DRX PROGRAMME — INDEPENDENT DRACHMA

HELLENIC MONETARY TECHNOLOGY INITIATIVE

White Paper and Ministerial Dossier

DRX PROGRAMME — INDEPENDENT DRACHMA · dig Δραχμή (ΔPAX)

Vendetta Labs · Gio (Kaspartizan)

1 September 2026

WHITEPAPER AND MINISTERIAL DOSSIER · PUBLIC RESEARCH VERSION · VERSION 0.9

Addressee: Hellenic Ministry of National Economy and Finance
Document type: Preliminary feasibility study; not legal advice, not an issuance resolution and not a recommendation to leave the eurozone
Decision sought: Approval of a limited Phase 0 study and a valueless testnet prototype

> **Litmus test:** A fisherman on Kalymnos receives a ΔPAX banknote on Sunday, deposits it at a bank on Monday and receives the same nominal amount digitally. Neither the bank nor any ministry can thereby create additional ΔPAX, freeze someone else's self-custody wallet or alter the constitutional maximum supply.

Publication status: Public research version of a private initiative by Vendetta Labs. Not commissioned, approved or endorsed by the state. Legal, macroeconomic and cryptographic counter-review is pending.

Table of contents

0. Executive One-Pager

0.1 What is proposed

ΔPAX is an independent unit of account with three carrier forms of equal rank: on-chain bearer value, pre-funded offline value in certified secure elements, and banknotes and coins. All forms belong to **one** money supply. Paper and metal are not a second currency and not a claim on an additional token. Every physical issuance presupposes that the same nominal amount has been digitally locked in a publicly auditable CashLot covenant.

The digital core is to be prototyped on **Kaspa Toccata** as a UTXO-native covenant family. ΔPAX is thereby neither KAS nor a KAS fork nor a wrapped token. In the first architecture, KAS serves only as the network fee and security asset. The monetary order itself is determined by conserving UTXO transitions, a pre-defined maximum supply and a publicly demonstrable genesis sunset.

0.2 What is expressly not proposed

- no CBDC with citizen accounts at a central bank;
- no peg to EUR or USD and no official peg-stability module;
- no minting against USDC, USDT, EURC or bank deposits;
- no discretionary money creation by government, bank or governance;
- no promise of fully anonymous intermediary services or trustless offline finality;
- no claim that other states, exchanges or banks could not exclude ΔPAX;
- no introduction as legal tender within the eurozone under Phase 0.

0.3 Recommended decision

Approval is sought solely for a **12- to 18-month Phase 0** with a budget corridor of **EUR 0.95 to 1.65 million** and a requested ceiling of **EUR 1.6 million**: legal opinions, macroeconomic simulations, a valueless Kaspa testnet prototype, CashLot and offline laboratory models, and independent security reviews. Neither mainnet value nor banknotes with face value nor acceptance for tax payments form part of this authorisation.

0.4 Ten constitutional rules

1. **One unit, one money supply:** $S = D + P + O + E$.
2. **Hard ceiling:** $S \leq M_{max}$; no emergency mint.
3. **Change of form without creation:** digital, offline, note and coin do not alter S.

4. **No freeze function in the core:** self-custody balances cannot be administratively frozen.
5. **No fiat linkage:** exchange rates form on the free market.
6. **No oracle dependency in the monetary core:** prices influence neither the existence nor the supply of ΔPAX.
7. **Genesis Steward for a fixed term:** privileged rights expire technically and in a publicly verifiable manner.
8. **The physical arm is institutional but fully backed:** every physical nominal value corresponds to a locked digital nominal value.
9. **Intermediaries fulfil legal obligations:** AML, consumer protection and supervision apply at custody, exchange and issuance points.
10. **No sovereignty rhetoric without an exit test:** dependencies on Kaspa, KAS fees, wallets and secure-element supply chains are measured and provided with migration paths.

1. Mandate, assumptions and decision horizons

1.1 Mandate

This study examines whether a state can launch a hard digital national currency whose daily use is simultaneously possible in self-custody, offline, as a banknote and as a coin, without a central bank or government being able, after the genesis window, to freeze accounts or increase the money supply at its discretion. Greece serves as the concrete use case. The document strictly distinguishes between technical feasibility, the current eurozone legal position and a legal-tender scenario relevant only under full monetary sovereignty.

1.2 Stipulated assumptions

- **A1:** The state wishes to weight transparency, rule-binding and technical self-restraint more heavily than short-term monetary flexibility.
- **A2:** Citizens may hold digital ΔPAX in self-custody. Banks and wallet providers remain optional service providers.
- **A3:** A physical carrier necessarily requires trustworthy issuance points, printing works, mints, authenticity verification and destruction controls.
- **A4:** Kaspa Toccata has been active on mainnet since 30 June 2026; compiler, wallet, indexer and audit maturity nevertheless remain young dependencies to be examined.
- **A5:** The eurozone remains the applicable legal framework in Phase 0 and in any voluntary research/complementary pilot.
- **A6:** Full statutory acceptance obligation, national banknotes with legal-tender status and tax denomination in ΔPAX are examined only in the sovereign scenario.
- **A7:** Figures in this draft are planning parameters. They become normative only after simulation, legal opinion and public consultation.

