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 are triggered deterministically by policyholders through a Hybrid Custody model: utilizing either a direct swap of distressed assets or, in the event of frozen protocols, an atomic escrow assignment. This ensures claims can be settled instantly without governance votes or subjective assessments, even if the underlying DeFi protocol has paused transfers. By combining modular risk assessment, tranched reinsurance protection, and salvage rights on payout, LayerCover delivers a capital-efficient alternative to mutualised risk pool designs, offering predictable and fully auditable protection for decentralised finance.

November 29, 2025

Contents

How LayerCover Works

1. Underwriters deposit USDC into capital pools backing specific DeFi protocols.
2. Policyholders purchase cover, paying premiums per second.
3. Policyholders claim by swapping their insured assets for instant USDC payouts. No votes, no delays.
4. Underwriters receive the insured assets as “salvage,” potentially recovering value over time.

That’s it. No governance votes. No waiting. No KYC. Just parametric, rules-based protection.

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.

Case Study: Black Thursday. In March 2020, MakerDAO’s liquidation system failed during a market crash, causing vault owners to lose collateral to near-zero bids. Users with Nexus Mutual coverage filed claims but members voted to reject all 16, with 99.96% opposing payouts. The dispute centred on whether this constituted a "smart contract failure" or simply adverse market conditions. This outcome illustrated a structural conflict: voters deciding claims are the same stakeholders whose capital pays them, creating systematic bias toward rejection when ambiguity exists.

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 pledge capital in their preferred asset (e.g. USDC, ETH) without exposure to governance tokens or volatile pool compositions. Multiple positions across different pools enable diversification while maintaining a predictable, controlled risk-return profile.

Dual-Revenue Efficiency: Underwriters earn from two sources: premiums from coverage sold, and yield from idle capital automatically deployed into low-risk strategies via yield adapters. The same principal can be pledged across multiple pools within solvency and leverage constraints set by the protocol.

Salvage Rights on Payout: Claims work like a swap: policyholders surrender their insured assets and receive USDC payouts. Underwriters receive the insured assets as "salvage." If those assets later recover value, underwriters benefit, converting a total loss into a partial one, or even a profit.

2.2 Policyholder Advantages

Flexible Coverage Options: LayerCover offers two pricing models. Variable-rate cover is perpetual and pay-as-you-go: premiums adjust dynamically based on pool utilisation, deposits can be topped up or refunded at any time, and policies lapse only when deposits run dry. For institutions requiring budget certainty, fixed-rate cover locks in a predetermined premium for a set duration.

Instant, Rules-Based Settlement: Claims settle automatically the moment a policyholder swaps a valid insured assets. No governance votes, no waiting periods, no subjective assessments. A small claim fee deters frivolous submissions.

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.

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

Underwriting in LayerCover is designed for capital efficiency. Unlike traditional models where liquidity is fragmented, underwriters deposit into a single main vault and virtually allocate that capital to multiple risk pools.

3.1.1 1. Deposit and Principal

Participation begins by depositing capital (e.g., USDC) into the **CapitalPool**, an ERC-4626 compliant vault.

- The vault issues shares at the current Price-Per-Share (PPS).
- This deposit forms the underwriter's **Principal**, which sits initially as "unpledged" capital earning passive yield from the underlying strategy.

3.1.2 Virtual Allocation (Pledging)

Underwriters actively manage risk by pledging their Principal to specific Risk Pools via the **Underwriter-Manager** contract.

- **No Token Movement:** Allocation is a bookkeeping operation. Assets do not physically move between contracts; the system simply records that a portion of the Principal is now backing coverage in the chosen pool.
- **Constraints:** Allocations are limited by the underwriter's **Risk Points Budget** and specific rules like **Mutex Groups** (which prevent exposure to correlated risks).
- **Effect:** Once allocated, the capital begins earning premium rewards immediately but also becomes liable for losses.

3.1.3 Managing Exposure (Deallocation)

If an underwriter wishes to reduce exposure to a specific pool without withdrawing funds from the protocol, they may submit a **Deallocation Request**.

- **Notice Period:** The request initiates a governance-defined notice period. This lock-up ensures underwriters cannot front-run imminent claims by instantly removing liquidity.
- **Execution:** Once the notice expires, the underwriter executes the deallocation. The pledge is removed, and the capital reverts to "unpledged" status within the vault.

3.1.4 Withdrawals and Auto-Scaling

To exit the protocol entirely, an underwriter requests to withdraw funds from the CapitalPool. This process includes a unique convenience feature:

- **Auto-Scaling Pledges:** Users do not need to manually deallocate from every pool before withdrawing. When Principal is withdrawn, the protocol automatically scales down the underwriter's active pledges across all pools in proportion to the reduction.
- **Solvency Protection:** To ensure the system remains collateralized, the manager enforces a **Coverage Floor**. If a requested withdrawal would leave a specific pool with insufficient capital to cover sold policies, the system executes the withdrawal only up to the safe limit, leaving the remainder pending until liquidity conditions improve.

3.2 Policyholder Operations

3.2.1 The Policy NFT Model

Policyholders obtain coverage by purchasing a **Policy NFT** from their chosen pool. Unlike fixed-term insurance, this NFT represents a perpetual, pay-as-you-go contract:

- **Flexible Funding:** The policy is backed by a user-controlled deposit that pays premiums second-by-second at the pool's current rate.
- **Transferability:** Ownership is tied to the NFT. Whoever holds the token controls the coverage, manages the deposit, and retains the right to file claims.
- **Active State:** As long as the deposit balance is sufficient to cover accrued costs, the policy remains active. If the deposit is exhausted, the policy lapses automatically.

3.2.2 Acquisition and Cooldowns

To purchase coverage, a user selects a pool, specifies the desired cover amount, and provides an initial premium deposit.

While the Policy NFT is minted immediately, coverage does not begin until a governance-defined **Cooldown Period** has elapsed. This delay is a critical security feature designed to prevent opportunistic behavior, such as purchasing cover immediately after an exploit has become public.

