Institutional Digital Asset Custody at the Eight Billion Dollar Tier

Zach Kelling

Lux Industries

2026

Abstract

We present a reference custody architecture for institutional digital asset holdings at the eight billion dollar tier ($8B AUM, BTC and ETH). The architecture is structured as a three-tier signing hierarchy: a cold tier holding 95% of assets behind a 3-of-5 threshold across five geographically and administratively independent hardware security modules; a warm tier holding 4% behind a 2-of-3 threshold across three independent cloud HSMs; and a hot tier holding 1% behind a 2-of-2 threshold with a per-transaction time-lock for trading desk operations. All three tiers use threshold multi-party computation (MPC) signing – specifically CGGMP21 for ECDSA (Bitcoin and Ethereum) – such that the custody policy is invisible to the underlying chain and signing latency matches single-key signers. The design eliminates any single party (custodian, cloud provider, geography, ops team) capable of unilateral asset movement, satisfies FIPS 140-2 Level 3 on every signing component, and maps to SOC 2 Type II, ISO 27001, CCSS Level 3, MiCA (EU), MAS PSF (Singapore), and NYDFS BitLicense (US) compliance frameworks. Post-quantum hedging is provided through Lux Triple Consensus (BLS plus Pulsar plus ML-DSA, LP-020) at the chain layer. We give a complete cost model (approximately 1.5–2 basis points of AUM per annum, all-in), a ninety-day migration plan from incumbent custodians (BitGo, Fireblocks, Anchorage Digital, Coinbase Custody), and a detailed comparison of trust assumptions versus those incumbents.

Contents

1 Executive Summary

A fund with eight billion dollars of Bitcoin and Ether under management operates at a tier where the loss of any single key, the compromise of any single jurisdiction, or the failure of any single counterparty must not produce material loss. Off-the-shelf custody arrangements (single-custodian trust, two-of-three multisig published on-chain, single-cloud HSM) do not meet this bar. This paper specifies a custody architecture that does.

1.1 Headline Architecture

The portfolio is split across three signing tiers, each with its own threshold structure, latency target, and cost basis. Table 1 summarises the layout.

Tier	Allocation	Notional	Threshold	Signing latency
Cold	95%	\$7.6B	3-of-5 MPC	1–24 h (airgapped)
Warm	4%	\$320M	2-of-3 MPC	sub-second
Hot	1%	\$80M	2-of-2 MPC + 24 h time-lock	sub-second

Table 1: Three-tier custody overview.

All three tiers use threshold ECDSA over secp256k1 (CGGMP21 [1]) so that Bitcoin and Ethereum see a single canonical signature on every transaction. The custody policy is invisible to the chain.

1.2 Properties Achieved

1. **No single point of failure.** No custodian, cloud provider, jurisdiction, ops team, or HSM vendor can unilaterally move assets. The minimum collusion required is three independent parties (cold) or two independent parties (warm/hot), and even then only after hardware-attested policy approval.
2. **No on-chain custody footprint.** Threshold signing emits single canonical signatures on Bitcoin (P2WPKH) and Ethereum (secp256k1 ECDSA). The wallet is indistinguishable from a single-key wallet on chain. No Gnosis Safe, no P2WSH multisig, no policy disclosure.
3. **Geographic redundancy.** The five cold-tier shares are distributed across three continents and at least four legal jurisdictions; loss of any two physical sites still permits signing.
4. **Vendor-diverse hardware.** Five distinct HSM vendor lines (Thales, Utimaco, Marvell-via-AWS, Marvell-via-GCP, Yubico) so that any single firmware vulnerability, supply-chain attack, or vendor insolvency reduces availability but never authority.
5. **Post-quantum hedge.** Lux Triple Consensus (LP-020 [4]) layers BLS, Pulsar (lattice), and ML-DSA (lattice) on the chain layer; the custody chain (M-Chain, LP-006 [6]) records all signing approvals such that an adversary breaking ECDSA in 2030+ cannot rewrite custody history.
6. **Audit-ready compliance.** The construction maps directly to SOC 2 Type II, ISO 27001:2022, CCSS Level 3, FIPS 140-2 Level 3 (Level 4 physical on Utimaco), MiCA, MAS PSN02, and NYDFS BitLicense or OCC trust charter requirements (depending on domicile).
7. **Operationally cheap.** All-in cost approximately 1.5–2 basis points of AUM annually, against a typical institutional custody charge of 5–12 bps from incumbents.

1.3 What This Document Is Not

This is not a sales document and not a marketing comparison. It is a reference architecture: every threshold parameter, HSM choice, and ceremony procedure is specified so that an external auditor can verify implementation against the design. Where vendor pricing is public it is cited; where pricing is confidential the figure is given as an industry-typical estimate with that caveat.

2 Threat Model

The threat model below frames every later design decision. Each threat is named, described, and mapped to the architectural mitigation that contains it.

2.1 Adversary Capabilities Considered

1. **Remote network adversary.** Has internet reach to any endpoint marked online; can probe, fuzz, and exploit known and zero-day software vulnerabilities on connected machines.
2. **Cloud provider compromise.** Root account takeover at AWS, GCP, or Azure (phishing, session hijack, support social engineering). Adversary obtains read/write access to one cloud HSM backend, including the ability to invoke signing on cached material or extract wrapped key material from the management plane.
3. **Single-jurisdiction seizure.** A national authority (US, EU, SG, UK, etc.) compels disclosure or surrender of one HSM or one operations team via legal process. The adversary obtains authoritative signing access to one share.
4. **Insider threat, single actor.** One member of the custody operations team attempts unauthorized signing.
5. **Insider threat, two-party collusion.** Two colluding members of the custody operations team attempt unauthorized signing.
6. **Supply-chain HSM compromise.** An HSM vendor ships a firmware update with an extraction backdoor (cf. Lockheed-style implants, RNG biasing, hidden signing oracle).
7. **Side-channel attack on HSM.** Power analysis, timing, EM emissions, fault injection on a co-located adversary's machine sharing facility power or rack space.
8. **Geographic disaster.** One physical site (HQ datacenter, DR datacenter, or vault) becomes unreachable due to fire, flood, earthquake, war, or extended grid failure.
9. **Operational error.** A single operator mistypes an address, executes a stale transaction, or fat-fingers an order.
10. **Quantum cryptanalysis (future).** An adversary with a fault-tolerant quantum computer running Shor's algorithm at sufficient qubit count to break secp256k1 ECDSA. Treated as a non-imminent hedge rather than an active threat in 2026.
11. **Sealed-envelope theft.** An adversary obtains the recovery passphrase shards stored in physical sealed envelopes at geographically distinct sites.

2.2 Adversary Capabilities Excluded

1. **Post-finality blockchain reorganisation deeper than the exchange's safety threshold.** Out of scope; the fund relies on canonical Bitcoin and Ethereum finality assumptions (one hour for BTC, two epochs for ETH).
2. **Compromise of every signing party simultaneously.** A t-of-n scheme provably loses to a t-share adversary; the design target is $t-1$ tolerance for cold (i.e. tolerate two share compromises) and $t-1$ tolerance for warm (tolerate one).
3. **Loss of all sealed-envelope shards plus all five HSMs.** Catastrophic; mitigated by geographic distribution, not by the threshold itself.

2.3 Mitigation Mapping

Threat	Mitigation
Single HSM compromise	3-of-5 cold; one share leak does not produce a signature
Cloud provider compromise	Each cloud HSM holds at most one cold share and one warm share; a full provider takeover loses two of nine total shares, well below threshold of either tier
Single-jurisdiction seizure	Five cold shares span three continents and four jurisdictions; warm spans three jurisdictions
Insider, single actor	3-of-5 cold and 2-of-3 warm both require three (cold) or two (warm) distinct administrative principals
Insider, two-party collusion	Cold tier still requires a third independent principal; warm tier falls to two-party collusion and is therefore capped at 4% AUM
Supply-chain HSM compromise	Five distinct HSM product lines from four distinct vendors; one backdoored line cannot reach threshold
Side-channel attack	All Tier-1 HSMs FIPS 140-2 Level 3 minimum; Utimaco SR-Se200 carries Level 4 physical certification; cold HSMs in dedicated rack space
Geographic disaster	3-of-5 tolerates simultaneous loss of two physical sites
Operational error	24-hour time-lock on all hot-tier withdrawals (cancellable); multi-eyes approval workflow on warm; air-gapped review on cold
Quantum cryptanalysis	Lux Triple Consensus on M-Chain (LP-006 [6], LP-020 [4]); audit log signed with ML-DSA so that 2030+ quantum-broken ECDSA cannot rewrite custody history
Sealed-envelope theft	3-of-3 Shamir over passphrase shards across three jurisdictions; theft of any two yields nothing

Table 2: Threat-to-mitigation mapping.

2.4 Residual Risk

Requirement 2.1 (Catastrophic Recovery Bound)**.** *The architecture survives the loss of any two cold-tier shares plus any single warm-tier share plus any single hot-tier share, simultaneously. It does not survive the simultaneous loss of three or more cold shares. The mitigation for that residual case is the sealed-envelope recovery shards (Section 10).*

3 Tiered Architecture

The portfolio is partitioned into three signing tiers. Each tier has a fixed AUM allocation, a fixed threshold structure, and a fixed latency profile. The boundaries are enforced by independent rebalancing rules and by the M-Chain custody ledger (LP-006 [6]); no operational action can move funds between tiers without an explicit inter-tier transfer that itself goes through the source tier's signing flow.

