



JITTER PROTOCOL / FINAL FORMAL VERIFICATION REPORT

Jitter Protocol Formal Verification

Arithmetic, solver, conservation, lifecycle, reward, registry, adapter, and mutation evidence

65	38	25	0
CANONICAL FINDINGS	RESOLVED OR REMOVED	ACKNOWLEDGED / CONDITIONAL	OPEN

Report date	2026-08-17
Assessment baseline	64a477bf9ae945ff585f9dd70231945a9a741ea9 plus reviewed working-tree changes
Primary scope	Jitter formal models and direct production proof targets, Move regressions, mutations, and the Jitter finding crosswalk
Classification	Internal Final Security Assessment

Zzyzx Security Review

Contents

01	Executive result and domain status
02	Evidence taxonomy and coverage
03	Direct proofs and protocol models
04	Formal findings and unresolved obligations
05	Mutation adequacy and executable evidence
06	Manual-audit traceability (reference only)
07	Trusted boundaries and reproduction

1. Executive Result

191/191 SHARED SUITE PROOFS	65 JITTER FINDINGS MAPPED	14/14 MUTATIONS DETECTED	10 OPEN PROOF OBLIGATIONS
---------------------------------------	-------------------------------------	------------------------------------	-------------------------------------

Formal conclusion

All canonical proof obligations in the shared verification suite passed and all deliberate mutations were detected. The Jitter-specific crosswalk below covers every assigned canonical finding. Formal success is supporting evidence, not automatic manual closure.

Manual Audit Status Reference

Why it is included: this reference confirms that the formal scope accounts for the complete known Jitter finding population, including acknowledged and deployment-excluded risks. The counts are copied from the separate Manual Security Audit; they are not findings or dispositions produced by Formal Verification.

32 RESOLVED	6 ARCHITECTURE ELIMINATED	25 ACKNOWLEDGED
0 CONDITIONAL / PENDING	0 OPEN	2 DEPLOYMENT EXCLUDED

2. Evidence Taxonomy and Coverage

D - direct proof over a production body or helper.

M - proof over a protocol state-machine model mapped to production behavior.

T - executable Move test, including boundary, attack, lifecycle, or regression cases.

S - structural evidence such as ABI, visibility, package graph, or deployment scans.

E - external or operational boundary outside the local Move proof.

Coverage interpretation

The shared canonical suite contains 191 proof functions across direct production targets and protocol models, with all first-party source modules classified by the coverage inventory. The conclusions in this report rely only on the Jitter-specific evidence matrix.

Soundness policy

Model proofs require an explicit production mapping and are interpreted together with executable tests and mutation checks. A duplicated toy implementation is not accepted as sufficient closure evidence.

3. Direct Proofs and Protocol Models

3.1 Exact solver boundary properties

Solver obligations prove boundedness, feasibility, and threshold tightness for modeled domains.

Formal excerpt: solver_model.move lines 34-61

```

34     high = mid - 1;
35     };
36     i = i + 1;
37     };

```

```

38     low
39 }
40
41 #[spec(prove)]
42 fun exact_in_binary_search_maximality_spec(threshold: u64, high: u64) {
43     requires(threshold <= high);
44     let result = solve_monotone_threshold(threshold, high);
45     ensures(result == threshold);
46     ensures(result <= high);
47     ensures(result == high || result + 1 > threshold);
48 }
49
50 #[spec(prove)]
51 fun exact_in_zero_threshold_spec(high: u64) {
52     let result = solve_monotone_threshold(0, high);
53     ensures(result == 0);
54 }
55
56 #[spec(prove)]
57 fun exact_in_full_threshold_spec(high: u64) {
58     let result = solve_monotone_threshold(high, high);
59     ensures(result == high);
60 }
61

```

3.2 Market ledger conservation

Lifecycle models preserve valid state and total SY conservation across mint, swap, liquidity, maturity, and final-drain transitions.

