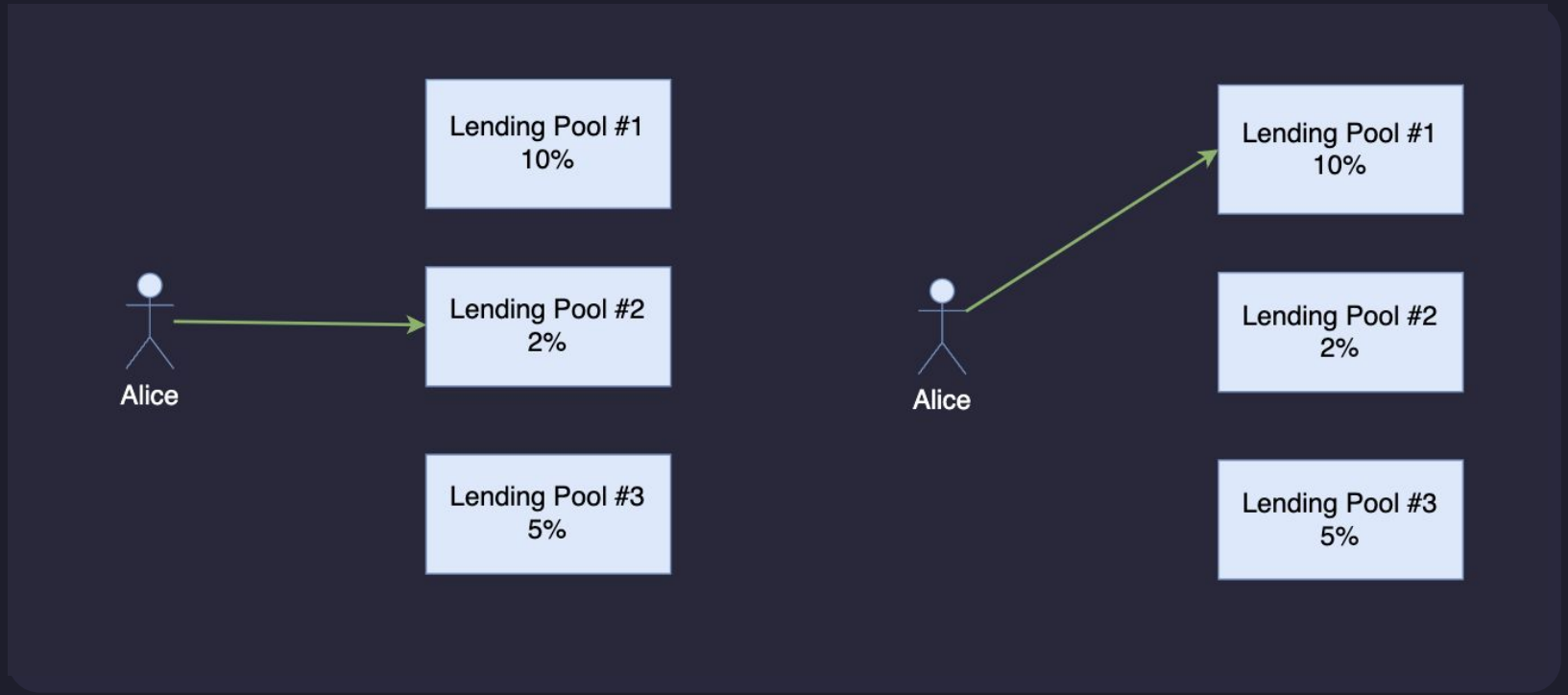
Yield Aggregators

Martinet Lee

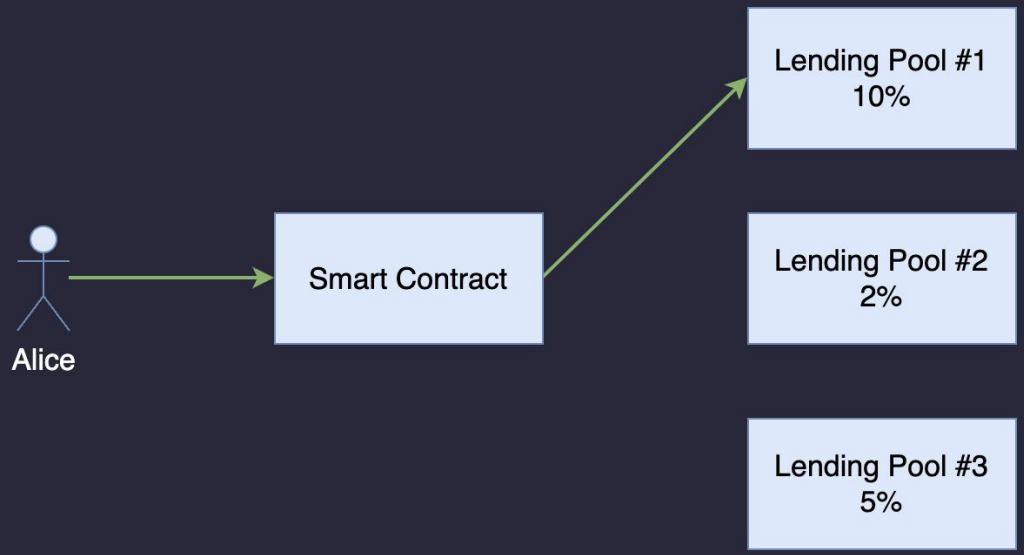
/Outline

- Why Yield Aggregators?
- YearnV1
- Governance tokens
- YearnV2, Harvest
- Classic attacks on Yield Aggregators

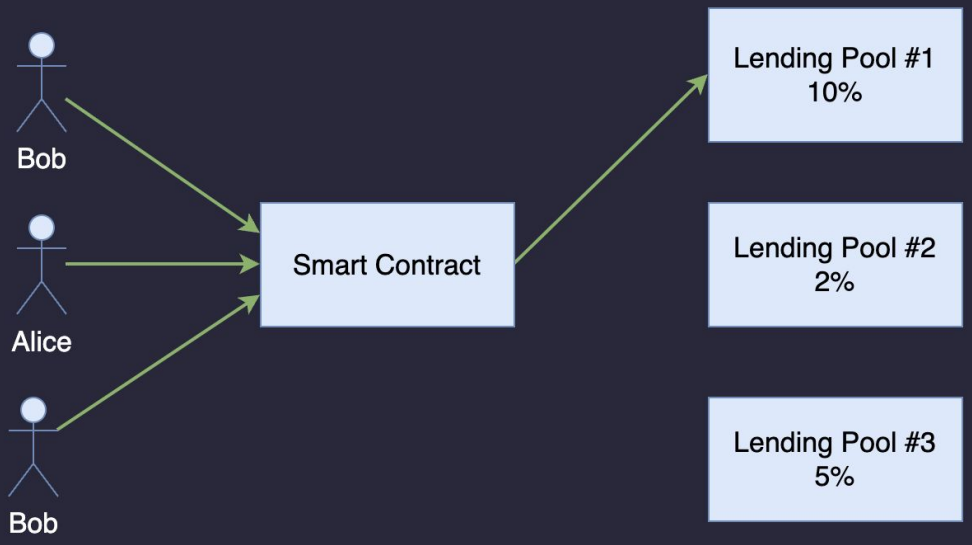
/Why Yield Aggregators



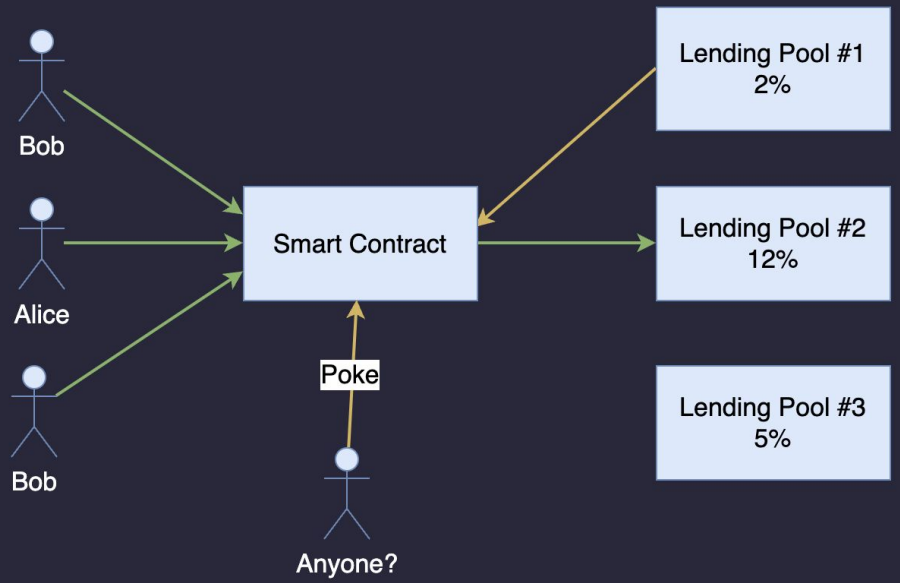
/Why Yield Aggregators



/Why Yield Aggregators



/Why Yield Aggregators



/The other side of Banking - Seeking for yields

- Besides loaning, banks also seek for different investment opportunities for the users and invest users' funds in them.
- One main difference - there's no transparency on how the banks are using our funds.

