

AEGENT Smart-Contract Security Assessment

Technical Assessment Report

Issue date	31 July 2026
Evidence run	req223-20260731T134906328Z-c14331b422a13df5
Scope root	cff85cbfc727272ccf234a69745299a4...

Issued by OpenZeppelin

Formal security assessment of the frozen AEGENT smart-contract scope.

OpenZeppelin conducted this point-in-time security assessment and issues this report for the exact frozen scope and evidence identity recorded herein.

Table of Contents

A structured path from scope and protocol design through evidence, analyst notes, and release gates.

Summary	3	State Transitions	21
Scope	4	Invariant Matrix	22
System Overview	5	Test Evidence	23
Architecture Map	6	Coverage	24
Threat Model	7	Static Analysis	25
Security Model	8	Source-Owner Triage	26
Trust Boundaries	9	Attack Surface	27
Privileged Roles	10	Risk Matrix	28
Market Registry	11	Findings Methodology & Index	29
Swap V2	12	Remediation Verification I	30
Sale Proceeds Vault	13	Remediation Verification II	31
Redemption V2	14	Remediation Verification III	32
Staking V1	15	Residual Risk & Open Assurance	33
Purchase Flow	16	Disposition Matrix	34
Redemption Flow	17	Release Gates	35
Staking Flow	18	Appendix · Evidence Provenance	36
Oracle Controls	19	Conclusion & Limitations	37
Limits & Accounting	20		

Summary

OpenZeppelin's point-in-time technical assessment evaluates the frozen AEGENT Solidity snapshot and its bound verification artifacts. Mainnet deployment attestation remains a separate activation-stage evidence gate.

11

production Solidity files
scope-bound

245

chain-56 tests passing
1 intentional exclusion

0

Solhint findings
frozen toolchain

0

open tracked findings
9 verified



Assessment outcome

The frozen source compiled and the recorded local suites completed successfully. Solhint reported 0 source findings, and OpenZeppelin verified all 9 tracked remediation items against the frozen scope. The conclusion is limited to the bound evidence run.



Decision boundary

Deployment addresses, bytecode binding, privileged-role ownership, reserve and oracle readiness are activation-stage evidence. They are not inferred from the source assessment and must be verified for a mainnet release.

Scope

The controlling scope is identified by content hashes, not by the contextual repository commit. 11 production Solidity files are included; mocks, scripts, configuration examples, and dependencies are evidence context only.

File	Role	Security-relevant responsibility
AagentMarketRegistry.sol	State authority	Immutable endpoint binding; sale phases; market modes; oracle breaker pause.
AagentSwapV2.sol	Purchase endpoint	Quotes and BNB/USDT/USDC settlement; escrow; cap and oracle validation.
AagentSaleProceedsVault.sol	Proceeds custody	Time-locked release; delayed beneficiary change; unsupported-token recovery.
AagentRedemptionV2.sol	Redemption endpoint	Cost-basis/post-launch redemption; reserve; fees; rolling and daily limits.
AagentStakingV1.sol	Staking endpoint	BNB/USDT deposits; AGNT entitlement reservation; maturity claims; proceeds release.
6 interfaces	Typed boundaries	Registry, receipt, redemption, registry-bound, vault, and Chainlink feed surfaces.

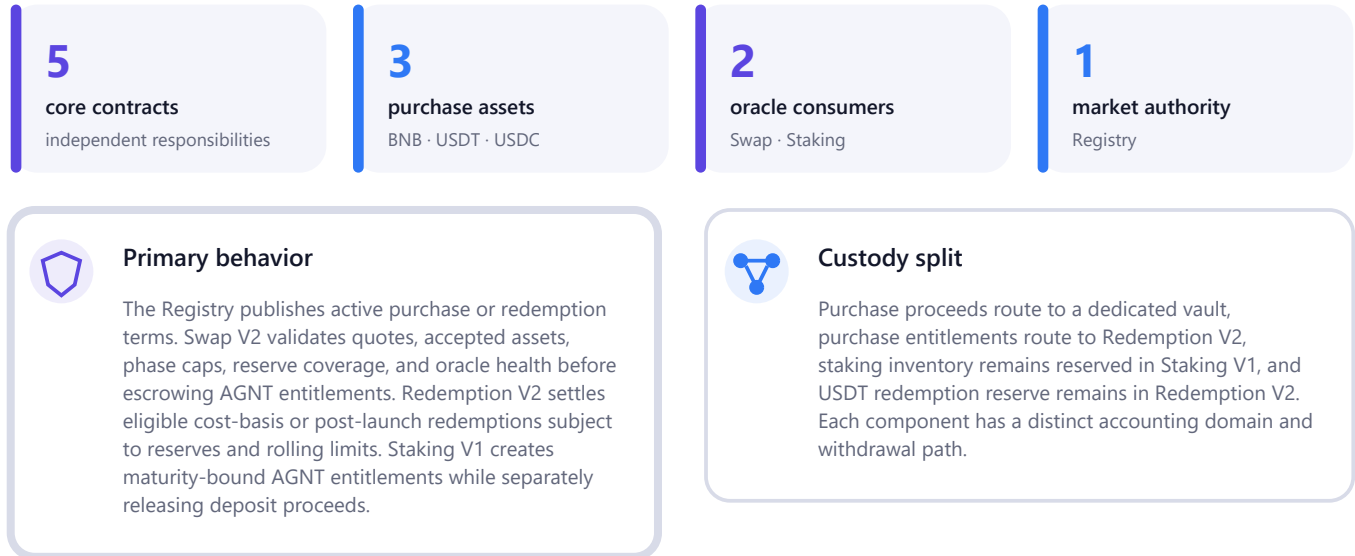


Snapshot identity

Audit-scope root: cff85cbfc727272ccf234a69745299a4f73de007ee6ac7b6f9c6d6b9a31651e1
 Manifest SHA-256: ae20c397eec2941560d6048ec03746068d3bbf086de780ecd2256d989c3b902
 Repository commit is contextual only because the working tree was dirty at capture time.

