LayerCover

Protocol Whitepaper

layercover.com

Abstract

DeFi has suffered over $8 billion in losses since 2020, while most on-chain capital remains uninsured. LayerCover is a rules-based insurance marketplace where professional underwriters quote fixed rates, policyholders buy coverage instantly, and claims settle without governance voting delays. The model combines transparent pricing, deterministic payout logic, and a four-layer capital waterfall (pool capital, external reinsurance, backstop, treasury). For investors, the core thesis is straightforward: a large protection gap, recurring premium revenue, capital-efficient underwriting, and distribution loops through partners and referrals. The protocol is designed to scale from crypto-native users to institutional participants by pairing on-chain execution with explicit risk controls.

February 13, 2026

Contents

1 Investor Snapshot **3**
1.1 What Problem Is Being Solved 3
1.2 How the Business Model Works 3
1.3 Why This Can Scale 4
1.4 What Could Go Wrong 4
2 Introduction **4**
2.1 Why Now 4
2.2 The Syndicate Model 4
2.3 Limitations of Current Models 4
2.4 Competitive Landscape 5
3 Key Benefits of LayerCover **5**
3.1 Supply-Side Economics 6
3.2 Demand-Side Economics 6
3.3 Distribution Economics 6
4 User Operations **6**
4.1 Underwriter Operations 6
4.2 Policyholder Operations 6
4.3 Managed Underwriting (Syndicates) 6
5 Core Protocol Mechanics **7**
5.1 Third-Party Reinsurance Integration 7
5.2 Multi-Layer Payout Waterfall 7
5.3 Loss Distribution 8
5.4 Reward Distribution 9
5.5 Premium Splits & Reinsurance Tax 10
5.6 Deterministic Settlement (Vault and Stablecoin Cover) 11
5.7 Optimistic Oracle Settlement (Parametric Markets) 11
6 Flexible Custody & Salvage Mechanics **12**
6.1 The Challenge: Frozen Assets 12
6.2 Model A: Direct Swap (Liquid Assets) 12
6.3 Model B: Vault Cover 12
7 Fixed-Rate Premium Pricing **15**
7.1 The Intent-Based Orderbook 15
7.2 Quote Validity and Anti-Gaming Controls 15
7.3 Pricing Authority and Design Choice 15
8 Governance and Risk Management **15**
8.1 Risk Points System 16
8.2 Pool Ratings and Constraints 16
8.3 Institutional Risk Alignment 16
8.4 Upgradeability and Trust Model 17
8.5 Known Risks and Limitations 17
9 Economic Scenario Analysis **18**
9.1 Baseline Assumptions 18
9.2 Worked Base Case 18
9.3 Stress Summary 18
10 Glossary of Key Terms **19**
11 Appendix A: Mathematical Specifications **21**

11.1 A.1 Fixed-Rate Premium Pricing 21
11.2 A.2 Core Accounting Price Neutrality 21
11.3 A.3 Loss Distribution Indexing 21
11.4 A.4 Reward Distribution Indexing 22
11.5 A.5 Premium Routing Invariants 22
11.6 A.6 Quote-Failure Compensation Bound 22

How LayerCover Works

1. Underwriters deposit USDC into capital pools backing specific DeFi protocols.
2. Policyholders purchase fixed-term cover by matching quotes on the orderbook and paying premiums upfront.
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. Just parametric, rules-based protection.

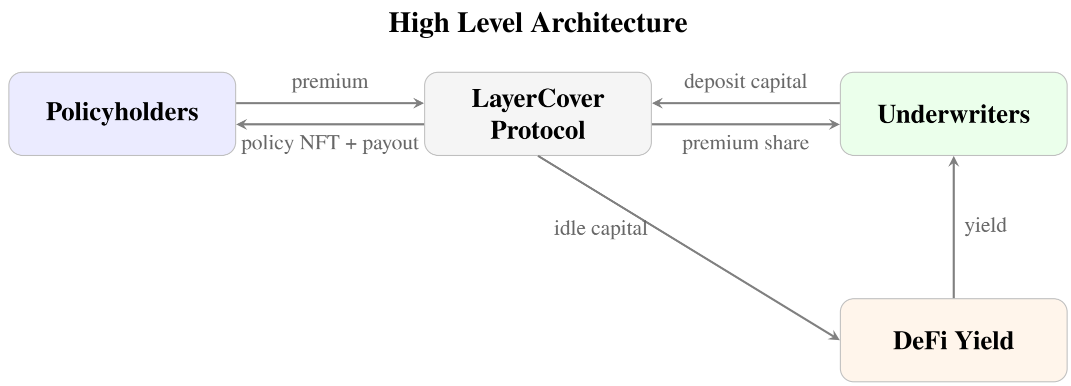

Figure 1: Policyholders pay premiums and receive Policy NFTs and claim payouts. Underwriters deposit capital and earn premium income. Idle capital is deployed into DeFi yield strategies, with returns flowing back to underwriters.

