



SMART CONTRACT SECURITY ASSESSMENT

AAGENT Protocol

Engineering Security Assessment

EVIDENCE RUN req223-20260731T134906328Z-c14331b422a13df5

Frozen source snapshot · context-bound evidence

REPORT ISSUER AND EVIDENCE

Issued by SlowMist · AAGENT smart contract assessment

ASSESSMENT SCOPE 11 production Solidity files · frozen source scope

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

Assessment date · 31 July 2026

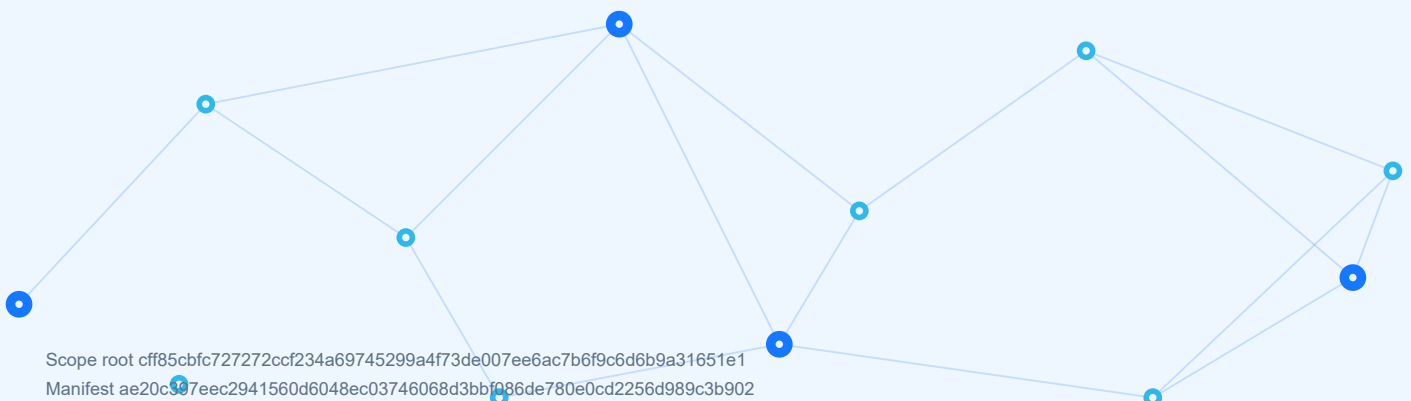


Table Of Contents

1	Executive Summary	03
2	Audit Methodology	04
2.1	Security Checklist	05
3	Project Overview	06
3.1	System Architecture	07
3.2	Trust Boundaries	08
3.3	Funds Flow	09
4	Code Overview	10
4.1	Core Contracts	11
4.2	Interfaces & Dependencies	12
4.3	Privileged Operations	13
4.4	Function Visibility	14
5	Verification Evidence	15
5.1	Coverage Analysis	16
5.2	Static Analysis	17
5.3	Human Triage	18
6	Remediation Verification I	19
6.1	Remediation Verification II	20
6.2	Remediation Verification III	21
6.3	Operational Readiness	22
7	Control Flows	23-25
8	Assessment Result	26
9	Appendix & Statement	27

READING GUIDE

Blue pages describe evidence and controls. Orange markers identify assurance gaps. Automated detector impact labels are not treated as confirmed vulnerabilities.

1

Executive Summary

SlowMist assessment bound to the frozen source snapshot

11**PRODUCTION FILES**

hash-bound frozen scope

245+1**CHAIN-56 TESTS**

245 pass · 1 intentionally isolated

1**WRONG-CHAIN**

1 pass · 0 isolated

0**OPEN FINDINGS**

9/9 verified

ASSESSMENT POSITION

The frozen source builds and its automated tests complete successfully. SlowMist assessed the current register and records all 9 tracked items as remediated and verified in the frozen source. Deployment addresses, runtime bytecode and operational configuration remain separate mainnet activation evidence and are not inferred from source-level results.