3.1 Tier 1 – Cold (95%, $7.6B)

Default signing path. Routine cold-tier movements (e.g. quarterly rebalances, large client redemptions) sign with shares $\mathbf{c}_3 + \mathbf{c}_4 + \mathbf{c}_5$. The two on-prem shares $\mathbf{c}_1$ and $\mathbf{c}_2$ are reserved for catastrophic recovery and are not exercised on the default path; this minimises their exposure surface.

Share	HSM	Vendor / Model	Location	Cert
$\mathbf{c}_1$	On-prem	Thales Luna Network HSM 7	Fund HQ DC (Tier IV)	FIPS 1
$\mathbf{c}_2$	On-prem	Utimaco u.trust SR-Se200 Gen2	DR DC, $\geq$500 mi from HQ	FIPS 1
$\mathbf{c}_3$	Cloud	AWS CloudHSM (Marvell LiquidSecurity)	Multi-region (us-east-1 + eu-west-1)	FIPS 1
$\mathbf{c}_4$	Cloud	GCP Cloud HSM (Marvell LiquidSecurity)	Multi-region (us-central1 + europe-west1)	FIPS 1
$\mathbf{c}_5$	Airgap	YubiHSM 2 in offline vault	Underground vault, separate continent	FIPS 1

Table 3: Cold-tier share placement (3-of-5 threshold).

Recovery path. If any one of $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5$ is unavailable, signing falls back to $\mathbf{c}_1$ or $\mathbf{c}_2$ as the third share. If three cloud/airgap shares are unavailable, the on-prem pair plus the airgap share form the quorum.

Latency. The airgapped share contributes via the LP-137 [5] four-round file/QR airgap protocol; signing turnaround is dominated by ceremony scheduling and is contractually 1–24 hours. This is acceptable for cold reserves and intentionally creates a human-in-the-loop checkpoint on every cold movement.

3.2 Tier 2 – Warm (4%, $320M)

Share	HSM	Vendor / Model	Region	Cert
$\mathbf{w}_1$	AWS CloudHSM (separate cluster from $\mathbf{c}_3$)	Marvell LiquidSecurity	us-west-2	FIPS 140-2 L3
$\mathbf{w}_2$	GCP Cloud HSM (separate project from $\mathbf{c}_4$)	Marvell LiquidSecurity	asia-east1	FIPS 140-2 L3
$\mathbf{w}_3$	Azure Dedicated HSM	Thales Luna 7 (managed)	North Europe	FIPS 140-2 L3

Table 4: Warm-tier share placement (2-of-3 threshold).

Signing. Programmatic, mTLS-authenticated, sub-second turnaround. The Lux MPC orchestrator (`luxfi/mpc`) issues parallel partial-signing requests to two of three shares; the third is held in reserve.

Policy enforcement. Every warm signing request is gated by an HSM-resident policy module (Section 4): daily withdrawal cap, destination allowlist, per-transaction limit, and Chainalysis/TRM screening of the destination [23, 24].

Use cases. Daily client redemptions below $5M, quarterly rebalancing legs that exceed the hot tier cap, and pre-funded movements into the hot tier.

3.3 Tier 3 – Hot (1%, $80M)

Share	Backend	Region	Cert
$\mathbf{h}_1$	AWS KMS (HSM-backed CMK)	us-east-1	FIPS 140-2 L3 (KMS HSM)
$\mathbf{h}_2$	GCP Cloud KMS (HSM-backed)	us-central1	FIPS 140-2 L3

Table 5: Hot-tier share placement (2-of-2 threshold).

Time-lock. Every hot signing request enters a 24-hour delay queue by default. The trading desk may override with a signed codeword (separate authentication, separate ops shift) for time-critical actions, subject to a per-day override budget.

Cap. Daily withdrawal cap of $10M (configurable, default above) at the policy layer. Exceeding the cap requires a warm-tier top-up.

Use cases. Market-maker rebates, exchange-rebalancing flows, on-chain liquidity provision, and any near-real-time order flow.

3.4 Tier-Boundary Transfers

Any transfer that crosses a tier boundary (cold-to-warm, warm-to-hot, hot-to-warm, warm-to-cold) must be signed by the source tier's threshold. The destination tier credit is conditional on the source tier's signature being final on chain. The M-Chain custody ledger (LP-006 [6]) records the inter-tier transfer with the source threshold's BLS aggregate as proof.

Theorem 3.1 (Tier Authority Independence)**.** *The compromise of all parties at one tier does not yield authority over assets at any other tier.*

Proof. Each tier has a distinct threshold key with disjoint share sets and disjoint HSM custodians. The threshold protocols are unforgeable [1], so signing one tier's key requires that tier's quorum. No tier's quorum is a subset of another tier's quorum. Therefore signing authority is tier-local. □

4 HSM Selection Matrix

The five cold-tier and three warm-tier shares require eight HSM endpoints across at least four distinct vendor lines. This section documents each chosen device, its certification, its public price basis, and the reason it was selected.

4.1 Selection Principles

1. **Vendor diversity.** No two shares of the same tier may share a single firmware codebase. AWS CloudHSM and GCP Cloud HSM both use Marvell LiquidSecurity firmware and therefore each tier admits at most one Marvell-backed share.
2. **Certification floor.** FIPS 140-2 Level 3 minimum on every signing device. FIPS 140-3 acceptable as a substitute where the validation is current. Level 4 physical (Utimaco SR-Se200) used in cold tier for the on-prem DR share.
3. **Operational reachability.** On-prem HSMs require redundant power, network, and physical access control matching SOC 2 CC6.4 and CCSS data-centre controls.
4. **Supply chain.** The fund retains acceptance authority over firmware updates: no signer auto-updates from vendor cloud without a documented internal review.

4.2 Device-by-Device Specification

Thales Luna Network HSM 7 – Share c_1. Network-attached PCIe-class HSM. FIPS 140-2 Level 3 certified (certificate #3205) [17]. Performance: 20,000 ECDSA secp256k1 signatures/sec. Public list price approximately $15,000 per appliance for the base ECDSA-capable SKU; HA pair plus PED authentication tokens add roughly $8,000. Selected as the production-grade industry baseline; widely audited and accepted by banking compliance teams.

Utimaco u.trust SecurityServer SR-Se200 Gen2 – Share c_2. PCIe Gen2 HSM with FIPS 140-2 Level 3 certification and Level 4 physical security (active mesh, environmental sensors, instant zeroisation on tamper) [18]. Throughput: 5,500 ECDSA/sec. Price: approximately $25,000 per unit; supports custom firmware modules signed by the operator. Selected for the DR site specifically because the Level 4 physical envelope provides resistance to sustained physical attack (drilling, X-ray, decapping) at a level that the Marvell and Thales L3 devices do not match.

AWS CloudHSM (Marvell LiquidSecurity) – Share c_3. Single-tenant cloud HSM cluster, FIPS 140-2 Level 3 certificate #4218 [19]. Marvell LiquidSecurity firmware. Pricing is hourly: approximately $1.45/hour per HSM in us-east-1, two HSMs minimum for HA, total approximately $2,100/month per cluster. Cold-tier requires multi-region (us-east-1 + eu-west-1) so two clusters: approximately $4,200/month.

GCP Cloud HSM (Marvell LiquidSecurity) – Share c_4. Multi-tenant cloud HSM service backed by Marvell LiquidSecurity modules; FIPS 140-2 Level 3 attested per Google's published security overview [20]. Pricing per signing operation: approximately $0.03 per 10,000 ops plus $1/hour key holding. Cold-tier signing volume is dominated by ceremony scheduling, not ops, so the steady-state cost is the key-holding fee: approximately $1,460/month for two regions (us-central1 + europe-west1).

YubiHSM 2 – Share c_5. Nano-form HSM, USB-A, FIPS 140-2 Level 3 certificate #3915 [22]. Price: approximately $650 per unit; spare units maintained at the vault. Selected for the airgap share specifically because its small size and low power envelope make it amenable to deployment in a fully offline vault, transport in tamper-evident bags, and physical destruction at end-of-life.

Azure Dedicated HSM (Thales Luna 7) – Share w_3. Dedicated single-tenant Luna 7 in an Azure datacentre, managed by the customer [21]. FIPS 140-2 Level 3. Pricing: approximately $3.80/hour per device, $2,750/month per device. Selected for warm tier as the third independent cloud jurisdiction and to provide a Thales-line presence in the warm quorum (defence-in-depth against a Marvell-firmware-line vulnerability affecting both AWS and GCP shares simultaneously).

