ASTRYUM · PRODUCT DECK · SEPTEMBER 2026

Legacy

Capital under rules. A family, a group or a foundation holds XRP together, governed by a council of real people — and nobody moves it alone. Not a member. Not us.

LIVE on XRPL Mainnet and Flare since July 2026

THE PROBLEM

Capital outlives the people who manage it. Keys don’t.

Option one: one person keeps the keys for everyone

It fails the day that person isn’t there — or the day they decide alone. “Shared” capital is a promise between people, not a property of the money.

Option two: a custodian keeps them for all of you

You no longer hold your XRP. The custodian decides when you may leave, and their rules are a setting in their app.

The design flaw has nothing to do with crypto: nothing in the world enforces that *three of four* must agree. A ledger does. That is the third option.

WHAT A LEGACY IS

A council on XRPL. A constitution anchored on the ledger. A vault on Flare that only obeys the constitution.

The council

Real people with weights and a quorum — 3 of 4, for example — as the account's SignerList. The original single key is switched off. Every decision needs the quorum; **the heirs do not wait for an event: they already are the quorum.**

The constitution

Written in plain language: who signs, for what, within which limits. Checked while still reversible, then anchored in the account's own record (DIDSet: hash + URI). It cannot be rewritten quietly.

The vault ("the cage")

A contract on Flare whose only council is the bridge that verifies the council's orders. It sends capital to approved venues and recalls it. It has no function to pay principal to anyone — including us.

Astryum prepares every transaction, shows all of it and stops. Every member signs in their own Xaman. We never hold a key.

THE CONSTITUTION CEREMONY

Six steps, each signed by the people it binds.

1 · Write
The constitution in plain language, from a template (family, foundation, child…). Astryum checks the plan while it is still reversible.

→

2 · SignerListSet
Members, weights, quorum (up to 32 signers). Signed once by the master key.

→

3 · DIDSet
SHA-256 of the text + URI anchored on the account. The vault references this hash for every governing call.

→

4 · Rehearsal
Every member signs a real multisig transaction (an EscrowCreate). Nobody closes a door they cannot open: quorum margin ≥ 1 is required.

→

5 · Master key off
AccountSet asfDisableMaster, irreversibility disclosed. Re-enabling needs the same quorum: cure possible, shortcut not.

→

6 · The cage is born
One memo instruction from the council deploys bridge + vault and makes the first deposit.

Health rules refuse dangerous actions with an exact quorum and only allow closing the door after a rehearsed quorum with margin. Proven on mainnet since 14–15 July (multisig coordinator) and 29 July (first order).

SIGNING, WITHOUT A COORDINATOR HOLDING ANYTHING

Each member signs their part, when they can. The browser combines. The backend never touches a signature.

The asynchronous tray

- Astryum fixes Sequence and Fee (base × (1 + signers)), sets `SigningPubKey = ""`, re-stamps the Source Tag — and **never signs, combines or broadcasts**.
- Xaman payloads with `submit: false, multisign: true`: each member signs their part from their own phone.
- Tickets keep the account's sequence free, so proposals do not block each other.
- The browser combines the signatures and broadcasts to public XRPL nodes.

What the ledger enforces, what we only read

- The quorum is enforced by consensus: an order without enough weight is not a valid transaction.
- Only validated `tesSUCCESS` counts — for receipts, metrics and the verifier. "Signed" is never painted as "done".
- The Source Tag survives multisig: each signer counts as an active account.
- The bridge on Flare attests transactions, not ledger state: the master key being off is a fact of the ceremony, verifiable on any explorer.

BIRTH OF THE CAGE

One signature deploys the stack and makes the first deposit.

Council's Payment

To the FAssets Core Vault, memo = hash of the batch (rail A). On a multisig-only account, producing this payment *is* the quorum.

FDC attests · executor delivers →

Council's Personal Account

Derived from the council's XRPL address. Executes the batch: `LegacyStackFactory.create` · `FXRP.approve(predicted vault)` · `LegacyVault.deposit`.

only this PA may create →

LegacyStackFactory

Checks `getPersonalAccount(council) == msg.sender`. Deploys bridge → vault(council = bridge) → bind. CREATE2 makes the vault's address predictable, so the approve can precede its existence.

→

One cage per Legacy, forever

`vaultOf(councilHash)` resolves which cage belongs to which council, on chain.

No anchor, no cage

The vault's `constitutionRef` is the DID hash. Nothing is born without an anchored constitution.

Own cap, written down

No external audit yet, so a Legacy cage is capped at 5 XRP in configuration. The number is small on purpose and said in public.

ORDERS — RAIL B

The council decides on XRPL. The contract on Flare obeys — or refuses.

Council
1-drop Payment to the anchor, memo = keccak(keccak(nonce, calldata)). Signed by the quorum.

