LayerCover

Protocol Whitepaper

layercover.com

Abstract

LayerCover is a fully on-chain, parametric cover protocol inspired by the Lloyd's of London marketplace. It enables capital providers (underwriters) to deploy single-sided liquidity across multiple independent risk pools, earning premiums while maintaining full control over capital allocation and risk exposure. Cover is underwritten and settled entirely by smart contracts. Payouts can be triggered at any time by policyholders through a direct swap of distressed assets for underwriter capital, removing the need for governance votes or subjective claims assessments (see Sec. 4.5). By combining modular risk assessment, flexible capital reuse, and salvage rights on payout (see Sec. 4.6), LayerCover delivers a capital-efficient alternative to mutualised risk pool designs, offering predictable and fully auditable protection for decentralised finance. This whitepaper defines the protocol's architecture, mechanics, and implementation.

September 3, 2025

Contents

1 Introduction

The global insurance industry has, for centuries, operated as a central marketplace where risk is underwritten, capital is pooled, and claims are settled according to mutually agreed terms. Lloyd's of London, founded in 1688, remains the archetype of such a marketplace where a network of syndicates and underwriters, each providing capital to cover specific risks, coordinated through a central governance framework. In decentralised finance (DeFi), the need for an equivalent mechanism is both clear and urgent. Protocol hacks, smart contract failures, oracle malfunctions, governance exploits, and other tail events have caused billions of dollars in losses in recent years. Unlike traditional finance, DeFi has no central clearinghouse or government-backed safety net. When failures occur, users are typically left with few options: absorb the loss, hope for a socialised bailout, or pursue unenforceable legal remedies.

1.1 Why Now

Decentralised finance (DeFi) has matured from experimental protocols to an ecosystem securing hundreds of billions of dollars in total value locked (TVL). Institutional investors, professional market makers, and on-chain treasuries are now active participants, bringing with them higher expectations for risk management and capital protection. Yet despite this growth, the overwhelming majority of DeFi capital remains uninsured.

A purpose-built, on-chain insurance primitive is required: parametric triggers, deterministic settlement, and composable capital. *LayerCover* addresses this gap with a marketplace for specialised underwriting and predictable, rule based payouts.

1.2 Limitations of Current Models

Today, the on-chain cover market is dominated by **mutualised risk pool** models. In these systems, large, undifferentiated capital pools are used to cover many protocols simultaneously. While aggregation offers certain efficiencies, these models suffer from several structural drawbacks:

- **Slow, subjective claims:** Claims decisions often rely on governance votes, introducing delays, uncertainty, and the risk of politicised outcomes eroding trust in the system.
- **Capital denomination risk:** In mutualised risk pools, underwriters must contribute to a shared pool whose assets are often volatile or denominated in the protocol's governance token. The inability to provide single-sided liquidity in a preferred stable or blue-chip asset exposes underwriters to unwanted market risk, reducing institutional appeal.
- **Fixed-term, prepaid cover:** Current mutual cover providers require buyers to commit to multi-month cover and pay the full premium upfront, even if the risk exposure changes. This lack of flexibility discourages usage for dynamic or short-term DeFi positions and limits recurring adoption.

These structural limitations have prevented mutual-based cover models from achieving meaningful market penetration. Despite hundreds of billions of dollars locked in stablecoins and DeFi protocols, active on-chain cover accounts for only a fraction of one percent of the total addressable market.

2 Key Benefits of LayerCover

A better system is possible. LayerCover improves upon the aforementioned issues, by offering the following advantages:

2.1 Underwriter Advantages

Single-Sided Liquidity: Underwriters can pledge capital in one asset of their choice (e.g. USDC, ETH). Each pledge to a pool is made in a single asset, but an underwriter may open multiple positions across different pools for different assets. This enables diversification while preserving the benefits of single-sided liquidity.The result is a more predictable, controlled risk-return profile, suitable for both institutional and sophisticated retail participants.

Dual-Revenue Efficiency: LayerCover enables the same principal capital to be pledged across multiple independent pools, each assigned a risk rating and governed by a total risk-points budget. This structure allows leveraged premium generation while maintaining strict solvency limits, with mutex groups further limiting exposure to correlated risks. In addition to premiums, underwriters also earn yield from idle capital deployed through yield adapters, these are contract modules that place unallocated funds into low-risk external strategies (see Glossary), while allowing instant recall for claims. By combining premium income with yield from integrated capital strategies, LayerCover delivers one of DeFi's most competitive venues for yield generation.

Salvage Rights on Payout: Underwriters receive distressed assets from claims, recovering potential residual value (see Sec. 4.6 for full mechanics).

2.2 Policyholder Advantages

Perpetual, Pay-As-You-Go Cover: Unlike fixed-term policies that require upfront payment, LayerCover offers a perpetual model in which cover remains active as long as the premium deposit sustains the pro-rated, per-second cost. Premiums dynamically adjust based on pool utilisation. Policies lapse automatically when deposits run dry, but holders can top up at any time, cancel for a refund of unused deposit, or request coverage increases, providing flexibility and cost efficiency.

Instant, Rules-Based Settlement: Claims paid automatically with no governance delay. A small claim fee is payable to deter frivolous claims. Full mechanics of the claim process are described in Sec. 3.2 and Sec. 4.6.

Protocol-native reinsurance protection: Backstop reserves ensure full claim settlement, during extreme liquidity events. This is a rare event, since solvency floors normally ensure primary pools remain capitalised. (see Sec. 3.3 for details).

2.3 Partner Advantages

Referral Program: Frontend operators such as DeFi protocols, aggregators, and wallets can join LayerCover's referral program by receiving unique referral codes to share with their users and communities.