3.2.3 Policy Management

Policyholders retain full flexibility to adjust their position during the life of the policy. Note the asymmetry between increasing and decreasing risk:

- **Increases (Subject to Delay):** Users can request to increase their coverage amount at any time. These requests enter a pending queue and are only finalized after their own Cooldown Period expires. This prevents users from "front-running" a hack with a sudden coverage spike.
- **Reductions (Immediate):** Users can reduce their coverage or cancel their policy entirely at any time. These actions take effect immediately. Upon cancellation, the protocol settles premiums up to the current block and refunds any unused deposit to the user.

3.2.4 Claims and Emergency Operations

If a covered event occurs, the policyholder transfers the insured asset (or its proofs) to the protocol. In return, they receive an immediate payout from the pool's pledged capital.

Emergency Logic: If a pool is paused due to an active incident, the protocol prioritizes user exits. New purchases and coverage increases are disabled, but existing policyholders may still reduce coverage, cancel policies, or file claims.

Lifecycle Example The following timeline illustrates the flexibility of the deposit and coverage model:

- **Day 0 (Purchase):** User buys $100k cover with a $5k deposit. The NFT is minted, and the Cooldown clock starts.
- **Day 10 (Top-Up):** The user adds $2k to the deposit. Coverage continues without interruption.
- **Day 20 (Increase):** User requests an additional +$50k cover. This request enters the pending queue.
- **Day 22 (Finalization):** The cooldown expires, and the total active cover updates to $150k.
- **Day 40 (Reduction):** User reduces cover by $30k. This takes effect immediately, lowering the premium burn rate.
- **Day 60 (Cancel):** User cancels the policy. The remaining deposit is refunded to their wallet.

3.3 Managed Underwriting (Syndicates)

While individual underwriters can manage their own allocations, LayerCover also supports a delegated, professionally managed underwriting model known as *Syndicates*. A Syndicate is a specialized, manager-led vault that aggregates user capital to deploy liquidity across LayerCover's risk pools.

3.3.1 Structure and Capital Flow

Syndicates function as ERC-4626 compliant vaults, serving as the sole entry and exit point for passive depositors. Instead of analyzing individual protocols and managing complex allocation weights personally, users deposit a single asset (e.g., USDC) into a Syndicate and receive syndicate shares. These shares represent their pro-rata ownership of the vault's underlying capital and accrued yield.

The Syndicate Manager, typically a professional risk assessor or a DAO retains the exclusive authority to allocate this pooled capital to specific underwriting pools via the `Underwriter Manager` contract. This structure allows the manager to actively adjust risk exposure, diversify across mutex groups, and manage leverage ratios on behalf of all depositors. Crucially, the underlying capital inherits the protocol's standard notice periods and loss settlement rules, ensuring that syndicate liquidity subject to the same solvency constraints as individual underwriters.

3.3.2 Fee Mechanics and Incentives

To align the interests of managers and depositors, Syndicates utilise a configurable, on-chain fee model. Managers may charge:

- **Performance Fees:** Calculated using a high-watermark formula based on the vault's share value appreciation (e.g., premiums earned minus realised losses).
- **Management Fees:** A streaming rate charged on the total assets under management.

Both fee types are capped at the factory level (e.g., 20%) to protect depositors. These fees are accrued automatically and claimed by the manager, ensuring that compensation is strictly tied to the successful preservation and growth of the Syndicate's capital.

3.3.3 Registry and Security

Syndicates are deployed via a `SyndicateFactory`, which automatically registers them within the protocol. The core `UnderwriterManager` checks this registry to enforce access controls, ensuring that only valid Syndicate contracts (or individual underwriters) can allocate capital. This architecture streamlines the flow from passive liquidity to active protection, removing the need for intermediate curator layers while maintaining full auditability.

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.

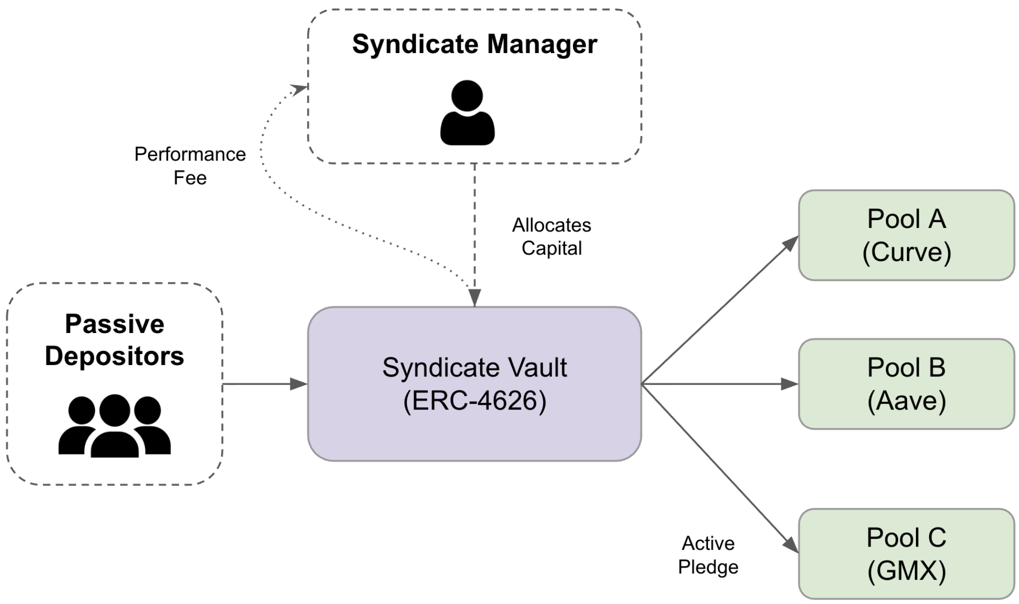

Figure 1: Syndicate Architecture: The Manager directs aggregated capital into diverse strategies, while Depositors retain passive exposure via a single vault token.