Coverage Type	Example Risks	Settlement Method	Salvage Required
Vault Cover	Yield vault exploits, lending protocol hacks	Deterministic (Asset Swap)	Yes
Stablecoin Depeg	USDC, DAI, FRAX de-peg events	Deterministic (Asset Swap)	Yes
Parametric Markets	Earthquakes, weather events, protocol incidents	Optimistic Oracle (UMA V3)	No

Table 1: LayerCover Coverage Types: Three product categories with distinct settlement mechanisms.

1 Investor Snapshot

1.1 What Problem Is Being Solved

DeFi users and treasuries face frequent tail risk (hacks, depegs, protocol failures) with limited reliable protection. LayerCover targets this protection gap with insurance-like products that can settle quickly and transparently.

1.2 How the Business Model Works

- **Revenue source:** policy premiums.
- **Supply side:** underwriters allocate capital and earn premium + yield.
- **Demand side:** policyholders pay for fixed-rate protection and fast claims.

- **Resilience:** losses are absorbed through a defined capital waterfall.

1.3 Why This Can Scale

- **Recurring premium flow** from ongoing coverage demand.
- **Transparent pricing** via competitive quotes rather than opaque curves.
- **Distribution leverage** through referrals, partner integrations, and wallets.
- **Institutional compatibility** through explicit risk controls and auditable on-chain data.

1.4 What Could Go Wrong

Key risks are systemic correlation during crises, oracle/dispute risk in parametric markets, and governance/upgrade execution risk. These are discussed in detail in Section 8.5.

2 Introduction

DeFi has reached meaningful scale, but its risk transfer infrastructure remains early. Since 2020, protocol failures and exploit events have created over $8 billion in losses [4, 3], while most capital remains uninsured. Traditional insurance markets solved this problem through specialist underwriting and pooled risk transfer [6]; DeFi still largely relies on ad hoc governance or self-insurance. LayerCover is designed to close that gap with transparent, programmable coverage and faster, rules-based settlement.

2.1 Why Now

Institutional and treasury participation in DeFi has increased, but insurance primitives have not kept pace. Capital allocators now expect predictable pricing, fast claims, and transparent risk controls. LayerCover addresses this by combining fixed-rate underwriting, deterministic settlement paths, and composable on-chain capital.

2.2 The Syndicate Model

At the heart of LayerCover is the **Syndicate**: a manager-led underwriting vault. Passive LPs supply capital, while specialist managers allocate risk and earn performance-linked fees. This separation creates clearer accountability, supports manager track records, and enables scaled underwriting capacity without requiring every LP to run active risk operations.

2.3 Limitations of Current Models

Today, the on-chain cover market is dominated by **mutualised risk pool** models [1]. 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. This can lead to situations where claims are rejected despite clear losses, as seen in the Black Thursday incident with Nexus Mutual [1, 3].
- **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.

- **Opaque pricing:** Premiums are set by utilisation curves, algorithmic functions that adjust rates based on pool capacity. These curves are difficult for policyholders to predict and for underwriters to reason about, creating pricing inefficiency and discouraging institutional participation.
- **No underwriter specialisation:** All capital in a mutualised pool bears the same risk profile. There is no mechanism for experienced risk managers to differentiate their exposure, charge bespoke rates, or build a track record, reducing the market's ability to price risk accurately.
- **No reinsurance integration:** Existing protocols lack hooks for external capital to backstop extreme events. When catastrophic losses exceed pool capacity, policyholders receive partial or no payouts with no systematic recovery path.

Illustrative failure mode. Black Thursday (March 2020) showed how governance-based claims can fail under stress: claim voters are often economically exposed to payouts, creating an embedded conflict during ambiguous events [1, 3].

2.4 Competitive Landscape

The following table compares LayerCover against the traditional insurance market (Lloyd's of London), the leading on-chain mutual alternative (Nexus Mutual), and prediction market-based approaches (Polymarket).