When cover is purchased through these codes, the referring partner earns a percentage of the premiums while the user benefits from a policy discount. Rewards are distributed automatically and transparently on-chain, creating a recurring, low-overhead revenue stream for partners.

Mutually Reinforcing Value: The referral system aligns incentives across all participants. End-users gain access to flexible on-chain protection, referrers earn a share of the premiums, and LayerCover scales its reach through trusted community and platform partners. This creates a positive feedback loop: protection for users, revenue for referrers, and ecosystem growth for the protocol.

3 User Operations

3.1 Underwriter Operations

Underwriters participate in the system by depositing capital into the CapitalPool, an ERC-4626 vault that issues shares at the current price-per-share (PPS). These deposits form the underwriter's principal, which can then be allocated across multiple risk pools through the UnderwriterManager contract (UM). Allocation does not physically move assets; rather, it records that a portion of the underwriter's principal is pledged to back coverage in the chosen pools. Each pool consumes part of the underwriter's finite risk-points budget, and allocation rules such as mutex groups or maximum pool counts apply. Once allocated, underwriters begin earning rewards from premiums, but they also become responsible for bearing losses. Rewards accrue continuously and can be claimed at any time, while losses are applied in shares so that they remain neutral to changes in PPS.

If an underwriter wishes to reduce their exposure to a pool, they may submit a deallocation request for a chosen amount. This request enters a governance-defined notice period, during which the specified capital is locked and cannot be reallocated elsewhere. The notice period protects solvency by preventing underwriters from instantly withdrawing in response to an imminent claim. Once the notice expires, the underwriter may execute the deallocation, at which point the pledge to that pool is cut and the capital becomes unpledged within the vault. Unpledged capital remains in the system until it is withdrawn, but no longer backs coverage in that pool.

Separately, an underwriter may request to withdraw funds from the CapitalPool. Withdrawals also follow a notice period, after which the request can be executed to burn shares and return the underlying asset. Importantly, withdrawals automatically scale down the underwriter's pledges across all pools in proportion to their reduced principal, meaning it is not necessary to first deallocate a matching amount from individual pools. To safeguard solvency, the UM enforces a coverage floor that requires each pool to retain capital in excess of its sold coverage and pending losses. As a result, if a withdrawal request would breach this floor, the system executes it only up to the allowed amount, leaving the remainder pending until conditions permit.

3.2 Policyholder operations

Policyholders obtain coverage by purchasing a **policy NFT** from their chosen pool. Each policy represents a fixed coverage amount backed by a deposit that continuously pays premiums at the pool's current rate. As long as the deposit can fund accrued costs, the policy remains active. Policies are transferable: whoever owns the NFT controls its coverage, deposit, and the right to make claims.

When a buyer purchases coverage, they select a pool, specify a coverage amount, and provide an initial premium deposit. The policy NFT is minted immediately, but coverage only becomes active after a governance-defined cooldown period. This prevents opportunistic behaviour, e.g. buying cover after an exploit has already begun. Both coverage and deposit must be non-zero at inception. Once active, the deposit is drawn down second by second. The policyholder may top up the deposit at any time; before accepting additional funds, the system first settles any premium owed to the current block and then updates the balance.

Coverage may also be adjusted over the life of a policy. If the owner wishes to increase their cover, they can submit a request that is placed into a pending queue. Each increase becomes effective only after its own cooldown, and is finalized automatically on the next interaction, such as a top-up, another increase request, or a claim. Multiple pending increases are allowed, subject to a bounded queue size to keep costs predictable. Conversely, reductions in coverage take effect immediately once premiums are settled. A partial reduction simply lowers the insured amount while leaving the deposit in place, whereas a full reduction closes the policy entirely and refunds the remaining deposit to the owner.

A policy can also be cancelled voluntarily. After activation, the holder may close their policy at any time; the protocol settles outstanding premium to the current block and refunds the unused deposit. Policies can also terminate automatically by lapse if the deposit is exhausted. Lapsed policies may be reactivated by topping up, but reactivation is subject to the cooldown period to prevent opportunistic behaviour during incidents.

If a covered event occurs, the policyholder may claim up to the current coverage amount. The claimant transfers any distressed asset (if required) to the protocol, and in return receives an immediate payout from the pool's pledged capital, net of the pool fee. Claimants receive their payout in the pool's underlying asset (see Sec. 4.6 for salvage rights distribution).

Example:

- User purchases $100k cover with $5k deposit → NFT minted.
- Ten days later, user tops up $2k → deposit extended.
- User requests +$50k cover → enters queue, finalises after cooldown.
- User reduces $30k cover → effective immediately.
- User cancels → unused deposit refunded.

Restrictions:

- If a pool is paused due to an incident (see Section 4.5), new purchases and increases are disabled, but reductions, cancellations, and claims remain available.
- Each new policy and increase is subject to cooldown; reductions and cancellations require the policy to already be active.

3.3 Backstop Depositors

The **BackstopPool** is an ERC–4626 vault that holds USDC and optionally deploys idle funds through a yield adapter (a module that deploys idle funds into external yield strategies, while allowing recall for claims). It functions as a protocol–native reinsurance layer, ensuring that policyholders are always paid in full and on time, even under stress. In practice, it closes the timing and liquidity gaps that individual underwriting pools cannot fully hedge without sacrificing efficiency.