1.3 Central conflicts of objectives

Hardness versus crisis elasticity. An immutable maximum supply protects against political dilution but removes from the state the classic instrument of the lender of last resort. The system must therefore operate with 100 %-reserve payment accounts, pre-funded liquidity buffers, orderly insolvencies and explicit stop criteria.

Decentralisation versus physical cash. Digital bearer value can be largely rule-based. Paper and metal require physical institutions. The solution is not to deny this zone of trust but to bound it tightly, collateralise it, audit it end to end and separate it from the right to create money.

Sovereignty versus an open world economy. An open global network reduces national censorship and operator dependency but creates dependency on foreign miners, KAS fees, network upgrades and global liquidity. Sovereignty is therefore defined as the ability to verify, to migrate and to decide legally for oneself - not as a claim of technical autarky.

1.4 Decision horizons

Horizon	Permissible statement	Expressly not included
Phase 0, 0-18 months	research, simulation, testnet, legal review	monetary value, mainnet, acceptance obligation, acceptance for tax payments
Optional eurozone pilot	voluntary, limited complementary use after clearance	national legal tender, compulsory wages, replacement of the euro
Sovereign scenario	full currency, banking and cash regime	recommendation or automatism towards Grexit

2. Monetary constitution

2.1 The unit

One ΔPAX is a nominally identical unit regardless of whether it is held as an on-chain UTXO, an offline claim, a banknote or a coin. The unit is **not** defined as a claim on an amount of euro, dollar, bitcoin or gold. Its exchange rate is freely formed. Its monetary hardness follows from supply, convertibility between carrier forms, transparent fiscal acceptance in the sovereign scenario and a credible legal order - not from a peg.

2.2 Money-supply identity

At every finalised block:

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

where:

- D: ΔPAX circulating freely in digital form;
- P: digital ΔPAX locked in CashLots, corresponding to issued banknotes and coins;
- O: ΔPAX locked in OfflineLock covenants;
- E: narrowly defined special states, such as legally pending destruction or recovery procedures;
- S: total existing money supply.

For every transaction the following must hold: Inputs + permissible emission = Outputs + demonstrable burn. Changes of form do not alter S. A public supply indexer reconstructs D, P, O and E independently of ministry, bank or wallet front end.

2.3 Genesis and maximum supply

Working parameters for the simulation:

- M0 = 90,000,000,000 ΔPAX genesis nominal supply;
- Rmax = 9,000,000,000 ΔPAX maximum emission corridor, encoded exclusively for network security and public infrastructure;
- Mmax = 99,000,000,000 ΔPAX absolute ceiling;
- R is halved in four-year epochs tied to block time and cannot be accelerated or repurposed;
- epoch entitlements not drawn lapse rather than being carried into later epochs;
- once the corridor is exhausted or expired, any further emission is contrary to consensus.

These figures are **not a political recommendation** but a complete set of simulatable parameters. An alternative with Rmax = 0 must be tested on an equal footing. The security tranche is an ex ante political distribution decision and must not be disguised as "purely technical".

2.4 Genesis distribution

Purpose	Share of M0	Locking logic
Civic base allocation	34 %	claim-based, staggered over time, non-transferable entitlement verification
Exchange/liquidity reserve for a sovereign start	22 %	public treasury without mint right, multi-year issuance rules
Banknote and coin CashLots	12 %	only against physical issuance; unused lots remain locked
Public wages/benefits - voluntary quota	10 %	only after a legal-tender act and at the recipient's option
Infrastructure and security fund	8 %	timelock, earmarked, public budget
Island/port pilot	4 %	local caps, unwinding clause
Diaspora and export liquidity	4 %	transparent auctions, no exchange-rate guarantee
Strategic emergency liquidity	4 %	no money creation; only already existing units
Research, audit and bug bounty	2 %	milestone vesting

Every allocation is visible on-chain in advance. No recipient acquires a protocol right to further issuance.

2.5 Value stability without a peg

The system promises no fixed purchasing power. An official **ΔPAX purchasing-power index** may track bread, electricity, ferry fares, olive oil, rent and diesel, but serves only statistics, wage and contract indexation. It must trigger neither automatic money creation nor redemption against a fiat basket. In this way the currency remains fiat-unbound while government, collective-bargaining partners and households can observe real purchasing power.

2.6 Seigniorage

Seigniorage arises only at genesis and in the encoded security tranche. It is not treated as ongoing government revenue. Proceeds from issuance, lost physical carriers or fees flow into a separate, publicly accounted infrastructure and loss-compensation fund. The government must not finance budget deficits through protocol issuance.

3. Technical architecture on Kaspa Toccata

3.1 Why Kaspa Toccata

Toccata extends Kaspa with UTXO-native covenants, Transaction v1, script pricing, inline ZK primitives and based application paths. A covenant can validate its own successor when spent. This self-continuation fits the ΔPAX core question: not an administrator, but every valid transaction proves supply conservation, state transition and authorisation.

Kaspa was chosen over an EVM app-chain because the UTXO model natively maps bearer value, parallel processing and local state transitions. The choice remains experimental: global singletons, indexer maturity, wallet UX, compiler audits, UTXO fragmentation, transaction mass and CashLot sharding must be evidenced on testnet.

3.2 No account model, no central token registry

ΔPAX is represented as a covenant family with a stable covenant ID. Ownership consists in the ability to spend the respective UTXO under the defined conditions. There is no global balances[address] store, no blacklist and no pauseAll() function. Wallets aggregate multiple bearer UTXOs into a user-friendly balance.

