

Draft for review. Not a locked spec. The whitepaper is the definition; if the two disagree, the whitepaper wins. [Whitepaper v0.0003](#). [PDF](#).

Version 0.1 · October 2026 · Draft

K0 Architecture Requirements

Companion to K0 Protocol Whitepaper v0.0003. Draft for review. Not a locked specification.

1. Purpose and status

The whitepaper defines K0 by nine properties and says a mechanism joins the protocol only if it keeps all nine. This note is the other half: what any candidate machine must provide, a reference architecture that could satisfy it, how a native coin fits, and how candidates will be tested.

Everything here is a **proposal**. Where a number appears it is a design target or an illustration, not a measured result. Nothing in this note changes the definition. If this note and the whitepaper disagree, the whitepaper wins.

2. Requirements traceability

Each whitepaper property becomes a requirement and a pass/fail test. A candidate that fails a test is not K0, however fast it is.

#	Property	Architecture requirement	Test
1	No protocol-level custody	Ledger records positions against a Responsible Party. No protocol-controlled key can move user funds. Fiat on/off-ramp only through regulated issuers.	Key audit: list every key that can move funds; none belongs to the protocol.

#	Property	Architecture requirement	Test
2	Payer cost zero	Transaction fees are sponsored. The payer never needs a fee balance.	Fresh account sends a payment with no prior funding other than the amount.
3	Merchant cost always ≤ 10 bps, shown separately	Fee is a rule on the ledger, charged in the payment's settlement unit, recorded as its own entry apart from fulfilment. Fee can be reduced or waived by rule with a named funding source.	The cap is enforced by the protocol, not by configuration: no rule, waiver or settlement mode can produce a total merchant cost above 10 bps (fee plus any conversion or spread charged to the merchant). Fee on a \$100 payment is at most \$0.10. Receipt shows fulfilment and fee separately. A waived fee shows zero to the merchant and the network side is still paid.
4	Cash-like privacy, auditable	Balances, amounts and counterparties are hidden from the public record. Selective disclosure to lawful authority is a ledger operation.	Public observer cannot read them. Authorized disclosure reveals only the scoped data. No operator can decrypt alone.
5	Compliance in the protocol	Attestation checks, thresholds and travel-rule attachment are rules enforced at transfer time.	Transfer that violates a rule is rejected by consensus, not by a company.
6	World scale	At least 65,000 TPS peak, linear scale-out, sub-second user confirmation.	Load test at target across geographies. Adding capacity raises throughput roughly in proportion.
7	Consumer experience	Human names, no seed phrase on day one, no gas token held by users.	Usability test: new user pays in under a minute with no crypto vocabulary.
8	Security	No equivocation loss, safe key recovery, no new reserve claim.	Formal and external audit of ledger, rules and bridge code.
9	Sufficient decentralization	No single operator can halt, rewrite or capture. Users and merchants can leave an operator without leaving their money.	Take down any one operator: network continues. Move an account to another operator without a custodial step.

3. Reference architecture (candidate)

3.1 Layers

Wallet / app	human names, sponsored fees, recovery
Operators	bundlers and gateways; submit transfers
Ledger	accounts · attestations · transfers · rules
coordinator	finalizes domain state, routes cross-domain transfers
domains (shards)	parallel execution, one rule set
Responsible Parties	licensed holders of the balances (bank, reserve bank, government body)
Stable-unit issuers	USDC today; issuance and reserves stay with the issuer

3.2 Ledger contents

The ledger holds four things (whitepaper §4A) and no others.

- **Accounts.** Controlled by holder keys. Each records a position against one Responsible Party. Names resolve to accounts (human names, not hex).
- **Attestations.** Verified-party records issued by an attester under a stated standard. The ledger stores the attestation or a commitment to it, never identity documents. Expiry and revocation are supported.
- **Transfers.** Signed, ordered by consensus, final when the protocol will not reverse the credit. A payment is **one atomic transfer with two entries**: fulfilment at the full amount, and the fee as a distinct entry against the merchant. One signature, one proof, one consensus slot. The fee is a rule applied inside the transfer, not a second transaction. On \$500 at 10 bps: \$500.00 fulfilment, \$0.50 fee, \$499.50 net to the merchant at settlement, both entries visible.
- **Settlement units.** The ledger is unit-agnostic. Each payment settles in one unit and the fee is charged in that same unit. USDC is the unit for the proving phase; the e-rupee and others join by registering an issuer and a Responsible Party for the unit, with no change to transfer rules. Units are held natively on the ledger. Host-chain gas appears only at the on/off-ramp edge.
- **Fee pool.** Fee entries credit one pool per unit. The pool is paid out to validators, operators, attesters and treasury in epoch batches, so a payment costs one pool credit however many parties share the fee.
- **Rules.** On-ledger programs run on every transfer: attestation checks, thresholds, travel-rule data attachment, fee collection, disclosure hooks. Rule changes go through governance with a timelock (§6).

