

Known issues — audit contest

This document describes **known economic behavior of the Metric OMM bin design**:

Findings that only restate this oracle-shock + two-leg cycle drain are **not eligible for reward**.

1. Summary

Topic	Status
Oracle update rescales bin price bounds; reserves unchanged until a trade	Known
Attacker two-leg cycle $s \rightarrow \text{intermediate} \rightarrow s$ can extract fair value after oracle shock	Known
Loss scales with bin width, shock size: ees reduce drain;	Known

2. Example (USDC / USDT)

Parameter	Value
token0	USDC
token1	USDT
Initial oracle / fair price	1.00 USDT per USDC
Bin bounds	$\pm 1\% \rightarrow p_{\text{lower}} = 0.99, p_{\text{upper}} = 1.01$
Initial bin position	0.5 (centered)
token0Amount (USDC)	1 000 000
token1Amount (USDT)	1 000 000

3. Exaggerated oracle shock (×1000)

Extreme shock so the mechanism is easy to follow. Real oracle moves are much smaller; the **same logic** applies (see §4).

3.1 After oracle moves 1 → 1000

	Before	After shock
Fair price	1.00	1000
p_lower / p_upper	0.99 / 1.01	990 / 1010
Stored bin position	0.5	0.5 (unchanged)
token0Amount / token1Amount	1M / 1M	1M / 1M
Price at cursor	1.00	1000 (= fair)

The pool **quotes fair price** at the cursor, but **equal 1M / 1M reserves are "disbalanced"** for $P = 1000$.

v before attack: **1 001 000 000**.

3.2 Attack: two-leg cycle 0.5 → 0 → 0.5

Leg 1 — pool sells all USDT (cursor left):

USDT out	1 000 000
USDC in	~1 005
Cursor	0.5 → 0

Leg 2 — pool sells USDC (cursor back to center):

USDC out	~500 503
USDT in	~498 000 013
Cursor	0 → 0.5

3.3 Pool loss (fee = 0%)

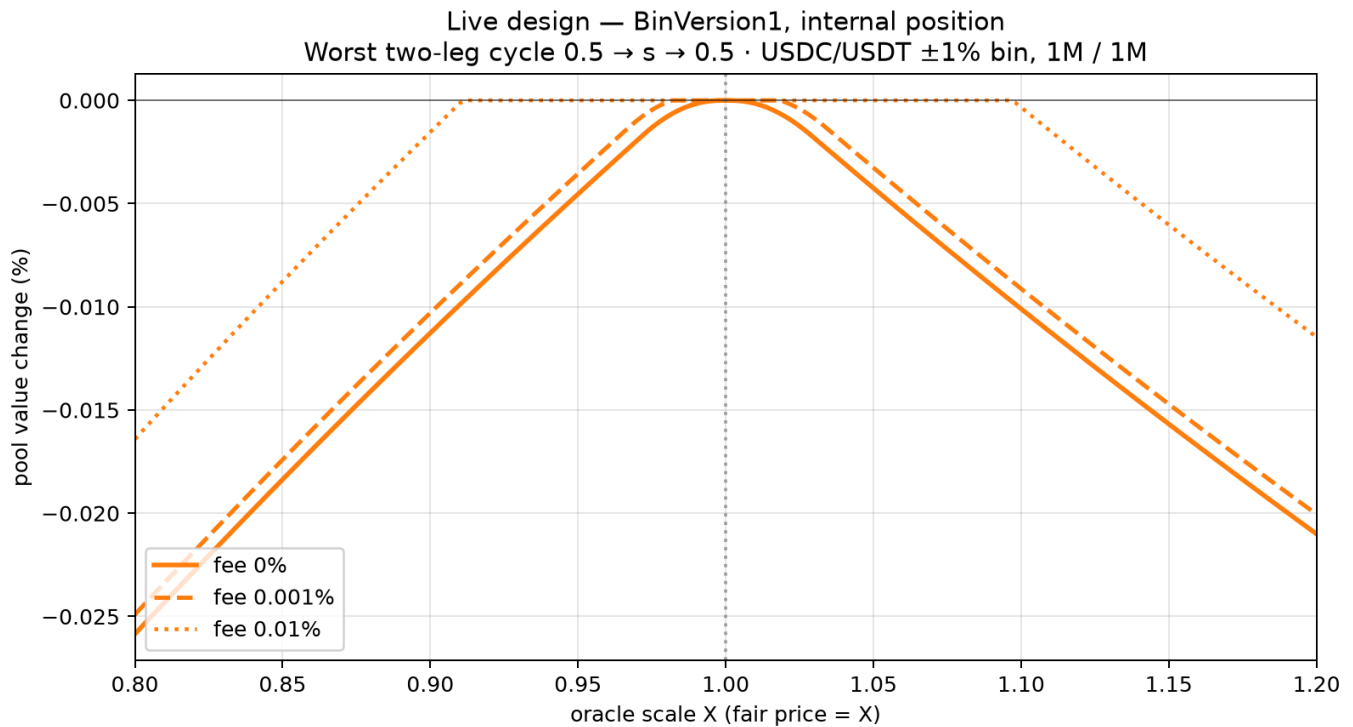
	Value
V before cycle	1 001 000 000
V after cycle	998 502 538
Absolute loss	~2 497 462
Relative loss	~0.25%

