PROGRAMM DRX — UNABHÄNGIGE DRACHME

GRIECHISCHE INITIATIVE FÜR WÄHRUNGSTECHNOLOGIE

Whitepaper und Ministerialdossier

PROGRAMM DRX — UNABHÄNGIGE DRACHME · dig Δραχμή (ΔPAX)

Vendetta Labs · Gio (Kaspartizan)

September 2026

WHITEPAPER UND MINISTERIALDOSSIER · ÖFFENTLICHE FORSCHUNGSFASSUNG · VERSION 0.9

Adressat: Hellenisches Ministerium für Nationale Wirtschaft und Finanzen
Dokumenttyp: Vorläufige Machbarkeitsstudie; keine Rechtsberatung, kein Emissionsbeschluss und keine Empfehlung zum Austritt aus der Eurozone
Entscheidungsgegenstand: Genehmigung einer begrenzten Phase-0-Studie und eines wertlosen Testnet-Prototyps

> **Prüfsatz:** Ein Fischer auf Kalymnos erhält am Sonntag eine ΔPAX-Banknote, zahlt sie am Montag bei einer Bank ein und erhält denselben Nominalbetrag digital. Weder die Bank noch ein Ministerium können dadurch zusätzliche ΔPAX erzeugen, eine fremde Self-Custody-Wallet einfrieren oder die verfassungsmäßige Maximalmenge ändern.

Veröffentlichungsstatus: Öffentliche Forschungsfassung einer privaten Initiative von Vendetta Labs. Nicht staatlich beauftragt, genehmigt oder gebilligt. Rechtliche, makroökonomische und kryptographische Gegenprüfung steht aus.

Inhaltsverzeichnis

0. Executive One-Pager

0.1 Was vorgeschlagen wird

ΔPAX ist eine eigenständige Rechnungseinheit mit drei gleichrangigen Trägerformen: on-chain Bearer Value, vorfinanzierter Offline-Wert in zertifizierten Secure Elements sowie Banknoten und Münzen. Alle Formen gehören zu **einer** Geldmenge. Papier und Metall sind keine zweite Währung und kein Anspruch auf einen zusätzlichen Token. Jede physische Ausgabe setzt voraus, dass derselbe Nominalbetrag digital in einem öffentlich prüfbaren CashLot-Covenant gesperrt wurde.

Der digitale Kern soll auf **Kaspa Toccata** als UTXO-nativer Covenant-Familie prototypisiert werden. ΔPAX ist dabei weder KAS noch ein KAS-Fork noch ein Wrapped Token. KAS dient in der ersten Architektur nur als Netzwerkgebühr und Sicherheitsasset. Die Geldordnung selbst wird durch konservierende UTXO-Übergänge, eine vorab definierte Maximalmenge und einen öffentlich nachweisbaren Genesis-Sunset bestimmt.

0.2 Was ausdrücklich nicht vorgeschlagen wird

- keine CBDC mit Bürgerkonten bei einer Zentralbank;
- kein Peg zu EUR oder USD und kein offizielles Peg-Stability-Modul;
- kein Minting gegen USDC, USDT, EURC oder Bankguthaben;
- keine diskretionäre Geldschöpfung durch Regierung, Bank oder Governance;
- kein Versprechen völlig anonymer Intermediärdienste oder trustloser Offline-Finalität;
- keine Behauptung, andere Staaten, Börsen oder Banken könnten ΔPAX nicht ausschließen;
- keine Einführung als gesetzliches Zahlungsmittel innerhalb der Eurozone im Rahmen von Phase 0.

0.3 Empfohlene Entscheidung

Genehmigt werden soll ausschließlich eine **12- bis 18-monatige Phase 0** mit einem Budgetkorridor von **0,95 bis 1,65 Mio. Euro** und einer beantragten Obergrenze von **1,6 Mio. Euro**: Rechtsgutachten, makroökonomische Simulationen, ein wertloser Kaspa-Testnet-Prototyp, CashLot- und Offline-Labormodelle sowie unabhängige Security Reviews. Weder Mainnet-Wert noch Banknoten mit Nennwert noch Steuerannahme sind Teil dieser Freigabe.

0.4 Zehn Verfassungsregeln

1. **Eine Einheit, eine Geldmenge:** S = D + P + O + E.

2. **Harte Obergrenze:** S ≤ Mmax; kein Notfall-Mint.
3. **Formwechsel ohne Schöpfung:** Digital, offline, Note und Münze verändern S nicht.
4. **Keine Freeze-Funktion im Kern:** Self-Custody-Bestände sind nicht administrativ sperrbar.
5. **Keine Fiat-Bindung:** Wechselkurse entstehen am freien Markt.
6. **Keine Oracle-Abhängigkeit im monetären Kern:** Preise beeinflussen weder Existenz noch Menge von ΔPAX.
7. **Genesis Steward auf Zeit:** privilegierte Rechte verfallen technisch und öffentlich nachprüfbar.
8. **Physischer Arm ist institutionell, aber vollständig gedeckt:** jeder physische Nominalwert entspricht einem gesperrten digitalen Nominalwert.
9. **Intermediäre erfüllen Rechtspflichten:** AML, Verbraucherschutz und Aufsicht gelten an Verwahrungs-, Wechsel- und Ausgabestellen.
10. **Keine Souveränitätsrhetorik ohne Exit-Test:** Abhängigkeiten von Kaspa, KAS-Gebühren, Wallets und Secure-Element-Lieferketten werden gemessen und mit Migrationspfaden versehen.

1. Auftrag, Annahmen und Entscheidungshorizont

1.1 Auftrag

Diese Studie untersucht, ob ein Staat eine harte digitale Landeswährung starten kann, deren tägliche Nutzung zugleich in Self-Custody, offline, als Banknote und als Münze möglich ist, ohne dass eine Zentralbank oder Regierung nach dem Genesis-Zeitfenster Konten sperren oder die Geldmenge diskretionär erhöhen kann. Griechenland dient als konkreter Anwendungsfall. Das Dokument unterscheidet strikt zwischen technischer Machbarkeit, heutiger Eurozonen-Rechtslage und einem nur bei vollständiger Währungssouveränität relevanten Legal-Tender-Szenario.

1.2 Gesetzte Annahmen

- **A1:** Der Staat will Transparenz, Regelbindung und technische Selbstbeschränkung stärker gewichten als kurzfristige geldpolitische Flexibilität.
- **A2:** Bürger dürfen digitale ΔPAX selbst verwahren. Banken und Wallet-Anbieter bleiben optionale Dienstleister.
- **A3:** Ein physischer Träger erfordert zwangsläufig vertrauenswürdige Ausgabestellen, Druckereien, Münzstätten, Echtheitsprüfung und Vernichtungskontrollen.
- **A4:** Kaspa Toccata ist seit 30. Juni 2026 auf Mainnet aktiv; Compiler-, Wallet-, Indexer- und Audit-Reife sind dennoch junge und zu prüfende Abhängigkeiten.
- **A5:** Die Eurozone bleibt in Phase 0 und jedem freiwilligen Forschungs-/Komplementärpilot der geltende Rechtsrahmen.
- **A6:** Volle gesetzliche Annahmepflicht, nationale Banknoten mit Legal-Tender-Status und Steuerdenomination in ΔPAX werden nur im souveränen Szenario untersucht.
- **A7:** Zahlen in diesem Entwurf sind Planungsparameter. Sie werden erst nach Simulation, Rechtsgutachten und öffentlicher Konsultation normativ.

1.3 Zentrale Zielkonflikte

Härte gegen Krisenelastizität. Eine unveränderliche Maximalmenge schützt gegen politische Verwässerung, nimmt dem Staat aber das klassische Instrument des Lender of Last Resort. Das System muss deshalb mit 100%-Reserve-Zahlungskonten, vorfinanzierten Liquiditätspuffern, geordneten Insolvenzen und expliziten Stop-Kriterien arbeiten.