4 Core Protocol Mechanics

4.1 Protocol-Native Reinsurance (Tranched Backstop)

The Reinsurance Layer functions as a protocol-native safety net, ensuring claim settlement even during extreme liquidity events. Unlike traditional monolithic pools, LayerCover implements a structured **Shared Asset Controller** architecture. This design aggregates liquidity from multiple independent **Tranche Vaults**, enabling capital providers to select their preferred risk-adjusted return profile through specific priority tiers: Junior, Mezzanine, or Senior.

4.1.1 Capital Seniority and Waterfall Mechanics

The system enforces a strict seniority structure, known as the "loss waterfall," to determine the order in which capital is utilised for payouts. Each tranche vault t is assigned a priority index P_t, where a lower index corresponds to higher seniority (lower risk).

In the event of a solvency shortfall in a primary underwriting pool, the protocol triggers a drawdown from the Shared Asset Controller. Realised losses are allocated in *reverse priority order*:

- **Junior Tranche (First Loss):** This capital acts as the first line of defense. It absorbs claims immediately after primary pool covers are exhausted. Due to this high exposure, it commands the highest share of premiums.
- **Mezzanine Tranche:** Capital is drawn from this layer only after the Junior tranche has been fully depleted. It balances moderate risk with moderate rewards.
- **Senior Tranche (Last Loss):** This capital is the most protected layer in the system (P_0). It is utilised only in catastrophic tail events where both Junior and Mezzanine liquidity have been exhausted.

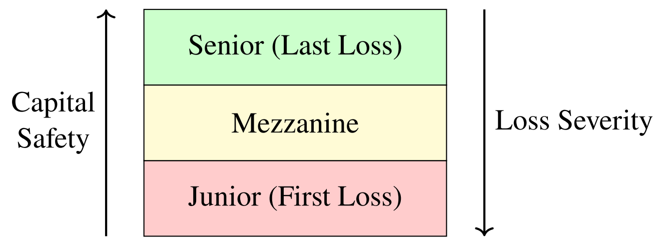

Figure 2: Reinsurance Capital Waterfall: Losses absorb from the bottom up (Junior → Senior), while capital safety increases from top to bottom.

4.1.2 Weighted Reward Distribution

To compensate for the asymmetric risk exposure defined by the waterfall, the "Reinsurance Tax" (the percentage of gross premiums routed to the backstop, see Sec. 4.5) is distributed differentially.

The Shared Asset Controller assigns a **Premium Weight** (W_t) to each tranche. Rewards are distributed pro-rata based on these weights rather than simple liquidity provision. This ensures that Junior depositors receive a significantly higher APY to compensate for their "First Loss" position, while Senior depositors earn a lower, more predictable yield reflecting their protected status.

4.1.3 Yield Efficiency via Shared Assets

While risk is segmented into tranches, liquidity is aggregated for efficiency. The Shared Asset Controller pools idle USDC from all tranches (Senior + Mezzanine + Junior) and deploys the aggregate balance into a single, whitelist-approved **Yield Adapter** (e.g., Aave V3 or Compound V3).

This architecture ensures that all reinsurance capital remains productive, earning external DeFi yields on top of their respective insurance premium shares, without fragmenting liquidity across multiple small deposit pools.

4.2 Loss Distribution

When a valid claim is processed, the protocol must allocate the financial loss across all active underwriters. To ensure this process is fair, manipulation-resistant, and gas-efficient, LayerCover employs a **Snapshot and**

Index model.

4.2.1 The Principle: Inescapable Liability

The core objective of the loss distribution engine is to ensure that liability is strictly pro-rata to the capital backing the risk *at the exact moment of the event*.

Once a claim is validated (block t_0), the protocol takes a snapshot of the pool's total eligible pledge base. This effectively "freezes" the liability.

- **No Front-Running:** An underwriter cannot avoid a loss by withdrawing their capital immediately after an exploit but before the claim is settled. If they had capital in the pool at t_0, they are liable.
- **No Retroactive Liability:** New capital entering the pool at block $t_0 + 1$ is never exposed to losses from events that occurred at t_0.

4.2.2 Mechanism: The Global Loss Index

Updating thousands of individual underwriter balances one-by-one is computationally expensive (high gas costs) and susceptible to DoS attacks. Instead, LayerCover uses an $O(1)$ **Global Loss Index**.

Similar to how a dividend stock tracks cumulative earnings, the pool tracks a cumulative *Loss-Per-Share*.

1. **The Global Update:** When a payout of amount X occurs, the pool calculates how many shares must be burned to cover X and adds this value to the Global Loss Index. This is a single, constant-time operation (See Appendix A.3).
2. **Lazy Settlement:** The system does not push updates to users immediately. Instead, an underwriter's share of the loss is calculated lazily the next time they interact with the protocol (e.g., claiming rewards, depositing, or withdrawing).
3. **Share Burning:** Upon interaction, the protocol compares the user's last observed index value against the current Global Index. It calculates the difference and burns the corresponding number of shares from the underwriter's balance.

4.2.3 Price Neutrality

A critical feature of this design is **Price Neutrality**. The system handles losses by burning shares rather than manipulating the Net Asset Value (NAV) arbitrarily.

When a claim is paid, the protocol reserves the necessary shares immediately. This ensures that the share price (PPS) remains accurate for incoming and outgoing users, and the economic cost of the loss is borne solely by reducing the share count of the affected underwriters.

4.2.4 Edge Case Resolution

- **Concurrent Claims:** If multiple claims occur simultaneously, they simply accumulate in the Global Index. The order of processing does not affect the final liability of the underwriters.
- **Zero Liquidity Events:** If a pool has zero eligible pledges at the time of a claim (an empty pool), the Global Index does not update. Instead, the claim is routed entirely to the **Backstop Pool** (see Section 3.3).
- **Dust and Rounding:** All divisions utilize fixed-point math with flooring. Any strict logical remainders ("dust") are left in the pool and effectively socialized, ensuring the protocol is never insolvent due to rounding errors.

