In-Class Activity: TBM2 — DAO Proposal Design — SOLUTIONS

Digital Finance – BSc Course — Prof. Dr. Joerg Osterrieder

Trustless Business Models | 15–20 min | Groups of 3

Context: BridgeDAO — 10 M BRG supply, \$40 M treasury, 4 % quorum of supply (400,000 BRG), > 50 % YES to pass.

Exercise 1 (sample proposal):

BIP-17: Fund Independent Security Audit (Q2 2026). *Rationale:* BridgeDAO holds \$40 M treasury + processes \$250 M monthly volume; cross-chain bridges lost \$2 B in 2022 (Ronin, Wormhole, Nomad). An independent audit is cheap insurance. *Budget:* \$5 M USDC from treasury — disbursed in 3 milestones (\$1 M scoping, \$3 M main audit, \$1 M re-test after fixes). *Success metric:* audit report published within 120 days; all critical findings fixed before release.

Exercise 2 (completed): Quorum = 400,000 BRG. Pass = quorum met AND YES > NO.

Case	YES	NO	Total cast	Quorum?	YES %	Passes?
α	250,000	80,000	330,000	**NO**	75.8 %	**FAIL (no quorum)**
β	310,000	120,000	430,000	**YES**	72.1 %	**PASS**
γ	180,000	450,000	630,000	**YES**	28.6 %	**FAIL (YES ¡ 50 %)**
δ	2.10 M	1.90 M	4.00 M	**YES**	52.5 %	**PASS**

Note case α: despite 75.8 % YES the proposal fails — apathy beats consensus. Only ∼ 3 % of supply voted, below the 4 % floor.

Exercise 3 (completed):

(a) **Quorum:** 800,000 BRG cast > 400,000 threshold → **YES, quorum met**.

(b) **Majority:** with 0 NO votes, YES % = 100 % → **PROPOSAL PASSES**. Attacker drains \$40 M treasury.

(c) Two design changes (pick any reasonable two):

(c.1) **Vote-escrow / timelock:** require tokens to be locked for ≥ 7 days before they can vote (flash-loaned tokens would need to be held past the loan horizon).

(c.2) **Execution delay (timelock controller):** any passing proposal is queued for 48 h before execution, letting the community veto a malicious proposal via a counter-vote or emergency pause.

- Other valid answers: snapshot voting at a historical block (prevents vote with just-bought tokens); quadratic voting (cost scales as n^2); conviction voting (power accrues over time held); delegated voting councils with identity requirements.

Debrief: "One token one vote" makes governance *tradeable* in the same market as any other asset. Beanstalk (Apr 2022) lost \$182 M to exactly this pattern — the fix is to make voting power *illiquid* at the moment of voting: timelocks, snapshots, or escrows.

Answer Key **E1:** Sample BIP with title/rationale/budget/metric (see above). **E2:** α FAIL (no quorum), β PASS, γ FAIL (YES < 50 %), δ PASS (52.5 %). **E3:** (a) quorum MET, (b) passes with 100 % YES, treasury drained. Fixes: timelock + snapshot / vote-escrow / execution delay. Lesson: liquid governance tokens + instant execution = **attack surface**. Beanstalk \$182 M (2022) is the canonical example.