Dezentralität gegen physisches Bargeld. Digitaler Bearer Value kann weitgehend regelbasiert sein. Papier und Metall benötigen physische Institutionen. Die Lösung ist nicht, diese Vertrauenszone zu

leugnen, sondern sie eng zu begrenzen, zu besichern, lückenlos zu auditieren und vom Recht zur Geldschöpfung zu trennen.

Souveränität gegen offene Weltwirtschaft. Ein offenes globales Netzwerk reduziert nationale Zensur- und Betreiberabhängigkeit, schafft aber Abhängigkeit von fremden Minern, KAS-Gebühren, Netzwerk-Upgrades und globaler Liquidität. Souveränität wird deshalb als Fähigkeit zu überprüfen, zu migrieren und rechtlich selbst zu entscheiden definiert - nicht als technische Autarkiebehauptung.

1.4 Entscheidungshorizonte

Horizont	Erlaubte Aussage	Ausdrücklich nicht enthalten
Phase 0, 0-18 Monate	Forschung, Simulation, Testnet, Rechtsprüfung	Geldwert, Mainnet, Annahmepflicht, Steuerannahme
Optionaler Eurozonen-Pilot	freiwillige, begrenzte Komplementärnutzung nach Freigabe	nationales Legal Tender, Zwangslohn, Ersatz des Euro
Souveränes Szenario	vollständige Währungs-, Banken- und Bargeldordnung	Empfehlung oder Automatismus zum Grexit

2. Monetäre Verfassung

2.1 Die Einheit

Eine ΔPAX ist eine nominell identische Einheit unabhängig davon, ob sie als on-chain UTXO, Offline-Claim, Banknote oder Münze gehalten wird. Die Einheit ist **nicht** definiert als Anspruch auf einen Euro, Dollar, Bitcoin oder Goldbetrag. Ihr Wechselkurs wird frei gebildet. Ihre monetäre Härte folgt aus Menge, Konvertibilität zwischen Trägerformen, transparenter Fiskalannahme im souveränen Szenario und glaubwürdiger Rechtsordnung - nicht aus einem Peg.

2.2 Geldmengenidentität

Zu jedem finalisierten Block gilt:

$S(t) = D(t) + P(t) + O(t) + E(t)$

mit:

- D: frei digital umlaufende ΔPAX;
- P: in CashLots gesperrte digitale ΔPAX, die ausgegebenen Banknoten und Münzen entsprechen;
- O: in OfflineLock-Covenants gesperrte ΔPAX;
- E: eng definierte Sonderzustände, etwa rechtshängige Vernichtungs- oder Wiederherstellungsverfahren;
- S: gesamte existente Geldmenge.

Für jede Transaktion muss gelten: Inputs + zulässige Emission = Outputs + nachweislicher Burn. Formwechsel verändern S nicht. Ein öffentlicher Supply-Indexer rekonstruiert D, P, O und E unabhängig von Ministerium, Bank oder Wallet-Frontend.

2.3 Genesis und Maximalmenge

Arbeitsparameter für die Simulation:

- M0 = 90.000.000.000 ΔPAX Genesis-Nominalmenge;
- Rmax = 9.000.000.000 ΔPAX maximaler, ausschließlich für Netzwerksicherheit und öffentliche Infrastruktur kodierter Emissionskorridor;
- Mmax = 99.000.000.000 ΔPAX absolute Obergrenze;
- R wird blockzeitgebunden in Vierjahres-Epochen halbiert und kann nicht beschleunigt oder umgewidmet werden;

- nicht abgerufene Epochenansprüche verfallen, statt in spätere Epochen übertragen zu werden;
- nach Ausschöpfung oder Ablauf ist jede weitere Emission konsensuswidrig.

Diese Zahlen sind **keine politische Empfehlung**, sondern ein vollständiger Satz simulierbarer Parameter. Eine Alternative mit Rmax = 0 muss gleichberechtigt getestet werden. Die Security-Tranche ist ein ex ante politischer Verteilungsentscheid und darf nicht als „rein technisch“ verschleiert werden.

2.4 Genesis-Verteilung

Zweck	Anteil an M0	Sperrlogik
Bürgerische Grundzuteilung	34 %	claim-basiert, zeitlich gestaffelt, nicht übertragbare Anspruchsprüfung
Umtausch-/Liquiditätsreserve für souveränen Start	22 %	öffentliches Treasury ohne Mint-Recht, mehrjährige Ausgaberegeln
Banknoten- und Münz-CashLots	12 %	nur gegen physische Ausgabe, ungenutzte Lots bleiben gesperrt
Öffentliche Löhne/Leistungen - freiwillige Quote	10 %	nur nach Legal-Tender-Gesetz und Wahlrecht des Empfängers
Infrastruktur und Sicherheitsfonds	8 %	Timelock, zweckgebunden, öffentliches Budget
Insel-/Hafenpilot	4 %	lokale Caps, Rückabwicklungsklausel
Diaspora- und Exportliquidität	4 %	transparente Auktionen, keine Wechselkursgarantie
Strategische Notfallliquidität	4 %	keine Geldschöpfung; nur bereits existente Einheiten
Forschung, Audit und Bug Bounty	2 %	Meilenstein-Vesting

Jede Zuteilung ist on-chain vorab sichtbar. Kein Empfänger erhält ein Protokollrecht zur weiteren Prägung.

2.5 Wertstabilität ohne Peg

Das System verspricht keine feste Kaufkraft. Ein amtlicher **ΔPAX-Kaufkraftindex** kann Brot, Strom, Fähre, Olivenöl, Miete und Diesel abbilden, dient aber nur der Statistik, Lohn- und Vertragsindexierung. Er darf weder automatische Geldschöpfung noch Einlösung gegen einen Fiatkorb auslösen. So bleibt die Währung fiat-ungebunden, während Regierung, Tarifpartner und Haushalte reale Kaufkraft beobachten können.

2.6 Seigniorage

Seigniorage entsteht nur bei Genesis und bei der kodierten Security-Tranche. Sie wird nicht als laufende Regierungseinnahme behandelt. Gewinne aus Ausgabe, verlorenen physischen Trägern oder Gebühren fließen in einen getrennten, öffentlich bilanzierten Infrastruktur- und Verlustausgleichsfonds. Die Regierung darf Budgetdefizite nicht durch Protokollprägung finanzieren.

3. Technische Architektur auf Kaspa Toccata

3.1 Warum Kaspa Toccata

Toccata erweitert Kaspa um UTXO-native Covenants, Transaction v1, Script Pricing, Inline-ZK-Primitive und based application paths. Ein Covenant kann beim Ausgeben seinen eigenen Nachfolger validieren. Diese Selbstfortsetzung passt zur ΔPAX-Kernfrage: Nicht ein Administrator, sondern jede gültige Transaktion beweist Mengenhaltung, Zustandsübergang und Berechtigung.

Kaspa wurde gegenüber einer EVM-App-Chain gewählt, weil das UTXO-Modell Bearer Value, parallele Verarbeitung und lokale Zustandsübergänge nativ abbildet. Die Wahl ist dennoch experimentell: globale Singletons, Indexer-Reife, Wallet-UX, Compiler-Audits, UTXO-Fragmentierung, Transaktionsmasse und CashLot-Sharding müssen im Testnet belegt werden.

3.2 Kein Kontomodell, keine zentrale Token-Registry

ΔPAX wird als Covenant-Familie mit stabiler Covenant-ID dargestellt. Besitz besteht in der Fähigkeit, den jeweiligen UTXO nach den festgelegten Bedingungen auszugeben. Es gibt keinen globalen balances[address]-Speicher, keine Blacklist und keine pauseAll()-Funktion. Wallets aggregieren mehrere Bearer UTXOs zu einer benutzerfreundlichen Bilanz.