Feature	LayerCover	Nexus Mutual	Polymarket	Lloyd's of London
Claim Settlement	Instant parametric; USDC payout	Governance vote; ETH/-DAI	Market resolution; USDC	Manual assessment; fiat
Pricing Model	Fixed-rate orderbook	Utilisation curve	AMM/CLOB speculation	Broker-negotiated
Transparency	Fully on-chain, non-custodial	Partially on-chain, pooled	Fully on-chain, order-based	Off-chain, paper-based
Underwriter Control	Per-pool allocation	Shared pool exposure	Position-based	Syndicate-specific
Coverage Guarantee	Instant settlement; pro-rata fallback	Capital-dependent	None (speculation only)	Contractual obligation
Salvage Rights	Tradeable on-chain tokens	None	N/A	Complex legal process
Reinsurance	Third-party integration	None (single pool)	None	External reinsurers

Table 2: Competitive comparison: LayerCover combines the professional syndicate model of Lloyd's with the trustless execution of DeFi, while eliminating the governance delays of mutual models and providing deterministic, instant settlement unlike speculative prediction markets.

For investors, the key distinction is that LayerCover is built for *protection markets*, not event speculation: underwriting capital is explicitly risk-bearing, premium flows are explicit, and payout paths are predefined.

3 Key Benefits of LayerCover

Investment-relevant advantages. LayerCover improves on legacy cover designs across supply, demand, and distribution.

3.1 Supply-Side Economics

- **Cleaner collateral profile:** Underwriters can remain in preferred assets (e.g. USDC) rather than forced exposure to governance tokens.
- **Two return streams:** Premium income plus yield on idle capital (see Section 4.3).
- **Recovery optionality:** Tradeable salvage rights can offset losses after claims (see Section 6).

3.2 Demand-Side Economics

- **Price certainty:** Premiums are fixed at purchase (see Section 7).
- **Lower claim friction:** Deterministic settlement paths reduce payout latency (see Section 5.6).
- **Higher payout resilience:** Reinsurance and waterfall layers improve fulfilment under stress (see Section 5.1).

3.3 Distribution Economics

- **Embedded distribution:** Wallets, apps, and protocols can earn referral share on premium volume.
- **Flywheel potential:** Better coverage availability improves user trust, which can increase covered volume and premium flow.

4 User Operations

4.1 Underwriter Operations

Underwriters deposit USDC into ERC-4626 vaults, receive shares, and allocate exposure across pools through bookkeeping pledges (no token movement between pools). Returns come from:

- policy premiums on active exposure;
- yield on idle capital via approved adapters.

Exposure reductions and withdrawals are constrained by lock duration and solvency floors. If a user withdraws, active pledges are auto-scaled to avoid manual deallocation from each pool.

4.2 Policyholder Operations

Policyholders buy fixed-term coverage by matching signed intents on the orderbook. Execution atomically:

1. locks underwriting capital,
2. transfers premium,
3. mints a transferable Policy NFT.

Coverage activation and increases are subject to cooldown windows; reductions and cancellations are immediate. Claims are rules-based: policyholders transfer the insured asset (or satisfy parametric resolution), then receive payout from available waterfall capacity.

4.3 Managed Underwriting (Syndicates)

Syndicates are manager-led underwriting vaults for passive LP capital. Managers control pool allocation and risk budgeting; LPs hold vault shares and receive pro-rata performance.

Manager compensation is on-chain and capped (e.g. management + performance fee bounds), with accrual tied to vault outcomes. Syndicate registration via factory contracts enforces access control and standard risk constraints.

5 Core Protocol Mechanics

This section explains how LayerCover enforces payouts, allocates losses, and routes premium cash flows. For investors, the objective is to make revenue and downside behavior explicit under both normal and stressed conditions.

5.1 Third-Party Reinsurance Integration

Status: *Contract hooks for third-party reinsurance are implemented; operational onboarding is phased.*

LayerCover supports excess-of-loss reinsurance for pool shortfalls. Each reinsurer specifies:

- attachment point A,
- payout limit L,
- optional aggregate annual limit.

Per-event payout is:

$$\text{Reinsurer Payout} = \min\left(\max(0, \text{Loss} - A), L\right) \tag{5.1}$$

Premium allocation to reinsurers can be risk-weighted:

$$P_{reinsurer} = P_{total} \cdot \tau_{reinsurance} \cdot \frac{C_{reinsurer} \cdot W_{risk}}{C_{total\_weighted}} \tag{5.2}$$

On shortfall, drawdown executes by attachment layer (lowest first), pro-rata within a layer. If total capacity is insufficient, claims settle pro-rata:

$$\text{Payout}_i = \text{Claim}_i \cdot \frac{\text{Available Capital}}{\text{Total Claims}} \tag{5.3}$$

Salvage rights are allocated by funded payout share, preserving deterministic attribution between primary underwriters and reinsurers.