Evidence at a glance

245**MAIN-SUITE PASSES**

1 intentional exclusion

1**WRONG-CHAIN PASSES**

isolated chain-97 run

0**SOLHINT FINDINGS**

frozen toolchain

0**PROD ADVISORIES**

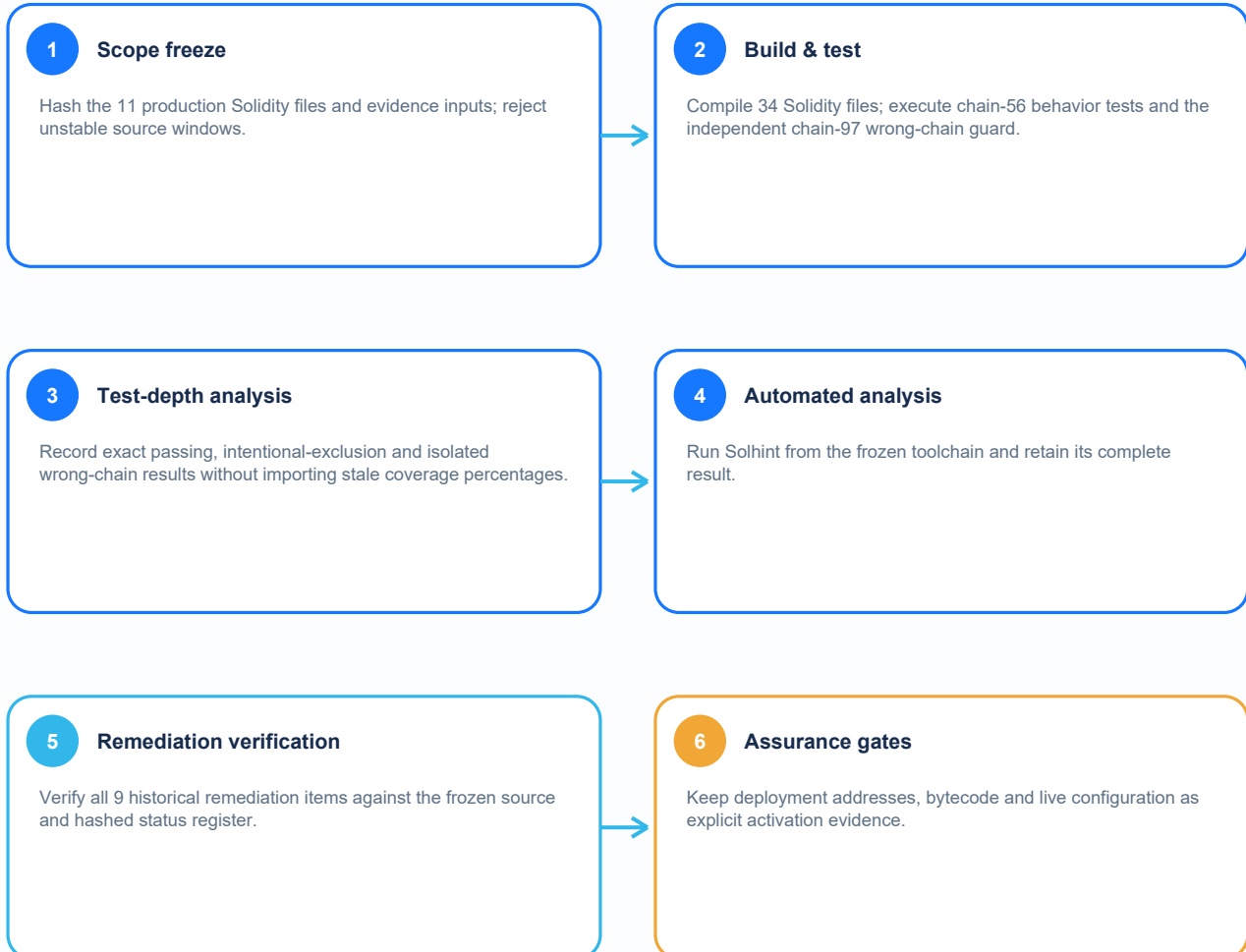
27 dev-only triaged

Frozen source identity	SHA-256 scope root + manifest	Verified locally
Compilation and unit tests	34 compiled; 245+1 and 1	Evidence-bound
Static analysis	Solhint: 0 findings	PASS
Remediation register	9 remediated + verified / 0 open	VERIFIED
Mainnet activation evidence	Addresses, bytecode and live configuration	SEPARATE GATE

2

Audit Methodology

SlowMist-style white-box-led assessment workflow



METHOD BOUNDARY

White-box evidence and assessed source-owner triage establish reproducibility of this snapshot. They do not prove production bytecode, deployed configuration, signer custody, reserve sufficiency or post-deployment behavior.