FDC XRPPayment proof →

XrplCouncilBridge
COUNCIL_ADDRESS_HASH immutable. Checks: proof · type & source · proof owner · source = council · tx succeeded · memo = hash · txId unused · nonce next.

vault.call(calldata) →

LegacyVault
12 actions: direct-to, recall, move, evacuate, propose/retire venue, set lineage fee, set payees, cede, end cession, set constitution ref…

outside the rules →

Revert
The "no" is given by the ledger. Astryum relays the proof with its own key and cannot alter a byte.

Anti-replay, twice

A consumed XRPL transaction id can never execute again; the nonce must be exactly the next one. The bridge is literally the vault's `council`: no other address can order it.

Proven

LIVE First order 29 Jul (directTo Kinetic, nonce 0 → 1). Four orders end to end by 4 Aug; the last in 1 min 40 s. Bridge `nextNonce = 4`, read 15 Sep.

THE VAULT'S RULES

What the contract cannot do is the product.

Does not exist in the code

- ✕ `withdrawPrincipal()`
- ✕ `transferTo(arbitrary address)`
- ✕ proxy, upgrade, pause, owner = Astryum
- ✕ a protocol fee above a hard 10 % cap (default 0)

The only relocation: `migrate`

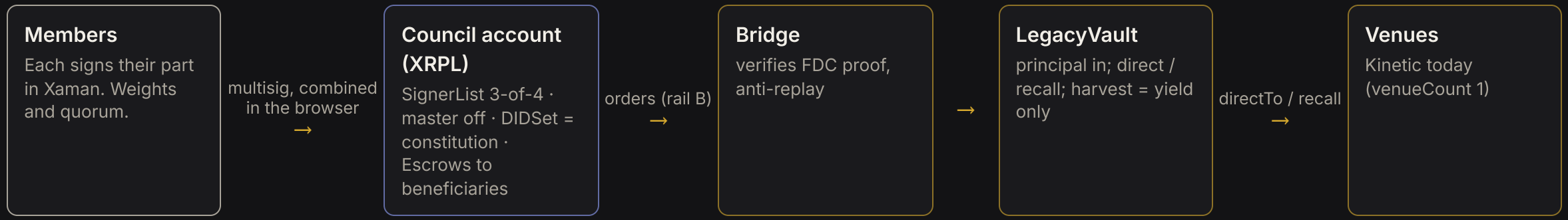
Proposed by the council, waits **30 days**, requires verified continuity of council, constitution and asset. Changing the rules means moving to a successor, not editing a setting.

What exists

- ✓ Principal moves only vault ↔ allow-listed venues (typed: ERC-4626, Compound-v2). Adding a venue waits 30 days.
- ✓ `harvest()` distributes **yield only**: lineage (capitalized, floor 10 % ceiling 40 %), payees, protocol fee (0).
- ✓ Every governing call requires the current `constitutionRef`.
- ✓ The director's seat can be ceded temporarily (`cede / endCession`) — never the exit.
- ✓ Scheduled payments to beneficiaries via XRPL Escrow: finish is permissionless; the ledger fixes destination and dates.

THE WHOLE STRUCTURE

People → council → bridge → vault → venues. Yield → lineage and beneficiaries.



XRPL PRIMITIVES

SignerList · DisableMaster · DIDSet · Tickets · Escrow · Payment + memo · Source Tag (survives multisig)

FLARE PIECES

FDC XRPPayment · Smart Accounts (council's PA) · FAssets FXRP · XrplCouncilBridge · LegacyVault · LegacyStackFactory

LEGAL VEHICLES

The same ceremony, seven legal shapes. The link lives on the root.

TYPOLOGY	WHO	LEGAL VEHICLE	STATE
T1 Personal with rules (reinforced)	one person, three keys	none (+ a will)	LIVE ceremony
T2 Family without an entity	a family, a council	private agreement	LIVE mainnet (template `familiar`)
T3 Minors / education	parents → child	parental authority, gift	template; coming-of-age credential missing
T4 Marital	a couple	marriage contract + regime	legal opinion pending
T5 Operating company	a commercial company	company + by-laws mirrored on chain	designed; Astryum's own company is the dogfood
T6 Patrimonial holding	partners with ownership	closed holding company	designed
T7 Foundation	beneficiaries without ownership	private foundation	template; the target model

Every vehicle has ONE root on XRPL, and the credentials on that root are the link to its legal existence. SignerList = the board or the trustees; DIDSet = the by-laws; credentials (company existence, trustee, sector) issued by a notary, a register or a trust-service provider — never by Astryum. When the root is the board's SignerList, a multisigned CredentialAccept *is* the board's resolution.

WHAT A STRUCTURE HAS TO SETTLE — AND WHERE ASTRYUM STOPS

Ten axes. One perimeter.