The use of the Backstop Pool is expected to be rare. Solvency floors and utilisation controls normally ensure that primary pools remain sufficiently capitalised, so the backstop activates only in exceptional circumstances such as multiple simultaneous large claims or when capital is temporarily locked in external yield strategies. Its role is to raise system reliability and capital efficiency. First, it guarantees solvency: if a pool's pledged capital and withdrawals from yield adapters are insufficient at the moment of a claim, the backstop instantly covers the shortfall so that policyholders are paid in full without delay or governance intervention. A yield adapter is a module that deploys idle pool capital into external low-risk yield strategies (see Glossary), while allowing recall for claims. Second, the backstop serves as a liquidity buffer: because yield adapters may take time to unwind, it provides immediate settlement capacity. Finally, it stabilises incentives across the system: underwriters can operate with prudent leverage and notice periods without introducing settlement risk, while backstop depositors are compensated with a share of premiums for absorbing residual systemic risk.

Withdrawals follow a 30–day notice period. This period is enforced to prevent depositors gaming the system by withdrawing cover before expected claims are made. Depositors request withdrawal by specifying a share amount, which starts the notice clock. After the notice elapses, they redeem the exact shares requested and receive the corresponding amount of USDC at the prevailing PPS. Redemption first uses idle USDC and, if needed, pulls additional liquidity from the yield adapter.

During claims, asset may be drawn from the backstop to cover payouts. These draws reduce Net Asset Value (NAV) and thus price-per-share (PPS) in real-time, making backstop pool depositors the underwriters of system–wide residual risk. In exchange, they benefit from premium inflows and yield.

4 System Functionality

4.1 Vaults and Their Purpose

Vaults are lightweight escrow contracts that hold policyholder deposits on behalf of both the insured user and the underwriters backing their risk. Each vault is created deterministically for a specific policy and is responsible for maintaining balances, enforcing rights, and ensuring that obligations can always be settled in underlying units. By design, vaults guarantee that ownership and risk assignments can be updated without requiring tokens to move between external accounts.

The need for vaults arises because many DeFi protocols restrict or pause transfers of user positions during incidents or exploits. If assets were held directly in a user wallet, such restrictions could prevent the transfer of salvage rights from policyholders to underwriters, breaking LayerCover's parametric payout model. By routing deposits into vaults instead, the protocol avoids this problem. Ownership of the vault itself remains constant, but rights over its assets can be reassigned internally between policyholder and underwriters. No token transfer is required, so even if the underlying protocol halts withdrawals or freezes positions, the LayerCover contracts can still enforce salvage rights and pay out claims instantly.

In practice, a vault's balance may be split into two categories: *unassigned* funds, which remain under policyholder control, and *assigned* funds, which represent coverage pledged to underwriters. Policyholders may sweep unassigned funds, while underwriters may sweep assigned funds, ensuring both sides interact with the same escrow safely. If the vault cannot redeem all of the requested amount from a yield adapter or integration, it reports a shortfall, which the RiskManager contract settles through the insured withdrawal process. This maintains deterministic settlement for policyholders while keeping underwriter exposures accurate.

4.2 Premium Pricing

Premiums in LayerCover are determined algorithmically using a utilisation–based pricing curve defined per pool. Each pool has an associated *rate model* set in the **PoolRegistry**, which encodes its base rate, slope parameters, and kink point. Together, these parameters define how the premium rate increases as utilisation rises, ensuring that pricing reflects real-time supply and demand for coverage.

Utilisation is measured as the ratio of total coverage sold to available capital in a pool. When utilisation is low, premium rates are close to the base rate, encouraging demand from policyholders. As utilisation increases toward the kink point, rates rise linearly along the first slope, reflecting the growing scarcity of available capital. Once utilisation surpasses the kink, rates increase more sharply according to the second slope, discouraging excessive concentration and incentivising new underwriter deposits. This dynamic adjustment aligns incentives on both sides: policyholders pay fair rates when capacity is abundant, while underwriters are compensated appropriately when risk exposure is high.

Governance configures each pool's rate model and risk rating, and may also set claim fees and pause states. These parameters allow calibration of expected returns for underwriters and expected costs for policyholders, while leaving day–to–day pricing entirely rule–based and on–chain. The result is a premium mechanism that is flexible, auditable, and resistant to manipulation, providing stable incentives for capital while ensuring coverage remains available at predictable, market–driven prices.

