CRYLO® Research

Methods Paper (v1.0.0)

Title: Guardrailed AI for Non-Custodial Digital-Asset Portfolios: Methods, Evaluation Protocol, and Public Dataset

Authors:
- Marcel Isler (https://orcid.org/0009-0003-5361-6642)
- CRYLO Research Team
- Collaborators at Lucerne University of Applied Sciences and Arts (HSLU)

Contact: research@crylo.ai

DOI: 10.5281/zenodo.17454874
Release: 2025-11-03

Permalinks:
Paper PDF {{pdf_url}};
Dataset: https://zenodo.org/records/17454874
Code: https://github.com/CRYLOai/ai-wealth-manager

Abstract

We present a transparent overview of CRYLO's risk-first, non-custodial portfolio methodology for digital-asset investors. Our approach combines rules-based portfolio construction, ensemble forecasting, and layered risk controls (volatility targeting, drawdown circuit breakers, and stress-scenario checks). The paper documents **what** is measured, **how** results are validated, and **how** users remain in control of custody—all without disclosing proprietary model internals (e.g., exact thresholds, hyperparameters, or architecture specifics). We release an anonymized dataset of market features and evaluation outputs, plus scripts to reproduce key metrics. Results indicate that under representative market regimes (2019–2025), guardrailed strategies maintain materially lower realized drawdowns at similar or improved risk-adjusted returns versus buy-and-hold baselines. We also detail compliance and reproducibility standards suited for Switzerland, Liechtenstein, and the EU.

1. Introduction

Retail access to digital assets often lacks guardrails common in traditional finance. CRYLO's objective is to deliver disciplined, rules-based portfolios that prioritize downside protection and transparency while preserving user custody. This paper documents our governance, inputs, evaluation protocol, and outputs necessary for independent scrutiny by journalists, researchers, and regulators—deliberately omitting trade secrets that would enable replication of proprietary alpha.

Contributions

1. A **risk-first framework** for non-custodial crypto portfolios.
2. A **public evaluation dataset** and metrics definitions enabling third-party validation.
3. A **compliance-aware, user-centric architecture** (no custody; broker/ramp neutrality).
4. A **replication guide** that proves outcomes without revealing sensitive internals.

2. System Overview (High-Level)

Non-custodial architecture. Users connect accounts/wallets at regulated ramps/brokers; CRYLO's algorithms provide recommendations and automation where permitted, but does not take custody.
Strategy engine. A 3-layer stack:

- **L1: Asset universe & eligibility** (liquidity, venue coverage, compliance filters).
- **L2: Portfolio construction** (rules-based weights bounded by risk bands; diversification across L1/L2 assets; stablecoins for residual risk budget).
- **L3: Guardrails** (volatility targeting, drawdown circuits, regime checks).
  Ensemble forecasting. 13+ models grouped into: momentum/seasonality, market-microstructure, cross-asset macro proxies, and risk-state classifiers. We disclose families and validation logic but not architectures, features weights, or hyperparameters.

3. Data Sources & Preprocessing

Markets. OHLCV and order-book snapshots for large-cap digital assets from multiple exchanges with exchange-quality filters.
Derived features. Range/volatility estimators, liquidity/impact proxies, term-structure approximations, and cross-asset signals (macro proxies).
Cleaning. Venue outlier removal; clock alignment to UTC; stablecoin depegs flagged; stale quotes filtered.
Anonymization. No client data is included. Dataset contains only public-market features and model evaluation outputs.
Licensing. Data: CC-BY 4.0 with permitted-use notes; Code: Apache-2.0 (examples only).

Dataset artifacts (this release)

- `/data/market_features.parquet` — aggregated feature table (minute/hour/day bars; see schema).
- `/data/eval_labels.parquet` — regime labels and realized outcomes for benchmark tasks.
- `/eval/baselines/` — baseline strategies (buy-and-hold, equal-weight, risk-parity proxy).
- `/eval/metrics.py` — metric implementations matching this paper.

- `/repro/repro.sh` — end-to-end regeneration script.

Feature schema (excerpt)
`timestamp_utc | asset | venue | px_open | px_high | px_low | px_close | volume | vwap | roll_vol_1d | roll_vol_7d | roll_corr_btc | liq_proxy | spread_bps | funding_est | regime_proxy`
Note: Additional engineered features used in production are omitted or obfuscated to prevent reverse engineering.

4. Portfolio Construction (Disclosed Rules)

- **Universe selection:** top-liquidity assets across approved venues; assets failing compliance/liquidity screens are excluded.
- **Risk budgets:** predefined bands per risk profile (Very Low → Very High).
- **Weighting:** rules-based weights with caps per asset/category; minimum stablecoin buffer for risk control.
- **Rebalance cadence:** periodic with drift thresholds; event-driven on guardrail triggers.

We do **not** disclose exact caps, drift thresholds, or mapping from model outputs to weights.

5. Guardrails & Risk Controls (Mechanisms Only)

Volatility targeting. Target ex-ante volatility within a band per risk profile using an EWMA-style estimator and scale factor (s_t). (Exact decay/targets redacted.)
Drawdown circuit breakers. If peak-to-trough drawdown exceeds a profile-specific band over rolling windows, exposure scales down to a floor (\alpha_{min}) for a cooldown period (\tau). (Thresholds redacted.)
Stress scenarios. Synthetic shocks (gaps, liquidity crunch, depeg) are injected into backtests; portfolios must satisfy max loss bounds under these scenarios to pass.
Position limits. Hard caps per asset/venue; concentration and turnover constraints.

