Blockchain als neutrale Infrastruktur im regulatorischen Umfeld

Architekturprinzipien für staatlich relevante Anwendungsfälle

Working Paper – Discussion Draft - Herausgegeben vom LEA Blockchain Projekt – 17.01.2026

> *Dieses Dokument ist ein technisches und konzeptionelles Diskussionspapier.*
> *Es erhebt keinen Anspruch auf Vollständigkeit, rechtliche Bewertung oder wissenschaftliche Beweisführung.*

Abstract

Digitale Infrastrukturen stehen zunehmend im Spannungsfeld zwischen technischer Innovation und regulatorischer Realität. Insbesondere Blockchain Systeme wurden häufig unter Annahmen entwickelt, die staatlichen Anforderungen wie klare Zuständigkeiten, Haftung oder langfristige Anpassungsfähigkeit nur unzureichend berücksichtigen.

Dieses Dokument argumentiert, dass regulatorische Anschlussfähigkeit weniger von einzelnen Regeln als von grundlegenden Architekturentscheidungen abhängt. Viele bestehende Blockchain Architekturen verankern Ausführungslogik und Verantwortung auf Protokollebene und erzeugen dadurch globale Abhängigkeiten, die lokale regulatorische Anpassungen erschweren.

Das Paper beschreibt ein alternatives Architekturmodell, das einen neutralen Konsenslayer mit souveränen, anwendungsspezifischen Ausführungsdomänen kombiniert. Regulatorische Logik wird dabei konsequent auf Anwendungsebene verlagert, ohne die Stabilität der Infrastruktur zu beeinflussen.

Anhand ausgewählter staatlich relevanter Anwendungsfelder wird gezeigt, warum eine solche Trennung eine strukturelle Voraussetzung für langfristige institutionelle Nutzung darstellt.

1. Einleitung: Öffentliche Digitalisierung unter regulatorischen Bedingungen

Die Digitalisierung staatlicher Prozesse folgt anderen Gesetzmäßigkeiten als technologische Innovation im privaten oder unternehmerischen Umfeld. Während Start-ups und Technologieunternehmen häufig iterativ vorgehen, regulatorische Fragen später adressieren oder bewusst Risiken eingehen, sind öffentliche Institutionen an rechtliche Stabilität, Zuständigkeit und Nachvollziehbarkeit gebunden.

Technologien, die im staatlichen Kontext eingesetzt werden sollen, müssen nicht nur funktional sein, sondern dauerhaft belastbar. Sie müssen Haftungsfragen klären können, Datenschutz gewährleisten, langfristig wartbar sein und in bestehende institutionelle Strukturen integrierbar bleiben. Diese Anforderungen sind nicht optional und lassen sich nicht nachträglich „aufsetzen", ohne das System grundlegend zu verändern.

Blockchain-Technologien werden in politischen Debatten häufig entweder als Heilsversprechen oder als Risikoquelle diskutiert. Beide Perspektiven greifen zu kurz. **Entscheidend ist nicht, ob Blockchain grundsätzlich geeignet ist, sondern welche Art von Blockchain-Architektur mit staatlichen Rahmenbedingungen kompatibel ist.**

Dieses Paper argumentiert, dass viele der bisherigen Konflikte zwischen Blockchain und Regulierung nicht aus rechtlichen Detailfragen resultieren, sondern aus technischen Designentscheidungen**,** die implizit politische und regulatorische Konsequenzen haben.

2. Das strukturelle Spannungsfeld: Globale Systeme, nationale Regeln

Rechtssysteme sind national oder regional organisiert. Zuständigkeiten, Steuerhoheit, Datenschutzvorgaben und Haftungsfragen unterscheiden sich nicht nur zwischen Staaten, sondern teilweise auch innerhalb föderaler Systeme. Digitale Infrastrukturen hingegen sind häufig global konzipiert, homogen betrieben und technisch schwer fragmentierbar.

Blockchain-Systeme verstärken dieses Spannungsfeld. Sie sind per Definition grenzüberschreitend, konsensorientiert und darauf ausgelegt, einheitliche Regeln für alle Teilnehmer durchzusetzen. Was aus technischer Sicht als Stärke gilt, wird im regulatorischen Kontext schnell zum Problem.

Insbesondere dann, wenn:

- Ausführungslogik global festgelegt ist
- ökonomische Mechanismen für alle Anwendungen identisch sind
- Sicherheitsannahmen nur zentral verändert werden können

entstehen Abhängigkeiten, die lokale regulatorische Anpassungen erschweren oder unmöglich machen.

