansatz der EF-Forschung sind technisch konvergiert (Threshold Encryption, unter anderem BLS-Threshold).

[310] Die 1-von-N-Annahme und die durchsetzenden Attester ruhen auf der Vielfalt des Validator-Sets. Der größte LST-Provider, Lido, hält im IST-Zustand rund 23 Prozent des gestakten ETH; der M1-Schwellenwert für die höchste Neutralitätsstufe liegt bei unter 33 Prozent für den größten einzelnen Provider, und diese Toleranz ist die engste aller II.1-Indikatoren. Die vollständige Behandlung der Staker-Konzentration erfolgt in 5.5-C.

[311] Original Inclusion Lists (EIP-7547, DEP) waren der erste Ansatz erzwungener Transaktionsinklusion und galten als zu restriktiv und unflexibel; sie wurden durch FOCIL mit seinem 1-von-N-Modell abgelöst.

obwohl der größte Teil seines Gewinns gerade aus der Anordnung stammt. Der vorliegende Abschnitt beantwortet die Frage, die an der offenen Stelle ansetzt: ob der Produzent den so erzielten Gewinn verwenden kann, um die Ökonomie der Validatoren an seine Konzentration zu koppeln.

Der Gewinn, um den es geht, entsteht allein aus der Wahl und der Anordnung der Transaktionen, und das Ökosystem führt ihn als MEV (vgl. Kapitel 4).[312] Solange der Gewinn dem Produzenten allein zufällt und mit dem Umfang der Produktion wächst, verbindet er die Konzentration des Bauens mit einem ökonomischen Anreiz, der auf die Validatoren wirkt. Der vorige Abschnitt hat den Gewinn an einer Stelle bereits berührt, weil der Encrypted Mempool dem Builder die Sicht auf den Transaktionsinhalt nahm und mit der inhaltlichen Auswahl zugleich das Front-Running entfiel. Der vorliegende Abschnitt fragt nach seiner Verteilung: wohin er nach dem Bau gelangt und ob seine Verteilung die Ökonomie der Validatoren an die Konzentration der Produktion bindet.

Die erste Antwort des Zielzustands lautet, dass das Bauen der Blöcke nicht fair wird, weil die Anreize, die wenige professionelle Builder an die Spitze der Produktion bringen, fortbestehen und das Protokoll keine von ihnen auflöst. Ein einzelner Builder stellt im Ausgangszustand rund die Hälfte aller Blöcke, und der Markt der Produktion zählt nach den üblichen Konzentrationsmaßen zu den am stärksten gebündelten überhaupt.[313] Drei strukturelle Ursachen halten diese Konzentration stabil, und keine liegt im Zugriff einer einzelnen Protokollregel, weil sie dem professionellen, vertikal integrierten und über mehrere Domänen reichenden Charakter des Marktes folgt.

---

[312] Maximal Extractable Value (MEV). Der Wert, den die Wahl und Anordnung der Transaktionen einem Block-Produzenten über die regulären Gebühren hinaus zuträgt. Front-Running und Sandwich-Angriffe, die das Vorauslesen des öffentlichen Mempools ermöglicht, wurden in 5.5-A am verschlüsselten Mempool behandelt; der vorliegende Abschnitt behandelt die Verteilung dieses Werts.

[313] Builder-Konzentration im IST-Ausgangszustand, Bezugspunkt der SOLL-Bewertung. Ein einzelner Betreiber, die kommerzielle Entität Titan mit eigener proprietärer Infrastruktur, baute im Februar 2026 rund die Hälfte aller Blöcke und im März 2026 etwa 47,6 Prozent. Der Anteil misst die Bauidentität eines Marktteilnehmers, nicht eine von vielen Validatoren genutzte Client-Software, sodass die Konzentration auf einen einzelnen Betreiber entfällt und von der separaten Frage der Client-Diversität zu trennen ist. Der Herfindahl-Hirschman-Index wurde an einer Beaverbuild-Titan-Duopol-Konstellation im März 2025 mit rund 3.892 bestimmt, weit über der DOJ-Schwelle von 1.800; die Einzelwerte schwanken, die Einordnung als hochkonzentriert bleibt stabil. IST-Befund: T. Wahrstätter (EF), ACDT #69 (Feb. 2026); CoinMetrics, State of the Network #356 (März 2026). Die SOLL-Bewertung hält fest, dass die Konzentration im Zielzustand fortbesteht.

Woher die Builder-Konzentration kommt

Die erste Ursache ist die Latenz, mit der ein Builder sein Gebot in der Auktion einreicht. Der Builder-Wettbewerb läuft als Auktion im festen Zeitfenster eines Slots, in dem Gebote bis zuletzt nachgeschärft werden, und der größte Teil des MEV stammt aus CEX-DEX-Arbitrage, deren Preisabstand sich bis zum letzten Moment bewegt. Wer näher an der Auktions- und Handelsinfrastruktur sitzt, bietet später und mit aktuelleren Preisen und trifft dennoch rechtzeitig ein, während ein entfernter Builder früher und mit veralteter Bewertung bieten muss. Den Vorsprung sichert eine am Handelsplatz kolokalisierte Niedriglatenz-Infrastruktur, deren Kosten im sechsstelligen US-Dollar-Bereich je Monat liegen.

Die zweite Ursache ist die Cross-Domain-Arbitrage zwischen der Basisschicht und den Layer-2-Netzen. Dieselben Vermögenswerte handeln über diese Domänen hinweg zu verschiedenen Preisen, und wer auf mehreren zugleich baut oder sequenziert, kann beide Seiten der Differenz atomar abschöpfen, während ein auf eine Domäne beschränkter Builder nur eine Seite sieht. Diese Koordination verlangt Betreiberrechte oder privilegierten Zugang auf mehreren Netzen und begünstigt die ohnehin vertikal integrierten Akteure, die schon die Basisschicht beherrschen. Ihr Ertrag wächst überlinear mit der Zahl der kontrollierten Domänen, weil eine ganze Klasse atomarer Gelegenheiten erst aufgeht, sobald ein Akteur mehrere Domänen gleichzeitig kontrolliert.

Die dritte Ursache ist der exklusive Order Flow, der privat zugeleitete Strom an Transaktionen. Etwa 54 Prozent des Blockwerts stammen aus Transaktionen, die am öffentlichen Mempool vorbei über private RPCs direkt an einen einzelnen Builder gehen und nur ihm zur Verfügung stehen. Ihre Quelle, etwa eine Wallet, ein Trading-Bot oder ein Aggregator, überlässt diesen Flow gegen eine bezahlte Absprache exklusiv einem Builder und schützt ihre Nutzer zugleich vor Front-Running, weil die Transaktion nie öffentlich wird. Der Zugang wirkt selbstverstärkend, weil ein größerer privater Zufluss höhere Blockbewertungen, häufigere Auktionssiege und größere Gewinnmargen erzeugt, die wiederum weiteren Flow anziehen.[314]

Dass die Produktion konzentriert bleibt, ist kein Ziel, das den Zielzustand

[314] Die drei strukturellen Barrieren des IST-Ausgangszustands, die im Zielzustand fortbestehen. Latenzvorteile (Gebote im letzten Moment, geographische Nähe zu den Proposern, Infrastrukturkosten im sechsstelligen US-Dollar-Bereich je Monat), Cross-Domain-Arbitrage (überlineare Erträge bei Stake in mehreren Domänen) und exklusiver Order Flow. Eine empirische Studie über Ethereum-Blöcke von Januar 2023 bis Mai 2024 beziffert den Anteil privat zugeleiteter Transaktionen am Blockwert auf 54,59 Prozent und weist den selbstverstärkenden Effekt nach: Builder mit höherem privaten Zufluss bewerten Blöcke höher, gewinnen häufiger und behalten größere Gewinnanteile. Das Protokoll adressiert den Relay-Trust, nicht dieses Wert-Capture. IST-Befund: Private Order Flows and Builder Bidding Dynamics, WWW '25 (arXiv:2410.12352); zur künstlichen Latenz arXiv:2312.09654.

verfehlt. Das Protokoll behandelt den konzentrierten Blockbau als hinzunehmende Tatsache, weil keine seiner Maßnahmen die drei Ursachen angreift, denn ePBS beseitigt das Vertrauen in den Relay und lässt die Anreize der Konzentration bestehen. Auch der prominenteste Versuch, das Bauen dennoch zu dezentralisieren, belegt nur deren Grenze. Das Builder-Netzwerk BuilderNet aus dem Flashbots-Umfeld lässt mehrere Betreiber gemeinsam an einem Block arbeiten, ohne dass einer die Beiträge der anderen einsieht, und hat damit einen Marktanteil von rund 27 Prozent erreicht, arbeitet aber außerhalb des Protokolls und beseitigt keine der drei Ursachen.[315] Zum Problem wird die Konzentration erst dort, wo der abgeschöpfte Wert aus dem Bau in die Ökonomie der Validatoren gelangt und die breite Menge der Staker an den Vorsprung des konzentrierten Builders bindet. Genau diesen Übergang unterbricht der Zielzustand an zwei Stellen, an denen er den Gewinn des Builders von der Belohnung der Validatoren trennt und seinen Grundbetrag an die Allgemeinheit zurückgibt.

Entkopplung und Sozialisierung

Die erste Stelle ist die Entkopplung, die den abgeschöpften Wert von der Belohnung des Validators trennt. Im Ausgangszustand entscheidet der zufällig bestimmte Validator, der einen Slot vorschlägt, über den Inhalt seines Blocks und erhält zugleich den daraus abgeschöpften Wert, sodass der Wert über ihn in die Staker-Ökonomie gelangt. Die Entkopplung trennt nun das Recht, den Inhalt eines Blocks zu bestimmen und vorzuschlagen, von den übrigen Pflichten des Validators und versteigert es an einen eigenen Markt von Käufern. Das Ökosystem führt die Trennung als Attester-Proposer Separation (APS). Sie nimmt zwei Formen an, die als Execution Ticket und als Execution Auction diskutiert werden und sich darin gleichen, dass sie das Recht dem Höchstbietenden zuschlagen und es nicht mehr dem zufällig bestimmten Validator zuteilen. Ihr Ziel ist, die breit verteilte Menge der Validatoren gegen die zentralisierende Wirkung des abgeschöpften Werts zu schützen, ohne in den Bau selbst einzugreifen. Weil der abgeschöpfte Wert danach beim Käufer des Rechts verbleibt und nicht mehr über den Validator läuft, erhält der Validator nach dem Bau allein die reguläre Konsens-Belohnung, und der Vorsprung des konzentrierten Builders erreicht die Staker-Ökonomie in beiden Formen nicht mehr. APS baut auf der protokollaren Trennung von Proposer und Builder auf, die ePBS (EIP-7732) im Konsens ver-

[315] BuilderNet (DEPL, außerhalb des Protokolls). Ein Block-Building-Netzwerk aus dem Flashbots-Umfeld, in dem mehrere Builder mit TEE-Isolation gemeinsam an einem Block arbeiten, ohne die Beiträge der anderen einzusehen; Marktanteil rund 27 Prozent. Es belegt die operative Möglichkeit dezentralen Bauens, beseitigt die strukturellen Barrieren nicht und liegt außerhalb des Protokolls.

ankert.[316]

Die zweite Stelle ist die Sozialisierung, die den Grundbetrag des abgeschöpften Werts an die Allgemeinheit zurückgibt. Das Protokoll verbrennt den Erlös der Versteigerung und gibt ihn damit an keinen einzelnen Akteur weiter. Es überträgt so die seit 2021 wirksame Gebührenverbrennung aus EIP-1559 auf den abgeschöpften Wert.[317] Weil der verbrannte Betrag das Angebot an ETH verknappt, kommt er rechnerisch jedem Halter zugute, während er dem Proposer und dem Builder entzogen wird. APS und MEV Burn greifen ineinander und konkurrieren nicht: APS versteigert das Recht, den Block zu bestimmen, und MEV Burn verbrennt den Erlös der Versteigerung.

Die Entkopplung beendet zugleich einen Anreiz, der die Konzentration bisher zusätzlich begünstigt. Im Ausgangszustand steigt die Belohnung des Proposers mit dem abgeschöpften Wert, und dieser Wert wächst mit jeder weiteren Sekunde, in der gehandelt wird. Ein Proposer hat deshalb einen Grund, die Veröffentlichung seines Blocks hinauszuzögern, um einen höheren Wert abzuschöpfen. Solche Verzögerungsstrategien, im Ökosystem als Timing Games geführt, verschieben die Zeitstruktur des Konsenses zugunsten der Akteure mit dem größten Latenzvorteil.[318] Sobald der abgeschöpfte Wert nicht mehr über den Proposer läuft, entfällt der Grund für die Verzögerung, und die ökonomische Ursache ist beseitigt. Die strukturelle Ursache, das Zeitfenster des Slots selbst, beseitigt erst die Single-Slot-Finalität, der sich ein späterer Abschnitt von 5.5 zuwendet.

Was der Zielzustand erreicht, liegt in der Verteilung des Werts und in der Ökonomie der Staker, während die Produktion selbst konzentriert bleibt. Der Builder schöpft den Wert weiterhin ab, doch er kann mit ihm weder die Allgemeinheit schädigen, deren Anteil verbrannt wird, noch die Validatoren von seiner

[316] Attester-Proposer Separation (APS), in den Formen Execution Ticket und Execution Auction (RES, Teil von „The Scourge“, getragen von der EF Robust Incentives Group; ePBS-abhängig, erwartet ab 2027). APS trennt das Recht, den Inhalt eines Blocks zu bestimmen und vorzuschlagen, von den übrigen Validator-Pflichten und versteigert es, sodass die Validator-Belohnung vom abgeschöpften Wert unabhängig und prädiktabel wird. Sie setzt die protokollare Proposer-Builder-Trennung von ePBS (EIP-7732, PLAN, SFI Glamsterdam) voraus, deren Kapazitäts- und Konvergenzfunktion 5.2-A behandelt; hier zählt allein die Entkopplung der Abschöpfung.

[317] MEV Burn (RES, ePBS-Add-on; aus dem Umfeld von Justin Drake / EF). Der Auktionserlös wird verbrannt und keinem einzelnen Akteur ausgeschüttet, analog zur Gebührenverbrennung aus EIP-1559 (DEPL seit 2021). Die Maßnahme glättet MEV-Spitzen, macht die Proposer-Belohnung prädiktabel und verknappt das ETH-Angebot.

[318] Timing Games. Strategien, bei denen ein Proposer die Block-Publikation verzögert, um mehr Wert abzuschöpfen, da der abschöpfbare Wert mit der Zeit steigt; sie gelten als ökonomische Neutralitätsverletzung zugunsten von Akteuren mit Latenzvorteilen. Die ökonomische Ursache beseitigt die Entkopplung der Abschöpfung; die strukturelle Ursache über die Single-Slot-Finalität und die ePBS-Lieferpflichten (Builder Staking, PTC-Attestation) behandelt 5.5-D. Kurzfristig bleibt die Eindämmung auf eine Koordination der Beteiligten außerhalb des Protokolls verwiesen, und die Forschung räumt ein, dass das gegenwärtige Design sie nicht vollständig ausschließt.

Konzentration abhängig machen, deren Belohnung von seinem Vorsprung getrennt ist. Die Konzentration der Produktion bleibt eine Tatsache des Ausgangszustands, doch ihre Wirkung auf die Neutralität ist an beiden Übergängen unterbrochen.

Beide Mechanismen stehen anders da als die erzwungene Inklusion, die der vorige Abschnitt getragen hat. APS und MEV Burn sind Forschungsvorhaben ohne festen Platz in einem benannten Fork, getragen von der EF Robust Incentives Group und der Forschung um Justin Drake. Sie sind damit die unreifsten der Antworten, die der Abschnitt versammelt. Sie gehören zur Roadmap-Phase gegen die systemischen Zentralisierungsrisiken, die das Ökosystem unter dem Namen „The Scourge" führt. Ihre Wirkung ist damit eine Richtung mit feststehender Mechanik und offenem Termin.

Die Entkopplung verhindert, dass die Produktion ihren Gewinn an die Staker-Ökonomie weiterreicht, und sie kehrt die Konzentration nicht um, die im Ausgangszustand bereits besteht. Der größte einzelne Staking-Anbieter hält rund 23 Prozent des gestakten ETH, und ob diese Schwelle dauerhaft trägt, prüft der folgende Abschnitt.[319] Was MEV Burn über die Fairness hinaus berührt, ist das Security Budget der Kette, weil der verbrannte Wert dem Protokoll zugutekommt und nicht die Belohnung einzelner Akteure erhöht, was in die ökonomische Tragfähigkeit eingreift, deren Synthese derselbe Abschnitt leistet. So beantwortet der Zielzustand die zweite der drei Gefahren, die von der konzentrierten Produktion ausgehen, indem er ihren Gewinn von der Ökonomie der Staker trennt und ihren Grundbetrag der Allgemeinheit zuführt. Das nachträgliche Verdrängen eines bereits bestätigten Blocks der letzten Gefahr und dem abschließenden Abschnitt vorbehalten bleibt.

[319] Staker-Konzentration und Security Budget als Vorausweis auf 5.5-C. Der größte einzelne Staking-Anbieter (Lido) hält im IST-Ausgangszustand rund ein Viertel des gestakten ETH; die Februar-2026-Angabe von Lido lautet 23 Prozent, Dune-Daten nennen etwa 24 Prozent, ausgehend von einem Höchststand über 32 Prozent (2023). Der M1-Schwellenwert für die höchste Neutralitätsstufe liegt bei unter 33 Prozent für den größten einzelnen Anbieter, und diese Toleranz ist die engste aller II.1-Indikatoren. Das Security Budget speist sich aus Staking-Belohnung, MEV und Transaktionsgebühren; MEV Burn leitet die MEV-Erlöse ans Protokoll um und greift damit in die Staking-Ökonomie ein, deren Synthese 5.5-C trägt (Lücken 7.2 und 7.10). IST-Befund: Lido Tokenholder-Update (Feb. 2026); Dune (hildobby).

5.5-C Staking-Ökonomie und die Grenze der Verteilung

Die Garantien der beiden vorigen Abschnitte hängen an einer Annahme, die keines von ihnen geprüft hat: Das Validator-Set bleibt vielfältig genug. Die erzwungene Inklusion braucht dafür einen einzigen ehrlichen Includer im Komitee (Abschnitt 5.5-A), und die Entkopplung der Belohnung schützt eine bestehende Verteilung der Staker, ohne sie herzustellen (Abschnitt 5.5-B). Die vorigen Abschnitte betrachteten die Konzentration der Produktion, die Frage, wer den Block baut. Nun geht es um die Konzentration des Stakes, um die Frage, wer überhaupt validiert und wie viele Anbieter das gestakte Kapital halten.

Daran knüpft der Abschnitt zwei Fragen an, die in der Bewertung auseinanderlaufen. Die erste ist ökonomisch und betrifft die dauerhafte Tragfähigkeit des Staking, an der die bezahlbare Sicherheit des Netzes hängt. Die zweite betrifft die Verteilung und fragt, ob das Protokoll verhindert, dass sich die Kontrolle über den Konsens in wenigen Händen sammelt. Auf die erste Frage antwortet das Protokoll mit einem stabilen Ja, auf die zweite nicht. Der erste Teil zeigt, wie die Ökonomie trägt, der zweite, warum die Verteilung offen bleibt.

Ökonomisch muss das Protokoll vor allem das Security Budget tragen, die Belohnung an die Staker, die den Erwerb eines Angriffsanteils teurer hält als den Gewinn daraus. Seine Höhe setzt sich aus drei Größen zusammen: der Issuance, den Transaktionsgebühren und dem Burn. Die Issuance bezahlt die Sicherheit, die Gebühren ergänzen sie, und der Burn hält über die Verknappung den Wert der ausgezahlten ETH hoch.

Von den drei Größen stellt das Protokoll nur die Issuance selbst ein, und nur bei ihr ist die künftige Höhe offen. Jeder neu erzeugte ETH verteilt den Bestand auf mehr Einheiten und entwertet die bereits gehaltenen, weshalb das Protokoll nur so viel erzeugen soll, wie die Sicherheit verlangt. Nach der heutigen Regel aber steigt die ausgeschüttete Menge, je mehr ETH insgesamt gestakt ist, sodass die Emission ohne Grenze mitwachsen kann. Die unter dem Stichwort Minimum Viable Issuance diskutierte Reform ändert die Regel: Sobald der gestakte Anteil eine Zielmarke übersteigt, sinkt die jährliche Rendite je Validator, und weiterer Stake verliert seinen Anreiz.[320] Die Reform sucht den Anteil, der hoch genug für die Sicherheit und niedrig genug bleibt, um die Emission gering zu hal-

[320] Issuance Reform / Minimum Viable Issuance (RES, ohne Governance-Verankerung; getragen von Anders Elowsson und weiteren). Eine reformierte Emissionskurve senkt die Validator-Rendite bei hohem Stake-Ratio und zielt auf eine Gleichgewichts-Issuance mit Ziel-Stake-Ratio als stationären Zustand, in dem sich das Security Budget zwischen Stake, Gebühren und Burn ausbalanciert. Der Streit um die richtige Zielgröße ist offen; die „Ultrasound Money"-Erzählung um den durch Burn deflationären ETH trug 2025 nicht mehr, nachdem die Verbrennung mit der Verlagerung der Aktivität auf die Layer-2-Netze sank und das Angebot wieder wuchs.

ten. Ihr Status bleibt offen, da die Forschung über die richtige Zielmarke noch streitet. Hinzu kommt, dass die Erzählung vom knappen, deflationären ETH, die das Ökosystem als Ultrasound Money führt, 2024 (folgend 2025) nicht mehr trug, als die sinkende Burnrate das Angebot wieder wachsen ließ.[321]

Die beiden übrigen Größen, die Gebühren und der Burn, stehen fester als die Issuance. Auf der Gebührenseite sichert die Blob Fee Stabilization (EIP-7918) einen Mindestpreis für die Daten, die Layer-2s auf der Layer 1 ablegen.[322] Sie verhindert, dass die Blob-Gebühren gegen Null fallen, und erhält den Gebührenanteil der Validatoren. Auf der Burn-Seite vernichtet das Protokoll schon heute den Grundpreis jeder Transaktion, im Zielzustand zusätzlich das MEV. Das MEV schwankt stark, da seltene Blöcke mit großen Liquidationen oder Arbitragen ein Vielfaches eines gewöhnlichen Blocks einbringen. Der MEV Burn vernichtet es über die Auktion der Blockbestimmung, sodass kein einzelner Block einem Proposer einen Sonderertrag verschafft und die Belohnung der Validatoren gleichmäßig bleibt.[323] Er zählt hier zur Burn-Seite des Budgets. In Abschnitt 5.5-B steht er unter der Fairness.

Die Erträge übersteigen die Betriebskosten nur bei einem effizienten Validieren, und hier wirkt MaxEB (EIP-7251), seit dem Pectra-Upgrade im Frühjahr 2025 ausgeliefert. Das Upgrade hat die maximale Effective Balance eines Validators von 32 auf 2.048 ETH angehoben.[324] Große Betreiber können seither tausende kleiner Nodes zu wenigen großen zusammenfassen, was ihre Kosten senkt und ihre Erträge verstetigt. Für die Ökonomie des Stakings zählt die Konsolidierung der Nodes als stabilisierender Faktor. Welche Folgen die Zusammenfassung für die Verteilung hat, klärt der zweite Teil.

Aus dem Zusammenspiel der drei Größen folgt ein Zustand, der sich selbst stabilisiert. Die Staking-Quote pendelt sich auf einen Wert ein, bei dem die Emis-

[321] Zurückzuführen auf das Dencun-Upgrade (März 2024), welches die Transaktionsgebühren auf Layer 1 drastisch senkte und die ETH-Verbrennungsrate einbrechen ließ. Für detaillierte Statistiken zum Angebotswachstum siehe: https://ultrasound.money.

[322] Blob Fee Stabilization (EIP-7918, DEPL mit Fusaka, 3. Dezember 2025). Ein Mindest-Blob-Base-Fee, an die Execution-Kosten gekoppelt und auf rund ein Sechzehntel der Execution-Base-Fee gesetzt, lässt den Blob-Preis bei Target-Utilization gegen einen ökonomisch rationalen Floor konvergieren und hält ihn über dem absoluten Minimum von einem Wei, was die Gebührenkomponente des Budgets gegen das Fee-Alignment-Problem stützt.

[323] MEV Burn (RES, ePBS-Add-on, aus dem Umfeld von Justin Drake / EF). Der vorliegende Abschnitt behandelt allein die ökonomische Funktion als Komponente des Security Budgets, nachdem 5.5-B die Sozialisierung des MEV hergeleitet hat; der Mechanismus glättet die MEV-Spitzen und macht die Proposer-Belohnung prädiktabel.

[324] MaxEB (EIP-7251, DEPL, Pectra, Mai 2025). Die Anhebung des maximalen effektiven Validator-Guthabens von 32 auf 2.048 ETH erlaubt die Konsolidierung vieler kleiner Nodes zu wenigen großen Clustern, senkt die Betriebskosten und macht Belohnungen vorhersehbarer. Sie wirkt auf die Betriebseffizienz und auf die Verkleinerung des Validator-Sets (Voraussetzung für SSF), nicht auf die Stake-Verteilung.

sion die Sicherheit gerade deckt. Der Burn gleicht die Emission so weit aus, dass das Netz seine Sicherheit nicht mit immer höheren Ausgaben erkaufen muss. Darauf beruht die hohe ökonomische Belastbarkeit des Netzes. Ein Angriff auf ein Drittel des Stakes verlangt den Erwerb von etwa 11,5 Millionen ETH. Der Kaufdruck einer solchen Menge triebe den Preis so weit hinauf, dass der Angriff unwirtschaftlich bliebe.[325] Die Schwelle hält selbst dann, wenn die Reform den gestakten Anteil maßvoll senkt, weil der vom Erwerb getriebene Preis stärker zählt als die zu kaufende Menge. Belastbar ist die Sicherheit damit, doch ihr Dollar-Wert hängt am ETH-Preis und am Nutzungsvolumen und ist nicht durch das Protokoll allein verbürgt.

Die ungelöste Konzentration

Alles bisher Beschriebene stabilisiert die Ökonomie des Stakings und rührt nicht an seine Verteilung. Kein Mechanismus der Roadmap senkt den Anteil, den ein einzelner Anbieter am gestakten Kapital hält. Jeder vorhandene Mechanismus setzt an der Ökonomie oder am Betrieb des Validierens an, und keiner verschiebt die Marktanteile der Anbieter. Die Grenze des Abschnitts zeigt sich, sobald die Mechanismen einzeln daraufhin geprüft werden, woran sie ansetzen.

Einen technologischen Lösungsansatz zur Risikominimierung bietet die *Distributed Validator Technology* (DVT). Diese dezentralisiert den Betrieb eines einzelnen Validators, indem sie dessen Aufgaben auf mehrere physische Maschinen und unterschiedliche Betreiber aufteilt. Dadurch wird der *Single Point of Failure* eliminiert: Weder der Ausfall einzelner Server noch der Verlust kryptographischer Schlüssel gefährden die Validierung oder führen zum Slashing. Implementierungen der Technologie sind über Protokolle wie Obol und SSV Network bereits im Einsatz, unter anderem innerhalb des Marktführers Lido. DVT betrifft die marktstrukturelle Zentralisierung allerdings nicht. Da die Technologie lediglich die technische Infrastruktur hinter den Validierungsschlüsseln aufteilt, bleibt der prozentuale Marktanteil der jeweiligen Staking-Anbieter am Gesamtkapital davon unberührt.

Für die Netzwerkverteilung entfaltet MaxEB eine dem ökonomischen Nutzen entgegengesetzte Dynamik. Während die Anhebung des maximalen Vali-

[325] 34-Prozent-Attacke und Security Budget im SOLL-Zustand. Das Security Budget aus Staking-Rewards, MEV und Gebühren muss ein gestaktes Kapital in der Größenordnung von 100 Milliarden Dollar incentivieren; eine Attacke auf ein Drittel des Stakes verlangt den Erwerb von etwa 11,5 Millionen ETH und bleibt bei realistischen Liquiditäts- und Preisverhältnissen unwirtschaftlich. Der statische Indikatorwert unterschreitet am Stichtag den M1-Schwellenwert von 30 Milliarden Dollar, die tatsächlichen Angriffskosten liegen wegen Marktilliquidität und Slippage beim Erwerb darüber. Der Indikator ist erfüllt mit Einschränkung, preissensitiv und nicht durch Protokolländerungen allein gesichert.

dierungsguthabens die Betriebseffizienz optimiert, fördert sie gleichzeitig die Konsolidierung von Nodes durch Großbetreiber, was strukturell zentralisierend wirkt. Eine Verschiebung der Marktanteile ist auch durch die modifizierte Emissionsrate nicht zu erwarten, da diese den Anreiz für dominante Akteure nur unwesentlich schmälert. Zudem bleibt die Mindestgrenze von 32 ETH unangetastet, da MaxEB allein die Obergrenze des effektiven Guthabens reformiert. Diese ökonomische Eintrittsbarriere blockiert nach wie vor das Wachstum des Solo-Stakings, das weiterhin einen Marktanteil von unter einem Prozent des aggregierten Stakes aufweist.

Eine unmittelbare Begrenzung von Marktanteilen ließe sich durch eine protokolleigene Obergrenze (*Staking Cap*) realisieren, die den maximalen Anteil eines einzelnen Anbieters protokollseitig festschreibt. Obwohl ein solcher Cap innerhalb der Community diskutiert wird, stellt er im aktuellen Zielzustand weder eine geplante noch eine beschlossene Maßnahme dar und steht folglich nicht in der offiziellen Roadmap.[326] Ein solcher Cap würde direkt in den marktwirtschaftlichen Wettbewerb eingreifen, was einer Regelung entspricht, mit der das Ethereum-Protokoll den Markt aus Gründen der Neutralität bislang bewusst sich selbst überlässt. Hierin liegt das eigentliche Defizit der Netzwerkverteilung, da das Problem der Zentralisierung ein ordnungspolitisches ist. Da die einzige strukturell wirksame Gegenmaßnahme in Form eines protokolleigenen Höchstanteils nicht in den Governance-Regeln des Protokolls verankert ist, fehlt Ethereum derzeit das protokolleigene Werkzeug, um eine monopolartige Konzentration von Staking-Macht zu verhindern.

Zudem befindet sich der Ansatz des *Rainbow Staking* noch in der Konzeptionsphase. Das Modell soll das Solo-Staking dadurch reaktivieren, dass es das Validierungssystem in zwei Klassen unterteilt: Kapitalstarke Akteure übernehmen die komplexe Netzwerksicherung, während private Kleinteilnehmer ohne teure Hardware-Anforderungen als Kontrollinstanz eingebunden werden, was die finanzielle und technische Einstiegshürde deutlich senkt.

