About NebulaBunny FREEZE Packages

(Technical Verification Overview)

I. Document Scope and Boundaries

1. Intended Readers: Potential institutional partners, technical due diligence teams, auditors, and investors (read-only).
2. Confidentiality: For read-only verification. No core algorithms or training data are included. Reverse engineering and redistribution are strictly prohibited.
3. Disclaimer: This document does not constitute investment advice. It is provided solely for technical validation and compliance archiving.

II. Quick Start

1. What You'll Get: A clear overview of the four package types (A/B/C/S) and their purposes.
2. How to Choose:
• Use A during the initial interest stage.
• Use B after signing an NDA for due diligence.
• Use C for signed deployment cooperation.
• Use S for heterogeneous or multi-site integration.

III. Overview of the FREEZE Packages

（Details of B/C/S are provided inside the B-package documentation.）

FREEZE_A （Public Demonstration Layer）
1. Deliverables: FREEZE_A_PUBLIC.* (result + manifest + replay_min).
2. How to Verify (the Four-Piece Set):
• Offline replay comparison (normalized diff, ignoring t/ts).
• If you modify any line in poc_data_, the results will immediately fail verification (ZC $\neq$ ALL PASS). Revert the change and it returns to ALL PASS — proving the hash chain works.
• All five fingerprints align (spec / code / data / random / env).
• cosign / sha256 verification passes, and release records can be cross-checked.
3. Usage: See the documentation inside the package.
4. Use Case: Marketing or initial due diligence.
5. Risk / Data Leak: None (no execution logic included).
6. If verification fails or results mismatch: check the FAQ first, then contact technical support.

FREEZE_B

(US $3000 — credited toward C/S upgrade; refundable if technical verification fails.)

1. Audit Pack-Lite (Desensitized Audit Bundle):

• TCA summary slices (no trade details).

• Pre-computed cost/slippage histograms (PNG / CSV).

• Key KPI explanation text (explain_lite.json).

2. Shadow-Delta Drill (Offline Simulation Demo):

• Includes a synthetic "pseudo-live" log (synthetic_live.jsonl, desensitized, fixed random seed) and the corresponding budget TCA.

3. Cost Profile Switch Demo (Low / Med / High):

• Three preset cost curves (JSON).

• Replay only for comparison and explanation; does not alter engine logic.

4. Fail-Explain Mini Report:

• If a "tamper test" is performed, an explain_fail.json (read-only) is generated, showing which assertion failed and by how much.

The B-package is an advanced validation version of A. It helps you evaluate whether to upgrade to C or S deployment collaboration.

Note: The following sections (IV, V, VI) mainly apply to the B package.

C Package （Deployment Cooperation Layer | Standard Image)

S Package （Custom Adaptation Layer | Heterogeneous Stack / Multi-Venue Access)

IV. Reproduction & Security Measures （Preventing Environment-Induced FAILs)

- Works offline and across systems with reproducible results.

- Any file tampering causes instant SHA256 mismatch.

- Uses fixed time windows and desensitized data to prevent replay drift.

- No private algorithms or trade data are ever included.

V. Verifiable Anchors (ZC Assertions）

Case Name	Meaning	Verification Tier
poc_meta_signed	Manifest includes poc_meta and passes SHA256 signature verification	Security / Signature
audit_lite_presence	audit_lite is complete and explain_lite.json has the correct structure	Integrity
shadow_drill_consistency	shadow_drill files are complete and structurally consistent	Integrity
cost_profiles_presence	All three cost profiles and comparison charts exist	Integrity
fail_explain_template_presence	Template and example for fail_explain are present	Integrity
replay_min_filelist_sha	SHA256 verification for all replay_min file entries passes (all green)	Core Hash

When all assertions show PASS, it means the package is intact, signatures are correct, the execution scope is consistent, and no private data was touched.

VI. Tangible Benefits (Direct & Indirect)

1. Visible Trust: Turns "we say it works" into reproducible, verifiable, self-proving evidence — sharply lowering due diligence and negotiation costs.
2. Lets LPs or audit teams view reproducible evidence with zero access to proprietary code.
3. Compliance & Disclosure: The FREEZE package plus verification list can directly serve as audit support material.
4. Operational Efficiency: Shadow and backtest results align quickly; anomalies can be located precisely, reducing trial-and-error cost.

VII. Practical Integration Patterns   (Typical Use Cases)

1. Fee / Rebate Table Integration → Aligns cost models, reducing funding-fee and commission discrepancies.

2. Queue Position & Passive Execution Preference → Tightens the p95 performance band.

3. Slice / Rhythm / Event-Window Optimization → Dramatically shrinks extreme tails.

4. Multi-Venue Primary-Backup Routing → Boosts stability during congestion, compressing tail risk.

5. Optional Near-Real-Time Visualization ("Trusted Self-Proof Chain"):

• Delay + Normalization: Curves start at 1, showing only relative performance; never reveal capital size; delay ≥15 minutes.

• Detail Masking: No exposure of positions or single trades; only drift metric ranges (e.g., p50/p95 bps).

• Triple-Anchor Proof: Short codes of spec_hash / code_git / freeze_sha show match / mismatch status.

• Threshold Alerts (Internal Use): When drift exceeds the limit, an internal alert triggers — never made public.

VIII. Legal & Compliance

1. Documents: LICENSE (for PoC use), NDA / Data Processing Addendum (DPA), and key risk-disclosure notes.

2. Regulatory Notice: Non-advisory, region-compliant, for read-only and delayed educational use.

IX. Contact & Access

General email: 214213973@qq.com (Responses within 24–48 hours on working days, Asia/Singapore time).

To apply for the A package, please use your corporate email and include: company name, contact person, position, intended use, and whether an NDA has been signed — this helps us verify and respond quickly.

X. Customization Options

① Mid-to-Large Private Funds / Hedge Funds
For: compliance filing, LP disclosure, and strategy transparency.
Provides: FREEZE audit package, spec_hash contract traceability chain, shadow-live drift audit.

② Quantitative Fund-of-Funds (FoF)
For: cross-audit of black-box sub-fund strategies.
Provides: FREEZE package reproducibility validation + demo-version replay_min toolchain.

③ Brokerage Asset-Management Units / Prop Quant Teams
For: strict internal model-management and audit-chain requirements.
Provides: Containerized reproducible package, FREEZE manifest, shared-risk-control standards.

④ Third-Party Audit Firms / Accounting Technology Divisions
For: verifying quantitative product performance during regulatory disclosure.
Provides: FREEZE + manifest + replay_min scripts for local KPI recalculation.

⑤ Research Institutes / Financial Engineering Labs
For: experimental reproducibility and academic re-validation.
Provides: Replayable A/B packages + spec_hash-verified publication mechanism.

⑥ Cloud Providers / Compute Platforms
For: trusted backtesting kernels.
Provides: Containerized freeze-runner + offline-verifiable reproducible engine.

⑦ Quantitative SaaS Vendors / Research Collaboration Platforms
For: trusted audit components and client-side confidence.
Provides: FREEZE-API endpoints + read-only triple-anchor verification (spec_hash_short / code_git_short / freeze_sha256_short).

⑧ Private-Fund Registration Agencies / Compliance Consultants
For: proving the source and authenticity of strategies.
Provides: A/B packages (offline verification) + audit-report templates.