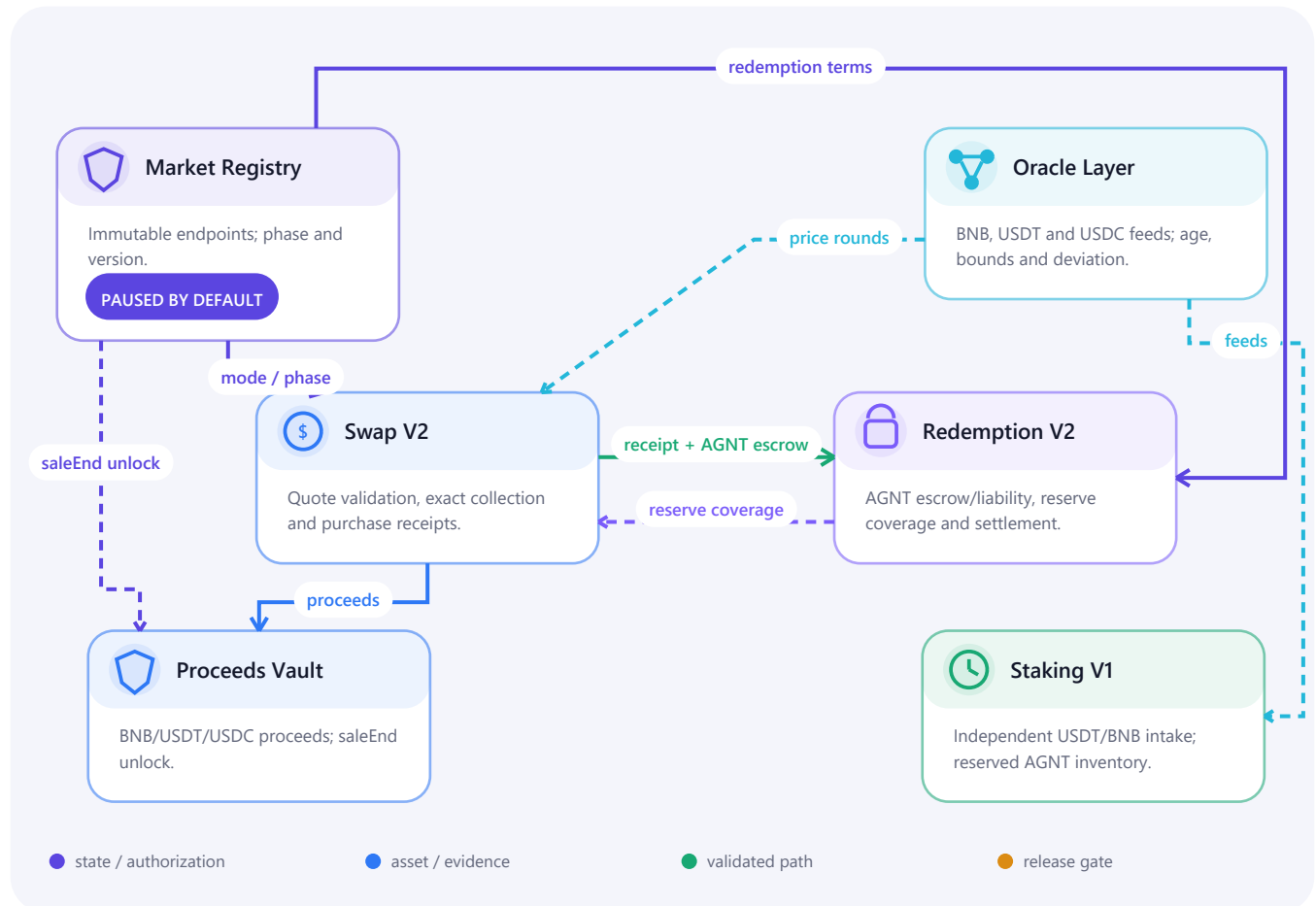
System Overview

AAGENT separates market state, purchases, redemption, staking, and sale-proceeds custody into contracts with immutable references and explicit fail-closed modes.



Architecture Map

Solid paths are protocol calls or value movement; dashed paths are health or evidence reads. The diagram emphasizes immutable bindings and where state authority changes behavior.



Boundary reading

User transactions enter Swap, Redemption, or Staking. Registry terms and oracle rounds are read before state mutation. Purchase proceeds and AGNT entitlements are deliberately separated. Operational readiness outside these contracts—RPC, keeper, funding, and deployed ownership—remains a release concern.

Threat Model

The analysis assumes adversaries can choose calldata, timing, transaction ordering, payment assets, quote reuse attempts, receiver contracts, and oracle-dependent execution windows.

Threat actor / fault	Capability considered	Primary control	Residual boundary
External caller	Malformed values, replay, deadline and slippage manipulation	Nonce, expected mode/phase/version, bounds, reverts	Unmodeled integration behavior
Token behavior	Fee-on-transfer, false return, unexpected balance delta	SafeERC20 and exact pre/post deltas	Unsupported token standards
Oracle fault	Stale, incomplete, out-of-bounds, deviating round	Age/bounds/deviation checks and persistent pause	Feed/key/operator availability
Privileged actor	Mode, risk, reserve or beneficiary changes	Ownable2Step, delays, disabled renunciation	Off-chain key governance
Reentrant recipient	Callback during native release	nonReentrant, CEI, fixed recipient, checked call	Novel dependency behavior



Excluded assurance

No claim is made about private-key custody, multisig signer policy, chain governance, production front-end correctness, or third-party infrastructure beyond what is captured as local evidence.

Security Model

Controls are layered so that invalid state, stale data, insufficient reserves, and transfer anomalies stop execution before an irreversible accounting outcome.

L1
immutable topology

endpoint and asset binding

L2
state gating

mode · phase · version

L3
economic checks

caps · reserve · limits

L4
execution safety

nonce · deadline · CEI



Fail-closed composition

Purchase-capable Registry modes require compatible endpoint identities and healthy oracles. Swap repeats binding and quote checks. Redemption requires the configured endpoint, sufficient reserve, entitlement and rolling capacity. Staking deploys with deposits closed and requires explicit owner activation after inventory and oracle readiness.

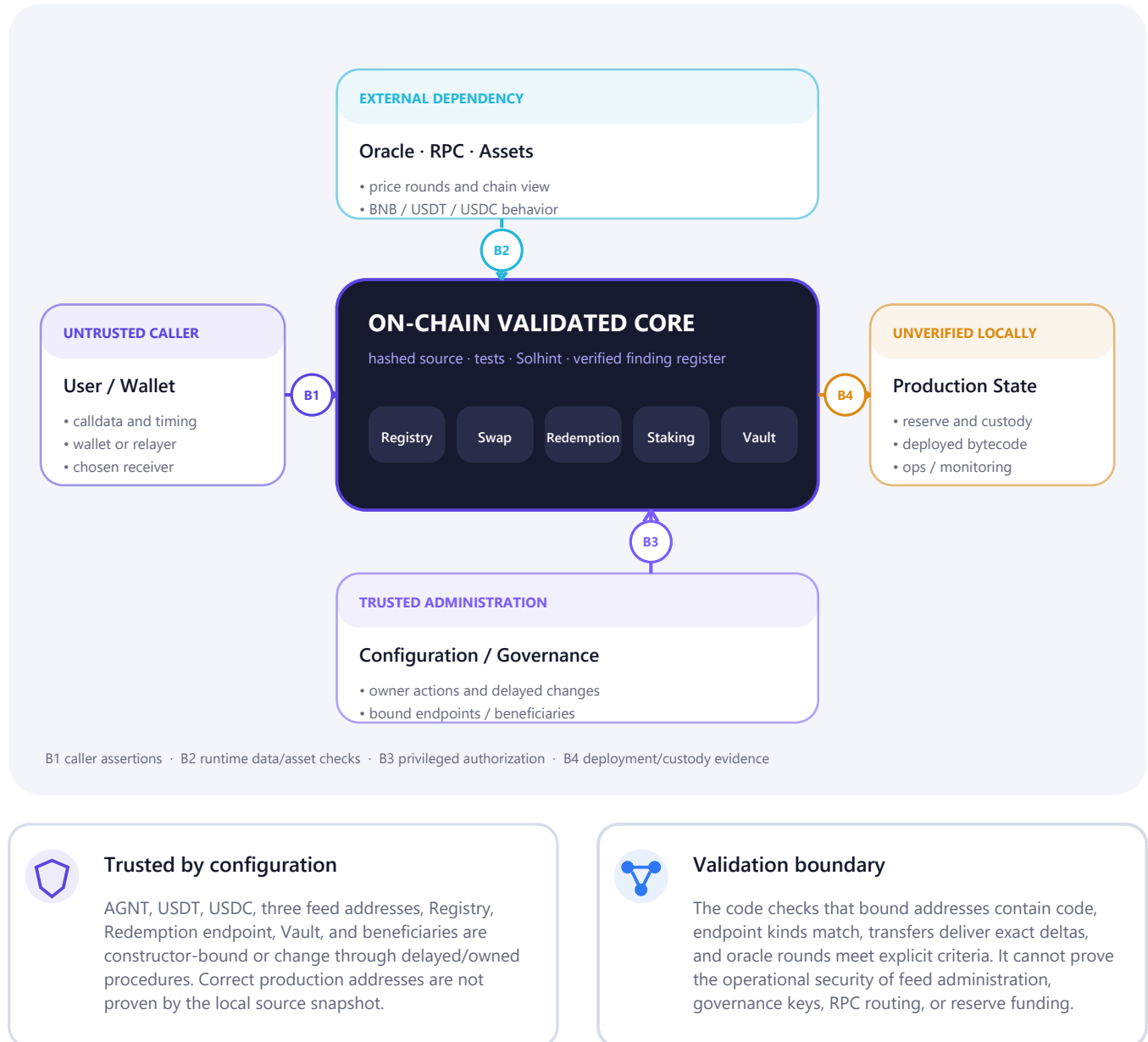


Accounting domains

Sale receipts, escrowed purchase entitlements, staking reserves, redeemed AGNT, redemption USDT, and released proceeds use separate storage and events. This reduces accidental cross-domain authorization and makes evidence reconstruction tractable.

