투표 조작방지 방법들

1. 투표권 스냅샷(Voting Power Snapshot): 거버넌스 투표 시작 시점 혹은 사전에 정해진 특정 블록 시점의 토큰 보유량이나 지분을 기준으로 투표권 확정
2. Whale Attack 방지: 투표 직전 토큰 대량매수 and 투표 직후 대량매도 방지
3. 공정성 확보: 투표 시작후 보유량이 변해도 모든사람의 기준시점이 동일하니 결과 왜곡이 없음.
4. 투표 중 실시간 토큰 이동 추적 불필요
5. 작동 방식: 스냅샷 블록 설정 🡪 투표권 확정 🡪 투표 진행
6. 위험: 스냅샷 직전까지는 매수매도 공격 가능 + 투표권 고정으로 보유 인센티브가 낮아질수 있음 + 유동성 낮은 토큰은 스냅샷 직전 가격조작 위험
7. (쿼럼) Quorum: 전체 투표권 중 최소 몇%이상 참여해야만 안건이 통과 🡪 근데 이건 최소 몇 %를 주작단들이 차지할 수 있어서 효과적인지는 잘 모르겠다.
8. 멀티시그(Multisig) 보안: 리밸런싱같은 민감한 실행 명령은 투표만으로 즉시 실행하지 않고 다중 서명자 그룹이 2차 검증
9. 적용 구조 예시
10. 거버넌스 투표
    * 예: DAO 토큰 보유자들이 특정 자산 비중 조정(리밸런싱)에 찬반 투표.
    * 투표 종료 후 “실행 제안(Proposal Execution)” 상태가 됨.
11. 멀티시그 검증 단계
    * 투표 결과가 유효(쿼럼·과반 등)하더라도, 바로 스마트컨트랙트에서 리밸런싱 실행 X.
    * 사전에 지정된 멀티시그 서명자 그룹(예: DAO 재무팀 5명 중 3명)이 결과를 검증하고 서명.
      + 검증 내용:
        - 투표 결과가 조건을 충족했는지
        - 실행 시 기술적 오류나 보안 취약점 없는지
        - 리밸런싱 대상 자산·비율이 맞는지
    * 서명자가 기준치(M-of-N) 이상 동의해야 실행 가능.
12. 실행
    1. 멀티시그 서명이 완료되면, 스마트컨트랙트가 자산 매매·이동을 실행.
    2. 실행 과정도 온체인 기록으로 남아 투명성 확보.
13. 타임 락(Time Lock): 투표가 끝나도 바로 실행하지 않고 정해진 대기시간을 거친 뒤 실행 가능. 🡪 악성 제안 차단 및 긴급 대응 가능+ 커뮤니티가 사각지대를 검토하고 투표 취소할 수 있는 기회 확보
14. 예시 흐름: 투표 개시 → 스냅샷 기준 투표권 확정 → 투표 종료(쿼럼 충족) →

타임락 기간(예: 48시간) → 멀티시그 서명자 검증(M-of-N) → 실행

1. 일반적인 DAO 방어 전략
   * 1. 시간 가중 스냅샷(Time-Weighted Snapshot): 일정 기간 동안의 평균 보유량을 기준으로 투표권을 계산 🡪 플래시론 방어 전략
     2. 암호화 투표 (Shielded Voting): Snapshot 기반 거버넌스에 암호화된 투표 방식(ShutterProtocol 기반)을 적용. 🡪 투표 결과가 사전 공개되지 않기에, 초기 투표 흐름을 보고 다수파가 몰리는 전략적 투표 방해 가능성이 줄어듦.