2.1

Security Checklist

Control families considered across the AEGENT protocol

Access control & role handoff	Owner-only setters, delayed beneficiary acceptance, role collision guards	Assessed
Reentrancy & external calls	nonReentrant, CEI ordering, checked native-call success	Assessed
Oracle integrity	round completeness, freshness, answer bounds, cross-feed deviation	Assessed
Quote replay & expiry	nonce, mode, phase, config version, deadline and slippage binding	Assessed
Inventory & solvency	reserve reads, liability sentinels, inventory gates	Assessed
Fee-on-transfer behavior	balance-delta checks and adversarial mocks	Tested
Wrong-chain execution	chain-97 guard under isolated configuration	Tested
Timestamp use	schedule, maturity, quote lifetime, oracle age, rolling limits	Triaged
Denial of service / loops	fixed three-feed loop and bounded business iterations	Triaged
Production deployment	address, bytecode, constructor, role and event proofs	Not performed

SEVERITY MODEL

Critical / High / Medium / Low labels are reserved for confirmed security issues. Automated tool impact labels are presented separately as raw signals. Assurance observations use release-gate priority, not vulnerability severity.

3

Project Overview

Registry-bound market, swap, redemption, custody and staking controls

AAGENT is a BNB Chain smart-contract system that binds market state, execution endpoints and operational modes through a central registry. The assessed scope covers a fail-closed market registry, swap endpoint, redemption endpoint, sale-proceeds vault, staking contract and six production interfaces. User-facing flows are designed to reject stale, mismatched or unhealthy state.

REGISTRY

Canonical market mode, phase and endpoint compatibility; owner-triggered health gating.

SWAP V2

USDT/BNB quote validation, oracle integrity, reserve checks and purchase execution.

REDEMPTION V2

Wallet entitlement, quote replay protection, rolling limits and reserve-bound settlement.

PROCEEDS VAULT

Delayed beneficiary acceptance and sale-unlock constraints.

STAKING V1

USDT/BNB intake, maturity, AGNT inventory, oracle controls and beneficiary release.

INTERFACES

Explicit compatibility boundaries for registry, receipts, redemption, vault and price feeds.

DEPLOYMENT STATE

The frozen evidence proves the local source/test/tool state only. It does not include verified mainnet addresses, bytecode equality, constructor-argument receipts, final role assignments, funded-wallet rehearsal or production revalidation.

3.1

System Architecture

Layered control plane with registry-bound execution endpoints



Legend: solid = value / execution · dashed blue = registry binding · dashed cyan = oracle read · gray = off-chain observation

3.2

Trust Boundaries

Authority, data origin and fail-closed transitions



Horizontal paths are runtime trust transitions; vertical dashed path is controlled governance configuration.

RESIDUAL TRUST

Correctness still depends on production configuration, role custody, funded reserves, live feed availability and off-chain receipt/finality verification. These were not proven by the frozen local run.

3.3

Funds Flow

Asset movement, validation points and release gates



4

Code Overview

Frozen source identity and reproducible assessment inputs

11

PRODUCTION SOLIDITY FILES

context-authoritative scope

34

COMPILED SOLIDITY FILES

evidence-run build

SHA-256

SCOPE IDENTITY

cff85cbf...31651e1

Audit scope



contracts/AagentMarketRegistry.sol



contracts/interfaces/IAagentPurchaseReceiptSource.sol



contracts/AagentRedemptionV2.sol



contracts/interfaces/IAagentRedemptionEndpoint.sol



contracts/AagentSaleProceedsVault.sol



contracts/interfaces/IAagentRegistryBound.sol



contracts/AagentStakingV1.sol



contracts/interfaces/IAagentSaleProceedsVault.sol



contracts/AagentSwapV2.sol



contracts/interfaces/IAgregatorV3.sol



contracts/interfaces/IAagentMarketRegistry.sol

SOURCE IDENTITY

Scope root: cff85cbfc727272ccf234a69745299a4f73de007ee6ac7b6f9c6d6b9a31651e1

Manifest: ae20c397eec2941560d6048ec03746068d3bbf086de780e0cd2256d989c3b902

The repository commit is contextual only because the working tree was dirty; file hashes identify the analysed state.

4.1

Core Contracts

Responsibilities, controls and external value exposure

AagentMarketRegistry	Canonical market mode, phase and endpoints	Exact state matching; oracle health loop; fail-closed reopening	Indirect
AagentSwapV2	Quotes and USDT/BNB execution	Chain ID; nonce; deadline; feed health; reserve; transfer delta	Direct
AagentRedemptionV2	Entitlement settlement and rate governance	Phase/config binding; rolling limits; reserve/liability sentinels	Direct
AagentSaleProceedsVault	Sale proceeds custody and release	Sale unlock; delayed beneficiary acceptance; protected addresses	Direct
AagentStakingV1	USDT/BNB intake, maturity and AGNT claim	Deposits default closed; inventory; oracle; reentrancy; beneficiary delay	Direct

Control concentration



INTERPRETATION

Percentages above are design-analysis emphasis indicators, not probability or security scores. Direct-value contracts require production address, bytecode, role and reserve verification before release.