Der Versuch, diese Probleme durch nachgelagerte Governance-Prozesse, Ausnahmeregelungen oder juristische Konstruktionen zu lösen, führt häufig zu Unsicherheit. Technische Änderungen werden politisiert, regulatorische Eingriffe wirken systemweit, und einzelne Anwendungsfälle können das gesamte Netzwerk betreffen.

Ein zentrales Zwischenfazit lautet daher:

Je stärker Regeln technisch auf Protokollebene verankert sind, desto höher ist das regulatorische Risiko des Gesamtsystems.

3. Grenzen bestehender Blockchain-Architekturen

3.1 Monolithische Architekturen

In monolithischen Blockchain-Systemen sind Konsens, Ausführung, Sicherheitsmechanismen und ökonomische Logik eng miteinander verknüpft. Änderungen an einem dieser Elemente wirken zwangsläufig auf das gesamte Netzwerk.

Für staatliche oder regulierte Anwendungsfälle ergeben sich daraus mehrere Probleme:

- Anpassungen an rechtliche Anforderungen erfordern Protokolländerungen
- Governance-Entscheidungen werden zu systemischen Risiken
- Unterschiedliche regulatorische Bedürfnisse können nicht parallel abgebildet werden

Ein einzelner Anwendungsfall kann dadurch implizit regulatorische Folgen für alle anderen Teilnehmer erzeugen. Das erhöht nicht nur die Komplexität, sondern auch die rechtliche Unsicherheit.

3.2 Modulare Stacks und Rollup-Modelle

Modulare Blockchain-Ansätze haben wichtige Fortschritte erzielt, insbesondere im Bereich Skalierung. Durch die Trennung von Datenverfügbarkeit, Settlement und Ausführung lassen sich technische Engpässe reduzieren.

Aus regulatorischer Sicht bleiben jedoch zentrale Probleme bestehen:

- Die Ausführungslogik ist weiterhin global innerhalb eines Rollups organisiert und gilt einheitlich für alle dort betriebenen Anwendungen.
- Verantwortlichkeiten werden auf zusätzliche Ebenen ausgelagert
- Regulatorische Anpassungen erfolgen außerhalb des Basissystems

Statt Regulierung strukturell zu integrieren, wird sie häufig in separate Layer, Organisationen oder juristische Konstrukte verschoben. Dies reduziert kurzfristig Konflikte, löst aber nicht das Grundproblem klarer technischer Zuständigkeit.

3.3 Ergebnis

Sowohl monolithische als auch heutige modulare Architekturen behandeln Regulierung primär als externes Problem. Die technische Architektur selbst bleibt unverändert und zwingt regulatorische Anforderungen in nachgelagerte Strukturen.

Für staatlich relevante Anwendungsfälle ist dieser Ansatz langfristig nicht tragfähig. Er erzeugt:

- komplexe Abhängigkeiten
- schwer kalkulierbare Risiken
- und eine hohe Eintrittshürde für institutionelle Nutzung

Damit wird deutlich, dass eine alternative Herangehensweise erforderlich ist, bei der **Regulierung nicht nachträglich integriert**, sondern **architektonisch ermöglicht** wird.

4. Architektur als Regulierungsfaktor

Regulatorische Fragen werden in der technischen Diskussion häufig als nachgelagerte Probleme behandelt. In dieser Logik wird zunächst ein System gebaut und anschließend versucht, rechtliche Anforderungen durch zusätzliche Regeln, Governance Prozesse oder externe Kontrollmechanismen abzubilden. Diese Vorgehensweise verkennt jedoch, dass technische Architektur selbst bereits normative Wirkung entfaltet.

Sie legt fest, ob Zuständigkeiten klar trennbar sind oder ob Änderungen zwangsläufig systemweite Folgen haben. In diesem Sinne ist Architektur kein neutraler Hintergrund, sondern ein strukturierender Rahmen für regulatorische Handlungsfähigkeit.

In Blockchain Systemen wird dieser Zusammenhang besonders deutlich. Wenn Ausführungslogik, Sicherheitsannahmen und ökonomische Regeln auf Protokollebene festgeschrieben sind, dann werden regulatorische Anpassungen zwangsläufig zu Eingriffen in den Kern des Systems. Jede Änderung erzeugt Unsicherheit für alle Teilnehmer, unabhängig davon, ob sie vom konkreten Anwendungsfall betroffen sind oder nicht.