"Smart contracts" in the general sense are available to build products on K0, but **only the rule set is part of the protocol**. General contracts may run in a separate execution environment so that a third-party contract can never alter a transfer rule.

3.3 Scale

Target: 65,000 TPS peak. Illustration, not a plan: 65 domains each sustaining 1,000 TPS. The design relies on domains running in parallel with a coordinator that carries only state roots and cross-domain messages. Cross-domain transfers are the hard case; the test in §2 must include them at realistic mix, not only same-domain payments.

3.4 Privacy and lawful audit

Requirements, not a chosen scheme:

- Shielded balances and amounts on the public record. Zero-knowledge proofs of validity are the expected tool.
- Selective disclosure through scoped viewing capability, released only against a lawful-process attestation. Threshold control, so no single operator, including K-0 in the pilot, can open an account alone.
- The public cannot be handed audit, and operators cannot be handed a backdoor (whitepaper §5).
- Mixing pools that exist to defeat lawful process are excluded.

3.5 Identity and compliance

- One-time attestation by a licensed attester. The attestation carries what a rule needs (for example, "verified individual, jurisdiction X, tier Y"), not the underlying documents.
- Rules read attestations. Large-value and travel-rule duties are expressed as rule conditions plus required data attached to the transfer for delivery to the required parties.
- Users who do not attest transact within the limits the law allows.

3.6 Responsible Party

During the pilot K-0 acts as Responsible Party (whitepaper §9). The architecture must make this role **replaceable**: the ledger addresses a Responsible Party by registered identity, and an account can be moved to another one. Handing the role to a bank or reserve bank must need no change to the ledger rules.

3.7 User experience

- Fee sponsorship by the operator (paid from the merchant fee, §4).
- Account abstraction for recovery, so that no seed phrase is needed at the start.
- No visible block, gas or chain concepts.

4. Incentive design and the native coin

4.1 Where the coin sits

The coin is a **layer beneath the payment**, not part of it.

- It is **not** the unit of account (settlement stays in the settlement unit).
- It is **not** held, bought or seen by payers or merchants.
- It exists to secure the ledger and to pay the parties who run it.

This is what the whitepaper §8 requires. The earlier U4U design (a fee token paid by users, pegged at \$0.01) conflicts with properties 2 and 7, and it is **retired as a user-facing instrument**.

4.2 Who needs incentives

Role	Does	Paid by
Validators	Run consensus on domains and coordinator	Fee share + coin rewards; stake at risk
Operators / bundlers	Submit and sponsor transfers, serve wallets	Fee share
Attesters	Verify parties, issue attestations	Per-attestation fee
Responsible Parties	Hold balances, carry the license	Contract with K-0 or the operator; outside the coin
Treasury / development	Maintain the protocol	Defined fee share

The Responsible Party is paid under its own licence and contract. It must never depend on the coin's price.

4.3 Fee flow (illustrative)

The merchant's fee is charged in the payment's settlement unit and recorded as its own entry (§3.2). It is paid into the per-unit fee pool, then split between validators, operators, attesters and treasury in epoch batches. Percentages are **undecided**. Conversion into the coin, if there is one, happens beneath, on the pool.

Waivers. The fee rule can return less than the standard fee, down to zero, per merchant, corridor or period. The merchant sees the discount, and the network side is still paid in full from a named source: a sponsor, the treasury, or bounded coin issuance. Each waiver is

published with its funding source and end date, so that a free period is a visible subsidy and not a hidden cost.

Why separate. Merchants book gross sales and fees as distinct entries; the fee can be waived without touching fulfilment; and the price of the network is visible on every receipt.

Settlement modes. The receiver chooses how the fee is settled. The mode changes timing and mechanics, never the amount, and the 10 bps cap holds in every mode.

Mode	Merchant receives	Fee
Netted	Payment less fee (e.g. \$499.50)	Fee entry visible, deducted at settlement
Prepaid	Full payment (\$500.00)	Drawn from a fee balance the merchant topped up in advance
Billed later	Full payment (\$500.00)	Accrued and invoiced, settled on a schedule
Other	As the rules allow	Any arrangement that keeps the cap and the separate entry

A prepaid balance is the merchant's own position, held with its Responsible Party, never with the protocol (§3.1). It must be refundable in full if the merchant leaves (property 9). If the merchant chooses nothing, the default is netted.