An dieser fortschreitenden Marktkonzentration stößt das protokollseitige Leitprinzip der Protokollneutralität an seine konzeptionelle Grenze. Zwar kann das Protokoll bestimmte Verhaltensweisen technisch erzwingen, wie die garantierte Aufnahme einer Transaktion (Abschnitt 5.5-A) oder die ökonomische Ent-

[326] Protokoll-Level-Staking-Cap und Rainbow Staking. Ein Cap, der einen Höchstanteil je Anbieter festschriebe, wird in der Community diskutiert, trägt im SOLL-Zustand weder den Status PLAN noch DEPL und bleibt damit eine Diskussion ohne implementierten Roadmap-Status; hier liegt die governance-seitige Lücke der Verteilung. Rainbow Staking (RES) würde die Validator-Rollen in leichte (Attestation) und schwere (Block Building) Aufgaben auffächern und die Einstiegsbarriere senken, ist aber ein Forschungs- und kein implementierter Mechanismus.

kopplung von Belohnungen (Abschnitt 5.5-B), die Akkumulation von Marktmacht durch eine schwindende Anzahl von Staking-Anbietern kann es jedoch nicht unterbinden. Die technischen Maßnahmen schützen das Netzwerk folglich vor dem akuten Missbrauch bestehender Machtstrukturen, sie bewirken jedoch keine strukturelle Umverteilung der Macht. Neben der internen Kapitalallokation existiert zudem eine externe, geographische Grenze der Neutralität, da sich rund 39 Prozent aller Nodes in den USA befinden.[327] Die Ursachen für die geographische Clusterbildung liegen außerhalb des Protokolleinflusses.

Ausgerechnet jene Dezentralisierung, die das Protokoll selbst nicht aktiv herbeiführen kann, bildet jedoch das Fundament für die Sicherheitsgarantien der vorangegangenen Abschnitte. So setzt die mathematische Annahme der erzwungenen Transaktionsinklusion ein hinreichend diverses Teilnehmernetzwerk voraus, während der Mechanismus der Entkopplung eine bestehende Verteilung zwar schützt, diese jedoch nicht künstlich reproduzieren kann. Die konzeptionelle Neutralität des gesamten Protokolls basiert somit auf einer strukturellen Vielfalt der Akteure, die im Zielzustand zwar zwingend vorausgesetzt, vom System selbst jedoch nicht garantiert wird.

5.5-D Der Preis der Finalität

Zwischen der Stimmabgabe der Attester und der endgültigen Bestätigung durch das Protokoll liegen aktuell rund 13 Minuten, in denen ein Block zwar als bestätigt, aber noch nicht als unumkehrbar gilt. In diesem Zeitraum gibt es zwei Probleme, die der vorige Abschnitt ökonomisch gelöst und zur technischen Behebung an den vorliegenden Abschnitt verwiesen hat. Das erste Problem ist das nachträgliche Verdrängen eines bereits bestätigten Blocks durch eine Kettenreorganisation (Reorg). Dies ist die dritte und letzte Hauptgefahr, die von einer konzentrierten Produktion ausgeht. Das zweite Problem ist die künstliche Verzögerung der Blockveröffentlichung (Timing Games). Den wirtschaftlichen Anreiz dafür hat die Trennung von Proposer und Builder dem Proposer zwar genommen, die zeitliche Möglichkeit dazu besteht jedoch weiterhin. Beide Probleme nutzen dieselbe tolerante Zeitstruktur des Netzwerks aus, welche Verzögerungen und nachträgliche Änderungen überhaupt erst technisch zulässt. Der fol-

[327] Geographische Node-Verteilung als zweite, exogene Grenze der Neutralität. Im IST-Zustand liegt der US-Anteil der Nodes nach aktueller Erhebung bei rund 39 Prozent (Etherscan, Anfang 2026, von 14.339 erfassten Nodes; ältere Erhebungen nannten bis zu 46 Prozent), sodass der US-Anteil je nach Erhebung in einer Spanne von 39 bis 46 Prozent liegt und die deutlichste geographische Konzentration der Node-Verteilung bildet. Stateless Clients senken die Hardware-Barriere strukturell, adressieren aber nicht die nicht-technischen Ursachen (Regulierung, Infrastrukturkosten, technisches Wissen). Eine direkte Roadmap-Maßnahme existiert nicht; die vollständige Behandlung als Resilienz-Thema erfolgt in 6.2. Quelle: Etherscan (Anfang 2026).

gende Abschnitt führt die Themen über die Single-Slot-Finalität zusammen, da eine sofortige, sekundengetaktete Block-Finalisierung sowohl Kettenreorganisationen als auch künstlichen Publikationsverzögerungen die operative Grundlage entzieht.

Die volle Mechanik der Verzögerung, die der vorige Abschnitt 5.5-B nur benannte, gehört hierher. Der Wert, den ein Proposer aus der Anordnung der Transaktionen abschöpft, wächst mit jeder Sekunde im Slot, da zeitliche Verschiebungen der Marktpreise zusätzliche Arbitrage-Möglichkeiten erzeugen und weitere Liquidationen ermöglichen. Ein Proposer, der seinen Block später veröffentlicht, schöpft mehr MEV ab (diese Verzögerungsstrategien, vgl. Abschnitt 5.5-B). Sie belohnen die Akteure mit dem größten Latenzvorteil, die spät genug bieten und dennoch rechtzeitig eintreffen, und verschieben die zeitliche Dynamik des Konsenses zugunsten weniger Betreiber.[328] Die mit APS eingeführte Entkopplung entzog der Verzögerung ihren direkten Lohn, indem sie den abgeschöpften Wert vom Proposer trennte. Sie ließ jedoch den Ermessensbereich des Slots unangetastet, in dem die Verzögerung stattfindet, sodass sich die Timing Games lediglich auf die Ebene der Builder verlagerten. Solange das Protokoll innerhalb eines Slots eine zeitliche Toleranz zulässt, bleibt die strukturelle Ursache für das Entstehen von Timing Games formal gegeben.

Das Risiko einer Kettenreorganisation (Reorg) nutzt dasselbe Zeitfenster aus, setzt jedoch an einer anderen Stelle an. Ein Block gilt als bestätigt, sobald die Attester für ihn gestimmt haben. Unumkehrbar wird er jedoch erst, wenn das Protokoll ihn nach zwei aufeinanderfolgenden Epochs (Checkpoints) finalisiert. In dem Zeitraum dazwischen kann eine Reorganisation der Kette den Block theoretisch wieder verdrängen und durch einen anderen ersetzen. Ein marktbeherrschender Akteur mit einem ausreichend großen Anteil an Validierungsstimmen könnte so einen bereits bestätigten Block austauschen. Auf die Weise ließe sich eine Transaktion nachträglich wieder aus der Chain entfernen, obwohl sie durch die Inclusion List (aus Abschnitt 5.5-A) gerade erst aufgenommen worden war. Mit dem Austausch des Blocks würde auch die darin enthaltene Transaktion wegfallen. Die vollständige Aufnahme von Transaktionen, die der erste Schutzmechanismus dieses Kapitels erzwingen sollte, bliebe gegen ein solches nachträg-

[328] Timing Games und ihre strukturelle Ursache. Strategien, bei denen ein Proposer die Block-Publikation verzögert, weil das abschöpfbare MEV monoton mit der Zeit im Slot steigt; sie gelten als ökonomische Neutralitätsverletzung, die die Zeitstruktur des Konsenses zugunsten latenzstarker Akteure destabilisiert. Die ökonomische Ursache beseitigt die Entkopplung (5.5-B); die ePBS-Lieferpflichten über Builder Staking und PTC-Attestation machen das strategische Zurückhalten unrentabel und adressieren zugleich das Free Option Problem (bis zu sechs Prozent leere Slots an volatilen Tagen). Die strukturelle Ursache, das lose Zeitfenster des Slots, beseitigt erst die Single-Slot-Finalität.

liches Verdrängen ungesichert. Die zugrundeliegende Trennung von Proposer und Builder (ePBS) bindet den Builder zwar bereits an ein festes Commitment. Mechanismen wie das Builder Staking und spezielle Validatoren-Bestätigungen des Payload Timeliness Committee (PTC) nehmen ihm zudem die Möglichkeit, einen fertigen Block einfach zurückzuhalten. Dadurch wird die nachträgliche Änderung der Blockchain auf maximal einen einzigen Slot begrenzt. Dieses Risiko bleibt allerdings so lange bestehen, wie die erste Bestätigung eines Blocks und seine unumkehrbare Finalisierung im Protokoll zeitlich voneinander getrennt sind.

Single-Slot-Finalität als Antwort

Die Single-Slot-Finalität ist das Ziel der Roadmap, um die zeitliche Lücke zwischen der ersten Bestätigung und der unumkehrbaren Finalität eines Blocks vollständig zu schließen. Der Begriff verspricht allerdings mehr, als das aktuell favorisierte Design tatsächlich einlöst. Die Forschung um Justin Drake, Buterin und andere setzt die praktisch erreichbare Finalisierung derzeit bei drei Slots an, weshalb das Konzept inhaltlich als Drei-Slot-Finalität verstanden werden muss. Eine Finalisierung im einzelnen Slot müsste die Attestationen des gesamten Validator-Sets innerhalb einer einzigen Spanne verbreiten und zu einem Beweis bündeln, was die verfügbare Zeit für Propagation und Aggregation übersteigt. Drei Slots räumen dem Netz diese Zeit ein und bleiben dennoch kurz genug, um Reorganisationen und Verzögerungen den Spielraum zu nehmen. Bei der heutigen Taktung von zwölf Sekunden je Slot sinkt der Zeitraum zwischen Bestätigung und Finalität von rund 13-15 Minuten auf etwa 36 Sekunden. Die beschleunigte Finalisierung verkürzt jedoch lediglich die Zeitspanne bis zum Erreichen der Sicherheitsgrenze, sie senkt diese Schwelle nicht ab. Sobald die Finalität nach 36 Sekunden erreicht ist, bleibt ein Widerruf der Kette wirtschaftlich genauso teuer und damit so gut wie unmöglich wie im heutigen System. Unabhängig davon sinkt die Zeit bis zur ersten Bestätigung über sogenannte Fork-Choice-Confirmations auf wenige Sekunden. Die Mechanik entfaltet Abschnitt 5.6-C. Die Finalisierung auf der kurzen Zeitskala der Slots beseitigt somit an einer einzigen Stelle sowohl das Risiko nachträglicher Kettenreorganisationen als auch die verbleibende technische Ursache der Timing Games.

Auf der Ebene des gesamten Validator-Sets erfordert die Finalität eine der tiefgreifendsten architektonischen Anpassungen der Blockchain überhaupt. Derzeit attestiert pro Slot nur ein Teilbereich (*Committee*) der Validatoren. Eine Single-Slot-Finalität (SSF) verlangt dagegen, die Attestationen des gesamten Validator-Sets innerhalb weniger Sekunden zu einem verifizierbaren Beweis zu

verdichten. Für diese enorme Last an Signatur-Aggregation ist keine der heutigen Konsens-Schichten ausgelegt. Die Roadmap sieht den Umbau unter dem Konzept des *Lean Consensus* vor und verortet den Endzustand in der Beam Chain, was einer vollständigen Neugestaltung der Konsens-Schicht entspricht, deren Implementierung als Forschungszustand jenseits 2029 ohne Fork-Termin liegt.[329] Die Anhebung der maximalen Effective Balance (MaxEB), die seit dem Pectra-Upgrade die Konsolidierung von Validatoren-Nodes vorantreibt, reduziert die absolute Anzahl der Validatoren und ist damit eine direkte funktionale Voraussetzung für die Aggregation. Die effiziente Komprimierung der Signaturen des gesamten Sets hängt zudem von der Marktreife fortgeschrittener ZK-Proofs ab. Damit fällt der Endpunkt der schnellen Finalität technologisch mit den anspruchsvollsten Bausteinen der Skalierung zusammen. Die Anforderungen an eine Single-Slot-Finalität reichen somit von der zeitlichen Feinstruktur des Slots bis tief in die grundlegende Architektur der Konsens-Schicht hinein.

Die kryptographische Basis der Herausforderung bildet das Signaturverfahren, auf dem die Aggregation heute beruht. Das BLS-Signaturverfahren fasst die Signaturen vieler Validatoren nativ zu einer einzigen zusammen, und genau die Eigenschaft macht die schnelle Aggregation rechentechnisch und kapazitär hochgradig effizient. Das hash-basierte Verfahren der leanXMSS-Linie, das BLS im Konsens ablösen soll, erzeugt jedoch um Größenordnungen größere Signaturen. Zudem bringt es keine native Aggregationsfähigkeit mit, sodass der Wechsel die Aggregation technisch massiv erschwert.[330] Das neue Verfahren wird als Maßnahme der Post-Quanten-Kryptographie gewählt, womit die Konsens-Schicht denselben Übergang zu hash-basierten Verfahren vorwegnimmt, den Abschnitt 5.3-D für die Verifikation hergeleitet hat. Die technologischen Anforderungen der Single-Slot-Finalität überschneiden sich hier mit den Notwendigkeiten der Quantensicherheit, ohne dass eine der beiden Herausforderungen die andere inhärent löst.

---

[329] Lean Consensus und Beam Chain (RES). Die Beam Chain ist die vollständige Neugestaltung der Consensus-Schicht mit Drei-Slot-Finalität und SNARK-Aggregation, Ablösung der heutigen Beacon Chain als Forschungszustand jenseits 2029 ohne Fork-Termin; sie absorbiert die Single-Slot-Finalität und MaxEB und hängt für die SNARK-Aggregation an der zkEVM-Reife, geführt als Endpunkt von Lean Ethereum. Das EF-Post-Quantum-Team besteht seit Januar 2026; die Reform des Inactivity Leak für das migrierte Verfahren ist Teilpunkt der Neugestaltung (vgl. 5.3-D). MaxEB (EIP-7251, DEPL, Pectra) verkleinert das Validator-Set über die Node-Konsolidierung und ist Voraussetzung der schnellen Aggregation; die Stake-Verteilungsfolgen behandelt 5.5-C.

[330] BLS und leanXMSS. BLS (DEPL) aggregiert die Konsens-Signaturen nativ zu einer einzigen, was die schnelle Aggregation billig hält; das hash-basierte Verfahren der leanXMSS-Linie (RES), das BLS im Konsens ablöst, erzeugt um Größenordnungen größere Signaturen und aggregiert nicht nativ. Die Quantenfrage selbst, ihr Rahmen und ihre Migrationslogik, ist in 5.3-D abgehandelt und wird hier allein in ihrer Funktion als gewähltes Sicherheitsniveau berührt. Implementierungsstände als leanSig (Rust) und leanSpec (Python).

Die größeren Signaturen des neuen Verfahrens fängt eine integrierte zkVM auf, die für sie einen kompakten Gültigkeitsbeweis erstellt. Über einen rekursiven SNARK faltet die in der Roadmap als leanVM geführte Instanz sie zu einem einzigen Beweis zusammen. Dadurch verkleinert sich die Datenlast um etwa das 250-fache, sodass die Finalität trotz der größeren Einzelsignaturen im Zeitfenster bleibt.[331] Die gleiche Aggregations-Mechanik, die 5.3-A′ für die quantenresistenten Beweise der Anwendungsebene herangezogen hat, macht so auch die Konsens-Signaturen wieder skalierbar. Das letzte Zeitfenster im Konsens zu schließen bedeutet folglich, ihn bis hinunter zu seinem Signaturverfahren umzubauen, und das neue Verfahren wird gleich quantensicher gewählt.

Damit ist die dritte und letzte Gefahr beantwortet: das nachträgliche Verdrängen eines bereits bestätigten Blocks, nach dem Ausschließen einer Transaktion und das Abschöpfen ihres Werts. Diese drei Antworten schützen die Neutralität der Konsens-Schicht vor ihren mächtigsten Akteuren, ohne die Konzentration der Block-Produktion selbst aufzulösen. Zudem basieren sie alle auf einer Diversität des Validator-Sets, die Abschnitt 5.5-C als nicht gesichert ausgewiesen hat. Welches Gewicht die ungesicherte Diversität gegenüber den erreichten Garantien hat, analysiert die Soll-Bewertung in 5.7, aus der das Kapitel in 5.8 sein Gesamturteil ableitet.

5.6 L2-Architektur und Settlement

5.6-A Die zweite Sicherheitsklasse und ihr Konvergenzpunkt

Der vorige Abschnitt hat die Neutralität der Layer 1 gegen ihre mächtigsten Produzenten protokollseitig adressiert, während eine Schicht höher das Zweiklassenproblem der Layer 2 fortbesteht. Wer eine Transaktion auf der Layer 1 sendet, vertraut allein dem Protokoll, dessen Konsens und Kryptographie jede Regelverletzung verwerfen. Wer dieselbe Transaktion auf einem Rollup sendet, vertraut zusätzlich dem Unternehmen, das das Rollup betreibt. Der Betreiber kontrolliert heute zwei Leistungen selbst: die korrekte Ausführung der Transaktionen (Execution) und die Reihenfolge ihrer Verarbeitung (Sequencing). Von der Layer 1 übernimmt ein Rollup bislang allein die Datenverfügbarkeit, deren Garantie Abschnitt 5.2 entwickelt hat. Der Zielzustand kehrt das Prüfverhältnis der Exe-

[331] leanVM und SNARK-Aggregation (RES). Ein minimaler zkVM faltet die größeren leanXMSS-Signaturen über einen rekursiven SNARK zu einem einzigen Beweis zusammen und komprimiert sie um etwa das 250-fache, sodass die Finalität trotz der größeren Einzelsignaturen schnell bleibt; die Mechanik teilt das Aggregations-Prinzip, das 5.3-A′ für die quantenresistenten Beweise trägt.

cution um: Heute beweist der Betreiber gegenüber der Layer 1 die Korrektheit seines Systems, künftig prüft die Layer 1 sie mit ihrer eigenen State Transition Function. Der vorliegende Abschnitt behandelt die Execution, der folgende das Sequencing. Aus der Konvergenz beider folgt die Grundlage der Settlement-Rolle: Ethereum als die Schicht, auf der andere Netzwerke und Anwendungen ihre Zustandsänderungen endgültig verbuchen.

Hinter der zweiten Sicherheitsklasse stehen benennbare Akteure, denn Betreiber eines großen Rollups ist jeweils ein einzelnes Unternehmen, Offchain Labs für Arbitrum, Coinbase für Base, Matter Labs für zkSync Era. Der Zustand folgt strukturell aus der rollup-zentrischen Skalierung, die die Ausführung auf die Rollups verlagerte und ihre Absicherung den Betreibern überließ. Das konkrete Problem liegt in einer Prüf-Lücke des Protokolls: Ein Rollup veröffentlicht seine Transaktionsdaten und den daraus resultierenden State-Root zwar auf der Layer 1, doch deren Konsens besitzt keine eigene Regel, die beides verbindet. Ob der behauptete State-Root tatsächlich aus der Ausführung der veröffentlichten Transaktionen folgt, prüft allein ein Verifier Contract, ein Smart Contract, den der Betreiber entwickelt, ausliefert und über die eigene Governance verändern kann. Die Layer 1 führt den Vertrag regelkonform aus, für die Richtigkeit seiner Prüf-Logik steht sie nicht ein, und ein Fehler in den Proving Circuits kann einen ungültigen Zustandsübergang als kryptographisch korrekt durchgehen lassen. Der Betreiber baut so eine Funktion nach, die die Layer 1 für ihre eigenen Blöcke längst nativ ausführt: die Verifikation von EVM-Zustandsübergängen.

Aus der Lücke folgen die drei Eigenleistungen, auf denen die Korrektheit eines Rollups heute beruht. Ein eigenständiges Proof-System belegt, dass der Betreiber den State seiner Nutzer korrekt fortschreibt, und ein Security Council, ein Gremium mit privilegierten Eingriffsrechten, kann das System im Notfall anhalten oder verändern. Hinzu kommt eine rollup-eigene Governance, die über Upgrades entscheidet, denen die Nutzer unterworfen sind. Optimism stützt sich auf das Fraud-Proof-System Cannon, Arbitrum auf BOLD, zkSync Era auf das ZK-System Boojum.[332] Jedes der drei Systeme erfordert eine eigene Codebasis und ein eigenes Audit, und jede Zeile eigener Beweis-Logik erhöht die Fehlerwahrscheinlichkeit, gegen die das Security Council bereitstehen muss. Für den Nutzer hängt die Sicherheit seiner Gelder folglich an der Kompetenz und Red-

[332] Eigenständige Proof-Systeme der Rollups im IST-Ausgangszustand (je Rollup ausgeliefert). Optimism betreibt das interaktive Fraud-Proof-System Cannon, Arbitrum das Dispute-Protokoll BOLD, zkSync Era das Validity-Proof-System Boojum; hinzu treten Security Councils, Multisig-Upgrade-Schlüssel und rollup-eigene Governance als institutionelle Sicherung. Diese proprietäre Infrastruktur trägt die zweite Sicherheitsklasse und bildet zugleich die Vendor-Lock-in-Quelle, die der SOLL-Zustand über Native Rollups auflöst.

lichkeit identifizierbarer Unternehmen und Gremien, an einer Abhängigkeit, die die Layer 1 protokollseitig beseitigt hat.

Der Gegenbegriff zur Absicherung durch den Betreiber ist Trustlessness, der Zustand, in dem die Gültigkeit jeder Operation allein aus Protokollregeln und kryptographischer Verifikation folgt und kein Vertrauen in identifizierbare Akteure erfordert. Wie viel Macht ein Betreiber gegenüber seinen Nutzern noch hält, lässt sich in drei Entwicklungsstufen einordnen, die die Analyseplattform L2BEAT, eine fortlaufende Dokumentation des Dezentralisierungsgrads der Rollups, als Stage-Schema führt. Auf Stage 0 kann der Betreiber das System jederzeit verändern oder Nutzergelder einfrieren. Auf Stage 1 ist ein funktionierendes Proof-System vorhanden und das Security Council auf den Notfall beschränkt, auf Stage 2 ist jeder privilegierte Eingriff ausgeschlossen und es gilt allein die mathematische Verifikation.

Kein Rollup auf Stage 2

Stand Anfang 2026 hat kein großer Rollup Stage 2 erreicht: Arbitrum, Base, Optimism, Starknet und Scroll stehen auf Stage 1, zkSync Era und Linea auf Stage 0.[333] Mehrere Betreiber haben die Abgabe der letzten Eingriffsrechte aus regulatorischen Gründen öffentlich unbeantwortet gelassen. In der zweiten Richtung besteht eine vergleichbare Konzentration, weil jeder große Betreiber den Sequencer, die Instanz, die die Reihenfolge der Transaktionen festlegt, als einzelne, selbst kontrollierte Komponente einsetzt. Der führende Versuch eines geteilten Sequencers, Astria, wurde 2025 eingestellt, und die Erwartung, die Betreiber würden ihre Stellung schrittweise aus eigener Kraft abgeben, hat sich in beiden Richtungen nicht erfüllt. Buterin zog die Konsequenz im Februar 2026 öffentlich: Der Fortschritt zu Stage 2 verlief weit langsamer und schwieriger als ursprünglich erwartet.[334] Die strategische Neubestimmung, die daraus folgt, trägt

[333] L2BEAT-Stage-System und L2-Dezentralisierungsstand im IST-Ausgangszustand (Erhebung Anfang 2026). Stage 0 erlaubt dem Betreiber jederzeitige Eingriffe bis zum Einfrieren von Nutzergeldern, Stage 1 verlangt ein funktionierendes Proof-System und beschränkt das Security Council auf den Notfall, Stage 2 untersagt jeden privilegierten Eingriff und lässt allein die mathematische Verifikation zu. Kein großer Rollup hat Stage 2 erreicht; Arbitrum, Base, Optimism, Starknet und Scroll stehen auf Stage 1, zkSync Era und Linea auf Stage 0, und mehrere Betreiber haben Stage 2 unter anderem aus regulatorischen Gründen öffentlich offengelassen. Alle großen Rollups fahren einen Single-Operator-Sequencer (Offchain Labs, Coinbase, Optimism Labs, Matter Labs, StarkWare), während der führende Shared-Sequencer-Versuch Astria 2025 eingestellt wurde; Vitalik Buterin nennt den Fortschritt zu Stage 2 weit langsamer und schwieriger als ursprünglich erwartet, ein Befund unter den empirischen Auslösern des strategischen Pivots.

[334] Empirischer Auslöser des strategischen Pivots (Februar 2026). Vitalik Buterin benennt in X-Beiträgen vom 3. und 5. Februar 2026 den weit langsamer und schwieriger als erwartet verlaufenen Fortschritt der Rollups zu Stage 2 als einen der beiden Befunde hinter der Neuausrichtung der L2-Rolle. Die strategische Deutung, das Spektrum von Vertrauensmodellen mit Stage 1 als Mindestschwelle für Rollups mit Ethereum-native Assets und die Rolle der protokollseitigen Verifikation, behandelt Abschnitt 5.1. Quellen: Vitalik Buterin, X (3. und

Abschnitt 5.1.

Die Stage-Einordnung beschreibt den Bestand, die Trajektorie des Zielbilds führt beide Rollup-Klassen dagegen auf denselben Endzustand zu. Die Trennung in Optimistic Rollups mit nachgelagerter Challengeperiode und zkRollups mit vorab beigelegtem Validity Proof löst sich in dem Maß auf, in dem Validity Proofs günstiger und in ihrer Reichweite allgemeiner werden. Am Ende erreichen die zkRollups den Beweis der vollständigen EVM-Ausführung, und die Optimistic Rollups geben die siebentägige Challengeperiode auf, sobald ein günstiger Validity Proof sie ersetzt. Am Ende beider Bewegungen steht dieselbe kryptographische Settlement-Sicherheit, bei der kein Nutzer dem Betreiber die Korrektheit glauben muss. Vollständig erreichbar ist sie für keine der beiden Klassen, solange der Betreiber das Proof-System selbst unterhält, und hier setzt der Zielzustand an: Die Verifikation der Zustandsübergänge wird in das Protokoll der Layer 1 verlagert.

Die Verifikation verlagert sich ins Protokoll

Native Rollups (EIP-8079, RES) verlagern die Verifikation über einen einzigen protokollseitigen Aufruf auf die Layer 1.[335] Den Kern bildet die EXECUTE-Precompile, die die in Abschnitt 5.3-A′ eingeführte Precompile-Schicht um einen Eintrittspunkt in Ethereums eigene State Transition Function erweitert. Der Betreiber reicht einen pre_state_root, einen post_state_root und einen Witness Trace ein, und die Precompile prüft, ob die Layer 1 aus dem Anfangszustand denselben Endzustand errechnet, den der Betreiber angibt. Der Witness Trace, eine kompakte Sammlung genau jener State-Werte, die der Rollup-Block liest und schreibt, ermöglicht die Verifikation, ohne dass die Layer 1 den vollständigen Rollup-State vorhalten muss. Die Behauptung des Betreibers prüfen so dieselben tausenden Validatoren, die jede Layer-1-Transaktion prüfen, und die Korrektheit eines Rollup-Blocks rückt von einer Vertragsregel des Betreibers zu einer Regel

5. Februar 2026); vgl. 5.1.

[335] Native Rollup Precompile (EIP-8079, RES; Draft im Standards Track Core seit dem 13. November 2025, Autoren Luca Donno von L2BEAT und Justin Drake von der Ethereum Foundation, ohne CFI-Bestätigung und ohne Fork-Headliner-Status). Die EXECUTE-Precompile exponiert die State Transition Function der Layer 1 und nimmt drei Inputs entgegen: den pre_state_root, den post_state_root und den Witness Trace mit den gelesenen und geschriebenen State-Werten. Sie ist abhängig von der kompakten Witness-Form der State-Restrukturierung und von der protokollseitigen Integration über die enshrined Proposer-Builder-Separation, während die SNARKification die Reife des Layer-1-zkEVM voraussetzt. Vitalik Buterin signalisierte am 19. Januar 2026 ausdrückliche Unterstützung; ein Proof-of-Concept des Ethrex-Client-Teams mit Ethereum Foundation und L2BEAT vom 11. März 2026 belegt die Verifikation per Re-Execution, ausdrücklich als research milestone und nicht als deployment decision. Konzeptioneller Ursprung ist Justin Drakes ethresear.ch-Beitrag zu Native Rollups vom Januar 2025; die EIP-Motivation benennt die Redundanz ausdrücklich, da EVM-äquivalente Rollups komplexe Proof-Systeme allein deshalb unterhalten, um nachzubilden, was die Layer 1 bereits bereitstellt. Quelle: Justin Drake, ethresear.ch (Januar 2025).

des Protokolls auf. Im Proof-of-Concept erfolgt die Verifikation durch Re-Execution, perspektivisch durch einen SNARK-Beweis, die jene Verifikations-Infrastruktur fortführt, die auf der Layer 1 das Nachrechnen vom Prüfen getrennt hat.

Für den Nutzer eines EVM-äquivalenten Rollups, dessen Ausführung der Spezifikation der Layer 1 exakt entspricht, wäre die Vertrauensgrundlage eine andere. Über die Gültigkeit der Rollup-Blöcke entschiede derselbe Konsens wie über eine Layer-1-Transaktion, sodass ein Angriff auf seine Gelder einen Angriff auf die Layer 1 selbst erfordern würde. Aus der übernommenen Client-Diversität entstünde ohne zusätzliche Infrastruktur ein Multi-Prover-System. Weil verschiedene Execution-Clients verschiedene Beweisverfahren verwenden, kann der Fehler eines einzelnen Verfahrens keinen falschen Zustand finalisieren, da die Abweichung im Konsens sichtbar würde und keine Mehrheit fände. Das Security Council des Betreibers wird überflüssig, und die automatische Kompatibilität mit den Hard Forks der Layer 1 ersetzt die nachgeführte rollup-eigene Governance. Die Bridge, die Verbindungsschicht für Ein- und Auszahlungen zwischen den Ebenen, entfällt als Vertrauensschicht, weil Withdrawals derselbe Konsens sicherte wie eine gewöhnliche Layer-1-Transaktion, ohne Security Council und ohne Challengeperiode. Auf der Seite künftiger Betreiber verschiebt sich die Einstiegshürde vom Millionen-Aufwand für Proof-System, Audit und Security Council auf die Konfiguration eines einzelnen Aufrufs reduzieren. Der permissionless Zugang, den die Layer 1 für einzelne Transaktionen gewährt, schließt das Erstellen ganzer Rollup-Netzwerke ein.