3.3 Covenant-Familien

Covenant	Aufgabe	Unveränderlicher Kern
Constitution	M0, Rmax, Mmax, Emissionskalender, Genesis-Sunset	absolute Obergrenze; keine nachträgliche Mint-Authority
Bearer	split, merge, transfer	Wertkonservation; keine Freeze-Prüfung
CashLot	Sperrung für Note/Münze, Serien-/Batch-Commitment, Vernichtung/Unlock	physischer Nominalwert ≤ gesperrter Wert
OfflineLock	vorfinanzierter Offline-Wert, Ablauf und Claim-Regeln	kein Offline-Wert ohne Lock
Recovery/Escrow	eng begrenzte Streit- und	keine verdeckte Geldschöpfung

Covenant	Aufgabe	Unveränderlicher Kern
	Verlustfälle	
Steward Sunset	Parametrisierung nur in Genesis-Fenster	automatischer Rechteverfall

3.4 Constitution Covenant

Der Constitution Covenant ist kein frei upgradebarer „Master Contract“. Er validiert nur die Nachfolger eines begrenzten Zustandsobjekts: bereits emittierte Menge, verbleibender Security-Korridor, Epoche und Sunset-Status. Jede Emissionstransaktion muss sowohl den kodierten Zeitplan als auch $S \le M_{max}$ erfüllen. Nach Sunset existiert kein Schlüssel, der neue Regeln autorisieren kann.

Ein globaler Singleton kann auf UTXO-Systemen zum Engpass werden. Deshalb wird der tägliche Zahlungsverkehr nicht durch den Singleton serialisiert. Nur seltene Emissionsereignisse berühren den Constitution State; normale Bearer-Transfers sind lokal konservierend.

3.5 Bearer-Transfers

Ein Transfer verbraucht einen oder mehrere ΔPAX-UTXOs und erzeugt Nachfolger derselben Covenant-Familie. Gültigkeit erfordert:

1. Covenant-ID und Asset-Domain stimmen;
2. Summe der ΔPAX-Werte in Inputs entspricht der Summe in Outputs, außer bei einem autorisierten Emissions- oder Burn-Pfad;
3. Signaturen und Script-Constraints sind erfüllt;
4. kein Output überschreitet Integer- oder Massengrenzen;
5. Dust- und Fragmentierungsregeln werden eingehalten.

3.6 Gebühren

In der ersten Version werden Netzwerkgebühren in KAS entrichtet. Wallets können die Gebühr über Sponsoring, Paymaster-ähnliche Services oder automatische KAS-Mikrobeschaffung abstrahieren; die Basisschicht bleibt aber KAS-abhängig. Ein offizieller Dienst darf dafür keine Wechselkursgarantie geben. Phase 0 misst KAS-Verfügbarkeit, Gebührenvolatilität, Zensurpfade und Abhängigkeit von Drittbörsen.

3.7 Indexer und öffentliche Auditierbarkeit

Mindestens drei unabhängig betriebene Indexer rekonstruieren:

- Gesamtmenge und Teilmengen D/P/O/E;
- Genesis- und Security-Emissionen;
- CashLot-Status je Batch;
- OfflineLock-Alter und Abrechnungsstatus;
- Steward-Schlüssel und Sunset-Zustand;
- Abweichungen zwischen physischen Registern und on-chain Commitments.

Ein Indexer ist Lesetechnik, keine Konsensusquelle. Bei Ausfall bleibt die Kette gültig; Nutzer benötigen jedoch alternative Indexer, Full-Node-Validierung und reproduzierbare Open-Source-Software.

3.8 Migration und Exit

Vollständige staatliche Souveränität kann auf einem fremden Netzwerk nicht behauptet werden. Daher ist ein Migrationstest Bestandteil der Phase 0: Snapshot einer definierten Covenant-Familie, unabhängige Rekonstruktion, Zwei-Wege-Claim mit eindeutiger Burn-/Lock-Regel und Schutz gegen Doppelgeltung. Eine reale Migration wäre nur durch Gesetz, lange Vorlaufzeit und öffentliches Opt-in zulässig. Der Test ist eine Risikoprüfung, keine Vorentscheidung für eine eigene Chain.

4. Bargeld und Metall: die physische Brücke

4.1 Grundsatz

Papier und Metall repräsentieren gesperrte digitale ΔPAX. Eine Banknote ist kein privater Bankschuldschein und kein zusätzlicher Token. Die rechtliche Verbindlichkeit liegt beim Protokoll-/Währungssystem; die ausgebende Cash Utility handelt als gesetzlich begrenzter Operator und haftet für ordnungsgemäße Ausgabe, Prüfung und Vernichtung.

4.2 CashLot-Lebenszyklus

1. Eine lizenzierte Bank oder Cash Utility sperrt x ΔPAX in einem CashLot-Covenant.
2. Der Covenant erzeugt einen nicht übertragbaren Produktions-Warrant mit Batch-ID, Nominalsumme, Stückelung, Druck-/Prägestelle und Ablaufdatum.
3. Druckerei oder Münzstätte produziert Träger mit Seriennummer, maschinenlesbarem Commitment und physischen Sicherheitsmerkmalen.
4. Ein unabhängiger Prüfer attestiert Menge und Qualität; erst dann wechselt der Lot in „Issued“.
5. Bei Rückgabe wird der Träger geprüft, entwertet und physisch vernichtet.
6. Vernichtungsnachweis, Mehrparteienattest und Serienstatus autorisieren die Freigabe desselben Nominalbetrags digital.

4.3 Zustände und Invarianten

Zustand	Physischer Umlauf	Digital verfügbar	Erlaubter Übergang
Locked/Unprinted	0	0	Produktion oder Rücknahme des Warrants
Printed/Cold	0	0	kontrollierter Transfer in Hot Inventory
Issued/Hot	Nominalwert	0	Umlauf, Rückgabe
Returned/Pending	gesperrt	0	Prüfung und Vernichtung
Destroyed/Released	0	Nominalwert	digitaler Transfer an Einzahler/Operator

Zustand	Physischer Umlauf	Digital verfügbar	Erlaubter Übergang
Disputed	konservativ als P gezählt	0	Schieds-/ Gerichtsverfahren

Der konservative Grundsatz lautet: Bei Unsicherheit bleibt der digitale Wert gesperrt. Dadurch kann ein Betriebsfehler Liquidität blockieren, aber keine zusätzlichen ΔPAX erzeugen.

4.4 Rollen

- **Cash Utility:** gesetzlich definierter Koordinator, keine Zentralbank und ohne Mint-Recht;
- **Druckerei/Münzstätte:** produziert nur gegen gültigen Warrant;
- **Banken/Kioske/Häfen:** verteilen und nehmen zurück, mit Bond und Limits;
- **Cash Auditor:** prüft Bestände, Serienregister, Vernichtung und on-chain Deckung;
- **Gerichte/Schiedsstellen:** entscheiden Eigentums- und Betrugsfälle, können aber nicht die Gesamtmenge ändern.

4.5 Sicherheitsmerkmale

Banknoten verwenden Baumwoll-/Polymermaterial nach Lebenszyklustest, Tiefdruck, taktile Merkmale, Fenster-/Fadenstruktur, UV/IR-Merkmale, Mikrotext und maschinenlesbare Serienbindungen. Münzen verwenden differenzierte Legierungen, Randprägung, elektromagnetische Signatur und maschinenlesbare Batchmerkmale. QR/NFC enthält keine personenbezogenen Daten und keinen frei kopierbaren Zahlungswert, sondern nur öffentliche Serien-/Batchinformationen und Prüfdaten.

