JELLEO | AUTONOMOUS SOLANA AUDIT

AUDIT REPORT · CYCLE 20260506-225557-5059332

Hunt cycle · percolator-live.

AUDITOR	Kirill Sakharuk · kirill@jelleo.com
CUSTOMER	percolator-live
WINDOW	cycle 20260506-225557-5059332
CYCLE	20260506-225557-5059332
ENGINE SHA	5059332
WRAPPER SHA	04b854e571
GENERATED	2026-05-08T22:33:06+00:00

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

CONFIRMED · DISCLOSED · FIXED · VERIFIED

49 REJECTED (FALSE POSITIVE)

SIGNED · ED25519

MCowBQYDK2VwAyEAvCFSLBecPuNClei48PWjHuelHlBX9uYZo4wELbQ7b+k=

verify with `audit-pipeline sign verify <file> <file>.sig --pubkey jelleo.ed25519.pub`
public key at
https://jelleo.com/keys/jelleo.ed25519.pub

PLATFORM · V0.1

JELLEO · The underwriting layer for Solana DeFi.

Methodology	jelleo.com/methodology.html
Disclosure	jelleo.com/security.html
Source	github.com/Copenhagen0x/audit-pipeline-cli

Apache-2.0 · contact security@jelleo.com

percolator-live · hunt cycle

`20260506-225557-5059332` · started 2026-05-06T22:55:57+00:00 · engine `5059332` · wrapper `04b854e571`