4.3 Reward Distribution

To incentivize liquidity provision, LayerCover ensures that underwriters receive value from every second their capital is active. Unlike legacy models that rely on lump-sum payments, this protocol employs a **Continuous Streaming** engine.

4.3.1 Revenue Sources

Underwriters do not rely on a single income stream. The protocol aggregates rewards from three distinct sources into a unified yield:

1. **Policy Premiums:** The primary revenue driver. Premiums paid by policyholders accrue continuously (per second) and are distributed pro-rata to the active risk pools.
2. **Strategy Yield:** Capital not currently utilized for payouts is not left idle. It is deployed into whitelisted Yield Adapters (e.g., Aave or Compound) to earn external DeFi yields, which are rebated directly to the pool.
3. **Incentives:** Governance may configure specific pools to receive additional token emissions (e.g., protocol governance tokens) to bootstrap liquidity for high-priority sectors.

4.3.2 The Mechanism: The Reward Index

To distribute these rewards efficiently without looping through thousands of users (which would cause high gas costs), the protocol utilizes an $O(1)$ **Reward Index**.

The system functions similarly to an odometer:

- **Global Accumulation:** Whenever premiums or yields enter the pool, the Global Reward Index increments. This tracks the cumulative "Reward-Per-Token" generated by the pool since inception.
- **Lazy Settlement:** Rewards are calculated lazily. When an underwriter interacts with the pool (e.g., to claim or deposit), the system compares the current Global Index against the user's last checkpoint. The difference represents their accrued earnings.
- **Multi-Token Support:** The index engine is multi-dimensional, capable of tracking and streaming multiple assets simultaneously (e.g., distributing USDC premiums alongside ERC-20 governance incentives) without friction.

4.3.3 Fairness and Robustness

The distribution logic enforces strict economic fairness:

- **Eligibility Symmetry:** The system uses the exact same snapshot logic for rewards as it does for losses. If your capital is exposed to risk (eligible for a loss), it is automatically eligible for the rewards generated during that same second.
- **Price Neutrality:** Rewards are settled in the underlying tokens (e.g., sending USDC to the user's wallet) rather than by minting new pool shares. This prevents the dilution of the pool's Net Asset Value (NAV).
- **DoS Resistance:** Because the index update is a constant-time operation, the cost of distribution remains low and predictable, regardless of how many underwriters or active policies exist in the pool.

4.4 Premium Splits & Reinsurance Tax

Gross premiums paid by policyholders are split at the source to ensure continuous capitalization of the reinsurance layer.

$$P_{total} = P_{underwriter} + P_{backstop} \tag{4.1}$$

Where:

- **Backstop Share ($P_{backstop}$):** A fixed percentage (Default: 20%) is routed directly to the Backstop Pool. This acts as a protocol-native reinsurance tax, incentivizing passive liquidity providers to cover tail risks.
- **Underwriter Share ($P_{underwriter}$):** The remaining 80% is streamed to the specific risk pool and distributed to active underwriters pro-rata to their pledged capital.

4.5 Oracle-Free Architecture & Unit-Based Accounting

A defining characteristic of LayerCover is its minimization of external dependencies. By removing reliance on off-chain data feeds for core operations, the protocol eliminates the most common attack vector in DeFi: oracle manipulation.

4.5.1 1. Deterministic Execution

In traditional on-chain insurance, claims often rely on subjective governance votes or continuous price feeds. LayerCover replaces these with deterministic logic:

- **Internal Settlement:** Policy management, premium accrual, and claim payouts are executed entirely on-chain.
- **No "Price" Dependency:** The system does not need to know the USD price of an asset to settle a claim. If a policy covers 100 ETH, the payout is calculated and settled in ETH, regardless of market volatility.

4.5.2 3. Unit-Based Accounting

To reinforce this robustness, all liabilities are denominated in the underlying asset itself (Unit-Based Accounting).

- **Transparency:** Underwriters and policyholders share a common unit of account. 1000 USDC of cover is backed by 1000 USDC of principal.
- **Conflict Elimination:** This eliminates valuation disputes. There is no need to calculate the "dollar value" of a loss at a specific timestamp, removing the risk of front-running stale price updates during high volatility.

5 Flexible Custody & Salvage Mechanics

LayerCover employs a **Hybrid Custody Architecture** that decouples financial settlement (payouts) from asset recovery (salvage). This design allows the protocol to support both censorship-resistant assets (via non-custodial swaps) and complex, potentially pausable DeFi positions (via escrow vaults) without fragmenting the underwriting capital.

5.1 The Challenge: Frozen Assets

A major limitation in DeFi insurance is the “Frozen Asset” scenario. During an exploit, protocols often pause transfers or freeze user positions. If a policyholder holds these assets in their own wallet, they cannot transfer them to the insurer to prove the loss, effectively breaking the settlement process.

To resolve this, LayerCover utilizes two distinct custody models depending on the nature of the insured asset.

5.2 Model A: Direct Swap (Liquid Assets)

For immutable assets (e.g., WETH, RAI) or protocols that remain unpaused, the claim mechanism operates as a perpetual American-style Put Option.

- **Execution:** The policyholder approves and transfers the distressed asset to the protocol.
- **Validation:** The RiskManager verifies the policy is active and the premium is paid. No governance vote is required.
- **Settlement:** The protocol accepts the asset as salvage and instantly pays out the covered amount in USDC.

5.3 Model B: Escrow Vaults (The "Ledger Flip")

For yield-bearing positions (e.g., aTokens, Vault Shares) where the underlying protocol may pause transfers, LayerCover routes deposits into deterministic **Escrow Vaults**.

5.3.1 Vault Architecture

Each policy is linked to a lightweight escrow contract that holds the position on behalf of the user. The vault maintains an internal ledger separating beneficial ownership into two states:

1. **Unassigned Funds:** User Capital. Fully controlled by the policyholder and sweepable at any time.
2. **Assigned Funds:** Underwriter Salvage. Locked for recovery.

5.3.2 The Atomic Assignment

In the event of a claim even if the underlying DeFi protocol has halted withdrawals the system performs a "Ledger Flip."