4.6 Datenschutz und Bargeldähnlichkeit

Die Öffentlichkeit sieht, ob eine Serie gültig, zurückgerufen oder vernichtet ist, nicht wer sie hält oder wann sie den Besitzer gewechselt hat. Serienabfragen dürfen nicht zu einem zentralen Bewegungsprofil werden. Online-Prüfdienste werden gecacht, gespiegelt und mit Privacy Budgets versehen. Für kleine Bargeldzahlungen gilt die gesetzliche Bargeldlogik; Banken und Cash Agents erfüllen KYC/AML bei Ausgabe, Rücknahme und verdächtigen Mustern.

4.7 Verlust, Beschädigung und Fälschung

Verlorene Bearer Notes werden grundsätzlich nicht ersetzt, weil sonst Doppelausgabe möglich wäre. Bei klar identifizierbaren beschädigten Trägern kann nach Quorum-Prüfung, Wartefrist und öffentlicher

Serien-Sperre Ersatz erfolgen. Fälschungen begründen keinen ΔPAX-Anspruch; Opferentschädigung erfolgt allenfalls aus einem begrenzten Versicherungsfonds und erzeugt keine neue Geldmenge.

5. Offline-Zahlungen

5.1 Realistische Sicherheitsdefinition

Eine Zahlung ohne Verbindung zur Kette kann nicht gleichzeitig global final, unbegrenzt, anonym und double-spend-sicher sein. ΔPAX verwendet deshalb **vorfinanzierten, begrenzten Offline-Wert**. Der Nutzer sperrt online einen Betrag in einem OfflineLock. Ein zertifiziertes Secure Element verwaltet lokale Einmalzähler, Gerätezertifikate und signierte Übergaben.

5.2 Limits für den Pilot

- maximal 150 ΔPAX je Gerät;
- maximal 50 ΔPAX je Zahlung;
- maximal drei Offline-Hops;
- Online-Synchronisation spätestens nach 72 Stunden;
- Händler-Risikolimit je Gerät und Tag;
- höhere Limits nur mit zusätzlicher Haftung/Bond, nicht durch weichere Kryptographie.

Diese Werte sind Testparameter. Inseln und Fähren sind geeignete Laborumgebungen, weil zeitweise Konnektivitätslücken real sind und die Rückkehr ins Netz planbar bleibt.

5.3 Abrechnung

Beim nächsten Netzaufbau werden signierte Transferketten eingereicht. Konflikte werden nach Zeitstempel-/Counterregeln und Gerätehaftung verarbeitet. Der Empfänger erhält keine falsche Zusage sofortiger on-chain Finalität; Wallets kennzeichnen Offline-Eingänge bis zur Abrechnung als risikobehaftet.

5.4 Lieferkettenrisiko

Secure Elements verlagern Vertrauen auf Chip-Hersteller, Betriebssysteme, Zertifizierungsstellen und Provisioning. Phase 0 verlangt mindestens zwei Lieferanten, offene Protokollspezifikation, Remote-Attestation-Audit, Schlüsselrotationsverfahren und eine Funktionsalternative über physisches Bargeld. Ein kompromittierter Hersteller darf weder Mmax noch on-chain Bestände verändern können; sein Schaden bleibt auf Offline-Limits begrenzt.

6. Banken-, Kredit- und Liquiditätsordnung

6.1 Zahlungskonten

Verwahrte Transaktionsguthaben werden zu 100 % in ΔPAX gehalten und täglich öffentlich attestiert. Kundenguthaben sind insolvenzfestes Sondervermögen. Die Bank darf diese Einheiten nicht verleihen oder verpfänden. Self-Custody bleibt gleichberechtigter Ausweg.

6.2 Kredit

Kredit entsteht aus ausdrücklich gebundenem Laufzeitkapital: Termineinlagen, Anleihen, Eigenkapital, Investmentfonds und Peer-to-Peer-Kreditpools. Ein Anleger sieht Laufzeit, Liquiditätsrisiko und Verlusttragfähigkeit. Ein Kreditvertrag schafft eine Forderung, aber keine neue ΔPAX-Einheit.

6.3 Kein unlimitierter Lender of Last Resort

Die harte Geldmenge schließt unbegrenzte Notfallprägung aus. Ersatzmechanismen sind:

1. 100%-Reserve für Zahlungsverkehr;
2. vorfinanzierter Einlagensicherungsfonds;
3. Liquiditätsauktionen aus bereits existierenden Treasury-Beständen;
4. Bail-in-fähige Laufzeitverbindlichkeiten;
5. schnelle, geordnete Abwicklung insolventer Institute;
6. zeitlich begrenzte Marktunterbrechungen nur an regulierten Handelsplätzen, nicht im ΔPAX-Kern.

Der Fonds wird im Pilot mit 2 %, 4 % und 8 % der verwahrten Zahlungsguthaben stresstested. Eine gesetzliche Garantie ohne vorab finanzierte Deckung wäre mit der Geldverfassung unvereinbar.

6.4 Makroökonomische Konsequenzen

Narrow Banking reduziert Runs auf Zahlungskonten, kann aber Kredit verteuern und Schattenbanken fördern. Eine fixe Geldmenge kann bei Produktivitätswachstum deflationär wirken, reale Schuldenlast erhöhen und Investitionen verschieben. Das Dossier behauptet keine automatische Wohlstandssteigerung. Vor einem souveränen Start sind mindestens folgende Modelle nötig:

- 30-, 50- und 70-prozentiger Einbruch externer Nachfrage;
- 20-prozentige Aufwertung und Abwertung gegenüber EUR innerhalb von 30 Tagen;
- gleichzeitiger Run auf Laufzeitfonds und Rückgang der Steuerzahlungen;

- Ausfall eines systemischen Custodians;
- KAS-Gebührenschock und Kaspa-Reorganisation;
- Bargeldhortung von 15 % der zirkulierenden Menge.

6.5 Staatsfinanzierung

Der Staat darf Defizite nicht durch ΔPAX-Prägung finanzieren. Er kann im souveränen Szenario Steuern in ΔPAX erheben und aus vorhandenen Beständen zahlen. Schuldenaufnahme erfolgt transparent am Kapitalmarkt und trägt Wechselkurs-, Laufzeit- und Ausfallrisiko. In Phase 0 und einem Eurozonen-Pilot nimmt der Staat keine ΔPAX-Schulden auf.

7. Governance und Genesis-Sunset

7.1 Prinzip

Dezentralität wird nicht durch eine DAO-Bezeichnung erzeugt, sondern durch das Entfernen bestimmter Befugnisse. Die Governance darf nach Sunset Parameter für Dienste, Limits und Listen vorschlagen, aber keine Geldmenge erhöhen, Self-Custody-Bestände einfrieren, die Fiat-Unabhängigkeit aufheben oder die Cash-Deckungsinvariante umgehen.

7.2 Genesis Steward

Mandatstext:

> Der Genesis Steward darf bis zum Sunset ausschließlich die in der Genesis-Spezifikation benannten Deployment-, Test-, Registrierungs- und Übergabehandlungen ausführen. Er darf keine ΔPAX außerhalb des kodierten Genesis- und Security-Korridors erzeugen, keine fremden Bearer Outputs beschlagnahmen, keine nachträgliche Blacklist einführen und keinen Sunset verschieben. Jede privilegierte Handlung ist öffentlich, zeitverzögert und widerrufbar. Mit Ablauf des Sunset erlöschen die Schlüsselrechte technisch; ein Gesetz oder Governance-Beschluss kann sie nicht reaktivieren, ohne ein neues, freiwillig zu übernehmendes System zu schaffen.

7.3 Zeitplan

Zeitpunkt	Befugnis	Kontrolle
Tag 0-90	Deployment, Testparameter, Bugfix-Upgrade im wertlosen Testnet	4-von-7 Multisig, 48h Timelock
Tag 91-365	nur sicherheitskritische, abwärtskompatible Änderungen	5-von-9, 14 Tage Timelock, öffentlicher Review
Monat 13-24	Übergabe, keine neue ökonomische Funktion	6-von-11, 30 Tage Timelock
Sunset	Schlüssel-Burn und Covenant-Nachweis	öffentliche Zeremonie, reproduzierbare Verifikation

Für eine reale Währung müsste der Sunset vor werttragendem Genesis gesetzlich und technisch fixiert sein. Ein „später festzulegender“ Sunset ist keine Dezentralität.