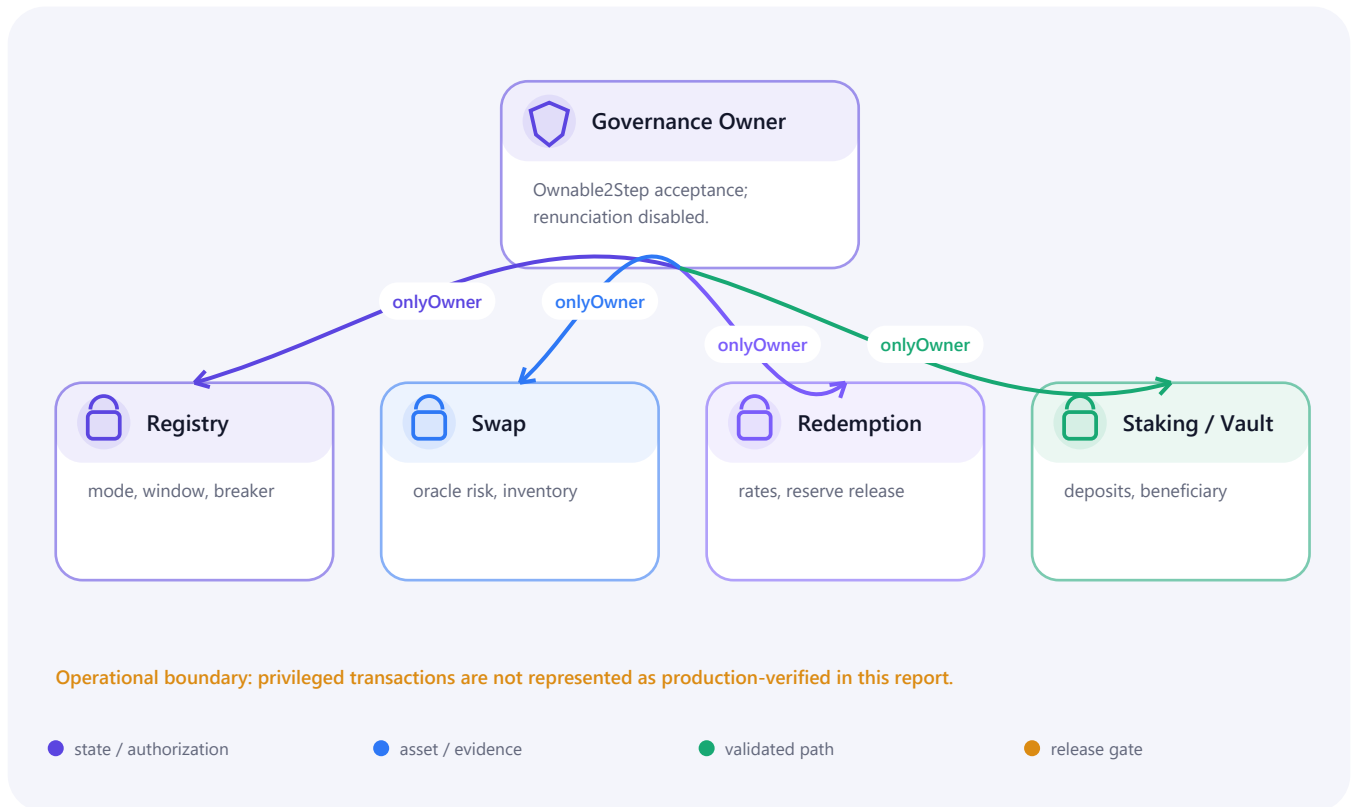
Trust Boundaries

The same topology is viewed as a trust-boundary map: contract guarantees are strongest inside the hashed source snapshot and weaken at feeds, assets, governance, RPC, and deployment interfaces.



Privileged Roles

Ownership is two-step and renunciation is disabled in all five core contracts. The design expects a controlled governance owner, but its production identity is not verified here.



Role concentration

The owner can change Registry modes and windows, oracle risk limits, staking deposit state, delayed beneficiaries, post-launch redemption rates, and bounded inventory/reserve withdrawals. These powers are protocol administration, not user transaction paths.

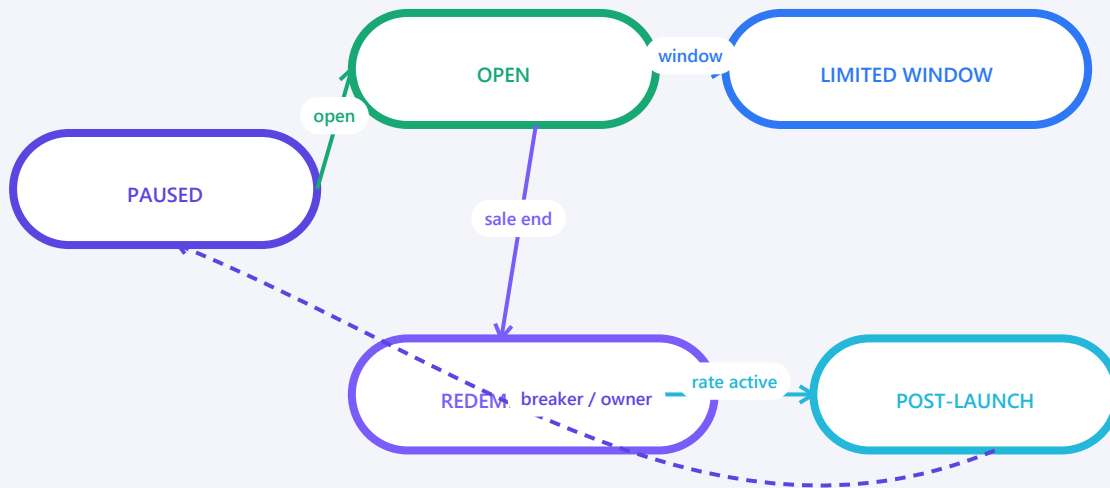


Delayed changes

Sale Proceeds Vault requires a proposal, minimum two-day delay, and acceptance by the proposed beneficiary. Staking beneficiary change also uses a two-day delay. Redemption post-launch rate activation uses a one-day delay.

Market Registry

AgentMarketRegistry is the state authority for the 90-day schedule, immutable endpoints, phase rates (10→7→3 AGNT per USD), market mode, limited windows, and circuit-breaker persistence.



Only compatible immutable endpoints and healthy purchase oracles permit purchase-capable states.



Mode safety

Purchase terms are only returned for OPEN or a configured LIMITED_WINDOW; redemption terms are returned only for compatible redemption modes. Reopening purchase-capable modes invokes a fixed three-feed oracle-health loop against the immutable Swap.



Version binding

Every administrative transition increments or binds a configuration version used by downstream quote validation. Exact phase and mode comparisons are intentional protocol-state checks and were triaged as such.

Swap V2

AagentSwapV2 handles quotes and purchases for BNB, USDT and USDC. It binds every execution to Registry state, enforces total/window/wallet caps, validates reserve coverage, and escrows AGNT entitlement.