/DeFi History

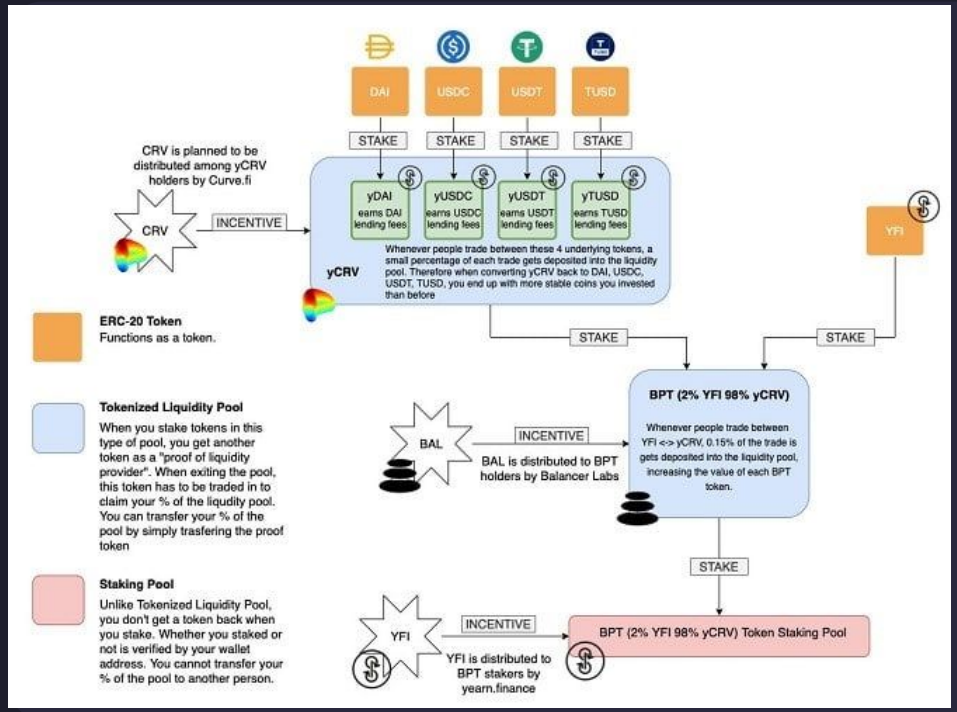
- Bitcoin - decentralized payment, 2009
- ICOs on Ethereum - decentralized raising money, 2017
- P2P to P2Pool ~2017 (Uniswap)
- 2020 MakerDAO incidence - stress test
- 2020 Defi Boom

/Comp Token Launch

/Incentivized Governance Token

- Attracting liquidity in the protocol (As shown in Comp's cases, liquidity 5x'ed)
- UniswapV2/Balancer to have liquidity for the token itself (so that there's a market and a price)
- Incentivizing liquidity providing of the tokens itself
- Back then, every protocol is talking about launching and incentivizing their liquidity providing pools…

/Defi Craze started from Yearn

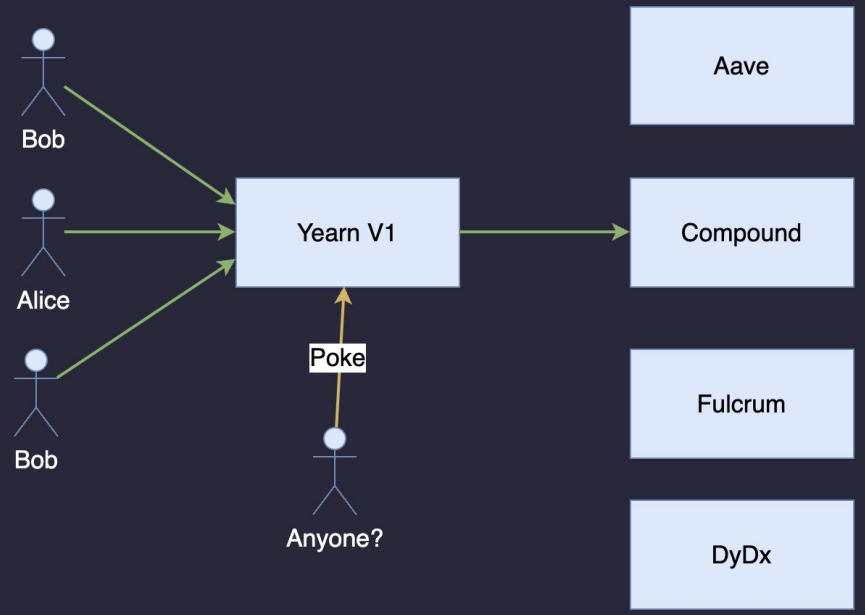


This graph does NOT represent the yearn protocol, rather the initial launch incentive design.

One of our goal today is to understand this graph.