5.3.3 Case Study: Capital Recycling (Euler Finance, March 2023)

To illustrate the critical value of tradeable salvage rights, consider a scenario modelled on the March 2023 Euler Finance exploit, where $197M in assets were frozen for three weeks before being returned.

The Trap: Illiquid Exposure Following the exploit, an underwriter with $100k pledged capital faces a difficult reality:

- A claim is processed, and $20k of their pledge is seized to pay policyholders.
- In exchange, they receive salvage rights to $20k worth of *frozen* Euler assets.
- Because the protocol is paused, these assets cannot be redeemed. The underwriter's capital is now "dead weight" earning zero yield and locked indefinitely.

The Solution: A Secondary Market for Risk LayerCover issues a transferable **Claim Right** token. This creates an immediate exit ramp via a secondary market trade:

Rational actors on both sides benefit from this transaction due to differing time horizons:

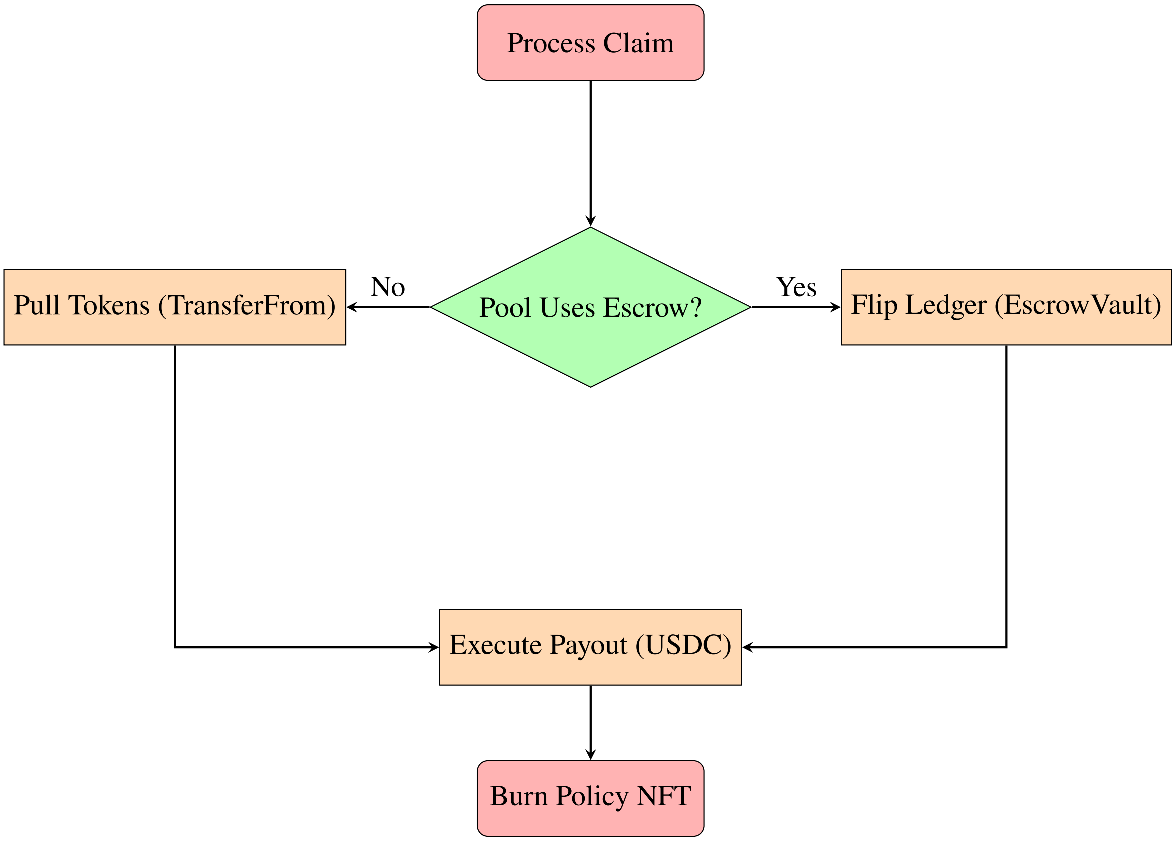

Figure 3: Logic flow for Claim Settlement showing the bifurcation between standard Token Salvage and Escrow Assignment paths.

1. **The Underwriter (Speed):** By accepting a realised loss today, they recover $4,000 immediately. This capital can be re-deployed into a healthy pool (e.g., Aave) to begin earning 8–12% yields again. They effectively swap "uncertainty" for "opportunity."
2. **The Buyer (Patience):** Specialised distressed debt funds operate with multi-year horizons. In the actual Euler case, the attacker returned ~90% of funds. A buyer at 20 cents would have realized a **4.5× return** in under a month.

Historical Context: The Cost of Waiting While Euler resolved quickly, other incidents highlight the danger of being unable to exit:

- **Multichain (2023):** Bridge funds remained frozen indefinitely. Underwriters without an exit option would hold worthless claims forever.
- **FTX (2022):** Creditors waited 18+ months for recovery. An underwriter trapped in such a claim would miss multiple market cycles.

Net Effect This mechanism transforms a binary outcome (total loss vs. full recovery) into a spectrum of liquidity options. It ensures that LayerCover underwriters are never forced to become long-term distressed debt holders against their will.

Metric	Seller (Underwriter)	Buyer (Distressed Fund)
Action	Sells frozen claim rights	Buys claim at deep discount
Price Execution	**20 cents** on the dollar	Pays $4,000 for $20k face value
Immediate Result	Recoups $4,000 liquidity	Assumes 100% of the lockout risk
Strategic Goal	**Capital Velocity**	**Asymmetric Upside**

Table 1: Anatomy of a Salvage Right Trade

6 Hybrid Premium Pricing

LayerCover employs a dual-pricing architecture designed to solve a critical DeFi insurance problem: balancing immediate liquidity availability for retail users with price certainty for large institutional hedgers. The system operates two distinct but interconnected pricing tiers:

1. **Variable Rate (Pool-Based):** A perpetual, pay-as-you-go model for flexible coverage.
2. **Fixed Rate (Intent-Based):** An RFQ-style marketplace for fixed-duration, fixed-rate contracts.