5.2 Multi-Layer Payout Waterfall

When a valid claim is processed, the protocol draws capital through an ordered sequence of funding layers. Each layer absorbs as much of the claim as it can before the next layer activates:

1. **Layer 1 – Pool Capital:** The primary source. Capital pledged by syndicates to the specific risk pool is used first. Losses are allocated pro-rata to underwriters based on their active pledge at the moment of the event (see Section 5.3).
2. **Layer 2 – Third-Party Reinsurance:** If syndicate capital is insufficient, the protocol draws from registered external reinsurers in order of their attachment points (see Section 5.1).
3. **Layer 3 – Backstop Pool:** A protocol-wide reserve funded by a percentage of all premiums (see Section 5.5). Provides a safety net independent of any single pool's capitalization.
4. **Layer 4 – Protocol Treasury:** Last resort. The protocol treasury absorbs any remaining deficit.

Figure 2: Capital is drawn through four successive layers; any remainder cascades to the next. If all layers are exhausted, the claim is partially paid.

If all four layers are exhausted, the claim is **partially paid**: the claimant receives whatever capital was gathered and the remainder is forfeited.

5.3 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.

In Simple Terms: When a claim occurs, the protocol takes a "snapshot" of who had capital in the pool at that moment. Those underwriters and only those underwriters share the loss proportionally. New deposits after the event are protected; withdrawals before the snapshot don't escape liability.

5.3.1 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.

5.3.2 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.

5.3.3 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.

5.3.4 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 through downstream waterfall layers (see Section 5.2).
- **Dust and Rounding:** All divisions utilise fixed-point math with flooring. Any strict logical remainders ("dust") are left in the pool and effectively socialised, ensuring the protocol is never insolvent due to rounding errors.

5.4 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.

5.4.1 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.

5.4.2 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.

5.4.3 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.

5.5 Premium Splits & Reinsurance Tax

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

$$P_{total} = P_{underwriter} + P_{backstop} \tag{5.4}$$

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.

To make the split explicit, define $\alpha \in [0, 1]$ as the backstop share:

$$P_{backstop} = \alpha P_{total}, \qquad P^{gross}_{underwriter} = (1 - \alpha) P_{total} \tag{5.5}$$

If governance enables an incentive redirect from the underwriter stream, let $\delta \in [0, \delta_{max}]$ denote that transfer fraction:

$$P_{incentive} = \delta P^{gross}_{underwriter}, \qquad P^{net}_{underwriter} = (1 - \delta) P^{gross}_{underwriter} \tag{5.6}$$

The conservation invariant remains:

$$P_{total} = P_{backstop} + P^{net}_{underwriter} + P_{incentive} \tag{5.7}$$

This prevents ambiguity around premium routing and guarantees that total premium allocation remains exactly 100% under all valid parameter settings.

5.6 Deterministic Settlement (Vault and Stablecoin Cover)

For vault cover and stablecoin depeg protection, LayerCover minimizes external dependencies through deterministic settlement:

- **Internal Settlement:** Policy management, premium accrual, and claim payouts are executed entirely on-chain without external price feeds.
- **Asset Swap Mechanics:** Claims settle via direct asset transfer: policyholders surrender the insured asset and receive instant USDC payouts at the snapshotted coverage amount.
- **No Price Oracle Dependency:** The system does not query external oracles to determine payout amounts. Coverage is denominated in the underlying asset units, eliminating oracle manipulation vectors.

5.7 Optimistic Oracle Settlement (Parametric Markets)

For parametric risk markets, including earthquake cover, weather events, protocol incidents, and other externally-verifiable outcomes, LayerCover integrates with **UMA Optimistic Oracle V3** [2] for trustless, objective resolution.

How It Works:

1. **Market Definition:** Each parametric pool is configured with an `oracleQuestionCID`, an IPFS-pinned assertion question that defines the exact conditions for a valid claim (e.g., "Did an earthquake of magnitude 6.0 or greater occur in California between [start] and [end]?").
2. **Claim Initiation:** When a policyholder believes a covered event has occurred, they submit an assertion to UMA's Optimistic Oracle.
3. **Challenge Period:** The assertion enters a dispute window (typically 2 hours). If unchallenged, it resolves as true.
4. **Dispute Resolution:** If disputed, UMA's decentralized Data Verification Mechanism (DVM) votes on the outcome, ensuring objective resolution.
5. **Automatic Settlement:** Upon positive resolution, the protocol automatically processes payouts to all valid policyholders.