Ein solches Design erzeugt zwei problematische Effekte. Erstens werden regulatorische Anforderungen als Risiko für die Stabilität des Netzwerks wahrgenommen. Zweitens entsteht ein politischer Druck, technische Weiterentwicklung zu bremsen oder vollständig zu vermeiden. Beides steht im Widerspruch zu den Anforderungen öffentlicher Digitalisierung, die auf langfristige Stabilität und kontrollierte Anpassungsfähigkeit angewiesen ist.

Eine regulatorisch anschlussfähige Architektur muss daher drei Eigenschaften erfüllen. Sie muss neutral gegenüber Anwendungslogik sein. Sie muss Verantwortlichkeiten klar trennen können. Und sie muss lokale Anpassungen ermöglichen, ohne globale Effekte auszulösen.

Diese Eigenschaften lassen sich nicht durch Policy oder Governance allein herstellen. Sie sind das Ergebnis bewusster architektonischer Trennung zwischen Ordnung und Bedeutung, zwischen Infrastruktur und Anwendung.

5. Referenzarchitektur: Neutraler Konsens und souveräne Ausführungsdomänen

Ausgehend von den beschriebenen Anforderungen lässt sich eine Referenzarchitektur formulieren, die staatlich relevante Anwendungsfälle nicht behindert, sondern strukturell ermöglicht. Der zentrale Gedanke besteht in der konsequenten Trennung zwischen einem neutralen Basissystem und anwendungsspezifischer Logik.

Der Konsenslayer erfüllt dabei ausschließlich infrastrukturelle Aufgaben. Er stellt sicher, dass Transaktionen eindeutig geordnet werden, dass Finalität hergestellt wird und dass relevante Daten verfügbar bleiben. Er interpretiert keine Inhalte, bewertet keine Regeln und kennt keine Anwendungslogik. In diesem Sinne fungiert er als neutrale Ordnungsschicht.

Alle inhaltlichen Entscheidungen werden in separaten Ausführungsdomänen getroffen. Diese Domänen sind anwendungsspezifisch, technisch klar abgegrenzt und tragen die volle Verantwortung für ihre Regeln. Sie definieren, welche Transaktionen gültig sind, welche Signaturen akzeptiert werden, wie Gebühren erhoben werden und welche regulatorischen Anforderungen gelten.

In der LEA Blockchain wird dieses Modell durch sogenannte PODs umgesetzt. PODs (Programmable Object Domains) sind souveräne Ausführungsdomänen, die Anwendungslogik, Prüfregeln und Zuständigkeiten in klar abgegrenzten technischen Einheiten kapseln.