4.2

Interfaces & Dependencies

Typed boundaries and external assumptions

IAgentMarketRegistry	Swap / Redemption / Staking	Read mode, phase, endpoints and version	Registry address and state are authentic
IAgentPurchaseReceiptSource	Redemption	Read wallet purchase entitlement	Receipt source is canonical and final
IAgentRedemptionEndpoint	Registry / clients	Endpoint compatibility and status	ABI and bound address match
IAgentRegistryBound	Endpoints	Registry identity binding	No substitute registry accepted
IAgentSaleProceedsVault	Deployment / Swap	Custody endpoint compatibility	Vault recipient and unlock are configured
IAggregatorV3	Swap / Staking	Chainlink-style feed reads	Round completeness, freshness and bounds hold

Dependency assurance

0

PRODUCTION ADVISORIES

npm audit --omit=dev

11

PRODUCTION FILES

Manifest-bound scope

34

COMPILED FILES

Frozen toolchain

BOUNDARY RULE

A clean npm advisory result is limited to published dependency advisories. It does not establish absence of contract, configuration, integration or operational risk.

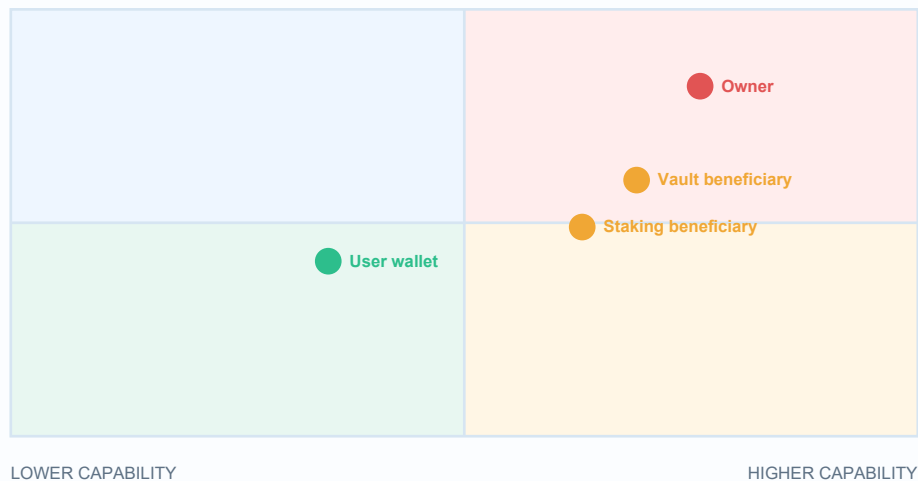
4.3

Privileged Operations

Role capability, delay and release impact matrix

Owner / governance	Registry mode, endpoint and configuration updates	onlyOwner; exact compatibility; health reads	Market availability or misbinding	Needs production role proof
Vault beneficiary	Receive sale proceeds after unlock	Delayed propose / accept; protected-address checks	Custody release destination	Needs funded rehearsal
Staking beneficiary	Receive released staking-side funds	Delayed rotation; checked fixed recipient	Release destination	Needs role verification
Oracle keeper / operator	Observe feed health and trigger safe operating procedures	Multi-feed validation and contract fail-closed checks	Availability / mode response	Off-chain runbook evidence open
User wallet	Submit signed purchase, redemption or staking transaction	Nonce/deadline/chain/mode/phase checks	Own funds only	Runtime wallet control

Privilege risk map



4.4

Function Visibility

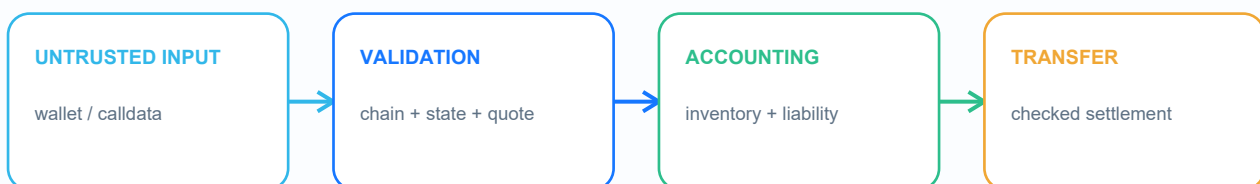
External surface and state-changing entry point inventory

AagentMarketRegistry	14	3	0	14
AagentSwapV2	11	3	4	22
AagentRedemptionV2	18	6	4	17
AagentSaleProceedsVault	7	4	3	4
AagentStakingV1	21	8	5	20

SURFACE ANALYSIS

Counts are mechanically extracted from the frozen source and provide orientation rather than a complete reachability model. Internal calls, inherited OpenZeppelin controls, receive handlers, callback behavior and deployment-time configuration were assessed separately.