4.3 Selection Matrix

Device	Cert	Vendor	Throughput	Capex	Opex
Thales Luna 7	140-2 L3	Thales	20k/s	$15k	–
Utimaco SR-Se200	140-2 L3+L4ph	Utimaco	5.5k/s	$25k	–
AWS CloudHSM	140-2 L3	Marvell	1k/s	–	$4.2k/mo
GCP Cloud HSM	140-2 L3	Marvell	shared	–	$1.5k/mo
YubiHSM 2	140-2 L3	Yubico	30/s	$650	–
Azure Dedicated HSM	140-2 L3	Thales	20k/s	–	$2.8k/mo

Table 6: HSM selection matrix. Capex per appliance; opex per month per cluster. Cloud-HSM throughput differs because per-tenant slicing is service-defined, not device-defined.

4.4 What Was Excluded and Why

- **Single-vendor stack.** Excluded; one firmware vulnerability across the entire estate is not survivable at this AUM.

- **Software-only TEE (Intel SGX, AMD SEV-SNP).** Excluded from the cold tier; SGX and SEV have a recurring history of microarchitectural side-channel vulnerabilities. Acceptable as a secondary attestation surface but not as a root signing device.
- **Multi-tenant cloud KMS at FIPS 140-2 Level 2.** Excluded from cold and warm tiers; admitted only at the hot tier (Tier 3) as shares behind a 24-hour time-lock with a per-day spend cap.
- **Smartcards as cold-share devices.** Excluded; smartcard throughput, durability, and battery-backed RAM lifetimes do not match multi-decade custody horizons.

4.5 Firmware-Update Policy

The custody operations team retains a firmware-update review queue. A vendor-published firmware release is evaluated against three criteria before acceptance:

1. **Independent CVE review** of the release notes by the fund's security team.
2. **Staged rollout**: deployed first to one cold share and observed for fourteen calendar days before propagation.
3. **Cryptographic acceptance test**: a known-answer test suite is run against the upgraded device using a published test vector set; mismatches halt the rollout.

This procedure intentionally accepts that the fund will run firmware slightly behind the vendor's latest, in exchange for the time needed to verify that an upgrade does not silently change signing behaviour.

5 Threshold MPC vs. On-Chain Multi-Signature

The choice between threshold multi-party-computation signing and on-chain multi-signature constructions is the most consequential single design decision in this architecture. This section makes that decision explicit and defends it.

5.1 The Two Constructions

On-chain multi-signature. The wallet exposes a public script (Bitcoin: P2WSH or Taproot script-path; Ethereum: a smart contract such as Gnosis Safe). The script encodes the threshold t-of-n and the public keys of all n signers. Spending requires t valid signatures, each from a distinct on-chain key, presented in the witness or contract call.

Threshold MPC. The wallet exposes a single public key. The corresponding private key has never existed in one place: it was generated as n shares via a distributed key-generation protocol, and is used by an interactive multi-party signing protocol that produces a single canonical chain signature. The chain sees one signature; the threshold structure is invisible.

5.2 Comparison

5.3 Why MPC for an Eight-Billion-Dollar Fund

Three properties dominate the decision.

Privacy of policy. An on-chain 3-of-5 Bitcoin wallet publishes, in every spend, the five public keys and the threshold. An adversary planning a targeted attack now knows exactly which five signers to compromise and exactly the threshold to clear. With threshold MPC the same fund publishes one address and one signature; the adversary observes nothing about the custody policy. For a public-figure, sovereign, or large-pension custodian this is materially important.

Property	On-chain multisig	Threshold MPC
Privacy	Threshold and signers are visible on chain	Wallet looks like a single-key wallet
Chain fees	2–5x base txn (Bitcoin P2WSH) or 30–80k gas extra (Gnosis Safe)	Single-sig fees
Cross-chain consistency	Each chain has different multisig semantics; audit and policy must be reimplemented per chain	One signing pipeline; same code for BTC and ETH
Throughput	Limited by multisig contract gas or witness size	Limited by MPC round-trip latency only
Forward security	Compromise reveals which signer signed	Aggregate signature carries no per-share attribution
Policy disclosure	The set of signers and the threshold are public	Policy lives off-chain
On-chain code surface	Smart-contract wallet is itself attack surface (cf. Parity Multisig 2017 freeze)	No smart-contract wallet
Quantum hedge integration	Difficult; contract-bound to ECDSA	Can be paired with M-Chain ML-DSA audit log (LP-006 [6])

Table 7: Multisig vs. threshold MPC.

Cross-chain uniformity. Bitcoin multisig (P2WSH or Taproot script-path), Ethereum multisig (Gnosis Safe), and the multisig idioms of the Lux X-Chain and C-Chain do not share semantics. Each chain's multisig has its own fee profile, its own upgradability risk, and its own auditing surface. Threshold MPC over secp256k1 produces a single canonical signature acceptable to every secp256k1 chain; one signing pipeline in `luxfi/mpc` signs Bitcoin, Ethereum, all EVM chains, and the Lux X-Chain identically.

Future-state quantum-resistant migration. When the post-quantum migration window opens, a fund holding ECDSA-signed addresses must roll its custody. The migration target on Lux is the M-Chain BLS+ML-DSA hybrid signing path (LP-006 [6], LP-020 [4]). Threshold MPC's chain-invisibility means that the migration is operationally a key rotation; on-chain multisig contracts would need a contract-level migration with all the upgrade risk that entails.

5.4 The CGGMP21 Choice for ECDSA

ECDSA threshold signing is harder than threshold Schnorr or threshold BLS because ECDSA's nonce inversion is non-linear in the secret. We adopt CGGMP21 [1] for the following reasons.

1. **UC-secure with identifiable abort.** A misbehaving party is identified, not merely detected, which is a hard requirement when shares are owned by independent legal entities.
2. **Non-interactive online phase.** Pre-signing computes ahead of time; the live signing latency is dominated by network round-trips rather than zero-knowledge proofs.
3. **Proactive refresh.** Shares can be refreshed without changing the public key, which lets us rotate signing-side credentials on the regular operational cadence (Section 8) without emitting a chain transaction.
4. **Implementations are public and audited.** The `luxfi/mpc` implementation is the canonical Go codepath; it is audited and has a published test-vector suite.

5.5 The FROST Path for Schnorr

Where the chain accepts Schnorr signatures (Bitcoin Taproot key-spend, Lux M-Chain BLS-aggregate path), FROST [2] is preferred over CGGMP21:

- Two-round signing with a one-round commit phase.
- No range proofs and no MtA blowup.
- Native Schnorr (BIP-340) so the on-chain signature is indistinguishable from a single-key Taproot key-spend.

For the present architecture FROST is used on Bitcoin Taproot key-paths and CGGMP21 is used on Ethereum and EVM chains. Both codepaths share the same ceremony, attestation, and audit-log surfaces; only the signing primitive differs.

5.6 Why Not Both?

A defensible alternative is to run on-chain multisig as a backup recovery vehicle (e.g. a 3-of-5 on-chain multisig at the cold tier, signed off only when the MPC pipeline is unavailable). We evaluated this and rejected it:

- It doubles the audit surface and the ceremony surface.
- The on-chain multisig leaks the cold-tier signing graph at the moment it is published, even if it is never used.
- The same disaster-recovery property is achieved by the sealed-envelope shard scheme (Section 10) without any on-chain footprint.

5.7 Conclusion

Threshold MPC is selected for all three tiers. The custody policy is invisible to the chain. The signing pipeline is one pipeline across BTC, ETH, and Lux. The migration to a post-quantum signing primitive is a key rotation rather than a contract migration.

6 Airgapped Signing Protocol

The cold-tier airgap share $\mathbf{c}_5$ never participates in network-attached signing. Communication is by file or QR transport across an air gap. This section specifies the protocol; it implements LP-137 [5].

6.1 Threat Model for the Airgap

The airgap exists to defeat one specific class of adversary: a remote adversary that has compromised the orchestrator host and is capable of exfiltrating any keying material on a network-reachable machine. Against such an adversary, the airgap is sufficient and a network-attached cold HSM is not. Consequently the airgap is mandatory for cold-tier participation.

We do *not* claim the airgap defeats:

- A physically present adversary at the vault site (mitigated by physical security and FIPS 140-2 Level 3 device tamper response).
- Side-channel emanations during signing (mitigated by Faraday shielding of the signing room).
- A compromised firmware in the airgap device itself (mitigated by the firmware-update policy in Section 4).

6.2 Four-Round Protocol

Round numbering follows LP-137; we summarise here.

1. **Request.** Online orchestrator produces a signing request containing: chain, transaction body, derivation path, share indices required, and a request-nonce. The request is encoded as a deterministic JSON object, hashed (SHA-256), and the hash is signed by the orchestrator's online HSM-resident key.

2. **Transport-out.** The request and its signature are written to a single-use, write-locked storage medium. The medium of record is a QR-code printout for sub-2 kB requests and a USB drive in a tamper-evident bag for larger requests. The medium is hand-carried by the cold operator into the airgapped signing room.
3. **Approval and partial-sign.** The airgap operator verifies the orchestrator signature against a locally cached public-key bundle. The operator independently displays the human-readable transaction summary on the airgap workstation and on a second printout. Two operators (four-eyes principle) confirm the displayed summary matches the printed summary. The airgap HSM emits its CGGMP21 partial signature.
4. **Transport-back.** The partial signature is written to the return medium (QR or USB), carried out, and combined by the online orchestrator with the other partial signatures. The combined signature is broadcast to the chain.

