PUBLIC SAMPLE — REDACTED · client identity removed; ▮▮ bars mark removed identifiers · methodology & findings intact

ARI

ECONOMIC MODELING ADDENDUM

ECONOMIC MODELING ADDENDUM — [redacted] · Track T3 — Treasury-yield pool + factory

PROJECT	TRACK	DATE
[redacted]	T3	8 May 2026
TYPE	**SCOPE**	**CLASSIFICATION**
Structural modeling	Full-tier (in scope)	PUBLIC SAMPLE

Disclaimer. This economic addendum is structural mechanism modeling, not a forecast, a solvency certificate, or formal verification. Models are parameterized on the configured/observed parameters and sweep unobservable off-chain inputs across ranges to mark the safe region; no probabilities of real-world events (defaults, runs, price moves) are asserted. It is a companion to the security review and penetration-test reports for the same track and is in scope for the Full tier. Not investment, legal, or financial advice. [redacted] may publish or share this report in full, unmodified form, including this disclaimer.

00 MASTER VARIABLES

The reward engine emits per token, undiluted by supply, and is funded from a **shared** off-chain-topped factory reserve. Two variables govern both the honest funding requirement and the abuse ceiling.

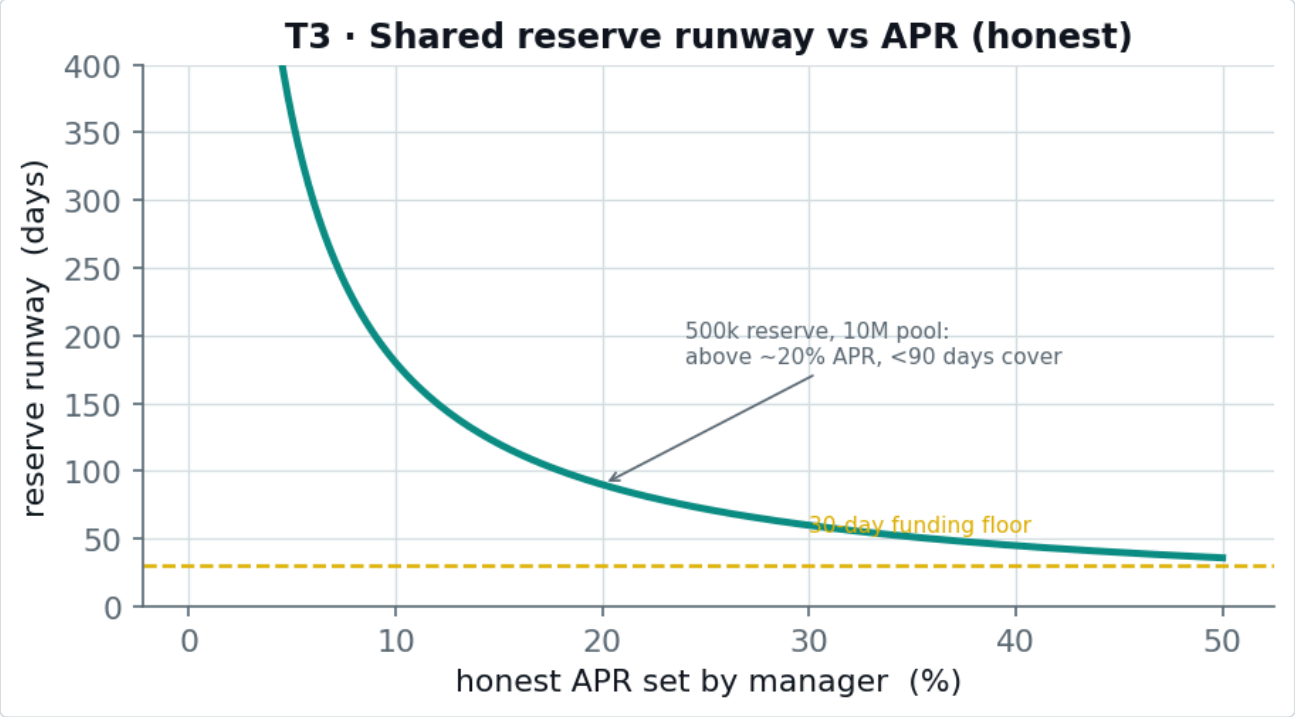
APR rate r (unbounded). A manager-settable uint256 with no cap. Emission = supply·r·t. r governs both the honest funding burn and — because it is unbounded — the single-block drain and the overflow-brick threshold.

Shared reserve F. One factory balance funds *all* pools' rewards with no per-pool sub-accounting, so one pool's emission draws down the pot backing every other pool. Runway = F / emission.