4. Realistic oracle range ($X \in [0.8, 1.2]$)

Same pool (internal position, BinVersion1, 1M / 1M, $\text{binPos} = 0.5$). **Worst two-leg cycle** $0.5 \rightarrow s \rightarrow 0.5$ vs oracle scale X :

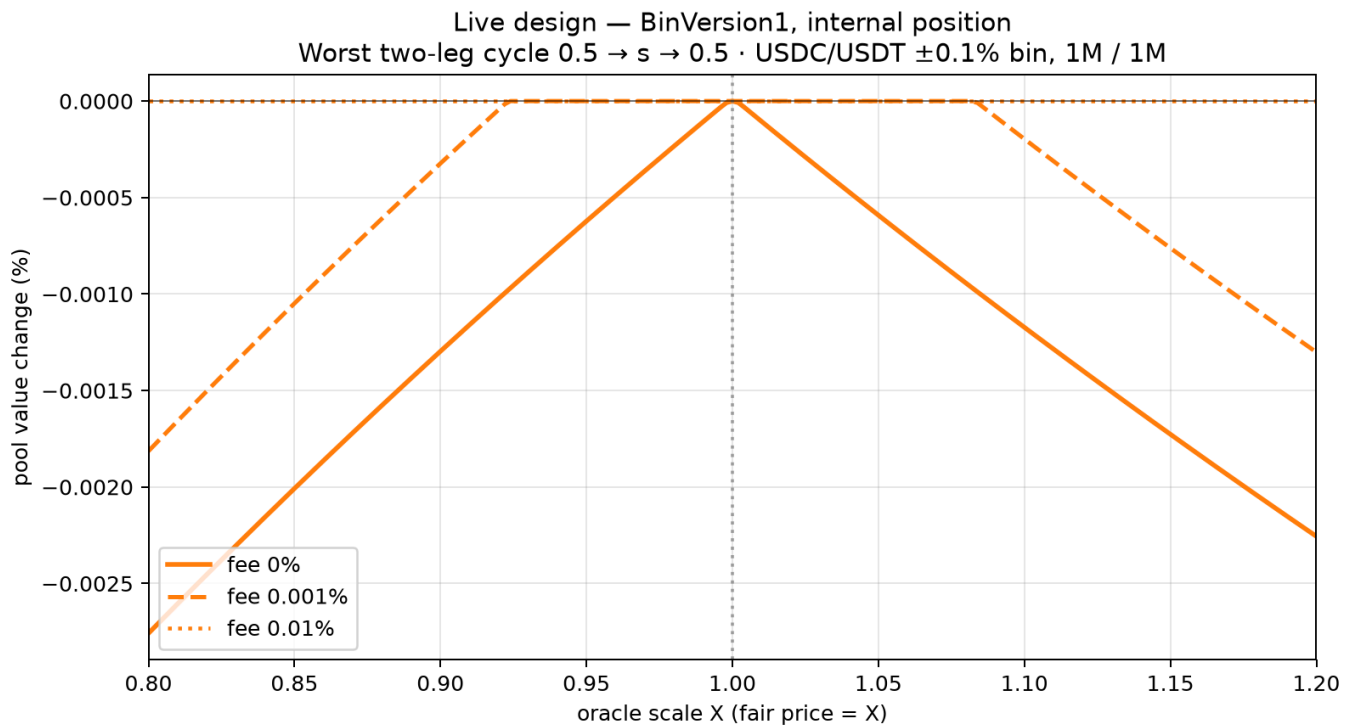
- **Solid** — 0% fee
- **Dashed** — 0.001% fee
- **Dotted** — 0.01% fee

$\pm 1\%$ bin ($p_{\text{lower}} = 0.99$, $p_{\text{upper}} = 1.01$)



X	0% fee	0.001% fee	0.01% fee
0.8	~-0.026%	~-0.025%	~-0.016%
1.1	~-0.010%	~-0.009%	~-0.0003%
1.2	~-0.021%	~-0.020%	~-0.011%

$\pm 0.1\%$ bin ($p_{\text{lower}} = 0.999$, $p_{\text{upper}} = 1.001$)



At $X = 1$ there is no shock and no loss. Narrower bins reduce drain for the same oracle move.

5. Mitigations (parameter levers, not in-scope fixes)

1. **Trading fees** — reduce attacker edge (see plot).
2. **Narrower bins** — less geometry mismatch per shock.
3. **Oracle quality / update bounds** — limit effective x between trades.

Out of scope: restating that after an oracle shock, there exists an attack that can drain up to $(p_{\text{upper}} / p_{\text{lower}} - 1) \times 100\% / 2$ (half the bin's relative price width).