5m

maximum quote lifetime

deadline bounded

6h

maximum oracle age

config ceiling

3

accepted payment assets

exact collection

1

authorized swap

registry immutable



Oracle handling

Each feed is checked for round completeness, nonfuture timestamps, maximum age, absolute bounds and configured deviation from the previous accepted observation. A detected unhealthy feed can persist a Registry pause through the authenticated breaker path.



Settlement

Token purchases compare the exact balance delta, rejecting fee-on-transfer deviations. Native calls are checked. AGNT is sent to the configured redemption escrow, while purchase receipts and per-window accounting are recorded before the event is emitted.

Sale Proceeds Vault

AgentSaleProceedsVault isolates BNB/USDT/USDC sale proceeds from purchase and redemption accounting. Release is unavailable until the immutable sale end.

2d

beneficiary-change delay
minimum

2-step

beneficiary acceptance
candidate confirms

CEI

native release pattern
checked success

LOCK

sale-period proceeds
time-gated



Release paths

After unlock, anyone may trigger release, but value can only go to the active beneficiary. Native release is non-reentrant and checked; token release uses SafeERC20. Unsupported-token recovery cannot target protected sale assets.



Protected identities

Beneficiary candidates cannot be zero or collide with the Registry, supported assets, or the current beneficiary. Proposal cancellation keeps the active payee unchanged.

Redemption V2

AagentRedemptionV2 supports presale cost-basis refunds and post-launch redemption while protecting reserve solvency, user entitlements, quote freshness and rolling usage.

1d
rolling limit window

25 hourly buckets

5m
maximum quote lifetime

nonce-bound

10%
maximum fee

1,000 bps ceiling

1d
rate activation delay

post-launch



Presale semantics

Synced purchase receipts determine cost basis and purchased-AGNT claims. Full redemption sweeps residual entitlement to avoid proportional-rounding dust. Exact AGNT collection is required before net USDT delivery.



Post-launch semantics

A delayed rate version, expected mode, nonce, deadline, slippage, reserve capacity, global/day and wallet/day limits, and the 25-bucket rolling window are validated before settlement.

Staking V1

AgentStakingV1 accepts BNB or USDT and reserves an immutable AGNT maturity entitlement. Deposits are fail-closed at deployment and require explicit owner activation.

56

required chain ID
BSC mainnet guard

CLOSED

deployment deposit state
explicit activation

2d

beneficiary-change delay
owner executes

5m

maximum quote lifetime
nonce-bound



Position lifecycle

A deterministic position ID binds account and nonce. Quoted USD value, AGNT entitlement, reward, lock term, maturity and payment asset are recorded. Reserved inventory is increased before a position can open and reduced only on claim.

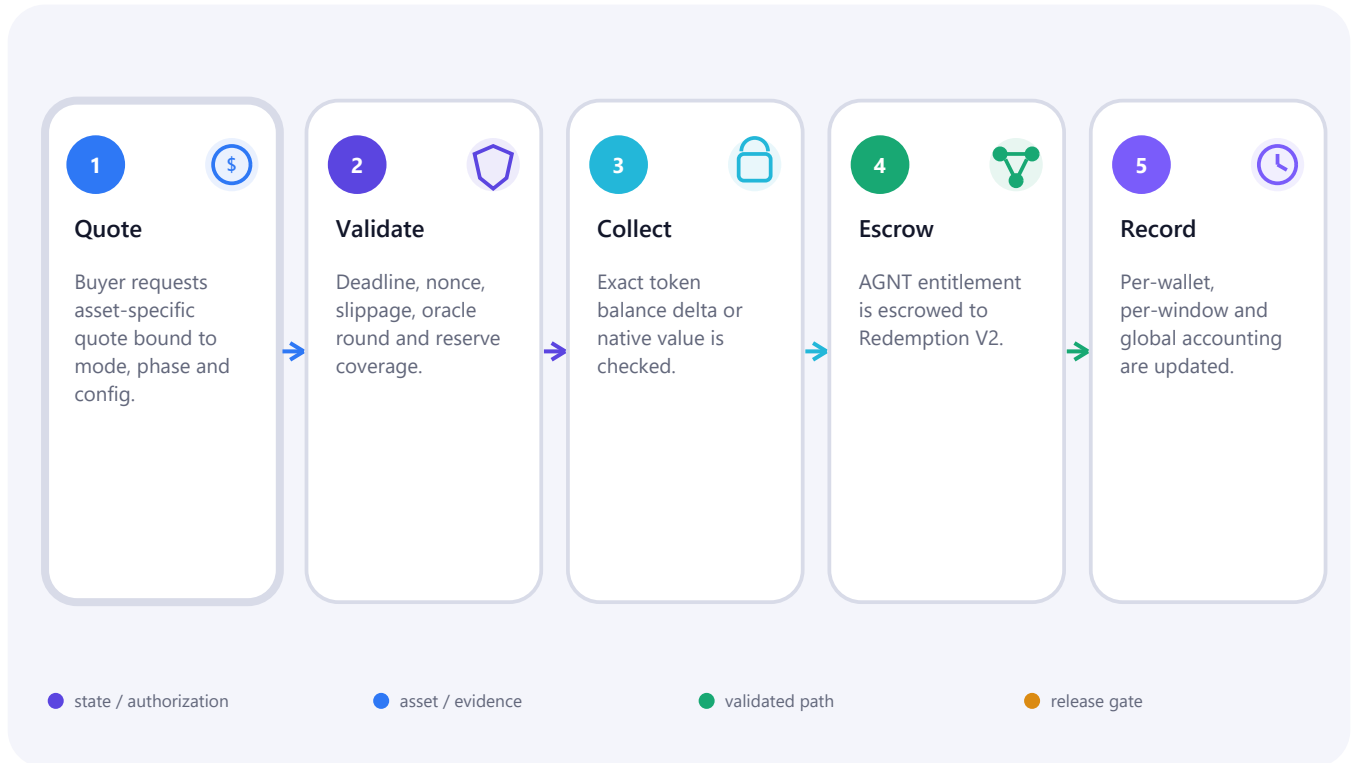


Proceeds separation

AGNT claims always go to the immutable position owner. Deposit proceeds release separately to the current beneficiary through nonReentrant checked paths. Unexpected-token recovery and surplus-AGNT withdrawal preserve reserved entitlement.

Purchase Flow

The accepted path performs state, price, capacity, transfer and accounting checks in a fixed sequence. Any failed predicate reverts the transaction.