Sanity check on the economics: 1 bp on a \$50 payment is \$0.005. The cost of validating, sponsoring and attesting one transfer has to fit inside that. This is the main economic risk of the whole design and should be modelled before any coin is designed.

4.4 Coin roles

If a coin exists, the whitepaper §8 rules apply. Concretely it can:

- be staked by validators, and slashed for provable misbehavior;
- fund waivers and be paid as emission during bootstrap, when fee volume is too low to pay operators, with emission falling as fee volume rises;
- carry governance weight, subject to the open question in §7 on whether governance and security should be the same asset.

It cannot back, collateralize or stand in for the settlement unit's reserves.

4.5 Two options

	A. Stake in the settlement unit	B. Native coin
Validator stake	Bonded USDC	Coin
Bootstrap reward	Fee share + funded budget	Fee share + emission
Security economics	Capped by bonded capital	Can grow with network value
Legal profile	Lighter (no new asset)	Heavy (securities, MiCA, other regimes)
Fit with whitepaper §8	Easy	Needs the seven rules
Fundraising	Fewer routes	Typical route, but restricted

Recommendation: design the ledger and fee flow so that option A works on its own, and treat B as an addition decided after legal advice. That keeps the protocol launchable if the coin is delayed or not cleared.

5. Candidate chain stacks

Qualitative, from general knowledge. Entries marked (verify) must be checked against current documentation before relying on them.

Candidate	Strengths for K0	Gaps to close
Polkadot SDK (Substrate)	Custom runtime so rules and compliance can be native; identity and contract pallets exist; parallel chains fit linear scale-out; grant routes exist (separate task)	No native privacy; sovereign chain needs own validators, parachain needs paid block space; 65k TPS unproven (verify)
Cosmos SDK	Sovereign appchains, interchain messaging, custom modules	Privacy and sponsored fees to build; throughput per chain (verify)
Starknet / ZK-rollup	Proofs and validity already native; Ethereum settlement	Gas model, general-purpose cost, compliance and privacy defaults not payment-shaped (verify)
Custom	Fit by design	Cost, time, security risk

Nothing here is chosen. The decision rule is the §2 tests, run on a prototype.

6. Governance

- Protocol definition (the nine properties) changes only by a new whitepaper version.
- Rule changes by governance with a timelock and published review period.
- Early on, multisig with timelock; transition to wider governance is a roadmap item, not a claim. No date is committed here.

- Emergency pause, if any, must be narrow, time-limited and visible. A permanent pause power fails property 9.

7. Open decisions

1. **Coin or no coin at launch** (option A or B in §4.5). Needs legal advice in the jurisdictions where K0 will operate. This is a blocker for any coin work.
2. **One asset or two.** Whether security staking and governance voting are the same asset.
3. **Fee split** and the cost per transfer. Needs the cost model in §4.3.
4. **Privacy scheme.** Which ZK construction, and how threshold disclosure is governed.
5. **General contracts.** In the protocol, beside it, or out of scope for v1.
6. **Chain stack.** Decide after a prototype passes the §2 tests.
7. **Who attests** in each pilot jurisdiction, and under whose licence.
8. **Responsible Party handover** path and timeline.
9. **Fee settlement modes shipped first.** Netted is the default. Which of prepaid, billed later and others come in the proving phase, and how a prepaid balance is held with the Responsible Party.
10. **Optional coin payment.** Whether a merchant may pay the fee in the coin for a discount, never required (whitepaper §8, rule 2).
11. **E-rupee mapping.** Issuer, Responsible Party roles and rules for a central-bank unit, and whether its regime allows a fee entry in that unit.

Tracked minor issues

- **Accountant check.** Whether a fee line is a taxable service (VAT/GST) in each jurisdiction, and how netted, prepaid and billed-later fees are booked. Not verified; needs an accountant before pilot.

8. Validation plan

1. **Paper gate.** Cost-per-transfer model against 1 bp (§4.3).
2. **Prototype gate.** One domain, accounts, attestations, transfers, rules, sponsored fee. Run §2 tests 1, 2, 3, 5, 7.
3. **Privacy gate.** Shielded transfers with scoped disclosure. Tests 4 and 8.
4. **Scale gate.** Multi-domain load test. Tests 6 and 9.
5. **Legal gate.** Written advice on the pilot as Responsible Party, and on any coin, before issuance.

A failed gate means the candidate is not K0.

K0 Architecture Requirements v0.1. Proposals only; the whitepaper is the definition.