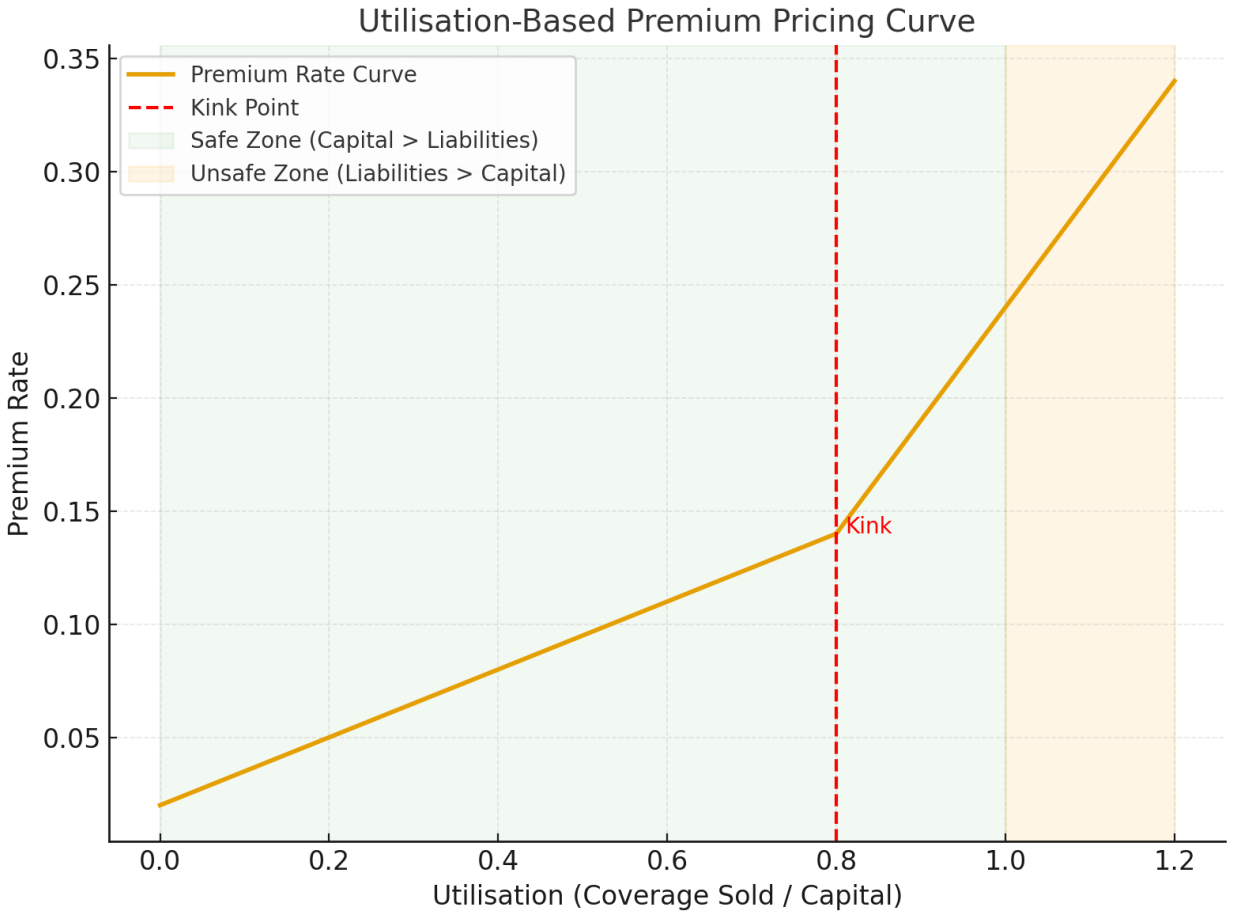

Figure 1: Utilisation–based premium curve

4.3 Loss Distribution

Summary. When a claim is paid, the resulting loss is prorated across all underwriters who had pledged capital to that pool at the time of the event. Each underwriter's share of the loss is proportional to their active pledge at that time. This ensures no one can avoid losses by withdrawing immediately after the event, and the system stays price–neutral and efficient even when many underwriters participate.

Objective. Allocate realised claim losses to underwriters in a way that is (i) pro–rata to the capital that actually backed the risk at the moment of the event, (ii) *price–neutral* with respect to pool PPS changes, and (iii) $O(1)$ to update regardless of underwriter count.

Snapshot and indexing. On a payout of total amount X units of the pool's underlying, the pool first takes a *price–neutral* snapshot by reserving shares corresponding to X using the current $valueToShares(\cdot)$ conversion (Def. 6.1):

$$\texttt{unsettledPayoutShares} \leftarrow \texttt{unsettledPayoutShares} + \texttt{valueToShares}(X).$$

This does not change NAV at the instant of snapshot; NAV moves only as assets are actually transferred (Sec. 6.1).

Losses are then accounted for with a *shares–per–pledge* index $D_i^{(sh)}$ maintained per pool i (Defs. 6.3–6.4). Let L be the realised loss value (in underlying units) attributable to the pool after any backstop injection (if applicable). Define

$$\texttt{lossShares} = \texttt{valueToShares}(L), \quad D_i^{(sh)} \leftarrow D_i^{(sh)} + \frac{\texttt{lossShares} \cdot \texttt{PRECISION}}{\texttt{totalPledged}_i^{\star}},$$

where $\texttt{totalPledged}_i^{\star}$ is the *eligible pledge base* at the event block: pledged capital after applying notices/locks and any solvency floor adjustments (§3.1). This freezes the loss base against subsequent reallocations.

Settlement at underwriter level. Each underwriter u in pool i tracks a per–pool snapshot $d_{u,i}^{(sh)}$. Their pending loss (in *shares*, not value) updates lazily on interaction:

$$\texttt{pendingLossShares}_{u,i} = \max\left(0,\ \left\lfloor \frac{P_{u,i}^{\text{active}} \cdot \Delta D_i^{(sh)}}{\texttt{PRECISION}} \right\rfloor - d_{u,i}^{(sh)}\right),$$

where $P_{u,i}^{\text{active}}$ is the underwriter's *eligible* pledge at the event block. Settlement burns these shares at current PPS, ensuring price–neutrality across time:

$$\text{burn}(\texttt{pendingLossShares}_{u,i}), \qquad d_{u,i}^{(sh)} \leftarrow d_{u,i}^{(sh)} + \text{increment}.$$

Edge cases and invariants.

- **Concurrent claims:** multiple events simply add to $D_i^{(sh)}$; order does not matter.
- **Zero eligible base:** if $\texttt{totalPledged}_i^{\star} = 0$, no index update occurs; the claim is fully met by the BackstopPool (Sec. 3.3), and backstop NAV absorbs the loss.
- **Withdrawal/deallocation after event:** attempts to avoid losses via post event actions are inert; the loss base is fixed at the event block by $\texttt{totalPledged}_i^{\star}$.

- **Contagion (optional):** if governance defines dependency edges between pools, a loss in pool A may emit synthetic losses into pools $\{B\}$ via pre–declared weights; each affected pool applies its own $D^{(sh)}$ tick with its local eligible base.
- **Rounding:** all divisions use flooring with `PRECISION` scale; any dust remains inside the pool and is socialised over time, consistent with fixed point rules (Ref. [19]).

