In-Class Activity: TBM2 — DAO Proposal Design

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

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

Context: DAOs coordinate thousands of strangers via on-chain token votes. Real participation is typically only 3–5 % of holders, and governance tokens are tradeable — opening the door to flash-loan governance attacks (Beanstalk 2022 drained $182 M in minutes). **Your DAO:** "BridgeDAO" — operates a cross-chain bridge. **Token supply:** 10 million BRG. **Treasury:** $40 M USDC. **Quorum rule:** $\geq 4\,\%$ of supply must vote YES + NO. **Pass rule:** $> 50\,\%$ YES of votes cast.

Exercise 1: Draft a Proposal In 3–5 short bullet lines write a BIP (BridgeDAO Improvement Proposal) that would spend $5 M of the treasury on a security audit. Include: title, rationale, budget, and a 1-line success metric. Write directly in the box below.

Exercise 2: Quorum & Participation Math Fill in the table. Quorum threshold = 4 % of 10 M = 400,000 BRG. Proposal passes if (a) quorum hit AND (b) YES > NO among cast votes.

Case	YES (BRG)	NO (BRG)	Total cast	Quorum met?	YES %	Passes?
α	250,000	80,000				
β	310,000	120,000				
γ	180,000	450,000				
δ	2,100,000	1,900,000				

Exercise 3: Governance Attack Analysis An attacker takes a $60 M flash loan, buys 800,000 BRG on DEXs, submits a malicious proposal that would drain the treasury to their address, votes YES with all 800,000, then repays the flash loan after the block. (a) Does this pass quorum? (b) Does it pass the majority rule if no one else votes? (c) List **two** design changes BridgeDAO could adopt to prevent this. Write them on the lines below.

(a) _____

(b) _____

(c.1) _____

(c.2) _____

Debrief: Why does "one token one vote" become a liability when tokens are cheap, liquid, and borrowable by the minute?