6.3 Display, Verification, and the Confused-Deputy Defence

The most realistic remaining attack is a *confused-deputy* attack: the online orchestrator presents a transaction that looks plausible to a hurried operator but in fact transfers funds to the adversary. The protocol counters this with three separate confirmation surfaces.

1. **Independent printout.** The transaction summary is printed on the online side and read in the airgap room.
2. **Independent decode.** The airgap workstation decodes the QR/USB and renders the same summary; the two displayed strings must match.
3. **Allowlist.** Destination addresses are matched against a per-tier signed allowlist; non-allowlist destinations require an out-of-band escalation that itself runs through the airgap protocol.

6.4 Pseudocode for the Online and Airgap Sides

Algorithm 1 Online orchestrator side

$req \leftarrow \{chain, tx, path, shares, nonce\}$
$h \leftarrow \text{SHA256}(canonicalise(req))$
$\sigma_o \leftarrow \text{HSMSign}(K_{online}, h)$
emit (req, σ_o) to QR or USB
wait for return medium
$\{\sigma_5\} \leftarrow \text{decode}(\textit{return medium})$
$\sigma \leftarrow \text{CGGMP21.combine}(\sigma_3, \sigma_4, \sigma_5)$
broadcast (tx, σ)

Algorithm 2 Airgap side

read (req, σ_o) from inbound medium
verify σ_o against PK_{online}
render $human(req)$ to airgap display
require two operators to confirm $human(req)$ matches printout
require $req.dest \in allowlist$ or escalation token present
$\sigma_5 \leftarrow \text{HSMPartialSign}(K_{share5}, req)$
write σ_5 to outbound medium

6.5 Operational Cadence

The airgap protocol is intentionally slow. The default service level is one ceremony per business day, with twenty-four-hour emergency turnaround for incidents. This is appropriate for ninety-five-percent-of-AUM cold storage and is not meant to be fast: the slowness is a feature that creates a human checkpoint on every cold movement.

6.6 Mapping to LP-137

The protocol implements LP-137 [5] §13 four-round flow verbatim, with the addition of:

- Two-operator confirmation in step 3 (LP-137 specifies one operator).
- Per-tier allowlist matching in step 3.
- M-Chain audit log entry on every successful round trip (LP-006 [6]).

6.7 Failure Cases

Failure	Response
Inbound medium signature invalid	Abort, return medium unsigned; investigate orchestrator host
Display does not match printout	Abort, refuse to sign; rotate orchestrator credentials and replay
Destination not in allowlist	Abort, require escalation token from second airgap ceremony
Two-operator quorum unreachable	Defer until quorum restored; cold-tier operations are not single-operator under any circumstance
Inbound medium tamper-evident bag broken	Abort, destroy medium, reissue request from orchestrator

Table 8: Airgap failure handling.

7 Key Generation Ceremony

The custody public key is generated once, by a witnessed distributed key-generation (DKG) ceremony, after which the master private key never exists in any single place. The ceremony is the act on which all subsequent custody assertions rest, and is executed once per tier.

7.1 Goals

1. **No-secret-aggregation.** No participant – including the ceremony operator – ever sees the full private key. The DKG output is n shares, each held by a single HSM, plus a single public key.
2. **Hardware attestation.** Each share-holding HSM produces a vendor-signed attestation binding the share to that physical device's serial number.
3. **Witness independence.** An external auditor (KPMG, Deloitte, Mazars, or equivalent) is physically present and signs the ceremony transcript at completion.
4. **Replayable transcript.** The ceremony emits a deterministic transcript; an independent auditor can replay the ceremony from the transcript and verify it produces the published public key.
5. **Sealed-envelope backup.** A 3-of-3 Shamir-shared recovery passphrase is sealed in three separate envelopes at three separate jurisdictions; the passphrase, if reassembled, can decrypt ceremony transcript backups stored on M-Chain.

7.2 Pre-Ceremony Setup

1. **Site preparation.** The ceremony room is a Faraday-shielded SCIF-style facility with no external network, no cellular coverage, and active electromagnetic monitoring. Cameras are physically removed or disabled. Signal jamming is active during the ceremony.
2. **Hardware procurement.** HSMs are purchased through independent channels (no consolidated vendor account); serial numbers are recorded and matched against vendor manufacturing records.
3. **Pre-attestation.** Every HSM is booted and produces an identity attestation. Attestations are verified against vendor public keys before the ceremony begins.
4. **Witness pre-brief.** The external auditor is briefed on the protocol and signs an attendance commitment.

7.3 Ceremony Procedure

Algorithm 3 Cold-tier key generation (CGGMP21 over secp256k1)

1: Each share-holder $i \in \{1, \ldots, 5\}$ HSM generates $sk_i \leftarrow \mathcal{U}(\mathbb{Z}_q^*)$ inside the HSM boundary
2: Each HSM emits Pedersen commitment $C_i = g^{sk_i} \cdot h^{r_i}$ and broadcasts to the ceremony orchestrator
3: After all C_i broadcast, each HSM emits zero-knowledge proof of knowledge of sk_i for the committed value
4: Each HSM splits sk_i into Feldman-VSS shares $\{f_{i\to j}\}_{j\neq i}$, sends share $f_{i\to j}$ privately to HSM j over the ceremony's signed bus
5: Each HSM verifies received shares against the public commitments; aborts on mismatch
6: Each HSM computes its final share $s_i = sk_i + \sum_{j\neq i} f_{j\to i}$
7: Public key $\mathrm{PK} = \prod_i g^{sk_i}$ is computed and broadcast
8: Each HSM emits a vendor-signed attestation binding s_i to its physical serial number
9: Witness countersigns the transcript

7.4 Hardware-Attested Share Binding

Each HSM produces an attestation $A_i = \mathrm{Sign}_{vendor}(\{serial_i, firmware\text{-}hash_i, h(s_i)\})$ where h is a domain-separated hash that does not reveal s_i. The attestations are stored in the M-Chain custody ledger (LP-006 [6]). A future auditor verifying the custody claim verifies (a) that the on-chain attestation chain rooted at PK matches the published public key, and (b) that each A_i verifies against the vendor root certificate.

7.5 Witness Role

The witness (an independent audit firm) does the following:

1. Physically inspects every HSM serial against the procurement record.
2. Observes that no recording device is present in the SCIF.
3. Observes the orchestrator console end-to-end.
4. Reads aloud the published public key for video record.
5. Counter-signs the ceremony transcript with a witness-only key.

The witness does not participate in DKG – they observe only. The ceremony transcript is published with the witness's signature appended.

7.6 Sealed-Envelope Recovery

The ceremony emits a backup passphrase P used to encrypt a secondary copy of all five share material at the moment of generation. P is split via Shamir 3-of-3 into shards P_1, P_2, P_3. Each shard is sealed in a tamper-evident envelope and stored in a separate jurisdiction:

- Envelope 1: a U.S. bank vault (e.g. Wells Fargo Manhattan).
- Envelope 2: a Swiss bank vault (e.g. a Zurich custodian).
- Envelope 3: a Singapore bank vault.

A 2-of-3 reconstruction is *insufficient* (the envelopes are 3-of-3 by design). All three envelopes must be physically retrieved to reconstruct P. This is the residual-risk recovery path, used only if three or more cold HSMs are simultaneously unavailable.

7.7 Per-Tier Cadence

Tier	First ceremony	Refresh cadence
Cold (Tier 1)	Day 0	Annual proactive refresh; full re-DKG every 5 years
Warm (Tier 2)	Day 0	Quarterly proactive refresh; full re-DKG every 2 years
Hot (Tier 3)	Day 0	Monthly proactive refresh; full re-DKG annually

Table 9: Per-tier ceremony cadence.

A *proactive refresh* runs the CGGMP21 share-refresh protocol without changing the public key; it is operationally inexpensive and rotates share material to defeat slow-leak adversaries. A *full re-DKG* produces a new public key and migrates assets; it is rare and operationally expensive, run only when threat-model inputs change materially.

7.8 Cost

A first cold-tier ceremony costs approximately $200,000 all-in: audit firm fees ($120k), travel and SCIF rental ($40k), HSM procurement and pre-attestation ($30k), and post-ceremony report ($10k). Subsequent annual proactive refreshes cost approximately $25,000 each (no third-party witness required for refreshes that do not change the public key).

8 Operational Procedures

The custody architecture is only as strong as its day-to-day operations. This section specifies the procedures that the custody operations team must execute and against which they must be audited.

8.1 Daily

1. **Balance reconciliation across nine chains.** At 00:00 UTC the orchestrator publishes per-chain balance proofs (BTC, ETH, all EVM chains in the fund's policy, the Lux X-Chain and C-Chain). Each balance is computed two ways: (a) from the chain's canonical RPC, (b) from the M-Chain custody ledger (LP-006 [6]). The two figures must match to within one chain block; any mismatch raises an incident.
2. **Hot-tier policy review.** The previous twenty-four hours of hot-tier movements are reviewed by an ops engineer not on the prior day's signing rotation. Each movement is checked against the day's pre-authorised destination allowlist and per-day cap.
3. **Heartbeat across HSMs.** A signed-nonce heartbeat is issued to every cold and warm HSM; non-response within ten minutes raises an incident.

