JELLEO | AUTONOMOUS SOLANA AUDIT

AUDIT REPORT · CYCLE 20260506-234757-04B854E

Hunt cycle · percolator-wrapper-live.

AUDITOR	Kirill Sakharuk · kirill@jelleo.com
CUSTOMER	percolator-wrapper-live
WINDOW	cycle 20260506-234757-04b854e
CYCLE	20260506-234757-04b854e
ENGINE SHA	04b854e
WRAPPER SHA	04b854e571
GENERATED	2026-05-08T22:33:09+00:00

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

CONFIRMED · DISCLOSED · FIXED · VERIFIED

52 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-wrapper-live · hunt cycle

`20260506-234757-04b854e` · started 2026-05-06T23:47:57+00:00 · engine `04b854e` · wrapper `04b854e571`

01 — CYCLE SUMMARY

CRITICAL	HIGH	MEDIUM	CONFIRMED
8	28	13	0

TOTAL VERDICTS: 52

Critical 8 · High 28 · Medium 13 · Low 3 · Info 0

02 — FINDINGS

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
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	—
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	`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 / MED	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	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
CRITICAL	V2-vault-balance-equation	For every market state transition, the change in vault balance equals the sum of (cash deposited into orderbook + claima	UNKNOWN / UNKNOWN	REJECTED	—
CRITICAL	V5-haircut-direction	The haircut (positive-PnL claim cap) only ever shrinks claimable PnL, never increases the residual cash that other claim	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	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	A5-pda-derivation-canonicality	Every PDA used as a vault or authority is derived with canonical seeds and the result is checked against the passed-in a	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	A7-wrapper-instruction-signer-routing	The BPF wrapper's instruction dispatch correctly routes signer privileges from the outermost transaction to the inner en	FALSE / MED	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	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	FALSE / HIGH	REJECTED	—
HIGH	AC7-account-bound-authority	An account's bound authority is set at materialize time and cannot be silently changed without explicit ownership-transf	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	UNKNOWN / UNKNOWN	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	UNKNOWN / UNKNOWN	REJECTED	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
HIGH	`AR4-catchup-no-overflow`	The accrue_market_to_chunked catch-up math cannot overflow when replaying a long staleness window, even with adversarial	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`CI4-self-trade-net-zero`	Self-trade (same authority on both sides) net-changes vault by exactly zero up to fees. No fund extraction via self-trad	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`CI6-batch-instruction-atomicity`	A batched instruction (e.g., place-and-cancel, deposit-and-fill) either succeeds atomically or rolls back fully. No part	UNKNOWN / UNKNOWN	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	`CI8-flash-fill-impossible`	A "flash fill" — open + close + withdraw within a single instruction — cannot extract more than the user's pre-instructi	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	`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	`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	FALSE / HIGH	REJECTED	—
HIGH	`L6-force-closure-conditions`	Force closure of a position can only occur under exactly the conditions enumerated in spec.md (MM breach, market-pause,	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`O1-position-q-bound`	Every account's |position_q| is bounded by MAX_POSITION_ABS_Q across every reachable state, including immediately after	UNKNOWN / UNKNOWN	REJECTED	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
HIGH	`O3-position-authority-binding`	An account's `position_q` and `claimable_pnl` can only be mutated when the account's bound authority signs (or via permi	UNKNOWN / UNKNOWN	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	—
HIGH	`O8-cross-margin-equity`	Cross-margin equity calculation is correct under partial liquidation, partial fills, and combined PnL realizations withi	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`P7-pnl-on-side-flip`	When an account flips side (long → short or vice versa), the realized PnL on the closing portion is correctly debited/cr	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`S2-resolved-mode-mature-claim`	Once a market enters Resolved mode, no further accrual of claimable_pnl is possible against the residual; only existing	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	`S4-touch-account-live-pairing`	Every public instruction that advances the engine's market clock (accrue_market_to / accrue_market_to_chunked) is paired	UNKNOWN / UNKNOWN	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 / MED	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	FALSE / HIGH	REJECTED	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
MEDIUM	`A8-multisig-threshold`	If a multisig is used, threshold is enforced atomically and cannot be partially bypassed by replaying signatures.	UNKNOWN / UNKNOWN	REJECTED	—
MEDIUM	`A9-pause-gate-coverage`	When the protocol is paused, every state-mutating instruction checks the pause flag and rejects. No instruction has a pa	UNKNOWN / UNKNOWN	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.	UNKNOWN / UNKNOWN	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	`IX3-rent-exemption-check`	Every account allocated by the program is rent-exempt, with sysvar rent verified at allocation time.	FALSE / HIGH	REJECTED	—
MEDIUM	`IX4-clock-sysvar-required`	Every instruction that consumes a timestamp uses the Solana clock sysvar (not a user-supplied value).	FALSE / HIGH	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	—
MEDIUM	`O7-position-zero-clears-basis`	When position_q reaches exactly 0, basis-related fields are zeroed atomically; subsequent fills don't inherit stale basi	UNKNOWN / UNKNOWN	REJECTED	—
MEDIUM	`O9-position-bedge-correct`	The "bedge" (basis-edge) accounting on partial closes correctly apportions realized PnL between the closed and remaining	UNKNOWN / UNKNOWN	REJECTED	—
MEDIUM	`S5-market-mode-transitions`	Market mode transitions (Active → Halted → Resolved) are one-way and irreversible without admin signer.	FALSE / HIGH	REJECTED	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
MEDIUM	`S6-time-monotonic`	Market clock time is monotonically non-decreasing. No instruction can rewind the clock.	UNKNOWN / UNKNOWN	REJECTED	—
MEDIUM	`S9-cancel-correctness`	Cancel-order instructions correctly unlock cash_locked back into vault and zero the order's slot.	UNKNOWN / UNKNOWN	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 / MED	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	—
LOW	`R3-finality-gate`	Settlement-class operations only consider state from finalized slots, never from confirmed-but-unfinalized state.	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)