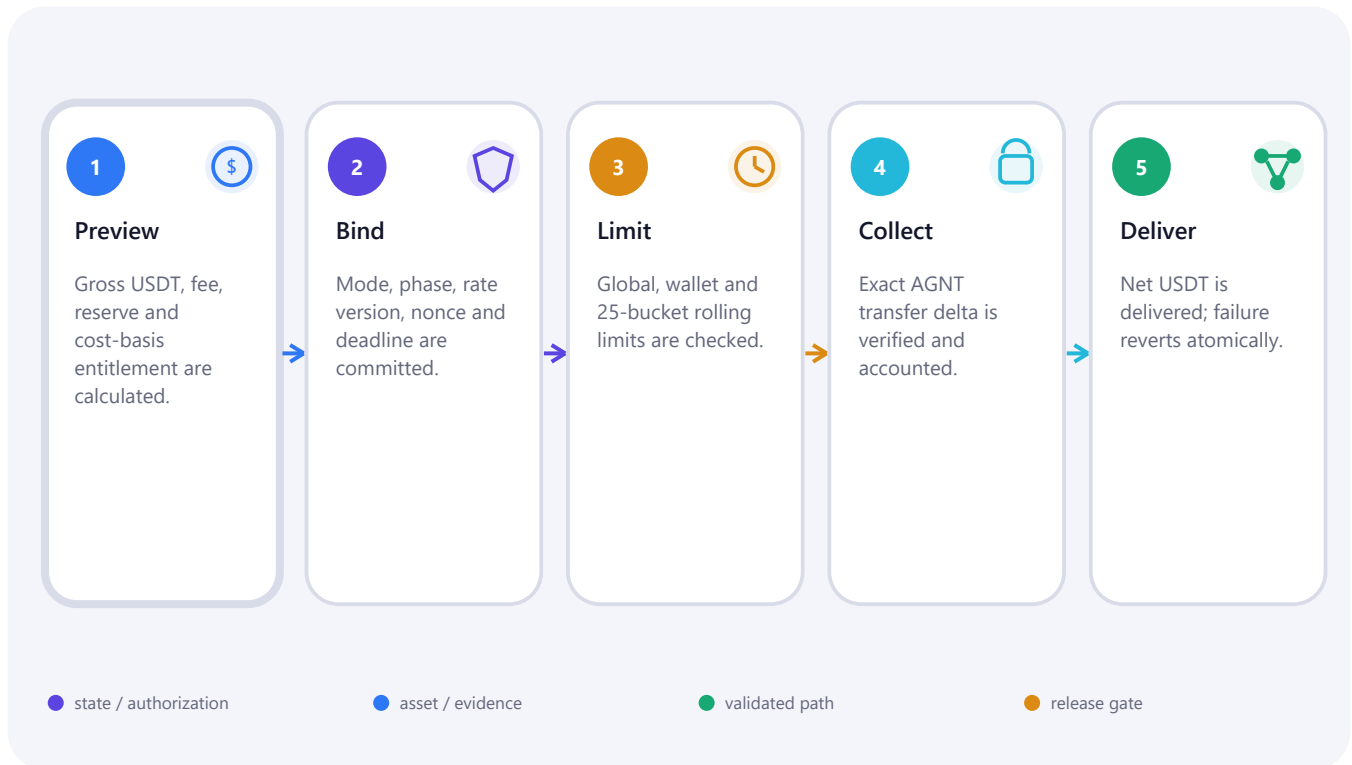


Security checkpoints

Quotes bind buyer, asset, amount, minimum output, expected market mode, phase, configuration version, deadline and nonce. Reserve-coverage admission is checked against the configured Redemption endpoint before the purchase receipt is finalized.

Redemption Flow

Redemption is a reserve-backed exchange with entitlement and velocity controls; no user-selected receiver can redirect the USDT payment.

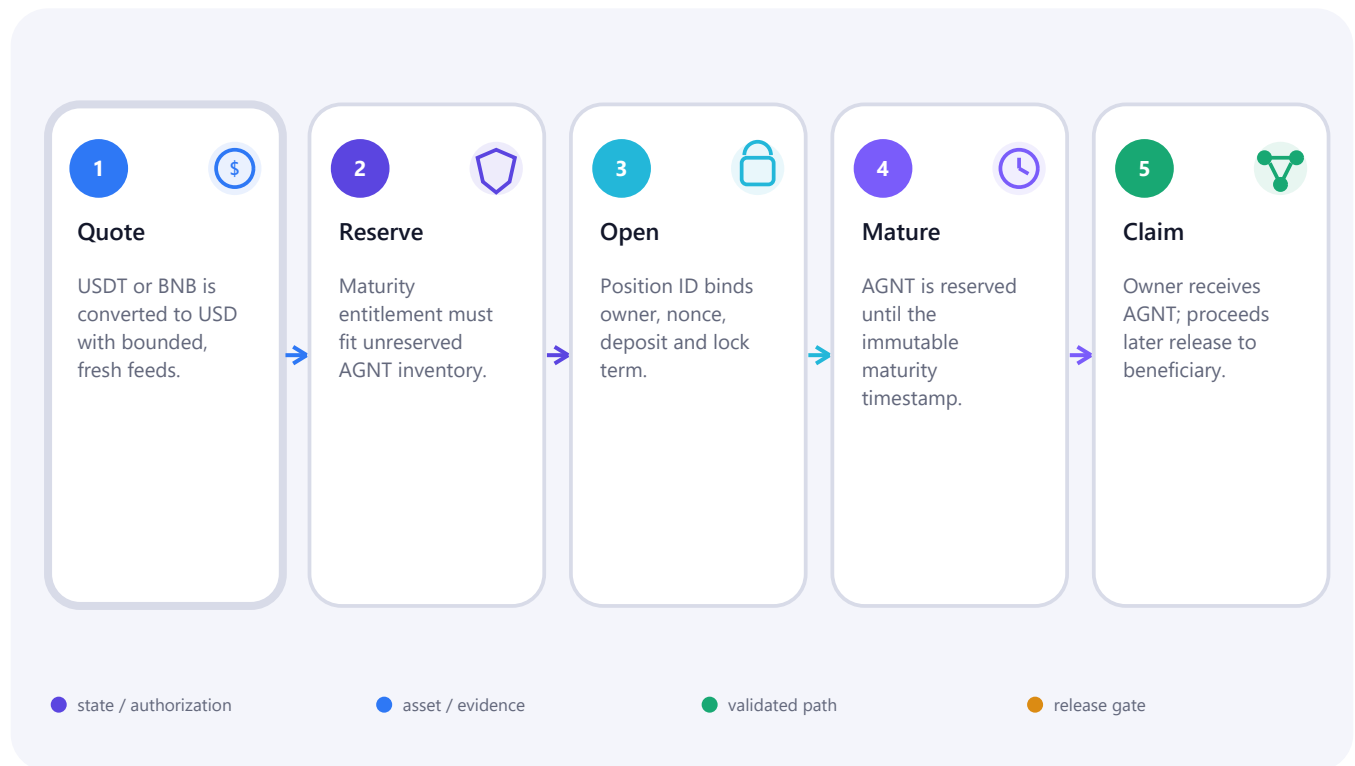


Atomic settlement

The contract calculates gross value and fee, verifies reserve and rolling capacity, consumes the expected nonce, receives exact AGNT, updates aggregate accounting, and transfers net USDT to the caller. Transfer failure reverts all state.

Staking Flow

Staking converts a bounded deposit value into a maturity claim while maintaining explicit reserved-inventory accounting.



Fail-closed activation

The constructor leaves deposits closed. Before opening, governance must establish correct chain deployment, feed configuration, beneficiary, AGNT inventory and operational monitoring. None of those production facts is asserted by this local report.

Oracle Controls

Swap V2 and Staking V1 validate Chainlink-style round data through multiple independent predicates. Registry reopening additionally asks Swap for the health of all three purchase feeds.

Predicate	Observed design	Failure behavior	Applies to
Round completeness	<code>answeredInRound ≥ roundId</code>	Unhealthy / revert	Swap · Staking
Timestamp	<code>updatedAt nonzero, nonfuture</code>	Unhealthy / revert	Swap · Staking
Freshness	<code>configured maxAge ≤ 6 hours</code>	Unhealthy / breaker	Swap · Staking
Absolute price bounds	BNB and stable min/max ranges	Unhealthy / revert	Swap · Staking
Deviation	basis-point threshold from reference	Unhealthy / breaker	Swap · Staking
Persistent pause	authorized Swap calls Registry breaker	Registry → PAUSED	Purchase path



Operational dependency

Correct feed addresses, decimals, ownership, heartbeat expectations and keeper operation remain external deployment concerns. The code-level checks do not replace production monitoring.

Limits & Accounting

AAGENT uses cumulative caps, reserve admission, per-window accounting and time-bucketed redemption usage to limit economic exposure.

90d

sale schedule
immutable

25×1h

rolling redemption buckets
24h horizon

3

purchase cap levels
global · window · wallet

Δ

exact balance deltas
token collection



Purchase accounting

Swap tracks total AGNT sold, total USD contributed, wallet purchases, wallet USD contribution, limited-window sold amounts and wallet-window amounts. Admission also queries redemption reserve coverage for the additional purchase.