Key Benefits:

- **No Salvage Required:** Unlike vault cover, parametric claims do not require policyholders to surrender assets; payouts are triggered purely by event verification.
- **Tamper-Proof Questions:** Resolution criteria are immutably stored on IPFS, preventing post-hoc modification of claim conditions.
- **Objective Verification:** UMA's economic security model ensures honest resolution through bonded assertions and slashing.
- **Real-World Coverage:** Enables insurance for physical events (earthquakes, hurricanes) and off-chain incidents that cannot be verified through on-chain state alone.

5.7.1 Unit-Based Accounting

To reinforce robustness across both settlement models, 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.

6 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 liquid assets (via direct swaps) and yield-bearing vault positions (via snapshot and transfer) without fragmenting the underwriting capital.

6.1 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.

6.2 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.
- **Settlement:** The protocol accepts the asset as salvage and instantly pays out the covered amount in USDC.

6.3 Model B: Vault Cover

For yield-bearing positions (e.g. ERC-4626 Vault Shares [10]) where the underlying protocol acts as the primary store of value, LayerCover utilises a Snapshot & Transfer model.

6.3.1 Value Snapshotting

When a user purchases cover for a vault, the protocol queries the vault's current exchange rate (`convertToAssets`) and records a `VaultCoverSnapshot`. This locks in the "Insured Value" in USDC terms.

User Custody:
The user retains full custody of their vault shares in their own wallet. They continue to earn yield and can exit the vault at any time (effectively cancelling the cover).

Fixed Liability:
The protocol's liability is fixed to the snapshot value. If the vault suffers an exploit and the share price crashes, the protocol is committed to paying the pre-loss value.

6.3.2 Claim Execution (The Asset Swap)

In the event of a claim, the settlement process mirrors a standard asset swap:

- **Transfer:** The policyholder transfers their vault shares to the Risk Manager contract.
- **Payout:** The protocol validates the transfer and instantly pays out the specific USDC amount recorded in the snapshot.
- **Salvage:** The protocol holds the transferred shares as salvage. Even if the vault is currently paused or the shares are devalued, the protocol retains the claim on the underlying assets for potential future recovery.

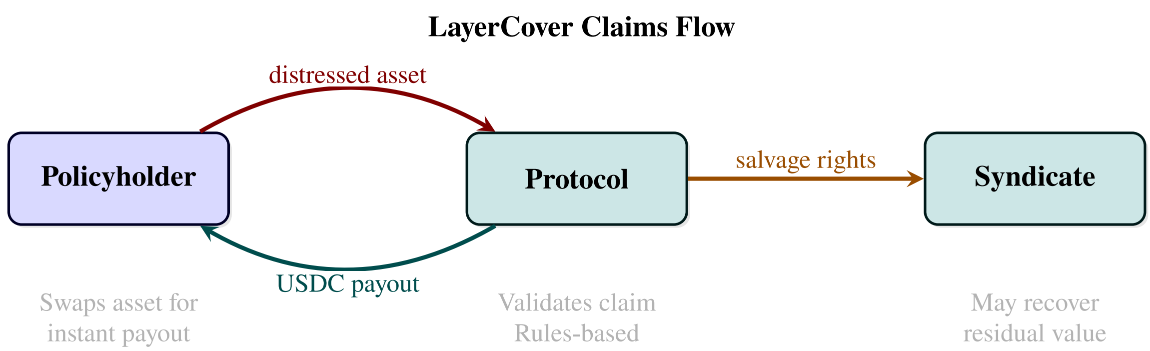

Figure 3: The claim process operates as an asset swap: policyholders transfer distressed assets and receive instant USDC payouts. Syndicates receive salvage rights with potential for future recovery.

6.3.3 Salvage Liquidity and Capital Recycling

Salvage rights are transferable, allowing underwriters to sell distressed exposure instead of waiting for uncertain recovery. This creates a secondary market where:

- liquidity-seeking underwriters can exit quickly at a discount;
- distressed-asset buyers can assume longer-duration recovery risk.

The result is faster capital recycling for active underwriters and clearer risk transfer without off-chain legal subrogation.

6.3.4 Euler Example (March 2023)

The Euler exploit is a practical example of why transferable salvage matters. In that event, a large share of funds was later recovered, but only after a period of uncertainty and temporary illiquidity [3].

Illustrative underwriting path:

- Underwriter principal: \$100k.
- Claim event consumes \$20k of capital.
- Underwriter receives salvage/claim rights with \$20k face value.
- Rights are sold at 20 cents on the dollar (\$4k immediate liquidity).

