JELLEO | AUTONOMOUS SOLANA AUDIT

AUDIT REPORT · CYCLE 20260506-194213-5059332

Hunt cycle · percolator-live.

AUDITOR	Kirill Sakharuk · kirill@jelleo.com
CUSTOMER	percolator-live
WINDOW	cycle 20260506-194213-5059332
CYCLE	20260506-194213-5059332
ENGINE SHA	5059332
WRAPPER SHA	04b854e571
GENERATED	2026-05-08T22:33:00+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

`20260506-194213-5059332` · started 2026-05-06T19:42:13+00:00 · engine `5059332` · wrapper `04b854e571`

01 — CYCLE SUMMARY

CRITICAL	HIGH	MEDIUM	CONFIRMED
4	18	9	0

TOTAL VERDICTS: 35

Critical 4 · High 18 · Medium 9 · Low 4 · Info 0

02 — FINDINGS

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
CRITICAL	`CI5-cross-market-isolation`	State changes in market A cannot affect accounts or vault in market B. Markets are fully isolated.	UNKNOWN / 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	FALSE / HIGH	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 / UNKNOWN	REJECTED	—
CRITICAL	`P5-funding-payment-zero-sum`	Funding payments are zero-sum across long and short positions. Total paid by longs equals total received by shorts (or v	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	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
HIGH	`IX1-ix-data-validation`	Every instruction validates the length and shape of `instruction_data` before reading typed fields. No out-of-bounds rea	UNKNOWN / UNKNOWN	REJECTED	—
HIGH	`IX2-account-list-length-check`	Every instruction enforces the expected number of accounts in the `accounts` array before indexing.	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	`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	`O1-position-q-bound`	Every account's |position_q| is bounded by MAX_POSITION_ABS_Q across every reachable state, including immediately after	FALSE / HIGH	REJECTED	—
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	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
HIGH	`P3-pnl-matured-bound`	`pnl_matured_pos_tot ≤ pnl_pos_tot` at all times. Matured claims are a subset of total claims.	UNKNOWN / UNKNOWN	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	FALSE / HIGH	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	`V3-vault-monotonic-on-deposit`	User-initiated deposits monotonically increase vault balance by exactly the deposited amount, with no off-by-one credit	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	`A6-account-discriminator-check`	Every parsed account verifies its discriminator (account-type tag) before reading typed fields, preventing type confusio	FALSE / HIGH	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	—
MEDIUM	`CI10-resolution-final`	Once a market is resolved and all matured claims are paid, the market account can be safely closed with no residual debt	UNKNOWN / UNKNOWN	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	`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 / HIGH	REJECTED	—

SEVERITY	HYPOTHESIS	TITLE	VERDICT	STATUS	POC
MEDIUM	`P8-self-trade-cash-flow`	A self-trade (same authority on both sides of a fill) is cash-flow neutral up to fees + IM transitions. No fund extracti	UNKNOWN / MED	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	`A9-pause-gate-coverage`	When the protocol is paused, every state-mutating instruction checks the pause flag and rejects. No instruction has a pa	FALSE / HIGH	REJECTED	—
MEDIUM	`AC8-account-zeroing-on-close`	When an account is closed (via reclaim or full settlement), all its persistent fields are zeroed before the slot is mark	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	`AR7-saturating-arithmetic-correctness`	Where the codebase uses saturating arithmetic, the saturation point is the documented protocol cap, not a primitive type	FALSE / MED	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	—
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.	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)