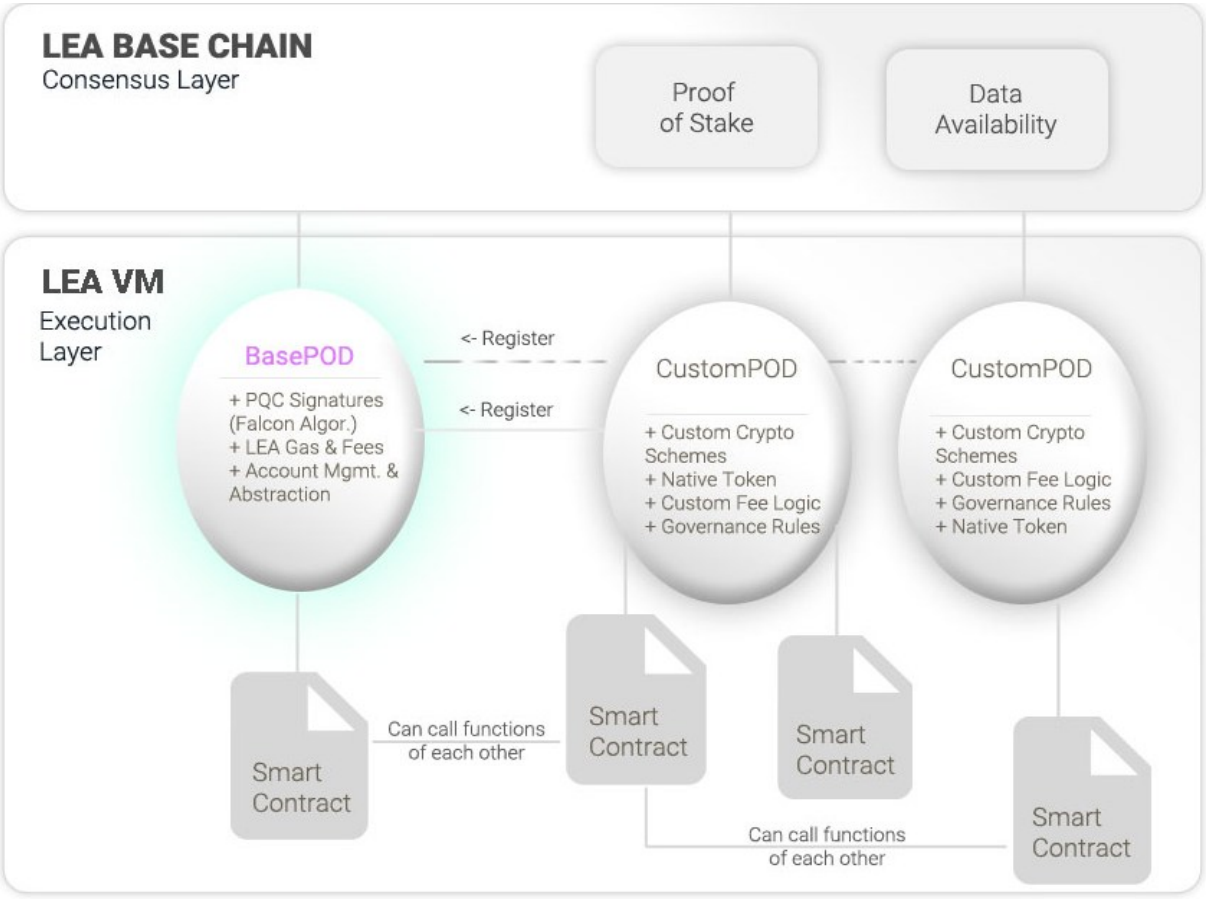

Abbildung 1 LEA Grobarchitektur und Programmable Object Domains (PODs)

Diese Ausführungsdomänen sind souverän im technischen Sinn und können unabhängig voneinander gestaltet, angepasst und weiterentwickelt werden. Änderungen innerhalb einer Domäne haben keine Auswirkungen auf andere Domänen oder auf den Konsenslayer. Dadurch wird lokale Anpassungsfähigkeit möglich, ohne globale Instabilität zu erzeugen.

Ein solches Modell erlaubt es, sehr unterschiedliche Anwendungsfälle auf derselben Infrastruktur zu betreiben. Regulierungsnahe Anwendungen können strenge Anforderungen umsetzen, während andere Domänen bewusst offen gestaltet bleiben. Beide nutzen dieselbe Ordnungsschicht, teilen sich dieselbe Finalität und profitieren von derselben infrastrukturellen Sicherheit, ohne sich gegenseitig zu beeinflussen.

Diese Architektur schafft klare Verantwortlichkeiten. Der Betreiber einer Ausführungsdomäne ist für deren Regeln verantwortlich. Regulatorische Anforderungen lassen sich eindeutig zuordnen, technisch überprüfen

und bei Bedarf ändern. Das Basissystem bleibt davon unberührt und behält seine Neutralität.

Die beschriebene Referenzarchitektur findet sich konkret in der LEA Blockchain wieder. LEA implementiert einen minimalen Konsenslayer, der ausschließlich für Ordnung und Verfügbarkeit zuständig ist. Sämtliche Ausführungslogik ist in klar abgegrenzte Ausführungsdomänen ausgelagert, die technisch als eigenständige Einheiten betrieben werden.

Dabei ist entscheidend, dass LEA keine regulatorischen Vorgaben vorgibt. Das System erzwingt weder Offenheit noch Einschränkung. Es stellt lediglich die strukturellen Voraussetzungen bereit, um regulatorische Anforderungen dort umzusetzen, wo sie hingehören, nämlich auf Anwendungsebene.

Damit unterscheidet sich dieser Ansatz grundlegend von Systemen, die versuchen, regulatorische Fragen durch globale Regeln oder nachträgliche Einschränkungen zu adressieren. Stattdessen wird Regulierung als legitimer Bestandteil einzelner Anwendungsdomänen verstanden, ohne den Charakter der Infrastruktur zu verändern.

6. Staatlich relevante Anwendungsfelder als architektonische Prüfsteine

Die Tragfähigkeit einer technischen Architektur zeigt sich nicht an abstrakten Leistungskennzahlen, sondern an ihrer Eignung für reale institutionelle Problemstellungen. In diesem Kapitel werden fünf Anwendungsfelder betrachtet, die aktuell politische und administrative Relevanz besitzen. Ziel ist keine Bewertung einzelner Maßnahmen, sondern eine strukturelle Einordnung der architektonischen Anforderungen.