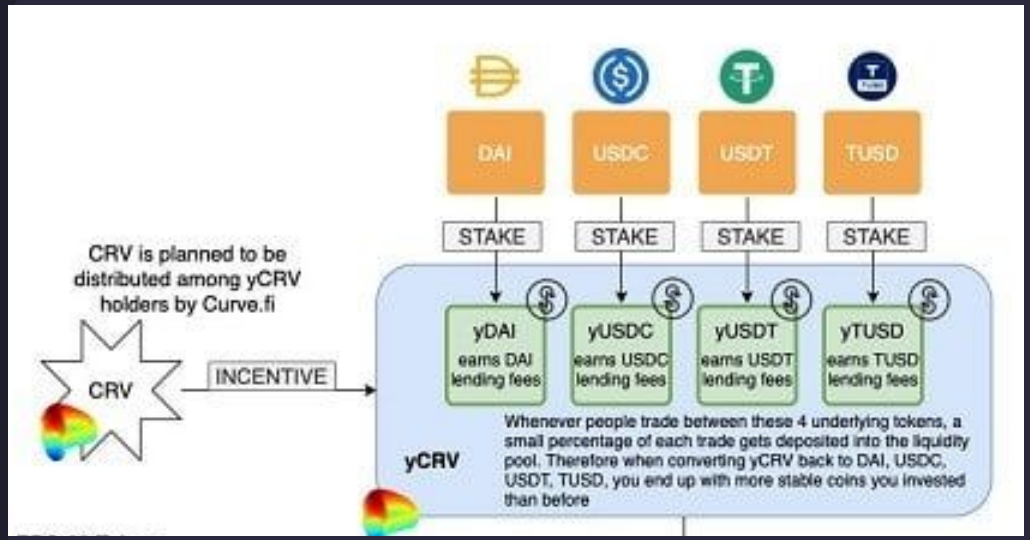
Credit: https://twitter.com/Weeb_Mcgee/status/1285397420373708801

/yDAI, yUSDC, yUSDT, yTUSD => yearnV1



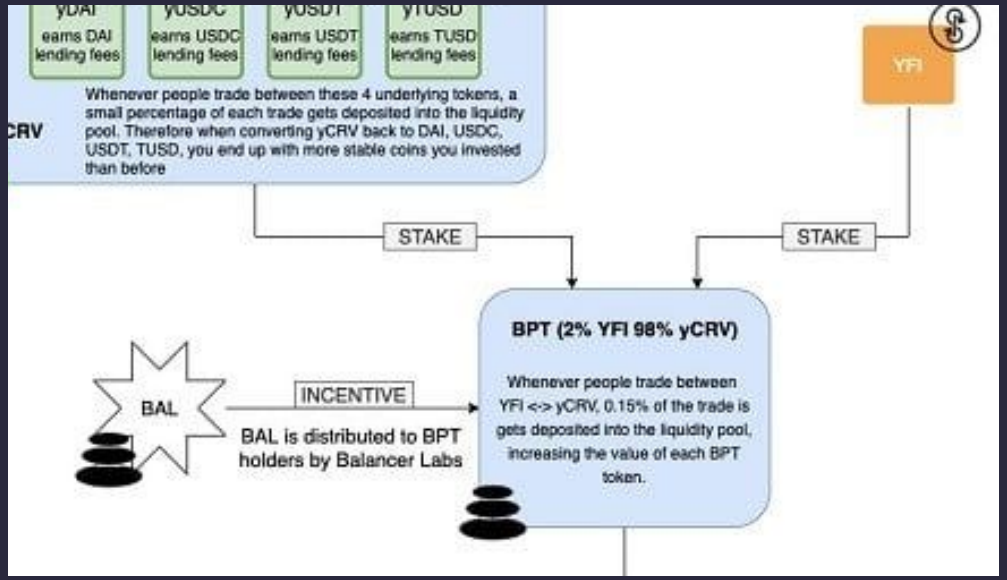
- If the base token is DAI, its yDAI, and so on.