Metric	**Underwriter (Seller)**	**Distressed Buyer**
Entry value	\$20k claim-right face value	Buys at discount
Execution	Sells at 20% (\$4k cash now)	Pays \$4k for \$20k face
If 90% eventually recovered	Foregoes upside for liquidity	Receives \$18k; high multiple on cost

This transfer is economically useful for both sides: the underwriter regains deployable capital quickly, while the specialist buyer assumes long-duration recovery risk.

7 Fixed-Rate Premium Pricing

LayerCover operates a **100% fixed-rate** pricing model. There is no algorithmic or utilisation-based pricing. All premium rates are set by professional underwriters (Syndicate Managers) who post binding quotes to a transparent on-chain orderbook.

7.1 The Intent-Based Orderbook

All coverage is purchased through the **Intent-Based** model:

1. **Syndicate Managers Post Quotes:** Managers of Syndicate vaults actively set premium rates based on their own risk assessment, market conditions, and portfolio strategy. They sign cryptographically verifiable "Intents" off-chain [11], binding offers to provide a specific amount of coverage at a fixed annualized rate for a fixed duration.
2. **Quotes Appear on Orderbook:** These signed intents are submitted to the protocol's Intent Orderbook, where they become visible and executable by policyholders.
3. **Policyholders Match Quotes:** When purchasing coverage, policyholders select from available quotes. The protocol automatically identifies the best-priced options matching their requirements (pool, duration, amount).
4. **Atomic Execution:** Upon confirmation, the protocol atomically locks the underwriter's capital, transfers the premium, and mints the Policy NFT to the buyer.

7.2 Quote Validity and Anti-Gaming Controls

To preserve market integrity, stale, invalid, or incompatible quote executions must fail safely.

- **Expiry Enforcement:** Each intent includes a hard expiry timestamp. Expired quotes are unfillable and cannot trigger premium transfer or capital lock.
- **Nonce Invalidation:** Makers and takers can invalidate older signed messages by increasing their nonce floor, preventing replay of stale intents/orders.
- **Signature Verification:** Matching requires valid EIP-712 signatures (including contract-signature support), preventing unauthorized quote execution.
- **Compatibility Checks:** Execution enforces pool, duration, and rate compatibility between intent and order, plus optional buyer allowlists and minimum fill constraints.

These controls keep quotes actionable while ensuring invalid or stale matches revert atomically without side effects.

7.3 Pricing Authority and Design Choice

Syndicate managers set quote rates directly (no utilisation curve). This preserves budget certainty for buyers and explicit risk ownership for underwriters. Competition between managers provides price discovery while avoiding curve-gaming around pool capacity.

8 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, pool-level fee settings, and reinsurance/capital controls. Execution of underwriting, loss distribution, and payouts is fully automated on–chain.

8.1 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:

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

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.

8.2 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:** Pool-level payout fee bps and fee-recipient configuration.
- **Rate Controls at Matching:** Underwriters set quote rates, buyers set max acceptable rates, and the matcher enforces compatibility on execution.

Ratings and constraints are updated through governance-controlled administrative actions. Changes to mutex groups or capacity limits affect only new allocations.

8.3 Institutional Risk Alignment

LayerCover controls can be mapped to familiar insurance and banking frameworks:

- pool ratings and risk points approximate risk-weight and concentration controls;
- mutex groups encode explicit correlation constraints;
- deterministic settlement improves loss-timing clarity for capital modelling;
- on-chain state provides auditable data lineage for ERM and reporting.

This supports institutional integration without introducing discretionary claims governance.

8.3.1 Catastrophic Event Metrics (Notation)

To avoid ambiguity between joint and conditional probabilities, this paper reports both:

- **Shortfall probability:** $p_{shortfall} = \mathbb{P}(S)$, where S is the event that pool capital alone is insufficient.
- **Catastrophic conditional probability:** $p_{cat|shortfall} = \mathbb{P}(C \mid S)$, where C is the event that all waterfall layers are exhausted.

- **Joint catastrophic probability:** $p_{cat \cap shortfall} = \mathbb{P}(C \cap S)$.

By definition:

$$\mathbb{P}(C \cap S) = \mathbb{P}(C \mid S)\mathbb{P}(S)$$

This notation separates "how often a shortfall happens" from "how severe shortfalls are when they occur," improving comparability across pools.

8.4 Upgradeability and Trust Model

LayerCover's core contracts are deployed behind **transparent proxy** contracts, allowing the protocol to apply security patches and feature upgrades without requiring users to migrate capital to new addresses.