Jedes Unterkapitel folgt derselben Logik. Zunächst wird das zugrundeliegende Problem beschrieben. Anschließend werden die architektonischen Anforderungen abgeleitet, die sich daraus ergeben. Abschließend wird eingeordnet, wie ein Modell aus neutralem Konsens und souveränen Ausführungsdomänen diese Anforderungen adressieren kann.

6.1 Umsatzsteuer und Steuerbetrug

Umsatzsteuerbetrug zählt seit Jahren zu den größten fiskalischen Schadensfeldern. Die zugrundeliegenden Mechanismen sind bekannt. Komplexe Lieferketten, grenzüberschreitende Transaktionen und zeitverzögerte Prüfprozesse schaffen Spielräume für Manipulation. Ein zentrales Problem besteht darin, dass steuerrelevante Informationen fragmentiert vorliegen und häufig erst ex post geprüft werden können.

Aus architektonischer Sicht ergibt sich daraus eine klare Anforderung. Steuerlich relevante Ereignisse müssen nachvollziehbar, zeitlich eindeutig und maschinenlesbar dokumentiert werden, ohne dabei Geschäftsgeheimnisse oder personenbezogene Daten offenzulegen. Gleichzeitig muss klar sein, wer für die Richtigkeit dieser Informationen verantwortlich ist.

Eine souveräne Ausführungsdomäne kann genau an dieser Stelle ansetzen. Sie bildet nicht den gesamten Geschäftsprozess ab, sondern ausschließlich steuerlich relevante Ereignisse. Rechnungen, Lieferungen oder Leistungszeitpunkte werden als überprüfbare Referenzen verankert, während die inhaltlichen Details außerhalb der Infrastruktur verbleiben. Prüfregeln können direkt in der Ausführungslogik implementiert werden, ohne Auswirkungen auf andere Anwendungen.

Der entscheidende Punkt ist die Trennung zwischen Infrastruktur und Steuerlogik. Der Konsenslayer stellt lediglich sicher, dass Ereignisse eindeutig geordnet und unveränderlich dokumentiert sind. Die steuerliche Interpretation liegt vollständig bei der jeweiligen Domäne und ihrem Betreiber.

6.2 Verifizierbare Fakten im Kontext zunehmender KI Nutzung

Mit der zunehmenden Verbreitung generativer KI Systeme verschiebt sich die gesellschaftliche Frage von der Erzeugung von Inhalten hin zur Überprüfbarkeit ihrer Herkunft. Für staatliche Institutionen stellt sich nicht die Aufgabe, Inhalte zu bewerten, sondern festzustellen, wann und unter welchen Bedingungen bestimmte Informationen entstanden sind und ob sie nachträglich verändert wurden.

Architektonisch ergibt sich daraus eine wichtige Unterscheidung. Nicht der Inhalt selbst muss öffentlich gespeichert werden, sondern der Nachweis seiner Integrität. Systeme, die beides vermischen, erzeugen entweder Datenschutzprobleme oder unnötige Offenlegung.

Eine eigenständige Ausführungsdomäne kann als Integritätslayer fungieren. Dokumente, Aussagen oder KI generierte Ergebnisse werden kryptografisch referenziert und zeitlich verankert, ohne dass ihr Inhalt öffentlich sichtbar wird. Mehrere vertrauenswürdige Akteure können als Herausgeber oder Bestätiger auftreten, ohne eine zentrale Instanz zu bilden.

Auch hier bleibt der Konsenslayer neutral. Er entscheidet nicht über Wahrheit oder Relevanz. Er stellt lediglich die zeitliche Ordnung und Unveränderlichkeit sicher. Die Bedeutung der verankerten Referenzen wird ausschließlich auf Anwendungsebene definiert.

6.3 Entstehende AI Ökonomien und steuerliche Zurechnung

Mit dem Einsatz autonomer oder teilautonomer KI Systeme entstehen neue ökonomische Strukturen. KI gesteuerte Prozesse können Umsätze generieren, Verträge auslösen oder Dienstleistungen erbringen. Das bestehende Steuerrecht ist auf solche Konstellationen nur begrenzt vorbereitet.

Aus technischer Sicht ist jedoch bereits heute entscheidend, dass Verantwortlichkeiten eindeutig abgebildet werden können. Wer betreibt das System, wem werden Umsätze zugerechnet, wer trägt die steuerliche Verantwortung. Wenn diese Fragen technisch nicht sauber lösbar sind, wird jede spätere Regulierung erheblich erschwert.