3.3 Covenant families

Covenant	Function	Immutable core
Constitution	M0, Rmax, Mmax, emission calendar, genesis sunset	absolute ceiling; no retroactive mint authority
Bearer	split, merge, transfer	value conservation; no freeze check
CashLot	locking for note/coin, serial/batch commitment, destruction/unlock	physical nominal value ≤ locked value
OfflineLock	pre-funded offline value, expiry and claim rules	no offline value without a lock
Recovery/Escrow	narrowly bounded dispute and loss cases	no covert money creation

Covenant	Function	Immutable core
Steward Sunset	parameterisation only within the genesis window	automatic expiry of rights

3.4 Constitution covenant

The Constitution covenant is not a freely upgradeable "master contract". It validates only the successors of a bounded state object: quantity already emitted, remaining security corridor, epoch and sunset status. Every emission transaction must satisfy both the encoded schedule and S ≤ Mmax. After the sunset there exists no key that could authorise new rules.

A global singleton can become a bottleneck on UTXO systems. Daily payment traffic is therefore not serialised through the singleton. Only rare emission events touch the Constitution state; ordinary bearer transfers are locally conserving.

3.5 Bearer transfers

A transfer consumes one or more ΔPAX UTXOs and creates successors of the same covenant family. Validity requires:

1. covenant ID and asset domain match;
2. the sum of ΔPAX values in the inputs equals the sum in the outputs, except on an authorised emission or burn path;
3. signatures and script constraints are satisfied;
4. no output exceeds integer or mass limits;
5. dust and fragmentation rules are observed.

3.6 Fees

In the first version, network fees are paid in KAS. Wallets can abstract the fee via sponsoring, paymaster-like services or automatic KAS micro-procurement; the base layer nevertheless remains KAS-dependent. An official service must give no exchange-rate guarantee for this. Phase 0 measures KAS availability, fee volatility, censorship paths and dependency on third-party exchanges.

3.7 Indexers and public auditability

At least three independently operated indexers reconstruct:

- total supply and the D/P/O/E sub-supplies;
- genesis and security emissions;
- CashLot status per batch;
- OfflineLock age and settlement status;
- steward keys and sunset state;
- discrepancies between physical registers and on-chain commitments.

An indexer is read technology, not a consensus source. If it fails, the chain remains valid; users, however, require alternative indexers, full-node validation and reproducible open-source software.

3.8 Migration and exit

Full state sovereignty cannot be claimed on a third-party network. A migration test is therefore part of Phase 0: snapshot of a defined covenant family, independent reconstruction, two-way claim with an unambiguous burn/lock rule and protection against double validity. A real migration would be permissible only by statute, with a long lead time and a public opt-in. The test is a risk examination, not a pre-decision for a chain of one's own.

4. Cash and metal: the physical bridge

4.1 Principle

Paper and metal represent locked digital ΔPAX. A banknote is neither a private bank promissory note nor an additional token. The legal liability rests with the protocol/currency system; the issuing Cash Utility acts as a statutorily bounded operator and is liable for proper issuance, verification and destruction.

4.2 CashLot life cycle

1. A licensed bank or Cash Utility locks x ΔPAX in a CashLot covenant.
2. The covenant creates a non-transferable production warrant with batch ID, nominal sum, denominations, printing/striking facility and expiry date.
3. The printing works or mint produces carriers with serial number, machine-readable commitment and physical security features.
4. An independent auditor attests quantity and quality; only then does the lot switch to "Issued".
5. On return, the carrier is verified, invalidated and physically destroyed.
6. Proof of destruction, multi-party attestation and serial status authorise the digital release of the same nominal amount.

4.3 States and invariants

State	Physical circulation	Digitally available	Permitted transition
Locked/Unprinted	0	0	production or withdrawal of the warrant
Printed/Cold	0	0	controlled transfer into hot inventory
Issued/Hot	nominal value	0	circulation, return
Returned/Pending	locked	0	verification and destruction
Destroyed/Released	0	nominal value	digital transfer to depositor/operator

State	Physical circulation	Digitally available	Permitted transition
Disputed	conservatively counted as P	0	arbitration/court proceedings

The conservative principle reads: in case of doubt, the digital value stays locked. An operational error can thereby jam liquidity but cannot create additional ΔPAX.

4.4 Roles

- **Cash Utility:** statutorily defined coordinator, not a central bank and without mint right;
- **Printing works/mint:** produces only against a valid warrant;
- **Banks/kiosks/ports:** distribute and take back, with bond and limits;
- **Cash Auditor:** verifies holdings, serial registers, destruction and on-chain backing;
- **Courts/arbitration bodies:** decide ownership and fraud cases but cannot alter the total supply.

4.5 Security features

Banknotes use cotton/polymer material selected by life-cycle testing, intaglio printing, tactile features, window/thread structures, UV/IR features, microtext and machine-readable serial bindings. Coins use differentiated alloys, edge lettering, electromagnetic signature and machine-readable batch features. QR/NFC contains no personal data and no freely copyable payment value, only public serial/batch information and verification data.

