In-Class Assignment TBM5: Governance Capture

Digital Finance – BSc Course Prof. Dr. Joerg Osterrieder

Context. A DAO uses 1-token-1-vote governance. Token GOV has 100M circulating supply at \$1.00 each (\$100M FDV). A proposal passes if it attracts *yes*-votes equal to 33% of supply (quorum *and* majority combined, for simplicity). Governance actions execute *instantly* on pass — no timelock. A flash-loan lender offers overnight GOV liquidity at 0.09% per loan (9 bps, repaid in the same transaction). This is the Beanstalk (Apr 2022, \$182M) setup.

Q1. An attacker wants to pass a malicious proposal that drains the DAO treasury. Compute the *dollar* cost of the flash-loan needed to meet the 33% threshold, and the fee paid to the flash-loan lender.

Solution. Tokens needed = $0.33 \times 100\text{M} = 33\text{M}$ GOV. Dollar notional of the loan = $33\text{M} \times \$1.00 = \$33\text{M}$. Flash-loan fee = $0.0009 \times \$33\text{M} = \$29{,}700$. The attacker votes *yes* with the borrowed tokens, the malicious proposal executes *in the same transaction*, the treasury is drained, and the flash loan is repaid — all atomically. Economic attack cost: ≈\$30k to steal the treasury.

Q2. Contrast instant execution vs. a 48-hour timelock. In 1–2 sentences, explain why the timelock defeats the flash-loan attack.

Solution. A flash loan lives for exactly one transaction — borrow, vote, execute, repay — so instant execution is the precondition that makes the attack economically viable. A 48-hour timelock forces a 2-day delay between *pass* and *execute*, during which the attacker must actually *hold* 33M tokens on-balance-sheet (\$33M of capital for 2 days), and honest token-holders can observe the queued transaction and counter-vote, fork, or pause the contract via guardian multisig.

Q3. Propose *one* additional DAO constitutional safeguard (beyond timelocks) that hardens the protocol against governance capture.

Solution. Any one of: (i) **Guardian / veto multisig**: a small, elected council can cancel any queued malicious proposal during the timelock window, trading pure decentralisation for crisis resilience (Uniswap, Compound). (ii) **Voter-turnout quorum**: require ≥X% of circulating supply to *vote* (not just *pass*), raising capital required from 33% to ≥50% and blocking low-turnout coups. (iii) **Token-lock / conviction voting**: voting weight grows with lock duration, so flash-borrowed tokens (0 s lock) carry zero weight (Curve veCRV, Compound Finance). (iv) **Snapshot block lag**: voting power is measured at a block *before* the proposal was submitted, so flash-borrowed tokens never count.