01 — CYCLE SUMMARY

CRITICAL	HIGH	MEDIUM	CONFIRMED
11	22	13	0

TOTAL VERDICTS: 49

Critical 11 · High 22 · Medium 13 · Low 3 · Info 0

02 — FINDINGS

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
CRITICAL	`P1-pnl-zero-sum`	Across all accounts in a market, sum(positive PnL) - sum(negative PnL) equals zero up to fees and funding payments. No P	UNKNOWN / UNKNOWN	REJECTED	—
CRITICAL	`V1-vault-residual-conservation`	The post-haircut residual cash (vault - cash_locked_in_orderbook - claimable_pnl - insurance_counter) is conserved acros	UNKNOWN / UNKNOWN	REJECTED	—
CRITICAL	`V7-insurance-counter-vault-coupling`	Every code path that mutates `insurance_fund.balance` is paired with an equal-magnitude mutation of `vault` in the same	FALSE / MED	REJECTED	—
CRITICAL	`A1-permissionless-no-drain`	Every public/permissionless instruction either requires a privileged signer OR provably cannot reduce vault below cash_l	UNKNOWN / UNKNOWN	REJECTED	—
CRITICAL	`A2-admin-instructions-signer-check`	Every admin-only instruction (pause, set-fee, set-cap, etc.) verifies the admin signer via Solana's signer flag, NOT jus	FALSE / HIGH	REJECTED	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
CRITICAL	`CI1-deposit-then-withdraw-zero`	Deposit X immediately followed by withdraw X (with no intervening activity) leaves vault + account-state byte-identical	FALSE / MED	REJECTED	—
CRITICAL	`CI5-cross-market-isolation`	State changes in market A cannot affect accounts or vault in market B. Markets are fully isolated.	UNKNOWN / UNKNOWN	REJECTED	—
CRITICAL	`IX6-account-owner-check`	Every account read by the program verifies the account's `owner` field matches the expected program_id, preventing fake-	FALSE / HIGH	REJECTED	—
CRITICAL	`L2-liquidation-only-on-mm-breach`	A liquidation can only successfully execute when the target account's MM is genuinely breached at the moment of executio	UNKNOWN / UNKNOWN	REJECTED	—
CRITICAL	`L4-keeper-authorization-surface`	Every public/permissionless instruction that reaches use_insurance_buffer requires either an admin signer OR cannot drai	UNKNOWN / UNKNOWN	REJECTED	—
CRITICAL	`O2-oi-conservation`	Open interest (sum of |position_q| across all longs == sum across shorts) is conserved by every fill. Long OI == Short O	UNKNOWN / HIGH	REJECTED	—
HIGH	`P4-funding-rate-mark-bias`	The funding rate captured by every instruction is computed BEFORE any mark_ewma_e6 / last_effective_price_e6 mutation in	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`P9-pnl-arithmetic-bounds`	The lazy mark-to-market computation pnl_delta = abs_basis * (K_now - K_snap) / (a_basis * POS_SCALE) cannot overflow i12	FALSE / MED	REJECTED	—
HIGH	`S1-init-state-invariants`	The post-init state of a market (vault, c_tot, insurance_fund.balance, pnl_pos_tot, pnl_matured_pos_tot, all OI counters	UNKNOWN / MED	REJECTED	—
HIGH	`S3-settle-after-close`	`settle_after_close` correctly distributes final residual to each account proportional to its claim, respecting the hair	UNKNOWN / UNKNOWN	REJECTED	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
HIGH	`S4-touch-account-live-pairing`	Every public instruction that advances the engine's market clock (accrue_market_to / accrue_market_to_chunked) is paired	FALSE / MED	REJECTED	—
HIGH	`V3-vault-monotonic-on-deposit`	User-initiated deposits monotonically increase vault balance by exactly the deposited amount, with no off-by-one credit	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`A10-upgrade-authority-frozen`	The program's upgrade authority is either set to a known multisig or explicitly burned — never left as a single-key dev	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`A3-cpi-safety`	Any cross-program invocation invoked from within an instruction either (a) targets a fixed pubkey hardcoded in the progr	FALSE / HIGH	REJECTED	—
HIGH	`A6-account-discriminator-check`	Every parsed account verifies its discriminator (account-type tag) before reading typed fields, preventing type confusio	FALSE / HIGH	REJECTED	—
HIGH	`AC4-free-only-on-zero-position`	free_slot / reclaim_empty_account refuses to free an account whose position_q != 0 or whose claimable_pnl != 0, preventi	FALSE / HIGH	REJECTED	—
HIGH	`AC5-account-capital-conservation`	Sum of all materialized accounts' (capital + claimable_pnl) plus vault residual equals total deposits minus total withdr	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`AC6-slot-reuse-no-aliasing`	A reused slot index cannot alias to two live accounts simultaneously. Materialize_at on an already-live slot is rejected	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`AR1-mul-div-floor-no-overflow`	Every callsite of mul_div_floor_u128 either uses bounded inputs that provably cannot overflow, or invokes the wide_mul_d	FALSE / HIGH	REJECTED	—
HIGH	`AR2-pnl-delta-i128-bound`	pnl_delta computed via abs_basis × ΔK / (a_basis × POS_SCALE) is provably bounded by 2^126 across any K-walk reachable t	FALSE / HIGH	REJECTED	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
HIGH	`AR8-rounding-direction`	Every rounding decision (floor/ceil/round-half-even) is set in the direction that does NOT favor the user against the pr	FALSE / HIGH	REJECTED	—
HIGH	`CI3-fill-then-cancel-impossible`	Once a maker order is filled (even partially), the filled portion cannot be canceled. Cancel only affects unfilled remai	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`IX7-readonly-vs-writable-correctness`	Every account in an instruction's accounts array is marked writable iff the program will mutate it, preventing transacti	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`L1-liquidation-discount-bounded`	Liquidation bonus paid to a liquidator cannot exceed the configured LIQUIDATION_INCENTIVE_PCT of seized collateral, even	FALSE / HIGH	REJECTED	—
HIGH	`L3-keeper-crank-cursor-budget`	The keeper crank's price-move consumption budget is not reset until every account in the swept window has actually been	FALSE / HIGH	REJECTED	—
HIGH	`L5-liquidation-no-fee-enrichment`	Liquidation does not transfer collateral to the liquidator beyond the configured incentive percentage + protocol-defined	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`L8-partial-liquidation-correctness`	Partial liquidation correctly reduces position_q + claims proportional to seized collateral. Resulting account state sti	FALSE / HIGH	REJECTED	—
HIGH	`O5-mm-trigger-correctness`	Maintenance-margin (MM) breach correctly triggers liquidation eligibility, and once flagged, the account cannot grow pos	UNKNOWN / UNKNOWN	REJECTED	—
MEDIUM	`P10-funding-index-monotonic-modulo-direction`	Cumulative funding index changes monotonically within a continuous funding-rate sign window; flips only on rate-sign cha	UNKNOWN / UNKNOWN	REJECTED	—
MEDIUM	`P6-mark-ewma-bound`	`mark_ewma_e6` cannot grow unbounded; bounded by configured EWMA half-life × max single-trade price impact.	UNKNOWN / UNKNOWN	REJECTED	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
MEDIUM	`R1-reorg-resilience`	A finalized state cannot be silently rewritten by a Solana reorg. Any reorg-affected state is either re-derivable or exp	FALSE / HIGH	REJECTED	—
MEDIUM	`S10-rebate-claim-correctness`	Rebate claims pay exactly the accumulated rebate balance and atomically zero the per-account rebate counter.	FALSE / HIGH	REJECTED	—
MEDIUM	`S9-cancel-correctness`	Cancel-order instructions correctly unlock cash_locked back into vault and zero the order's slot.	UNKNOWN / UNKNOWN	REJECTED	—
MEDIUM	`V9-rebate-accumulation-bounded`	Maker-rebate accumulation across all accounts is bounded by the configured rebate-rate × cumulative volume; never exceed	FALSE / HIGH	REJECTED	—
MEDIUM	`A8-multisig-threshold`	If a multisig is used, threshold is enforced atomically and cannot be partially bypassed by replaying signatures.	FALSE / HIGH	REJECTED	—
MEDIUM	`AR5-fee-calc-overflow`	Fee calculation (size × fee_rate / FEE_SCALE) cannot overflow under MAX_POSITION_ABS_Q × MAX_PRICE bounds.	FALSE / HIGH	REJECTED	—
MEDIUM	`AR6-square-root-bounds`	Any sqrt-based computation (e.g., for vega-style adjustments) is bounded and never produces NaN-equivalents on integer a	FALSE / HIGH	REJECTED	—
MEDIUM	`AR7-saturating-arithmetic-correctness`	Where the codebase uses saturating arithmetic, the saturation point is the documented protocol cap, not a primitive type	UNKNOWN / UNKNOWN	REJECTED	—
MEDIUM	`IX3-rent-exemption-check`	Every account allocated by the program is rent-exempt, with sysvar rent verified at allocation time.	UNKNOWN / UNKNOWN	REJECTED	—
MEDIUM	`IX4-clock-sysvar-required`	Every instruction that consumes a timestamp uses the Solana clock sysvar (not a user-supplied value).	UNKNOWN / UNKNOWN	REJECTED	—
MEDIUM	`L9-cascade-liquidation-bound`	A single instruction cannot trigger more than the configured cascade bound of liquidations (preventing griefing via long	FALSE / HIGH	REJECTED	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
LOW	`R3-finality-gate`	Settlement-class operations only consider state from finalized slots, never from confirmed-but-unfinalized state.	FALSE / HIGH	REJECTED	—
LOW	`R5-rpc-staleness-tolerance`	Off-chain components reading state via RPC tolerate up to N slots of staleness without acting on stale information.	UNKNOWN / UNKNOWN	REJECTED	—
LOW	`IX9-compute-budget-respect`	Every instruction completes within the configured compute budget; no instruction is denial-of-service-able by adversaria	UNKNOWN / UNKNOWN	REJECTED	—