Entry-point control ladder



IMPORTANT LIMITATION

Function visibility alone does not prove authorization correctness. Production role assignments and bytecode equality are explicit open assurance gates.

5

Verification Evidence

Compilation, behavioral tests and isolated wrong-chain guard



Compilation + chain-56 tests	frozen run command	34 compiled; 245 pass; 1 intentionally isolated	Local behavior recorded in context
Wrong-chain isolation	frozen wrong-chain run	1 pass; 0 isolated	Chain mismatch evidence recorded
Coverage instrumentation	not collected in final run	No percentage claimed	No stale result reused
Source stability	pre/post SHA-256 window	Hashes match	Evidence run used stable inputs

ISOLATED CASE

The one isolated chain-56 case is intentional: the wrong-chain scenario is executed under a dedicated chain-97 Hardhat configuration, where it passes independently. It is not counted as a failed behavior test.

SCOPE OF PROOF

Tests establish behavior under controlled local fixtures. They do not prove mainnet feed behavior, reserve funding, signer custody, deployed bytecode or post-deployment role configuration.

5.1

Test Depth & Evidence Quality

Exact final-run results without stale coverage percentages



Main suite	245 passing / 1 intentional exclusion	112057d3eaa5f2e1...	PASS
Wrong-chain suite	1 passing / 0 excluded	112057d3eaa5f2e1...	PASS
Compilation	34 Solidity files	54dda9d4ac9d0e6c...	PASS
Instrumentation coverage	Not collected in final run	No earlier run imported	NOT CLAIMED

Future depth priorities

- 1 Compound revert paths where registry mode, feed health, reserve state and quote validity fail simultaneously.
- 2 Boundary transitions around maturity, quote expiry, sale opening/closing and rolling 24-hour redemption windows.
- 3 Adversarial token behavior beyond current fee-on-transfer and reentrancy fixtures.
- 4 Production-fork scenarios using verified deployed addresses, real feed rounds and funded inventories.

NO COVERAGE CLAIM

The final frozen run did not collect instrumentation coverage. This report deliberately excludes percentages from all earlier runs; a future percentage requires its own bound snapshot, build and toolchain hashes.

5.2

Static Analysis

Context-bound Solhint and dependency results

SOLHINT PASS · 0 SOURCE FINDINGS · 0 PRODUCTION ADVISORIES

Static-analysis tool	Solhint	Frozen toolchain execution
Reported source findings	0	No Solhint issue recorded
Open tracked findings	0	9 remediation items verified
Production advisories	0	npm production dependency scope only
Evidence authority	req223-20260731T134906 328Z-c14331b422a13df5	Shared pipeline context; no embedded run identity

INTERPRETATION BOUNDARY

Solhint completed successfully with 0 reported source findings. The production audit recorded 0 advisories; 27 development-toolchain advisories were classified as dev-only and triaged with no unresolved critical finding.

5.3

Remediation Verification

All 9 historical remediation items verified against frozen source

9/9**ITEMS VERIFIED**

Frozen status register

27**DEV ADVISORIES**

Dev-only triage complete

9**COMPLETED RECORDS**

All controls present

0**OPEN FINDINGS**

Zero source findings

Finding index · full detail on pages 19-21

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

ANALYSIS BOUNDARY

SlowMist assessed the remediation evidence against the frozen source, build and toolchain identity. All nine tracked source items are remediated, verified and closed; zero source findings remain open.

6.1

Verified Remediation Records 1 of 3

All records on this page are completed, verified and closed in the frozen source

REMEDIATED · VERIFIED

MED-01

Cumulative redemption threshold enforcement

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

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

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

Source-owner disposition assessed · production evidence and continuing controls remain separate gates

6.2

Verified Remediation Records 2 of 3

All records on this page are completed, verified and closed in the frozen source

REMIEDIATED · VERIFIED

MED-04

Hardened staking oracle validation

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

REMIEDIATED · VERIFIED

LOW-01

Rolling 24-hour redemption limits

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

REMIEDIATED · VERIFIED

INFO-01

Timelock and threshold-Safe ownership gate

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

Source-owner disposition assessed · production evidence and continuing controls remain separate gates

6.3

Verified Remediation Records 3 of 3

All records on this page are completed, verified and closed in the frozen source

REMIATED · VERIFIED

INFO-02

Delayed two-step beneficiary rotation

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

REMIATED · VERIFIED

INFO-03

Complete settlement evidence events

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

REMIATED · VERIFIED

INFO-04

Permissionless matured-position completion

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

Source-owner disposition assessed · production evidence and continuing controls remain separate gates

