Audit

git : https://github.com/kaymin128/Dex_solidity/blob/main/src/Dex.sol

commit : `1b37751893d23ec3119147f4e8e6d804fb40d1d1`

ID	요약	위험도
KAY-001	컨트랙트에서 LP토큰이 존재하지 않습니다.	Critical

Description

이 컨트랙트에서는 **LP 토큰을 발행하거나 소각하는 로직이 없습니다**.

Impact

Critical

LP 토큰이 없으면 유동성 제공자의 지분은 DEX 내에서만 유효하며, 외부에서 거래나 양도가 불가능해집니다.

Recommendation

- ERC20을 상속받아 LP 토큰 발행

ID	요약	위험도
KAY-002	`addLiquidity` 함수에서 유동성 비율 계산 없이 유동성 풀에 추가됩니다.	High

Description

`addLiquidity` 함수는 사용자가 두 개의 토큰(`amount_x` , `amount_y`)을 제공하여 유동성 풀에 추가할 때, 현재 유동성 풀의 비율에 따라 `amount_x` 와 `amount_y` 를 계산하지 않고 바로 추가합니다.

이는 유동성 풀의 균형을 고려하지 않은 방식입니다.

Impact

High

공격자가 풀의 비율을 조작하려면 **상당한 자산이 필요**하며, 이로 인해 공격 비용이 높을 수 있습니다.

하지만 **풀 비율을 충분히 조작시킬 수 있다면**, 공격자는 막대한 이익을 얻을 수 있습니다.

Recommendation

- 유동성 풀 비율 검증 로직 추가