Eine souveräne Ausführungsdomäne erlaubt es, KI basierte Prozesse eindeutig einem Betreiber oder einer juristischen Einheit zuzuordnen. Einnahmenflüsse werden technisch nachvollziehbar erfasst, ohne dass das Basissystem Annahmen über deren rechtliche Bewertung trifft. Änderungen an regulatorischen Vorgaben können innerhalb der Domäne umgesetzt werden, ohne dass die Infrastruktur angepasst werden muss.

Damit wird kein regulatorisches Problem gelöst, aber ein strukturelles Hindernis vermieden. Die Technik verhindert nicht die Anwendung von Recht, sondern ermöglicht sie.

6.4 Entwicklungszusammenarbeit und staatliche Transfers

In der Entwicklungszusammenarbeit spielen Transparenz, Nachvollziehbarkeit und Kostenkontrolle eine zentrale Rolle. Gleichzeitig bestehen berechtigte Sicherheitsbedenken hinsichtlich der Offenlegung operativer Details. Klassische Systeme erzeugen entweder Intransparenz oder neue Abhängigkeiten von zentralen Akteuren.

Aus architektonischer Sicht ist hier entscheidend, dass Mittelbewegungen nachvollziehbar sind, ohne sensible Kontextinformationen offenzulegen. Zweckbindungen müssen überprüfbar sein, ohne operative Freiheit einzuschränken.

Eine eigenständige Ausführungsdomäne kann Transfers als überprüfbare Zustandsänderungen abbilden. Mittelzuweisungen, Zweckbindungen und Abrufe werden technisch nachvollziehbar, während Details zur operativen Umsetzung außerhalb des Systems verbleiben. Unterschiedliche Rollen können klar voneinander getrennt werden, ohne dass eine zentrale Kontrollinstanz erforderlich ist.

Der Konsenslayer fungiert ausschließlich als neutrale Ordnungsschicht. Politische oder operative Bewertungen finden nicht statt.

6.5 Digitale Nachweise zwischen Nutzbarkeit und Datenschutz

Digitale Nachweise wie Zeugnisse, Zertifikate oder Berechtigungen gewinnen an Bedeutung. Gleichzeitig bestehen hohe Anforderungen an Datenschutz, Widerrufbarkeit und Zweckbindung. Eine vollständige Speicherung personenbezogener Daten in unveränderlichen Systemen ist mit diesen Anforderungen nicht vereinbar.

Die architektonische Lösung liegt in der klaren Trennung zwischen Nachweis und Inhalt. Eine Ausführungsdomäne kann bestätigen, dass ein bestimmter Nachweis existiert, gültig ist oder widerrufen wurde, ohne personenbezogene Daten öffentlich zu machen. Gültigkeitszeiträume, Aktualisierungen und Widerrufe lassen sich technisch sauber abbilden.

Auch hier gilt, dass der Konsenslayer keinerlei Kenntnis über den Inhalt der Nachweise hat. Er stellt lediglich die Integrität der Zustandsänderungen sicher. Datenschutz wird nicht umgangen, sondern architektonisch berücksichtigt.

Zwischenfazit

Die betrachteten Anwendungsfelder unterscheiden sich erheblich in ihrer fachlichen Ausprägung. Gemeinsam ist ihnen jedoch eine zentrale Anforderung. Regulatorische Logik muss lokal umsetzbar sein, ohne die Stabilität einer gemeinsamen Infrastruktur zu gefährden.

Eine Architektur aus neutralem Konsens und souveränen Ausführungsdomänen erfüllt diese Anforderung strukturell. Sie ersetzt keine rechtlichen Prozesse und trifft keine politischen Entscheidungen. Sie stellt jedoch die technische Voraussetzung bereit, um staatlich relevante Anwendungsfälle überhaupt realistisch abbilden zu können.

7. Abgrenzung und bewusste Nichtziele der Architektur

Eine klare Abgrenzung ist notwendig, um Fehlannahmen zu vermeiden und die Rolle technischer Infrastruktur realistisch einzuordnen. Die in diesem Paper beschriebene Architektur versteht sich ausdrücklich nicht

als rechtliches, politisches oder administratives Instrument, sondern als technische Grundlage, die bestimmte Handlungsoptionen ermöglicht oder verhindert.

Die Architektur trifft keine rechtlichen Bewertungen. Sie entscheidet nicht darüber, welche Regeln gelten sollen, sondern schafft lediglich die strukturellen Voraussetzungen, damit unterschiedliche Regeln technisch sauber umgesetzt werden können. Die Verantwortung für inhaltliche Vorgaben liegt stets bei den jeweiligen Betreibern der Ausführungsdomänen und den zuständigen Institutionen.