7.4 Bürger- und Fachaufsicht

Ein nicht handelbarer Civic Pass kann Vorschläge, Auditprioritäten und Vetos gegen Fiat-Kollateral im Umfeld koordinieren. Er darf keine Konten sperren und keine Geldmenge ändern. Datenschutz verlangt Trennung zwischen Steuer-ID-Prüfung und on-chain Pseudonym; ein Zero-Knowledge-Eligibility-Proof ist Forschungsgegenstand, kein Startversprechen.

7.5 Notfallmechanik

Der unveränderliche Kern besitzt keinen globalen Pause-Schalter. Wallets, Bridges, Cash-Ausgabe und regulierte Märkte können lokal pausieren. Ein zeitlich auslaufender Guardian darf in der Bootstrap-Phase nur neue CashLots und OfflineLocks stoppen, niemals Bearer-Transfers oder Auszahlungen aus bereits erfüllten Claims. Dieses Muster übernimmt die Sunset-Disziplin des 1kUSD-Projekts, nicht dessen Peg-/Oracle- oder Adminarchitektur.

8. Rechtliche Architektur

8.1 Liga A: Forschung und freiwilliger Pilot innerhalb der Eurozone

Art. 128 AEUV ordnet die Genehmigung der Euro-Banknotenausgabe der EZB zu; Euro-Banknoten sind gesetzliches Zahlungsmittel. Die Verordnung (EG) Nr. 974/98 bildet den Rahmen, in dem der Euro die Währung der teilnehmenden Mitgliedstaaten ist. Daraus folgt für dieses Dossier: Griechenland darf ΔPAX in Phase 0 nicht als nationales gesetzliches Zahlungsmittel mit allgemeiner Annahmepflicht ausgeben.

Fiktiver Gesetzestitel: „Gesetz über die interdisziplinäre Erforschung programmierbarer, bargeldkompatibler digitaler Rechnungseinheiten (Νόμος Πειραματικής Ψηφιακής Λογιστικής Μονάδας)“.

Artikelstruktur:

1. Zweck und ausdrücklicher Ausschluss von Legal-Tender-Status;
2. Einrichtung eines befristeten Forschungsprogramms;
3. Testnet ohne realen Geldwert;
4. unabhängige Rechts-, Datenschutz- und Sicherheitsgutachten;
5. Verbot öffentlicher Schuldenaufnahme und Steuerannahme in ΔPAX;
6. Veröffentlichungspflichten und parlamentarische Kontrolle;
7. automatische Beendigung nach 18 Monaten ohne Anschlussgesetz.

Annahmepflicht: nein. **Steuerwirkung:** keine. **Strafen:** irreführende Legal-Tender-Werbung, Ausgabe werttragender Testinstrumente oder Umgehung regulierter Finanzdienstleistungen. **Übergangsfrist:** keine; Sunset unmittelbar nach Forschungsende.

8.2 MiCA und griechische Zuständigkeiten

MiCA ist seit 30. Dezember 2024 vollständig anwendbar. Das griechische Gesetz 5193/2025 enthält nationale Durchführungsmaßnahmen und verteilt Kompetenzen insbesondere zwischen Bank of Greece und Hellenic Capital Market Commission. Ob ein staatlich gesetzlich geschaffenes Instrument, sein Testnet-Abbild oder ein späterer ΔPAX-Token als ART, sonstiges Krypto-Asset oder außerhalb von MiCA einzuordnen wäre, verlangt ein formelles Rechtsgutachten. Weil kein Anspruch auf EUR und kein stabiler Wert gegenüber einer amtlichen Währung besteht, ist die EMT-Schublade nicht naheliegend. Ein Kaufkraftindex darf nicht faktisch als Einlösungsversprechen ausgestaltet werden.

CASPs, Banken, Börsen, Custodians, Wallet-Provider und Cash Agents können je nach Dienst erlaubnis-, kapital-, Governance-, Marktmissbrauchs-, Informations- und Verbraucherschutzpflichten unterliegen. Die Bank of Greece erhält daraus kein Protokoll-Vetorecht; sie kann jedoch Institute, Bankzugang und regulierte Dienste beaufsichtigen.

8.3 AML, Travel Rule und Datenschutz

Die EU-Verordnung 2023/1113 erstreckt Informationspflichten auf bestimmte Krypto-Transfers; die AML-Verordnung 2024/1624 bildet den weiterentwickelten EU-Rahmen. Regulierter Umtausch, Verwahrung, Massenausgabe und Rücknahme benötigen risikobasierte KYC-/Monitoringprozesse. Direkte Self-Custody-Transfers sind technisch anders als CASP-vermittelte Transfers, aber nicht pauschal „rechtsfrei".

Öffentliche UTXO-Daten können bei Verknüpfung personenbezogen werden. Deshalb gelten Datenminimierung, getrennte Identitätsschichten, keine Klarnamen on-chain, Datenschutzfolgenabschätzung, Löschkonzepte für Off-Chain-Daten und gesetzlich enge Auskunftsverfahren.

8.4 Liga B: fiskalische Gravitation ohne Grexit

Eine freiwillige Komplementärnutzung für Gebühren, Gutscheine oder vertragliche Zahlungen ist nur nach Einzelfallprüfung denkbar. Je stärker Staat, Löhne, Steuern und öffentliche Aufträge systematisch in ΔPAX verlagert werden, desto größer ist das Risiko, dass EU-Institutionen das Instrument als unzulässige Parallelwährung mit Währungscharakter behandeln. Dieses Dossier empfiehlt daher in der Eurozone keine fiskalische Gravitation, bevor ein gemeinsames Gutachten mit EU-Kommission, EZB, BoG und HCMC vorliegt.

8.5 Liga C: vollständige Währungssouveränität

Nur in einem Szenario vollständiger Währungssouveränität könnte ein nationales Währungsgesetz ΔPAX zur Rechnungseinheit, zum Steuerzahlungsmittel und zum gesetzlichen Zahlungsmittel erklären. Das würde weit über Technik hinausreichen: Target2, Bankenrekapitalisierung, Einlagensicherung, Kapitalverkehr, Euro-Schulden, Vertragsumstellung, Bargeldlogistik, Zentralbankgesetz, öffentliche Rechnungslegung und internationale Abkommen.

Fiktiver Gesetzestitel: „Gesetz über die nationale Rechnungseinheit, das dezentrale Währungsprotokoll und die Bargeldordnung (Νόμος Εθνικής Λογιστικής Μονάδας και Αποκεντρωμένου Νομισματικού Πρωτοκόλλου)".

Kernartikel: Definition; Legal Tender; Steuerdenomination; Übergangskurs ohne Dauer-Peg; Schutz bestehender Verträge; Bankenreserven; Cash Utility; Protokollverfassung; Sunset; Gerichts- und Insolvenzregeln; Kapitalverkehr nur befristet und verhältnismäßig; internationale Anerkennung.

Diese Liga ist eine Szenarioskizze und keine Empfehlung zum Austritt aus der Währungsunion.

9. Weltwirtschaftliche Einbindung

9.1 Was internationale Relevanz tatsächlich erzeugt

Eine Währung gewinnt Gewicht nicht durch Unausweichlichkeit, sondern durch handelbare Märkte, Rechtsstaatlichkeit, verlässliche Verträge, tiefe Liquidität, produktive Wirtschaft, sichere Anlagen und grenzüberschreitende Zahlungsnutzen. Technische Zensurresistenz kann diese Faktoren unterstützen, aber nicht ersetzen.