This design yields constant time pool updates and strictly pro–rata underwriter attribution, while remaining robust to PPS drift between event and settlement.

4.4 Reward Distribution

Summary. Premiums and incentives are streamed continuously to underwriters in proportion to pledged capital. This ensures fairness and prevents underwriters from avoiding losses by withdrawing post-event. Settlement is atomic and safe from transaction interruption, eliminating this as an attack surface..

Sources. Underwriter rewards comprise (i) streaming premiums from active policies, (ii) pool incentive tokens (if configured), and (iii) strategy yield rebated to the pool. All rewards are accounted *per token* τ via an $R_{i,\tau}$ index (Sec. 6.2).

Streaming and indexing. Premiums accrue continuously per second from each active policy and are periodically consolidated into the pool's reward stream. On each credit of amount Q of token τ to pool i:

$$R_{i,\tau} \leftarrow R_{i,\tau} + \frac{Q \cdot \texttt{PRECISION}}{\texttt{totalPledged}_i^{\dagger}},$$

where $\texttt{totalPledged}_i^{\dagger}$ is the *current* eligible pledge base at the time of distribution. For an underwriter u:

$$\texttt{pendingReward}_{u,i,\tau} = \max\left(0,\ \left\lfloor \frac{P_{u,i}^{\text{active}} \cdot \Delta R_{i,\tau}}{\texttt{PRECISION}} \right\rfloor - d_{u,i,\tau}\right),$$

with $d_{u,i,\tau}$ the underwriter's last reward snapshot. Rewards settle (transfer to u) on any user or pool interaction; settlement also advances $d_{u,i,\tau}$.

Multi–token and fees. The mechanism supports multiple τ concurrently (e.g., USDC premiums, incentive ERC–20s). Claim fees (if set) are split according to governance parameters among (i) active underwriters, (ii) the BackstopPool, and/or (iii) a treasury, each via its own index.

Fairness and robustness.

- **Price neutrality:** rewards are paid in tokens, not shares; no implicit mint/burn of pool equity occurs.
- **Eligibility symmetry:** the same notion of $P_{u,i}^{\text{active}}$ used for losses is used for rewards, so capital that backs risk also earns the stream that compensates it.
- **DoS resistance:** index updates are $O(1)$, independent of the number of underwriters or active policies.
- **Rounding:** flooring at distribution ensures the pool never over pays; unallocated dust accumulates to the pool and is socialised.

4.5 Oracle–free design and unit–based accounting

A defining feature of the protocol is its independence from external price oracles. Core functions including policy management, premium accrual, and claim settlement are executed deterministically on–chain, without reliance on off–chain feeds. The sole oracle function is circuit breaking: for example, the protocol may pause new policy issuance if an oracle reports that an asset has de–pegged beyond a set threshold. This safeguard prevents policyholders from purchasing cover only after a loss event has already occurred.

This design removes a major DeFi attack vector: stale/manipulated prices and governance exploits. By avoiding oracle dependencies, LayerCover ensures predictable execution and minimizes systemic risk.

Unit–based accounting reinforces this robustness: all liabilities and payouts are denominated in the underlying asset itself. Underwriters and policyholders share a common unit of account, eliminating valuation disputes and ensuring transparency of obligations.

In contrast, many on–chain insurance models rely on continuous oracle inputs or governance votes to adjudicate claims mechanisms that introduce delay, discretion, and manipulation risk. LayerCover's oracle–free, unit–based approach guarantees that claims resolve instantly and mechanically.

4.6 Salvage Rights

Summary. When payouts occur, underwriters do not simply lose capital; they also acquire rights to the distressed assets surrendered by policyholders. These salvage rights are allocated pro rata to losses borne, offering potential recovery if the assets retain or regain value. This structure reduces net losses and aligns incentives between underwriters and policyholders.

Principle. During a claim, the policyholder transfers the distressed asset (or an enforceable right to it) to the protocol, and receives underlying units from the pool. Salvage entitlements are then distributed to underwriters *in proportion to their share of the loss*.

The underwriting token must correspond to the same asset class or denomination as the coverage, ensuring that payouts and salvage accounting remain purely mechanical. For example, an underwriter may backstop BTC denominated derivatives (aBTC, compBTC, etc.) using BTC, or underwrite USDC coverage with USDT (or equivalent stablecoins where the protocol treats them as fungible). What is not permitted is underwriting across unrelated assets. For instance, using BTC to underwrite USDC coverage. This one–to–one (or denomination consistent) basis eliminates reliance on external oracles for the protocol's core day-to-day operations.

Atomic assignment. Within a claim transaction:

1. The pool snapshots the payout (price–neutral) and transfers X units of the underlying asset to the policyholder.
2. The policy vault (Sec. 4.2) reassigns ownership of the covered distressed asset slice to the pool/underwriters, even if external transfers are paused upstream.
3. A *salvage index* $S_{i,a}$ (per pool i and asset a) is updated:

$$S_{i,a} \leftarrow S_{i,a} + \frac{q_a \cdot \texttt{PRECISION}}{\texttt{lossBase}_i},$$

where q_a is the quantity of asset a received (or credited via the vault), and $\texttt{lossBase}_i$ is the eligible pledge base used for that loss tick. Crucially, no oracle inputs are required: the index records quantities, not valuations.