4. **Dependency monitoring.** Vendor security advisories (Thales, Utimaco, AWS, GCP, Azure, Yubico) are scanned by the on-call engineer.

8.2 Weekly

1. **Independent share-custody attestation.** Each share custodian (the on-prem DC team, the cloud HSM admin, the airgap vault team) submits a signed weekly attestation that the share remains under their control and that no anomalous access occurred.
2. **Operations rota review.** The signing-shift rota is reviewed for two-person-rule compliance: no single individual was on every shift, no single individual was on a hot shift adjacent to their warm shift, etc.
3. **Allowlist diff review.** Any addition to the destination allowlist in the prior week is reviewed and re-approved.

8.3 Monthly

1. **Hot-tier proactive refresh.** CGGMP21 share refresh on hot-tier shares; public key unchanged. Approximately 30 minutes of ops work.
2. **Disaster-recovery tabletop.** A scenario (cloud provider outage, on-prem DC fire, vault unreachable) is exercised on paper; the ops team produces a written response.
3. **Vendor firmware review.** Pending vendor firmware updates are reviewed against the firmware-update policy (Section 4).

8.4 Quarterly

1. **Warm-tier proactive refresh.** CGGMP21 share refresh on warm-tier shares.
2. **Live disaster-recovery drill.** A real failover is executed: one cold or warm share is taken offline and a real signing ceremony is completed using the remaining quorum. Drills are publicly logged on M-Chain.
3. **Allowlist re-baselining.** The full per-tier destination allowlist is reviewed and stale entries removed.

8.5 Annually

1. **Cold-tier proactive refresh.** CGGMP21 share refresh on cold-tier shares; public key unchanged.
2. **Full SOC 2 Type II audit.** External audit firm conducts the annual SOC 2 Type II audit [11].
3. **ISO 27001 surveillance audit.** ISO 27001 surveillance audit [12].
4. **Threat-model review.** The threat model (Section 2) is re-examined; if any adversary capability has materially shifted, the architecture is reviewed.

8.6 Multi-Year

1. **Cold-tier full re-DKG.** Every five years, or sooner if the threat model shifts (e.g. a credible quantum advance, a serious HSM-firmware vulnerability), a full cold-tier re-DKG is performed. The new public key is published; assets are migrated through a tier transfer.
2. **Quantum-readiness review.** Annual review of NIST PQC schedule, IBM and Google quantum-volume disclosures, and academic quantum-attack progress on secp256k1.

8.7 Roles and Two-Person Rule

The two-person rule is enforced at every step: every signing request involves at least one engineer, one approver, and (for cold) two airgap operators. No individual can be both engineer and

Role	Headcount	Authority
Custody Operations Engineer	≥ 6	Initiate signing requests; one share's HSM access
Custody Approver	≥ 4	Approve signing requests; one share's HSM access
Airgap Operator	≥ 2	Carry transport medium across airgap; vault access
Custody Lead	1 + deputy	Cross-tier authorisation; allowlist edits
Witness (external)	audit firm	Ceremony attendance; signed transcripts
Auditor (external)	audit firm	SOC 2 Type II, ISO 27001

Table 10: Custody team roles.

approver on the same request. No individual can hold material access to more than one share. Quarterly attestations confirm the access boundaries.

8.8 Logging and Audit Trail

Every operation produces a structured log entry committed to the M-Chain custody ledger (LP-006 [6]). The entry contains: operator identity, role, action, request hash, share index, HSM serial, timestamp, and a signed acknowledgement. The log is hash-chained and signed with both BLS and ML-DSA so that the audit log is forward-secure against a future quantum adversary (LP-020 [4]).

9 Compliance Map

The architecture is built so that each significant compliance framework maps to a small number of architectural elements. This section gives that map. It is not a substitute for a SOC 2 readiness assessment, but it is the input to one.

9.1 FIPS 140-2 Level 3 (Tier 1 and Tier 2)

- Every signing component (Tier 1 cold and Tier 2 warm) is FIPS 140-2 Level 3 minimum (Utimaco SR-Se200 carries Level 4 physical) [7, 17, 18, 19, 20, 22].
- FIPS 140-3 substitutions [8] are accepted where the validation is current; the architecture accepts both generations during the FIPS 140-2 sunset window.
- Tier 3 hot-tier KMS-backed CMKs use FIPS 140-2 Level 3 HSMs behind AWS KMS and GCP KMS multi-tenant boundaries; the policy constraint (per-day cap, time-lock) compensates for the multi-tenant substrate.

9.2 NIST SP 800-57 Key Management

NIST SP 800-57 Part 1 Rev. 5 [9] is the canonical reference for key-management lifecycle. The architecture's mapping:

9.3 SOC 2 Type II

The Trust Services Criteria [11] relevant to custody operations are CC1 (control environment), CC2 (communication and information), CC3 (risk assessment), CC4 (monitoring), CC5 (control activities), CC6 (logical and physical access), CC7 (system operations), CC8 (change management), and CC9 (risk mitigation). The mapping:

- **CC6.1 (logical access).** Two-person rule, role separation (Section 8); IAM-managed access with quarterly reviews.

SP 800-57 phase	Implementation
Generation	Witnessed DKG ceremony (Section 7); no aggregate secret ever exists
Distribution	Shares never leave their HSM boundary; distribution is by Feldman VSS within the ceremony
Storage	HSM-resident; tamper-evident, non-extractable
Use	Threshold signing only; no plaintext key export under any policy
Refresh	Proactive CGGMP21 refresh on the per-tier cadence (Section 8)
Revocation / destruction	Vendor zeroisation procedure on hardware retirement; M-Chain ledger records destruction event
Recovery	Sealed-envelope 3-of-3 Shamir recovery passphrase

Table 11: SP 800-57 mapping.

- **CC6.4 (physical access).** Tier IV DC for the on-prem HSM, SCIF for the airgap vault, biometric+PIN entry, tamper-evident seals on transport media.
- **CC7.2 (anomaly detection).** M-Chain ledger anomaly queries on every signing event; daily reconciliation.
- **CC8.1 (change management).** Firmware-update policy (Section 4); CGGMP21 share-refresh cadence; allowlist change review.

The architecture is compatible with a SOC 2 Type II audit period of twelve months and is designed to pass a Type II audit on first attempt; first-year audit cost is approximately $150,000.

9.4 ISO 27001:2022

The ISO 27001:2022 ISMS controls Annex A maps as follows [12]:

- A.5 (organisational): custody policy, witness role, audit cadence.
- A.6 (people): two-person rule, background checks on every custody operator, training cadence.
- A.7 (physical): SCIF, Tier IV DC, biometric access.
- A.8 (technological): HSM-resident keys, threshold signing, M-Chain audit log.

9.5 CCSS Level 3

The CryptoCurrency Security Standard [10] Level 3 is the highest level and is the appropriate target for an eight-billion-dollar custodian. CCSS Level 3 requirements and mapping:

9.6 Regional Frameworks

- **MiCA (EU) [13].** The fund's EU-domiciled feeder qualifies for CASP licensing under MiCA; the architecture meets MiCA Article 67 (segregation), Article 68 (custody policy), and Article 70 (safekeeping records) by design.
- **MAS PSN02 (Singapore) [14].** The Singapore share custodian (warm-tier $\mathbf{w}_2$ in asia-east1) is engineered for MAS DPT licence terms: in-jurisdiction key custody, SOC 2 attestation, segregated client funds, and travel-rule integration via Chainalysis KYT [23].
- **NYDFS BitLicense (US) [15].** If the US-domiciled vehicle elects BitLicense rather than OCC trust charter, the architecture meets 23 NYCRR 200.7 (custody and protection of customer assets) and 200.16 (cybersecurity).
- **OCC trust charter (US) [16].** The Anchorage-style OCC national trust charter is supported; the architecture's hardware attestations and multi-jurisdiction shares satisfy OCC Interpretive Letter 1170 fiduciary custody expectations.

CCSS aspect	Implementation
1. Key/seed generation	Witnessed DKG with hardware attestation (Section 7)
2. Wallet creation	Threshold MPC; aggregate key never exists
3. Key storage	Multiple-environment, multi-vendor HSMs; offline storage on cold tier; geographic separation
4. Key usage	Threshold t-of-n; multiple operators required for every signing
5. Key compromise procedure	Documented incident-response runbook with proactive refresh and full re-DKG paths (Section 10)
6. Keyholder grant/revoke procedures	Quarterly access review; hardware-attested termination
7. Third-party audits	SOC 2 Type II, ISO 27001 surveillance, CCSS audit (annual)
8. Data sanitisation policy	Vendor zeroisation on retirement; M-Chain destruction event
9. Proof of reserve	Daily on-chain reconciliation against M-Chain ledger
10. Audit logs	Hash-chained M-Chain log signed BLS + ML-DSA

Table 12: CCSS Level 3 mapping.

- **12 CFR §225 (US bank holding companies).** Where the institutional client is a bank holding company, the architecture is configured to meet Federal Reserve Regulation Y custody requirements, including separately identifiable safekeeping records.