6.3

Operational Readiness

Production activation gate sequence

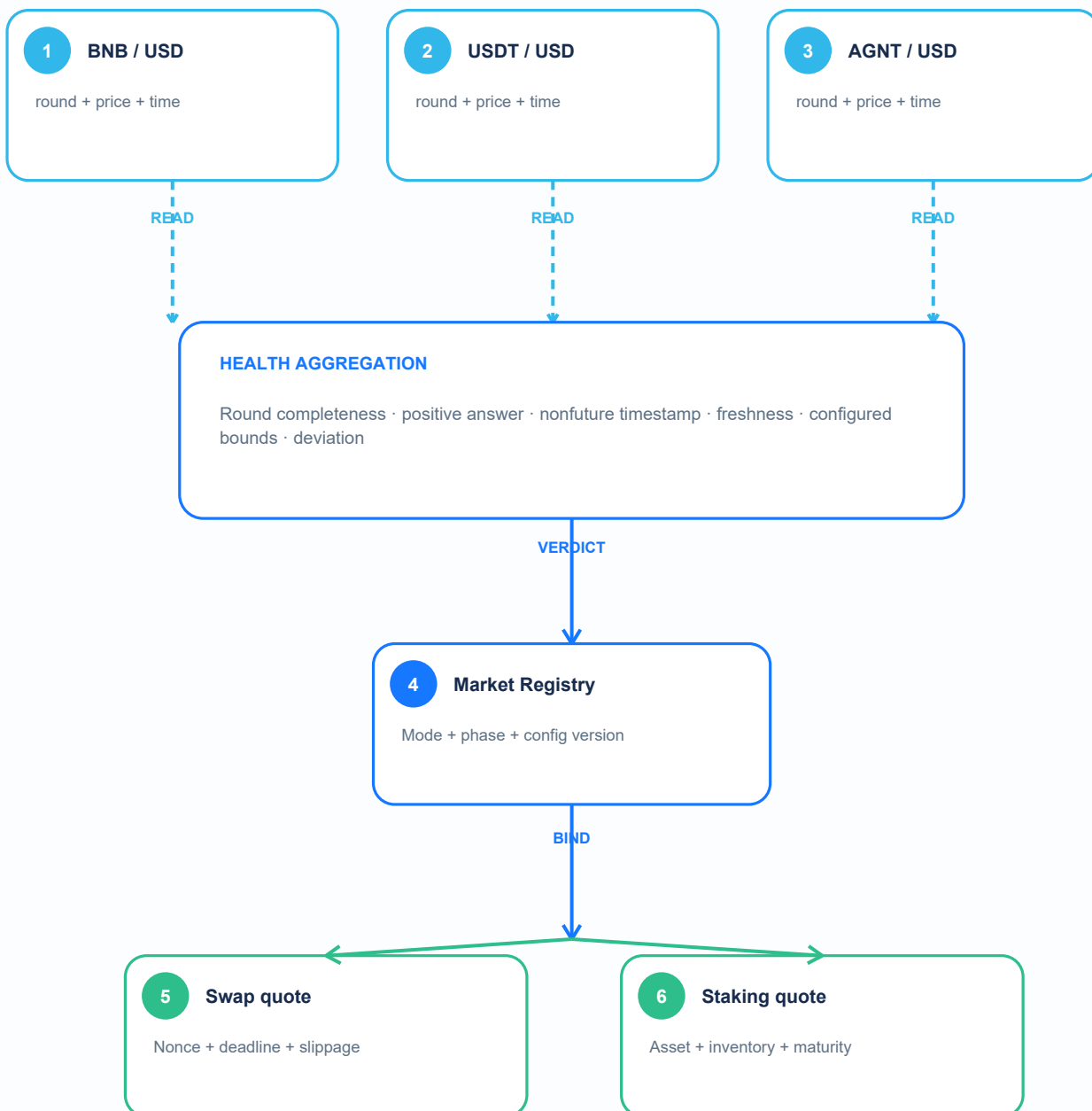


* Source-owner triage assessed against the frozen scope; production closure remains separate.