9.2 Schifffahrt

UNCTAD weist Griechenland für Januar 2025 als größte Ship-owning Nation mit 16,4 % der globalen Flottenkapazität aus. Ein freiwilliger ΔPAX-Beachhead könnte Hafenentgelte, Besatzungs-Mikropayments, Bunker-/Serviceverträge, maritime Versicherungsprämien oder tokenisierte Handelsfinanzierung untersuchen. Verträge bleiben frei, Sanktionen und internationales Privatrecht gelten. Es gibt keinen Zwang und keinen offiziellen Wechselkurs.

9.3 Tourismus und Inselwirtschaft

Die Bank of Greece meldet für 2025 Reiseeinnahmen von 23,6268 Mrd. Euro und einen Überschuss der Reiseverkehrsbilanz von 20,2878 Mrd. Euro. Ein späterer freiwilliger Pilot könnte Naxos, Kalymnos und Syros vergleichen:

- **Naxos:** breiter Tourismus- und Landwirtschaftsmix;
- **Kalymnos:** Fährabhängigkeit, Diaspora und kleinere Händlernetze;
- **Syros:** Verwaltung, Hafen, ganzjährige Wirtschaft und technische Infrastruktur.

Touristen erhalten optional ein „ΔPAX-Heft“ aus kleinen Banknoten/Münzen oder eine Wallet. Händler zeigen Dual Pricing. Rücktausch erfolgt zu freien Marktpreisen und ohne staatliche Garantie.

9.4 Diaspora und Remittances

Remittances sind ein klarer Nutzen, wenn On-/Off-Ramps transparent, kostengünstig und rechtskonform sind. Das Protokoll betreibt keinen offiziellen EUR-Schalter. Regulierte Anbieter konkurrieren; Gebühren, Spread, Ausführungszeit und Reservequalität werden veröffentlicht.

9.5 Kapitalmarkt und Reservefonds

Ein vom monetären Kern getrennter Reserve-/Liquiditätsfonds darf BTC, ETH, tokenisiertes allokiertes Gold und liquide Staats-/Unternehmenswerte halten. Seine Vermögenswerte sichern **nicht** die Existenz oder Einlösung jeder ΔPAX und erlauben kein Minting. Der Fonds stabilisiert nur Marktliquidität aus bereits vorhandenen Beständen. Damit wird Weltwirtschaftsanbindung ermöglicht, ohne Oracle-, Bridge- oder Verwahrungsrisiken in die Geldmengenverfassung zu importieren.

9.6 Warum Bitcoin-Verbindung nicht Deckung bedeutet

BTC/ΔPAX und KAS/ΔPAX können natürliche Marktpaare sein. Bitcoin kann im Reservefonds, in Zahlungswegen und als neutraler Referenzmarkt dienen. Eine automatische Prägung von ΔPAX gegen BTC würde jedoch Volatilität, Liquidation, Oracle- und Custody-Risiken in den Kern holen. Sie wird daher ausgeschlossen.

10. Sicherheit und Threat Model

10.1 Schutzziele

1. keine Verletzung von Mmax;
2. keine Doppelzählung zwischen D, P, O und E;
3. keine unberechtigte Freigabe aus CashLots;
4. keine Reaktivierung von Genesis-Rechten;
5. kein systemischer Schaden durch kompromittierte Wallets, Indexer oder Secure Elements;
6. reproduzierbare Prüfung ohne Vertrauen in ein Regierungsdashboard.

10.2 Hauptrisiken

Risiko	Frühindikator	Gegenmittel	Residualrisiko
Covenant-/ Compilerfehler	unterschiedliche Ausführung, Audit-Finding	formale Spezifikation, Mehrfachcompiler, Testnet, Bug Bounty	hoch bis unabhängige Audits vorliegen
Kaspa-Reorg/51%-Angriff	ungewöhnliche Reorg-Tiefe, Hashrate-Konzentration	Finalitätsfenster, Alarmierung, Cash-Ausgabe stoppt lokal	externes Netz bleibt abhängig
UTXO-Fragmentierung	steigende Inputzahl/Mass	Wallet-Konsolidierung, Mindeststückelung, Gebührenmodell	UX-/Kostenrisiko
CashLot-Betrug	physischer Bestand > on-chain Lock	Mehrparteienattest, Bond, unangekündigte Inventur	institutionelle Kollusion
Falschgeld	steigende Ablehnungsquote	Sicherheitsmerkmale, Serienstatus, Maschinenprüfung	soziale Schäden trotz keiner Geldschöpfung
Offline-Double-Spend	Konfliktquote, Counter-Anomalien	Limits, Haftung, Synchronisationspflicht	begrenzter Händlerverlust
Governance Capture	Stimmkonzentration, verkürzte Timelocks	unveränderlicher Kern, lange Timelocks, Sunset	externe Dienste beeinflussbar
Staatlicher Zugriff	Gesetzes-/	Self-Custody, Schlüssel-	Staat kann Nutzung

Risiko	Frühindikator	Gegenmittel	Residualrisiko
	Beschlagnahmerisiko	Burn, Rechtsmittel	kriminalisieren, nicht technisch löschen
KAS-Gebührenschock	Kosten/Tx und Liquiditätsengpass	Sponsoring, Puffer, Migrationstest	keine autonome Fee-Policy
Bank-Run/ Liquiditätskrise	Abflüsse aus Laufzeitfonds	100%-Reserve-Zahlungskonten, Bail-in, Fonds	Kreditkontraktion
Datenschutz-Leak	Cluster deanonymisieren Nutzer	Coin Selection, getrennte Identität, ZK-Forschung	öffentliche Ledger-Metadaten
Sanktionsnarrativ	Verlust von Korrespondenzbanken	Compliance an Ramps, keine Umgehungspositionierung	geopolitisches Risiko

10.3 Audit-Reihenfolge

1. formale Invarianten und ökonomische Zustandsmaschine;
2. Silverscript-/Covenant-Compiler und generierte Scripts;
3. Bearer Split/Merge/Transfer;
4. Constitution und Emissionsschedule;
5. CashLot und Recovery;
6. Offline-Protokoll und Secure Element;
7. Wallet, Indexer, Monitoring;
8. Betriebs-, Druck- und Vernichtungsprozesse;
9. Red-Team-Übung über Technik, Recht und Operations.

Kein einzelnes Audit genügt. Vor werttragendem Pilot sind mindestens zwei unabhängige Smart-Contract-/Covenant-Audits, ein Compilerreview, ein Hardwareaudit und ein makroökonomischer Stresstest erforderlich.

10.4 1kUSD als Referenz, nicht als Codebasis

Wiederverwendbar sind ausschließlich methodische Erfahrungen aus dem abgeschlossenen 1kUSD-Stablecoin-Projekt: ein expliziter Invariantenkatalog, Threat Modeling, dokumentierte Systemgrenzen, öffentliche Telemetrie, zeitlich auslaufende Notfallrechte sowie Invariant-/Fuzz-Testdisziplin. Nicht zu übernehmen sind USD-Peg, PSM, Oracle-Architektur, Mock-Oracles, EVM-Adminstruktur, Tokenökonomie und Branding. Nicht öffentlich prüfbare interne Dateipfade oder Architekturentscheidungen werden in DRAX nicht als Beleg verwendet.