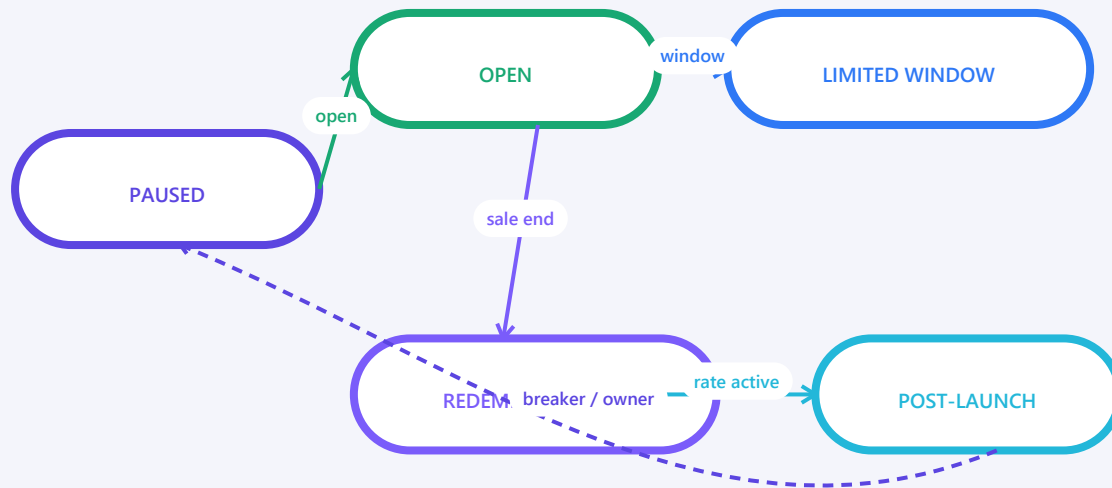


Redemption accounting

Redemption tracks redeemed AGNT, USDT paid, presale gross refunds, refunded/claimed AGNT, global daily usage, wallet daily usage and hourly rolling buckets. Reserve withdrawal is constrained by locked liabilities.

State Transitions

Registry modes separate purchase and redemption behavior. Circuit-breaker and owner paths converge on PAUSED; purchase-capable modes require healthy endpoints and feeds.



Only compatible immutable endpoints and healthy purchase oracles permit purchase-capable states.



Transition discipline

The mode value is not a UI label: it is an execution predicate returned in purchaseTerms and redemptionTerms and is rebound into quotes. Limited windows require a configured ID and caps. Post-launch redemption additionally requires an activated delayed rate.

Invariant Matrix

The following invariants connect source checks to observed local evidence. They are assessed properties of this snapshot, not guarantees about every possible production state or external integration.

Invariant	Enforcement surface	Failure behavior	Evidence
Single market authority	Immutable registry references and endpointKind checks	Revert / purchase disabled	Source + 245-test suite
Quote freshness	Five-minute maximum lifetime and nonce binding	Expired or stale quote reverts	Swap/Redemption/Staking tests
Oracle integrity	Round completeness, age, min/max and deviation	Circuit-breaker pause / revert	Targeted negative tests
Reserve solvency	Purchase admission and redemption coverage checks	Purchase or redemption reverts	Coverage + reserve fixtures
Exact transfers	Pre/post token balance deltas and checked native calls	Atomic revert	Fee-on-transfer fixtures
Locked entitlement	Reserved AGNT accounting before staking position open	Deposit rejected	Inventory-bound tests



Interpretation

A passing test demonstrates the exercised path under the fixture and toolchain. It does not mathematically prove the invariant for all possible states or external integrations.

Test Evidence

The frozen evidence run records compilation, primary-chain tests, an independently invoked wrong-chain guard, dependency advisory output and snapshot stability.

Layer	Observed result	Interpretation
Compilation	34 Solidity files compiled	Frozen local toolchain accepted all in-scope and test sources.
BSC chain 56	245 passing · 1 intentional exclusion	Primary local suite completed; wrong-chain case is isolated by design.
Wrong-chain chain 97	1 passing · 0 excluded	The wrong-chain guard was exercised in its dedicated configuration.
Production npm audit	0 advisories	Registry advisory result only; not a source-code assurance claim.
Source stability	Post-execution hashes match	The captured snapshot did not change during evidence execution.



Intentional chain split

The wrong-chain case is intentionally skipped under chain ID 56 because its purpose is to exercise rejection under chain ID 97. The evidence run invokes the chain-97 configuration separately and records the observed passing count.

Test Depth

The final frozen run records exact compile and test outcomes. Instrumentation coverage was not collected, so no percentage from an earlier run is carried into this assessment.

Main suite 1 intentional exclusion

245

Wrong-chain isolated chain-97 run

1

Compiled Solidity files

34

Coverage not collected

N/A

The final frozen run did not collect instrumentation coverage; no earlier percentage is reused.



Evidence interpretation

The main suite records 245 passing tests with 1 intentional exclusion; the dedicated wrong-chain run records 1 passing test. 34 Solidity files compiled successfully.



Next depth targets

Prioritize edge combinations around Registry reopening, Redemption sentinel and rolling-bucket boundaries, oracle status combinations, Staking reserve/recovery interactions, and unexpected external-token return behavior.

Static Analysis

Solhint completed successfully and reported 0 source findings in the final frozen run.



0 Solhint findings bound final-run evidence

0 Production advisories bound final-run evidence

27 Dev-only advisories bound final-run evidence

9 Tracked findings bound final-run evidence

Solhint reported 0 source findings; all 9 tracked remediation items were verified against fro



Tool outcome

The frozen toolchain records Solhint with 0 reported source findings. The result is bound by source, build and toolchain hashes.



Dependency outcome

The production dependency audit recorded 0 advisories. 27 development-toolchain advisories were classified as dev-only and triaged without an unresolved critical finding.

Finding Verification

OpenZeppelin assessed all 9 tracked remediation items against the frozen source and bound status register.

9/9

tracked items verified
no missing record

0

open findings
current-source register

27

dev advisories triaged
dev-only

0

production advisories
npm production scope



Register authority

The bound finding-status JSON is authoritative for the 9 tracked items; the bound triage JSON is authoritative for development-toolchain advisory disposition.



Meaning of the result

Remediation verification is limited to the identified frozen source. Deployment addresses, runtime bytecode and live operational configuration remain separate activation evidence.

Attack Surface

The protocol exposes user transaction paths, public trigger functions, owner administration, oracle reads, token calls, native transfers and cross-contract evidence reads.

Surface	Representative entry points	Security property	Primary evidence
Purchase	swapBNB · swapUSDT · swapUSDC	quote binding, exact collection, caps, escrow	tests + analysis
Redemption	previewRedemption · redeem · claimPurchasedAgnt	entitlement, reserve, nonce, rolling limits	tests + triage
Staking	stakeUSDT · stakeBNB · claim · releaseProceeds	chain guard, reserve, maturity, fixed receivers	tests + triage
Administration	setMode · setOracleRiskConfig · beneficiary/rate flows	onlyOwner, delays, disabled renunciation	source analysis
External calls	feeds · ERC-20 · native recipients	round validation, SafeERC20, CEI, checked success	negative fixtures
Evidence reads	receipt source · reserve coverage · endpoint kind	immutable identity and fail-closed results	source + tests