7.1

Oracle & Market Controls

Multi-feed health, registry mode and quote binding



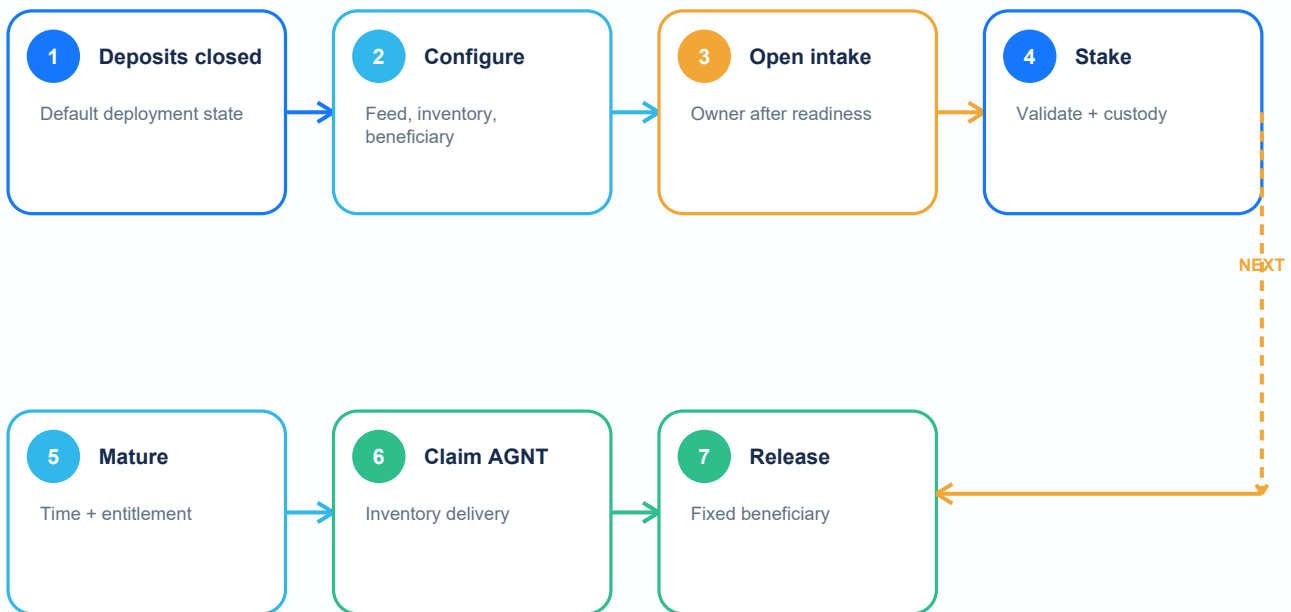
FAIL-CLOSED BEHAVIOR

Unreadable, stale, incomplete, out-of-bounds or mismatched feed state blocks the dependent operation; production feed addresses and live rounds still require deployment-time verification.

7.2

Staking Lifecycle

USDT/BNB intake, maturity, AGNT delivery and proceeds release



Intake	Deposits explicitly open; quote and feed healthy	Revert
Accounting	Actual received amount and inventory capacity	Revert
Maturity	Position exists, unclaimed and time reached	Revert
Claim	AGNT transfer succeeds; claim marked atomically	Revert
Release	Authorized path, fixed recipient, checked call	Revert