6.1 Variable Rate Model (Adaptive Base Rate)

For standard users, coverage is purchased via the **Variable Pool**. Unlike traditional models that rely solely on utilization (supply and demand) to set prices, LayerCover utilizes an **Adaptive Base Rate (ABR)**.

The ABR mechanism links the variable pool to the open market. It continuously monitors the "implied risk" signal from professional market makers in the Fixed Rate order book. If professional underwriters raise their prices to account for new risks, the Dynamic Rate Engine automatically lifts the floor price of the variable pool.

This creates a self-correcting market:

- **Protection:** It prevents "lazy" capital in the variable pool from being sold cheaply during high-risk events that professionals have already priced in.
- **Failsafe:** If the market order book is empty or unreliable, the system reverts to a governance-defined Fallback Rate to ensuring coverage is always purchasable.

6.2 Resilience Against Market Manipulation

Since the Adaptive Base Rate (ABR) relies on open market signals, the protocol implements specific defenses against both downward pressure ("spoofing") and upward pressure ("anchoring").

6.2.1 Defense Against Spoofing: The Arbitrage Trap

To prevent underwriters from posting artificially low quotes to suppress the variable rate, the protocol enforces the **Arbitrage Trap**. Any quote posted to the order book is instantly executable.

If an attacker posts a quote below the true risk premium to manipulate the ABR, rational hedgers or arbitrage bots can atomically fill that quote. This forces the attacker to underwrite the risk at a financial loss, ensuring that the cost of manipulation exceeds the potential gain.

6.2.2 Defense Against Anchoring: Outlier Rejection

Conversely, underwriters may attempt to artificially inflate pool premiums to discourage competition. LayerCover neutralizes this by exclusively utilizing the **lowest valid ask** (R^{min}_{fixed}) to calculate the base rate.

$$\text{ABR} = \min(Q_1, Q_2, \ldots, Q_n) \times \alpha$$

By applying this minimization function, quotes priced significantly above the market rate are automatically filtered out. These high outliers remain in the order book as valid future offers but have zero impact on the current Variable Pool pricing.

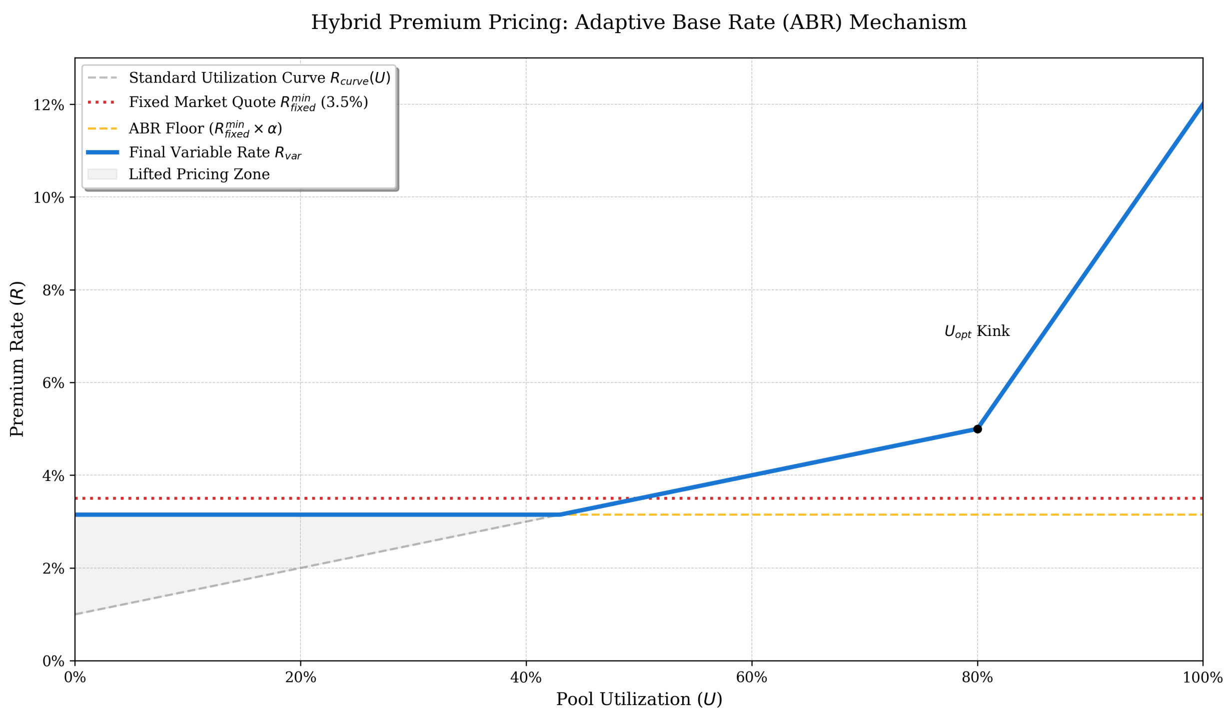

Figure 4: Utilisation–based premium curve

6.3 Fixed Rate Model (Intent-Based)

Institutional hedgers and market makers often require budgetary certainty that variable rates cannot provide.

In the **Intent-Based** model, Underwriters (via Syndicates) sign cryptographically verifiable "Intents" off-chain. These are binding offers to provide a specific amount of coverage at a fixed annualized rate for a fixed duration.

- **Capital Efficiency:** When a policyholder matches an intent, the underwriter's capital is locked in their Syndicate vault for the exact duration of the policy.
- **Direct Revenue:** Unlike the socialized variable pool, the underwriter matches directly with the buyer and receives 100% of the specific premium generated by that policy.