Der Gewinn bleibt an zwei Bedingungen geknüpft, von denen die erste die Kosten der Verifikation betrifft. Als zweite Bedingung muss der Witness Trace on-chain vorliegen und erreicht die Größenordnung des fünf- bis zehnfachen Rollup-Batches, ein Aufwand, der nur deshalb tragbar bleibt, weil die Datenverfügbarkeits-Kapazität der Layer 1 strukturell gewachsen ist.[336] Kompakt bleibt der Witness dabei nur unter der restrukturierten State-Organisation aus Abschnitt 5.4, mit der heutigen Baumstruktur wäre er um zwei Größenordnungen größer und prohibitiv. Hinzu kommt eine Grenze des Durchsatzes, weil in der ersten Phase jeder Node der Layer 1 jede Invocation der Precompile vollständig nachrechnet. Die Zahl der Aufrufe je Block bleibt deshalb be-

[336] DA-Overhead des Witness Trace im SOLL-Designzustand. Eine typische Rollup-Batch liegt zwischen 125 und 750 Kilobyte, während der on-chain bereitzustellende Witness Trace bei der kompakten Witness-Form in der Größenordnung von drei Megabyte je EXECUTE-Invocation liegt, woraus ein Overhead vom Fünf- bis Zehnfachen der Batch folgt; mit der heutigen Merkle-Patricia-Struktur erreichte der Witness rund 300 Megabyte und wäre prohibitiv. Der Aufwand bleibt allein deshalb tragbar, weil die Datenverfügbarkeits-Kapazität der Layer 1 strukturell gewachsen ist.

grenzt, bis die SNARKification die wiederholte Ausführung ersetzt. Die zweite Bedingung betrifft die Reichweite der Auflösung, denn die exponierte State Transition Function unterstützt weder Custom-Opcodes noch eigene Precompiles oder abweichende Transaktionstypen. Jede Abweichung von der EVM-Äquivalenz führt deshalb in ein selbstverwaltetes Settlement zurück, in dem der Nutzer wieder den Institutionen des Betreibers vertraut. Die meisten Rollups sind heute EVM-kompatibel, aber nicht EVM-äquivalent, und die Auflösung steht zunächst nur dem Teil des Ökosystems offen, dessen Ausführung der Spezifikation der Layer 1 entspricht.

Im Zielzustand wäre die Ausführung damit der ersten Sicherheitsklasse zugeführt, soweit ein Rollup EVM-äquivalent bleibt und die kompakte Witness-Form sowie die protokollseitige Verifikation verfügbar sind. Ein Forschungsstrang untersucht die Generalisierung der EXECUTE-Precompile auf eine VM-agnostische Basis, ein Ansatz, der zur Lean-Ethereum-Richtung gehört und hier als Ausblick steht. Für die bestehenden Rollups mit eigenem Proof-System bliebe die Bridge mit ihren Vertrauensannahmen ein Übergangsphänomen, das mit der Verbreitung der Native Rollups an Bedeutung verlöre. Eine Macht behält der Betreiber gleichwohl, die Reihenfolge der Transaktionen, über die der zentral kontrollierte Sequencer weiterhin allein entscheidet. Der folgende Abschnitt behandelt die Verlagerung auch des Sequencing auf die Layer 1. Aus der Konvergenz beider Richtungen ergeben sich der vollständige Trustless-Zustand mit seinem Finalitäts-Stack und die Settlement-Rolle, in der ein heterogenes Ökosystem von Chains seine Zustandsänderungen auf Ethereum endgültig verbucht.

5.6-B Die geteilte Ordnung: Based Sequencing und Based Preconfirmations

Die Auflösung der Ausführungs-Ressource lässt dem Betreiber eine letzte Leistung: die Reihenfolge, in der die Transaktionen seines Rollups verarbeitet werden. Der Sequencer, den jeder große Betreiber als einzelne, selbst kontrollierte Komponente einsetzt, bündelt drei Befugnisse. Er kann eine Transaktion auslassen, womit auf der Rollup-Ebene eine lokale Zensur möglich bleibt, die die Layer 1 für ihre eigenen Blöcke protokollseitig adressiert (Abschnitt 5.5). Er bestimmt die Anordnung der Transaktionen und kann den Wert abschöpfen, der aus ihr folgt. Und sein Ausfall hält das gesamte Rollup an, weil die Liveness an der Infrastruktur eines einzelnen Unternehmens hängt. Für den Nutzer heißt das, dass die Aufnahme seiner Transaktion und der Zeitpunkt seiner Withdrawals von der Verfügbarkeit einer Komponente abhängen, die kein Protokoll bindet. Die drei Befugnisse wiederholen strukturell, was der vorige Abschnitt für die Layer 1 verhandelt hat, doch sie liegen in der Hand eines dritten Akteurs, des Betreibers, der neben die Builder und die Staker der Basisschicht tritt. Der Zielzustand übergibt die Ordnung an die Layer 1: Based Sequencing lässt den Proposer des jeweiligen Slots die Rollup-Transaktionen ordnen, und Based Preconfirmations geben dem Nutzer dafür eine Bestätigung in rund 2 Sekunden.

Der Mechanismus beruht auf einer Eigenschaft, die jedes Rollup ohnehin besitzt: Seine Ausführung folgt deterministisch aus der Reihenfolge seiner Transaktionen. Steht die Sequenz fest, errechnet jeder Rollup-Node aus ihr denselben Zustand, und wer die Reihenfolge festlegt, hat deshalb alles Entscheidende getan, ohne selbst auszuführen. Based Sequencing nutzt die Eigenschaft und verzichtet auf eine eigene ordnende Instanz: Der Proposer des jeweiligen Layer-1-Slots nimmt den nächsten Rollup-Block als Datenpaket in seinen eigenen Block auf, und mit der Aufnahme ist die Reihenfolge der Rollup-Transaktionen verbindlich.[337] Der Nutzer sendet seine Transaktion weiterhin an das Rollup, sie wandert als Teil des Pakets durch den Layer-1-Block, ohne selbst eine Layer-1-Transaktion zu werden, und die Rollup-Nodes führen die fixierte Sequenz anschließend aus. An die Stelle des einen Firmenservers tritt so das gesamte Validator-Set der Lay-

[337] Based Sequencing (DEPL über das Taiko-Mainnet, konzeptuell ohne eigenes EIP). Vorgeschlagen von Justin Drake im März 2023 (ethresear.ch, Based rollups als L1-Sequencing); Based Preconfirmations folgten im November 2023. Der Proposer des jeweiligen L1-Slots nimmt in Kollaboration mit den Buildern den nächsten Rollup-Block in den L1-Block auf; das Rollup erbt das Validator-Set der Layer 1 (rund 1 Million Validatoren) als Sequencing-Infrastruktur, ohne eigene Sequencer-Komponente, ohne zusätzlichen Konsens und ohne Escape Hatch, und die Rollup-Regeln folgen automatisch den Hard Forks der Layer 1. Von den drei Modulen, die die Layer 1 einem Rollup bereitstellt, Inclusion (Datenverfügbarkeit), Ordering (Sequencing) und Execution (Settlement), nutzt ein Based Rollup auch das zweite; das dritte holt die native Verifikation (vgl. 5.6-A).

er 1, die Liveness des Rollups ist mit der Liveness der Layer 1 identisch, und die Teilnahme an der Ordnung ist permissionless. Mit dem Sequencer entfällt die Infrastruktur um ihn herum: zusätzlicher Konsens, Escape Hatch und eigene Ordnungsregel jenseits der Layer 1 entfallen. Ein Based Rollup ist kein Netzwerk mit eigener Ordnung mehr, seine Blöcke entstehen als Teil der Layer-1-Blöcke, und was bleibt, ist eine Ausführungsumgebung über der gemeinsamen Ordnung.

Weil alle Based Rollups dieselbe Ordnung nutzen, ordnet derselbe Proposer ihre Blöcke innerhalb desselben Slots, eine Grundlage, deren Tragweite für das Zusammenspiel der Rollups Abschnitt 5.6-D entfaltet. Die Neutralitätsschicht des vorigen Abschnitts erstreckt sich in der Folge auf das Rollup, in demselben Umfang und mit demselben Vorbehalt, mit dem sie dort adressiert ist. Ein Baustein fehlt dem Verfahren noch, denn wer eine Zusage über die kommende Ordnung geben soll, muss vorher feststehen. Die Festlegung leistet der Deterministic Proposer Lookahead (EIP-7917, DEPL seit Fusaka): Das Protokoll berechnet im Voraus und verbindlich, welcher Validator in welchem der kommenden Slots den Block vorschlägt, eine öffentlich einsehbare Abfolge der nächsten Proposer.[338] Vor der Festschreibung war die Abfolge manipulierbar, weil ein Validator über Änderungen seiner effektiven Balance die Zuteilung verschieben konnte, ein Weg, den die deterministische Berechnung schließt.

Der Preis der Übergabe ist die Geschwindigkeit, denn ein zentraler Sequencer bestätigt in rund 0,25 Sekunden, ein Based Rollup ohne weitere Mechanik erst mit dem nächsten Layer-1-Block, nach bis zu 12 Sekunden. An dem Unterschied hing bislang die Entscheidung der Betreiber für den eigenen Sequencer. Die Antwort des Zielzustands sind Based Preconfirmations, im Folgenden Preconfs. Ein Teil der Validatoren registriert sich freiwillig als Preconfirmer und hinterlegt dafür zusätzlichen Stake als Sicherheit. Wer eine Transaktion sendet, erhält vom nächsten zuständigen Preconfirmer, den die Abfolge des Lookahead ausweist, eine sofortige Zusage über Aufnahme und Position seiner Transaktion.[339] Hält der Preconfirmer die Zusage nicht ein, verliert er einen Teil des hinterlegten Sta-

[338] Deterministic Proposer Lookahead (EIP-7917, DEPL seit Fusaka, 3. Dezember 2025; Autoren Lin Oshitani, Nethermind, und Justin Drake, Ethereum Foundation). Die Proposer-Zuständigkeit kommender Slots wird deterministisch und protokollseitig berechnet, womit die Identität des bevorstehenden L1-Proposers vorausberechenbar wird und Preconf-Garantien abgegeben werden können; zugleich entfällt das Grinding der effektiven Balance als Angriff auf die Vorhersage. Primärzuordnung 5.6-B als Voraussetzung von Based Sequencing und Based Preconfirmations.

[339] Based Preconfirmations (DEPL partiell, Taiko Phase 1). Ein Teil der Validatoren registriert sich über einen Registry Contract mit hinterlegtem Stake als Preconfirmer; der Nutzer identifiziert den nächsten zuständigen Preconfirmer über den Lookahead, sendet die Transaktion mit Preconfirmation Request und erhält eine Zusage in der Spanne von rund 100 Millisekunden bis 2 Sekunden, deren Bruch über Slashing sanktioniert wird. Die Garantie ist ökonomisch besichert; ihre Einordnung als erste Schicht des Finality-Stacks leistet 5.6-C.

kes durch Slashing. Die Zusage erreicht den Nutzer nach rund 2 Sekunden, und sie ist ökonomisch besichert. Die kryptographische Finalität bleibt aus, ein Rest, den erst der Finalitäts-Stack des folgenden Abschnitts einordnet. Somit bildet die Verlagerung des Sequencing den zweiten Baustein der strategischen Neubestimmung, deren Rahmen Abschnitt 5.1 trägt.

Der Existenzbeweis der Architektur läuft seit Mai 2024 auf dem Mainnet: Taiko operiert seither als erster Based Rollup und hat bis April 2026 über 900 Millionen Transaktionen ohne Ausfallzeit verarbeitet.[340] Seit August 2025 laufen die Preconfs auf dem Mainnet, in einer ersten Phase über eine zugelassene Liste von Preconfirmern, mit Bestätigungszeiten von rund 2 Sekunden. Der Beweis hat einen Vorbehalt: Die Preconf-Schicht läuft permissioned, und ihre Öffnung steht auf der Roadmap für 2026 und damit noch aus. Als Ethereum-äquivalenter Rollup erfüllt Taiko zugleich die Bedingung, an der der geerbte Schutz der Ausführungs-Ressource hängt, und der Kandidat für die Konvergenz beider Richtungen ist benannt.

Drei offene Grenzen

Offen bleiben drei Grenzen, von denen die erste ökonomisch ist: Mit der Ordnung verlagern sich ihre Erlöse, der Wert der Anordnung fließt an die Proposer der Layer 1, und dem Betreiber entfällt eine Einnahmequelle. Der Wert landet dort, wo er die Sicherheit finanziert, denn die Erlöse speisen das Security Budget, dessen Komposition Abschnitt 5.5-C entwickelt hat. An dem Verlust hängt die Zurückhaltung der bestehenden Betreiber, und die operativen Belege folgen dem Muster: Taiko startete als Based Rollup, und kein bestehender großer Betreiber hat die Umstellung vollzogen. Die zweite Grenze betrifft die Voraussetzung selbst, weil der deterministische Lookahead, der die Preconfs ermöglicht, den künftigen Proposer öffentlich vorhersagbar und so zum erreichbaren Ziel eines gezielten Denial-of-Service-Angriffs macht. Eine Forschungslinie unter dem Namen Single Secret Leader Election verfolgt das Gegenteil und hält die Identität des Proposers bis zur Ausführung seines Slots geheim, um ihn dem Angriff zu entziehen. Die Vorab-Zusage der Preconfs und der Schutz des Proposers

[340] Taiko Alethia als operativer Existenzbeweis (DEPL). Mainnet seit Mai 2024 als erster Based Rollup, bis April 2026 über 900 Millionen verarbeitete Transaktionen ohne Ausfallzeit; Preconfirmations seit dem 11. bis 13. August 2025 auf dem Mainnet in Phase 1 über eine permissioned Whitelist von Preconfirmern mit rund 2 Sekunden Bestätigungszeit; Roadmap: vollständig dezentralisierte Preconfirmations und formale Protokoll-Spezifikation Q1 2026, Sub-Sekunden-Latenz und Stage-2-Pfad Q2 2026. Taiko führt sich als Ethereum-äquivalenter (Typ-1) ZK-EVM-Rollup. Quelle: Taiko-Ankündigung und Dokumentation (August 2025).

stehen deshalb gegenwärtig als architektonische Entscheidung gegeneinander.[341] Die dritte Grenze ist die Trennung der Richtungen: Die geteilte Ordnung macht ein Rollup nicht trustless, solange seine Execution beim eigenen Verifier Contract bleibt, und die Auflösung des vorigen Abschnitts und die des vorliegenden greifen erst gemeinsam.

Im Zielzustand wären die beiden Leistungen, die ein Rollup heute selbst erbringt, einzeln an die Layer 1 verlagert: die Verifikation der Ausführung über die protokollseitige Prüfung, die Ordnung über das geteilte Sequencing. Der Betreiber, der am Anfang des Abschnitts beide Richtungen hielt, hielte keine mehr. Der folgende Abschnitt setzt aus den beiden Richtungen das vollständige Bild zusammen: das Rollup als Ausführungsumgebung, deren Ordnung und Korrektheit die Layer 1 selbst trägt und deren Bestätigungen ein dreischichtiger Finalitäts-Stack einordnet.

5.6-C Die Konvergenz: der trustless Rollup und sein Finalitäts-Stack

Das Rollup, das am Ende des vorigen Abschnitts stand, hat seinen Sequencer abgegeben und ist dennoch nicht trustless. Sein Betreiber (das jeweilige Rollup-Unternehmen) kann keine Transaktion mehr korrumpieren, und kein Ausfall seiner Infrastruktur hält das Rollup mehr an. Die Reihenfolge legen die Proposer der Layer 1 fest. Doch was die geordnete Sequenz bewirkt, prüft weiterhin der Verifier Contract des Betreibers. Akzeptiert er einen fehlerhaften State-Root, etwa durch einen Fehler in den Proving Circuits, sind die Gelder der Nutzer falsch verbucht, obwohl die Reihenfolge stimmte. Ein Rollup, das umgekehrt nur die EXECUTE-Verifikation nutzt, wird vom Konsens der Layer 1 geprüft, doch sein Betreiber ordnet weiterhin und kann auslassen oder ausfallen. Das Zweiklassenproblem, der Befund vom Anfang des Abschnitts, ist so in beiden Fällen nur halbiert, und erst die Verbindung beider Mechanismen schließt beide Lücken zugleich. Der Abschnitt beschreibt zuerst, was ein solches Rollup ist, und danach die drei Bestätigungsstufen, die ein Nutzer dort erhält, von der ersten Zusage bis zur endgültigen Finalität.

Ein Rollup, das beide Mechanismen verbindet, im Folgenden der „konvergierte Rollup“, nutzt alle drei Module der Layer 1: die Datenverfügbarkeit (Abschnitt 5.2), die Reihenfolge der Transaktionen (Abschnitt 5.6-B) und die Verifi-

[341] Lookahead-SSLE-Spannung. Die Single Secret Leader Election (SSLE, RES) hält die Identität des Proposers bis zur Ausführung seines Slots geheim und schützt ihn vor gezielten Denial-of-Service-Angriffen, relevant für I.4 (Liveness unter Angriff) und II.1; der Deterministic Proposer Lookahead (EIP-7917) verfolgt mit der deterministischen Vorhersage das Gegenteil. Das Verhältnis stellt eine architektonische Entscheidung zwischen L2-Preconf-Enabling und DoS-Schutz dar und ist im SOLL-Zustand unaufgelöst.

kation der Execution (Abschnitt 5.6-A). Nachdem die Rollup-Nodes aus der fixierten Sequenz den neuen Zustand errechnet haben, bestätigt die EXECUTE-Verifikation den Übergang durch denselben Konsens, der auch die Blöcke der Layer 1 prüft. Der Verifier Contract des Betreibers, an dem eben noch die Gelder hingen, wird gegenstandslos, und mit ihm das Risiko des fehlerhaften State-Root. Ein konvergierter Rollup trägt deshalb keine Vertrauensannahme mehr, die über die Layer 1 hinausgeht. Was von ihm bleibt, ist eine Ausführungsumgebung: ein eigener Gebührenmarkt, ein eigener State und die Anwendungen darauf, ohne eigenen Sequencer, ohne eigenes Proof-System, ohne Security Council und ohne eigene Governance. Im Diskurs des Ökosystems trägt der konvergierte Rollup den Namen Ultrasound Rollup, und mit Taiko Gwyneth ist eine Implementierung in Entwicklung, die die Verbindung beider Mechanismen ausdrücklich anstrebt.[342] Das Erstellen eines Native Rollups ist auf einen Aufruf der EXECUTE-Precompile geschrumpft, und weil die Ordnung allen Validatoren offensteht, wäre ein solches Rollup das erste, das sich permissionless vervielfältigen lässt. Die Folgen des Zusammenspiels für das Verhältnis der Rollups untereinander entwickelt Abschnitt 5.6-D.

Protokollseitig stützen sich beide Mechanismen auf die enshrined Proposer-Builder-Separation, die das Kapitel als Kapazitätsbaustein (Abschnitt 5.2) und als Neutralitätsbedingung (Abschnitt 5.5) bereits getragen hat. Die Trennung von Bau und Vorschlag gibt dem Proposer die Stellung, aus der er die Rollup-Blöcke ordnet. Und sie öffnet das Zeitfenster, in dem die EXECUTE-Verifikation in den Layer-1-Block integriert wird.[343] Die Verifikation selbst mündet in die Infrastruktur, die Abschnitt 5.2 für die Layer 1 entwickelt hat: die L1-zkEVM, die einen Block per Beweis validiert und das Nachrechnen ablöst. Die per SNARK-Beweis geführte EXECUTE-Verifikation kehrt das heutige Verhältnis der Proof-Systeme um. Im Ausgangszustand unterhält jedes Rollup ein eigenes, im Zielzustand prüft ein einziges, die zkEVM der Layer 1 mit ihren mehrfach implementierten Provern, die Zustandsübergänge aller EVM-äquivalenten Rollups.[344] Die

[342] Konvergenz Native plus Based (Zielbild, abhängig vom Forschungsstatus der EXECUTE-Precompile, EIP-8079, RES). Die Kombination bildet den maximalen Anbindungsgrad: Inclusion, Ordering und Execution stammen sämtlich von der Layer 1, das System ist vollständig trustless; im Ökosystem-Diskurs wird die Bauform als Ultrasound Rollup geführt. Taiko Gwyneth ist als Based Rollup mit synchroner Composability zu Ethereum in Entwicklung und zielt ausdrücklich auf die Konvergenz.

[343] Enshrined Proposer-Builder-Separation als Konvergenzpunkt (EIP-7732, PLAN, SFI Glamsterdam; vgl. 5.2-A zur Kapazitäts- und 5.5-A zur Neutralitätsfunktion, hier die dritte und letzte Begegnung). ePBS bildet den Konvergenzpunkt der Roadmap, der unter anderem die EXECUTE-Integration der Native Rollups und das Proving Window der zkEVM (Slot N+1) konditioniert.

[344] L1-zkEVM / Optional Execution Proofs (EIP-8025, PLAN, EF-Implementation-Roadmap mit sechs Sub-Themes vom 26. Januar 2026, ohne Hard-Fork-Erfordernis und damit von neuartigem Governance-Status). Validierung durch Beweis statt Re-Execution, mit 3-of-5-Multi-Prover über die Client-Diversität; das Realtime-Proving-Ziel

Zeitpläne beider Vorhaben sind ausdrücklich gekoppelt, denn der Reifegrad der zkEVM ist zugleich die Voraussetzung der protokollseitigen Rollup-Verifikation.

Der gestaffelte Finalitäts-Stack

Was der Nutzer eines konvergierten Rollups als Bestätigung erhält, staffelt sich in drei Schichten mit drei verschiedenen Garantiearten. Die erste Schicht liefert nach rund 2 Sekunden die Preconf, die ökonomisch besicherte Zusage eines dafür registrierten Validators der Layer 1. Die zweite Schicht liefert die Fast Confirmation Rule (PLAN), eine attestationsbasierte Regel ohne Hard Fork, die als Pull Request der consensus-specs spezifiziert und in Client-Implementierung ist.[345] Sie erklärt einen Layer-1-Block für deterministisch bestätigt, sobald hinreichend viele Attestationen ihn tragen, nach rund 13 Sekunden. Sie setzt voraus, dass mindestens drei Viertel des Stakes ehrlich attestieren und die Netzlatenz unter drei Sekunden bleibt. Mit ihr sinkt die Bestätigung der Layer 1 von rund 13 Minuten auf rund 13 Sekunden, was die Einzahlungen bei Börsen und das Bridging um rund 98 Prozent beschleunigt.

Die dritte Schicht ist die Finalität selbst. Das Roadmap-Ziel heißt Single-Slot-Finalität, doch das praktisch konvergierende Design, dessen Architektur und Preis Abschnitt 5.5-D als Drei-Slot-Finalität entwickelt hat, senkt die unumkehrbare Finalisierung im Zielzustand auf rund 36 Sekunden.[346] Der Stack staffelt drei Garantiearten in aufsteigender Stärke: die besicherte Zusage nach rund 2 Sekunden, die deterministische Bestätigung nach rund 13 Sekunden und die kryptographische Finalität nach rund 36 Sekunden. Für den Nutzer eines konvergierten Rollups entspricht jede Wartezeit einer benennbaren Garantie, und die letzte Garantie kostet keine Minuten mehr.

(99 Prozent der Blöcke unter zehn Sekunden) wurde im Dezember 2025 erreicht, mit einer Verbesserung von 16 Minuten auf 16 Sekunden Proving-Latenz und rund 45-facher Kostenreduktion, während die formale Sicherheitshärtung in gestuften Meilensteinen aussteht (100-bit bis Glamsterdam, 128-bit bis Ende 2026). Vitalik Buterin koppelt die Zeitlinien ausdrücklich: Die Adoption von ZK auf der Layer 1 und die Einführung der Native-Rollup-Precompiles verlaufen im Wesentlichen synchron. Die Primärbehandlung der zkEVM trägt 5.2; hier zählt die L2-Wirkung über die SNARKifizierte EXECUTE-Prüfung.

[345] Fast Confirmation Rule (consensus-specs PR #4747, PLAN, reines Client-Feature ohne Hard Fork, Client-Implementierung laufend mit Rollout in den kommenden Monaten). Attestationsbasierte Bestätigung: Bei mindestens 75 Prozent ehrlichem Stake und einer Netzlatenz unter drei Sekunden gilt ein Block nach rund 13 Sekunden als deterministisch bestätigt; Einzahlungen bei Börsen und das Bridging von der Layer 1 auf die Layer 2 beschleunigen sich um rund 98 Prozent. Die Regel ist unabhängig von ePBS und von der Single-Slot-Finalität und bildet die zweite Schicht des Finality-Stacks zwischen den Based Preconfirmations und der SSF.

[346] Single-Slot-Finalität als dritte Schicht (RES, Horizont nach 2028; die vollständige Behandlung einschließlich der inhaltlichen Einordnung als Drei-Slot-Finalität trägt 5.5-D). Im Zielzustand sinkt die unumkehrbare Finalisierung auf rund 36 Sekunden (drei Slots); im vorliegenden Abschnitt zählt allein die Stack-Funktion als kryptographische Endgültigkeit über der deterministischen Bestätigung.

Die Reichweite der Konvergenz bleibt begrenzt, und ihre Grenzen sind die der beiden Richtungen. Sie gilt für Rollups, die EVM-äquivalent bleiben und Based Sequencing übernehmen. Beides ist eine Entscheidung der Betreiber, und das Ökosystem behält deshalb ein Spektrum von Anbindungsgraden, von der vollen Konvergenz bis zur souveränen Chain mit minimaler Bindung an die Layer 1. Der Stack selbst ist ungleich gereift: Die mittlere Schicht ist aktiv, die erste läuft partiell und permissioned, die dritte ist Forschungsgegenstand jenseits 2029. Hinzu kommen zwei Vorbehalte der Träger. Die zkEVM erreicht ihre Geschwindigkeit derzeit auf Sicherheitsannahmen, deren formale Härtung in gestuften Meilensteinen aussteht. Und die deterministische Bestätigung beruht auf der Ehrlichkeit von drei Vierteln des Stakes, einer Voraussetzung, die an die ungesicherte Verteilung aus Abschnitt 5.5-C zurückverweist.

Im Zielzustand wäre das Zweiklassenproblem damit für den konvergierten Teil des Ökosystems aufgelöst. Ein Rollup ist dort eine Ausführungsumgebung der Layer 1, geordnet von deren Proposern, geprüft von deren Konsens, bestätigt in deren Stack. Welche Lasten eine solche Schicht tragen kann, sobald andere Systeme auf ihr verbindlich verbuchen, entwickeln die beiden folgenden Abschnitte: zunächst das Settlement tokenisierter Werte, dann die Rolle für ein heterogenes Ökosystem von Chains.

5.6-D Das Verhältnis der Rollups und das Settlement tokenisierter Werte

Das Rollup, das am Ende des vorigen Abschnitts als Ausführungsumgebung der Layer 1 stand, existiert im Zielzustand nicht allein. Wer heute Gelder von einem Rollup in ein anderes bewegt, überquert die Grenze zwischen zwei fremden Sicherheitssystemen, mit eigener Brücke, eigenen Fristen und eigenen Vertrauensannahmen auf beiden Seiten. Die Konvergenz beider Mechanismen verändert die Grenze selbst, denn mit dem Sicherheitssystem des einzelnen Rollups löst sich auch die Fremdheit zwischen den Rollups auf. Beide Fragen des Abschnitts hängen an derselben Eigenschaft, denn was die Rollups einander garantieren können, ist zugleich das, was die Schicht externen Nutzern anbietet. Der vorliegende Abschnitt entwickelt deshalb zuerst, was aus der gemeinsamen Ordnung und dem gemeinsamen Finalitätshorizont für das Verhältnis der Rollups untereinander folgt. Danach fragt es, welche Lasten die Schicht trägt, sobald nicht mehr nur das eigene Ökosystem auf ihr verbucht. Die Antwort findet es beim tokenisierten Kapital der traditionellen Finanzwelt, dessen Verbuchung das anspruchsvollste Anforderungsprofil stellt.

Das neue Verhältnis beginnt bei der Ordnung, denn die Übergabe des Sequen-

cing wirkt über das einzelne Rollup hinaus: Derselbe Proposer ordnet die Blöcke aller Based Rollups innerhalb desselben Slots (Abschnitt 5.6-B). Die relative Reihenfolge der Transaktionen zweier Rollups entsteht so in einem einzigen Akt, gilt über die Rollup-Grenze hinweg und hängt an keiner Abstimmung unabhängiger Systeme mehr. Wer auf zwei Rollups zugleich handelt, plante gegen eine einzige verbindliche Sequenz und nicht gegen zwei voneinander unabhängige Abfolgen, deren Verhältnis niemand garantiert. Weil dieselbe Verifikation über die Zustandsübergänge aller konvergierten Rollups befindet, teilen deren Einträge außerdem einen gemeinsamen Finalitätshorizont. Eine Überweisung zwischen zwei solchen Rollups würde auf beiden Seiten im selben Stack endgültig, nach denselben Fristen und unter denselben Annahmen (Abschnitt 5.6-C). Eine Brücke mit eigenen Vertrauensannahmen, deren Wegfall Abschnitt 5.6-A für das Verhältnis zur Layer 1 entwickelt hat, bräuchte sie nicht mehr. Für eine Anwendung, die über mehrere Rollups reicht, verschöbe sich die maßgebliche Unsicherheit vom Vertrauen in fremde Systeme auf die Wartezeit bis zur Finalität.

Composability, die Fähigkeit von Anwendungen, über Systemgrenzen hinweg ineinanderzugreifen, erreicht ihre stärkste Form in der atomaren Verbindung, bei der zwei Operationen im selben Block stehen und gemeinsam gelingen oder gemeinsam scheitern.[347] Die atomare Form bleibt im Zielzustand unerreichbar, weil sie eine synchrone Kommunikation zwischen den Rollups innerhalb eines einzelnen Slots verlangte, die weder die gemeinsame Ordnung noch die protokollseitige Verifikation liefern. Erreichbar wäre die zweite Stufe der vierstufigen Logik der Arbeit: asynchrone Composability mit deterministischen Garantien, tendenziell unterhalb eines Slots. Gegenüber dem Ausgangszustand, in dem die meisten Verbindungen über die dritte Stufe laufen, läge der Gewinn weniger in der Geschwindigkeit als in der Art der Garantie. An die Stelle des Vertrauens in dritte Systeme träte eine benennbare Frist mit kryptographischer Deckung. Der vorige Abschnitt hat eine zweite Folge angekündigt, und sie betrifft das Wachstum des Ökosystems. Weil sich ein konvergierter Rollup permissionless vervielfältigen ließe und jede Kopie unter derselben Ordnung entstünde, träte jedes neue Rollup von Beginn an in das beschriebene Verhältnis ein. Das Ökosystem wüch-

[347] Cross-L2-Composability in der vierstufigen M1-Tier-Logik: atomare Composability (gleicher Block, keine Vertrauensannahmen), asynchrone Composability unter einer Stunde, Trust-Bridge-basierte Composability, keine strukturelle Composability. Der IST-Zustand operiert für die meisten L2-Interaktionen auf Stufe 3; der SOLL-Zustand erreicht über die Kombination aus Based Sequencing (DEPL) und nativer Verifikation (RES) Stufe 2, asynchron mit deterministischen Finality-Garantien und tendenziell unterhalb eines Slots; Stufe 1 bleibt im SOLL-Zeitraum unerreichbar, weil sie eine gemeinsame Execution-Umgebung oder synchrone Cross-L2-Kommunikation innerhalb eines einzelnen Slots erfordern würde. Taiko Gwyneth führt sich als „based rollup synchronously composable with Ethereum“; der Anspruch bezeichnet die synchrone Composability eines einzelnen Based Rollups zur Layer 1, keine atomare Composability zwischen Rollups, und bleibt Projektanspruch einer Implementierung in Entwicklung.

se als Menge von Ausführungsumgebungen über einer gemeinsamen Grundlage, und seine Vielfalt bliebe eine Frage der Spezialisierung, weniger der Sicherheit.