Underwriter entitlements. Each underwriter u maintains a per–asset salvage snapshot $s_{u,i,a}$. Their pending salvage balance (in units of a) accrues deterministically:

$$\texttt{pendingSalvage}_{u,i,a} = \max\left(0,\ \left\lfloor \frac{P_{u,i}^{\text{active}} \cdot \Delta S_{i,a}}{\texttt{PRECISION}} \right\rfloor - s_{u,i,a}\right).$$

When claimed, underwriters receive the underlying asset a (if liquid) or a claim token/receipt referencing vault rights if upstream withdrawals are paused. Salvage entitlements are independent of pool PPS and excluded from pool NAV unless governance explicitly reintegrates recovered assets.

5 Governance and Risk Management

The **LayerCover** protocol is designed to minimise discretionary governance intervention. Governance primarily sets static parameters such as pool risk ratings, mutex group definitions, and pricing curves. Execution of underwriting, loss distribution, and payouts is fully automated on–chain.

5.1 Risk Points System

The *risk points system* provides a quantitative budget that constrains how much leverage an underwriter can take across multiple pools.

Definition. Each pool i is assigned a risk cost c_i in *risk points*, proportional to its perceived underwriting risk. An underwriter u has a maximum budget TOTAL_RISK_POINTS, enforced at allocation time:

$$\sum_{i \in A_u} c_i \ \leq\ \text{TOTAL\_RISK\_POINTS}. \tag{1}$$

Purpose.

- Prevent concentration of exposure across many high–risk pools.
- Enable differentiated leverage: lower–rated pools consume fewer points.
- Allow governance to tune systemic risk without micromanaging capital flows.

5.2 Pool Ratings and Constraints

Each pool has a *risk rating* and associated *constraints* recorded in the `PoolRegistry`:

- **Risk Rating:** Discrete labels (AAA, AA, A, BBB, BB, B, C) reflect the perceived risk of the protocol or asset.
- **Mutex Groups:** Exclusion sets prevent underwriters from allocating to correlated pools (e.g., DAI and USDC).
- **Capacity Limits:** Optional per–pool caps in absolute terms or as a % of total NAV, preventing over–concentration.
- **Fee Parameters:** Governance–set minimum/maximum premium rates and payout fee bps.

Ratings and constraints are updated via governance proposals, subject to timelocks to avoid disruption. Changes to mutex groups or capacity limits affect only new allocations.

5.3 Risk Framework Alignment with Traditional Capital Models

Although **LayerCover** is DeFi–native, its risk ratings, leverage constraints, and pool–level controls can be mapped to established solvency frameworks used by insurers and banks. This alignment helps institutional participants translate on–chain exposures into familiar capital adequacy metrics.

5.3.1 Mapping to Solvency II (Insurance)

The EU Solvency II regime requires holding capital to survive a $1/200$ year event (the Solvency Capital Requirement, SCR). LayerCover parallels this structure as follows:

- **Pool Ratings ⇒ SCR calibration.** Ratings (driven by protocol risk, liquidity, volatility, resilience) correspond to Solvency II standard formula or internal models for capital requirements.
- **Risk Points ⇒ concentration controls.** A portfolio–wide cap on risk points mirrors SCR concentration add–ons and dependency modelling.
- **Mutex Groups ⇒ dependency structure.** Exclusion sets replicate correlation constraints in SCR aggregation.
- **Parametric Payouts ⇒ predictable loss quantification.** Deterministic triggers reduce model risk and shorten settlement, improving capital modelling.

5.3.2 Mapping to Basel III/IV (Banking)

Basel standards focus on risk–weighted assets (RWA), leverage, and liquidity coverage. Analogues include:

- **Pool Ratings ⇒ risk weights.** Each pool's rating maps to a risk weight for pledged exposure, yielding an RWA–like measure.
- **Leverage via Pledges ⇒ leverage ratio.** Total pledged exposure relative to principal acts as a non–risk–based leverage cap.
- **Stress Testing ⇒ correlated scenarios.** Historical exploit data, TVL drawdowns, and oracle disruptions can emulate Basel stress tests.
- **Liquidity Coverage.** Pool buffers and backstops emulate a Liquidity Coverage Ratio (LCR)–style requirement.

5.3.3 Institutional Integration Benefits

- **ERM Reporting:** Immutable on–chain records support export into enterprise risk management and compliance systems.
- **Auditability:** Public, append–only state creates a native audit trail for supervisors and internal audit.

5.3.4 At–a–Glance Mapping

LayerCover Feature	Solvency II Analogue	Basel III/IV Analogue
Pool risk rating	SCR calibration (standard formula / internal model)	Risk weight assignment (RWA)
Risk points budget	Concentration limits in SCR aggregation	Portfolio–level leverage constraints
Mutex groups	Dependency / correlation structure	Correlation caps across asset classes
Parametric claim triggers	Predictable loss quantification	Deterministic loss recognition
Liquidity/backstop config	Liquidity planning for claims	LCR/NSFR–style liquidity buffers
Pledge leverage vs. principal	Capital add–ons for risk	Non–risk–based leverage ratio
On–chain audit trail	Auditability for supervisors	Data lineage for internal control

This modal enables institutional capital to flow on–chain without breaking off–chain governance, risk, and compliance (GRC) guardrails.

6 Core Economics & Accounting

LayerCover's economics boil down to a few composable rules:

- Shares price the pool by dividing total asset value (NAV) over an effective supply that excludes payout-reserved shares, so deposits and withdrawals are always fair.
- Payouts are price-neutral at the moment they're declared—NAV doesn't jump, we just reserve shares—so no one is diluted or advantaged mid-event.
- Rewards accrue continuously via simple indices, with each underwriter's stake adjusted for any notices or locks.
- Losses are realised by burning shares, with a shares-per-pledge index ensuring fairness regardless of PPS changes.
- Premiums are set by a transparent utilisation curve, making pricing predictable under load.