4.6 Data protection and cash-likeness

The public sees whether a series is valid, recalled or destroyed, not who holds it or when it changed hands. Serial queries must not become a central movement profile. Online verification services are cached, mirrored and equipped with privacy budgets. For small cash payments, statutory cash logic applies; banks and Cash Agents fulfil KYC/AML at issuance, redemption and suspicious patterns.

4.7 Loss, damage and counterfeiting

Lost bearer notes are in principle not replaced, because double issuance would otherwise be possible. In the case of clearly identifiable damaged carriers, replacement may occur after quorum verification, a waiting period and a public serial block. Counterfeits establish no claim to ΔPAX; compensation of victims occurs at most from a limited insurance fund and creates no new money supply.

5. Offline payments

5.1 Realistic security definition

A payment without connection to the chain cannot simultaneously be globally final, unlimited, anonymous and double-spend-proof. ΔPAX therefore uses **pre-funded, limited offline value**. The user locks an amount online in an OfflineLock. A certified secure element manages local one-time counters, device certificates and signed handovers.

5.2 Limits for the pilot

- maximum 150 ΔPAX per device;
- maximum 50 ΔPAX per payment;
- maximum three offline hops;
- online synchronisation within 72 hours at the latest;
- merchant risk limit per device and day;
- higher limits only with additional liability/bond, not through softer cryptography.

These values are test parameters. Islands and ferries are suitable laboratory environments because temporary connectivity gaps are real there and the return to the network remains plannable.

5.3 Settlement

At the next network connection, signed transfer chains are submitted. Conflicts are processed according to timestamp/counter rules and device liability. The recipient receives no false promise of immediate on-chain finality; wallets flag offline receipts as risk-bearing until settlement.

5.4 Supply-chain risk

Secure elements shift trust onto chip manufacturers, operating systems, certification bodies and provisioning. Phase 0 requires at least two suppliers, an open protocol specification, remote-attestation audit, key-rotation procedures and a functional alternative via physical cash. A compromised manufacturer must be able to alter neither Mmax nor on-chain balances; the damage it can cause remains bounded by the offline limits.

6. Banking, credit and liquidity regime

6.1 Payment accounts

Custodied transaction balances are held 100 % in ΔPAX and publicly attested daily. Customer balances are insolvency-remote segregated assets. The bank must not lend or pledge these units. Self-custody remains an equivalent way out.

6.2 Credit

Credit arises from expressly committed term capital: time deposits, bonds, equity, investment funds and peer-to-peer credit pools. An investor sees maturity, liquidity risk and loss-bearing capacity. A credit contract creates a claim, but no new ΔPAX unit.

6.3 No unlimited lender of last resort

The hard money supply rules out unlimited emergency issuance. Substitute mechanisms are:

1. 100 % reserve for payments;
2. a pre-funded deposit-insurance fund;
3. liquidity auctions from already existing treasury holdings;
4. bail-in-able term liabilities;
5. fast, orderly resolution of insolvent institutions;
6. time-limited market suspensions only at regulated trading venues, not in the ΔPAX core.

In the pilot, the fund is stress-tested at 2 %, 4 % and 8 % of custodied payment balances. A statutory guarantee without pre-funded backing would be incompatible with the monetary constitution.

6.4 Macroeconomic consequences

Narrow banking reduces runs on payment accounts but can make credit more expensive and foster shadow banks. A fixed money supply can act deflationarily under productivity growth, increase the real debt burden and shift investment. The dossier claims no automatic increase in prosperity. Before a sovereign start, at least the following models are required:

- a 30-, 50- and 70-per-cent collapse in external demand;
- a 20-per-cent appreciation and depreciation against EUR within 30 days;
- a simultaneous run on term funds and a decline in tax payments;

- failure of a systemic custodian;
- a KAS fee shock and Kaspa reorganisation;
- cash hoarding of 15 % of the circulating supply.

6.5 State financing

The state must not finance deficits through ΔPAX issuance. In the sovereign scenario it can levy taxes in ΔPAX and pay from existing holdings. Borrowing occurs transparently on the capital market and bears exchange-rate, maturity and default risk. In Phase 0 and in a eurozone pilot, the state takes on no ΔPAX debt.

7. Governance and genesis sunset

7.1 Principle

Decentralisation is not created by a DAO label but by the removal of specific powers. After the sunset, governance may propose parameters for services, limits and lists, but may not increase the money supply, freeze self-custody balances, abolish fiat independence or circumvent the cash-backing invariant.

7.2 Genesis Steward

Mandate text:

> Until the sunset, the Genesis Steward may perform exclusively the deployment, testing, registration and handover acts named in the genesis specification. It may create no ΔPAX outside the encoded genesis and security corridor, seize no third-party bearer outputs, introduce no retroactive blacklist and postpone no sunset. Every privileged act is public, time-delayed and revocable. Upon expiry of the sunset, the key rights lapse technically; a statute or governance resolution cannot reactivate them without creating a new system to be adopted voluntarily.

7.3 Schedule

Point in time	Power	Control
Day 0-90	deployment, test parameters, bugfix upgrade on the valueless testnet	4-of-7 multisig, 48 h timelock
Day 91-365	only security-critical, backwards-compatible changes	5-of-9, 14-day timelock, public review
Month 13-24	handover, no new economic function	6-of-11, 30-day timelock
Sunset	key burn and covenant proof	public ceremony, reproducible verification

For a real currency, the sunset would have to be fixed by statute and technically before any value-bearing genesis. A sunset "to be determined later" is not decentralisation.