- **Ownership** — the vehicle, or its declared absence.
- **Organs and quorum** — SignerList with weights.
- **Membership** — credentials + a rotation ceremony.
- **Beneficiaries** — beneficiary credentials + governed MoneyFlows.
- **Continuity** — succession on a legal-fact credential (death, incapacity).
- **Supremacy** when law and ledger diverge — a clause + anchored hash + curing ceremony with a delay.
- **Exit of all capital** when the law demands it — the “release vessel” via migrate (not built).
- **Privacy** — hashes and pointers, never data on the ledger.
- **Tax** — an opinion; we never advise.

Astryum’s perimeter

Software, templates, ceremonies and a verifier. **Never** custodian, signer, administrator, trustee, issuer or registrar. The legal wrapper belongs to the family and their notary; Astryum provides the rail. Credentials are issued by third parties: the chain of trust always ends in a regulated party in the real world.

Copy rule: never “licensed”, “regulated” or the name of a regulation. Only *a credential verified on the ledger.*

WHAT IS LIVE ON MAINNET

A real council, real orders, real capital — read on 15 September 2026.

3 of 4

real council: quorum enforced by XRPL, master key off, constitution anchored (DIDSet)

4

orders executed end to end (bridge nextNonce = 4); first on 29 Jul; last in 1 min 40 s

≈4.70 FXRP

in the vault, one venue, lineage fee 30 % — under the 5 XRP own-capital cap

22 Jul · 5 Aug

bridge + vault deployed · factory deployed (one cage per Legacy)

Tests

Foundry: LegacyVault 22 + 3 invariants · XrplCouncilBridge 18 · LegacyStackFactory 15 — inside the repository's 168/168.

Reinforced account — the same dial, personal size

2-of-3 of your own keys, master off, no constitution, no cage. Same ceremony; a shorter one. Landmines refused and documented: a RegularKey is an OR, a pure 2-of-2 is a freezer, closing the master needs the master.

TRUST MODEL

Who can move the family's capital alone? Nobody.

A member?

No. The quorum is enforced by the network and the single key is off. Re-enabling it needs the same quorum.

Astryum?

No — by absence of capability. We never hold a key; the relayer carries bytes the quorum already committed to. The contract has no owner we could use and no function that pays principal to an address.

If Astryum disappears?

The council signs from any XRPL client; the vault unwinds positions on redeem; the constitution and the credentials live on the family's own account. Nothing needs our permission.

Failures we already had, and what they built: a signed order took forty minutes to execute while the screen said "done" → no screen turns green before real settlement · a repeated signature could double-dispatch → only an error that proves nothing left allows a retry · the escrow keeper stamped the project tag → two explicit attribution modes, fixed by tests.

NEXT AND AFTER

Ceremonies still to build — and the arm that reaches other chains.

NEXT Ceremonies

- **Rotation** — a credential (appointment / legal fact) → verification → SignerListSet. The transversal primitive.
- **Succession** — a legal-fact credential (death, incapacity) + a designated successor → rotation or release.
- **Amendment** — new text + new anchored hash, atomic in intention.
- **Release vessel** — the exit of all capital when the law demands it, via migrate with its 30-day anti-coercion delay.
- The on-ledger door on the anchor (DepositAuth + credential preauth) switched on in mainnet.

LATER Cage v2 and protocol-managed wallets

- The family moves to the cage v2 (registry-governed venues, payee cap in the cage) when Flare's protocol-managed wallets exist.
- A TEE key as *one signer among people* in the SignerList: native to XRPL; Flare governs when it signs.
- Capital in wallets the cage governs on other chains — a locked arm: cannot be taken out, can be put to work. Isolated module; frame exists, arm reverts on purpose.

EVIDENCE

Check it on an explorer. /proof does it in your browser.

XRP Ledger

```
Legacy order anchor rK4tsuGhmbhaNQuvucL8n1RKLtARBCp3qm
FAssets Core Vault rfkXSaCZKTg1EZzec2rLDyrWHxRVJdtVXj
Source Tag 2607090002
```

Flare (chain 14)

```
XrplCouncilBridge 0x02aE9fcB76768e42b8D3Ed9FE842238A6616b26F
LegacyVault 0xc8379c79779cCE3B738424892709fe0D4339E3b1
LegacyStackFactory 0xF93A8A0bd93e95514fF02285349b0b1c1a5a3e0a
Constitution ref 0x7884821f…efc36 · 4 orders executed
```

Sample order (1 Aug): XRPL tx `720C2D1D…898D4` → Flare tx `0x241c4efd…8b1e` (recall). Product: astryum.xyz/app/legacy · /proof · code: GitHub.

ASTRYUM LEGACY

Governance on the XRP Ledger. Rules on Flare. Nobody moves the capital alone.

Not a member. Not us.