The formulas below are the minimal math to understand value, yield, and risk transfer; operational details (notices, deallocations, coverage floors) live in the appendix and don't change these core incentives.

6.1 Shares, NAV, and Price Neutrality

Effective circulating supply.

$$\text{EffShares} \equiv \text{TotalShares} - \text{unsettledPayoutShares}.$$

Conversions.

$$\text{valueToShares}(V) = \begin{cases} V, & \text{if NAV} = 0 \text{ or EffShares} = 0 \\ \left\lfloor \dfrac{V \cdot \text{EffShares}}{\text{NAV}} \right\rfloor, & \text{otherwise} \end{cases} \tag{6.1}$$

$$\text{sharesToValue}(S) = \begin{cases} S, & \text{if EffShares} = 0 \\ \left\lfloor \dfrac{S \cdot \text{NAV}}{\text{EffShares}} \right\rfloor, & \text{otherwise.} \end{cases} \tag{6.2}$$

Payout snapshot (price-neutral). On a payout of total amount X the pool increases

$$\text{unsettledPayoutShares} \leftarrow \text{unsettledPayoutShares} + \text{valueToShares}(X),$$

so snapshotting does not change NAV at that instant; NAV moves as assets are actually transferred.

6.2 Rewards & Losses (High Level)

Reward indexing. When amount Q of reward token τ is distributed over pool i,

$$R_{i,\tau} \leftarrow R_{i,\tau} + \frac{Q \cdot \text{PRECISION}}{\text{totalPledged}_i}.$$

An underwriter's claimable reward is

$$\text{Pending}_{u,i,\tau} = \max\left(0,\ \left\lfloor \frac{P_{u,i}^{\text{active}} \cdot R_{i,\tau}}{\text{PRECISION}} \right\rfloor - d_{u,i,\tau}\right),$$

where $P_{u,i}^{\text{active}}$ is the user's *effective* pledge after notices/locks

Loss indexing (shares-based). On a realised loss L in pool i:

$$\text{lossShares} = \text{valueToShares}(L), \tag{6.3}$$

$$\mathcal{D}_i^{(\text{sh})} \leftarrow \mathcal{D}_i^{(\text{sh})} + \frac{\text{lossShares} \cdot \text{PRECISION}}{\text{totalPledged}_i}. \tag{6.4}$$

Users' pending loss shares are computed from their pledge and the change in $\mathcal{D}_i^{(\text{sh})}$ since their last snapshot; these shares are burned at settlement, reducing value at the then-current PPS.

6.3 Premium Pricing and Cost

Available capital and utilisation. Let

$$\text{availableCapital} = \max\big(0,\ \text{totalPledged} - \text{pendingWithdrawals}\big).$$

Utilisation in basis points is:

$$\text{utilBps} = \begin{cases} \dfrac{\text{sold} \cdot \text{BPS}}{\text{availableCapital}}, & \text{availableCapital} > 0 \\ \text{BPS}, & \text{otherwise.} \end{cases}$$

Capacity checks for new or increased coverage also account for any pending policy increases.

Rate curve (piecewise linear).

$$\text{Rate}_{\text{bps}} = \begin{cases} \text{base} + \dfrac{\min(\text{utilBps}, \text{kink}) \cdot \text{slope1}}{\text{BPS}}, & \text{utilBps} \le \text{kink} \\ \text{base} + \text{slope1} + \dfrac{(\text{utilBps} - \text{kink}) \cdot \text{slope2}}{\text{BPS}}, & \text{otherwise.} \end{cases}$$

Policy cost.

$$\text{PremiumCost} = \left\lfloor \frac{\text{Coverage} \cdot \text{Rate}_{\text{bps}} \cdot \text{ElapsedSeconds}}{\text{SECS\_YEAR} \cdot \text{BPS}} \right\rfloor.$$

6.4 Backstop (One-Paragraph Economics)

Premiums sent to the BackstopPool increase NAV without minting shares. Operational details of the Backstop mechanism are described in Sec. 3.3.

$$\text{NAV}' = \text{NAV} + \text{Premium}, \qquad \text{TotalShares}' = \text{TotalShares}.$$

6.5 Worked Examples

To illustrate how capital flows through the system, consider the following scenario with real numbers.

Scenario Setup

- Total value locked (TVL) in a DeFi protocol: **$10m**.
- Policyholders purchase cover totaling **$2m** from a LayerCover pool.
- The pool has **100 underwriters**, each pledging **$100k** in USDC, so pledged capital = **$10m**.
- Premium rate = **10% annualized**, utilisation-based.
- Coverage sold = **$2m**, so pool utilisation = **20%**.

Premium Flow

- Annual premium for $2m coverage at 10% = **$200k/year**, or $\approx \$16.7k$/month.
- This premium accrues per-second and is distributed pro-rata to underwriters.
- Each underwriter with a 1% share of the pool ($100k / $10m) earns:
  - **$2k/year** in premium income ($200k \times 1\%$).

Claim Event

- Six months later, the protocol suffers an exploit; distressed assets fall in value.
- Policyholders trigger a claim for the full **$2m** coverage.
- The pool pays out **$2m** in USDC to claimants instantly.
- Losses are allocated proportionally:
  - Each underwriter's share of pool = 1%.
  - Each bears **$20k** of the $2m loss.
  - Their principal reduces from $100k $\rightarrow$ $80k.

Salvage Rights

- Claimants transfer distressed assets (e.g., protocol tokens now worth **$500k** in secondary markets) into the pool as salvage.
- These are distributed to underwriters pro-rata to their loss share.
- Each underwriter receives **$5k worth** of distressed tokens.
- Effective net loss per underwriter: $20k payout – $5k salvage = **$15k**.