Formal excerpt: `market_ledger_model.move` lines 63-108

```

63     requires(sy_in > 0 && py_out > 0);
64     requires(state.external_sy >= sy_in);
65     requires(state.py_sy <= std::u128::max_value!() - sy_in);
66     requires(state.user_pt <= std::u128::max_value!() - py_out);
67     requires(state.pt_supply <= std::u128::max_value!() - py_out);
68     requires(state.user_yt <= std::u128::max_value!() - py_out);
69     requires(state.yt_supply <= std::u128::max_value!() - py_out);
70     let before_sy = sy_total(&state);
71
72     state.external_sy = state.external_sy - sy_in;
73     state.py_sy = state.py_sy + sy_in;
74     state.user_pt = state.user_pt + py_out;
75     state.pt_supply = state.pt_supply + py_out;
76     state.user_yt = state.user_yt + py_out;
77     state.yt_supply = state.yt_supply + py_out;
78
79     ensures(valid(&state));
80     ensures(sy_total(&state) == before_sy);
81     ensures(state.pt_supply >= py_out && state.yt_supply >= py_out);
82 }
83
84 #[spec(prove)]
85 fun redeem_paired_py_conserve_ledger_spec(
86     mut state: Ledger,
87     py_in: u128,
88     sy_out: u128,
89 ) {
90     requires(valid(&state));
91     requires(py_in > 0);
92     requires(state.user_pt >= py_in && state.user_yt >= py_in);
93     requires(state.pt_supply >= py_in && state.yt_supply >= py_in);
94     requires(state.py_sy >= sy_out);
95     requires(state.external_sy <= std::u128::max_value!() - sy_out);
96     let before_sy = sy_total(&state);
97
98     state.user_pt = state.user_pt - py_in;

```

```

99     state.pt_supply = state.pt_supply - py_in;
100    state.user_yt = state.user_yt - py_in;
101    state.yt_supply = state.yt_supply - py_in;
102    state.py_sy = state.py_sy - sy_out;
103    state.external_sy = state.external_sy + sy_out;
104
105    ensures(valid(&state));
106    ensures(sy_total(&state) == before_sy);
107 }
108

```

3.3 Calendar reward lot conservation

Funding-lot models prove funded-total conservation, scheduled-to-allocated transitions, no-exposure behavior, closure, and bounded claim settlement.

Formal excerpt: `coin_reward_lot_model.move` lines 88-121

```

88 }
89
90 #[spec(prove)]
91 fun checkpoint_with_exposure_preserves_hard_cap_spec(
92     state: RewardVault,
93     newly_vested: u128,
94 ) {
95     requires(valid(&state));
96     requires(!state.closed);
97     requires(state.scheduled >= newly_vested);
98     requires(state.allocated <= std::u128::max_value!() - newly_vested);
99     let total = funded_total(&state);
100    let next = checkpoint(state, newly_vested, true);
101    ensures(valid(&next));
102    ensures(funded_total(&next) == total);
103    ensures(next.allocated == state.allocated + newly_vested);
104 }
105
106 #[spec(prove)]
107 fun checkpoint_without_exposure_cannot_backpay_future_users_spec(
108     state: RewardVault,
109     newly_vested: u128,
110 ) {
111     requires(valid(&state));
112     requires(!state.closed);
113     requires(state.scheduled >= newly_vested);
114     requires(state.undistributed <= std::u128::max_value!() - newly_vested);
115     let allocated = state.allocated;
116     let next = checkpoint(state, newly_vested, false);
117     ensures(valid(&next));
118     ensures(next.allocated == allocated);
119     ensures(next.undistributed == state.undistributed + newly_vested);
120 }
121

```

4. Formal Findings and Unresolved Obligations

FV-01 - PY index interest intermediate domain is not closed

Severity: Medium. Status: Acknowledged. Extreme but representable amount and index combinations may require more than 256 bits in an intermediate even if the final result fits u128. The project will not enable an uncalibrated guard because it could block legitimate growth or settlement; deployment is limited to the tested domain with monitoring and an upgrade path.

FV-02 - Model proofs are not direct bytecode proofs

Severity: Informational. Model-to-production mapping remains a trusted boundary for ordering, rounding, object ownership, and edge behavior.

FV-03 - Transcendental and complete solver call graphs retain a proof frontier

Severity: Informational. Full indexed-quote zero-edge bodies, production log2 and ln, and full-domain sqrt_u256 are not yet symbolically closed.