7.4 Civic and expert oversight

A non-tradeable Civic Pass can coordinate proposals, audit priorities and vetoes against fiat collateral in the periphery. It may freeze no accounts and alter no money supply. Data protection requires separation between tax-ID verification and the on-chain pseudonym; a zero-knowledge eligibility proof is a research subject, not a launch promise.

7.5 Emergency mechanics

The immutable core has no global pause switch. Wallets, bridges, cash issuance and regulated markets can pause locally. A time-expiring guardian may, during the bootstrap phase, only stop new CashLots and OfflineLocks, never bearer transfers or pay-outs from already satisfied claims. This pattern adopts the sunset discipline of the 1kUSD project, not its peg/oracle or admin architecture.

8. Legal architecture

8.1 League A: research and voluntary pilot within the eurozone

Article 128 TFEU assigns the authorisation of euro banknote issuance to the ECB; euro banknotes are legal tender. Regulation (EC) No 974/98 forms the framework within which the euro is the currency of the participating member states. For this dossier it follows: in Phase 0, Greece must not issue ΔPAX as national legal tender with a general obligation of acceptance.

Fictitious statute title: "Act on the interdisciplinary investigation of programmable, cash-compatible digital units of account (Νόμος Πειραματικής Ψηφιακής Λογιστικής Μονάδας)".

Article structure:

1. purpose and express exclusion of legal-tender status;
2. establishment of a time-limited research programme;
3. testnet without real monetary value;
4. independent legal, data-protection and security opinions;
5. prohibition of public borrowing and acceptance for tax payments in ΔPAX;
6. publication duties and parliamentary control;
7. automatic termination after 18 months absent a follow-up statute.

Acceptance obligation: none. **Tax effect:** none. **Penalties:** misleading legal-tender advertising, issuance of value-bearing test instruments or circumvention of regulated financial services. **Transitional period:** none; sunset immediately after the end of research.

8.2 MiCA and Greek competences

MiCA has been fully applicable since 30 December 2024. Greek Law 5193/2025 contains national implementing measures and allocates competences in particular between the Bank of Greece and the Hellenic Capital Market Commission. Whether a state-created statutory instrument, its testnet representation or a later ΔPAX token would be classified as an ART, another crypto-asset or outside MiCA requires a formal legal opinion. Because there is no claim on EUR and no stable value relative to an official currency, the EMT category is not the obvious one. A purchasing-power index must not be structured de facto as a redemption promise.

CASPs, banks, exchanges, custodians, wallet providers and Cash Agents may, depending on the service, be subject to authorisation, capital, governance, market-abuse, information and consumer-protection

obligations. The Bank of Greece thereby acquires no protocol veto right; it can, however, supervise institutions, bank access and regulated services.

8.3 AML, Travel Rule and data protection

EU Regulation 2023/1113 extends information obligations to certain crypto transfers; AML Regulation 2024/1624 forms the developed EU framework. Regulated exchange, custody, mass issuance and redemption require risk-based KYC/monitoring processes. Direct self-custody transfers are technically different from CASP-mediated transfers, but not blanket "law-free".

Public UTXO data can become personal data when linked. Accordingly, the following apply: data minimisation, separate identity layers, no clear names on-chain, a data-protection impact assessment, erasure concepts for off-chain data and statutorily narrow disclosure procedures.

8.4 League B: fiscal gravity without Grexit

Voluntary complementary use for fees, vouchers or contractual payments is conceivable only after case-by-case review. The more systematically the state, wages, taxes and public procurement are shifted into ΔPAX, the greater the risk that EU institutions will treat the instrument as an impermissible parallel currency with monetary character. This dossier therefore recommends no fiscal gravity within the eurozone before a joint opinion with the EU Commission, ECB, BoG and HCMC is available.

8.5 League C: full monetary sovereignty

Only in a scenario of full monetary sovereignty could a national currency act declare ΔPAX the unit of account, the means of tax payment and legal tender. That would reach far beyond technology: Target2, bank recapitalisation, deposit insurance, capital movements, euro-denominated debt, contract conversion, cash logistics, the central-bank act, public accounting and international agreements.

Fictitious statute title: "Act on the national unit of account, the decentralised monetary protocol and the cash regime (Νόμος Εθνικής Λογιστικής Μονάδας και Αποκεντρωμένου Νομισματικού Πρωτοκόλλου)".

Core articles: definition; legal tender; tax denomination; conversion rate without a permanent peg; protection of existing contracts; bank reserves; Cash Utility; protocol constitution; sunset; court and insolvency rules; capital movements only time-limited and proportionate; international recognition.

This league is a scenario sketch, not a recommendation to leave the monetary union.

9. Global economic integration

9.1 What actually creates international relevance

A currency gains weight not through inevitability but through tradeable markets, the rule of law, reliable contracts, deep liquidity, a productive economy, safe investments and cross-border payment utility. Technical censorship resistance can support these factors but cannot replace them.

9.2 Shipping

UNCTAD identifies Greece as of January 2025 as the largest ship-owning nation with 16.4 % of global fleet capacity. A voluntary ΔPAX beachhead could examine port dues, crew micropayments, bunker/service contracts, marine insurance premiums or tokenised trade finance. Contracts remain free; sanctions and international private law apply. There is no compulsion and no official exchange rate.