Outcome After 6 Months

- Premiums earned before the claim: $2k $\times$ 0.5 years = **$1k** per underwriter.
- Net result per underwriter:
  - Initial capital = $100k.
  - Loss = –$15k.
  - Premiums = +$1k.
  - Ending position = **$86k** value ($80k USDC + $5k distressed assets + $1k premium).

System-Level Observations

- Policyholders are fully compensated in stable USDC.
- Underwriters absorb the loss but partially offset it with premiums and salvage rights.
- Salvage creates asymmetric recovery: if distressed assets recover above $500k in value, underwriters' realised losses shrink further.

7 Glossary of Key Terms

Active Pledge (P^{active}) The amount of an underwriter's capital currently backing coverage in a pool, after applying notice locks, cooldowns, and solvency floor constraints.

Backstop Pool An ERC-4626 vault that provides protocol-native reinsurance. It covers claim shortfalls when underwriting pools are temporarily illiquid or undercapitalised.

Claim Fee A small fee payable by the policyholder when raising a claim. Designed to deter frivolous claims while keeping settlement predictable.

Cooldown Period A governance-defined delay before new or increased coverage becomes active. Prevents policyholders from purchasing cover opportunistically after a loss event has begun.

Coverage Floor The minimum capital each pool must retain, enforced by the `UnderwriterManager`, to ensure solvency when withdrawals or reallocations are requested.

Effective Shares (EffShares) The circulating pool shares used for NAV calculations. Defined as:

$$\text{EffShares} \equiv \text{TotalShares} - \text{unsettledPayoutShares}.$$

Loss Index ($D_i^{(\text{sh})}$) A per-pool shares-per-pledge index tracking realised claim losses. Ensures losses are attributed pro-rata and price-neutral regardless of PPS changes.

NAV (Net Asset Value) The total value of assets held in a pool or vault, denominated in the underlying token.

Notice Period A governance-defined waiting period before underwriters can deallocate or withdraw pledged capital. Protects solvency by preventing pre-claim withdrawals.

Oracle-Free Design Core functions (premium accrual, policy management, claim settlement) operate deterministically on-chain without external price feeds. The sole oracle use is circuit-breaking (pausing new policies on de-peg events).

Pending Loss Shares The shares an underwriter must burn to settle their portion of a claim, calculated from the change in the pool's loss index since their last snapshot.

Policy NFT A non-fungible token representing an active policy. Encodes coverage amount, deposit balance, and the right to claim. Transferable between users.

Premium Rate Curve A piecewise linear function defining how premium rates increase as pool utilisation rises, with separate slopes before and after a kink point.

Salvage Index ($S_{i,a}$) A per-pool, per-asset index tracking distressed assets received during claims. Updates in raw units (not valuations) and allocates salvage entitlements pro-rata.

Salvage Rights Entitlements of underwriters to distressed assets surrendered by policyholders during claims. Provides potential recovery of residual value.

Solvency Floors Capital requirements applied to ensure that total pledged assets in a pool always exceed coverage sold and pending losses.

Unsettled Payout Shares Shares reserved at the moment of a payout snapshot. NAV does not change until assets are actually transferred.

Utilisation The ratio of total coverage sold to available capital in a pool. Drives dynamic premium pricing.

`valueToShares` / `sharesToValue` Conversion functions between underlying token amounts and pool shares, ensuring price neutrality for deposits, withdrawals, and losses.

References

[1] F. Vogelsteller and V. Buterin, “ERC-20 Token Standard (EIP-20),” Ethereum Improvement Proposal, 2015. https://eips.ethereum.org/EIPS/eip-20

[2] W. Entriken, D. Shirley, J. Evans, and N. Sachs, “ERC-721 Non-Fungible Token Standard,” Ethereum Improvement Proposal, 2018. https://eips.ethereum.org/EIPS/eip-721

[3] M. Moody et al., “ERC-4626: Tokenized Vault Standard,” Ethereum Improvement Proposal, 2022. https://eips.ethereum.org/EIPS/eip-4626

[4] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger (Yellow Paper),” original 2014, living spec. https://ethereum.github.io/yellowpaper/paper.pdf

[5] Trail of Bits, “Smart Contract Security Best Practices,” guides and papers, ongoing. https://trailofbits.github.io

[6] Nexus Mutual, *Nexus Mutual Documentation*, ongoing. https://nexusmutual.io

[7] Sherlock, *Sherlock Protocol Documentation*, ongoing. https://docs.sherlock.xyz

[8] Unslashed Finance, *Unslashed Protocol Documentation*, ongoing. https://docs.unslashed.finance

[9] Rekt.news, “DeFi Exploit Postmortems (Euler, Curve, Mango, etc.),” ongoing. https://rekt.news

[10] Chainalysis, “Crypto Crime Report 2022,” ongoing. https://blog.chainalysis.com/reports

[11] Gauntlet, “Risk Assessment for On-Chain Insurance Markets,” Gauntlet Research, 2023.

[12] Bank for International Settlements, “DeFi Risk and Regulation,” BIS Quarterly Review, 2022.

[13] Lloyd’s of London, “About Lloyd’s: History and Market Structure,” overview page, ongoing. https://www.lloyds.com

[14] Basel Committee on Banking Supervision, “Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems,” Bank for International Settlements, 2011 (rev. updates). https://www.bis.org/bcbs/basel3.htm

[15] European Parliament and Council, “Directive 2009/138/EC (Solvency II),” Official Journal of the European Union, 2009 (as amended). https://eur-lex.europa.eu/eli/dir/2009/138/oj

[16] Centre Consortium, “USDC: Technical and Policy Resources,” ongoing. https://www.circle.com/en/usdc