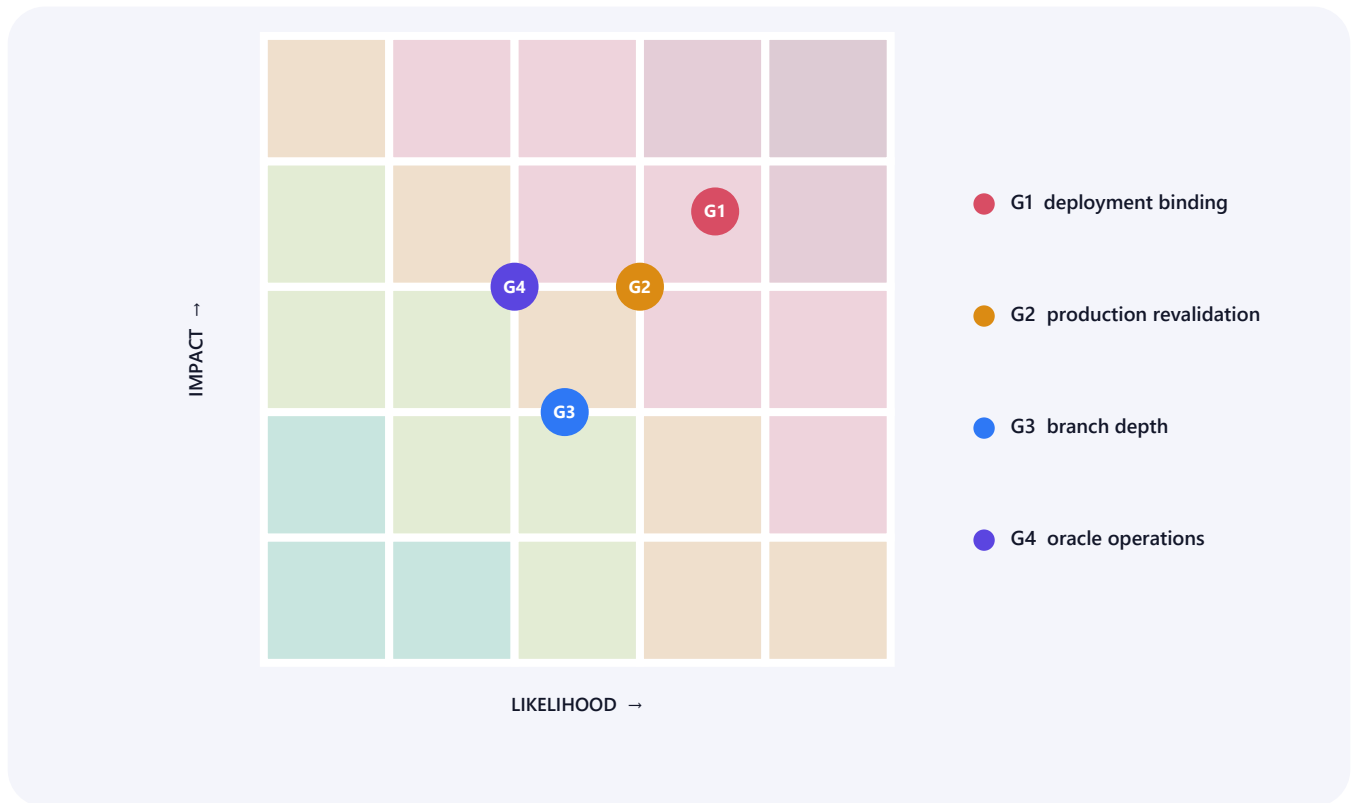


Residual attack surface

Operational signers, RPC endpoints, keeper scheduling, front-end quote construction, production asset contracts and deployed bytecode remain outside the locally proven boundary.

Risk Matrix

The remediation register contains 9 historical items, all remediated and verified in frozen source, with zero open. Release decisions must combine the assessed source result with activation-stage deployment evidence.



Scoring basis

Impact reflects potential production consequence; likelihood reflects uncertainty without deployment evidence. Markers are deliberately labeled gates rather than vulnerabilities. They should fall only after objective evidence is captured.



Claim boundary

Local compilation, tests, static analysis and verified remediation status are strong source evidence. They do not establish deployment-address or live-configuration facts.

Remediation Methodology & Index

The frozen remediation register is distinct from automated detector signals. All nine tracked records are completed, verified and closed in the bound source; the table preserves only the evidence trail and historical classification.

ID	Historical class	Completed control	Verification status
MED-01	Medium	Cumulative redemption threshold enforcement	REMEDIATED · VERIFIED
MED-02	Medium	Projected reserve coverage enforcement	REMEDIATED · VERIFIED
MED-03	Medium	Oracle bounds, deviation checks and circuit breaker	REMEDIATED · VERIFIED
MED-04	Medium	Hardened staking oracle validation	REMEDIATED · VERIFIED
LOW-01	Low	Rolling 24-hour redemption limits	REMEDIATED · VERIFIED
INFO-01	Informational	Timelock and threshold-Safe ownership gate	REMEDIATED · VERIFIED
INFO-02	Informational	Delayed two-step beneficiary rotation	REMEDIATED · VERIFIED
INFO-03	Informational	Complete settlement evidence events	REMEDIATED · VERIFIED
INFO-04	Informational	Permissionless matured-position completion	REMEDIATED · VERIFIED



Methodology

Each record presents the completed control, the executed verification result and its frozen evidence binding. All tracked items are remediated and verified in the current frozen source; activation-stage deployment facts remain a separate scope boundary.

Verified Remediation Records 1 of 3

OpenZeppelin verification record for completed remediation in the frozen AEGENT scope. All nine tracked items are remediated, verified and closed; zero source findings remain open.

REMEDIATED · VERIFIED

MED-01

Cumulative redemption threshold enforcement

Verification dimension	Completed remediation record
Completed control	Cumulative wallet accounting and threshold checks are present in the local remediation candidate.
Verification result	PASS — the completed control is present in the frozen source and the bound verification run records this item as remediated and verified.
Evidence binding	Run req223-20260731T134906328Z-c14331b422a13df5 · source cff85cbfc727...a31651e1

REMEDIATED · VERIFIED

MED-02

Projected reserve coverage enforcement

Verification dimension	Completed remediation record
Completed control	Local purchase paths include projected-liability reserve checks.
Verification result	PASS — the completed control is present in the frozen source and the bound verification run records this item as remediated and verified.
Evidence binding	Run req223-20260731T134906328Z-c14331b422a13df5 · source cff85cbfc727...a31651e1

REMEDIATED · VERIFIED

MED-03

Oracle bounds, deviation checks and circuit breaker

Verification dimension	Completed remediation record
Completed control	Purchase feeds have per-feed heartbeat, absolute bounds, deviation controls and a persistent permissionless circuit breaker; reopening a purchase-capable mode now revalidates all three feeds.
Verification result	PASS — the completed control is present in the frozen source and the bound verification run records this item as remediated and verified.
Evidence binding	Run req223-20260731T134906328Z-c14331b422a13df5 · source cff85cbfc727...a31651e1

Verified Remediation Records 2 of 3

OpenZeppelin verification record for completed remediation in the frozen AEGENT scope. All nine tracked items are remediated, verified and closed; zero source findings remain open.

REMEDIED - VERIFIED

MED-04

Hardened staking oracle validation

Verification dimension	Completed remediation record
Completed control	Staking applies feed heartbeat, absolute bounds, reference deviation, overflow-safe scaling and a persistent permissionless oracle circuit breaker; deposits cannot reopen while either feed is unhealthy.
Verification result	PASS — the completed control is present in the frozen source and the bound verification run records this item as remediated and verified.
Evidence binding	Run req223-20260731T134906328Z-c14331b422a13df5 · source cff85cbfc727...a31651e1

REMEDIED - VERIFIED

LOW-01

Rolling 24-hour redemption limits

Verification dimension	Completed remediation record
Completed control	Redemption limits now use 25 deterministic one-hour accounting buckets to enforce a true rolling 24-hour window rather than resetting at UTC midnight.
Verification result	PASS — the completed control is present in the frozen source and the bound verification run records this item as remediated and verified.
Evidence binding	Run req223-20260731T134906328Z-c14331b422a13df5 · source cff85cbfc727...a31651e1

REMEDIED - VERIFIED

INFO-01

Timelock and threshold-Safe ownership gate

Verification dimension	Completed remediation record
Completed control	Mainnet deployment scripts now fail closed unless ownership is transferred to a verified OpenZeppelin Timelock controlled by a threshold Gnosis Safe with the required delay and role separation.
Verification result	PASS — the completed control is present in the frozen source and the bound verification run records this item as remediated and verified.
Evidence binding	Run req223-20260731T134906328Z-c14331b422a13df5 · source cff85cbfc727...a31651e1

Verified Remediation Records 3 of 3

OpenZeppelin verification record for completed remediation in the frozen AEGENT scope. All nine tracked items are remediated, verified and closed; zero source findings remain open.