01 MODEL SET

SHARED RESERVE RUNWAY (HONEST OPERATION)

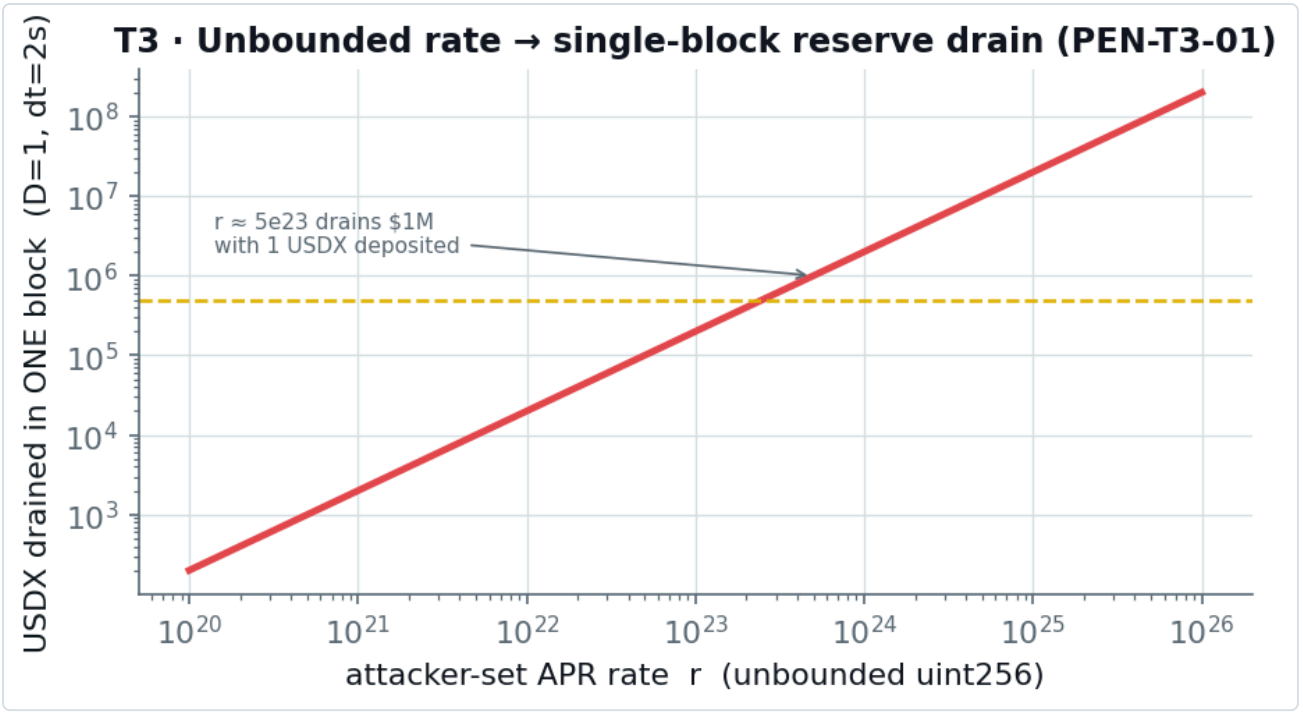
Even with an honest APR, the undiluted emission grows linearly with TVL and the reserve is shared. A $500k reserve against a $10M pool gives under ~90 days of cover above a 20% APR — and any second pool draws the same pot. Funding is an off-chain responsibility with no on-chain guarantee.



Shared-reserve runway vs the honest APR (10M pool, $500k reserve)

UNBOUNDED-RATE SINGLE-BLOCK DRAIN (PEN-T3-01)

Because emission is per-token and undiluted, a manager needs only a trivial deposit and one block: stolen S = D·dt·r/1e18. With 1 [redacted] deposited and a 2-second block, r ≈ 5e23 drains $1,000,000 from the shared reserve in a single block — starving every other pool. The bound is only the reserve balance.



[redacted] drained in one block vs the attacker-set rate (D=1, dt=2s)"/>
[redacted] drained in one block vs the attacker-set rate (D=1, dt=2s)

OVERFLOW BRICK THRESHOLD (PEN-T3-02, STRUCTURAL)

The accrual computes supply_wei·(dt·r) before dividing by 1e18, so under 0.8 checked math it overflows when supply_wei·dt·r > $2^{256}-1$. For a 1-token pool and a 1-second step that boundary is $r \approx 1.16 \cdot 10^{59}$. Above it, every deposit/withdraw/transfer reverts and the reset path — which accrues before it can lower the rate — overflows too, so the pool is **permanently** bricked. The entire abuse region (drain and brick) sits inside the unbounded rate.

02 SURFACE RANKING

S = existential · A = severe · B = bounded. Both S-vectors are manager-privileged (not permissionless), but the manager key is a hot operational key.

	VECTOR	WHY
S	**Unbounded-rate cross-pool drain / brick**	No MAX_RATE ⇒ a manager+accomplice drains the shared reserve in one block or overflow-bricks a pool with a self-locking reset. Hub vector — both live inside the unbounded rate.
A	**Reserve insolvency (honest over-set)**	Undiluted per-token emission + shared reserve + off-chain funding ⇒ a high honest APR or TVL growth exhausts cover and cross-defaults other pools.
B	**KYC principal leak**	withdraw()/transfer ungated ⇒ compliance bypass on principal (not rewards) — regulatory, not solvency.

03 STANDOUT ACTION

Highest-leverage change: a single MAX_RATE bound on the rate setters. It closes the entire S-vector at once — the drain becomes bounded and the overflow-brick becomes unreachable — and it also caps the honest emission so the reserve runway is calculable. Pair with per-pool reserve sub-accounting (so one pool cannot draw another's funding) and a timelock/multisig on the factory owner and beacon upgrades.