6. Modeling (Family-Level Disclosure Only)

Ensemble of 13+ AI/ML models across four families:

1. **Trend & seasonality:** multi-horizon trend filters, intraday/weekly seasonality models.
2. **Microstructure:** order-book imbalance signals (venue-normalized), spread/liquidity state classifiers.
3. **Cross-asset/macro proxies:** PCA-compressed risk factors including BTC/ETH dominance, risk-off proxies.
4. **Risk-state classifiers:** regime detection (calm, volatile, crisis) feeding guardrails.

Omissions (intentional): precise architectures (e.g., feature sets, window sizes), training targets, regularization schemes, and ensembling weights are **not disclosed**. The open dataset provides **evaluation labels** and **baseline predictions** only.

7. Evaluation Protocol

Backtest periods. Rolling windows 2019-2025 with walk-forward evaluation; exchange survivorship bias controls.
Benchmarks. (i) BTC buy-and-hold, (ii) top-N equal-weight, (iii) risk-parity proxy fixed to public vol proxies.
Reproducibility. Deterministic seeds; transaction cost model; venue outages simulated; funding/fees included.
Out-of-sample. Walk-forward with expanding training set and fixed test slices; **no** look-ahead features.
Stress tests. Shock scenarios as in §5.
Leakage checks. Timestamp alignment audits and forward-fill guards.

8. Metrics (Definitions)

- **Annualized Return (AR)**, **Annualized Volatility (AV)**, **Sharpe** (rf≈0), **Sortino**.
- **Max Drawdown (MDD)** and **Calmar**.
- **Rolling 90-day MDD** distribution.
- **Hit Ratio**, **Tail Ratio (95th/5th)**.
- **Value-at-Risk (VaR)** and **Expected Shortfall (ES)** (historical).
- **Turnover** and **Implementation Shortfall**.
- **Uptime** (days within guardrail bands).
- **Compliance flags** (asset/venue eligibility adherence).

Metric formulas and reference implementations are included in `/eval/metrics.py`.

9. Results (Summary; No Proprietary Internals)

We report aggregated results over all risk profiles and test slices; full tables are in the repository.

- Guardrailed strategies exhibit **lower median and tail drawdowns** versus baselines across market regimes.
- Risk-adjusted performance (Sharpe/Sortino) is **competitive or higher** with **lower volatility** for low/medium risk bands.
- Stress scenarios confirm **bounded losses** within predefined envelopes.

Note: Exact parameter values, model weights, rebalancing thresholds, and mapping from regimes to exposures remain confidential.

10. Compliance & Non-Custodial Design

- CRYLO does **not** take custody. Execution and custody occur at user-selected third-party providers.
- Strategy recommendations adhere to jurisdictional eligibility and asset filters.
- Audit trails: timestamped recommendations, configs, and guardrail states are logged (hashed) for attestations without revealing IP.

11. Limitations & Risks

- Digital-asset markets are subject to structural breaks; past performance is not indicative.
- Dataset redactions may limit exact replication of production results; evaluation parity is provided via baselines and metrics.
- Exchange data quality varies; we apply filters yet residual noise may remain.
- Non-custodial setups rely on third-party availability.

12. Ethics & Transparency

We publish metrics, datasets, and code sufficient for scrutiny of **outcomes and guardrail effectiveness**, while withholding sensitive details that would enable cloning. We will accept responsible-disclosure reports for any issues in data or evaluation code.

13. Reproducibility Checklist

- `repro.sh` runs end-to-end on a clean environment.
- All metrics match this paper's definitions.
- Deterministic seeds documented.
- Costs/fees/funding modeled and declared.
- No look-ahead or leakage (tests included).
- Figures regenerate from code.
- Dataset card completed (below).

14. Dataset Card (Template)

Name: CRYLO-Public-Eval-v1.0.0
DOI:
Slices: Minute/Hour/Day bars; assets: BTC, ETH, large-cap index proxy.
Time range: 2019-2025
Fields: see schema in §3.
Provenance: Consolidated from {{providers_list}}; cleaned per §3.
Intended use: Academic/journalistic evaluation of risk-control outcomes and baseline comparisons.
Out-of-scope: Trading advice; production deployment.
Licenses: Data CC-BY 4.0; Code Apache-2.0.
Ethics: No personal data; no wallet identifiers; only public-market series.
Known gaps: Some venues/assets filtered; engineered features redacted or obfuscated.
Contact: research@crylo.ai

15. How to Cite

Isler, M., & CRYLO Research. (2025). CRYLO Research: Methods & Evaluation Kit (Version v1.0.0) [Computer software]. DOI: https://doi.org/10.5281/zenodo.17454874. Available at: https://github.com/CRYLOai/ai-wealth-manager

16. Appendix A: Pseudocode (Redacted)

```
# Volatility Targeting (structure only; parameters redacted)
for each rebalance_date:
    sigma_hat = ewma_vol(returns, decay=<redacted>)
    scale = target_vol(<redacted_band>) / max(sigma_hat, eps)
    w_scaled = clip(w_base * scale, lower=<redacted>, upper=<redacted>)
# Drawdown Circuit (structure only)
if peak_to_trough(window=<redacted>) > dd_band(<profile>):
    exposure = max(exposure * <redacted>, alpha_min)
    lockout = <redacted_tau>
# Regime Classifier (signals omitted)
state = classifier(features=<redacted>)  # calm / volatile / crisis
exposure = exposure_policy(state, profile=<redacted>)
```

17. Appendix B: Compliance Notes

- Non-custodial model with third-party on/off-ramps; execution subject to provider terms and local regulations.
- Strategy recommendations and eligible assets filtered by jurisdictional rules.
- This paper is informational; it is **not** investment advice.

18. Release Notes

- V1.0.0 (this draft): Initial public methods description; dataset/eval baselines included; proprietary internals withheld.