11. Implementierungsakte und Phase-0-Plan

11.1 Arbeitspakete

AP	Inhalt	Ergebnis	Budgetband
1	EU-/GR-Recht, MiCA, AML, Legal Tender	gemeinsames Rechtsgutachten und Negativliste	140-220 Tsd. €
2	monetäre/ makroökonomische Simulation	Open-Source-Modell, Szenarien, Sensitivitäten	120-200 Tsd. €
3	Toccata Covenant PoC	wertloser Testnet-Prototyp für Constitution/Bearer/CashLot	220-380 Tsd. €
4	Wallet und öffentliche Indexer	Demo-Wallet, drei reproduzierbare Indexer	120-220 Tsd. €
5	Offline-/Secure-Element-Labor	zwei Lieferanten, Double-Spend- und Ausfalltests	100-180 Tsd. €
6	Bargeldprozess-Design	Sicherheits-/ Vernichtungs-/ Auditprotokoll, keine Wertnoten	70-130 Tsd. €
7	unabhängige Reviews/Bug Bounty	Security, Compiler, Datenschutz, Operations	120-220 Tsd. €
8	Programmsteuerung/ Transparenz	öffentliche Berichte, Parlament/Stakeholder	60-100 Tsd. €

Gesamtkorridor: 0,95-1,65 Mio. Euro einschließlich Reserve; Freigabevorschlag gedeckelt auf 1,6 Mio. Euro. Jeder Auftrag ist meilensteinbasiert. Keine Produktionsinfrastruktur, keine Banknotenproduktion und keine Mainnet-Liquidität.

11.2 Team

- accountable Chief Architect;
- zwei Toccata/Silverscript-Engineers;
- Wallet-/Indexer-Engineer;
- Kryptographie- und Hardware-Security Lead;
- EU-/griechisches Währungsrecht;
- Banken-/Insolvenzrecht;
- Makroökonomie und Zahlungsverkehr;
- Bargelddruck-/Münztechnik;
- Datenschutz/AML;
- Insel-/Hafen-Operations;
- zwei unabhängige Auditfirmen.

11.3 Meilensteine

Monat 0-3: Mandat, Rechtsfragenkatalog, Systeminvarianten, Quellenregister, Testnet-Umgebung. **Monat 4-6:** Constitution/Bearer PoC, Supply-Indexer, erste Makrosimulation. **Monat 7-9:** CashLot-Prototyp, Offline-Labormodell, externe Architekturprüfung. **Monat 10-12:** Angriffssimulation, Migrationstest, Datenschutz- und AML-Gutachten. **Monat 13-15:** integrierte Demo ohne Geldwert, öffentliche Dokumentation, Red Team. **Monat 16-18:** Abschlussgutachten mit Go/No-Go/Research-Only-Entscheidung.

11.4 Harte Abbruchkriterien

- keine belastbare Rechtsposition für selbst einen wertlosen/geschlossenen Pilot;
- kritische Mmax- oder Doppelzählungsinvariante nicht formal und praktisch prüfbar;
- Silverscript-/Toccata-Toolchain ohne ausreichend prüfbaren Release-/Auditstand;
- Offline-Betrugsverlust oberhalb des genehmigten Risikobudgets;
- physischer Lebenszyklus nicht lückenlos mit on-chain Locks abgleichbar;
- KAS-Gebühren-/Beschaffungsabhängigkeit ohne akzeptablen Betriebspfad;
- Migrationstest erzeugt Doppelgeltungs- oder Enteignungsrisiko;
- Makrosimulation zeigt keine tragfähige Banken-/Krisenordnung;
- Governance-Sunset kann nachträglich verschoben oder umgangen werden;
- Projekt wird politisch als verdeckter Grexit oder Sanktionsumgehung instrumentalisiert.

11.5 Definition of Done für Phase 0

Phase 0 ist erfolgreich, wenn ein unabhängiges Team die Geldmenge aus Chain-Daten rekonstruiert, Formwechsel ohne Mengenerhöhung demonstriert, CashLot-Fehlzustände abweist, Offline-Risiko quantifiziert, Genesis-Rechte nachweislich terminiert und der Minister eine belastbare Rechts-/Makroentscheidung treffen kann. Erfolg ist **nicht** Marktkapitalisierung, Tokenpreis oder mediale Aufmerksamkeit.

12. Ministerialer Entscheidungsantrag

12.1 Beantragter Beschluss

Das Ministerium möge:

1. eine ressortübergreifende Machbarkeitsstudie „ΔPAX Phase 0“ für höchstens 18 Monate einrichten;
2. ein Gesamtbudget von maximal 1,6 Mio. Euro unter meilensteinbasierter Freigabe vorsehen;
3. BoG, HCMC, Datenschutzbehörde, Rechnungshof, Universitäten, Banken- und Inselvertreter zur Beobachtung einladen;
4. ein wertloses Kaspa-Testnet-PoC und offene Referenzimplementierungen erlauben;
5. ausdrücklich ausschließen: Mainnet-Wert, nationale Banknoten/Münzen mit Nennwert, Steuerannahme, öffentliche Schulden oder Legal-Tender-Werbung;
6. nach Monat 9 einen Zwischenbeschluss und nach Monat 18 einen automatischen Projekt-Sunset verlangen;
7. eine Fortsetzung nur durch neuen, gesonderten Ministerial- und gegebenenfalls Parlamentsbeschluss zulassen.

12.2 Nicht beantragte Entscheidungen

Nicht beantragt werden Währungsaustritt, Kapitalverkehrskontrollen, Bankenumstellung, Steuerdenomination, öffentlicher ΔPAX-Verkauf, Mainnet-Deployment, Ausgabe echter Banknoten/Münzen oder Anerkennung als gesetzliches Zahlungsmittel.

12.3 Erwarteter Erkenntnisgewinn

Der Staat erhält für einen begrenzten Betrag eine prüfbare Antwort auf fünf Fragen: Kann die Geldmengenverfassung technisch gehalten werden? Kann physisches Geld ohne Doppelzählung angebunden werden? Ist Offline-Risiko begrenzbar? Ist ein legaler Forschungs-/Pilotpfad möglich? Welche makroökonomischen Kosten hätte eine harte Währung ohne Zentralbankelastizität?

13. Anhang A - Genesis- und Protokollparameter

Parameter	Arbeitswert	Änderbarkeit
M0	90.000.000.000 ΔPAX	nur vor Genesis
Rmax	9.000.000.000 ΔPAX	nur vor Genesis; Null-Alternative testen
Mmax	99.000.000.000 ΔPAX	unveränderlich
Dezimalstellen	8	unveränderlich
Security-Epoche	4 Jahre	unveränderlich
Halbierung	50 % je Epoche	unveränderlich
Genesis-Sunset	spätestens 24 Monate nach wertlosem PoC; vor Wertstart neu zu fixieren	nicht verlängerbar
CashLot-Quorum	3-von-5 Produktion; 4-von-7 Vernichtung	parametrierbar vor Wertstart
Offline-Gerätelimit	150 ΔPAX	gesetzlich/operativ senkbar, nicht über Kern erhöhbar
Offline-Zahlung	50 ΔPAX	wie oben
Offline-Sync	72 Stunden	wie oben
Offline-Hops	3	wie oben

14. Anhang B - Beispieltransaktionen

14.1 Taverne auf Naxos, bar

Der Händler nimmt eine 20-ΔPAX-Note an, prüft Sicherheitsmerkmale und optional Serienstatus. Es entsteht keine on-chain Transaktion. Die Note bleibt Teil P. Am Tagesende kann sie als Wechselgeld umlaufen oder bei einer Bank eingezahlt werden.

14.2 Einzahlung einer Note

Die Bank prüft die Note, markiert sie „Returned/Pending“, entwertet sie und übergibt sie an eine kontrollierte Vernichtung. Erst nach Quorum-Attest wird 20 ΔPAX aus dem zugehörigen CashLot freigegeben und an die Wallet des Einzahlers übertragen. S bleibt unverändert.

14.3 Digitaler Transfer

Eine Wallet konsumiert einen 100-ΔPAX-Bearer-UTXO und erzeugt 35 ΔPAX an den Empfänger sowie 65 ΔPAX Change. KAS bezahlt die Netzwerkgebühr. Kein Register aktualisiert eine Kontobilanz; die UTXO-Nachfolger beweisen Wertkonservation.