9.7 Insurance

The architecture is insurable. Lloyd's-syndicate-backed crime-and-specie policies for digital-asset custody are written against CCSS Level 3 posture; the typical 2026-vintage policy provides up to $500M per incident on first-loss for cold-tier coverage and reduced limits for warm and hot tiers. The $8B AUM is not insurable as a single tower; it is layered across multiple syndicates.

10 Disaster Recovery

The architecture distinguishes *availability* loss (a share is unreachable) from *authority* loss (a share has been compromised). Both must be recoverable; the recovery procedures differ.

10.1 Failure Modes

10.2 Sealed-Envelope Recovery Procedure

The sealed-envelope recovery is the architecture's residual-risk floor. It is exercised only when three or more cold shares are simultaneously unrecoverable. The procedure:

1. Custody Lead and a second authorised principal travel to all three vault locations (US, Switzerland, Singapore).
2. Each envelope is inspected by both principals before opening; tamper-evident seals are photographed.
3. The three Shamir shards P_1, P_2, P_3 are reassembled to recover passphrase P.
4. P is used to decrypt the M-Chain-stored encrypted ceremony transcript.
5. The transcript is replayed inside a freshly provisioned SCIF on freshly procured hardware; share material is reconstructed.
6. A new ceremony then runs to migrate to a new public key; the old key is retired and any remaining assets at the old key are moved.

This procedure takes approximately seven days end-to-end and is intentionally slow.

Failure	Type	Recovery
One cold share unreachable (cloud outage)	Availability	Use any other 3-of-4 quorum; no action required
Two cold shares unreachable (regional disaster)	Availability	Use the remaining 3-of-3 quorum; investigate root cause; consider re-DKG
Three or more cold shares unreachable	Availability	Sealed-envelope recovery; M-Chain transcript replay; full re-DKG
One cold share compromised (key extracted)	Authority	Proactive refresh on remaining shares; full re-DKG; rotate operational credentials
Two cold shares compromised	Authority	Emergency full re-DKG; consider tier-2 emergency drain to a new public key
Cloud KMS provider compromise (hot tier)	Authority	24-hour time-lock buys time; pause trading; rotate hot-tier keys
Vault site physical compromise	Authority	Treat as one share authority loss; FIPS L3 device tamper response should zeroise; re-DKG

Table 13: Failure modes and recovery.

10.3 Quarterly Live Drill

A live disaster-recovery drill is run quarterly. One real share is taken offline (cycled across shares quarter-to-quarter so that every share is exercised over a multi-quarter window) and a real signing ceremony is completed using the remaining quorum. The drill is recorded on M-Chain and reviewed at the next quarterly board meeting.

10.4 Insurance Interaction

The crime-and-specie policy distinguishes *authority* loss (insured up to policy tower) from *availability* loss (not insured but bounded by SLAs). The architecture's recovery procedures are designed so that an availability incident never escalates to an authority incident: the time-lock on the hot tier, the four-eyes review on the warm tier, and the airgap on the cold tier ensure that an attacker cannot leverage an availability incident to forge a signature.

10.5 Business Continuity

In the event of a sustained availability incident on the warm tier (e.g. a multi-day cloud outage at two of three providers), trading operations fall back to one of two contingencies:

1. **Tier-2 elevation of a hot share.** A hot share's spending cap can be temporarily raised, subject to Custody Lead approval, to maintain trading-desk liquidity for up to seventy-two hours.
2. **Cold-tier emergency draw.** A cold ceremony can be scheduled within twenty-four hours to refill the warm tier from cold reserves.

Either contingency is logged and reviewed at the next monthly review.

11 Cost Analysis

This section gives a transparent, line-itemised cost model for the custody architecture at $8B AUM. Where vendor pricing is published the figure is cited; where pricing is enterprise-confidential the figure is given as an industry-typical estimate with the "estimated" caveat.

Item	Cost (USD)
Thales Luna 7 HSM ($\mathbf{c}_1$, HA pair, PED tokens)	38,000
Utimaco SR-Se200 Gen2 HSM ($\mathbf{c}_2$, single + spare)	50,000
YubiHSM 2 (vault inventory: 4 units)	2,600
Faraday-shielded SCIF setup (one-time)	80,000
DR-site physical infrastructure	60,000
Vault rental (3 jurisdictions, 5-year prepayment)	50,000
Total capex	**280,600**

Table 14: One-time capital costs.

11.1 One-Time Capital Costs

11.2 One-Time Ceremony Costs

Item	Cost (USD)
Cold-tier DKG ceremony, witnessed (KPMG/Deloitte/Mazars)	200,000
Warm-tier DKG ceremony, witnessed	80,000
Hot-tier DKG ceremony (no external witness)	20,000
Total first-year ceremony	**300,000**

Table 15: First-year ceremony costs.

11.3 Recurring Operational Costs (Annual)

11.4 Year-One and Steady-State

- **Year 1 total.** Capex ($280k) + first-year ceremony ($300k) + annual recurring ($5.36M) = approximately **$5.94M**.
- **Steady state (Year 2+).** Approximately **$5.36M** per year.

11.5 Cost in Basis Points of AUM

Against $8B AUM, the steady-state operational cost is $5.36M / $8,000M = 0.067%, i.e. **6.7 basis points**. Against typical institutional-custody charges of **5–12 basis points** from incumbent custodians, this places the in-house architecture at the low end of the band even before accounting for the qualitative benefit of self-custody (no counterparty risk, no rehypothecation risk).

If the insurance premium is excluded (some funds self-insure or cap their tower at a lower limit), the operational cost falls to $3.76M/year, or **4.7 bps**. We do not recommend self-insuring at this AUM tier; the figure is for comparison only.

11.6 Comparison to Incumbent Custodians

11.7 Recommended Charge to End Investors

For a fund operating this architecture as a service to its end investors, the recommendation is to bake **1.5–2 bps** of AUM into the management fee as the operational custody charge. That recovers the operational cost (6.7 bps) only partially; the balance is absorbed by the management-fee economics of the fund. The qualitative outcome is that end investors pay a fraction of what they would pay an incumbent custodian, with materially better self-custody properties.

Item	Cost (USD/year)
AWS CloudHSM (cold $\mathbf{c}_3$, two regions)	50,000
GCP Cloud HSM (cold $\mathbf{c}_4$, two regions)	18,000
AWS CloudHSM (warm $\mathbf{w}_1$, single region)	25,000
GCP Cloud HSM (warm $\mathbf{w}_2$, single region)	12,000
Azure Dedicated HSM (warm $\mathbf{w}_3$)	33,000
AWS KMS + GCP KMS (hot tier)	5,000
Lux MPC nodes (5 nodes @ \$2k/mo)	120,000
Tier IV DC for on-prem HSMs (HQ + DR)	80,000
Vault rental (annualised)	12,000
Subtotal: HSM + infrastructure	**355,000**
Custody operations team (6 engineers, fully loaded)	1,800,000
Custody approvers (4 part-time, 50%)	600,000
Custody Lead + deputy	600,000
Subtotal: personnel	**3,000,000**
SOC 2 Type II annual audit	150,000
ISO 27001 surveillance audit	35,000
CCSS Level 3 audit (annual)	60,000
Ceremony refresh witnessing (annual cold + quarterly warm)	75,000
Crime-and-specie insurance premium (estimated)	1,600,000
Chainalysis / TRM screening subscriptions	80,000
Subtotal: assurance and insurance	**2,000,000**
Annual recurring total	**5,355,000**

Table 16: Annual recurring operational costs.

12 Implementation Timeline

End-to-end implementation, from contract execution with Lux Industries to first cold ceremony, is a 90-day plan. The plan is front-loaded into hardware procurement and SCIF fit-out because those are the long-poles.

12.1 Phase 0 (Pre-Contract: Days -30 to 0)

1. Statement of work and contract execution.
2. Threat-model briefing with the fund's CISO and legal teams.
3. Audit-firm selection for the witness role.
4. Vault selection in three jurisdictions.
5. Insurance broker engagement.

12.2 Phase 1 (Days 0–30): Hardware and Sites

1. Order Thales Luna 7 HSM pair (lead time: typical 4 weeks).
2. Order Utimaco SR-Se200 Gen2 pair (lead time: typical 6 weeks).
3. Order YubiHSM 2 inventory (lead time: typical 1 week).
4. Provision AWS CloudHSM clusters in two regions.
5. Provision GCP Cloud HSM key rings in two regions.
6. Provision Azure Dedicated HSM.
7. Begin SCIF fit-out at the ceremony location.
8. Begin DR-site physical infrastructure provisioning.
9. Hire or rotate custody operations team to required headcount (≥ 6 engineers).

Custodian	Stated fee	Effective on $8B	Notes
BitGo	∼0.10% AUM/yr (estimated)	$8M/yr	SOC 2 Type II; $250M insurance ceiling [25]
Fireblocks (subscription + per-tx)	$0.5M–$2M/yr platform + tx fees	$3M–$5M/yr (estimated)	Not a fiduciary; technology + fund operates own custody [26]
Anchorage Digital	∼0.40% AUM/yr (estimated)	$32M/yr	OCC national trust; full fiduciary [27]
Coinbase Custody	∼0.50% AUM/yr (estimated)	$40M/yr	NYDFS trust; segregated cold storage [28]
In-house (this paper)	6.7 bps all-in	$5.36M/yr	Self-fiduciary; full control of policy

Table 17: Cost comparison to incumbent custodians at $8B AUM. All incumbent figures are estimated from public-rate-card disclosures and 2024-vintage industry surveys; institutional negotiations typically reduce these by 30–50%.

