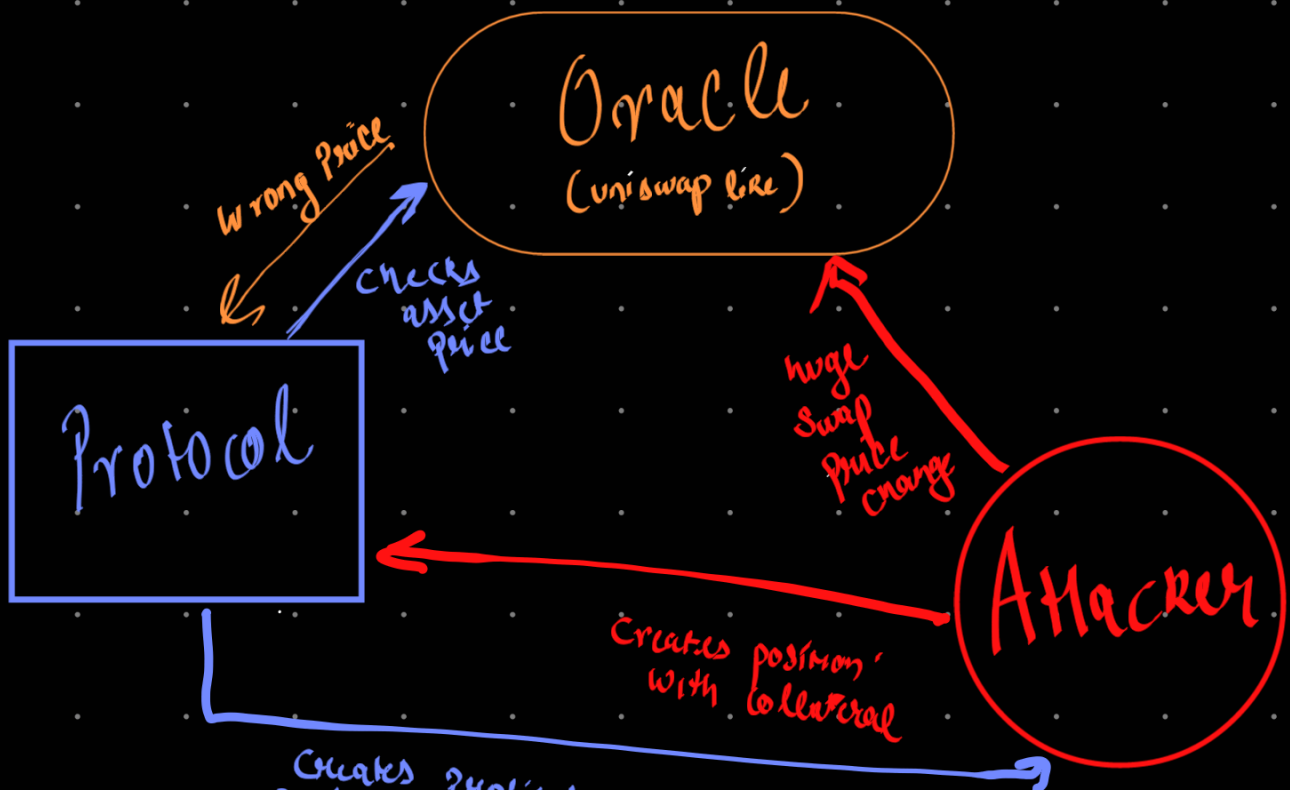


Oracle Manipulation

Number one most common DeFi exploit out of real attacks in the past



Position Profitable
Price with wrong

If protocol is trying to get prices by reading
Uniswap v3 'slot 0' or any other on-chain
oracle it is probably vulnerable eg Cream Finance

UNISWAP Partial Solution:

TWAP

Time Weighted Average Price

- Over the last 30 min Ether was 1599\$

It makes the same attack extremely unlikely
as an attacker would have to manipulate
pool for multiple blocks without getting
arbitraged.

It would be pretty unfeasible to perform this
in PoW system.

A bit more possible in PoS system but
highly unlikely as exploit would still cost
hundreds of millions.