Praktisch nutzbar wird das Verhältnis durch eine Schicht, die dem Nutzer die Verwaltung der Grenzen abnimmt. Ein Intent ist die Erklärung eines gewünschten Ergebnisses anstelle eines vorgegebenen Ausführungspfads. Der Nutzer legt fest, welcher Wert auf welchem Rollup ankommen soll, und ein Solver, ein darauf spezialisierter Marktakteur, übernimmt Weg und Ausführung gegen Entgelt. Der Standard ERC-7683 (Cross-Chain Intents, DEPL) normiert die Form solcher Intents über die Rollups hinweg, und das Open Intents Framework (DEPL) versammelt die zugehörige Infrastruktur des Ökosystems.[348] Die deterministische Bestätigung der Layer 1 verkürzt dabei die Frist, nach der das Settlement eines Solvers feststeht, eine Funktion des Finalitäts-Stacks aus dem vorigen Abschnitt. Solver operieren dort, wo Liquidität und Settlement-Sicherheit am höchsten liegen, und tragen die Nachfrage deshalb auf die Schicht, die beides vereint. Die Grenze liegt unterhalb des Standards: ERC-7683 macht Intents portabel, doch Solver halten protokollspezifische Liquiditätsbestände und eigene Routing-Logik vor, sodass sich die Ausführungsumgebung langsamer vereinheitlicht als die Form der Intents.

Verbindliche Verbuchung tokenisierter Werte

Verbindliche Verbuchung stellt ein Anforderungsprofil, das über den Durchsatz hinausgeht. Ein Eintrag muss in benennbarer Frist endgültig werden, seine Ausführung darf niemanden bevorzugen, seine Richtigkeit muss ohne Erlaubnis prüfbar sein, und sein Bestand muss über Jahrzehnte beanspruchbar bleiben. Die konvergierte Schicht lieferte jede der vier Anforderungen aus dem Bestand des Kapitels. Die Finalität trüge der gestaffelte Finalitäts-Stack (Abschnitt 5.6-C), die Gleichbehandlung die protokollseitige Neutralität (Abschnitt 5.5), die Prüfbarkeit die allgemein zugängliche Verifikation (Abschnitt 5.3) und den Daueranspruch das differenzierte State-Management (Abschnitt 5.4). Dabei ist die Gleichbehandlung mehr als eine Fairness-Eigenschaft, denn ein Verbuchungsort, der einzelne Einträge verzögern oder auslassen kann, taugt nicht als neutrale In-

[348] Cross-Chain Intents (ERC-7683, DEPL; auditierter Code seit Januar 2025) und Open Intents Framework (OIF, DEPL; Start durch die Ethereum Foundation im Februar 2025, über 30 Teams). ERC-7683 normiert Order-Strukturen und Settler-Interfaces für Cross-L2-Intents, mit über 70 integrierenden Projekten und Cross-Chain-Ausführung in rund 2 Sekunden; per April 2026 liefen produktive Endpunkte unter anderem bei Across, UniswapX, CoW Protocol und Eco. Die Vereinheitlichung der Solver-Ebene verläuft langsamer als die der Standard-Ebene, weil Solver protokollspezifische Liquiditätsbestände und Routing-Logik vorhalten. Die Fast Confirmation Rule beschleunigt das Settlement der Intents über die deterministische Bestätigung der Layer 1 (vgl. 5.6-C).

frastruktur zwischen Wettbewerbern. Hinzu kommt eine Eigenschaft, die kein einzelnes Modul liefert: Der Eintrag hängt an keinem Verwahrer, dessen Fortbestand der Inhaber prüfen muss, er hinge am Protokoll selbst. Für institutionelle Nutzer übersetzte sich der Stack in eine Garantie, deren Stärke mit jeder seiner Schichten wächst und deren stärkste Form keine Geschäftstage mehr kostet.

Die Nachfrage nach einer solchen Schicht ist kein Postulat des Zielzustands. Tokenisierte Werte, im Finanzdiskurs als Real World Assets geführt, liegen bereits in zweistelliger Milliardenhöhe auf dem Ethereum-Mainnet, dem größten einzelnen Verbuchungsort der Kategorie.[349][350] Die amerikanische Marktinfrastruktur hat die Kategorie Ende 2025 regulatorisch geöffnet, hält die Finalität in ihrer Pilotarchitektur jedoch beim zentralen Verwahrer, während die konvergierte Schicht sie als Eigenschaft des Konsenses trüge.[351] Was heute dort liegt, nutzt die Garantien des Ausgangszustands, und das Anforderungsprofil dieser Nutzer ist zugleich der Maßstab, an dem sich der Zielzustand messen lassen muss. Eine Anforderung erfüllt die Schicht selbst nicht: die Vertraulichkeit der Geschäftsvorgänge, denn die öffentliche Verbuchung legt Positionen und Gegenparteien offen, die institutionelle Akteure nicht preisgeben können, und das protokollseitige Zielbild dafür entwickelt Abschnitt 5.1.

Der Abschnitt begann mit einem strukturellen Problem und endet mit einer Eigenschaft, die aus dessen Auflösung folgt. Eine Schicht, die ihre eigenen Rollups ohne institutionelles Vertrauen trüge, womit das Zweiklassenproblem für den konvergierten Teil aufgelöst wäre, böte externem Kapital genau die Garantien, an denen verbindliche Verbuchung hängt. Zufließendes Kapital vertieft die Liquidität, und die vertiefte Liquidität zieht Solver und weiteres Kapital an. Je-

[349] Tokenisierte Werte (Real World Assets, RWA) auf Ethereum, primärer Datenstand Februar 2026: über $17 Mrd. auf dem Mainnet, rund 315 Prozent Jahreswachstum gegenüber rund $4,1 Mrd. im Vorjahr; Marktanteil je nach Messung rund 34 Prozent (The Block) bis deutlich über 50 Prozent (rwa.xyz); Stablecoin-Bestand auf dem Mainnet über $175 Mrd. Verifikation per Juni 2026: $16,6 Mrd. und 52,85 Prozent Marktanteil nach rwa.xyz; Gesamtmarkt über $65 Mrd. mit Ethereum bei rund 33 Prozent nach The Block. Die Divergenz der Anteilswerte ist methodisch bedingt (unterschiedliche Abgrenzung der Kategorie und der erfassten Netzwerke) und wird hier ausgewiesen, nicht aufgelöst. Quellen: The Block (Februar und Mai 2026); rwa.xyz/Token Terminal (Juni 2026).

[350] BlackRock USD Institutional Digital Liquidity Fund (BUIDL) als Benchmark-Produkt der Kategorie: tokenisierter Geldmarktfonds, Auflage März 2024 mit Securitize auf Ethereum; rund $2,5 Mrd. AUM per Mitte Mai 2026, größter tokenisierter Treasury-Fonds; Emission auf mehreren Chains mit Ethereum als Mehrheitsträger des Volumens. Im Mai 2026 reichte BlackRock zwei weitere tokenisierte Geldmarktfonds bei der SEC ein. Quellen: BlackRock/Securitize (Fondsdokumentation); Token Terminal (AUM-Stand Mai 2026).

[351] No-Action-Letter der SEC Division of Trading and Markets an die Depository Trust Company vom 11. Dezember 2025: Drei-Jahres-Pilot („Preliminary Base Version") der DTCC Tokenization Services, der Security Entitlements an US-Treasuries, Russell-1000-Aktien und ausgewählten Index-ETFs als Token auf zugelassenen, auch permissionless Blockchains abbildet; Start in der zweiten Jahreshälfte 2026 vorgesehen. Vorbehalte: Tokenisierte Entitlements erhalten im Pilot keinen Settlement- oder Collateral-Wert, die DTC bleibt Quelle der Settlement-Finalität und behält die Letztaufzeichnung; die erste angekündigte Umsetzung läuft mit Digital Asset auf dem Canton Network. Der Letter öffnet die Kategorie regulatorisch, ohne sie einem Netzwerk zuzuweisen. Quelle: SEC/DTCC (Dezember 2025).

de Stufe erhöhte die wirtschaftlichen und sicherheitsseitigen Wechselkosten. Ein Verbuchungsort, dessen Verlassen stetig teurer wird, nähert sich dem Zustand, in dem seine Funktion nicht mehr ersetzbar ist. Die Qualifikation beruht nicht auf einer einzelnen Neuerung, sie beruht auf dem Zusammenwirken der Architekturen, die das Kapitel von der Kapazität bis zur Neutralität entwickelt hat. Damit steht der Befund: Zwei Mechanismen, die je eine Richtung an die Layer 1 holen, ergäben eine Schicht, nach innen deterministisch geordnet, nach außen ein Verbuchungsort ohne institutionelle Vorbedingung. Ob diese Rolle über das eigene Ökosystem hinaus auf Chains reicht, die keine Rollups sind, behandelt der abschließende Abschnitt von 5.6.

5.6-E Forschungshorizont: heterogene Chains und autonome Agenten

Die Frage, mit der der vorige Abschnitt geschlossen hat, reicht über den Zielzustand hinaus, und das verändert den Status der Antwort. Ob die konvergierte Schicht auch Systeme trägt, die keine Rollups sind, und Akteure bedient, die keine Menschen sind, beantwortet keine Spezifikation der Roadmap. Beide Erweiterungen gelten im Umfeld der Roadmap als Ziel der Schicht, und gerade deshalb verlangt ihre Darstellung die ausdrückliche Markierung ihres Status. Der vorliegende Abschnitt unterscheidet daher zwei Größen: die Architektur, die in den vorigen Abschnitten entwickelt ist und hier nur angewandt wird, und die Übernahme durch neue Systeme und Akteure, die keinen Reifegrad trägt und als Forschungshorizont geführt wird. Das Urteil von 5.6, das mit dem vorigen Abschnitt geschlossen ist, hängt an keiner der folgenden Aussagen.

Die erste Frage betrifft Chains mit eigenem Konsens, die sich an die Schicht binden wollten, ohne Rollups zu werden. Strukturell stünde einem solchen System der schwächere Teil des Angebots offen: Es könnte seine Blockhistorie periodisch in der Schicht festschreiben und gewönne eine Finalität, die sein eigener Konsens nicht erzeugt. Streit über die eigene Vergangenheit lässt sich so gegen einen externen Maßstab entscheiden, dessen Neutralität das System nicht selbst stellen muss. Was es nicht gewinnt, ist die Eigenschaft des konvergierten Rollups, denn die Verifikation seiner Zustandsübergänge bleibt seine eigene, und mit ihr jede Annahme seines Konsenses. Auch eine ökonomische Bindung ist denkbar, etwa über Sicherheiten, die auf der Schicht hinterlegt werden, doch sie ersetzte die Annahmen des fremden Konsenses nicht, sie ergänzte sie um weitere. Die Bindung heterogener Systeme bleibt deshalb eine ökonomische oder institutionelle, während Rollups eine kryptographische erhalten, und das Zweiklassenproblem, das der Abschnitt für Rollups schloss, kehrte an ihrer Außengrenze in an-

derer Form wieder. Der Diskurs des Ökosystems führt die Schicht gleichwohl als Grundlage ganzer Chain-Ökosysteme, im Anspruch einer zivilisatorischen Infrastruktur, deren Tragweite über jede einzelne Anwendung hinausreicht.[352] Welche Mechanismen eine solche Rolle tragen könnten und ob fremde Konsenssysteme sie annähmen, ist im Zielzustand nicht angelegt und bleibt Gegenstand offener Forschung.

Autonome Agenten als Nutzer

Die zweite Frage betrifft eine Akteursklasse, deren Bedarf das Anforderungsprofil verbindlicher Verbuchung in zugespitzter Form stellt. Autonome Agenten, Software-Systeme, die ohne menschliche Freigabe Leistungen beauftragen, erbringen und bezahlen, bleiben von Bankkonto, Vertragsunterzeichnung und Rechtsform ausgeschlossen. Ein Verbuchungsort ohne institutionelle Vorbedingung (Abschnitt 5.6-D) wäre für solche Akteure nicht die bessere Option unter mehreren, er wäre die einzige. Maschinelle Gegenparteien könnten einander keinen Kredit aus Beziehung gewähren, jede Leistung verlangte Zug um Zug ein Settlement, dessen Garantie geprüft und nicht verhandelt wird. Die Beträge sind klein, die Frequenz hoch und die Gegenpartei wechselnd, ein Profil, für das die institutionelle Zahlungsinfrastruktur weder Konten noch Preise vorsieht. Ein Agent hielte sein Guthaben selbst, stellte Sicherheiten aus eigenem Bestand und bräuchte für beides keinen Verwahrer, der für ihn handelt. Der Pfad dafür steht nicht aus: Die Intent-Schicht (Abschnitt 5.6-D) trägt die Koordination und Bezahlung zwischen Agenten, ohne dass zwischen Auftrag und Settlement eine menschliche Vermittlung steht. Die Schicht verbucht, was ihre Regeln erfüllt, unabhängig davon, wer ein Ergebnis erklärt, und genau darin liegt die Anschlussfähigkeit für Akteure ohne Rechtsform.

Die Garantien der Schicht wären maschinenlesbar, ihre Fristen benennbar, und ihre Zugangsbedingung erschöpfte sich im Besitz eines Schlüssels, eine Kombination, die kein institutionelles Settlement-System anbietet. Dass die Bestätigung in Sekunden und deterministisch vorliegt, eine Funktion des Finalitäts-Stacks (Abschnitt 5.6-C), passt die Frist an die Frequenz maschineller Interaktion an. Hinzu träten Anforderungen, die menschliche Nutzer so nicht stellen: ei-

[352] Die Rahmung der Schicht als zivilisatorische Infrastruktur geht auf Vitalik Buterins Neujahrs-Post auf X (@VitalikButerin, 1. Januar 2026) zurück, der Ethereum jenseits kurzfristiger Markt- und Tokenisierungs-Narrative als dauerhafte, neutrale und zensurresistente Grundlage für Finanzen, Identität und Governance über Jahrzehnte fasst und am Maßstab des walkaway test misst. Die Ausweitung auf die Schicht als Grundlage ganzer Chain-Ökosysteme ist Position des breiteren Ökosystem-Diskurses, die der Body berichtet und zugleich begrenzt, nicht eine Aussage der Arbeit. Quellen: V. Buterin, Neujahrs-Post auf X (1. Januar 2026); CoinDesk, Vitalik Buterin on the two goals Ethereum must meet to become the world computer (1. Januar 2026).

ne Identität, die an keiner Person hängt, eine Reputation, die maschinell prüfbar ist, und eine Verifikation erbrachter Leistungen ohne Gericht und ohne Vertragspartner. Für die erste davon steht die Antwort bereits im Kapitel, denn die Kontoarchitektur aus Abschnitt 5.3 bindet Autorisierung an programmierbare Regeln und nicht an eine Person. Der Entwurf ERC-8004 normiert dafür Identitäts-, Reputations- und Validierungsregister auf der Schicht, ein ausdrücklich früher Bezugspunkt, der eine Richtung belegt.[353] Was der Entwurf nicht trägt, ist die Frage der Haftung und der Aufsicht, denn ein Akteur ohne Rechtsform ist auch ein Akteur, gegen den kein Anspruch vollstreckbar ist. Der strukturelle Befund hängt an diesem Reifegrad nicht: Dieselbe Schicht trägt zwei Nachfrageklassen unter dem Eigenschaftsbündel, das der vorige Abschnitt für das tokenisierte Kapital hergeleitet hat, und die maschinellen Akteure verlangen dasselbe Bündel aus denselben Gründen, nur ohne die Alternative. Ob aus der Akteursklasse eine Nachfrageklasse wird, hängt an Entwicklungen außerhalb des Protokolls, und keine Aussage des Kapitels gewinnt oder verliert mit ihr.

Beide Fragen teilen denselben Status: Sie liegen jenseits des Zielzustands, den die Roadmap spezifiziert, und jenseits der Reifegrade, mit denen die Arbeit ihre Befunde deckt. Der Abschnitt hält sie fest, weil die Architektur sie nahelegt, und er beantwortet sie nicht, weil die Annahme an keiner Spezifikation hängt, gegen die sich eine Antwort prüfen ließe. Die offene Größe ist dabei ihre Übernahme durch Systeme und Akteure, über die das Protokoll nicht entscheidet. Für das Gesamtbild des Abschnitts verbindet die Architektur damit beide Dimensionen der Settlement-Rolle bereits. Das Zielbild ist insoweit architektonisch vollständig, und offen bleibt allein, ob die zweite Nachfrageklasse eintritt. Die Bewertung des folgenden Abschnitts gilt deshalb dem Zielzustand, den die Abschnitte 5.2 bis 5.6 entwickelt haben, und nicht dem Horizont, den dieser Abschnitt markiert.

[353] ERC-8004 („Trustless Agents"), Draft-Standard seit August 2025, entstanden im Umfeld der Ethereum Foundation mit Beteiligung von MetaMask, Google und Coinbase; knüpft an das Agent-to-Agent-Protokoll (A2A) an und ergänzt es um drei On-Chain-Register: Identität (als ERC-721), Reputation und Validierung. Die Register sind deployt; auf der DevConnect im November 2025 wurden erste Implementierungen gezeigt, die Zahl der beteiligten Entwickler lag nach Angaben von Davide Crapis (Ethereum Foundation) bei 1.000 bis 2.000. Einstufung der Arbeit: Draft mit deployten Registern, oberhalb reinen Forschungsstatus, unterhalb produktiver Reife; der Standard belegt eine Entwicklungsrichtung, keine eingetretene Nachfrage der Akteursklasse. Quellen: ERC-8004-Spezifikation (Ethereum Magicians, August 2025); DevConnect (November 2025).

5.7 SOLL-Bewertung

5.7-A SOLL-Bewertung der Kritischen Bedingungen

Die vorangegangenen Abschnitte haben den Zielzustand entlang seiner technischen Richtungen entfaltet, von der Execution über die Verifikation und den State bis zur Neutralität und zur Architektur der Layer 2. Die folgende Bewertung wechselt das Register und ordnet das Entfaltete den zwölf Kriterien des Bewertungsrahmens zu, beginnend mit den drei Kritischen Bedingungen, deren Stufe das Gesamturteil deckelt. Sie gilt dem SOLL-Zustand als architektonisch kohärentem Designzustand und nicht dem operativen IST. Durchgehend trägt sie die Reifegrade der Taxonomie mit, von der gelieferten Deployment-Reife (DEPL, IMPL) über die Planungs-Verankerung (PLAN) bis zur ungesicherten Forschung (RES), weil keine Einordnung ihren Reifegrad überschreiten darf. Die Bewertung bleibt zugleich auf die Architektur-Ebene reduziert, da der IST-Vergleich, die volle Drei-Ebenen-Synthese und die Belastbarkeit gegen Teilrealisierung in Kapitel 6 gehören.

I.2 Sicherheits- und Vertrauenslast

Die Sicherheits- und Vertrauenslast (I.2) erreicht im Zielzustand die Stufe Erfüllt mit Einschränkung.[354] Die in 5.5 entfaltete Relay-Elimination durch ePBS trägt die Vertrauenslast-Reduktion auf der Konsens-Schicht, sodass die Relay-Vertrauensannahme des IST-Zustands, über die heute der Großteil der Blöcke läuft, im Zielzustand entfällt. Die in 5.3 entwickelte zkEVM-Verifikation senkt die Validator-Vertrauensannahme, indem die Korrektheit der Ausführung kryptographisch bewiesen und nicht länger sozial angenommen wird, während die Stateless Clients aus derselben Verifikations-Architektur die Abhängigkeit von kommerziellen RPC-Providern auflösen. Aus der Zuordnung der genannten Mechaniken zum Kriterium ergibt sich eine systematische, über nahezu jede Protokollschicht reichende Reduktion der Vertrauensannahmen, deren epistemische Belastbarkeit von der gelieferten Inter-Layer-Vereinfachung bis zur planungsverankerten ePBS-Aktivierung gestuft ist.

Die Stufe bleibt unterhalb von Erfüllt, weil zwei Restrisiken nicht durch Protokolländerung erreicht werden. Das erste liegt in der zkEVM selbst, deren

[354] SOLL-Bewertung I.2. Die Stufe Erfüllt mit Einschränkung folgt der gestuften Vertrauenslast-Reduktion über nahezu jede Protokollschicht, getragen von Relay-Trust-Elimination via ePBS (PLAN/SFI Glamsterdam), Validator-Trust-Reduktion via zkEVM (Aktive EF-Roadmap) und RPC-Trust-Reduktion via Stateless Clients und Helios (DEPL/IMPL). Die zwei nicht protokollseitig erreichbaren Residual-Risiken sind die zkEVM-Proving-Conjecture und die Access-Schicht (Wallets, Frontends, DNS).

Proving-Sicherheit auf mathematischen Annahmen mit noch offenem Beweis beruht. Die Verifikation verschiebt das Vertrauen dadurch auf die Integrität der zugrunde liegenden Annahmen, statt ihn aufzulösen. Das zweite liegt auf der Access-Schicht, denn die Vertrauenslast der Wallets, der Frontends und der DNS-Auflösung liegt außerhalb des Protokolls und wird durch keine Roadmap-Komponente erreicht, weil der Großteil der Nutzer über vermittelnde Anwendungen statt über eigene Nodes interagiert. Beide Risiken markieren die Grenze der protokollseitigen Vertrauensreduktion und tragen die Einschränkung der Stufe.

I.4 Minimale tragfähige Garantien

Das breiteste der drei Kriterien sind die Minimalen tragfähigen Garantien (I.4), die vier Aspekte umfassen: die Finalität, die Liveness, einen Degradation Mode und die Zensurresistenz unter Angriff. Die vier Aspekte sind in den vorhergehenden Abschnitten konzentriert, die Finalität und die Liveness in der Finalitäts-Architektur aus 5.5, der Degradation Mode im Inactivity Leak aus 5.3-D und die Zensur im Neutralitätsblock aus 5.5, sodass für sie eine knappe Synthese nach vorn genügt. Zwei weitere Substanzen liegen quer zu den vier Aspekten und werden außerhalb der Vierergruppe als Zusatzmaterial geführt: die State-Persistenz, die 5.4 als zusammenhängender Abschnitt entfaltet, und die Post-Quantum-Robustheit, die über mehrere Abschnitte verteilt ist und eine eigene Sammlung verlangt, die das Material erst sichtbar macht. Die größere Tiefe der Post-Quantum-Sammlung folgt der Verteilung ihres Materials.

Die in 5.5 entfaltete Finalitäts-Architektur verstärkt die Garantie im Zielzustand mehrschichtig und nach Reifegrad gestaffelt. Auf der Ebene der Layer 2 liefern Based Preconfirmations Bestätigungen im Sub-Zwei-Sekunden-Bereich, die in 5.6 entfaltete Confirmation Rule (FCR) verkürzt die Konsens-Bestätigung auf rund 13 Sekunden, und die Drei-Slot-Finalität bindet die endgültige Finalität der Layer 1 auf rund 36 Sekunden.[355] Den M2-Schwellenwert von unter 15 Minuten unterschreiten bereits die reiferen Schichten weit: Die deployten Based Preconfirmations und die als Pull Request der consensus-specs spezifizierte, in Client-Implementierung befindliche Confirmation Rule bringen die Bestätigung der Layer 1 in den Sekundenbereich, unabhängig vom Reifegrad der Drei-Slot-Finalität. Die langfristige Richtung auf Single-Slot-Finalität bleibt

[355] Based Preconfirmations rund 2 Sekunden (DEPL, Ebene der Layer 2) und Drei-Slot-Finalität rund 36 Sekunden (RES, Horizont jenseits 2029, ohne Fork-Termin) gemäß der in 5.5 getragenen Finalitäts-Architektur. Die Confirmation Rule (FCR) rund 13 Sekunden ist als consensus-specs PR #4747 (März 2026) spezifiziert, befindet sich in Client-Implementierung mit Rollout in den kommenden Monaten und trägt damit den Status PLAN, nicht IMPL.

als Konsens-Endzustand nennbar, ohne den nahen SOLL-Wert zu bestimmen. Gegen das Kriterium bedeutet die Staffelung, dass die Finalitäts-Garantie über Schichten unterschiedlichen Reifegrads redundant getragen wird, von den deployten Based Preconfirmations über die in Client-Implementierung befindliche Confirmation Rule bis zur Drei-Slot-Finalität im Forschungsstatus, statt an einem einzelnen Mechanismus zu hängen.

Die Liveness, die Fähigkeit, unter Stress weiter Blöcke zu produzieren, verstärkt sich im Zielzustand über dieselbe Finalitäts-Architektur, weil die gestaffelten Bestätigungsschichten die Blockproduktion nicht mehr an einen einzelnen Mechanismus binden, und die Single-Slot-Finalität behält den in 5.3-D entfalteten Inactivity Leak ausdrücklich als Rückfall-Mechanismus bei, der die Kette bei einem Ausfall von über einem Drittel der Validatoren weiterlaufen lässt. Der Degradation Mode beruht auf demselben Inactivity Leak, der auf dem Mainnet erprobt und operativ ist und den geordneten Rückfall bei einem Ausfall nichtpartizipierender Validatoren trägt, und er greift unter der Single-Slot-Finalität granularer, sodass die Garantie im Zielzustand gehalten und geschärft wird. Die Zensurresistenz wird protokollseitig über FOCIL erzwungen, dessen Bewertung als Mechanismus in II.1 steht und hier nur als Mindestgarantie verbucht wird. Der Querverweis ist methodisch notwendig, weil I.4 die Existenz der Garantie als Anforderung definiert und II.1 ihre Erfüllung bewertet.

Über die vier bewerteten Garantien Finalität, Liveness, Degradation Mode und Zensurresistenz erreicht I.4 die Stufe Erfüllt, weil alle vier im Zielzustand gestärkt oder gehalten sind und keine strukturelle Einschränkung die Stufe begrenzt.[356] Die State-Persistenz und die Post-Quantum-Robustheit tragen die Stufe nicht.

II.1 Neutralität und Zensurresistenz

Die Neutralität und Zensurresistenz (II.1) trug im IST-Zustand als einzige Kritische Bedingung die Stufe Bedingt erfüllt und bildete damit den schwersten Einzelbefund der Arbeit. Im Zielzustand verändert sich ihr Fundament, indem die Zensurresistenz von einer emergenten Markteigenschaft zu einem protokollseitig erzwungenen, dreischichtigen System aufsteigt. Die in 5.5 entfaltete Inklusions-Erzwingung durch FOCIL, die Relay-Elimination durch ePBS und die Pre-Inclusion-Privacy durch den Encrypted Mempool greifen komplementär

[356] SOLL-Bewertung I.4. Die vier I.4-Aspekte (Finalität, Liveness, Degradation Mode und Zensurresistenz unter Angriff) sind im Zielzustand gestärkt oder gehalten und an Ort und Stelle bewertet; die State-Persistenz und die Post-Quantum-Robustheit liegen quer zu den vier Aspekten, die erste in der Bewertung der Langfristigen Stabilität, die zweite in der Schluss-Sammlung als Material inventarisiert. FOCIL trägt PLAN/SFI Hegotá-Headliner.

ineinander. Das 1-of-N-Honesty-Modell von FOCIL trägt die formal stärkere Garantie, weil ein einziges ehrliches Committee-Mitglied die Inklusion erzwingt. Mit der Zuordnung der dreischichtigen Architektur zum Kriterium steigt die Stufe von Bedingt erfüllt auf Erfüllt mit Einschränkung, und der Sprung ist notwendig, weil er die Deckelung des zweiten Kaskadenschritts aufhebt.[357]

Die Begrenzung auf Erfüllt mit Einschränkung hat drei Gründe, die sämtlich außerhalb der Reichweite der Roadmap liegen. Die Builder-Konzentration bleibt eine operative Realität, deren strukturelle Ursachen, von den Latenzvorteilen bis zum exklusiven Order Flow, ePBS nicht adressiert, weil die Relay-Elimination die Vermittler entfernt, ohne die Ökonomie der Block-Produktion umzubauen. Ohne implementierten Protokoll-Cap bleibt die Konzentration der Liquid-Staking-Token, an deren Spitze Lido heute rund 23 Prozent des gestakten ETH hält, fortgeschrieben in den Zielzustand mit rückläufiger Tendenz, eine strukturelle Einschränkung.[358] Die geographische Node-Verteilung schließlich, mit rund 39 Prozent der Nodes in den Vereinigten Staaten, verbessert sich technisch durch die Hardware-Zugänglichkeit der Stateless Clients, ohne dass die Roadmap die nicht-technischen Ursachen der Konzentration erreicht. Die drei Einschränkungen bilden die Brücke zu Kapitel 6, das die persistenten Grenzen führt, und sie begründen die Stufe, ohne hier weiter bewertet zu werden.

Mit der Bewertung der drei Kritischen Bedingungen wechselt der Abschnitt in ein inventarisierendes Register, das die über fünf Abschnitte verteilte Post-Quantum-Substanz als Material sichtbar macht. Die Post-Quantum-Migration ist im Designzustand eine verteilte architektonische Bewegung über die drei Ebenen Consensus, Data und Execution. Auf der Consensus-Ebene liegt die hash-basierte Ablösung der BLS-Validator-Signaturen in 5.5-D, mit der Beam Chain aus 5.1-B als langfristigem Endzustand SNARK-basierter Consensus Proofs. Auf der Data-Ebene führt 5.2-D den Übergang von den kurvenbasierten KZG-Commitments zu hash-basierten Verfahren im Full-Danksharding-Endzustand. Der Migrationspfad der Execution-Ebene läuft weg von ECDSA über die Native Account Abstraction, mit den Validation Frames aus 5.3-E als primärem Opt-in-Vehikel des ECDSA-Ausstiegs. Als gemeinsame Trag-Schicht verortet 5.3-A′ die hash-basierte Aggregation, eine rekursive Proof-Aggregation, die als Compute- und Kostenproblem zu führen und nicht mit der Signatur-Aggregation im Live-

[357] SOLL-Bewertung II.1. IST-Stufe Bedingt erfüllt als einzige Kritische Bedingung, SOLL-Stufe Erfüllt mit Einschränkung. Reifegrade: ePBS PLAN/SFI Glamsterdam, FOCIL PLAN/SFI Hegotá-Headliner, Encrypted Mempool RES.

