**Dodo contract:**

Dodo is a DAO that customers deposit funds and gain interest. Dodo allows users to ask for a flash loan that they need to return at the end of the transaction, if they didn’t the transaction should revert. Attacker noticed that the *init* function is public and allow every one to change the type of coins used.

The attacker took a flash loan, when the Dodo contract asks to return it, the callee function that supposed to return the funds first change the tokens type and returns the loan with the new token, which worth nothing and the Dodo contract counts it as it was the real token.

Text

Description automatically generated

At the marked line the attacker get control and use the public *init* function to change the tokens type.

The invariant broken is that token0 and token1 shouldn’t change during flashLoan call. This invariant should be true also for deposit and withdraw functions.