- **Proxy Architecture:** All core contracts (CapitalPool, PolicyManager, PayoutManager, RiskManager, etc.) use the ERC-1967 transparent proxy pattern. Users interact with a stable proxy address; the underlying implementation can be upgraded by governance.
- **Timelock Protection:** All upgrade operations are routed through a `TimelockController`, enforcing a mandatory delay (e.g. 48 hours) between proposal and execution. This provides the community with a window to review changes and exit if desired.
- **Role-Based Access Control:** Administrative functions are gated by OpenZeppelin `AccessControl` roles. Different actions (pausing, upgrading, parameter changes) require different roles, preventing single-key compromise from affecting the entire protocol.
- **Emergency Pause:** A dedicated `CoverCircuitBreaker` contract can pause new policy issuance for specific pools during active incidents, while preserving existing policyholders' ability to file claims and withdraw.
- **Immutable Parameters:** Certain critical parameters (e.g. fee caps, minimum lock durations) are enforced at the factory level and cannot be changed post-deployment, providing hard guarantees to participants.

Path to Immutability. As the protocol matures and its mechanics are battle-tested, governance may choose to renounce upgrade rights on individual contracts, rendering them fully immutable. This staged approach balances the need for early-stage flexibility with the long-term goal of trustless execution.

8.5 Known Risks and Limitations

LayerCover materially reduces discretionary settlement risk, but several residual risks remain:

- **Oracle and data risk (parametric markets):** UMA-based outcomes depend on assertion quality, challenge participation, and liveness.
- **Extreme correlation risk:** In systemic crises, correlated failures can overwhelm all waterfall layers and force partial payout.
- **Upgrade governance risk:** Proxy-based upgrades introduce trust assumptions around timelock governance and key management.
- **Liquidity timing risk:** Reinsurance and backstop capacity may be temporarily constrained under simultaneous drawdowns.
- **Market liquidity risk for salvage:** Distressed assets can trade at deep discounts or remain illiquid for extended periods.

9 Economic Scenario Analysis

We use a representative pool to show economics under normal and stress conditions.

9.1 Baseline Assumptions

- Pool capital: \$10m (100 underwriters at \$100k each).
- Coverage sold: \$2m (20% utilisation).
- Premium rate: 10% annualised (\$200k gross premium).
- Backstop share: 20% of premium.
- Reinsurance: \$500k external layer.

9.2 Worked Base Case

If annual claims are \$300k and salvage recovery is \$120k, then per underwriter:

- premium income (net of backstop): +\$1,600;
- yield income (4% on \$100k): +\$4,000;
- claim loss share: $-\$3,000$;
- salvage share: +\$1,200.

Net result: **+\$3,800**, ending value **\$103,800**.

9.3 Stress Summary

Regime	Claims	Waterfall Usage	Indicative Per-UW Net	Coverage Fulfilment
Normal	\$0.3m	Pool capital only	+\$3.8k	100%
Contagion	\$2.0m	Pool + reinsurance	$-\$6.4k$	100%
Systemic collapse	\$14.0m	All layers exhausted	$-\$87.4k$	85.7%

Catastrophic Coverage Metric.

$$\text{Coverage Fulfilment Ratio} = \frac{\text{claims paid}}{\text{claims requested}}, \quad p_{cat \cap shortfall} = \mathbb{P}(C \cap S), \quad p_{cat|shortfall} = \mathbb{P}(C \mid S)$$

Reporting both conditional and joint catastrophic probabilities avoids misranking pools with different baseline shortfall frequencies.

10 Glossary of Key Terms

Active Pledge (P^{active}) Capital currently backing coverage in a pool.
Backstop Pool Protocol-native reserve used when primary pool and reinsurance capacity are insufficient.
Coverage Fulfilment Ratio

$$\frac{\text{claims paid}}{\text{claims requested}}$$

Cooldown Period A delay before new or increased coverage becomes active.
Effective Shares (EffShares) Circulating shares used for NAV calculations:

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

Loss Index ($D_i^{(\mathbf{sh})}$) Per-pool shares-per-pledge index for realized claim losses.
NAV (Net Asset Value) Total value of pool assets in underlying token units.
Policy NFT Transferable token representing fixed-term coverage and claim rights.
Salvage Rights Entitlements to insured assets transferred during claims.
Shortfall / Catastrophic Probabilities

$$p_{shortfall} = \mathbb{P}(S), \quad p_{cat|shortfall} = \mathbb{P}(C \mid S), \quad p_{cat \cap shortfall} = \mathbb{P}(C \cap S)$$

References

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

[2] UMA Protocol, "Optimistic Oracle V3: Specification and Design," 2023. https://docs.uma.xyz