[358] Auf der Infrastrukturebene von II.1: Lido rund 23 Prozent des gestakten ETH, rückläufig vom 2023-Höchst über 32 Prozent, ohne implementierten Protokoll-Cap, geographische Node-Verteilung rund 39 Prozent Vereinigte Staaten.

Konsens zu verwechseln ist, deren Charakter ein Problem der Netzwerk-Koordination bleibt.

Der Reifegrad der verteilten Bewegung lässt sich statusbasiert inventarisieren, ohne einen Zeitpunkt zu versprechen. Deployment-fähig ist die secp256r1-Precompile (EIP-7951), kurvenbasiert und selbst nicht quantenresistent, die über FIDO2- und WebAuthn-Passkeys die Signatur-Verfahren diversifiziert und so die Infrastruktur des Migrationspfads bereitstellt. Auf gleichem Reifegrad steht der Helios-Light-Client als Verifikations-Vorstufe. Die Validation Frames (EIP-8141) stehen dagegen auf einer früheren Stufe, der Spezifikationsphase der Hegotá-Fork als Platzhalter-Commitment per Checkpoint #9, und markieren den ECDSA-Migrationspfad.[359] Die Vor-Bereitung verankert sich im Post-Quantum-Research-Team der Ethereum Foundation, das im Januar 2026 gegründet wurde und mit zweiwöchentlichen ACD Calls, ausgeschriebenen Research Prizes und Live-Testnets arbeitet. Hinzu treten die generische Precompile-Position EIP-7932 im Forschungsstatus, die Binary Trees als STARK-kompatible State-Tree-Architektur und der als Backstop signalisierte Emergency Response Plan.[360] Die Lücken bleiben gleichwohl sichtbar, denn die Full-Stack-Migration über den Consensus Layer, die Ablösung der KZG-Commitments durch STARKs und der Übergang zu Binary Trees bilden zusammen ein Generationenprojekt, dessen Beam-Chain-Timeline jenseits 2029 ohne Fork-Termin liegt. Die Wahl der Hash-Funktion ist zudem eine mehrere Ebenen zugleich betreffende Upstream-Entscheidung, und eine protokoll-weite Migrations-Sequenz bleibt unkoordiniert. Die Signatur-Größen der Post-Quantum-Verfahren, die bei ML-DSA zwischen 2,4 und 4,6 Kilobyte und bei SLH-DSA zwischen 7,9 und 49,9 Kilobyte gegen 64 Byte bei ECDSA liegen, erzeugen mit einem State-Bloat in der Größenordnung des 59-Fachen bei ML-DSA eine offene State-Frage.[361] Die im Beitrag Buterins vom 26. Februar 2026 referenzierte Metaculus-Schätzung gibt die Wahrscheinlichkeit kryptographisch relevanter Quantum Computer vor 2030 mit rund 20 Prozent an, geführt als zitierter Reifegrad-Kontext und nicht als eigene Eintrittswahrscheinlichkeits-Aussage der Arbeit.[362]

[359] PQ-Vor-Material 5.7-A. secp256r1-Precompile EIP-7951 (DEPL), Helios-Light-Client (DEPL), Frame Transactions EIP-8141 (CFI Hegotá Non-Headliner, Platzhalter-Commitment per Checkpoint #9).

[360] PQ-Vor-Material 5.7-A. Post-Quantum-Research-Team der Ethereum Foundation gegründet Januar 2026, EIP-7932 (DFI Glamsterdam, weiter im Forschungsstatus), Binary Trees (RES, signalisiert im EF Protocol Priorities Update vom 18. Februar 2026), Emergency Response Plan aus dem Vitalik-PQ-Roadmap-Post.

[361] Strawmap (Post-Quantum L1 North Star), referenziert im PQ-Vor-Material 5.7-A. Signatur-Größen ML-DSA 2,4 bis 4,6 Kilobyte und SLH-DSA 7,9 bis 49,9 Kilobyte gegen 64 Byte bei ECDSA, State-Bloat in der Größenordnung des 59-Fachen bei ML-DSA.

[362] Vitalik-PQ-Roadmap-Post vom 26. Februar 2026, referenzierte Metaculus-Schätzung. Zitierter Reifegrad-Kontext, keine Eigenprognose der Arbeit.

Als Robustheits-Material tritt der in 5.3-D entfaltete Degradation Mode hinzu. Der Inactivity Leak entzieht nicht-partizipierenden Validatoren schrittweise Stake, bis die partizipierenden eine Zwei-Drittel-Supermajorität zurückgewinnen, und er ist auf dem Mainnet erprobt und operativ. Unter einem Quantum-Angriff, der schneller käme als die Migration, griffe der Stress-Modus, sodass das Netzwerk weiter produziert, während kompromittierte Validatoren über den Leak ausscheiden, wobei die Single-Slot-Finalität den Trigger granularer und früher greifen ließe. Die Verfügbarkeit des Stress-Modus ist hier nur als vorhanden inventarisiert und geht als Material in die I.4-Robustheits-Bewertung in Kapitel 6.

Die Inventarisierung benennt die verteilte Architektur, ihren gestuften Reifegrad und den verfügbaren Degradation Mode, ohne über ihre Hinlänglichkeit zu befinden. Ob die Migration ausreicht, ob die Timeline trägt und ob die Lücken kritisch sind, entscheidet die integrierte Belastbarkeitsbewertung in Abschnitt 6.1 und nicht der vorliegende Abschnitt. Die Sammlung stellt das Material für dieses Urteil bereit.

5.7-B SOLL-Bewertung der Strukturellen und Qualitativen Kriterien

Nach den drei Kritischen Bedingungen, deren Stufe das Gesamturteil deckelt, treten die Strukturellen Bedingungen hinzu. Sie bestimmen die Tragfähigkeit des Systems über die Kritischen Bedingungen hinaus und begrenzen das Gesamturteil im dritten Kaskadenschritt, sobald zwei oder mehr von ihnen schwach stehen. Sie werden in der Reihenfolge I.1, I.3 und III.1 eingeordnet.

Die Strukturellen Bedingungen

Ethereums Unersetzbarkeit als Settlement-Layer erreicht im Zielzustand auf allen drei Anker-Indikatoren die höchste Stufe, weshalb I.1 als Erfüllt zu bewerten ist.[363] Die in 5.6 entfaltete Native-Rollup-Bindung stützt die Bewertung asymmetrisch. Sie koppelt L2-Systeme protokollseitig an Ethereum und schafft eine Verankerungstiefe, die dem System als Schelling Point der Settlement-Schicht keine technische Wechseloption mehr offenlässt.[364] Auf der Infrastrukturebene verstärkt die ebenfalls in 5.6 beschriebene Settlement-Attraktion über ERC-7683 die Bindung, weil sie Solver-Netzwerke ökonomisch dorthin zieht, wo Liquidi-

[363] Die drei Anker-Indikatoren der Funktionalen Unersetzbarkeit (DeFi-TVL-Dominanz, Stablecoin-Issuance, Developer-Ökosystem) erreichen im Zielzustand jeweils die höchste Ankerstufe oberhalb der 50-Prozent-Schwelle.

[364] Zur Mechanik der Native Rollups (Reifegrad RES) und der Settlement-Attraktion über ERC-7683 vgl. 5.6, zur Kapazitäts-Skalierung vgl. 5.2.

tät und Settlement-Sicherheit zusammenfallen. Die in 5.2 entfaltete Kapazitäts-Skalierung stützt die Verankerung zusätzlich, indem sie den Raum verbreitert, in dem sich diese Aktivität abspielt.

Eine Einschränkung bleibt benennbar, ohne die Stufe zu drücken. Die Cloud-Konzentration der Node-Infrastruktur adressiert die Roadmap nicht direkt: rund 59 Prozent der gehosteten Execution-Layer-Nodes verteilen sich auf drei Provider, davon rund 35,5 Prozent auf AWS, rund 13,8 Prozent auf Hetzner und rund 9,7 Prozent auf OVHcloud, mit seit 2022 rückläufiger Tendenz.[365] Der Befund relativiert die Tiefe der Verankerung, ändert die Stufe aber nicht. I.1 prüft die Verankerung als Schelling Point, und die Konzentration auf externe Provider hebt diese Verankerung nicht auf. Sie verlagert einen Teil der Abhängigkeit auf eine Infrastrukturschicht, die das Kriterium nicht misst, weshalb sie als qualifizierter Faktor erscheint.

Die Koordinationsfunktion erweitert sich im Zielzustand qualitativ und erfüllt I.3 in einer gegenüber dem Ausgangszustand vergrößerten Reichweite.[366] Was zuvor vor allem Settlement und Datenverfügbarkeit für L2-Netzwerke koordiniert, dehnt sich auf Execution, Verifikation und die Steuerung der MEV-Ökonomie aus, wie die Abschnitte 5.5 und 5.6 sie entfalten. Das Protokoll absorbiert dabei Funktionen, die heute externe Vertrauensannahmen erfordern. Die Relay-Koordination der Blockproduktion verlagert sich protokollseitig in ePBS, die Verifikation der L2-State-Transitions in die Native-Rollup-Bindung an Ethereums eigene Ausführung.

Die Koordinationsleistung bleibt über Netzwerkeffekte an das spezifische Ethereum-Ökosystem gebunden, sodass ein Wechsel zu einem konkurrierenden System den Verlust der aufgebauten Netzwerkeffekte bedeutete. Im Zielzustand wickeln alle Top-10-L2s ihr Settlement auf Ethereum ab, was den Indikator auf der höchsten Stufe hält, und die Native-Rollup-Implementierung erhöht die Wechselkosten strukturell, weil sie L2s die technische Option eines Settlement-Layer-Wechsels nimmt.[367] I.3 ist erfüllt, in erweiterter Reichweite, ohne eine die Stufe drückende Einschränkung.

Auf die Langfristige Stabilität antwortet der Zielzustand mit drei Entkopp-

[365] Stand des Execution-Layer-Node-Hostings: rund 59 Prozent auf drei Providern (AWS rund 35,5%, Hetzner rund 13,8%, OVHcloud rund 9,7%), seit 2022 rückläufig. Vgl. die Erhebung in Kapitel 4.

[366] Zum Hinzukommen der protokollseitigen Verifikation als viertem Koordinationsprimitiv neben Settlement, Execution und Data Availability vgl. 5.5 und 5.6. Reifegrade: ePBS PLAN/SFI (Glamsterdam), Native Rollups RES.

[367] Alle Top-10-L2s settlen im Zielzustand auf Ethereum (höchste Stufe). Die Native-Rollup-Implementierung nimmt implementierenden L2s die technische Option eines Settlement-Layer-Wechsels.

lungen, die III.1 erfüllen.[368] Die zkEVM löst die Verifikation von der Execution-Kapazität, die Stateless Clients lösen die Verifikation von der State-Größe, und Tiered State löst das permanente State-Wachstum von der Gesamtkapazität. Jede der Entkopplungen entsteht am Ort ihres Mechanismus, den die Abschnitte 5.2, 5.3 und 5.4 jeweils entfalten.

Den Befund stützt der Upgrade-Track-Record. Shanghai, Dencun, Pectra und Fusaka wurden ohne Mainnet-kritische Incidents ausgeliefert, und mit Fusaka wurde der halbjährliche Hard-Fork-Zeitplan erstmals eingehalten.[369] State-Wachstum, Client-Diversität und Upgrade-Robustheit sind im Zielzustand getragen, sodass die Stufe Erfüllt erreicht ist.

Auch III.1 trägt eine benannte Einschränkung, die die Stufe nicht drückt. Die Validator-Konzentration verändert sich strukturell nicht, und kein Roadmap-Feature adressiert sie direkt, sodass Lido voraussichtlich bei rund 23 Prozent verbleibt, die 33-Prozent-Schwelle deutlich unterschreitet und weiter zurückgeht.[370] Der Faktor ist benannt, aber nicht stufentragend. III.1 prüft die Langfristige Stabilität gegen State-Wachstum, Client-Diversität und Upgrade-Robustheit, und diese drei Eigenschaften trägt der Zielzustand, während die Stake-Verteilung eine andere Frage berührt, die das Kriterium hier nicht entscheidet.

Die Qualitativen Kriterien

Nach den Kritischen und Strukturellen Bedingungen differenzieren die sechs Qualitativen Kriterien den Grad innerhalb der erreichten Eignungskategorie, ohne das Gesamturteil nach unten zu deckeln. Die offene Generativität (II.2) liefert die erste Antwort. Der Zielzustand erweitert die generative Kapazität des Systems auf drei Ebenen, deren Mechanik die vorangegangenen Abschnitte entfaltet haben. Sie reichen von der Rechenkapazität über zkEVM und Full Danksharding über die Nutzungserfahrung via Native Account Abstraction bis zur Erzeugung neuer Layer-2-Netzwerke über Native Rollups. Die Composability-Garantie und die EVM-Stabilität bleiben erhalten, sodass bestehende Entwickler-Investitionen geschützt sind. Die Einschränkung liegt in zwei offenen Punkten, die die Stufe halten: RISC-V als alternative Ausführungslaufzeit bleibt ein ex-

[368] Die drei Entkopplungen entstehen am jeweiligen Ort ihres Mechanismus: zkEVM (aktive EF-Roadmap, 5.2), Stateless Clients über den Verkle- oder Binary-Trees-Pfad (beide RES; das Migrations-Bundle EIP-7612/7748/4762 bleibt gegenüber der Tree-Wahl invariant, 5.3), Tiered State (RES, 5.4).

[369] Shanghai, Dencun, Pectra und Fusaka wurden ohne Mainnet-kritische Incidents ausgeliefert. Mit Fusaka wurde der halbjährliche Hard-Fork-Zeitplan erstmals eingehalten. Zustandsentlastend wirken zudem History Expiry (EIP-4444, Phase 1 DEPL) und die SELFDESTRUCT-Limitation (EIP-6780, DEPL).

[370] Die Validator-Konzentration bleibt strukturell unverändert: Ohne Protokoll-Level-Staking-Cap verbleibt Lido voraussichtlich bei rund 23 Prozent und unterschreitet die 33-Prozent-Schwelle deutlich, mit rückläufiger Tendenz. Kein Roadmap-Feature adressiert die Konzentration direkt.

plorativer Forschungspfad ohne Governance-Verankerung, und der Verzicht auf EOF lässt eine Verbesserung der Developer Experience aus, die strukturell möglich gewesen wäre. Im Zielzustand steht die offene Generativität auf Erfüllt mit Einschränkung.[371]

Die unabhängige Verifizierbarkeit (II.3) erfüllt im Zielzustand alle drei Indikatoren, und die formale Spezifikationsgrundlage verbessert sich strukturell, weil die Execution Layer Specification als ausführbare Referenzimplementierung den operativen Spezifikationsstandard für neue Protokoll-Features bildet. Die eine kritische Einschränkung, die die Stufe hält, entsteht aus der zkEVM selbst: Sie verschiebt die Verifikationsaufgabe von der Re-Execution zur Prüfung kryptographischer Beweise, und die formale Korrektheit des Provers, die damit zur neuen Vertrauensgrundlage des Stacks wird, ist im Zielzustand noch nicht formal beweisbar. Ein vollständiger Prover-Circuit übersteigt in seiner Komplexität die Kapazität der gegenwärtigen formalen Methoden, sodass das Verifikationsangebot zwar protokollär verankert bleibt, an seiner kritischsten Stelle aber eine ungelöste Aufgabe trägt. Die unabhängige Verifizierbarkeit steht auf Erfüllt mit Einschränkung.[372]

Bei der niedrigschwelligen Inklusivität (II.4) senkt der Zielzustand die Teilnahmebarrieren für drei der vier Rollen. Die Nutzer profitieren von Native Account Abstraction und der Passkey-Authentifizierung über die secp256r1-Precompile, die Verifizierer von Stateless Clients, die den vollständigen State nicht mehr lokal vorhalten müssen, und die Entwickler von einem stabilen, über die EVM-Garantie geschützten Toolkit. Die Einschränkung liegt in der vierten Rolle: Die 32-ETH-Schwelle für Solo-Staking bleibt bestehen, und der Zielzustand mildert sie lediglich indirekt über die Hardware-Entlastung der Validatoren, ohne die ökonomische Barriere selbst zu senken. Auf Erfüllt mit Einschränkung steht die niedrigschwellige Inklusivität.[373]

Die adaptive Governance (III.2) ist das erste der Qualitativen Kriterien, das die volle Stufe trägt. Das Governance-Modell demonstriert anpassende Kapazität

[371] Zu den Reifegraden: die zkEVM steht auf der aktiven EF-Roadmap, Full Danksharding auf RES, Native Account Abstraction über EIP-8141 auf PLAN als CFI-Non-Headliner für Hegotá, mit der bereits aktivierten EIP-7702 (DEPL) als operativem Beleg, Native Rollups auf RES. RISC-V als VM-Alternative ist ein explorativer Forschungspfad (RES) ohne Governance-Verankerung, EOF wurde aus der Fusaka-Roadmap zurückgestellt.

[372] Die Execution Layer Specification ist eine ausführbare Referenzimplementierung der EVM-Semantik und im Zielzustand der operative Spezifikationsstandard für neue Features. Die formale Verifikation des zkEVM-Prover-Circuits steht auf RES und übersteigt die Kapazität gegenwärtiger formaler Methoden.

[373] Nutzerseitige Reifegrade: EIP-7702 (DEPL) und die secp256r1-Precompile über EIP-7951 (DEPL) für Passkeys. Die Stateless-Client-Migration über Verkle Trees steht auf PLAN. Die 32-ETH-Schwelle wird durch kein Roadmap-Feature direkt gesenkt, die Hardware-Entlastung erfolgt indirekt über zkEVM-basierte Attestation.

auf allen drei Ebenen, und der in 5.1 entfaltete strategische Pivot ist der stärkste Beleg, ein paradigmatischer Richtungswechsel innerhalb des bestehenden Modells ohne Krise, Fork oder formale Abstimmung. Weil die Eigenschaft strukturell und historisch belegt ist und nicht von einer künftigen Roadmap-Lieferung abhängt, steht die adaptive Governance auf Erfüllt.[374]

Denselben Befundtyp trägt die souveräne Portabilität (III.3), weil der Zielzustand die proprietären Lock-ins des Ausgangszustands systematisch auflöst: die Relay-Abhängigkeit über ePBS, die L2-Proof-Systeme über Native Rollups und die RPC-Konzentration über Trustless RPC. Die EVM bleibt ein bilateraler struktureller Lock-in, der die Entwickler an Ethereum und Ethereum an die EVM bindet, ohne die Stufe zu drücken, sodass die souveräne Portabilität auf Erfüllt steht.[375]

Die Hardware-Agnostik (III.4) verlangt eine Begründung. Im Zielzustand ist die architektonische Hardware-Agnostik des Protokolls vollständig, ohne ASIC-Abhängigkeit und mit ARM-Kompatibilität aller großen Clients. Die Verifikation wird durch Stateless Clients von der State-Größe entkoppelt, sodass sie bis hin zu Smartphones und Browsern auf Consumer-Hardware möglich bleibt. Die eine Einschränkung bleibt die Cloud-Konzentration, mit rund 59 Prozent der gehosteten Execution-Layer-Nodes auf drei Providern, einem seit 2022 rückläufigen Wert, den die Roadmap nicht durch ein direktes Feature adressiert. Entscheidend für die Stufe ist, dass der Zielzustand den Wert nicht verschlechtert, weil Stateless Clients die Hardware-Hürde für Home-Staking senken, ohne die ökonomischen Treiber der Cloud-Nutzung aufzuheben, sodass die Konzentration unverändert bleibt. Ein unveränderter Indikator kann nicht unter seine Ausgangsstufe absteigen, und weil die IST-Bewertung in Kapitel 4 die Hardware-Agnostik auf Erfüllt mit Einschränkung führt, hält der Zielzustand diese Stufe, statt auf Bedingt erfüllt zu fallen.[376]

Mit der Bewertung aller zwölf Kriterien im Zielzustand ist das vollständige SOLL-Profil sichtbar.

---

[374] Der strategische Pivot von einer rollup-zentrierten zu einer L1-orientierten Skalierungsstrategie (Februar 2026) ist demonstriert und gilt als eingetretenes Faktum, die übrigen Governance-Eigenschaften sind strukturell und historisch belegt. Vgl. Abschnitt 5.1.

[375] Reifegrade der Lock-in-Auflösung: ePBS auf PLAN (SFI, Glamsterdam), Native Rollups auf RES, Trustless RPC auf RES/PLAN. Die EVM bleibt ein struktureller Lock-in des Protokolls.

[376] Die IST-Bewertung der Hardware-Agnostik steht im finalisierten Kapitel 4 auf Erfüllt mit Einschränkung, die Cloud-Konzentration dort auf rund 59 Prozent der gehosteten Execution-Layer-Nodes über drei Provider (AWS 35,5 %, Hetzner 13,8 %, OVHcloud 9,7 %), rückläufig seit 2022 (Ethernodes, Anfang 2026). Weil der Zielzustand die Cloud-Konzentration weder verschlechtert noch direkt verbessert, hält das Kriterium die IST-Stufe. Den Architektur-Support (x86 und ARM) und die Stateless-Client-Verifikation behandeln die Abschnitte 5.3 und 5.7-B.

5.7-C Das SOLL-Gesamtprofil

SOLL-Profil-Karte

Stufe	Kriterien	Anzahl
Erfüllt	I.1, I.3, I.4, III.1, III.2, III.3	6
Erfüllt mit Einschränkung	I.2, II.1, II.2, II.3, II.4, III.4	6
Bedingt erfüllt	keine	0
Offen	keine	0

Tabelle 5.1 Die SOLL-Profil-Karte: die vier Bewertungsstufen mit den zugehörigen Kriterien und ihrer Anzahl.

SOLL-Profil: 6-6-0-0.

Alle sechs Qualitativen Kriterien stehen im Zielzustand auf mindestens Erfüllt mit Einschränkung, was nach der Grad-Skala aus Kapitel 2 den Grad Gut trägt.[377] Das vollständige Profil und seine Auswertung über die M3-Kaskade zum Gesamturteil trägt der folgende Abschnitt.

5.8 Gesamturteil

Die Bewertung der zwölf Kriterien im vorangegangenen Abschnitt ergibt das vollständige SOLL-Profil, das die M3-Kaskade nun zum Gesamturteil führt. Sechs Kriterien stehen im Zielzustand auf Erfüllt, die anderen sechs auf Erfüllt mit Einschränkung, und kein Kriterium fällt auf Bedingt erfüllt oder Offen. Unter den drei Kritischen Bedingungen erreichen die Minimalen tragfähigen Garantien (I.4) volles Erfüllt, während die Sicherheits- und Vertrauenslast (I.2) und die Neutralität und Zensurresistenz (II.1) auf Erfüllt mit Einschränkung stehen. Auf der strukturellen Seite tragen die Funktionale Unersetzbarkeit (I.1), die Koordinationsfunktion (I.3) und die Langfristige Stabilität (III.1) durchgehend Erfüllt, sodass das numerische Profil 6-6-0-0 lautet.[378]

Die Kaskade prüft dieses Profil in fünf aufeinanderfolgenden Schritten, deren erste drei das Gesamturteil nach unten deckeln können. Die erste Prüfung gilt der Frage, ob eine der drei Kritischen Bedingungen auf Offen steht, was das

[377] Die Grad-Skala aus Kapitel 2 definiert den Grad Gut, wenn alle sechs Qualitativen Kriterien mindestens auf Erfüllt mit Einschränkung stehen. Die IST-Bewertung in Kapitel 4 vergibt denselben Grad bei identischer Lage der Qualitativen Kriterien. Vgl. Abschnitt 2.3 sowie Kapitel 4, Gesamtsynthese.

[378] Vgl. die Profil-Karte in 5.7-C. Auf Erfüllt stehen I.1, I.3, I.4, III.1, III.2 und III.3, auf Erfüllt mit Einschränkung I.2, II.1, II.2, II.3, II.4 und III.4. Bedingt erfüllt und Offen bleiben unbesetzt.

Urteil auf Bedingt geeignet begrenzte. Keine der drei steht dort, denn I.2 und II.1 tragen Erfüllt mit Einschränkung und I.4 trägt Erfüllt. Die Deckelung auf Bedingt geeignet greift nicht.

Die zweite Prüfung fragt, ob eine Kritische Bedingung auf Bedingt erfüllt steht, was das Urteil auf Geeignet unter erheblichen Bedingungen qualifizierte. Im IST-Zustand trug die Neutralität und Zensurresistenz (II.1) als einzige Kritische Bedingung die Stufe Bedingt erfüllt und löste die Deckelung auf die mittlere Eignungskategorie aus. Im Zielzustand steigt II.1 auf Erfüllt mit Einschränkung, weil das in 5.5 entfaltete dreischichtige System die Zensurresistenz von einer emergenten Markteigenschaft zu einer protokollseitig erzwungenen Garantie hebt. Damit greift die zweite Prüfung nicht mehr, und die Deckelung des IST-Urteils fällt.

Die dritte Prüfung fragt, ob zwei oder mehr Strukturelle Bedingungen geschwächt sind. Weil I.1, I.3 und III.1 sämtlich auf Erfüllt stehen, greift auch sie nicht. Da keine der drei deckelnden Prüfungen greift, liegt das Urteil oberhalb der mittleren Kategorie: weder bei Bedingt geeignet noch bei Geeignet unter erheblichen Bedingungen. Weil I.2 und II.1 unterhalb von vollem Erfüllt verbleiben, ist das schlichte Geeignet nicht erreicht. Es bleibt Geeignet mit Bedingungen.[379]

Innerhalb der erreichten Kategorie bestimmen die sechs Qualitativen Kriterien den Grad. Nach der Grad-Skala aus Abschnitt 2.3.3 trägt das den Grad Gut, und die finalisierte IST-Bewertung in Kapitel 4 vergibt bei identischer Schwellenlage den Grad Gut, sodass der Zielzustand denselben Grad trägt.[380] Der Grad bleibt gleich, obwohl zwei Qualitative Kriterien sich verbessern: Die Adaptive Governance (III.2) und die Souveräne Portabilität (III.3) steigen von Erfüllt mit Einschränkung auf volles Erfüllt. Gut ist die höchste Stufe der Skala. Beide Verbesserungen bleiben deshalb ohne Ausdruck im Gesamturteil, weil Qualitative Kriterien allein den Grad bestimmen und dieser bereits im Ausgangszustand gesichert war. Der kategoriale Vergleich zum IST-Zustand lautet damit präzise: ein Urteils-Schritt höher bei gleichem Grad. Der Fortschritt der Roadmap liegt im Fundament der Eignung, nicht in der Feinqualität der bewerteten Eigenschaften.

Ein Befund entsteht zwischen den stufentragenden Einzelbewertungen, sam-

[379] Zur M3-Kaskade und ihren fünf Prüfungsschritten vgl. Abschnitt 2.3. Im IST-Zustand setzte die zweite Prüfung das Urteil auf die mittlere Kategorie, weil II.1 als einzige Kritische Bedingung auf Bedingt erfüllt stand (vgl. Kapitel 4, Gesamtsynthese).

[380] Die finalisierte IST-Bewertung in Kapitel 4 vergibt den Grad Gut, wenn alle sechs Qualitativen Kriterien mindestens auf Erfüllt mit Einschränkung stehen. Der Zielzustand erfüllt sie bei identischer Schwellenlage. Vgl. Kapitel 4, Gesamtsynthese.

melt sich aus ihrer Zusammenschau und gehört keiner von ihnen, weshalb die Kaskade ihn nicht selbst produziert. Die strukturellen Konzentrationen bleiben bestehen, weil kein Roadmap-Feature sie direkt aufhebt. Die Builder-Konzentration in der Block-Produktion erreicht ePBS an ihrer ökonomischen Wurzel nicht, und die Konzentration des Liquid Staking um Lido verbleibt ohne protokollären Cap. Die informelle Governance verschärft den Befund, weil ihre Notfall-Reaktion auf dokumentierten Aktionsplänen ruht und nicht auf protokollär erzwungenen Mechanismen. Zusammengenommen bilden die drei Faktoren eine Krisen-Reaktions-Lücke, die in keinem einzelnen stufentragenden Kriterium auftaucht und quer über die Neutralität (II.1), die Langfristige Stabilität (III.1) und die Adaptive Governance (III.2) liegt.[381] Die Reaktionsfähigkeit des Systems auf dringliche Konzentrations- und Krisenrisiken beruht auf sozialer Koordination, die das Protokoll nicht erzwingt, und ihre Tiefe wie ihr Gewicht für die Eignung führt Kapitel 6.

Das Gesamturteil Geeignet mit Bedingungen, Grad Gut, steht auf architektonischer Kohärenz bei abgestufter Implementierungsreife. Die kryptographische Tragfähigkeit zeigt diese Abstufung besonders deutlich. Die Post-Quantum-Migration ist architektonisch verteilt angelegt, mit der Verifikations-Schicht als Anker und der Beam Chain als langfristigem Endzustand, und diese Verteilung stützt die Tragfähigkeit der Architektur, ohne sie zu sichern.[382] Ob die Roadmap die Bedingungen belastbar einlöst, ob die Teilrealisierung trägt und ob die Lücken kritisch sind, entscheidet die integrierte Belastbarkeitsbewertung in Abschnitt 6.1, die zugleich die persistenten Grenzen führt. Der vorliegende Abschnitt trägt das Urteil, dessen Belastbarkeit Abschnitt 6.1 prüft.

[381] Die Konzentrationswerte tragen Kapitel 4 (Builder-Konzentration in der Block-Produktion) und 5.7 (Lido rund 23 Prozent des gestakten ETH, rückläufig, ohne Protokoll-Cap). Zum Emergency Response Plan als dokumentiertem statt protokollär erzwungenem Notfall-Mechanismus vgl. 5.7-A.

[382] Zur verteilten Post-Quantum-Architektur mit der Verifikations-Schicht als Anker und der Beam Chain als langfristigem Endzustand sowie zu ihrem gestuften Reifegrad vgl. die Inventarisierung in 5.7-A. Ihre Hinlänglichkeit bewertet Kapitel 6.

Kapitel 6

Delta, Grenzen und Gesamturteil

6.1 Delta IST→SOLL

Das Gesamturteil des Zielzustands steht eine Eignungskategorie über dem Befund, den Kapitel 4 für den operativen Ausgangszustand getroffen hat. Der Ausgangszustand trägt Geeignet unter erheblichen Bedingungen bei einem IST-Profil von 0-11-1-0, der Zielzustand trägt Geeignet mit Bedingungen bei einem SOLL-Profil von 6-6-0-0. Der Abstand zwischen beiden Urteilen misst, was die Roadmap an der Eignung bewegt.[383] Den Vergleich, der aus dem in 5.8 gefällten Urteil erst die Antwort auf die Leitfrage der Arbeit macht, hat die SOLL-Bewertung ausgelassen und Kapitel 6 zugewiesen. Die folgende Gegenüberstellung der zwölf Kriterien führt ihn und legt zugleich offen, woran jede Verbesserung hängt.