A — SEVERITY RUBRIC

TIER	DEFINITION
CRITICAL	Direct loss of user funds or full protocol takeover with no meaningful preconditions. Reachable from a permissionless instruction by any signer. Must be patched immediately.
HIGH	Significant loss of user funds or protocol invariant violation under realistic preconditions (specific market state, signer with limited but obtainable role). Patch should ship in next release.
MEDIUM	Hardening issue, partial loss possible, or invariant violation requiring privileged signer or improbable state. Worth fixing in normal cadence.
LOW	Minor issue with no plausible path to fund loss. Code-quality or defense-in-depth concern.
INFO	Informational. No security impact. Documentation or style suggestion.

B — METHODOLOGY

This cycle was produced by Jelleo's continuous, hypothesis-driven Solana audit loop. Every finding originates as a falsifiable invariant claim from a per-protocol hypothesis library, dispatched to multi-agent recon (Layer 1), promoted on contested verdicts via adversarial debate (Layer 1.5), and confirmed empirically via a `cargo test` proof-of-concept (Layer 2) before transitioning to `confirmed`. Confirmed findings auto-fire structural sibling derivation and cross-protocol propagation hooks, then move through a restricted lifecycle (`new → triaged → confirmed → disclosed → fixed → verified`). Every cycle is signed Ed25519 against the platform key — see the cover-page receipt.

Full spec: docs/methodology/ (eleven sections, §01–§10) · Live reference: jelleo.com/methodology.html · Inaugural disclosure: aeyakovenko/percolator-prog#39 (F7, 2026-04)