Ebenso ersetzt die Architektur keine staatlichen Prozesse. Steuerprüfung, Aufsicht, Genehmigung oder Durchsetzung bleiben Aufgaben öffentlicher Stellen. Die technische Infrastruktur kann diese Prozesse unterstützen, aber nicht automatisieren oder substituieren.

Die Architektur ist auch kein Instrument zur Durchsetzung politischer Kontrolle. Der neutrale Konsenslayer bewertet keine Inhalte, priorisiert keine Anwendungsfälle und greift nicht in Ausführungslogik ein. Er ist bewusst inhaltsagnostisch gestaltet, um seine Rolle als öffentliche Infrastruktur langfristig erfüllen zu können.

Schließlich ist die Architektur kein Garant für Compliance. Sie verhindert keine Fehlanwendung und ersetzt keine Governance. Sie reduziert jedoch strukturelle Risiken, indem sie regulatorische Anpassungen lokal begrenzt und systemweite Effekte vermeidet.

Diese bewussten Nichtziele sind zentral für die Einordnung der Architektur. Sie begrenzen Erwartungen und erhöhen zugleich ihre langfristige Anschlussfähigkeit.

8. Blockchain als öffentliche Infrastruktur

Öffentliche Infrastrukturen zeichnen sich durch bestimmte Eigenschaften aus. Sie müssen stabil sein, langfristig nutzbar bleiben und unabhängig von einzelnen Anwendungsfällen funktionieren. Gleichzeitig müssen sie flexibel genug sein, um neue Anforderungen aufnehmen zu können, ohne ihre Grundstruktur ständig zu verändern.

Historische Beispiele zeigen, dass Infrastrukturen dann scheitern, wenn sie zu stark auf spezifische Nutzungsszenarien zugeschnitten sind. Erfolgreich sind jene Systeme, die klare Trennlinien zwischen Infrastruktur und Nutzung ziehen.

Überträgt man diese Perspektive auf Blockchain Systeme, wird deutlich, dass viele bestehende Architekturen ihre infrastrukturelle Rolle nicht konsequent einnehmen. Sie verbinden Ordnung mit inhaltlichen Annahmen und werden dadurch anfällig für politische und regulatorische Veränderungen. Eine klar getrennte Infrastruktur vermeidet diese Kopplung und bleibt langfristig anpassungsfähig. Für staatliche Kontexte ist diese Unterscheidung entscheidend. Nur wenn die Infrastruktur selbst neutral bleibt, kann sie in unterschiedlichen politischen und rechtlichen Rahmenbedingungen eingesetzt werden. Nur wenn Anpassungen lokal möglich sind, bleibt das System langfristig tragfähig.

In diesem Sinne ist die hier beschriebene Architektur weniger eine technologische Innovation als eine strukturelle Voraussetzung für nachhaltige Nutzung.

9. Fazit

Die Diskussion um Blockchain und staatliche Nutzung wird häufig entlang einzelner Anwendungsfälle oder regulatorischer Detailfragen geführt. Dieses Paper vertritt eine andere Perspektive. Es argumentiert, dass die entscheidende Frage auf der Ebene der Architektur liegt.

Technische Systeme legen fest, welche Formen von Regulierung möglich sind und welche nicht. Wenn Ausführungslogik global verankert ist, wird Regulierung zum Systemrisiko. Wenn Verantwortung nicht klar trennbar ist, entsteht Unsicherheit. Wenn Anpassungen nur durch Eingriffe in den Kern möglich sind, wird technischer Fortschritt politisiert.

Eine Architektur, die Ordnung und Ausführung konsequent trennt, adressiert diese Probleme strukturell. Sie ermöglicht regulatorische Vielfalt, ohne die Stabilität der Infrastruktur zu gefährden. Sie schafft klare Verantwortlichkeiten, ohne zentrale Kontrolle zu erzwingen. Und sie erlaubt Innovation, ohne institutionelle Anforderungen zu unterlaufen.

Die Frage ist daher nicht, ob Blockchain für staatliche Anwendungsfälle geeignet ist. Die Frage ist, welche Architekturen staatliche Nutzung überhaupt zulassen.

Glossar

Das folgende Glossar dient der Klarstellung zentraler Begriffe, wie sie in diesem Dokument verwendet werden. Es erhebt keinen Anspruch auf allgemeingültige Definitionen außerhalb dieses Kontexts.