[383] IST-Profil 0-11-1-0 und Gesamturteil Geeignet unter erheblichen Bedingungen: Kapitel 4, Gesamtsynthese. SOLL-Profil 6-6-0-0 und Gesamturteil Geeignet mit Bedingungen: 5.7-C und 5.8. Der Grad Gut folgt in beiden Zuständen der in Kapitel 2 definierten, in Kapitel 4 angewandten Schwelle, nach der alle sechs Qualitativen Kriterien mindestens auf Erfüllt mit Einschränkung stehen.

Kriterium	IST (Kapitel 4)	SOLL (5.7)	Kaskaden-Rolle
I.1 Funktionale Unersetzbarkeit	Erfüllt mit Einschränkung	Erfüllt	Strukturell
I.2 Sicherheits- und Vertrauenslast	Erfüllt mit Einschränkung	Erfüllt mit Einschränkung	Kritisch
I.3 Koordinationsfunktion	Erfüllt mit Einschränkung	Erfüllt	Strukturell
I.4 Minimale tragfähige Garantien	Erfüllt mit Einschränkung	Erfüllt	Kritisch
II.1 Neutralität und Zensurresistenz	Bedingt erfüllt	Erfüllt mit Einschränkung	Kritisch
II.2 Offene Generativität	Erfüllt mit Einschränkung	Erfüllt mit Einschränkung	Qualitativ
II.3 Unabhängige Verifizierbarkeit	Erfüllt mit Einschränkung	Erfüllt mit Einschränkung	Qualitativ
II.4 Niedrigschwellige Inklusivität	Erfüllt mit Einschränkung	Erfüllt mit Einschränkung	Qualitativ
III.1 Langfristige Stabilität	Erfüllt mit Einschränkung	Erfüllt	Strukturell
III.2 Adaptive Governance	Erfüllt mit Einschränkung	Erfüllt	Qualitativ
III.3 Souveräne Portabilität	Erfüllt mit Einschränkung	Erfüllt	Qualitativ
III.4 Hardware-Agnostik	Erfüllt mit Einschränkung	Erfüllt mit Einschränkung	Qualitativ

Tabelle 6.1 Die zwölf Kriterien im Übergang vom IST der Kapitel 4 zum SOLL des Abschnitts 5.7, mit ihrer Rolle in der Kaskade.

IST-Profil 0-11-1-0, SOLL-Profil 6-6-0-0.

Sieben der zwölf Kriterien verbessern sich, fünf bleiben konstant, und vier Bewegungen tragen die Hebung des Gesamturteils. Die sieben Verbesserungen umfassen die Funktionale Unersetzbarkeit (I.1), die Koordinationsfunktion (I.3), die Minimalen tragfähigen Garantien (I.4), die Neutralität und Zensurresistenz (II.1), die Langfristige Stabilität (III.1), die Adaptive Governance (III.2) und die Souveräne Portabilität (III.3). Von ihnen verlässt allein die Neutralität und Zensurresistenz (II.1) die Zone des Bedingt erfüllt und steigt auf Erfüllt mit Einschränkung. Die übrigen sechs bewegen sich von Erfüllt mit Einschränkung auf Erfüllt. Drei von ihnen, die Funktionale Unersetzbarkeit (I.1), die Koordinationsfunktion (I.3) und die Langfristige Stabilität (III.1), sind Strukturelle Bedingungen und lösen mit diesem Aufstieg die Deckelung des dritten Kaskadenschritts. Der Sprung von II.1 hebt die Deckelung des zweiten Kaskadenschritts, der Aufstieg von I.1, I.3 und III.1 die des dritten. Erst beide zusammen führen das Gesamturteil eine Kategorie höher. Die drei übrigen Bewegungen heben weder die Kategorie noch den schwellenbasierten Grad, der bei Gut schon im Ausgangszustand gesichert war. Wie in 5.8 festgehalten: ein Urteils-Schritt höher bei gleichem Grad, getragen von vier Bewegungen.

Der Wechsel des Fundaments

Die tragende Bewegung gewinnt ihre Substanz aus dem Wechsel des Fundaments, auf dem die Zensurresistenz beruht. Im Ausgangszustand war sie eine emergente Markteigenschaft, deren OFAC-konforme Block-Produktion von 79 Prozent im November 2022 auf rund 15 Prozent zurückging, marktgetrieben und ohne protokolläre Erzwingung. Die Bewertung führte sie deshalb als reversibel und das Kriterium als Bedingt erfüllt. Im Zielzustand erzwingt das in 5.5 entfaltete dreischichtige System aus FOCIL, ePBS und Encrypted Mempool die Inklusion protokollseitig. Die Garantie wird so von einer Marktlage zu einer durch das 1-of-N-Honesty-Modell getragenen Eigenschaft. Die Stufe steigt auf Erfüllt mit Einschränkung und bleibt unterhalb von Erfüllt, weil die Relay-Elimination durch ePBS die Vermittler der Block-Produktion entfernt, ohne deren ökonomische Konzentration zu beheben. Die protokollseitige Erzwingung verändert die Garantie und lässt die strukturelle Ursache hinter ihr unberührt.

Neben der tragenden Bewegung beziffern die übrigen Delta-Zeilen, wie weit der Zielzustand das Fundament verschiebt, und die schärfste von ihnen trägt die Finalität unter den Minimalen tragfähigen Garantien (I.4). Der Ausgangszustand finalisiert über Casper-FFG in 12,8 Minuten, der Zielzustand bindet die endgültige Finalität der Layer 1 über die Drei-Slot-Finalität auf rund 36 Sekunden und verkürzt sie um etwa den Faktor 21. Ein nach Reifegrad gestaffelter Stack aus Based Preconfirmations, der Confirmation Rule und der Drei-Slot-Finalität selbst trägt den SOLL-Wert.[384] Die Single Slot Finalität bleibt als Konsens-Endzustand jenseits 2029 ohne Fork-Termin nennbar, ohne den nahen SOLL-Wert zu verschieben. Die drei strukturellen Verbesserungen folgen demselben Muster, weil jede eine Abhängigkeit auflöst, die der Ausgangszustand noch trug. Die Funktionale Unersetzbarkeit (I.1) steigt auf Erfüllt, weil die Native-Rollup-Bindung die L2-Schicht protokollseitig an Ethereums Ausführung koppelt. Die Koordinationsfunktion (I.3) erweitert ihre Reichweite von Settlement, Execution und Datenverfügbarkeit auf die protokollseitige Verifikation. Die Langfristige Stabilität (III.1) entkoppelt das State-Wachstum, die Validierungskosten und die Verifikationslast von der Gesamtkapazität.[385]

Den Verbesserungen stehen die fünf konstanten Kriterien gegenüber, die

[384] IST-Finalität 12,8 Minuten über Casper-FFG: Kapitel 4. SOLL-Finalitäts-Stack aus Based Preconfirmations (rund 2 Sekunden, DEPL), Confirmation Rule (rund 13 Sekunden, PLAN) und Drei-Slot-Finalität (rund 36 Sekunden, RES): 5.7-A. Die Single Slot Finalität bleibt Konsens-Endzustand jenseits 2029 ohne Fork-Termin und bestimmt den nahen SOLL-Wert nicht.

[385] Zu den drei strukturellen Hebungen vgl. 5.7-A und 5.7-B: Native-Rollup-Bindung und Settlement-Attraktion über ERC-7683 (I.1), Erweiterung der Koordination auf Execution und Verifikation (I.3), drei Entkopplungen über zkEVM, Stateless Clients und Tiered State (III.1).

auf Erfüllt mit Einschränkung bleiben, weil die Roadmap ihre tragenden Einschränkungen weder aufhebt noch verschärft. Die Sicherheits- und Vertrauenslast (I.2) trägt weiterhin zwei nicht protokollseitig erreichbare Restrisiken, die zkEVM-Proving-Annahme und die Access-Schicht aus Wallets, Frontends und DNS, über die der Großteil der Nutzer interagiert. Die offene Generativität (II.2), die unabhängige Verifizierbarkeit (II.3) und die niedrigschwellige Inklusivität (II.4) halten ihre Stufe, weil der Zielzustand sie spürbar stärkt, ohne ihre jeweilige Kerneinschränkung zu lösen. Die Kerneinschränkungen reichen von der ungelösten Prover-Formalisierung bis zur 32-ETH-Schwelle des Solo-Stakings. Bei der Hardware-Agnostik (III.4) folgt die Konstanz einer eigenen Logik, weil die Cloud-Konzentration mit rund 59 Prozent der gehosteten Execution-Layer-Nodes auf drei Providern vom Zielzustand weder verbessert noch verschlechtert wird. Der in 5.7-B begründete Grundsatz (ein unveränderter Indikator sinkt nicht unter seine Ausgangsstufe) hält die Hardware-Agnostik auf Erfüllt mit Einschränkung.[386] Die fünf Konstanten sichern den Grad, indem keine von ihnen unter das im Ausgangszustand erreichte Niveau zurückfällt.

Woran das SOLL-Urteil hängt

Mit dem vollständigen Delta tritt die Frage hervor, woran das SOLL-Urteil hängt. Das SOLL-Urteil beruht auf der Annahme, dass die Roadmap liefert, und genau diese Annahme bildet die größte Angriffsfläche der Bewertung. Die integrierte Belastbarkeitsbewertung beantwortet den Einwand mit einer Aussage über den heutigen Reifegrad jeder tragenden Komponente. Das Urteil über die Neutralität und Zensurresistenz (II.1) beruht auf FOCIL und ePBS, die beide den Planungs-Status tragen, und es ist damit das am wenigsten gesicherte der drei Kritischen Bedingungen. Das Urteil über die Minimalen tragfähigen Garantien (I.4) setzt in seiner Finalitäts-Schicht teils bereits deployte Based Preconfirmations und die in Client-Implementierung befindliche Confirmation Rule voraus, und da mit den Based Preconfirmations die L2-Bestätigung bereits im Sekundenbereich liegt, während die L1-Bestätigung an der Confirmation Rule hängt, hält es auch in konservativer Lesart. Der Reifegrad sortiert die Verbesserungen, ohne ihr Eintreten zu datieren.

Die größte konzentrierte Abhängigkeit der Roadmap liegt in der zkEVM, die auf der aktiven EF-Roadmap zwischen ungesicherter Forschung und Planungs-

[386] Cloud-Konzentration im Ausgangszustand rund 59 Prozent der gehosteten Execution-Layer-Nodes auf drei Providern (AWS rund 35,5 Prozent, Hetzner rund 13,8 Prozent, OVHcloud rund 9,7 Prozent), seit 2022 rückläufig: Kapitel 4. Zur Nicht-Verschlechterungs-Logik der Hardware-Agnostik im Zielzustand vgl. 5.7-B.

Verankerung steht und fünf Kriterien zugleich trägt. Sie senkt die Validator-Vertrauenslast (I.2), trägt mit der protokollseitigen Verifikation ein viertes Koordinationsprimitiv neben Settlement, Execution und Datenverfügbarkeit (I.3), verstärkt den Ausführungsdeterminismus der Mindestgarantien (I.4), entkoppelt die Validierungskosten von der Execution-Kapazität (III.1) und entlastet die Validator-Hardware (III.4). Drei der fünf Kriterien sind Verbesserungen, die ohne die zkEVM nicht auf Erfüllt kämen: die Koordinationsfunktion (I.3), deren erweiterte Reichweite zusätzlich auf ePBS und der Native-Rollup-Bindung beruht, die Mindestgarantien (I.4) und die Langfristige Stabilität (III.1). Die beiden anderen, die Sicherheits- und Vertrauenslast (I.2) und die Hardware-Agnostik (III.4), bleiben Konstanten, deren Stufe die zkEVM auf Erfüllt mit Einschränkung mitträgt. Eine verzögerte oder ausbleibende zkEVM schwächte deshalb die Belastbarkeit der drei Hebungen, ohne bei den beiden Konstanten eine Verbesserung zu gefährden, weil dort keine Hebung auf dem Spiel steht. Kein anderes Einzelfeature bündelt eine vergleichbare Querschnittswirkung, weshalb die konzentrierte Abhängigkeit der präziseste technische Ausdruck des größten Implementierungsrisikos ist.[387]

Die Reifegrad-Logik greift über die zkEVM hinaus und sortiert die sieben Verbesserungen nach der Reife ihrer schwächsten tragenden Komponente, wobei die Spanne weit auseinanderläuft. Am robustesten steht die Adaptive Governance (III.2), deren Fundament ein rein demonstrierter Prozess ist, getragen vom strategischen L1-Pivot des Februars 2026 und von einer Hard-Fork-Kadenz ohne Kettenspaltung. Die Adaptive Governance fällt selbst im pessimistischsten Teillieferungs-Szenario nicht zurück. Am schwächsten steht die Langfristige Stabilität (III.1), deren zentrales Element, das Tiered State System, auf ungesicherter Forschung ohne eigenes EIP beruht und sie zur taxonomisch fraglichsten Verbesserung des Deltas macht. Zwischen den Polen liegen die tragenden Komponenten mittlerer Reife, ePBS mit seiner Planungs-Verankerung ohne garantierten Fork-Slot und die Native Account Abstraction, die inkrementell auf der bereits deployten EIP-7702 aufsetzt.[388] Näher am schwachen Pol liegen die Funktionale Unersetzbarkeit (I.1) und die Koordinationsfunktion (I.3), deren Hebung an den Native Rollups (EIP-8079) hängt. Diese stehen als Draft-EIP im Forschungsstatus schwächer verankert als die Planungsstufe von ePBS, aber stärker als das

[387] Zur Querschnittswirkung der zkEVM über I.2, I.3, I.4, III.1 und III.4 vgl. die jeweiligen SOLL-Bewertungen in 5.7-A und 5.7-B. Reifegrad: aktive EF-Roadmap zwischen ungesicherter Forschung und Planungs-Verankerung.

[388] Zum strategischen L1-Pivot (Februar 2026) als demonstriertem Faktum vgl. 5.1 und 5.7-B, zum Tiered State System auf ungesicherter Forschung ohne eigenes EIP vgl. 5.4 und 5.7-A, zu ePBS (Planungs-Verankerung, Glamsterdam) und Native Account Abstraction (aufsetzend auf der deployten EIP-7702) vgl. 5.5 und 5.3.

Tiered State System ohne eigenes EIP. Die Verteilung der Reife und die Verteilung der Urteilslast laufen gegeneinander. Die Adaptive Governance, die robusteste der sieben Verbesserungen, trägt das Gesamturteil nicht, weil sie als Qualitatives Kriterium allein den Grad berührt, der schon im Ausgangszustand gesichert war. Urteilstragend sind neben der Neutralität und Zensurresistenz (II.1) gerade jene Bewegungen, die am schwachen Pol liegen: die Funktionale Unersetzbarkeit (I.1), die Koordinationsfunktion (I.3) und die Langfristige Stabilität (III.1). Von den dreien genügen zwei, weil der dritte Kaskadenschritt erst bei zwei schwachen Ausprägungen unter die erreichte Kategorie deckelt. Das SOLL-Urteil ruht damit auf einer unersetzbaren Bewegung und auf zwei von drei weiteren, die an Forschungslinien ohne finalisierte Spezifikation hängen, und es ist von unfertiger Arbeit abhängiger, als die Reifesortierung für sich genommen erkennen lässt. Was die Roadmap strukturell nicht löst, verschiebt sich an den folgenden Abschnitt.

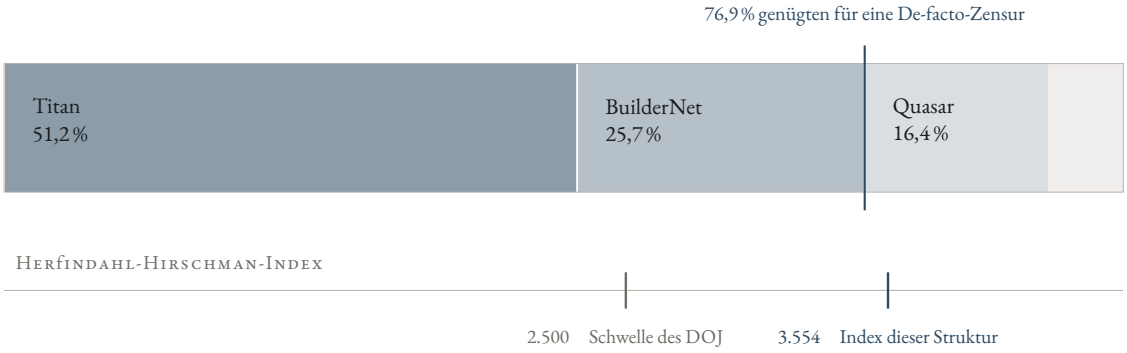
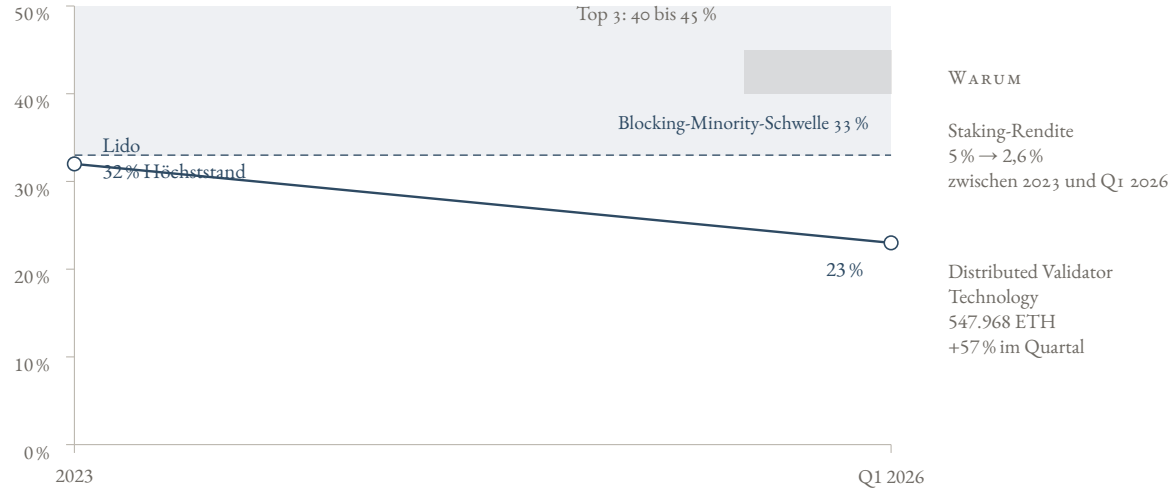


Abbildung 6.1 Die Konzentration der Block-Produktion. Gemessen am Anteil der drei Builder und am Herfindahl-Hirschman-Index.



Die Konzentration sinkt, und gerade das trägt den Befund: Kein einzelner Anbieter erreicht die Schwelle, die Top-3-Summe überschreitet sie. Der Rückgang ist ökonomisch verursacht, nicht protokollär gesichert. Eine formale Selbstbeschränkung auf 22 Prozent lehnte die Lido DAO 2022 ab.

Abbildung 6.2 Die Staking-Konzentration im Rückgang. Gegen die Blocking-Minority-Schwelle aufgetragen.

6.2 Persistente Grenzen: Die Krisen-Reaktions-Lücke

Was die Roadmap strukturell nicht löst, sammelt sich an drei Stellen, die ihre volle Lieferung überstehen, weil kein Feature ihre strukturelle Ursache behebt. An der Spitze der Block-Produktion bleibt ein einzelner Builder, im Liquid Staking ein einzelnes Protokoll, in der Notfall-Reaktion ein dokumentierter Plan ohne erzwingenden Mechanismus. Der Zielzustand reagiert auf dringliche Konzentrations- und Krisenlagen über soziale Koordination und nicht über protokollär erzwungene Mechanismen. Diese Lücke ist kein Versäumnis der Bewertung, sondern ihr verankerter Befund. Kein Feature der geprüften Roadmap führt einen solchen Mechanismus ein, und das Risiko liegt quer über drei Kriterien.

Die Block-Produktion trägt die schärfste der drei Konzentrationen, und sie sitzt am kritischsten Pfad des Systems. Titan baut 51,2 Prozent der Blöcke, BuilderNet 25,7 und Quasar 16,4, sodass drei Builder-Adressen rund 93 Prozent der Produktion kontrollieren. Der Herfindahl-Hirschman-Index dieser Struktur liegt bei 3.554 und überschreitet die Schwelle des US-Justizministeriums (DOJ) für hochkonzentrierte Märkte von 2.500 deutlich. Koordinierten Titan und BuilderNet ihre 76,9 Prozent, reichte das für eine De-facto-Zensur des Großteils der MEV-Boost-Blöcke. Die Ursache der Konzentration ist ökonomisch, weil mehr privater Order Flow profitablere Blöcke und höhere Proposer-Gebote erlaubt und die Marktposition des effizientesten Builders sich selbst verstärkt. Genau hier setzt ePBS nicht an (vgl. 5.7-A zur Relay-Elimination). Die Latenzvorteile und der exklusive Order Flow bleiben als strukturelle Treiber bestehen. Die Gegenmaßnahme liegt in BuilderNet, das die Konzentration durch eine kollaborative Multi-Operator-Architektur durchbrechen soll. Das lokale Bauen steht jedem Proposer offen, allerdings mit 2,66- bis 5,57-fach geringerem Ertrag. Der Schutz ist real, doch er besteht aus Marktanreizen und nicht aus Protokollgarantien, und die Erfahrung des OFAC-Höchststands von 79 Prozent zeigt, dass regulatorischer Druck ökonomische Anreize übersteuern kann. Für die Reaktionsfähigkeit bedeutet das eine Abwehr, die hält, solange der Markt sie trägt, und keinen Mechanismus, der die Konzentration im Krisenfall protokollär auflöste.[389]

[389] Builder-Marktanteile (Titan 51,2 Prozent, BuilderNet 25,7 Prozent, Quasar 16,4 Prozent), Herfindahl-Hirschman-Index 3.554, DOJ-Schwelle 2.500 und OFAC-Peak 79 Prozent: Kapitel 4 (relayscan.io, 27. März

Im Liquid Staking wiederholt sich das Muster mit umgekehrtem Vorzeichen, weil die Konzentration hier zurückgeht und gerade ihr Rückgang den Befund trägt. Lido hält rund 23 Prozent des gestakten ETH, rückläufig vom Höchststand rund 32 Prozent des Jahres 2023 und deutlich unter der Blocking-Minority-Schwelle von 33 Prozent. Die kumulierte Top-3-Konzentration liegt bei 40 bis 45 Prozent und überschreitet die 33-Prozent-Blocking-Minority-Schwelle allein als koordinierte Summe, während kein einzelner Anbieter sie erreicht. Kein Feature der Roadmap führt einen Protokoll-Cap ein, sodass die Konzentration strukturell bleibt, auch wo sie sinkt. Die naheliegendste Gegenmaßnahme, eine formale Selbstbeschränkung auf 22 Prozent, lehnte die Lido DAO 2022 per Abstimmung ab, womit der Cap sozial verworfen und nicht protokollär gesetzt wurde. An seine Stelle trat Distributed Validator Technology mit 547.968 ETH und einem Quartalszuwachs von 57 Prozent. Die verteilte Validierung verteilt den Operator-Betrieb und reduziert den Single Point of Failure im Validator-Set. Der Rückgang selbst entstammt der sinkenden Rendite von rund 5 auf 2,6 Prozent zwischen 2023 und dem ersten Quartal 2026, der Konkurrenz jüngerer Protokolle und dem öffentlichen Community-Druck, einer markt- und sozialgetriebenen Bewegung ohne protokollären Mechanismus. Für die Reaktionsfähigkeit folgt daraus, dass selbst die günstige Entwicklung der Konzentration auf Kräften beruht, die das Protokoll weder erzeugt noch im Krisenfall verlässlich abrufen könnte.[390]

Die informelle Governance verschärft den Befund (vgl. 5.8): ihre Notfall-Reaktion beruht auf dokumentierten Plänen, nicht auf erzwungenen Mechanismen. Die Bilanz ist stark. Sie reicht von der sozialen Intervention des DAO-Forks und den beiden Notfall-Hard-Forks 2016 gegen die im September begonnene Geth-DoS-Serie bis zu vier Post-Merge-Upgrades ohne Kettenspaltung. Die Grenze liegt in der fehlenden Pausetaste, weil bei einem Zero-Day-Konsens-Bug niemand das Netzwerk anhalten kann. Die einzige Antwort ist ein Notfall-Hard-Fork, der die Koordination aller Client-Teams verlangt und Wochen dauern kann. Für ein System, das über 100 Milliarden US-Dollar sichert, ist eine solche Reaktionszeit eine Einschränkung. Der als Backstop signalisierte Emergency Response Plan bleibt ein dokumentierter Aktionsplan und kein protokollär

2026). Zum Ertragsnachteil des lokalen Bauens (2,66- bis 5,57-fach), zur Relay-Elimination durch ePBS und zu BuilderNet als kollaborativer Gegenmaßnahme vgl. 5.5.

[390] Lido-Anteil (rund 23 Prozent, rückläufig vom Höchststand rund 32 Prozent des Jahres 2023), kumulierte Top-3-Konzentration (40 bis 45 Prozent) und die 33-Prozent-Blocking-Minority-Schwelle: Kapitel 4. Zur 2022 abgelehnten Lido-Selbstbeschränkung, zu Distributed Validator Technology (547.968 ETH, plus 57 Prozent im Quartal) und zur Renditeentwicklung (von 5 auf 2,6 Prozent zwischen 2023 und dem ersten Quartal 2026) vgl. 5.5.

erzwungener Mechanismus. Die Gegenprobe lieferte der Prysm-Bug im Dezember 2025, der keinen Notfall-Fork erforderte, weil die Client-Diversität ihn absorbierte und die beste Reaktion die war, die nicht gebraucht wurde. Doch diese Diversität ist selbst Ergebnis aktiver Community-Arbeit und kein automatischer Gleichgewichtszustand, sodass auch die erfolgreiche Absorption auf sozialer Koordination beruht. Die stärkste Sicherung des Systems liegt dort, wo eine Reaktion sich erübrigt.[391]

Ein Befund quer über drei Kriterien

Die drei Faktoren bleiben einzeln unterhalb der Schwelle, an der ein stufentragendes Kriterium die Stufe wechselt, und treten erst in ihrer Zusammenschau als ein einziger Befund hervor. Der gemeinsame Befund liegt quer über die Neutralität (II.1), die Langfristige Stabilität (III.1) und die Adaptive Governance (III.2), ohne in einem der drei den Ausschlag zu geben.[392] Jeder Faktor trägt eine reale Gegenmaßnahme, BuilderNet und das lokale Bauen, den Rückgang Lidos samt verteilter Validierung, die Fork-Bilanz samt Client-Diversität, doch jede dieser Gegenmaßnahmen ist selbst markt- oder sozialgetrieben. Die Einordnung bestätigt den Befund, weil das System selbst dort, wo es erfolgreich reagiert, sozial reagiert und keinen erzwingenden Mechanismus ansetzt. Die Reaktionsfähigkeit beruht damit auf sozialer Koordination, nicht auf protokollärer Erzwingung.

6.3 Grenzen des Bewertungsrahmens: Was kein Kriterium misst

Die Krisen-Reaktions-Lücke des vorigen Abschnitts ist eine Grenze, die der Bewertungsrahmen noch erfasst, weil sie quer über drei seiner Kriterien liegt und als deren gemeinsamer Befund eintritt. Eine zweite Grenze betrifft die Reichweite des Instruments und nicht das System, weil vier Eigenschaften Ethereums außerhalb dessen liegen, worauf überhaupt eines der zwölf Kriterien zielt. Das Urteil über die Eignung als Infrastruktur hat sie nicht schwach bewertet, sondern gar nicht adressiert, und über das, was kein Kriterium misst, kann es nichts aussagen.

---

[391] DAO-Fork 2016, vier Post-Merge-Upgrades ohne Kettenspaltung, die Emergency-Hard-Forks vom Oktober und November 2016 gegen die Geth-DoS-Serie und die Absorption des Prysm-Bugs vom Dezember 2025 durch Client-Diversität: Kapitel 4.

[392] Zu den SOLL-Bewertungen der drei berührten Kriterien, der Neutralität (II.1), der Langfristigen Stabilität (III.1) und der Adaptiven Governance (III.2), über die der gemeinsame Befund quer liegt, ohne eine einzelne Stufe zu kippen, vgl. 5.7.

Vier Eigenschaften außerhalb des Rasters

Permissionless Composability erscheint im Bewertungsrahmen, doch nur in einer Verengung. Das zweite Kriterium der zweiten Dimension (II.2) prüft die atomare Composability als binären Indikator, ob Smart Contracts innerhalb einer Transaktion miteinander interagieren können. Das Kriterium ergänzt den Indikator um die erlaubnisfreie Deployment-Möglichkeit und das offene Tooling. Außerhalb der Messung liegt die Composability als kombinatorische Systemeigenschaft, das exponentielle und erlaubnisfreie Zusammenspiel beliebig vieler Contracts zu Konstruktionen, die niemand vorhergesehen hat. In den sogenannten Money Legos der DeFi-Protokolle nimmt das Zusammenspiel Gestalt an. Das Kriterium erfasst, ob Contracts interagieren können, und nicht die generative Mächtigkeit ihrer offenen Kombinierbarkeit als eigene Qualität. Über diese Mächtigkeit macht das Urteil keine Aussage, weil das Kriterium sie auf eine Ja-Nein-Frage zurückführt, die ihr Bestehen voraussetzt, ohne ihre Reichweite zu messen.

Die kryptographische Systemzustandsverifikation steht dem Bewertungsrahmen näher und bleibt ihm doch entzogen. Das dritte Kriterium der zweiten Dimension (II.3) prüft, ob Verifikation überhaupt möglich ist. Das Kriterium liest das aus formalen Verifikationswerkzeugen, einer formalen EVM-Spezifikation und der Verbreitung von Audits, als Angebotsseite zur Vertrauenslast (I.2). Jenseits der bloßen Möglichkeit liegt die beweisgestützte Form der Verifikation, in der das System seinen eigenen Gesamtzustand mathematisch beweist, über zkEVM und Stateless Clients, statt ihn über institutionelles Vertrauen abzusichern. Das Kriterium misst, ob ein Contract sich prüfen lässt, und nicht, dass das System den kryptographischen Beweis seiner Korrektheit in sich trägt. Über die Verschiebung von institutionellem zu mathematischem Vertrauen sagt das Urteil nichts, weil das Kriterium die Möglichkeit der Verifikation erfasst und nicht den Grund, auf dem sie beruht.