FV-04 - Toolchain and specification completeness are trusted boundaries

Severity: Informational. Results depend on the Move-to-Boogie translation, Boogie, Z3, local patches, and the specification expressing the intended property.

Ten unresolved symbolic obligations

#	OBLIGATION	CURRENT EVIDENCE	RESIDUAL
1-4	Indexed quote zero-edge bodies A-D	Move boundary regressions	Edge abort and output behavior
5	Production log2_u64	Dense and boundary tests	Monotonicity, floor, overflow
6	Production log2_u128	Dense and boundary tests	Monotonicity, floor, overflow
7-8	Power-of-two log2 specifications	Exact-vector tests	Exact boundary result
9	Production ln_u64	Golden vectors	Approximation and domain
10	Full-domain sqrt_u256	Bounded direct proofs	Maximum-width convergence

Proof-frontier status

These are coverage gaps, not confirmed vulnerabilities. A gap becomes a release blocker when production parameters can reach the unproven domain.

5. Mutation Adequacy and Executable Evidence

All 14 deliberate mutations were detected. Jitter-relevant mutations target full-width arithmetic, Q64 rounding, exp2 scale, exact-in and exact-out search, reserve-fee remainder, reward backpay, registry reverse indices, adapter conversion direction, and final user-fund preservation.

Executable evidence

Companion Move tests cover large-input and near-drain AMM behavior, exact-in and exact-out rounding, multi-user add and remove liquidity, final LP drain, maturity lifecycle, PT and YT redemption, interest and treasury accounting, parallel reward lots, rate changes, point remainders, adapter conversion boundaries, and withdrawal queue conservation.

6. Manual Audit Traceability Matrix

Why this matrix appears in a Formal Verification report

This is not a second manual assessment. It maps every manual-audit finding to the proof, model, executable test, structural evidence, or trusted boundary that addresses it. This prevents the formal program from proving convenient properties while omitting security-relevant findings. The MANUAL STATUS* column is copied from the Manual Security Audit for reference only. A passing proof cannot reduce severity, close a finding, or change its disposition; only the Manual Security Audit may do so after the production root cause and residual risk are reviewed.

All 65 Jitter canonical findings are mapped below for completeness and evidence traceability. *Manual status is quoted from the separate Jitter Manual Security Audit and is not a formal-verification conclusion.

Oracle and Adapter Findings

ID	MANUAL STATUS*	EVIDENCE	FORMAL COVERAGE / RESIDUAL
ORC-01	Deployment Excluded	S/T	Structural and test evidence supports deployment exclusion; no production guarantee is claimed.
ORC-02	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
ORC-03	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
ORC-04	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
ORC-05	Acknowledged	M/T/E	External or operational assumptions remain trusted boundaries.
ORC-06	Acknowledged	M/T/E	Ember is not deployed. The project acknowledges the current integration state and will add an authoritative upstream timestamp plus production-ABI freshness tests before activation.
ORC-07	Acknowledged	T/E	External or operational assumptions remain trusted boundaries.
ORC-08	Acknowledged	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
ORC-09	Acknowledged	M/T/E	Current and NAVI are not deployed. The project acknowledges the current integration state and will enforce actual payout equality before either adapter is activated.
ORC-10	Acknowledged	T/E	Current is not deployed. The project acknowledges the current integration state and will validate the production rate domain and overflow behavior before activation.
ORC-11	Acknowledged	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
ORC-12	Acknowledged	T/E	External or operational assumptions remain trusted boundaries.
ORC-13	Acknowledged	T/E	NAVI is not deployed. The project acknowledges the incomplete lifecycle and will finish AccountCap, residual recovery, and migration handling before activation.
ORC-14	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
ORC-15	Acknowledged	T/E	Suilend is not deployed. The project acknowledges the unresolved upstream semantics and will validate compound and refresh behavior against the production ABI before activation.