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

[4] Chainalysis, "Crypto Crime Report," annual editions 2021–2024. https://blog.chainalysis.com/reports

[5] DefiLlama, "Hacks Dashboard," ongoing. https://defillama.com/hacks

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

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

[8] Basel Committee on Banking Supervision, "Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems," Bank for International Settlements, 2011 (rev. 2017). https://www.bis.org/bcbs/basel3.htm

[9] 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

[10] Ethereum Improvement Proposals, "EIP-4626: Tokenized Vaults," 2022. https://eips.ethereum.org/EIPS/eip-4626

[11] Ethereum Improvement Proposals, "EIP-712: Typed Structured Data Hashing and Signing," 2017. https://eips.ethereum.org/EIPS/eip-712

11 Appendix A: Mathematical Specifications

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

11.1 A.1 Fixed-Rate Premium Pricing

11.1.1 Premium Cost Calculation

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

$$P_{intent} = \frac{C \cdot r_{fixed} \cdot T}{365 \times 10000} \tag{11.1}$$

Where:

- C: Coverage amount in underlying units (e.g. USDC)
- r_{fixed}: The annualized rate in basis points, locked at purchase
- T: Policy duration in days

11.1.2 Example Calculation

For a policy with \$100,000 coverage at 500 bps (5%) for 90 days:

$$P_{intent} = \frac{100{,}000 \cdot 500 \cdot 90}{365 \times 10000} = \$1{,}232.88 \tag{11.2}$$

11.2 A.2 Core Accounting Price Neutrality

11.2.1 Share Conversion

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

$$\text{EffShares} = \text{TotalShares} - \text{unsettledPayoutShares} \tag{11.3}$$

$$\text{valueToShares}(V) = \begin{cases} V & \text{if } NAV = 0 \text{ or EffShares} = 0 \\ \lfloor \frac{V \cdot \text{EffShares}}{NAV} \rfloor & \text{otherwise} \end{cases} \tag{11.4}$$

11.3 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 $D^{(sh)}$.

11.3.1 Global Index Update

On a realized loss L (in underlying units):

$$\text{lossShares} = \text{valueToShares}(L) \tag{11.5}$$

$$D_i^{(sh)} \leftarrow D_i^{(sh)} + \frac{\text{lossShares} \cdot \text{PRECISION}}{\text{totalPledged}_i} \tag{11.6}$$

11.3.2 Underwriter Settlement

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

$$\text{PendingLossShares}_{u,i} = \max\left(0, \frac{P_{u,i}^{active} \cdot \Delta D_i^{(sh)}}{\text{PRECISION}}\right) \tag{11.7}$$

These shares are burned to settle the liability:

$$\text{burn}(\text{PendingLossShares}_{u,i}) \tag{11.8}$$

11.4 A.4 Reward Distribution Indexing

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

$$R_{i,\tau} \leftarrow R_{i,\tau} + \frac{Q \cdot \text{PRECISION}}{\text{totalPledged}_i} \tag{11.9}$$

The claimable reward for underwriter u is:

$$\text{PendingReward}_{u,i,\tau} = \max\left(0, \left\lfloor \frac{P_{u,i}^{active} \cdot R_{i,\tau}}{\text{PRECISION}} \right\rfloor - d_{u,i,\tau}\right) \tag{11.10}$$

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

11.5 A.5 Premium Routing Invariants

Let total premium be P_{total}, backstop share parameter $\alpha \in [0,1]$, and optional incentive redirect parameter $\delta \in [0, \delta_{max}]$.

$$P_{backstop} = \alpha P_{total}, \qquad P_{underwriter}^{gross} = (1-\alpha)P_{total} \tag{11.11}$$

$$P_{incentive} = \delta P_{underwriter}^{gross}, \qquad P_{underwriter}^{net} = (1-\delta)P_{underwriter}^{gross} \tag{11.12}$$

$$P_{total} = P_{backstop} + P_{underwriter}^{net} + P_{incentive} \tag{11.13}$$

Therefore premium conservation holds exactly for all valid (α, δ).

11.6 A.6 Quote-Failure Compensation Bound

For a failed executable quote with quoted premium P_{quoted}, compensation is bounded by:

$$C_q \leq \min(C_{max}, \rho \cdot P_{quoted}) \tag{11.14}$$

with governance parameters $C_{max} \geq 0$ and $\rho \in [0,1]$.

Operational constraints:

- Compensation is valid only for maker-attributable failure.
- One signed intent can produce at most one compensation event.
- Claims must satisfy a bounded submission window.