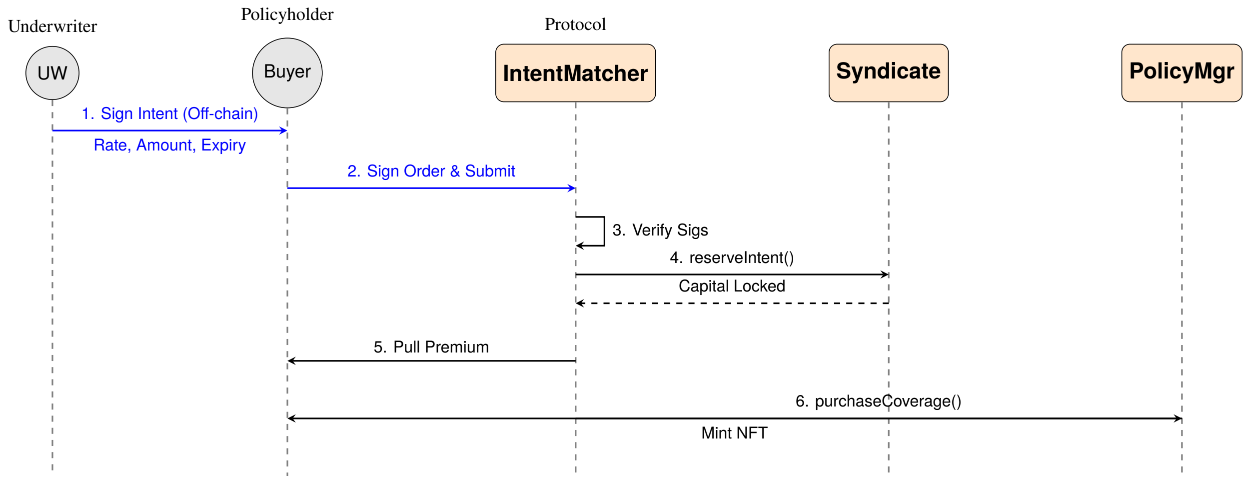

Figure 5: Intent Matching Lifecycle: An atomic RFQ process where off-chain signatures from the Underwriter and Buyer are matched on-chain, triggering simultaneous capital locking and policy issuance.

7 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.

7.1 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.

[tikz,border=10pt]standalone tikz

7.2 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.

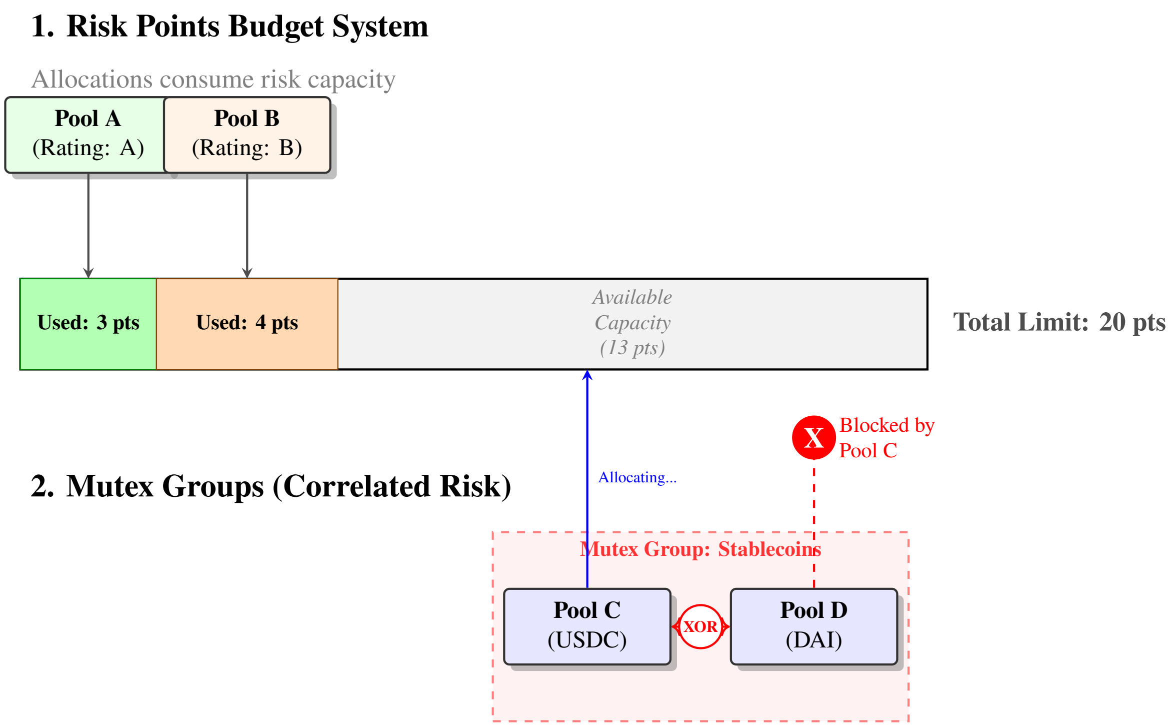

Figure 6: Risk Points and Mutex Group Architecture

7.3 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.

7.3.1 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.

7.3.2 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.

7.3.3 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.

7.3.4 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.

8 Economic Scenario Analysis

To illustrate how capital flows through the system in practice, consider the following scenario using real numbers.

8.1 Scenario Setup

- **TVL:** A DeFi protocol has $10m Total Value Locked.
- **Coverage:** Policyholders purchase cover totaling **$2m** from a LayerCover pool.
- **Capital:** The pool has 100 underwriters, each pledging $100k USDC. Total Pledged = **$10m**.
- **Utilization:** Coverage sold ($2m) / Available Capital ($10m) = **20% Utilization**.
- **Rate:** Based on the curve, the premium rate is **10% annualized**.

8.2 Premium Flow (Income)

The annual premium for $2m coverage at 10% is $200k/year. This accrues per second and is distributed pro-rata to underwriters.

- Each underwriter owns a 1% share of the pool ($100k / $10m).
- Each earns **$2k/year** in premium income ($200k \times 1\%$).

8.3 The Claim Event (Loss)

Six months later, the protocol suffers an exploit. Policyholders trigger a valid claim for the full $2m.