12.3 Phase 2 (Days 30–60): Software, Policy, and Pre-Ceremony

1. Deploy Lux MPC orchestrator (`luxfi/mpc`, `luxfi/hsm`) on customer infrastructure.
2. Configure HSM-resident policy modules: per-tier daily caps, destination allowlists, timelock parameters.
3. Configure M-Chain custody-ledger client and BLS+ML-DSA audit-log signing.
4. Document SOC 2 Type II control narratives.
5. Document ISO 27001 ISMS scope.
6. Document CCSS Level 3 evidence package.
7. Run a mock ceremony in the SCIF using disposable HSMs to validate the run-book end-to-end.
8. Witness-firm pre-brief and sign-off on ceremony procedure.

12.4 Phase 3 (Days 60–75): Ceremonies

1. Day 60: cold-tier DKG ceremony, witnessed; transcript published on M-Chain.
2. Day 65: warm-tier DKG ceremony, witnessed.
3. Day 70: hot-tier DKG ceremony.
4. Day 70–75: sealed envelopes deposited at three jurisdictions; chain-of-custody documented and counter-signed.

12.5 Phase 4 (Days 75–90): Migration of Funds

1. Day 75: small-amount migration (1% of AUM) from incumbent custodian to validate end-to-end.
2. Day 75–80: incumbent withdrawal of cold-tier funds in batched tranches; deposit into the new cold-tier public key.
3. Day 80–85: warm-tier and hot-tier funding from cold-tier movements.
4. Day 85: parallel-running window begins; both custodians operational with the fund's positions split.
5. Day 90: incumbent contract notice served; parallel-running continues per the migration plan (Section 14).

12.6 Phase 5 (Days 90–180): Audits

1. Day 90–150: SOC 2 Type II audit period begins (Type II requires a minimum 6-month observation window).
2. Day 150: ISO 27001 stage-1 audit.
3. Day 180: ISO 27001 stage-2 audit; certificate issuance expected day 200.
4. Day 180: CCSS Level 3 audit.

12.7 Critical-Path Items

The two critical-path items are **HSM lead times** (Utimaco SR-Se200 at 6 weeks is the longest) and **SCIF fit-out** (4–6 weeks depending on existing infrastructure). Both must start on day 0; any slip cascades into the ceremony date. Cloud HSMs have no lead time and are not on the critical path.

Item	Lead time	Phase
Utimaco SR-Se200 procurement	6 weeks	Phase 1
Thales Luna 7 procurement	4 weeks	Phase 1
SCIF fit-out	4–6 weeks	Phase 1
Cloud HSM provisioning	1–3 days	Phase 1
YubiHSM 2 procurement	1 week	Phase 1
SOC 2 Type II audit period	6 months minimum	Phase 5

Table 18: Critical-path lead times.

13 Comparison to Existing Custodians

We compare the proposed architecture against the four custodians most likely to be the incumbent for an $8B fund: BitGo, Fireblocks, Anchorage Digital, and Coinbase Custody. The comparison is on *trust assumptions* (which entities must remain honest for the custody to remain sound), not on user-experience or feature checklists.

13.1 Trust-Assumption Framework

For any custody arrangement we ask: **which set of parties, acting together, can move the assets?** Smaller is worse (more fragile); more diverse is better (less correlated risk).

13.2 BitGo

BitGo Trust Company is a South Dakota-chartered trust company. Its multi-sig (three-key, two-of-three) places one key with BitGo, one key with the user, and one in cold backup. Trust assumptions [25]:

- BitGo must remain honest with respect to its key. (The user typically delegates the user-key to BitGo as well, in practice collapsing to a single-custodian model.)
- The on-chain multi-sig is publicly visible: P2WSH on Bitcoin, contract on Ethereum.
- Insurance ceiling: published $250M aggregate; well below an $8B portfolio's potential exposure.
- Single jurisdiction (US) for the trust company.

13.3 Fireblocks

Fireblocks is a technology platform, not a fiduciary. The fund operates its own custody using the Fireblocks MPC-CMP signing service. Trust assumptions [26]:

- The Fireblocks software (closed-source) must be free of extraction back-doors.
- The Fireblocks signing infrastructure (their portion of the MPC) must be honest.
- Threshold structure is configurable by the fund; the fund typically deploys three signers, one of which is the Fireblocks co-signer.
- Not a fiduciary: counterparty risk is the fund's, not Fireblocks'.
- Not insured by Fireblocks; the fund must arrange its own insurance.

13.4 Anchorage Digital

Anchorage is a US OCC-chartered national trust bank. Trust assumptions [27]:

- Anchorage as a fiduciary must remain honest and solvent.
- Anchorage's SGX-based key infrastructure must be free of microarchitectural attack.
- Single fiduciary point of failure (mitigated by OCC oversight, not by cryptographic redundancy).
- Single jurisdiction (US).
- Insurance: undisclosed amount, behind an $8B portfolio is likely under-covered.

13.5 Coinbase Custody

Coinbase Custody Trust Company LLC is NYDFS-regulated. Trust assumptions [28]:

- Coinbase as a fiduciary must remain honest and solvent.
- Coinbase's cold-storage architecture (dispersed cold storage, multi-vendor) must remain sound.
- Single fiduciary point of failure.
- Single jurisdiction (US).
- Insurance: $320M policy, below $8B exposure.

13.6 The In-House Architecture

Trust assumptions of this paper's architecture:

- No single fiduciary. The fund itself is the custodian.
- Three of five independent HSM-vendor lines must remain honest (cold tier).
- No single jurisdiction can compel asset transfer; cold-tier shares span at least three continents.
- No single cloud provider controls signing authority on its own; cloud shares are bounded by 2-of-9 across all tiers.
- Insurance is independently arranged at $500M+ tower from Lloyd's syndicates, layered.
- Custody policy is invisible to the chain.

13.7 Side-by-Side

13.8 When the Incumbent is Defensible

The proposed architecture is not the right answer for every fund. A small fund ($< $200M AUM) with a small operations team is plausibly better served by an incumbent custodian, because the overhead of running this architecture (six-engineer custody team, six-month SOC 2 window) does not amortise. The break-even is approximately $1B AUM for the operational economics; below that band an incumbent is the rational choice.

For an $8B fund the operational economics decisively favour self-custody on this architecture, and the trust-assumption diversification is a step function improvement.

Property	BitGo	Fireblocks	Anchorage	In-house
Trust root	Trust co.	Software vendor	Trust bank	Self
Threshold	2-of-3	3-of-3 (varies)	internal	3-of-5 (cold)
Chain footprint	Public multisig	MPC (single sig)	internal	MPC (single sig)
Vendor diversity	Single	Single	Single	4 distinct lines
Jurisdiction count	1 (US)	1 (US)	1 (US)	≥ 3
Insurance ceiling	\$250M	user-arranged	undisclosed	\$500M+
Fiduciary	Yes	No	Yes	Self
Effective fee on \$8B	∼\$8M/yr	∼\$3–5M/yr	∼\$32M/yr	\$5.36M/yr

Table 19: Side-by-side custody comparison. Fee figures are best estimates from rate-card disclosures where public.

14 Migration Plan

A fund with \$8B at an incumbent custodian cannot migrate in a single movement. The migration is structured as a 90-day staged transfer overlapping the implementation timeline, with explicit checkpoints and rollback paths.

14.1 Pre-Migration Checklist

Before any client funds move, the following must be in place:

1. Cold, warm, and hot DKG ceremonies complete; transcripts witnessed and published on M-Chain.
2. Sealed envelopes deposited at three vault jurisdictions; chain-of-custody documented.
3. M-Chain custody ledger online with daily reconciliation running.
4. Daily test-transactions of \$1k each on BTC and ETH executing end-to-end through the new architecture for at least seven calendar days, with two operator review of every test.
5. Insurance tower bound and certificate of insurance received.
6. SOC 2 Type II observation window started.
7. Notice provisions of the incumbent contract reviewed; required notice served (typical: 30–90 days).

14.2 Stage 1: Pilot (Day 75–80, 1% of AUM = \$80M)

1. Withdraw \$80M from incumbent (typically equal weight BTC and ETH).
2. Deposit to the new *warm* tier address.
3. Verify deposit on chain and on M-Chain ledger.
4. Execute one rebalance through warm tier; verify M-Chain ledger matches chain.
5. Execute one warm-to-cold transfer; verify cold tier deposit.
6. Execute one cold-to-warm transfer; verify ceremony, time-lock, and on-chain finality.

The pilot exercises every signing path on real funds at a size that is recoverable if anything goes wrong.

14.3 Stage 2: Bulk Migration (Day 80–85, 50% of AUM = \$4B)

1. Daily withdrawal of \$1B from incumbent to new cold-tier address, four daily tranches.
2. Each tranche verified on chain and on M-Chain.
3. Daily reconciliation runs as normal during migration.
4. Pause-and-investigate trigger: any reconciliation discrepancy, any signing-path delay outside SLA, any audit-log anomaly.