9.3 Tourism and the island economy

The Bank of Greece reports travel receipts of EUR 23.6268 billion for 2025 and a travel-services balance surplus of EUR 20.2878 billion. A later voluntary pilot could compare Naxos, Kalymnos and Syros:

- **Naxos:** broad tourism and agriculture mix;
- **Kalymnos:** ferry dependency, diaspora and smaller merchant networks;
- **Syros:** administration, port, year-round economy and technical infrastructure.

Tourists optionally receive a "ΔPAX booklet" of small banknotes/coins or a wallet. Merchants display dual pricing. Redemption occurs at free market prices and without a state guarantee.

9.4 Diaspora and remittances

Remittances are a clear benefit where on/off-ramps are transparent, inexpensive and compliant. The protocol operates no official EUR desk. Regulated providers compete; fees, spread, execution time and reserve quality are published.

9.5 Capital market and reserve fund

A reserve/liquidity fund separated from the monetary core may hold BTC, ETH, tokenised allocated gold and liquid government/corporate securities. Its assets do **not** secure the existence or redemption of every ΔPAX and permit no minting. The fund stabilises only market liquidity from already existing

holdings. Global economic linkage is thereby enabled without importing oracle, bridge or custody risks into the money-supply constitution.

9.6 Why a Bitcoin link does not mean backing

BTC/ΔPAX and KAS/ΔPAX can be natural market pairs. Bitcoin can serve in the reserve fund, in payment paths and as a neutral reference market. Automatic issuance of ΔPAX against BTC would, however, bring volatility, liquidation, oracle and custody risks into the core. It is therefore excluded.

10. Security and threat model

10.1 Protection objectives

1. no breach of Mmax;
2. no double counting between D, P, O and E;
3. no unauthorised release from CashLots;
4. no reactivation of genesis rights;
5. no systemic damage from compromised wallets, indexers or secure elements;
6. reproducible verification without trust in a government dashboard.

10.2 Principal risks

Risk	Early indicator	Countermeasure	Residual risk
Covenant/compiler error	divergent execution, audit finding	formal specification, multiple compilers, testnet, bug bounty	high until independent audits are available
Kaspa reorg/51 % attack	unusual reorg depth, hashrate concentration	finality window, alerting, cash issuance stops locally	external network remains a dependency
UTXO fragmentation	rising input count/mass	wallet consolidation, minimum denominations, fee model	UX/cost risk
CashLot fraud	physical stock > on-chain lock	multi-party attestation, bond, unannounced inventory checks	institutional collusion
Counterfeiting	rising rejection rate	security features, serial status, machine verification	social harm despite no money creation
Offline double spend	conflict rate, counter anomalies	limits, liability, synchronisation duty	bounded merchant loss
Governance capture	vote concentration, shortened timelocks	immutable core, long timelocks, sunset	external services influenceable

Risk	Early indicator	Countermeasure	Residual risk
State access	seizure risk by statute	self-custody, key burn, legal remedies	state can criminalise use, not technically delete it
KAS fee shock	cost/tx and liquidity bottleneck	sponsoring, buffers, migration test	no autonomous fee policy
Bank run/liquidity crisis	outflows from term funds	100 %-reserve payment accounts, bail-in, fund	credit contraction
Data-protection leak	clusters deanonymise users	coin selection, separate identity, ZK research	public ledger metadata
Sanctions narrative	loss of correspondent banks	compliance at ramps, no circumvention positioning	geopolitical risk

10.3 Audit sequence

1. formal invariants and economic state machine;
2. Silverscript/covenant compiler and generated scripts;
3. Bearer split/merge/transfer;
4. Constitution and emission schedule;
5. CashLot and Recovery;
6. offline protocol and secure element;
7. wallet, indexer, monitoring;
8. operational, printing and destruction processes;
9. red-team exercise across technology, law and operations.

No single audit suffices. Before a value-bearing pilot, at least two independent smart-contract/covenant audits, a compiler review, a hardware audit and a macroeconomic stress test are required.

10.4 1kUSD as a reference, not a codebase

Only methodological experience from the completed 1kUSD stablecoin project is reusable: an explicit invariant catalogue, threat modelling, documented system boundaries, public telemetry, time-expiring emergency powers and invariant/fuzz testing discipline. Not to be adopted are the USD peg, PSM, oracle

architecture, mock oracles, EVM admin structure, token economics and branding. Non-publicly-verifiable internal file paths or architecture decisions are not used as evidence in the DRX project.

11. Implementation acts and Phase 0 plan

11.1 Work packages

WP	Content	Result	Budget band
1	EU/GR law, MiCA, AML, legal tender	joint legal opinion and negative list	EUR 140-220 thousand
2	monetary/ macroeconomic simulation	open-source model, scenarios, sensitivities	EUR 120-200 thousand
3	Toccata covenant PoC	valueless testnet prototype for Constitution/Bearer/CashLot	EUR 220-380 thousand
4	wallet and public indexers	demo wallet, three reproducible indexers	EUR 120-220 thousand
5	offline/secure-element laboratory	two suppliers, double-spend and failure tests	EUR 100-180 thousand
6	cash-process design	security/destruction/ audit protocol, no value notes	EUR 70-130 thousand
7	independent reviews/bug bounty	security, compiler, data protection, operations	EUR 120-220 thousand
8	programme management/transparency	public reports, parliament/stakeholders	EUR 60-100 thousand

Total corridor: EUR 0.95-1.65 million including contingency; authorisation proposal capped at EUR 1.6 million. Every contract is milestone-based. No production infrastructure, no banknote production and no mainnet liquidity.