/yCRV



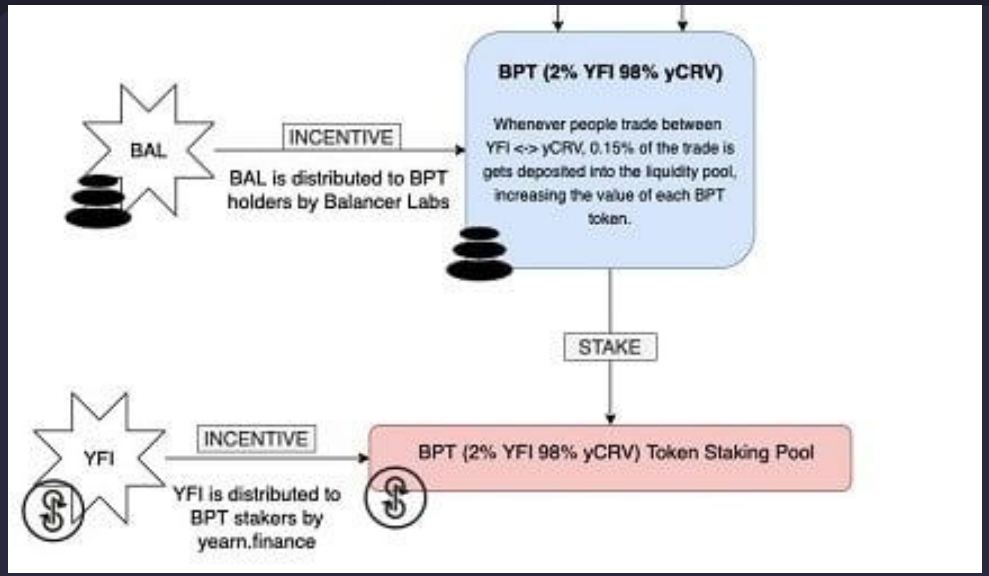
- Curve, is a specialized AMM for stable coins - or asset with nearly the same price.
- Curve has created a trading pool for yDAI, yUSDC, yUSDT, yTUSD

/98% yCRV 2% YFI Balancer Pool



- Balancer is another trading pool that is specialized in creating pools with different ratio.
- yCRV and YFI are combined to provide liquidity (again!) in Balancer Pool.
- Note that “Stake” here is incorrect in my opinion.

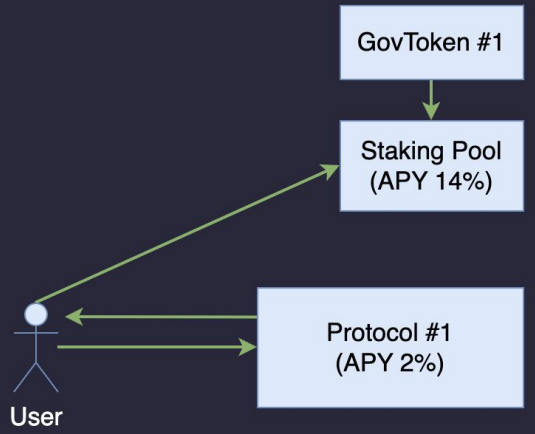
/Liquidity Incentive - Staking pool



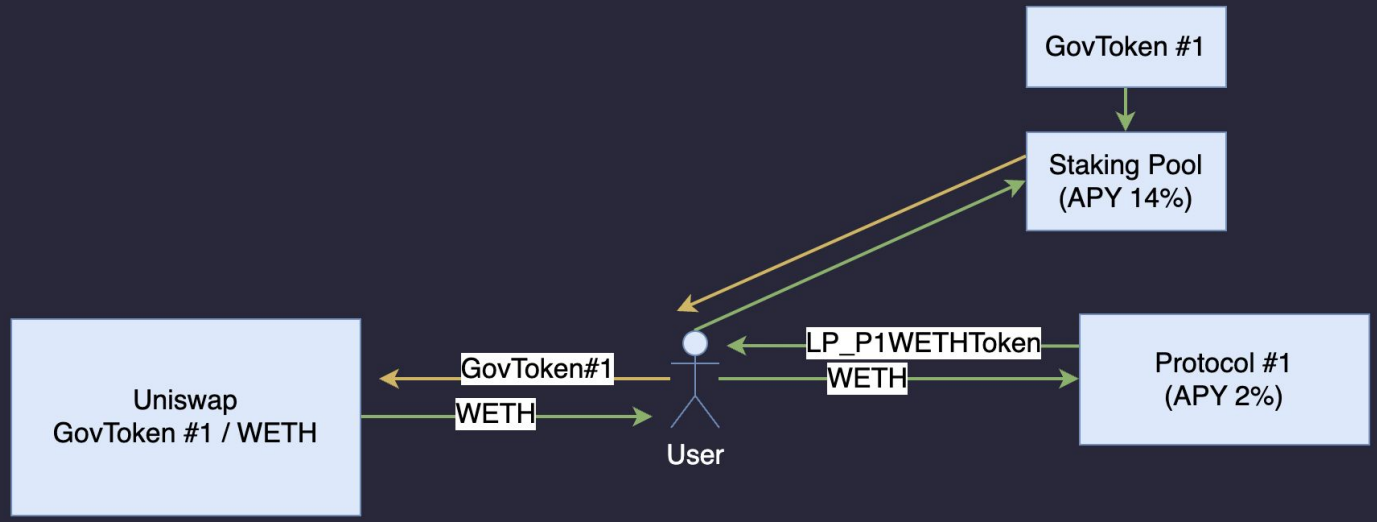
- After liquidity providing in Balancer, user will again get a ERC20 BPT token.
- Finally, user stake into a “staking pool” that is incentivized by YFI