Die dezentrale Selbstentwicklungsfähigkeit findet im Bewertungsrahmen ein Kriterium, das an ihr vorbeigreift. Das zweite Kriterium der dritten Dimension (III.2) prüft, ob die Governance adaptiv ist, ob das System sich weiterentwickeln und auf neue Anforderungen reagieren kann. Außerhalb der Adaptivität liegt die Selbstentwicklung ohne Zentrum, die Weiterentwicklung über Rough Consensus ohne eine Instanz, die Änderungen anordnen könnte. Jede Änderung muss freiwillig von einer Mehrheit der Node-Betreiber übernommen werden. Kapitel 2 nennt dieses Modell selbst einen Extremfall der Mayntz-Spannung zwischen Steuerung und Selbstorganisation, weil das System sich entwickelt, ohne

dass eine zentrale Stelle es lenkt. Das Kriterium erfasst, ob adaptive Governance vorliegt, und nicht die zentrumslose Selbstentwicklung, sodass das Urteil das Fehlen einer Steuerungsinstanz nicht in den Blick bekommt.

Privacy fällt aus dem Bewertungsrahmen heraus, und im Unterschied zu den drei vorigen Grenzen verengt kein Kriterium sie, weil überhaupt keines auf sie zielt. Keine der drei Dimensionen, weder die Strukturelle Fundierung noch die Qualitative Tragfähigkeit noch die Resilienz und Souveränität, enthält eine Frage nach Vertraulichkeit. Bei den ersten drei Grenzen verengt ein Kriterium die Eigenschaft auf einen Indikator, hier fehlt der Messpunkt vollständig. Die Lücke besagt, es gebe gar kein Kriterium. Außerhalb des Bewertungsrahmens liegt die Vertraulichkeit als Protokolleigenschaft, in die Architektur eingebaut über Encrypted Mempool und Pre-Inclusion-Privacy. Privacy ist die einzige der vier Grenzen, die in der geprüften Roadmap ein Korrelat besitzt, verankert im Lean-Ethereum-Programm (5.1-B und 5.1-C). Über eine real angelegte Eigenschaft des Zielzustands verliert das Urteil dennoch kein Wort, weil das Instrument für sie keinen Messpunkt vorsieht.

Die vier Eigenschaften sind kein verstreuter Rest, den die Kriterien zufällig nicht trafen, denn sie teilen eine gemeinsame Lage, jeweils außerhalb dessen zu liegen, worauf die Bewertung überhaupt zielt. Jede von ihnen liegt dort, wo das System eine Eigenschaft trägt und das Instrument keine Frage stellt. Dass es vier sind und kein Einzelfall, verrät ein Muster, dessen Deutung über die Reichweite dieser Bewertung hinausweist und die Kapitel 7 aufnimmt.

6.4 Synthese und Beantwortung der Forschungsfrage

Ethereum trägt heute als Settlement- und Datenverfügbarkeits-Schicht ein Kapital in der Größenordnung von 100 Milliarden US-Dollar, das über 60 Prozent des gesamten On-Chain-gesicherten DeFi-Kapitals ausmacht. Auf derselben Infrastruktur werden Stablecoins im Wert von etwa 166 Milliarden US-Dollar emittiert, mehr als die Hälfte des globalen Stablecoin-Marktes, und rund 65 Prozent aller neuen Smart Contracts entstehen auf den Layer-2-Systemen, deren Settlement und Datenverfügbarkeit die Basisschicht trägt. Das System bindet über 31.000 aktive Entwickler und damit mehr als 70 Prozent aller Blockchain-Entwickler weltweit. Das ist die konkrete Substanz, um die es in der Bewertung geht, bevor die Frage nach ihrer Eignung beantwortet werden kann. Erfüllt diese Architektur die Anforderungen, die an eine fundamentale digitale Infrastruktur zu stellen sind? Die Antwort lautet ja, in beiden untersuchten Zuständen, aber in beiden nur bedingt.

Fast alle Anforderungen erfüllt das System schon heute, jede mit Abstrichen, und die eine, die es am deutlichsten nach unten zieht, ist die Zensurresistenz auf der Ebene der Blockproduktion. Gegenwärtig laufen etwa 15 Prozent der Blöcke über Relays, die Transaktionen sanktionierter Adressen ausschließen, während Titan als größter Builder offen darauf verzichtet. Im November 2022 lag der Anteil bei 79 Prozent, was bedeutete, dass eine staatliche Sanktionsliste faktisch kontrollierte, welche Transaktionen ein erlaubnisfreies System verarbeitete. Dieser marktgetriebene Rückgang vollzog sich ohne jeden Eingriff in das Protokoll, allein weil nicht-zensierende Builder profitabler arbeiten und der Markt sich zu ihnen verschoben hat. Das ist die erhebliche Bedingung in einem Bild: Die Zensurresistenz funktioniert, doch sie beruht auf der Marktstruktur, und eine Marktstruktur kann sich umkehren.

Genau an dieser Bedingung setzt die Roadmap an, und zwei Entwürfe würden sie protokollseitig auflösen. FOCIL, ein Validator-Komitee-basiertes Inclusion-List-System, würde die Aufnahme jeder benannten Transaktion protokollseitig erzwingen. ePBS, die protokollnative Verankerung der Proposer-Builder-Separation, würde die Relays als Off-Chain-Vermittler entfernen, über die das OFAC-Filtern heute überhaupt erst stattfindet. Beide tragen den Status PLAN, sind entworfen, aber nicht geliefert. Darin liegt der eigentliche Wandel, denn die Art der Bedingung selbst verschiebt sich: Heute hängt die Eignung daran, wie sich der Builder-Markt verhält, nach voller Umsetzung hinge sie daran, ob die geplanten Mechanismen halten, was ihr Entwurf vorsieht. Die Roadmap tauscht damit eine Marktabhängigkeit gegen eine Umsetzungsabhängigkeit, und

die Bedingung wird dadurch nicht kleiner, sie wird von anderer Art.

Die Bedingtheit lässt sich nicht ablösen

Selbst die vollständige Umsetzung der Roadmap löst die Bedingtheit nicht auf, und ein einzelner fehlender Mechanismus macht das greifbar: Ethereum besitzt keine Pausetaste. Wie in 6.2 gezeigt, kann bei einem kritischen Bug niemand das Netzwerk anhalten. Die einzige Antwort bleibt ein aufwendiger Notfall-Hard-Fork. Die fehlende Pausetaste ist kein Feature, das eine spätere Roadmap nachreicht, sie ist die Kehrseite der Zentrumslosigkeit selbst. Wer die Bedingtheit auflösen wollte, müsste eine Instanz einführen, die im Krisenfall eingreift, anhält oder haftet, und gäbe genau die Eigenschaft auf, die Ethereum zu dem macht, was die Arbeit bewertet hat. Solange das System ohne Zentrum bleibt, bleibt seine Reaktion auf akute Krisen an soziale Koordination gebunden. Die Bedingtheit ist daher keine Unfertigkeit, die eine kommende Roadmap behebt, sondern eine Folge der Architekturentscheidung gegen ein Zentrum.

Ein Vorbehalt zum Instrument

Ein Vorbehalt gehört zum Urteil, und er betrifft das Instrument, nicht den Gegenstand. Das Bewertungsraster ist regelbasiert aufgebaut und nicht aufsummierend, sodass kleine Einschränkungen unterhalb seiner Schwellen nicht ins Gesamturteil durchschlagen. Zwei Systeme von sehr verschiedener Substanz können deshalb das gleiche Urteil tragen, und der Ausgangszustand und der Zielzustand zeigen das aneinander: in der Substanz weit auseinander, im formalen Urteil nur einen Schritt. Wer allein das Urteil liest, übersieht, wie viel Substanz zwischen den beiden Zuständen liegt. Das ist keine Schwäche des Urteils, es ist eine Eigenschaft des Instruments, die der Leser mitführen muss.

Das Urteil steht damit fest: Ethereum ist als fundamentale digitale Infrastruktur geeignet, heute unter erheblichen, nach voller Umsetzung der Roadmap mit Bedingungen, in keinem der beiden Zustände unbedingt. Was die bedingte Eignung über das Bewertungsergebnis hinaus bedeutet, für die Akteure, die auf der Infrastruktur aufbauen, ihr vertrauen oder sie regulieren, nimmt Kapitel 7 auf. Das letzte Wort behält das Urteil, nicht der Vorbehalt.

Kapitel 7

Implikationen

Nach dem Urteil

Die Forschungsfrage ist beantwortet, Ethereum eignet sich als fundamentale digitale Infrastruktur, sowohl am Stichtag vom März 2026, den ich als IST-Zustand benannt habe, als auch im Zustand unter vollständiger Umsetzung der Roadmap (dem SOLL-Zustand). Unter einem genaueren Kriterienvergleich zwischen den beiden Zuständen erfüllt der unter der Roadmap, wie zu erwarten, die gestellten Bedingungen vollständiger, bleibt aber ebenso an Bedingungen gebunden. Das ist das Ergebnis der Arbeit, die abgeschlossen ist und nicht mehr Gegenstand von Kapitel 7 ist.

Hier wird nicht mehr bewertet und entsprechend nicht mehr geurteilt. Ab hier wird zu der Tonalität des Vorwortes zurückgekehrt, denn mit der vorliegenden Antwort aus Kapitel 6 lassen sich nun zwei Fragen beantworten, die vom Anfang dieser Arbeit an offen geblieben sind. Die erste gilt den Akteuren, die mit dem Netzwerk interagieren, jenen, die auf der Infrastruktur aktiv aufbauen (Institute, und mit ihnen die in 1.1 nicht eigens genannten Entwickler), jenen, die ihr monetär vertrauen (Kapitalgeber und Nutzer), und jenen, die sie regulieren (Politik und Recht). Abschnitt 1.1 hielt fest, dass sie ihre Prüfung sorgfältig führen, dass sie dabei aber unter einer Annahme handeln, die sich der Prüfung entzog, weil ihr der Maßstab fehlte. Die Frage, die daraus folgt, lautet sinngemäß: Woran hängt die Annahme über den dauerhaften Bestand, unter der jene bereits handeln, die auf dem System aufbauen, ihm vertrauen oder es regulieren, wenn keine Instanz für ihn einsteht? Die zweite ist die eingangs von mir naiv gestellte Frage, die mich überhaupt erst zur Konzeption dieser Arbeit inspiriert hat: „Was ermöglicht ein solches kryptographisches System über dezentralen Zahlungsverkehr hinaus, und muss es überhaupt darüber hinausgehen?“ Die Auflösung beider Fragen ist Gegenstand von Kapitel 7.

Das Bild, wenn alles gebaut ist

Um die Fragen zu beantworten und einen klaren roten Faden zu haben, zeichne ich zunächst die Züge des SOLL-Zustands zusammengefügt auf. Aus ihnen lässt sich eine vereinfachte Definition ableiten, mit der sich die Fragen nachvollziehbarer und intuitiver beantworten lassen.

Ein Block, der ein Vielfaches des heutigen Volumens trägt, kostet den, der ihn prüft, genauso viel wie ein leerer. Dieser Satz ist der Angelpunkt des Bildes, das entsteht, wenn die Roadmap vollständig gebaut ist. Validatoren rechnen die Transaktionen nicht mehr einzeln nach. Sie prüfen einen Beweis für die korrekte Blockausführung, den ein Prover erzeugt, also ein darauf spezialisierter Rechner, der die Ausführung einmal für alle übernimmt. Diese Prüfung dauert nur wenige Millisekunden, unabhängig davon, wie viele Transaktionen der Block enthält. Dadurch skaliert die Kapazität des Netzwerks, ohne die Verifikationskosten zu steigern. Heute verarbeitet Ethereum bei 60 Millionen Gas zwischen 15 und 30 Transaktionen pro Sekunde, abhängig von der Transaktionskomplexität. Die Zielmarke der Basisschicht liegt bei rund 10.000, langfristig erreichbar über einen gestaffelten Ausbaupfad der Ausführung. Zugleich bleibt die Souveränität der Teilnehmer gewahrt: Wer dem kryptographischen Beweis nicht vertraut, kann Transaktionen weiterhin wie gewohnt vollständig selbst ausführen und verifizieren.

Diese Verifikation läuft direkt auf herkömmlichen Endgeräten wie Laptops oder Smartphones. Der Speicherbedarf eines verifizierenden Node sinkt dadurch von 2 bis 4 Terabyte auf unter 100 Megabyte, während der benötigte Arbeitsspeicher auf unter 1 Gigabyte und die Rechenlast auf einen einzigen Prozessorkern reduziert werden. Auch die Erstsynchronisation, die derzeit noch Stunden oder Tage beansprucht, verkürzt sich auf wenige Sekunden. Ein Beispiel hierfür ist der Client Helios, der im Browser-Tab und auf Hardware der Raspberry-Pi-Klasse läuft, ohne eine eigene Kopie der Blockchain vorzuhalten.

Dies steht im starken Kontrast zur aktuellen Praxis, in der rund 70 Prozent der Nutzer über zentralisierte Infrastrukturanbieter wie Infura oder Alchemy auf das Netzwerk zugreifen und sich dabei ungeprüft auf deren Daten verlassen müssen. Im angestrebten Zielzustand tritt an die Stelle der Notwendigkeit eine Möglichkeit: Wer prüfen will, kann es auf dem eigenen Gerät tun, und die dafür benötigten Daten bezieht er aus einem dezentralen Peer-to-Peer-Netzwerk. Ein einzelner Anbieter steht dazwischen nicht mehr.

Auch das Konto selbst ändert seine Natur: Schrieb das Protokoll bislang vor, wie ein Konto eine Transaktion autorisiert, übergibt es die Aufgabe künftig di-

rekt an das Konto selbst. Dessen Validierungsregeln werden damit frei programmierbar.

Für Nutzer bedeutet das: Sie können ihr Konto per Fingerabdruck entsperren, wodurch das Endgerät selbst zur Wallet wird. Geht das Gerät verloren, können mehrere selbst gewählte Vertrauensinstanzen den Zugang gemeinsam wiederherstellen, ohne dass eine von ihnen allein über das Guthaben verfügen kann. Zudem lassen sich die Netzwerkgebühren in einer beliebigen Währung wie USDT entrichten, oder die jeweilige Anwendung übernimmt sie direkt im Hintergrund. Zudem lässt sich die Unterschrift auf eine quantensichere Logik umstellen.

Unter derselben Voraussetzung, der vollständig umgesetzten Roadmap, bemisst sich die Bestätigungszeit einer Zahlung nicht mehr in Minuten. Bereits nach etwa 2 Sekunden liegt die besicherte Zusage eines Validators vor, nach circa 13 Sekunden folgt die deterministische Bestätigung auf Layer 1 und nach rund 36 Sekunden ist die unumkehrbare Finalität erreicht. Zum Vergleich: Aktuell nimmt sie noch 12,8 Minuten in Anspruch. Jede der Wartezeiten repräsentiert eine klar definierte Sicherheitsgarantie für den Nutzer, wobei selbst die stärkste der Garantien in Sekunden gesichert ist.

Die Entscheidung darüber, welche Transaktionen in einen Block aufgenommen werden, liegt nicht mehr bei einem einzelnen Akteur. Pro Slot erstellen 16 zufällig bestimmte Validatoren gemeinsam mit dem Proposer eine verpflichtende Liste zu inkludierender Transaktionen (Inclusion List), wobei ein einziger ehrlicher unter den 16 ausreicht, damit eine übergangene Transaktion dennoch auf die Liste gelangt. Ein Proposer, der die Liste ignoriert, verliert die Stimmen der Attester und somit den gesamten Block.

Da Builder ihre Gebote künftig direkt an die Blockchain richten, entfallen auch Relays, über die heute rund 15 Prozent der Blöcke laufen und die dabei Zensurfilter wie die OFAC-Listen anwenden. Ergänzend bleibt der Transaktionsinhalt bis zur endgültigen Sequenzierung verschlüsselt, sodass niemand gezielt Transaktionen ausschließen kann, deren Inhalt er nicht kennt. Die Zensurresistenz ist damit im Protokoll verankert. Zuvor hing sie am Wohlverhalten der Betreiber. Sie trägt, solange das Validator-Netzwerk breit gestreut bleibt.

Die Sicherheitsgarantien der Basisschicht enden nicht an deren Systemgrenzen. Überträgt ein Rollup die Sequenzierung seiner Blöcke an die Proposer der Layer 1 und lässt seine Zustandsübergänge durch deren Konsens validieren, benötigt es keinen eigenen Sequencer, kein separates Proof-System, kein Security Council und keine eigene Governance. Übrig bleibt eine reine Ausführungsumgebung mit einem eigenen Gebührenmarkt und State.

Transaktionen zwischen zwei solchen Rollups erfordern dadurch keine Bridges mit zusätzlichen Vertrauensannahmen mehr. Das gilt für Rollups, die EVM-äquivalent bleiben und ihre Blockreihenfolge vollständig an die Basisschicht abtreten. Da die Implementierung letztlich im Ermessen der Betreiber liegt, bleibt ein breites Spektrum an Integrationsgraden bestehen, von der vollständigen Konvergenz bis hin zur souveränen Chain, die kaum noch Schnittstellen mit der Basisschicht teilt.

Was es im Kern ist

Das ist das Bild des SOLL-Zustands, zusammengefasst. Von hier aus lässt es sich vereinfachen, zu einer allgemeinen Definition des Gegenstands.

Ethereum ist im Kern ein Zustand, ein Verzeichnis dessen, wer was besitzt und welche vertraglichen Regeln für dessen Veränderung verbindlich sind. Vier Merkmale machen ihn aus.

Er ist gemeinsam, alle Teilnehmer führen denselben Zustand und nicht jeder seine eigene Fassung mit eigener Wahrheit. Er ist prüfbar, jeder Eintrag lässt sich gegen die Regeln des Protokolls überprüfen, ohne dass ein Dritter seine Richtigkeit bezeugen müsste. Er ist verbindlich, ein Eintrag, der einmal gilt, kann sich durch keine nachträgliche Instanz mehr aufheben lassen. Und er ist zentrumslos, keine Stelle existiert, die ihn eigenmächtig führt, ändert oder abschalten könnte. Diese Beschreibung gilt für den heutigen Zustand ebenso wie für den Zustand nach vollständiger Umsetzung der technischen Roadmap. Die vier Merkmale liegen heute vor, aber sie sind nicht überall eingelöst. Die vollständige Umsetzung der Roadmap macht sie skalierbar, zugänglich und vom Protokoll erzwungen. Heute beruht ihre Einlösung auf der Marktlage.

Der Bewertungsrahmen selbst hat vier Eigenschaften nicht erfasst, weil kein Kriterium auf sie zielte. Die zwölf Kriterien stammen aus Infrastrukturen, deren Betrieb jemandem gehört und deren Finanzierung von außen kommt. Wo Ethereum genau darin abweicht, hat der Maßstab keinen Messpunkt.

Ein Verzeichnis für sich genommen ist nichts Ungewöhnliches, da Institutionen wie Banken seit Jahrhunderten Register führen. Dass dieser Zustand weit über ein bloßes Kontobuch hinausreicht, beruht auf drei grundlegenden Prinzipien.

Der Besitz eines Eintrags beruht auf einem kryptographischen Nachweis. Wer diesen Nachweis führen kann, verfügt auf Protokollebene absolut über den Eintrag. Keine Bank, keine Börse und keine Behörde kann die Verfügung erteilen oder entziehen. Das ist eine andere Art von Eigentum als jene, die eingeräumt

wird. Sie beruht auf dem Nachweis.

Zudem vollstrecken sich die im Zustand hinterlegten Regeln selbst. Sobald die definierte Voraussetzung eintritt, vollzieht sich die zugehörige Folge im System automatisch, ohne dass es einer anordnenden, überwachenden oder erzwingenden Instanz bedarf. Was sich hierbei vollstreckt, ist der reine Vollzug der Regel. Das Protokoll führt eine fehlerhafte Regel mit derselben unerbittlichen Verlässlichkeit aus wie eine fehlerfreie Regel.

Schließlich lässt sich jeder Eintrag frei mit jedem anderen verbinden, ohne dass die Beteiligten einander kennen oder um Erlaubnis fragen müssen. In ihrer stärksten Form stehen zwei Operationen innerhalb derselben Schicht in einem einzigen, unteilbaren Schritt, sodass sie entweder gemeinsam gelingen oder gemeinsam scheitern. Über die Grenze zwischen verschiedenen Schichten hinweg gilt sie zwar nicht mehr, das Prinzip der freien Kombinierbarkeit bleibt jedoch bestehen.

Ein reines Zahlungssystem nutzt von ihnen nur das Einfachste, nämlich die reine Verschiebung von Guthaben. Vor dem Bild stehen die beiden Fragen, die offen sind: woran die Annahme über den dauerhaften Bestand hängt, unter der jene bereits handeln, die auf diesem Zustand aufbauen, ihm vertrauen oder ihn regulieren, und was er über dezentrales Payment hinaus ermöglicht.

Wer baut, wer vertraut, wer reguliert

Institutionelle Akteure handeln längst unter dieser Annahme. Der tokenisierte Geldmarktfonds von J.P. Morgan operiert ausschließlich auf Ethereum, und Crédit Agricole gab über ihre Verwahrtochter einen MiCA-konformen Euro-Stablecoin auf derselben Kette heraus, beides wie in 1.1 belegt. Beide Institute unterzogen das System im Vorfeld einer detaillierten praktischen Prüfung. Die weitreichendere Annahme entzog sich der Prüfung jedoch: dass die Blockchain auch in zehn Jahren noch verlässlich läuft, alle Teilnehmer gleichbehandelt, sich nicht einseitig abschalten lässt und zukünftige, heute noch unbekannte Nutzungsformen ermöglicht. Was die Akteure in ihrer Praxis voraussetzen, sind Dauerhaftigkeit, Neutralität, die Unmöglichkeit einseitiger Abschaltung und Offenheit. Es sind die vier Merkmale des Zustands, von der Praxis her benannt. Die erste Gruppe, die unter diesen Vorzeichen handelt, baut direkt auf dem System auf.

Wer auf Ethereum entwickelt, profitiert ab dem ersten Moment von der Architektur. Ein Entwickler, der ein neues DeFi-Protokoll erstellt, kann die Liquiditätspools von Uniswap, die Lending-Märkte von Aave und die Stablecoin-Logik von MakerDAO in seine eigene Anwendung integrieren. Dafür braucht er weder eine Vertragsbeziehung zu diesen Protokollen noch deren Genehmigung, und ihre Betreiber müssen von der Integration nicht einmal erfahren. In dieser Struktur entfällt das klassische Gegenparteirisiko. Die Dauerhaftigkeit zeigt sich praktisch daran, dass Smart Contracts aus dem Jahr 2017 bis heute unverändert ausgeführt werden. Einzige systematische Ausnahmen bilden Protokoll-Upgrades zur Anpassung der Transaktionsgebühren, die in seltenen Fällen Programmiercode beeinträchtigten, der feste Gebührenwerte voraussetzte. Ein Institut, das eine Anwendung hier verankert, erhält die Neutralität und Schnittstellenstabilität ohne Verträge, Verhandlungen oder Verlängerungen.

Diese Garantien gelten allerdings vor allem auf der Basisschicht, auf der die wenigsten Akteure direkt aufbauen. Die Realität zeigt eine Hürde: Nutzer, die über MetaMask auf einen DeFi-Dienst auf einem Rollup zugreifen, bewegen sich über vier Vertrauensebenen, die das Ethereum-Protokoll nicht direkt absichert. Dabei weichen die Sicherheitsbedingungen stark voneinander ab. Während das Netzwerk Base ein Exit-Window von null Tagen hat, beträgt es bei Arbitrum One 17 Tage. Die Nutzung plattformspezifischer Funktionen wie Stylus oder spezifischer Precompiles erschwert zudem einen Wechsel zu alternativen Systemen. Damit verlagern sich die ursprünglichen Erwartungen an die Blockchain auf eine vorgelagerte Ebene mit eigenen Betreibern, Fristen und Wechselkosten. Selbst nach der vollständigen Umsetzung der technischen Roadmap

bleibt die Wahl der Ebene entscheidend, da deren Implementierung im Ermessen der Betreiber liegt und von vollständig angepassten bis zu völlig eigenständigen Netzwerken reicht. Kapitel 4 beschreibt diese Einschränkung als Diskrepanz zwischen den theoretischen Möglichkeiten des Protokolls und der tatsächlichen operativen Praxis. Für Entwickler beschreibt das die reale Entscheidungslage, da die gewählte Schicht über die tatsächliche Sicherheit entscheidet.

Kapitalgeber hingegen treffen weniger technische Entscheidungen, bringen dem System dafür aber großes Vertrauen entgegen. Institutionelle Akteure vertrauen auf den Fortbestand des Netzwerks über die nächsten zehn Jahre und verweisen auf die ununterbrochene Verfügbarkeit trotz fünfzehn großer Upgrades in der Vergangenheit. Die vorliegende Bewertung ordnet dieses Vertrauen zeitlich ein. Auf Sicht von fünf bis zehn Jahren präsentiert sich Ethereum als stabil, der Upgrade-Prozess läuft verlässlich, die wirtschaftliche Absicherung umfasst rund 26 Milliarden US-Dollar und die Validator-Infrastruktur ist intakt. Über einen Zeitraum von zwanzig Jahren gefährden ungelöste Probleme wie das unkontrollierte Datenwachstum der Kette, die ungeklärte langfristige Belohnungsstruktur für die Absicherung sowie die ausstehende Umstellung auf quantenresistente Kryptographie die Tragfähigkeit. Die Risiken sind unterschiedlich weit fortgeschritten. Für das Datenwachstum existieren theoretische Lösungen, die jedoch laut Kapitel 6 auf ungesicherter Forschung ohne konkreten Umsetzungsplan basieren. Zur langfristigen Finanzierung der Netzwerksicherheit gibt es noch kein beschlossenes Konzept, während die Umstellung auf Quantenresistenz bereits in Testnetzwerken erprobt wird. Der Verweis auf die bisherige Stabilität stützt somit nur die mittelfristige Prognose. Die Erwartung einer jahrzehntelangen Dauerhaftigkeit, wie Abschnitt 1.1 sie beschreibt, geht über die gegenwärtig nachweisbaren Fundamente hinaus. Eine Eigenheit ohne Entsprechung in den sieben untersuchten Referenzsystemen ist, dass der Wert der eigenen Währung direkt die Sicherheit des Gesamtsystems bestimmt. Kapitalgeber halten keinen Anspruch gegen ein Unternehmen. Sie stützen mit ihrem Vermögen unmittelbar die Integrität des Systems.

Auch Endnutzer stützen sich unbewusst auf die Annahmen, obwohl Abschnitt 1.1 sie nicht explizit nennt. Sie profitieren von der direkten, unantastbaren Kontrolle über ihre digitalen Werte über eigene Schlüssel, ohne Abhängigkeit von Intermediären wie Banken oder Behörden. Die Ausfallsicherheit zeigte sich eindrücklich im Mai 2023, als nach zwei aufeinanderfolgenden Störungen die Netzwerkbeteiligung unter die kritische Zwei-Drittel-Schwelle fiel. Das Protokoll reagierte selbstständig, entzog inaktiven Validatoren schrittweise ihre Anteile und stellte die vollständige Funktionsfähigkeit nach 96 Minuten ohne

menschliches Eingreifen oder externe Koordination wieder her. Klassische Systeme wie das Internet-Adressverzeichnis, das SWIFT-Netzwerk oder Stromnetze erfordern bei Ausfällen stets manuelle Rettungsmaßnahmen, Notfallpläne oder physische Eingriffe. Ethereums Protokoll benötigt solche externen Hilfen nicht.

Trotz der technischen Stärken klafft eine Lücke zwischen der theoretischen Möglichkeit und der tatsächlichen Nutzung. Zwar kann theoretisch jeder Nutzer einen eigenen Node betreiben und die Kette unabhängig prüfen, in der Praxis scheitert das jedoch meist an den hohen Hürden für Hardware, Wartung und technisches Wissen. Viele Anwender lagern die Verwahrung freiwillig an zentrale Börsen aus. Besonders deutlich wird das beim Absichern des Netzwerks. Die Mindestanforderung von 32 ETH entsprach beim Stichtagskurs rund 67.000 US-Dollar, und der Anteil privat geführter, unabhängiger Validatoren liegt unter einem Prozent des Gesamtvolumens. Dienstleister senken die Barriere zwar auf Kleinstbeträge ab 0,01 ETH, übernehmen im Gegenzug aber die Kontrolle über die Validierung. Der wirtschaftliche Zugang ist somit offen, während die tatsächliche Kontrolle über die Infrastruktur hinter technischen und finanziellen Barrieren verbleibt. Laut Kapitel 6 überstehen die Einschränkungen, einschließlich der 32-ETH-Schwelle und der vorgelagerten Nutzerschnittstellen, auch die vollständige Umsetzung der Roadmap, weil kein Feature ihre strukturelle Ursache behebt.

Bei staatlichen Regulierungsbehörden zeigt sich ein anderes Bild, da der Zugriff auf der Anwendungsebene ansetzt. Der am 18. Juli 2025 unterzeichnete US-amerikanische GENIUS Act reguliert zwar die Herausgeber von Stablecoins hinsichtlich Reserveanforderungen, Transparenzpflichten und Lizenzierung, klammert die darunterliegende Protokollschicht jedoch aus. Er reguliert Circle und Tether als Emittenten, betrifft jedoch weder das Ethereum-Protokoll selbst noch die zugrundeliegenden Smart Contracts zur Verwaltung von USDC und USDT. Für dezentrale Anwendungen ohne identifizierbare Herausgeber existiert bisher kein vergleichbarer Rahmen. Diese Entscheidung begrenzt den rechtlichen Zugriff auf die Anwendungsschicht.

Während private Akteure Verantwortung an das Protokoll abgeben, suchen Regulierungsbehörden nach konkreten Ansprechpartnern. Da das Protokoll selbst keinen Adressaten bietet, verschiebt sich der Fokus auf zentrale Schnittstellen. Drei kommerzielle Akteure kontrollieren rund 93 Prozent der Block-Produktion, angeführt von Titan mit 51,2 Prozent. Der Herfindahl-Hirschman-Index liegt bei 3.554 und überschreitet die US-Schwelle für hochkonzentrierte Märkte von 2.500 deutlich. Der Betrieb der Nodes konzentriert sich zudem auf wenige Cloud-Anbieter, rund 59 Prozent der gehosteten Execution-Layer-

Nodes laufen auf dreien. Geographisch befinden sich 39 Prozent in den USA, 14,5 Prozent in Deutschland und 14 Prozent in China, sodass rund 53 Prozent auf lediglich zwei Länder entfallen. Staatliche Eingriffe setzen folglich an den physischen Konzentrationspunkten an.

Die Tragweite der Konzentration zeigte sich im November 2022, als 79 Prozent der Blöcke Transaktionen von sanktionierten Adressen filterten. Die Einschränkung führte jedoch nur zu minimalen Verzögerungen von wenigen Blöcken. Gegenwärtig liegt der Anteil bei etwa 15 Prozent, da der größte Akteur Titan bewusst auf Filterungen verzichtet. Dieser Rückgang vollzog sich ohne Protokolländerungen, rein aus wirtschaftlichen Anreizen des Marktes. Der Van-Loon-v.-Treasury-Entscheid im November 2024 und das OFAC-Delisting von Tornado Cash im März 2025 fielen in denselben Zeitraum. Ein solcher regulatorischer Zugriff bleibt jedoch instabil, da er auf veränderlichen Marktstrukturen beruht. Laut Kapitel 6 wird eine hohe Konzentration an der Spitze der Block-Produktion auch nach der vollständigen Umsetzung der technischen Roadmap fortbestehen.