11.2 Team

- accountable chief architect;
- two Toccata/Silverscript engineers;

- wallet/indexer engineer;
- cryptography and hardware-security lead;
- EU/Greek monetary law;
- banking/insolvency law;
- macroeconomics and payments;
- banknote printing/minting technology;
- data protection/AML;
- island/port operations;
- two independent audit firms.

11.3 Milestones

Month 0-3: mandate, catalogue of legal questions, system invariants, source register, testnet environment.
Month 4-6: Constitution/Bearer PoC, supply indexer, first macro simulation.
Month 7-9: CashLot prototype, offline laboratory model, external architecture review.
Month 10-12: attack simulation, migration test, data-protection and AML opinions.
Month 13-15: integrated demo without monetary value, public documentation, red team.
Month 16-18: final assessment with Go/No-Go/Research-Only decision.

11.4 Hard termination criteria

- no robust legal position even for a valueless/closed pilot;
- a critical Mmax or double-counting invariant not formally and practically verifiable;
- Silverscript/Toccata toolchain without a sufficiently auditable release/audit baseline;
- offline fraud loss above the approved risk budget;
- physical life cycle not fully reconcilable with on-chain locks;
- KAS fee/procurement dependency without an acceptable operating path;
- migration test creates double-validity or expropriation risk;
- macro simulation shows no viable banking/crisis regime;
- governance sunset can be retroactively postponed or circumvented;
- the project is politically instrumentalised as a covert Grexit or sanctions evasion.

11.5 Definition of done for Phase 0

Phase 0 succeeds if an independent team reconstructs the money supply from chain data, demonstrates changes of form without supply increases, rejects CashLot fault states, quantifies offline risk, demonstrably terminates genesis rights and the minister can take a robust legal/macro decision. Success is **not** market capitalisation, token price or media attention.

12. Ministerial decision application

12.1 Requested resolution

The Ministry is requested:

1. to establish a cross-departmental feasibility study "ΔPAX Phase 0" for at most 18 months;
2. to provide a total budget of at most EUR 1.6 million under milestone-based release;
3. to invite BoG, HCMC, the Data Protection Authority, the Court of Audit, universities and banking and island representatives as observers;
4. to permit a valueless Kaspa testnet PoC and open reference implementations;
5. to exclude expressly: mainnet value, national banknotes/coins with face value, acceptance for tax payments, public debt or legal-tender advertising;
6. to require an interim resolution after month 9 and an automatic project sunset after month 18;
7. to permit continuation only through a new, separate ministerial and, where applicable, parliamentary resolution.

12.2 Decisions not requested

Not requested are currency exit, capital controls, bank conversion, tax denomination, a public ΔPAX sale, mainnet deployment, issuance of real banknotes/coins or recognition as legal tender.

12.3 Expected gain in knowledge

For a limited amount, the state receives a verifiable answer to five questions: Can the money-supply constitution be technically upheld? Can physical money be linked without double counting? Can offline risk be bounded? Is a lawful research/pilot path possible? What macroeconomic costs would a hard currency without central-bank elasticity entail?

13. Annex A - Genesis and protocol parameters

Parameter	Working value	Mutability
M0	90,000,000,000 ΔPAX	only before genesis
Rmax	9,000,000,000 ΔPAX	only before genesis; test the zero alternative
Mmax	99,000,000,000 ΔPAX	immutable
Decimal places	8	immutable
Security epoch	4 years	immutable
Halving	50 % per epoch	immutable
Genesis sunset	at latest 24 months after the valueless PoC; to be fixed anew before value start	not extendable
CashLot quorum	3 of 5 production; 4 of 7 destruction	parameterisable before value start
Offline device limit	150 ΔPAX	lowerable by statute/operation, not raisable via the core
Offline payment	50 ΔPAX	as above
Offline sync	72 hours	as above
Offline hops	3	as above

14. Annex B - Example transactions

14.1 Taverna on Naxos, cash

The merchant accepts a 20-ΔPAX note, checks the security features and optionally the serial status. No on-chain transaction occurs. The note remains part of P. At the end of the day it can circulate as change or be deposited at a bank.

14.2 Deposit of a note

The bank verifies the note, marks it "Returned/Pending", invalidates it and hands it over for controlled destruction. Only after the quorum attestation are 20 ΔPAX released from the associated CashLot and transferred to the depositor's wallet. S remains unchanged.

14.3 Digital transfer

A wallet consumes a 100-ΔPAX bearer UTXO and creates 35 ΔPAX to the recipient and 65 ΔPAX of change. KAS pays the network fee. No register updates an account balance; the UTXO successors prove value conservation.

14.4 Offline ferry

A traveller locks 80 ΔPAX online in an OfflineLock. On the ferry, the secure element transfers 12 ΔPAX to the terminal. The merchant sees "offline pending". After a Wi-Fi connection, both devices submit the signed handover chain; the merchant receives an on-chain bearer output.

14.5 Diaspora remittance

A regulated provider buys ΔPAX on the free market and sends it to a self-custody wallet in Greece. There is no official EUR rate. The provider fulfils KYC/Travel-Rule obligations where applicable; the recipient can hold digitally or obtain physical units via a Cash Agent.

