JELLEO | AUTONOMOUS SOLANA AUDIT

AUDIT REPORT · CYCLE 20260508-025038

Hunt cycle · percolator-live.

AUDITOR	Kirill Sakharuk · kirill@jelleo.com
CUSTOMER	percolator-live
WINDOW	cycle 20260508-025038
CYCLE	20260508-025038
ENGINE SHA	3c9c84908b
WRAPPER SHA	04b854e571
GENERATED	2026-05-08T22:33:25+00:00

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

CONFIRMED · DISCLOSED · FIXED · VERIFIED

35 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

`20260508-025038` · started 2026-05-08T02:50:38+00:00 · engine `3c9c84908b` · wrapper `04b854e571`

01 — CYCLE SUMMARY

CRITICAL	HIGH	MEDIUM	CONFIRMED
7	15	9	0

TOTAL VERDICTS: 35

Critical 7 · High 15 · Medium 9 · Low 4 · Info 0

02 — FINDINGS

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
CRITICAL	`V1-vault-residual-conservation`	The post-haircut residual cash (vault - cash_locked_in_orderbook - claimable_pnl - insurance_counter) is conserved acros	FALSE / HIGH	REJECTED	—
CRITICAL	`V10-claimable-pnl-conservation`	Sum of claimable_pnl across all account materializations equals the engine-tracked `pnl_pos_tot - pnl_neg_tot` for the m	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	—
CRITICAL	`CI1-deposit-then-withdraw-zero`	Deposit X immediately followed by withdraw X (with no intervening activity) leaves vault + account-state byte-identical	FALSE / HIGH	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-	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	FALSE / MED	REJECTED	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
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 / UNKNOWN	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	—
HIGH	`S7-epoch-staleness-gate`	Risk gates that depend on per-epoch state (e.g., funding-window mark) reject when the captured epoch is stale relative t	FALSE / HIGH	REJECTED	—
HIGH	`V4-vault-cap-respect`	Vault balance is provably bounded by MAX_VAULT_TVL across every reachable state. No accounting helper can push vault pas	FALSE / HIGH	REJECTED	—
HIGH	`V6-insurance-floor`	Insurance fund balance is monotonically non-decreasing across user-only activity (deposits, withdraws, fills) and only d	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`V8-cash-locked-conservation`	`cash_locked_in_orderbook` equals the sum of all unfilled order sizes times their respective limit prices, for every mar	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	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	`CI7-wrapper-instruction-equivalence`	Calling an engine function via the BPF wrapper produces equivalent state changes to calling the engine function directly	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	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
HIGH	`IX8-replay-protection`	No instruction can be replayed within the same market state to double-credit a user (e.g., via signer-replay or stale-st	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	UNKNOWN / UNKNOWN	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	—
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	`S6-time-monotonic`	Market clock time is monotonically non-decreasing. No instruction can rewind the clock.	UNKNOWN / UNKNOWN	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	`AR3-funding-rate-bounds`	Computed funding rate is bounded by configured |max_funding_rate| across all reachable mark/index states.	UNKNOWN / UNKNOWN	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	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
MEDIUM	`AR7-saturating-arithmetic-correctness`	Where the codebase uses saturating arithmetic, the saturation point is the documented protocol cap, not a primitive type	FALSE / HIGH	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	`O10-orderbook-side-balance`	Total bid-side cash locked equals sum of (size × price) for all open bids; analogous for asks. Cannot be drained by help	UNKNOWN / UNKNOWN	REJECTED	—
LOW	`R3-finality-gate`	Settlement-class operations only consider state from finalized slots, never from confirmed-but-unfinalized state.	FALSE / HIGH	REJECTED	—
LOW	`R4-leader-rotation-safety`	Leader rotation between two adjacent slots cannot expose a transient state where invariants fail.	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.	FALSE / HIGH	REJECTED	—
LOW	`IX10-error-codes-distinct`	Every distinct failure mode returns a distinct error code, so off-chain monitoring can disambiguate without log parsing.	FALSE / HIGH	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)