Das System steht unter dem Recht, weicht aber von dessen klassischen Zugriffsmechanismen ab. Die Schnittstelle zwischen programmgesteuerter und staatlicher Durchsetzung bleibt weitgehend ungeklärt. Kapitel 3 verdeutlicht das im Vergleich der Infrastrukturen: Keine der untersuchten Plattformen besitzt physische Durchsetzungsmacht. Das Stromnetz kann die Versorgung unterbrechen, das Internet Daten blockieren und SWIFT Teilnehmer ausschließen, aber keines dieser Systeme kann Zwang gegen Personen ausüben. Demgegenüber behält das Rechtssystem als übergeordnete Instanz seine volle Macht über Personen, Unternehmen und Standorte. Auf der dezentralen Blockchain findet der rechtliche Zugriff jedoch keine direkte Adresse.

Das Fehlen einer zentralen Pausetaste verdeutlicht die Unabhängigkeit. Bei kritischen Fehlern lässt sich das System nicht stoppen, die einzige Antwort bleibt ein Notfall-Hard-Fork, der die Koordination aller Client-Teams verlangt. Dass es vermeidbar ist, zeigte der Prysm-Bug im Dezember 2025, dessen Auswirkungen die Diversität der Client-Software abfing. Die Stabilität beruht jedoch auf kontinuierlicher sozialer Koordination und stellt kein automatisches Gleichgewicht dar. Eine Pausetaste ist als Funktion nicht vorgesehen, da sie der Zentrumslosigkeit widerspricht. Wer eine solche Kontrollinstanz einführen würde, zerstörte das eigentliche Fundament des Systems. Der dauerhafte Bestand der Infrastruktur hängt somit von keinem einzelnen Akteur ab. Er beruht auf dem Zusammenspiel der zentrumslosen Struktur und auf der kontinuierlichen sozialen Koordination, die sie trägt. Damit ist die erste Kernfrage beantwortet, während die zwei-

te Frage die Handlungsmöglichkeiten jenseits reiner Wertübertragungen untersucht.

Es ging nie nur um Payment

Ich hielt im Vorwort fest, dass sich enorme Summen bewegen, dass große Erzählungen über Zahlung, Identität und die Verwaltung des eigenen Vermögens ohne Mittelsmann kursieren und dass dennoch seltsam unklar bleibt, worum es im Kern geht. Was ich suchte, war der Kern. Payment war der Begriff, mit dem ich ihn umriss, und offen blieb, was jenseits davon liegt. Der Zustand liegt nun benannt vor, mitsamt seinen drei Prinzipien. Die Antwort beginnt bei dem Wort, das die Frage mitbringt, ohne es zu klären.

Payment hieß für mich Zahlungsverkehr und die Autonomie über die eigenen Schlüssel. Beides beruht auf dem ersten der drei Prinzipien. Wer den kryptographischen Nachweis führen kann, verfügt auf Protokollebene absolut über den Eintrag, ohne dass eine Bank, eine Börse oder eine Behörde ihm die Verfügung erteilt. Die reine Verschiebung von Guthaben ist die einfachste Handlung, die sich aus einer solchen Verfügung ableiten lässt. Sie ändert eine Zahl an zwei Stellen und ist danach fertig. Vom Zustand braucht sie wenig. Er muss den Nachweis anerkennen und die Änderung verbindlich verzeichnen, mehr verlangt eine Zahlung nicht von ihm.

Was ich Payment nannte, ist ein Prinzip von dreien, und zwar in seinem einfachsten Gebrauch. Damit ist beantwortet, worum es im Kern geht, und die Antwort lautet: nicht um Payment. Der Kern ist der Zustand. Payment ist eine Art, ihn zu benutzen. Wer Ethereum als Zahlungssystem beschreibt, beschreibt einen Gebrauch, den es zulässt, und lässt zwei Prinzipien von dreien unerwähnt. Die Frage nach dem, was über Payment hinausgeht, ist deshalb keine Frage nach Zusatzfunktionen. Sie ist die Frage, welches Problem die beiden übrigen Prinzipien lösen, das ohne sie ungelöst bliebe.

Was liegen bleibt, sind der Selbstvollzug und die freie Kombinierbarkeit. Beide arbeiten an einem Problem, das älter ist als jede Technik und das Kapitel 3 dem Rechtssystem zugeschrieben hat. Wie kommen Fremde zu verbindlichen Vereinbarungen? Die Wirtschaftshistorie zeigt, dass Transaktionen vor der Entwicklung institutionellen Rechts nur innerhalb von Clan-, Familien- oder ethnischen Netzwerken funktionierten, weil reputationsbasierte Durchsetzung über kleine Gruppen hinaus nicht skaliert. Kapitel 3 hat das an Avner Greifs Untersuchung ausgeführt. Erst das staatlich durchgesetzte Vertragsrecht öffnete die Kooperation für Millionen Fremde. Wer sich vorher binden wollte, musste einan-

der kennen, und die Reichweite einer Vereinbarung endete an der Reichweite der Gruppe, die den Bruch bestrafen konnte. Das Rechtssystem, das im vorigen Abschnitt als Zugriffsmacht auftrat, steht hier auf der anderen Seite: als das, was Vereinbarungen zwischen Fremden überhaupt trägt. Es unterscheidet sich von allen anderen Infrastrukturen dadurch, dass hinter seiner Durchsetzung das Gewaltmonopol des Staates steht. Verbindlichkeit unter Fremden gab es bisher nur unter einer Instanz, die notfalls zugreift.

Der Selbstvollzug erzeugt die Verbindlichkeit ohne eine solche Instanz. Sobald die definierte Voraussetzung eintritt, vollzieht sich die zugehörige Folge im System automatisch, ohne dass jemand sie anordnet, überwacht oder erzwingt. Das Beispiel liegt im Protokoll selbst. Das Slashing-System bestraft Fehlverhalten von Validatoren, ohne dass eine Behörde daran beteiligt wäre. Die Durchsetzung ist algorithmisch und deterministisch. Treten die definierten Bedingungen ein, folgt die vorgesehene Konsequenz, ob die betroffene Partei einverstanden ist oder nicht.

Die freie Kombinierbarkeit setzt fort, was der Selbstvollzug beginnt. Jeder Eintrag lässt sich mit jedem anderen verbinden, ohne dass die Beteiligten einander kennen oder um Erlaubnis fragen müssen. Kapitel 6 fasst die kombinatorische Eigenschaft in ihrer schärfsten Form, als das exponentielle und erlaubnisfreie Zusammenspiel beliebig vieler Contracts zu Konstruktionen, die niemand vorhergesehen hat. Beide Prinzipien zusammengenommen ergeben, was über die Verschiebung von Guthaben hinausgeht: verbindliche Kooperation zwischen Fremden ohne eine Instanz, die sie durchsetzt. Was das Vertragsrecht an Reichweite gewann, gewann es um den Preis einer Instanz mit Zugriff. Der Zustand hält die Reichweite und lässt den Preis aus.

Zwei Grenzen begleiten diese Leistung. Die erste liegt darin, dass allein der Vollzug abgenommen wird. Über die Richtigkeit der Regel entscheidet das Protokoll nicht, es führt sie mit derselben Verlässlichkeit aus wie eine fehlerfreie. Die zweite Grenze liegt in der Ausdrucksfähigkeit des Codes. Streitigkeiten über Absichten, Interpretationen, fahrlässiges Verhalten und außervertragliche Ansprüche bleiben auf institutionelle Durchsetzung angewiesen. Das Rechtssystem wird nicht ersetzt. Was entsteht, ist eine komplementäre Durchsetzungsschicht für Fälle, in denen die institutionelle Durchsetzung zu langsam oder zu teuer ist, über Jurisdiktionen hinweg nicht greift oder für den Anwendungsfall gar nicht vorgesehen war.

Bleibt die zweite Hälfte der Frage. Muss das System über Payment hinausgehen? Sie ist die Frage eines Investors, der wissen will, ob er Komplexität trägt, die niemand braucht.

Für Zahlungsverkehr lautet die Antwort nein, das Mehr ist Ballast. Wer nur verschiebt, braucht keinen Selbstvollzug, weil eine Überweisung nichts vollstreckt außer sich selbst. Er braucht keine Kombinierbarkeit, weil eine Verschiebung sich mit nichts verbindet. Beide Prinzipien lägen im Zustand und blieben unbenutzt. Ein Zahlungssystem, das sie mitträgt, trägt sie umsonst, und der Verdacht des Investors trifft an dieser Stelle zu.

Für Infrastruktur kehrt sich der Befund um. Kapitel 2 hat mit Brett Frischmann festgehalten: Infrastruktur definiert sich durch das, was sie ermöglicht, nicht durch das, was sie ist. Sie dient als Produktionsfaktor für weiterführende Aktivitäten und ist kein Endprodukt. Ein System, das nur zahlt, ist ein Endprodukt. Selbstvollzug und Kombinierbarkeit sind die Bedingung dafür, dass der Begriff Infrastruktur überhaupt greift. Was ein Zahlungssystem ungenutzt liegen ließe, ist genau das, woran ein Bauender ansetzt. Ohne den Selbstvollzug gäbe es nichts zu verankern, ohne die Kombinierbarkeit nichts, woran anzuschließen wäre.

Meine naiv gestellte Frage war damit genau die Unterscheidung, die Kapitel 2 später als Begriffsarbeit hergeleitet hat: Endprodukt oder Input. Im Vorwort steht, an genau diesem Begriff schärfe sich die weite Ausgangsfrage zu einer prüfbaren. Das System entscheidet die Unterscheidung nicht, es lässt beides zu. Wer die Frage stellt, entscheidet sie mit, weil er mit ihr angibt, wozu er das System gebraucht.

Beide Fragen sind beantwortet. Die eine hing an einer Annahme, die sich der Prüfung entzog, weil ihr der Maßstab fehlte, die andere an einem Wort, das ich benutzt habe, ohne seinen Gegenstand zu kennen. Was sich an ihnen zeigt, gilt nicht Ethereum allein. Ich habe das Netzwerk als Repräsentanten gewählt, weil sich die Frage an etwas Konkretem prüfen lassen musste, und die Antwort gilt der Klasse solcher Systeme. Sie gilt nicht der Frage, welches der Systeme sich am Ende behauptet. Was das Schreiben daran mit meinem eigenen Blick gemacht hat, gehört in die letzten Zeilen dieser Arbeit.

Mehr als Software, ein paar letzte Worte

Ich schreibe diesen letzten Abschnitt des letzten Kapitels nach nun fast sieben Monaten Arbeit, Recherche, Lesen, Lernen, Schreiben, Iteration, Unterhaltungen und vielem Nachdenken. Offen gestanden weiß ich gar nicht, wie man so eine Arbeit wirklich abschließt. Die Wahrscheinlichkeit ist hoch, dass die nun geschriebenen Zeilen zu einer weiteren der unzähligen Iterationsrunden gehören, nachdem ich eine KI gebeten habe, das Geschriebene strukturell und inhaltlich einzuordnen.

Die selbst initiierte Arbeit hat mich viel lernen lassen. Allein die Tatsache, solch ein Thema anzugehen und einen Startpunkt zu finden, war eine Aufgabe für sich. Aus einer banalen Fragestellung und einer gewissen Ungewissheit, die während einer blutigen Marktphase fast in Frustration kippte, eine logische These und einen Einstieg zu finden, fühlte sich an wie in jenem Meme: ein kleiner Ritter mit gezücktem Schwert, der einem unbezwingbar großen Ritter gegenübersteht.

So undurchdringlich ein solcher Start ohne fremd gegebene Vorgaben und Rahmen auch ist, so hat er mich doch befähigt, eigenständig zu werden. Das schiere Drauflosles en und Verschlingen des Lern-Abschnitts auf ethereum.org binnen weniger Tage, der von absoluten Einsteiger-Artikeln bis zu ersten komplexeren Begriffen und Architekturen reichte, verwies bereits darauf, dass die Arbeit länger werden könnte als erwartet. Die teils neu erlangten Informationen, die sich für mich nicht einordnen ließen und meine Motivationsfrage nicht beantworteten, führten mich überhaupt erst dazu, einen echten Rahmen zu setzen und die Frage neu zu definieren. So durfte ich herausfinden, wie eine Arbeit anzugehen ist, die eben nicht unter schulischer Aufsicht steht und nicht auf die üblichen acht bis fünfzehn Seiten beschränkt werden sollte.

Mit einer klar definierten Frage, die sich an einem fundamentalen Rahmen prüfen ließ, erschlossen sich plötzlich ein Horizont und eine Struktur, in denen sich mit Gewissheit arbeiten ließ. Die Recherche erstreckte sich von nun an über Infrastrukturtheorien sowie physikalische, philosophische, politische und geographische Themen und vieles mehr. Neben der Recherche und den verschiedenen Perspektiven gab eine Kapitelstruktur, die einen Zustand bewertet, einen klaren Leitfaden, an dem ich mich entlanghangeln konnte und der die Recherche mit einer gewissen Gelassenheit noch sortierter erscheinen ließ. Denn der Gegenstand entwickelt sich stetig weiter, nahezu im Wochentakt finden Pivots, Iterationen und Präzisierungen statt. Ohne die Zweiteilung in den Stichtags-Zustand (in der Arbeit „IST-Zustand“) und den werdenden Zustand („SOLL-Zustand“)

ließe sich darüber kaum in aller Ruhe schreiben, ohne dass am nächsten Tag alles über Bord ginge. Die Herangehensweise hat mich Bitteres erfahren lassen und mich zugleich liebevoll über diverse Instrumente aufgeklärt, die nicht nur für das Recherchieren und Schreiben hilfreich waren, sondern besonders für die eigene gedankliche Sortiertheit und das Verknüpfen von Zusammenhängen.

Damit zum sich ständig weiterentwickelnden Gegenstand selbst. Bei der Betrachtung eines solchen dynamischen Systems liegt die Vermutung nahe, dass seine Evolution stets einem durchstrukturierten, breit gefächerten Plan folgt und auf einem klaren Konsens aller Beteiligten beruht. Während des Verfassens dieser Arbeit, in einem Zeitraum von knapp sieben Monaten, durfte ich jedoch hautnah miterleben, dass sie selbst für die aufgeklärtesten Akteure keineswegs der Realität entspricht.

Ein prägnantes Beispiel, das die Diskrepanz zwischen rationaler Planung und chaotischer Realität verdeutlicht, ist die jüngste Debatte um die Ethereum Foundation. Sie drehte sich im Kern darum, wie sich das Netzwerk in Zukunft positionieren soll. Während die Stiftung an den ideologischen, fast schon romantischen Cypherpunk-Idealen festhalten wollte, forderten Teile der Nutzer, der Community und des Teams angesichts des harten Wettbewerbs mit anderen Chains pragmatische, marktwirtschaftliche Anpassungen. Die Debatte legte offen, dass selbst bei einem der Netzwerke, die als technologisch am fortschrittlichsten gelten, kein automatischer Konsens über den Pfad der Weiterentwicklung herrscht. Vielmehr ist Fortschritt das Resultat schmerzhafter Reibungspunkte, interner Richtungsstreite und des ständigen Ringens zwischen Idealismus und Pragmatismus.

Neben der Debatte selbst haben sich im Verlauf der Monate angekündigte Features und Architekturen stetig geändert, verschoben oder gar gestrichen. Am weittragendsten war, auch für den Fokus dieser Arbeit, die im Februar 2026 angestoßene Neuausrichtung hin zur direkten L1-Skalierung. Mit dem Pivot korrigierte das Forschungsumfeld, angestoßen von Vitalik Buterin, die jahrelang dominierende Strategie, die Skalierung primär auf externe Layer-2s auszulagern. Stattdessen rückte die Erhöhung der Kapazität der Layer 1 selbst wieder in den Fokus. Ein solch abrupter Paradigmenwechsel bestätigt die gewählte Zweiteilung dieser Arbeit. Er zeigt, dass sich der „IST-Zustand“ zwar präzise einfangen lässt, der „SOLL-Zustand“ jedoch ein dynamisches Konstrukt bleibt, das sich starr vorgezeichneten Roadmaps entzieht und sich im Konsensprozess immer wieder neu ausrichtet.

Die Neuausrichtungen sind unter anderem auf die Unsicherheiten der Entwickler, Researcher und sonstigen beteiligten Akteure zurückzuführen, die teil-

weise unabhängig vom Fokus der Ethereum Foundation und ihrem Aufgabenbereich agieren. Sie führten innerhalb der Foundation und darüber hinaus zu Umstrukturierungen. Zugleich verdeutlichen sie, dass es kein vollständig definiertes Zukunftsbild geben kann, wenn bereits die Forscher selbst monatlich bis jährlich iterieren. Das tut der Arbeit und vor allem dem Netzwerk keinen Abbruch. Ich halte es sogar für völlig normal und angebracht, denn gerade Ethereum muss sich bei stetig wachsenden technologischen Möglichkeiten und Gefahren wie künstlicher Intelligenz, Quantencomputern oder reinen Fortschritten in der Mathematik mit der Zeit ändern, und Planung wie Forschung sind entsprechend anzupassen.

Um mir ein Bild von der Forschung und dem sonst überwiegend digital stattfindenden Austausch zu machen, hat mich die Arbeit auf verschiedene Zusammenkünfte und Events gebracht, genauer gesagt auf die Berlin Blockchain Week. Dort durfte ich zum ersten Mal Menschen kennenlernen, die am Projekt und in seinem Umfeld arbeiten. Nicht, dass die Reise mein Urteil geändert hätte, eher umgekehrt: Das Urteil, oder gerade die Arbeit und das damit erlangte Verständnis, hat mich neugierig gemacht, das sonst rein digitale Kommunizieren, Lernen und Kennenlernen auch auf einer physischen Ebene zu erleben. Ich bin dankbar, dass mir dieses Stück Schrift solche Erfahrungen und Erkenntnisse eröffnet und das Ticket zu den Konferenzen ermöglicht hat.

So viel zur eigenen Dokumentation und zu dem, was ich im Verlauf dieser sieben Monate lernen und erleben durfte. Bleibt der Rückbezug auf das Vorwort und die dort versprochene Auskunft über das, was ich denke.

Wenn man die technische Infrastruktur von Ethereum analysiert und sie dann, wie in Berlin, plötzlich lebendig vor sich sieht, drängt sich der Impuls auf, den Blick radikal zu weiten. Es geht hier nämlich um mehr als Software.

Momentan wird Ethereum in der breiten Öffentlichkeit meist noch pragmatisch als technologische Alternative zu unseren bestehenden, zentralisierten Finanzsystemen begriffen. Ich deute die Entwicklung jedoch fundamentaler: Nach meiner Auffassung bringt der Bauplan unserer Realität zu jedem Pol einen Gegenpol hervor, so wie es zu einem Oben ein Unten oder zu einer Aktion eine Reaktion gibt.

Aus dieser Perspektive ist Ethereum keine zufällige Erfindung. Die strukturelle Schablone für ein dezentrales Netzwerk lag im logischen Raum bereit, und Ethereum hat sie besetzt. Genau diese Polarität erklärt, warum die gängigen Vergleiche der Gegenwart das Phänomen unterschätzen.

Das Gefälle im reinen Zahlungsverkehr ist zwar riesig, weil der weit überwiegende Teil über zentralisiertes Fiatgeld abgewickelt wird und nur ein verschwin-

dender Anteil über den gesamten dezentralen Sektor. Da es, wie in dieser Arbeit bereits herausgestellt, jedoch nicht um reine Zahlungsabwicklung geht, greift ein rein prozentualer Vergleich zu kurz. Er stellt lediglich das dezentral abgewickelte Zahlungsvolumen dem zentralisierten gegenüber und lässt die eigentliche Dimension daneben unberührt.

Selbst auf dem schmalen Feld, dem reinen Bewegen von Guthaben, hat Ethereum den Gegenpol besetzt, obwohl das die Disziplin ist, in der es am wenigsten von einem klassischen Zahlungssystem abweicht. Das eigentliche, unbesetzte Feld liegt jedoch dort, wo es nie um die Zahlung allein ging: bei allem, was Menschen verbindlich miteinander vereinbaren, ohne einander zu kennen und ohne eine übergeordnete Instanz, die im Streitfall zugreift. Dieser Raum lässt sich heute noch nicht in Prozenten ausdrücken. Der Grund dafür ist, dass er zum größten Teil noch gar nicht betreten wurde. Was sich jedoch sagen lässt, ist das Kleinere und zugleich Entscheidende: Die Infrastruktur, die ihn eröffnet, existiert. Ob und wie schnell er sich füllt, ist eine Frage an die Regulierung, die Gewohnheiten, den Erfindergeist, die Einfachheit der Nutzung und die Umstände, unter denen Menschen beginnen, einer Ordnung ohne Mittelpunkt mehr zu trauen als der mit einem.

Abbildungen

Tabellen

Quellen

Die Arbeit belegt überwiegend aus Primärquellen: Spezifikationen, Vorschlagstexten und öffentlich abrufbaren Daten. Das Verzeichnis führt sie in drei Abteilungen. Alle Angaben stehen wortgleich in den Fußnoten des Haupttextes.

Literatur

Aschauer, David Alan (1989): Is Public Expenditure Productive? Journal of Monetary Economics, 23(2), S. 177–200.

Buterin, Vitalik (2014): A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum Whitepaper.

Buterin, Vitalik (2020): A rollup-centric ethereum roadmap. Blogpost, Oktober 2020.

Buterin, Vitalik (2025): Stages as a framework for evaluating rollup maturity. Blogpost.

Buterin, Vitalik / Conner, Eric / Dudley, Rick / Slipper, Matthew / Norden, Ian / Bakhta, Abdelhamid (2019): EIP-1559: Fee market change for ETH 1.0 chain. Ethereum Improvement Proposal. Aktiviert im London-Upgrade, August 2021. Vgl. Ethereum Foundation Blog für die technische Dokumentation.

Buterin, Vitalik / Griffith, Virgil (2019): Casper the Friendly Finality Gadget. arXiv:1710.09437. Für die kombinierte Gasper-Spezifikation vgl. Buterin, Vitalik / Hernandez, Diego / Kamphefner, Thor / Pham, Khiem / Qiao, Zhi / Ryan, Danny / Sin, Juhyeok / Wang, Ying / Zhang, Yan X (2020): Combining GHOST and Casper. arXiv:2003.03052.

Buterin, Vitalik / Hernandez, Diego / Kamphefner, Thor / Pham, Khiem / Qiao, Zhi / Ryan, Danny / Sin, Juhyeok / Wang, Ying / Zhang, Yan X (2020): Com-

bining GHOST and Casper. arXiv:2003.03052.

Daian, Philip / Goldfeder, Steven / Kell, Tyler / Li, Yunqi / Zhao, Xueyuan / Bentov, Iddo / Breidenbach, Lorenz / Juels, Ari (2020): Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. In: IEEE Symposium on Security and Privacy (S&P), 2020. DOI: 10.1109/SP40000.2020.00040.

Davidson, Sinclair / De Filippi, Primavera / Potts, Jason (2018): Blockchains and the Economic Institutions of Capitalism. Journal of Institutional Economics, 14(4), S. 639–658. DOI: 10.1017/S1744137417000200.

Dimitropoulos, Georgios (2020): The Law of Blockchain. Washington Law Review, 95(3), S. 1117–1200, der Blockchain als „infrastructural commons" konzipiert.

Dylan-Ennis, Paul / Kavanagh, Donncha / Araujo, Luis (2023): The Dynamic Imaginaries of the Ethereum Project. Economy and Society, 52(1), S. 87–109. DOI: 10.1080/03085147.2022.2131280.

Frischmann, Brett M. (2012): Infrastructure: The Social Value of Shared Resources. Oxford University Press.

Gencer, Adem Efe et al. (2018): Decentralization in Bitcoin and Ethereum Networks. In: Financial Cryptography and Data Security. Springer, S. 439–457.

Greif, Avner (1994): Cultural Beliefs and the Organization of Society. Journal of Political Economy, 102(5), S. 912–950.

Grimmelmann, James / Windawi, A. Jason (2023): Blockchains as Infrastructure and Semicommons. William & Mary Law Review, 64(4), S. 1097–1129.

Hanseth, Ole / Lyytinen, Kalle (2010): Design Theory for Dynamic Complexity in Information Infrastructures: The Case of Building Internet. Journal of Information Technology, 25(1), S. 1–19.

Hodgson, Geoffrey M. (2016): Conceptualizing Capitalism: Institutions, Evolution, Future. University of Chicago Press.

Jabareen, Yosef (2009): Building a Conceptual Framework: Philosophy, Definitions, and Procedure. International Journal of Qualitative Methods, 8(4), S. 49–62.

Jensen, Johannes R. / von Wachter, Victor / Ross, Omri (2021): How Decentralized is the Governance of Blockchain-based Finance: Empirical Evidence from four Governance Token Distributions. In: Proceedings of the 29th Eu-

ropean Conference on Information Systems (ECIS 2021).

Mayntz, Renate (1993): Große technische Systeme und ihre gesellschaftstheoretische Bedeutung. Kölner Zeitschrift für Soziologie und Sozialpsychologie, 45(1), S. 97–108.

Mnookin, Robert H. / Kornhauser, Lewis (1979): Bargaining in the Shadow of the Law: The Case of Divorce. Yale Law Journal, 88(5), S. 950–997.

Nabben, Kelsie (2023): Web3 as 'Self-Infrastructuring': The Challenge Is How. Big Data & Society, 10(1). DOI: 10.1177/20539517231159002.

Ostrom, Elinor (1990): Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge University Press.

Ovezik, Christina / Karakostas, Dimitris / Milad, Mary / Kiayias, Aggelos / Woods, Daniel W. (2025): SoK: Measuring Blockchain Decentralization. arXiv:2501.18279. Auch publiziert in: Fischlin, M. / Moonsamy, V. (Hrsg.): Applied Cryptography and Network Security (ACNS 2025). Lecture Notes in Computer Science, Bd. 15825. Springer, Cham. DOI: 10.1007/978-3-031-95761-1_7.

Pincheira, Miguel et al. (2023): An Infrastructure Cost and Benefits Evaluation Framework for Blockchain-Based Applications. Systems, 11(4), 184. DOI: 10.3390/systems11040184.

Rozas, David / Tenorio-Fornés, Antonio / Díaz-Molina, Silvia / Hassan, Samer (2021): When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance. SAGE Open, 11(1), S. 1–14. DOI: 10.1177/21582440211002526.

Saltzer, Jerome H. / Reed, David P. / Clark, David D. (1984): End-to-End Arguments in System Design. ACM Transactions on Computer Systems, 2(4), S. 277–288.

van Schewick, Barbara (2010): Internet Architecture and Innovation. MIT Press. Van Schewicks Argument, dass die End-to-End-Architektur des Internets Innovation an den Rändern ermöglicht, ist auf Ethereums permissionless Smart-Contract-Layer übertragbar.

Spencer-Hicken, Scott et al. (2023): Blockchain Feasibility Assessment: A Quantitative Approach. Frontiers in Blockchain, 6. DOI: 10.3389/fbloc.2023.1155125.

Srinivasan, Balaji S. / Lee, Leland (2017): Quantifying Decentralization. Preprint/Blogpost.

Star, Susan Leigh (1999): The Ethnography of Infrastructure. American Behavioral Scientist, 43(3), S. 377–391.

Tilson, David / Lyytinen, Kalle / Sørensen, Carsten (2010): Research Commentary — Digital Infrastructures: The Missing IS Research Agenda. Information Systems Research, 21(4), S. 748–759.

Wood, Gavin (2014/2024): Ethereum: A Secure Decentralised Generalised Transaction Ledger (Yellow Paper). Aktuelle Version: Berlin Version, 2024.

Ølnes, Svein / Jansen, Arild (2018): Blockchain Technology as Infrastructure in Public Sector: An Analytical Framework, sowie dies. (2021): Blockchain Technology as Information Infrastructure in the Public Sector; ferner Grimmelmann, James / Windawi, A. Jason (2023): Blockchains as Infrastructure and Semicommons, Dimitropoulos, Georgios (2020): The Law of Blockchain, und Nabben, Kelsie (2023): Web3 as 'Self-Infrastructuring'. Die vollständigen Angaben stehen in den Fußnoten zu Abschnitt 2.1.

Ølnes, Svein / Jansen, Arild (2021): Blockchain Technology as Information Infrastructure in the Public Sector. In: Reddick, C.G. / Rodríguez-Bolívar, M.P. / Scholl, H.J. (Hrsg.): Blockchain and the Public Sector. Public Administration and Information Technology, Bd. 36. Springer, Cham, S. 19–46. DOI: 10.1007/978-3-030-55746-1_2.

Ethereum Improvement Proposals

Zitierte Vorschläge mit den Seiten ihres Vorkommens. Die Texte selbst stehen unter https://eips.ethereum.org.

Web-Quellen und Daten

Summary of the AWS Service Event in the Northern Virginia (US-EAST-1) Region, Dezember 2021. https://aws.amazon.com/message/12721/

https://blog.ethereum.org/2022/09/15/the-merge

https://eips.ethereum.org/EIPS/eip-1

https://ethereum.foundation/report-2024.pdf

Für die Ethereum Foundation Dokumentation der Client-Architektur vgl. https://ethereum.org/en/developers/docs/nodes-and-clients/

https://ethereum.org/en/whitepaper/

https://ethernodes.org

https://etherscan.io/chart/gaslimit

https://etherscan.io/nodetracker

Gaia-X European Association for Data and Cloud. https://gaia-x.eu

https://l2beat.com/scaling/summary

Internet Shutdown in Iran during Mahsa Amini Protests, September 2022. https://netblocks.org/reports/internet-disrupted-in-iran-amid-mahsa-amini-protests-X8qVE8Ap

https://news.earn.com/quantifying-decentralization-e39db233c28e

Post-Quantum-Security-Team, eingerichtet im Januar 2026 unter der Leitung von Thomas Coratger. https://pq.ethereum.org

https://protocol-guild.readthedocs.io

Für detaillierte Statistiken zum Angebotswachstum siehe. https://ultrasound.money

https://vitalik.eth.limo/general/2020/10/08/rollup.html

Bericht zur Eigenkapitalverzinsung, 2024. https://www.bundesnetzagentur.de

Developer Report 2025. https://www.developerreport.com

Why Europe Needs Galileo. https://www.esa.int/Applications/Satellite_navigation/Galileo/Why_Galileo

Government. https://www.gps.gov/systems/gps/space/

IANA Functions Stewardship Transition, 2016. https://www.icann.org

Submarine Cable Map, 2025. https://www.submarinecablemap.com

Annual Review 2024. https://www.swift.com