/Staking pool

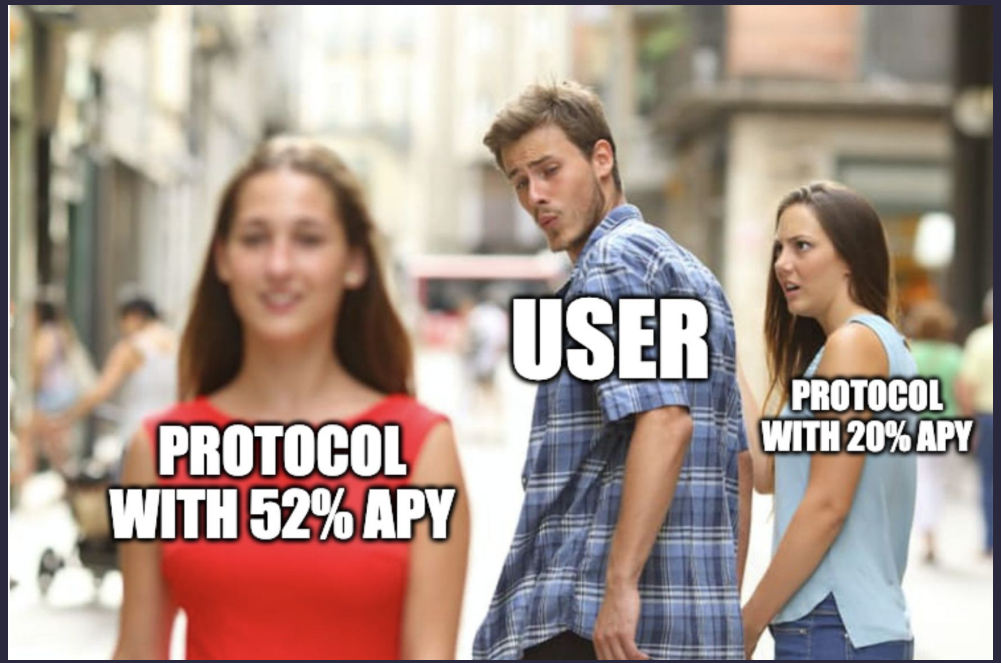
Only 500% APR.. (?)



/Getting the best yield #1: Compounding - APR to APY



/Getting the best yield #2: Finding the best crop



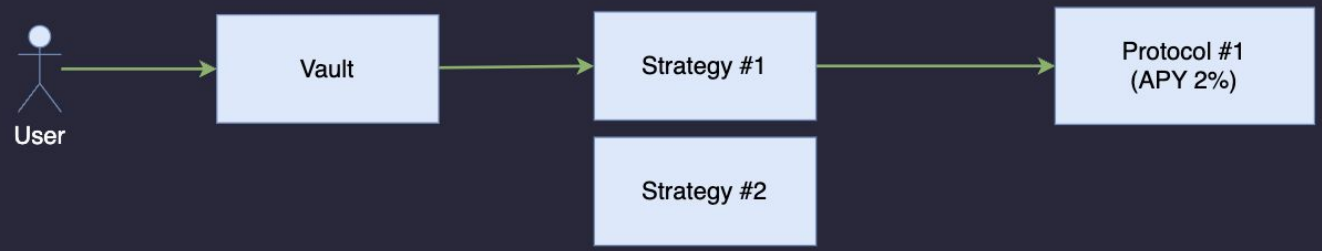
/Getting the best yield #2: Finding the best crop

- Problems for user?

/Getting the best yield #2: Finding the best crop

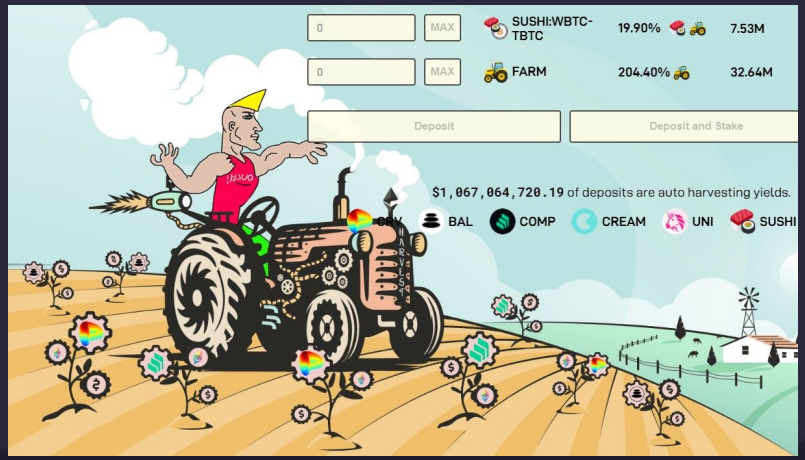
- Problems for user?
  - Hard to assess security
  - Cannot keep up with new opportunities all the time
  - Gas