Jitter Core Findings

ID	MANUAL STATUS*	EVIDENCE	FORMAL COVERAGE / RESIDUAL
JIT-01	Acknowledged	M/T	The arithmetic-domain obligation remains unproved but is explicitly acknowledged under FV-01; deployment is restricted to the tested domain with monitoring and an upgrade path.
JIT-02	Architecture Eliminated	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
JIT-03	Acknowledged	M/T/E	External or operational assumptions remain trusted boundaries.
JIT-04	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
JIT-05	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
JIT-06	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
JIT-07	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
JIT-08	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
JIT-09	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
JIT-10	Acknowledged	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
JIT-11	Architecture Eliminated	S/T	Executable or structural evidence only; no universal theorem is claimed.
JIT-12	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
JIT-13	Acknowledged	T/E	External or operational assumptions remain trusted boundaries.
JIT-14	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
JIT-15	Resolved	S	Executable or structural evidence only; no universal theorem is claimed.
JIT-16	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.

Rewards and Points Findings

ID	MANUAL STATUS*	EVIDENCE	FORMAL COVERAGE / RESIDUAL
EXT-01	Architecture Eliminated	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
EXT-02	Architecture Eliminated	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
EXT-03	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
EXT-04	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
EXT-05	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
EXT-06	Acknowledged	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
EXT-07	Acknowledged	M/T/E	External or operational assumptions remain trusted boundaries.
EXT-08	Acknowledged	M/T	Terminal claimant-set exhaustion is not formally closed; the project acknowledges sub-raw residual dust because principal is unaffected and the residual is monitored.
EXT-09	Architecture Eliminated	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
EXT-10	Acknowledged	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
EXT-11	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.

Policy and Auxiliary Findings

ID	MANUAL STATUS*	EVIDENCE	FORMAL COVERAGE / RESIDUAL
AUX-02	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
AUX-03	Deployment Excluded	M/T/E	Structural and test evidence supports deployment exclusion; no production guarantee is claimed.
AUX-06	Architecture Eliminated	S/T	Executable or structural evidence only; no universal theorem is claimed.
AUX-10	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.

Math and Solver Findings

ID	MANUAL STATUS*	EVIDENCE	FORMAL COVERAGE / RESIDUAL
MATH-01	Resolved	D/M/T	Direct production proof plus executable evidence; specification completeness still applies.
MATH-02	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
MATH-03	Acknowledged	D/T	Direct production proof plus executable evidence; specification completeness still applies.
MATH-04	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
MATH-05	Acknowledged	D/M/T	The reviewed replacement package is not live and normal validated-domain arithmetic is covered. The project acknowledges the extreme index frontier and will recalibrate the guard or extend the proof before enabling a broader production domain.
MATH-06	Resolved	D/S/T	Direct production proof plus executable evidence; specification completeness still applies.
MATH-07	Acknowledged	D/T	Direct production proof plus executable evidence; specification completeness still applies.

Admin and Registry Findings

ID	MANUAL STATUS*	EVIDENCE	FORMAL COVERAGE / RESIDUAL
ADM-01	Acknowledged	M/T/E	External or operational assumptions remain trusted boundaries.
ADM-02	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
ADM-03	Acknowledged	S/E	External or operational assumptions remain trusted boundaries.
ADM-04	Acknowledged	M/T/S	Model fidelity to production transitions remains a trusted mapping boundary.
ADM-05	Acknowledged	M/T	The default-listed invariant is not formally closed; the project acknowledges the discovery-layer risk and requires SDK and indexer revalidation.

Version-Control Findings

ID	MANUAL STATUS*	EVIDENCE	FORMAL COVERAGE / RESIDUAL
VC-01	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
VC-02	Resolved	T/E	External or operational assumptions remain trusted boundaries.
VC-03	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
VC-04	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.
VC-05	Resolved	M/T/E	External or operational assumptions remain trusted boundaries.
VC-06	Resolved	S/T	Executable or structural evidence only; no universal theorem is claimed.
VC-07	Resolved	M/T	Model fidelity to production transitions remains a trusted mapping boundary.

7. Trusted Boundaries and Reproduction

Not proven: third-party adapter semantics, oracle economic truth, honest administration or keeper operation, arbitrary PTB gas feasibility, RPC availability, frontend correctness, wallet behavior, key custody, economically bounded storage growth, or completeness of the specification.

Reproduction

Primary runners are `contract/jitter_formal/run-verified-suite.ps1`, `contract/jitter_formal/check-coverage-matrix.ps1`, and `contract/jitter_formal/run-mutation-checks.ps1`. Reproduction must use a frozen release commit and pinned verifier toolchain.