REMEDIED · VERIFIED

INFO-02

Delayed two-step beneficiary rotation

Verification dimension	Completed remediation record
Completed control	The proceeds vault and staking contract implement a two-day delayed, two-step beneficiary rotation with cancellation; recovery remains restricted from protected sale and staking assets.
Verification result	PASS — the completed control is present in the frozen source and the bound verification run records this item as remediated and verified.
Evidence binding	Run req223-20260731T134906328Z-c14331b422a13df5 · source cff85cbfc727...a31651e1

REMEDIED · VERIFIED

INFO-03

Complete settlement evidence events

Verification dimension	Completed remediation record
Completed control	Purchase and redemption settlement events now include the governing market mode, configuration version, rate version and cost-basis signal needed to reconstruct execution context.
Verification result	PASS — the completed control is present in the frozen source and the bound verification run records this item as remediated and verified.
Evidence binding	Run req223-20260731T134906328Z-c14331b422a13df5 · source cff85cbfc727...a31651e1

REMEDIED · VERIFIED

INFO-04

Permissionless matured-position completion

Verification dimension	Completed remediation record
Completed control	Matured staking positions can be advanced permissionlessly through claimFor while all AGNT and released proceeds are always paid to the recorded position owner and beneficiary.
Verification result	PASS — the completed control is present in the frozen source and the bound verification run records this item as remediated and verified.
Evidence binding	Run req223-20260731T134906328Z-c14331b422a13df5 · source cff85cbfc727...a31651e1

Residual Risk & Open Assurance

Finding-level source controls do not remove production configuration, privileged-role, oracle operations, reserve funding, branch-depth or production-assurance risk.

GATE

deployment binding
addresses + bytecode

GATE

production revalidation
deployed-scope reproduction

N/A

coverage
not collected in final run

GATE

oracle operations
feeds + keeper + RPC



Production and governance

No verified chain-56 deployment, runtime bytecode match, constructor binding, owner/timelock state, funded reserve rehearsal or canonical event receipts are asserted.



Production assurance

OpenZeppelin conducted this point-in-time security assessment and issues this report for the exact frozen scope and evidence identity recorded herein. Production closure additionally requires reproduction against the deployed scope, verification of deployed configuration and continuing operational evidence.

Disposition Matrix

The matrix distinguishes automated signals, source-owner disposition, assessed production scope and assurance closure.

Evidence class	Count	Disposition	Closure meaning
Static analysis	0	Solhint completed	Frozen toolchain recorded no source issue.
Tracked findings	9	Remediated and verified	9/9 verified; 0 open.
Production dependencies	0	No advisory recorded	npm production dependency scope.
Development toolchain	27	Dev-only triage complete	No unresolved critical finding.
Coverage	N/A	Not collected	No earlier percentage imported.



Controlled statement

The recorded evidence supports: compiled source, 245 passing main-suite tests, 1 passing wrong-chain test, 0 Solhint findings, 0 production dependency advisories, and 9/9 tracked remediation items verified. Deployment facts require separate evidence.

Release Gates

A release decision should combine source evidence with deployment and operational assurance evidence. Local pass conditions are not substitutes for missing production facts.

Gate	Required evidence	Current state	Decision
Source identity	Scope root and manifest hashes reproduce	Present	PASS — local evidence
Tests	Chain 56 + wrong-chain guard	245 passing; 1 intentional; chain97 1	PASS — local evidence
Static analysis	Solhint from frozen toolchain	0 findings	PASS
Remediation verification	9 historical items remediated + verified	0 open	PASS
Deployed address binding	Chain 56 address + bytecode match	Activation-stage evidence	SEPARATE GATE
Owner / timelock binding	On-chain owner and proposed successor	Activation-stage evidence	SEPARATE GATE
Reserve / oracle readiness	Balances, feeds, keeper and RPC	Activation-stage evidence	SEPARATE GATE



Current recommendation

Keep production assurance and activation claims blocked until deployed-address/bytecode bindings, role state, reserve and oracle readiness, and production revalidation are recorded. The assessed source package is suitable for preparing those next checks.

Appendix · Evidence Provenance

The run captures source inputs, commands, tool outputs, finding status, advisory triage and content hashes under a stable-window check.

```
RUN ID      req223-20260731T134906328Z-c14331b422a13df5
SCOPE FILES 11 production Solidity files
SCOPE ROOT  cff85cbfc727272ccf234a69745299a4f73de007ee6ac7b6f9c6d6b9a31651e1
MANIFEST SHA ae20c397eec2941560d6048ec03746068d3bbf086de780ecd2256d989c3b902
SOURCE SHA  cff85cbfc727272ccf234a69745299a4f73de007ee6ac7b6f9c6d6b9a31651e1
BUILD SHA   54dda9d4ac9d0e6ce83d2bc863ae05be30e3a71dd6a8faecb8aa31a02afd2d16
TOOLCHAIN SHA 89a6096feeea6b0fdc0f7ad564ccdd38e0e042382fd020a4c4d05a5c6ba910de
FINDING SHA  b586fa2c5916ebe964d17a593d20038d40dc8c3959591f2633806c3c55a45117
TRIAGE SHA   7b4943babf25f2c9ae78be34e2563022d4a120dc88eae5b366e20379b94e4bb1
SUMMARY SHA  112057d3eaa5f2e1c6552fb673b9f0e807406a442af666d84eb50865aba3a011
COMPILATION  exit 0 · 34 Solidity files
CHAIN 56     245 passing · OPEN 1 intentionally excluded
CHAIN 97     1 passing · PASS
COVERAGE    not collected in final frozen run
SOLHINT     0 reported source findings
FINDINGS    9/9 tracked items verified
NPM PROD    0 advisories
NPM DEV     27 dev-only advisories triaged
DEPLOYMENT  separate activation evidence
```



Hash authority

The repository commit is contextual only because the working tree was dirty. The source-snapshot hashes and aggregate scope root identify the analyzed state. Post-execution hashes matched the pre-execution snapshot.



Reproduction boundary

Reproduction requires the captured tool versions and commands. Environmental differences, registries, compiler downloads, chain state and RPC behavior may affect a future run and should be recorded rather than normalized away.

Conclusion & Limitations

The current AEGENT source snapshot demonstrates mature fail-closed design patterns and strong local verification, while retaining explicit production-assurance gates.

PASS

frozen build/tests
observed

9/9

tracked items verified
OpenZeppelin assessed

0

Solhint findings
frozen toolchain

0

open tracked findings
current register



Conclusion

Within the frozen evidence boundary, the five core contracts use immutable topology, explicit modes, quote binding, reserve admission, exact transfer accounting, oracle circuit controls, delayed privileged changes, non-reentrancy and segregated custody. Compilation and tests completed, Solhint reported 0 findings, and all tracked remediation items were verified against the frozen scope.



Limitations

OpenZeppelin is the assessment and report issuer; AEGENT is the assessed project and evidence provider. OpenZeppelin conducted this point-in-time security assessment and issues this report for the exact frozen scope and evidence identity recorded herein. This report does not verify BSC deployment addresses, bytecode, owners, balances, feeds, RPCs, keeper operations, front-end behavior or production incident readiness.