14.4 Stage 3: Final Migration (Day 85–90, remaining 49% = $3.92B)

1. Final tranche transfer; settle to within 2% residual at incumbent for tail wind-down.
2. Reduce the incumbent's authority by closing the active withdrawal whitelists at the incumbent and revoking API keys.
3. Maintain incumbent custodial relationship for residual 2% as a 30-day belt-and-braces; close fully on day 120.

14.5 Parallel-Run Risk Controls

For days 75–90 the fund is split between custodians. The risk controls during parallel running:

- **Daily reconciliation** runs on both sides; the sum must match the prior-day NAV plus any P&L.
- **Two-custodian board attestation**: both the incumbent's SOC report and the new architecture's interim attestation are delivered to the fund board weekly.
- **Withdrawal moratorium** on the incumbent for days 75–90 except the planned migration tranches.
- **Insurance gap coverage**: temporary cap on the fund's trading until the new architecture's insurance tower is fully bound.

14.6 Rollback Procedure

If at any point during the migration a critical defect is discovered (e.g. a signing-path failure that cannot be explained in 24 hours), the rollback is:

1. Halt all forward migration; freeze new deposits.
2. Reverse-transfer the most recently migrated tranche back to the incumbent.
3. Investigate root cause; remediate.
4. Resume forward migration only after a fresh witnessed attestation that the defect is fixed.

The rollback is exercised once on the pilot ($\geq$ $1k) before any bulk migration begins, to validate that the reverse path works.

14.7 Post-Migration

1. Day 120: incumbent custodial relationship fully closed; final asset reconciliation signed off.
2. Day 150: SOC 2 Type II observation window completes; auditor report ordered.
3. Day 180: ISO 27001 certification expected; CCSS Level 3 audit completes.
4. Year 1 anniversary: full audit cycle complete; cost actuals compared to plan; threat-model review.

14.8 Migration Cost

Item	Cost (USD)
Incumbent withdrawal fees (estimated 5 bps on $8B)	400,000
On-chain transaction fees (BTC + ETH bulk movements)	50,000
Parallel-run insurance gap coverage	100,000
Migration ops surge (2 additional engineers, 90 days)	150,000
Legal review of incumbent contract termination	75,000
Migration total	**775,000**

Table 20: One-time migration costs (incremental to capex and ceremony costs).

The migration cost amortises against the steady-state savings relative to incumbent fees within the first year for any incumbent custodian charging more than $5.4M per annum on $8B

AUM. For Anchorage Digital and Coinbase Custody at the published rate-card levels, payback is well under a year.

15 Conclusion

The architecture specified in this paper is a complete, auditable, and operationally tractable custody design for an institutional digital-asset fund at the eight-billion-dollar tier. Its load-bearing properties are:

1. **No single point of authority.** No custodian, cloud, jurisdiction, vendor, or operator can move the fund's assets alone. The minimum collusion required is three independent parties at the cold tier, two at the warm tier, and two with a 24-hour delay at the hot tier.
2. **No on-chain custody footprint.** Threshold MPC over secp256k1 produces a single canonical signature on every chain; the custody policy is invisible to the chain.
3. **Vendor and jurisdiction diversity.** Five HSM share-holders span four vendor lines (Thales, Utimaco, Marvell, Yubico) and at least three jurisdictions on the cold tier; warm tier spans three jurisdictions.
4. **Post-quantum hedge.** Lux Triple Consensus (LP-020 [4]) on the M-Chain custody ledger (LP-006 [6]) provides forward security against future quantum break of secp256k1.
5. **Compliance-ready.** The architecture maps directly to SOC 2 Type II, ISO 27001:2022, CCSS Level 3, FIPS 140-2 Level 3, MiCA, MAS PSN02, and US OCC trust-charter or NYDFS BitLicense fiduciary controls.
6. **Operationally cheap.** Steady-state cost is approximately 6.7 bps of AUM, comfortably below the 5–12 bps typical of incumbent custodians and competitive even against the low end of that band.

The migration from any of the four leading incumbents (BitGo, Fireblocks, Anchorage Digital, Coinbase Custody) is a 90-day operation; the architecture can be in steady-state operation by day 90 and fully audit-attested by day 180.

We emphasise that the design contains no novel cryptography. Every component – CGGMP21 threshold ECDSA, Feldman VSS distributed key generation, Shamir secret sharing, vendor-attested HSM-resident keys, BLS+ML-DSA hybrid audit log – is published, peer-reviewed, and deployed in production at multiple institutions. The contribution of this paper is the integration: the specification that places each component on the path that does the most work, and the operational policy that ensures the integration's properties hold under realistic adversaries and realistic ops teams.

The architecture is implemented end-to-end in the `luxfi/mpc` and `luxfi/hsm` reference codebases. Reference deployment manifests, ceremony run-books, SOC 2 control narratives, and CCSS evidence packages are available to implementors under the licence terms of those repositories.

References

[1] R. Canetti, R. Gennaro, S. Goldfeder, N. Makriyannis, and U. Peled. UC non-interactive, proactive, threshold ECDSA with identifiable aborts. *ACM CCS*, 2020.

[2] C. Komlo and I. Goldberg. FROST: Flexible round-optimized Schnorr threshold signatures. *Selected Areas in Cryptography (SAC)*, 2020.

[3] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[4] Lux Industries. LP-020: Triple-proof consensus (BLS + Pulsar + ML-DSA). *Lux Improvement Proposals*, 2025.

[5] Lux Industries. LP-137: GPU residency, attestation, and airgapped signing flow. *Lux Improvement Proposals*, 2026.

[6] Lux Industries. LP-006: M-Chain (MPC custody chain) specification. *Lux Improvement Proposals*, 2024.

[7] NIST. *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, 2001 (validation programme active through 2026).

[8] NIST. *FIPS PUB 140-3: Security Requirements for Cryptographic Modules*, 2019.

[9] NIST. *SP 800-57 Part 1 Rev. 5: Recommendation for Key Management*, 2020.

[10] CryptoCurrency Certification Consortium (C4). *CryptoCurrency Security Standard (CCSS), v8.0*, 2024.

[11] AICPA. *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (SOC 2)*, 2017.

[12] ISO/IEC. *ISO/IEC 27001:2022 – Information security management systems.*

[13] European Parliament. *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)*, 2023.

[14] Monetary Authority of Singapore. *Notice PSN02: Prevention of Money Laundering and Countering the Financing of Terrorism — Digital Payment Token Service*, 2020 (revised 2024).

[15] New York Department of Financial Services. *23 NYCRR Part 200: Virtual Currencies (BitLicense)*, 2015.

[16] Office of the Comptroller of the Currency. *Interpretive Letter 1170: Custody of Cryptocurrency Assets*, 2020.

[17] Thales Group. *Luna Network HSM 7 Product Brief and FIPS 140-2 Level 3 Certificate #3205*, 2024.

[18] Utimaco. *u.trust SecurityServer Se-Series Gen2 Datasheet — FIPS 140-2 Level 3 (Level 4 for physical)*, 2024.

[19] Amazon Web Services. *AWS CloudHSM (Marvell LiquidSecurity) Service Documentation and FIPS 140-2 Level 3 Certificate #4218*, 2024.

[20] Google Cloud. *Cloud HSM Documentation: FIPS 140-2 Level 3 attested via Marvell LiquidSecurity*, 2024.

[21] Microsoft Azure. *Azure Dedicated HSM (Thales Luna 7) Product Documentation*, 2024.

[22] Yubico. *YubiHSM 2 Product Specification — FIPS 140-2 Level 3 Certificate #3915*, 2023.

[23] Chainalysis Inc. *KYT (Know Your Transaction) API Reference*, 2024.

[24] TRM Labs. *Transaction Monitoring API Reference*, 2024.

[25] BitGo Trust Company. *SOC 2 Type II Report (excerpts) and $250M Insurance Disclosure*, 2024.

[26] Fireblocks. *Architecture White Paper: MPC-CMP and Policy Engine*, 2023.

[27] Anchorage Digital Bank. *OCC National Trust Charter and Custody Operations Disclosure*, 2021.

[28] Coinbase Custody Trust Co. LLC. *NYDFS Trust Charter Filing and Cold Storage Architecture Disclosure*, 2018–2024.

Reproducibility

Source code. `github.com/luxfi/threshold` (MPC custody backbone, commit `TBD`); HSM adapters at `github.com/luxfi/hsm`; key-management policy at `github.com/luxfi/kms`.
Build. `go build ./...`; HSM integration tests require vendor SDKs (Thales Luna, Utimaco, YubiHSM, AWS CloudHSM, GCP Cloud HSM).
Hardware tested. TBD (Tier-1 HSM lab: Thales Luna 7, Utimaco SR-Se200, YubiHSM 2; cloud Tier-1: AWS CloudHSM, GCP Cloud HSM).
Standards referenced. FIPS 140-2 Level 3, FIPS 140-3, SOC 2 Type II, ISO 27001:2022, CCSS Level 3, MiCA, MAS PSN02, US OCC trust charter, NYDFS BitLicense.
Contact. security@lux.network.