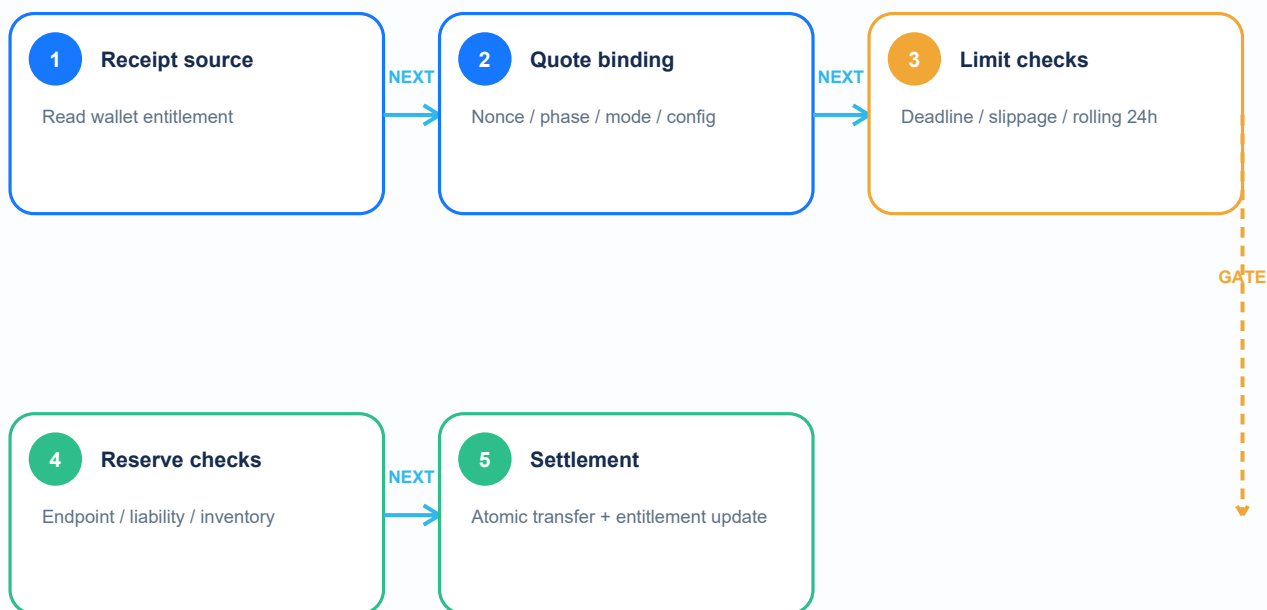
PRODUCTION GATE

The contract now deploys with deposits closed. Opening production intake still requires verified bytecode, configured feeds, funded AGNT inventory, beneficiary proof and operational rehearsal.

7.3

Redemption Lifecycle

Entitlement, quote binding, rolling limits and reserve settlement



Replay and stale-state resistance

Nonce	Single-use authorization	Replayed quote or transaction
Mode + phase	Correct market lifecycle	Execution under stale operating state
Configuration version	Endpoint / policy coherence	Quote made before governance update
Deadline + slippage	Bound execution expectation	Expired or materially changed settlement
Rolling 24-hour limit	Rate-limit redemption exposure	Window-cap excess

ASSURANCE BOUNDARY

Local tests cover these invariants. Production receipt finality, reserve funding, canonical addresses and live role bindings remain outside this evidence run.

8

Assessment Result

Snapshot-bound source assessment with separate activation gates

FROZEN SOURCE ASSESSMENT · VERIFIED

9 TRACKED FINDINGS VERIFIED · 0 OPEN · MAINNET ACTIVATION EVIDENCE SEPARATE

Source identity	Verified locally	11 files; scope root cff85cbf...31651e1
Build and local tests	Evidence recorded	34 compiled; chain-56 245+1; chain-97 1
Coverage	Not collected	No percentage from an earlier run reused
Static analysis	Solhint: 0 findings	Frozen toolchain result
Dev dependency triage	27 advisories	Dev-only; no unresolved critical finding
Remediation register	VERIFIED	9 remediated + verified / 0 open
Production advisories	0	npm production dependency scope only
Mainnet activation evidence	SEPARATE GATE	Addresses, bytecode, roles and live configuration

CONCLUSION

The frozen AEGENT evidence records 9 tracked findings as remediated and verified, with 0 open. SlowMist conducted this point-in-time security assessment and issues this report for the exact frozen scope and evidence identity recorded herein. The result applies to the identified source and evidence run; mainnet addresses, runtime bytecode and live operational configuration require their own activation evidence.

Appendix & Statement

Evidence scope, issuer identity and use limitations

ISSUER

SlowMist is the assessment and report issuer. AEGENT is the assessed project and source-evidence provider. SlowMist conducted this point-in-time security assessment and issues this report for the exact frozen scope and evidence identity recorded herein.

SNAPSHOT BOUNDARY

Conclusions apply only to frozen evidence run req223-20260731T134906328Z-c14331b422a13df5 and the 11-file scope identified by SHA-256 root cff85cbfc727272ccf234a69745299a4f73de007ee6ac7b6f9c6d6b9a31651e1.

AUTOMATED ANALYSIS

Solhint completed with 0 reported source findings. The remediation register remains authoritative and records 9 historical items, all remediated and verified in frozen source, with 0 open.

CHANGE CONTROL

Any source, compiler, dependency, configuration, endpoint, role, feed, reserve or deployment change can invalidate this report and requires a new evidence run.

Snapshot manifest	ae20c397eec2941560d6048ec03746068d3bbf086de780e0cd2256d989c3b902
Source snapshot	cff85cbfc727272ccf234a69745299a4f73de007ee6ac7b6f9c6d6b9a31651e1
Build snapshot	54dda9d4ac9d0e6ce83d2bc863ae05be30e3a71dd6a8faecb8aa31a02afd2d16
Toolchain	89a6096feeea6b0fdc0f7ad564ccdd38e0e042382fd020a4c4d05a5c6ba910de
Finding status	b586fa2c5916ebe964d17a593d20038d40dc8c3959591f2633806c3c55a45117
Triage	7b4943babf25f2c9ae78be34e2563022d4a120dc88eae5b366e20379b94e4bb1
Run summary	112057d3eaa5f2e1c6552fb673b9f0e807406a442af666d84eb50865aba3a011

Evidence manifest SHA-256

ae20c397eec2941560d6048ec03746068d3bbf086de780e0cd2256d989c3b902