Anwendungslogik	Die innerhalb einer Ausführungsdomäne definierten Regeln und Prüfmechanismen, die deren fachlichen Zweck bestimmen. Die Anwendungslogik ist vom Konsenslayer getrennt.
Ausführungsdomäne	Ein klar abgegrenzter technischer Anwendungsraum innerhalb einer Blockchain Architektur mit eigener Logik und Zuständigkeit. Ausführungsdomänen sind unabhängig voneinander gestaltbar.
Blockchain	Eine digitale Infrastruktur zur geordneten und unveränderlichen Dokumentation von Zustandsänderungen. In diesem Dokument als neutrale Ordnungsschicht verstanden, nicht als Anwendung oder Finanzinstrument.
Finalität	Der Zustand, in dem eine Transaktion oder Zustandsänderung als endgültig gilt und nicht mehr rückgängig gemacht werden kann.
Integritätsnachweis	Ein technischer Beleg dafür, dass ein Zustand oder Dokument zu einem bestimmten Zeitpunkt existierte und seitdem unverändert geblieben ist.
Konsenslayer	Die Basisschicht eines Blockchain Systems, die für Ordnung, Finalität und Datenverfügbarkeit zuständig ist und keine Anwendungslogik interpretiert.
Neutralität der Infrastruktur	Das Prinzip, dass die Basisschicht eines Systems keine inhaltlichen oder regulatorischen Annahmen trifft und keine Anwendungen bevorzugt.
PODs Programmable Object Domains	Projektspezifischer Begriff für souveräne Ausführungsdomänen innerhalb der LEA Architektur. PODs kapseln Anwendungslogik und Zuständigkeiten in eigenständigen technischen Einheiten.

Regulatorische Anschlussfähigkeit	Die Fähigkeit eines technischen Systems, regulatorische Anforderungen umzusetzen, ohne Änderungen an der grundlegenden Infrastruktur zu erfordern.
Rollup	Ein separates Ausführungssystem, in dem Transaktionen außerhalb einer Basischain verarbeitet und gebündelt auf dieser dokumentiert werden, primär zur Skalierung.
Souveränität einer Ausführungsdomäne	Die Fähigkeit einer Ausführungsdomäne oder POD, ihre Regeln und Anpassungen unabhängig vom Basissystem zu verändern.
Transaktionsordnung	Die eindeutige zeitliche Reihenfolge von Zustandsänderungen, bereitgestellt durch den Konsenslayer.
Zuständigkeit	Die klar zuordenbare Verantwortung für Regeln und Entscheidungen innerhalb einer Ausführungsdomäne.

Literatur und weiterführende Grundlagen

Lessig, Lawrence (1999).
Code and Other Laws of Cyberspace. Harvard University Press.

Yeung, Karen (2018).
Algorithmic regulation: A critical interrogation.
Regulation & Governance, 12(4), 505–523.

Brownsword, Roger (2019).
Law, Technology and Society. Routledge.

Werbach, Kevin (2018).
The Blockchain and the New Architecture of Trust. MIT Press.

De Filippi, Primavera; Wright, Aaron (2018).
Blockchain and the Law: The Rule of Code. Harvard University Press.

Buterin, Vitalik (2017).
On-chain governance: Why it's hard. Ethereum Research.

Buterin, Vitalik (2021).
A rollup-centric Ethereum roadmap. Ethereum Foundation.

Al-Bassam, Mustafa et al. (2018).
Fraud proofs: Maximising light client security and scaling blockchains with dishonest majorities.
IEEE Symposium on Security and Privacy.

OECD (2017).
Technology Tools to Tackle Tax Evasion and Tax Fraud. OECD Publishing.

OECD (2020).
The OECD Digital Government Policy Framework. OECD Publishing.

European Commission (2019).
VAT Fraud and the Digital Economy. Publications Office of the European Union.

Finck, Michèle (2018).
Blockchain and the General Data Protection Regulation.
European Parliament Study.

W3C (2022).
Decentralized Identifiers (DIDs) and Verifiable Credentials.
World Wide Web Consortium Recommendation.

World Economic Forum (2020).
Blockchain Deployment Toolkit for Governments.

Mazzucato, Mariana (2018).
The Value of Everything. Penguin Random House.

LEA

LEA ist ein Blockchain Infrastrukturprojekt mit Fokus auf modulare Ausführungsdomänen und regulatorische Anschlussfähigkeit. Das Projekt entwickelt eine neutrale Konsensschicht für staatlich und institutionell relevante Anwendungen.

Website: https://getlea.org
Kontakt: info@getlea.org
Version: Discussion Draft 1.0
Stand: Januar 2026