1. **Payout:** The pool pays out $2m in USDC instantly.
2. **Loss Allocation:** Losses are allocated proportionally.
   - Each underwriter bears 1% of the loss ($20k).
   - Their principal reduces from $100k → **$80k**.

8.4 Salvage Recovery

Policyholders must surrender their insured assets (e.g., protocol tokens) to receive the payout. Suppose these tokens still trade at $0.25 on secondary markets (total value $500k).

- These assets are distributed to underwriters as salvage.
- Each underwriter receives **$5k** worth of tokens ($500k \times 1\%$).
- **Effective Net Loss:** $20k (Payout) - $5k (Salvage) = **$15k**.

8.5 Final Outcome (After 6 Months)

- **Premiums Earned:** $1k (6 months of streaming income).
- **Net Result:**

$$\$100k \text{ (Initial)} - \$15k \text{ (Net Loss)} + \$1k \text{ (Premiums)} = \textbf{\$86k Ending Value}$$

Observation: The system ensured policyholders were fully compensated in stable USDC immediately. Underwriters absorbed the loss but successfully mitigated 25% of it via salvage rights and offset it further with earned premiums. If the salvage assets later recover in value, the underwriters' net loss shrinks further.

9 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 ($D_i^{(\mathbf{sh})}$) 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 insured assets received during claims. Updates in raw units (not valuations) and allocates salvage entitlements pro-rata.

Salvage Rights Entitlements of underwriters to insured 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] Nexus Mutual, *Nexus Mutual Documentation*, ongoing. https://nexusmutual.io

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

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

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

[5] Chainalysis, "Crypto Crime Report 2022," ongoing. https://blog.chainalysis.com/reports

[6] Gauntlet, "Risk Assessment for On-Chain Insurance Markets," Gauntlet Research, 2023.

[7] Bank for International Settlements, "DeFi Risk and Regulation," BIS Quarterly Review, 2022.

[8] Lloyd's of London, "About Lloyd's: History and Market Structure," overview page, ongoing. https://www.lloyds.com

[9] 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

[10] 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

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

10 Appendix A: Mathematical Specifications

This appendix formalizes the core pricing, accounting, and settlement mechanisms described in the LayerCover protocol.

10.1 A.1 Hybrid Premium Pricing

10.1.1 Variable Rate Calculation

The variable premium rate R_{var} is calculated dynamically at the time of purchase. It is the greater of the standard utilization curve or the market-driven Adaptive Base Rate (ABR).

$$R_{var}(U, R_{fixed}^{min}) = \max\left(R_{curve}(U), \quad R_{fixed}^{min} \times \alpha\right) \tag{10.1}$$

Where:

- $R_{curve}(U)$: The standard utilization-based interest rate curve.
- R_{fixed}^{min}: The lowest valid fixed-rate quote currently available in the active Intent Orderbook.
- α: A governance-controlled dampening factor (e.g., 0.9) to prevent deep arbitrage.

10.1.2 Utilization Curve

The underlying pricing curve follows a dual-slope model to manage capital efficiency and solvency.

$$R_{curve}(U) = \begin{cases} R_{base} + \frac{U}{U_{opt}} \cdot S_1 & \text{if } U \leq U_{opt} \\ R_{base} + S_1 + \frac{U - U_{opt}}{1 - U_{opt}} \cdot S_2 & \text{if } U > U_{opt} \end{cases} \tag{10.2}$$

10.1.3 Fixed Rate (Intent) Cost

For fixed-rate policies, the total premium P_{intent} is deterministic and paid upfront.

$$P_{intent} = \frac{C \cdot r_{fixed} \cdot T}{365 \times 10000} \tag{10.3}$$

Where C is coverage amount, r_{fixed} is the annualized rate in basis points, and T is duration in days.

10.2 A.2 Core Accounting Price Neutrality

10.2.1 Share Conversion

To ensure deposits and withdrawals do not dilute existing participants, the protocol tracks an effective circulating supply.

$$\text{EffShares} = \text{TotalShares} - \text{unsettledPayoutShares} \tag{10.4}$$

$$\text{valueToShares}(V) = \begin{cases} V & \text{if } NAV = 0 \text{ or EffShares} = 0 \\ \left\lfloor \frac{V \cdot \text{EffShares}}{NAV} \right\rfloor & \text{otherwise} \end{cases} \tag{10.5}$$

10.3 A.3 Loss Distribution Indexing

Realized losses are allocated pro-rata to underwriters based on their active pledge at the block of the event, using a global shares-per-pledge index $D^{(sh)}$.

10.3.1 Global Index Update

On a realized loss L (in underlying units):

$$\text{lossShares} = \text{valueToShares}(L) \tag{10.6}$$

$$D_i^{(sh)} \leftarrow D_i^{(sh)} + \frac{\text{lossShares} \cdot \text{PRECISION}}{\text{totalPledged}_i} \tag{10.7}$$

10.3.2 Underwriter Settlement

An underwriter u's pending loss is calculated lazily upon interaction:

$$\text{PendingLossShares}_{u,i} = \max\left(0, \frac{P_{u,i}^{active} \cdot \Delta D_i^{(sh)}}{\text{PRECISION}}\right) \tag{10.8}$$

These shares are burned to settle the liability:

$$\text{burn}(\text{PendingLossShares}_{u,i}) \tag{10.9}$$

10.4 A.4 Reward Distribution Indexing

Premiums are streamed continuously. When an amount Q of token τ is distributed to pool i:

$$R_{i,\tau} \leftarrow R_{i,\tau} + \frac{Q \cdot \text{PRECISION}}{\text{totalPledged}_i} \tag{10.10}$$

The claimable reward for underwriter u is:

$$\text{PendingReward}_{u,i,\tau} = \max\left(0, \left\lfloor \frac{P_{u,i}^{active} \cdot R_{i,\tau}}{\text{PRECISION}} \right\rfloor - d_{u,i,\tau}\right) \tag{10.11}$$

Where $d_{u,i,\tau}$ is the underwriter's last observed reward snapshot.