14.6 Kaspa disruption

In the event of a severe reorganisation, the Cash Utility and regulated issuance points locally pause new CashLots and large withdrawals. Bearer UTXOs are not centrally frozen. After final chain selection, independent indexers reconstruct the states. A statutory migration event would be a separate, public process.

15. Annex C - Glossary

Bearer asset: an asset whose disposition is determined by possession of the cryptographic spending right.
CashLot: on-chain lock position backing a clearly defined physical batch.
Covenant: a script condition that fixes not only the current spend but properties of permissible successors.
D/P/O/E: sub-supplies digital free, physically bound, offline bound and special states.
Genesis Steward: time-limited technical start operator without permanent monetary sovereignty.
Legal tender: statutory means of payment with the respective statutory acceptance effects.
Mmax: absolute protocol-level maximum supply.
Narrow banking: separation of fully backed payment balances from risk-bearing credit financing.
OfflineLock: pre-funded on-chain lock for limited offline transfers.
Self-custody: the user controls their own spending keys.
Sunset/key burn: technically demonstrable and non-extendable expiry of privileged rights.
Toccata: Kaspa programmability stack with UTXO-native covenants and further execution primitives.

16. Annex D - Source and verification register

1. **Kaspa Docs, Toccata Dev Guide and Agent Brief.** Primary source for mainnet activation, UTXO-native covenants and the development model. https://docs.kaspa.org/toccata and https://docs.kaspa.org/toccata/agent-brief
2. **Kaspanet, Silverscript repository.** Compiler/language status and testnet/maturity notes must be re-checked before every implementation. https://github.com/kaspanet/silverscript
3. **Kaspanet, vProgs repository.** Maturity and prototype status of based applications. https://github.com/kaspanet/vprogs
4. **TFEU Art. 128.** Euro banknotes, authorisation competence and legal-tender status. https://eur-lex.europa.eu/eli/treaty/tfeu_2012/art_128/oj/deu
5. **Regulation (EC) No 974/98.** Introduction of the euro and the monetary framework of the participating member states. https://eur-lex.europa.eu/eli/reg/1998/974/oj
6. **Regulation (EU) 2023/1114 (MiCA).** Crypto-asset regulation. https://eur-lex.europa.eu/eli/reg/2023/1114/oj
7. **Bank of Greece, MiCA.** Law 5193/2025, competent authorities and BoG competences. https://www.bankofgreece.gr/en/main-tasks/supervision/regulation-eu-2023_1114-on-markets-in-crypto-assets

8. **Regulation (EU) 2023/1113.** Information accompanying transfers of funds and certain crypto-assets. https://eur-lex.europa.eu/eli/reg/2023/1113/oj
9. **Regulation (EU) 2024/1624.** EU anti-money-laundering framework. https://eur-lex.europa.eu/eli/reg/2024/1624/oj
10. **ECB, Digital Euro FAQs.** Centralised settlement platform; not DLT-based, though using individual DLT design principles. https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.html
11. **UNCTAD, Review of Maritime Transport 2025.** Greece as the leading ship-owning nation with 16.4 % of global fleet capacity. https://unctad.org/system/files/official-document/rmt2025overview_en.pdf
12. **Bank of Greece, Developments in the balance of travel services: 2025.** Travel receipts and tourism data. 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.** The criteria singleness, elasticity and integrity as a counter-benchmark. https://www.bis.org/publications/aer-2025/next-generation-monetary-financial-system
14. **IMF, Currency Boards and Lender of Last Resort.** Limits of hard monetary regimes and crisis liquidity. https://www.elibrary.imf.org/view/journals/007/1999/009/article-A004-en.xml
15. **1kUSD as a methodological reference.** Only general audit and verification principles are adopted; internal files, the USD peg, PSM, oracle and EVM architecture are no source or basis of DRX.

16.1 Open legal questions [UNCERTAIN]

- the precise MiCA classification of a state-initiated, later decentralised non-peg asset;
- permissibility of a value-bearing voluntary complementary pilot and limited fiscal use within the eurozone;
- the relationship of bearer self-custody to the AMLR, the Travel Rule, national cash and tax law;
- the legal quality of a Cash Utility as issuer of record without a central-bank function;
- the contractual, insolvency and property-law treatment of CashLots and offline claims;
- requirements for data protection and traceability of serial/UTXO data.

17. Honest residual risk

ΔPAX can be designed technically very hard and robust against retroactive issuance. It cannot, however, simultaneously be fully sovereign, globally open, crisis-elastic, offline final, anonymous and institution-

free. Kaspa reduces operator centrality but replaces neither an independent security nor a migration strategy. Paper and metal require trustworthy human processes. A fixed money supply prevents monetary rescue and can exacerbate deflation and credit scarcity. Law cannot technically delete self-custody retroactively, but it can restrict use, intermediaries and markets. International relevance arises only through the real economy, the rule of law and voluntary liquidity. The project is therefore defensible as a verifiable research programme; an introduction would be responsible only after positive legal, security and macro results.

Litmus test, in closing: note on Sunday, token on Monday, identical nominal amount - and no one in Athens holds a key with which, after the sunset, they could mint new ΔPAX or freeze the fisherman's self-custody wallet.