/yearnV2 & Harvest

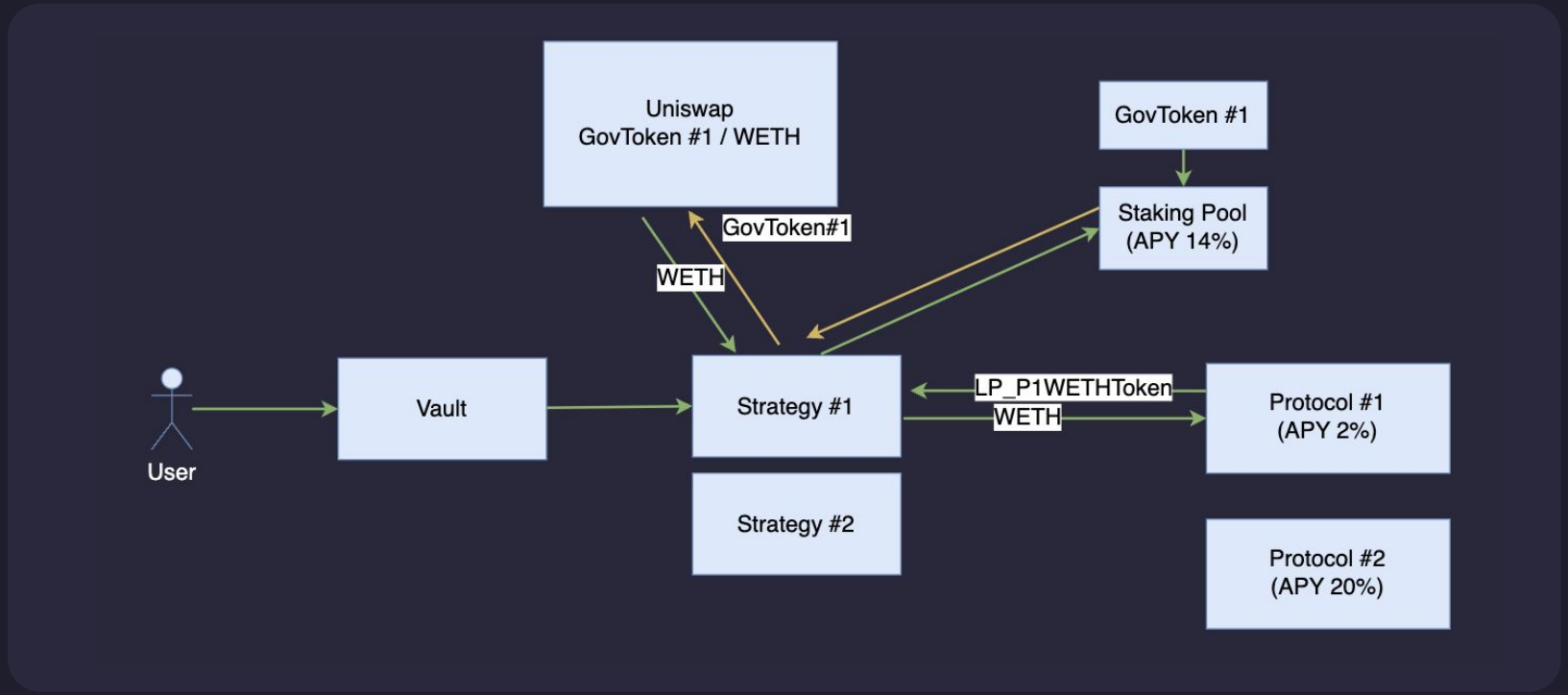


Create a structure that has is flexible, can switch between protocols

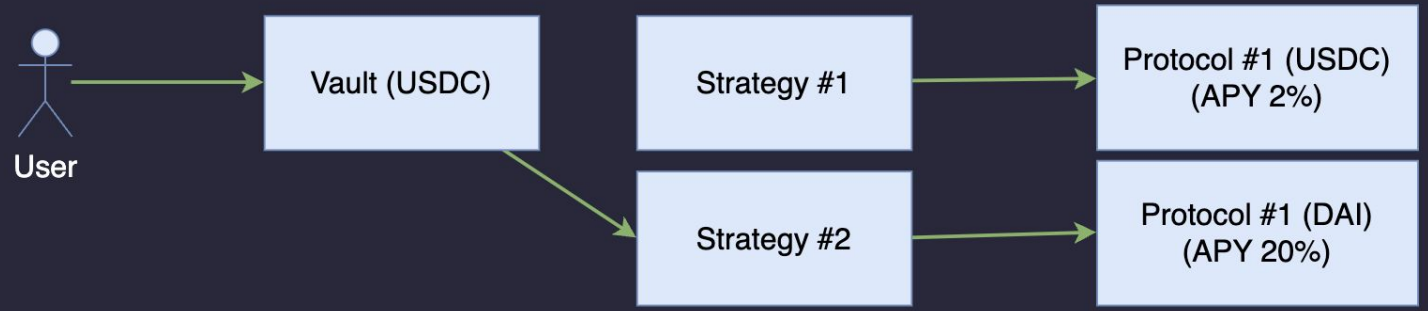
/yearnV2 & Harvest



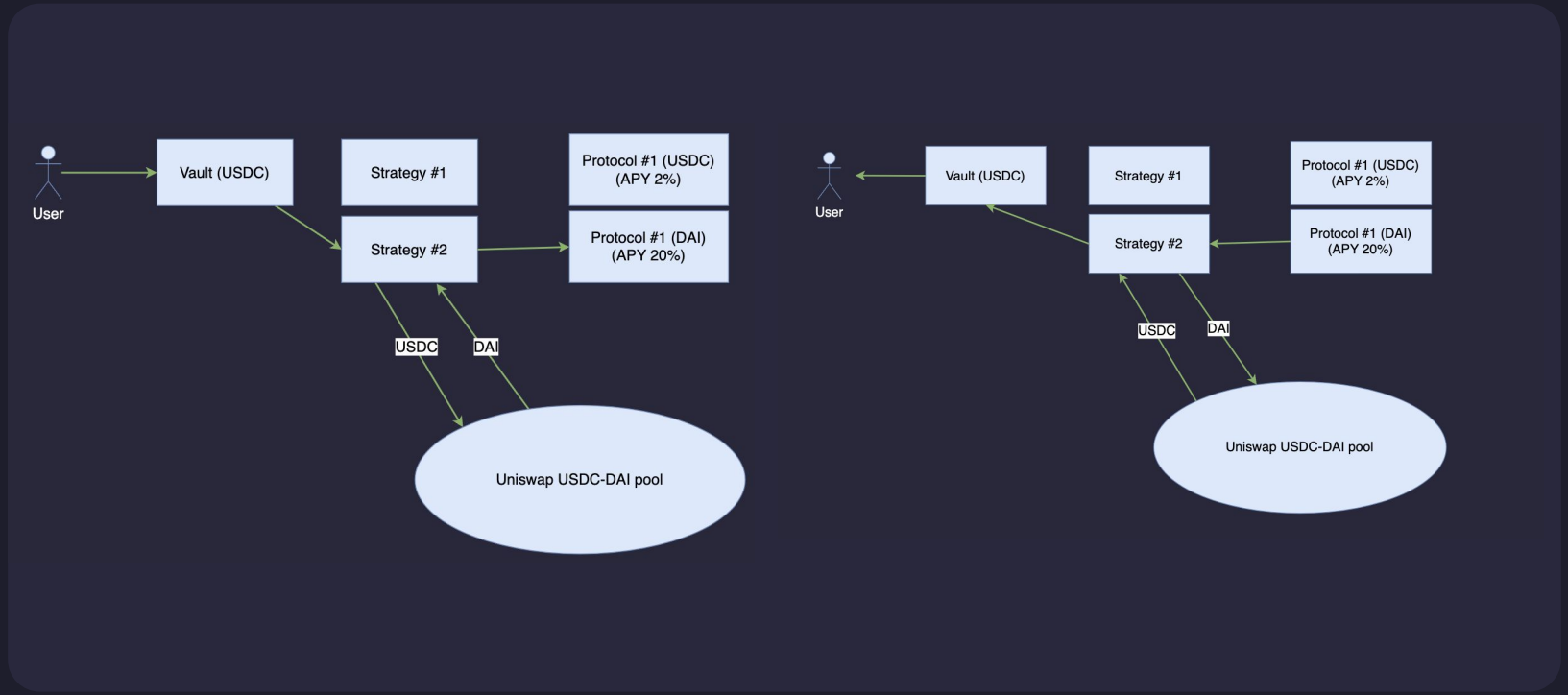
/yearnV2 & Harvest



/A classical mistake & attack on yield aggregator



/A classical mistake & attack on yield aggregator



/Observation & Attack Angle

- Let’s say Deposit forces conversion from USDC to DAI
- The whole USDC in vault is converted altogether

Basic Attack:

1. Manipulate and skew the Uniswap market, make DAI very expensive
2. Force the vault to convert USDC to DAI in a shitty price. Strategy gets little DAI comparing to normal times.
3. Unskew the market, gain profit.

/Observation & Attack Angle

1. Flashloan a lot of USDC
2. Manipulate and skew the Uniswap market, make DAI very expensive: Buy as much DAI with all the USDC loaned
3. Force the vault to convert USDC to DAI in a shitty price. Strategy gets little DAI comparing to normal times.
4. Sell back all the DAI. Get excessive USDC.
5. Return Flashloan

/THAT'S A WRAP!  (mic drop)