14.4 Offline-Fähre

Ein Reisender sperrt 80 ΔPAX online in OfflineLock. Auf der Fähre überträgt das Secure Element 12 ΔPAX an das Terminal. Der Händler sieht „offline pending“. Nach WLAN-Verbindung reichen beide Geräte die signierte Übergabekette ein; der Händler erhält einen on-chain Bearer Output.

14.5 Diaspora-Überweisung

Ein regulierter Anbieter kauft ΔPAX am freien Markt und sendet sie an eine Self-Custody-Wallet in Griechenland. Es gibt keinen offiziellen EUR-Kurs. Der Anbieter erfüllt KYC/Travel-Rule-Pflichten, soweit anwendbar; der Empfänger kann digital halten oder über einen Cash Agent physische Einheiten beziehen.

14.6 Kaspa-Störung

Bei schwerer Reorganisation pausieren Cash Utility und regulierte Ausgabestellen lokal neue CashLots und große Abhebungen. Bearer-UTXOs werden nicht zentral eingefroren. Nach finaler Kettenwahl rekonstruieren unabhängige Indexer die Zustände. Ein gesetzlicher Migrationsevent wäre ein separater, öffentlicher Prozess.

15. Anhang C - Glossar

Bearer Asset: Vermögenswert, dessen Verfügung durch Besitz des kryptographischen Ausgaberechts bestimmt wird.
CashLot: On-chain Sperrposition, die eine klar definierte physische Charge deckt.
Covenant: Scriptbedingung, die nicht nur den aktuellen Spend, sondern Eigenschaften zulässiger Nachfolger festlegt.
D/P/O/E: Teilmengen digital frei, physisch gebunden, offline gebunden und Sonderzustände.
Genesis Steward: befristeter technischer Startoperator ohne dauerhafte Währungshoheit.
Legal Tender: gesetzliches Zahlungsmittel mit den jeweiligen gesetzlichen Annahmewirkungen.
Mmax: absolute protokollseitige Maximalmenge.
Narrow Banking: Trennung voll gedeckter Zahlungsguthaben von risikotragender Kreditfinanzierung.
OfflineLock: vorfinanzierter on-chain Lock für begrenzte Offline-Transfers.
Self-Custody: Nutzer kontrolliert seine Ausgabeschlüssel selbst.
Sunset/Key Burn: technisch nachweisbarer und nicht verlängerbarer Ablauf privilegierter Rechte.
Toccata: Kaspa-Programmability-Stack mit UTXO-nativen Covenants und weiteren Ausführungsprimitiven.

16. Anhang D - Quellen- und Verifikationsregister

1. **Kaspa Docs, Toccata Dev Guide und Agent Brief.** Hauptquelle für Mainnet-Aktivierung, UTXO-native Covenants und Entwicklungsmodell. https://docs.kaspa.org/toccata und https://docs.kaspa.org/toccata/agent-brief
2. **Kaspanet, Silverscript Repository.** Compiler-/Sprachstatus und Testnet-/Reifehinweise sind vor jeder Implementierung erneut zu prüfen. https://github.com/kaspanet/silverscript
3. **Kaspanet, vProgs Repository.** Reife- und Prototypstatus based applications. https://github.com/kaspanet/vprogs
4. **AEUV Art. 128.** Euro-Banknoten, Genehmigungszuständigkeit und Legal-Tender-Status. https://eur-lex.europa.eu/eli/treaty/tfeu_2012/art_128/oj/deu
5. **Verordnung (EG) Nr. 974/98.** Einführung des Euro und Währungsrahmen der teilnehmenden Mitgliedstaaten. https://eur-lex.europa.eu/eli/reg/1998/974/oj
6. **Verordnung (EU) 2023/1114 (MiCA).** Krypto-Asset-Regulierung. https://eur-lex.europa.eu/eli/reg/2023/1114/oj
7. **Bank of Greece, MiCA.** Law 5193/2025, zuständige Behörden und BoG-Kompetenzen. https://www.bankofgreece.gr/en/main-tasks/supervision/regulation-eu-2023_1114-on-markets-in-crypto-assets

8. **Verordnung (EU) 2023/1113.** Informationen bei Geld- und bestimmten Kryptotransfers. https://eur-lex.europa.eu/eli/reg/2023/1113/oj
9. **Verordnung (EU) 2024/1624.** EU-Geldwäschebekämpfungsrahmen. https://eur-lex.europa.eu/eli/reg/2024/1624/oj
10. **ECB, Digital Euro FAQs.** Zentralisierte Settlement-Plattform; nicht DLT-basiert, jedoch Nutzung einzelner DLT-Designprinzipien. https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.html
11. **UNCTAD, Review of Maritime Transport 2025.** Griechenland als führende Ship-owning Nation mit 16,4 % der globalen Flottenkapazität. https://unctad.org/system/files/official-document/rmt2025overview_en.pdf
12. **Bank of Greece, Developments in the balance of travel services: 2025.** Reiseeinnahmen und Tourismusdaten. https://www.bankofgreece.gr/en/news-and-media/press-office/news-list/news?announcement=27a32287-1c58-44e7-b900-2c92c53ffe9c
13. **BIS Annual Economic Report 2025, Next-generation monetary and financial system.** Kriterien Singleness, Elasticity und Integrity als Gegenmaßstab. https://www.bis.org/publications/aer-2025/next-generation-monetary-financial-system
14. **IMF, Currency Boards und Lender of Last Resort.** Grenzen harter Geldordnungen und Krisenliquidität. https://www.elibrary.imf.org/view/journals/007/1999/009/article-A004-en.xml
15. **1kUSD als methodische Referenz.** Übernommen werden nur allgemeine Audit- und Verifikationsprinzipien; interne Dateien, USD-Peg, PSM, Oracle- und EVM-Architektur sind keine Quelle oder Grundlage von DRAX.

16.1 Offene Rechtsfragen [UNSICHER]

- genaue MiCA-Einordnung eines staatlich initiierten, später dezentralen Nicht-Peg-Assets;
- Zulässigkeit eines werttragenden freiwilligen Komplementärpilots und einer begrenzten fiskalischen Nutzung in der Eurozone;
- Verhältnis von Bearer-Self-Custody zu AMLR, Travel Rule, nationalem Bargeld- und Steuerrecht;
- rechtliche Qualität einer Cash Utility als Issuer of Record ohne Zentralbankfunktion;
- vertrags-, insolvenz- und eigentumsrechtliche Behandlung von CashLots und Offline Claims;
- Anforderungen an Datenschutz und Rückverfolgbarkeit von Serien-/UTXO-Daten.

17. Ehrliches Restrisiko

ΔPAX kann technisch sehr hart und gegen nachträgliche Prägung robust gestaltet werden. Sie kann aber nicht gleichzeitig vollständig souverän, global offen, krisenelastisch, offline final, anonym und

institutionenfrei sein. Kaspa reduziert Betreiberzentralität, ersetzt jedoch keine eigene Sicherheits- und Migrationsstrategie. Papier und Metall brauchen vertrauenswürdige menschliche Prozesse. Eine fixe Geldmenge verhindert monetäre Rettung und kann Deflation sowie Kreditknappheit verschärfen. Recht kann Self-Custody technisch nicht rückwirkend löschen, aber Nutzung, Intermediäre und Märkte beschränken. Internationale Relevanz entsteht nur durch reale Wirtschaft, Rechtsstaatlichkeit und freiwillige Liquidität. Das Vorhaben ist daher als überprüfbares Forschungsprogramm vertretbar; eine Einführung wäre erst nach positiven Rechts-, Sicherheits- und Makroergebnissen verantwortbar.

Prüfsatz, abschließend: Schein am Sonntag, Token am Montag, identischer Nominalbetrag - und niemand in Athen besitzt einen Schlüssel, mit dem er nach dem Sunset neue ΔPAX prägen oder die Self-Custody-Wallet des Fischers einfrieren kann.