THE UNIVERSITY of EDINBURGH
informatics

Yield Aggregators in DeFi

Presenter: Yu SHEN

Outline

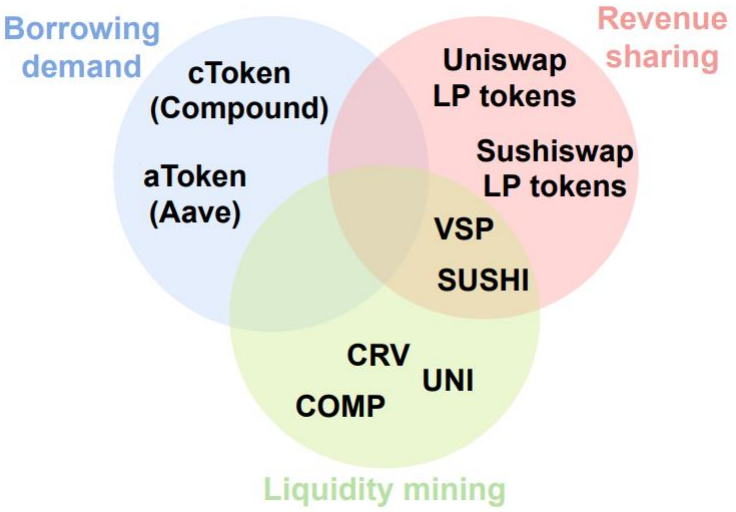
- What is yield aggregator?
- Protocol workflow
- Common strategies
- Major yield aggregators in DeFi
- Benefits & Potential risks

Yield Aggregators

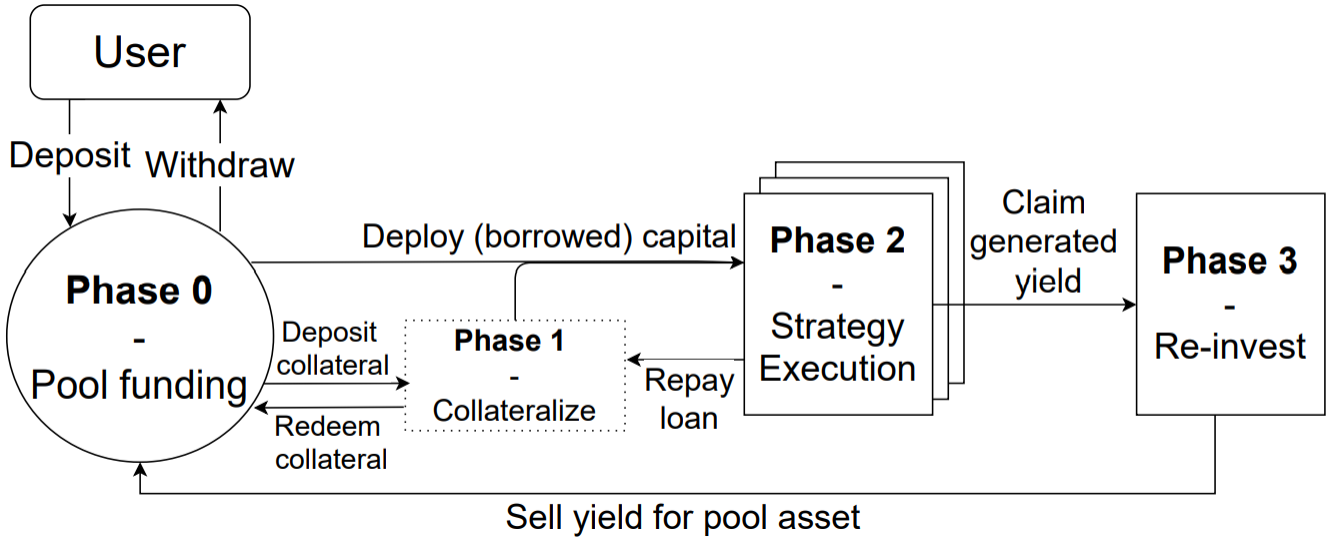
- Yield: the total amount of profit or income produced from a business or investment.
- Often measured in terms of Annual Percentage Yield (APY).

- Yield aggregator: a set of smart contracts that pools investors' funds and reinvests them in an array of yield-producing products or services through interacting with their respective protocols.

- Yield sources: borrowing demand, liquidity mining, revenue sharing

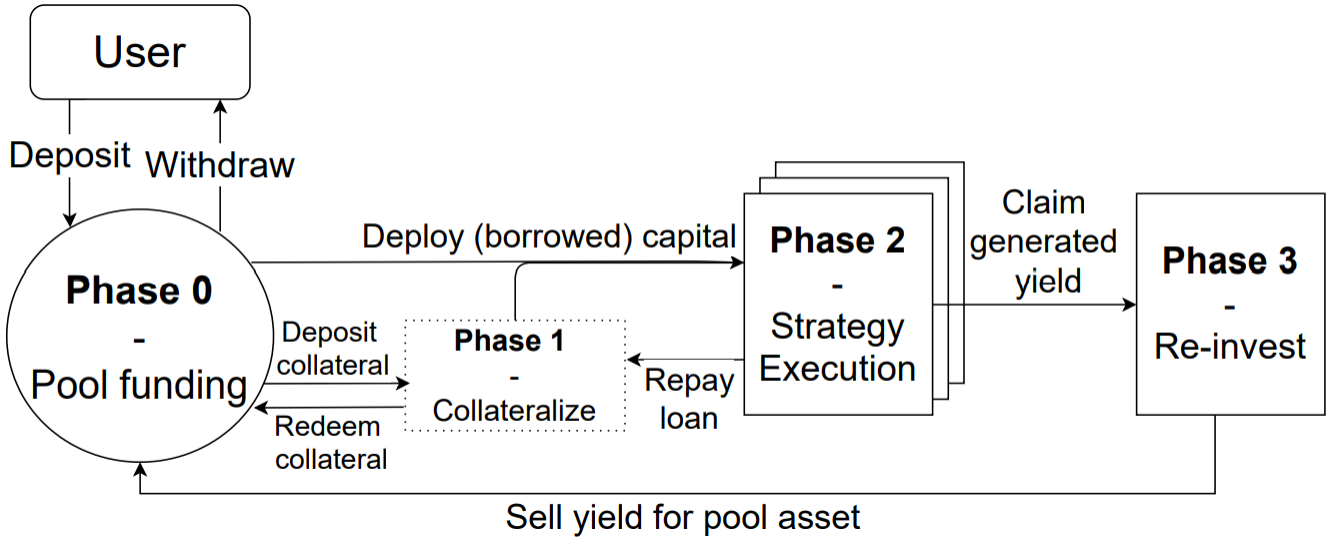


Protocol Workflow



- 3 or 4 phases
- Can happen in random order after bootstrapping.

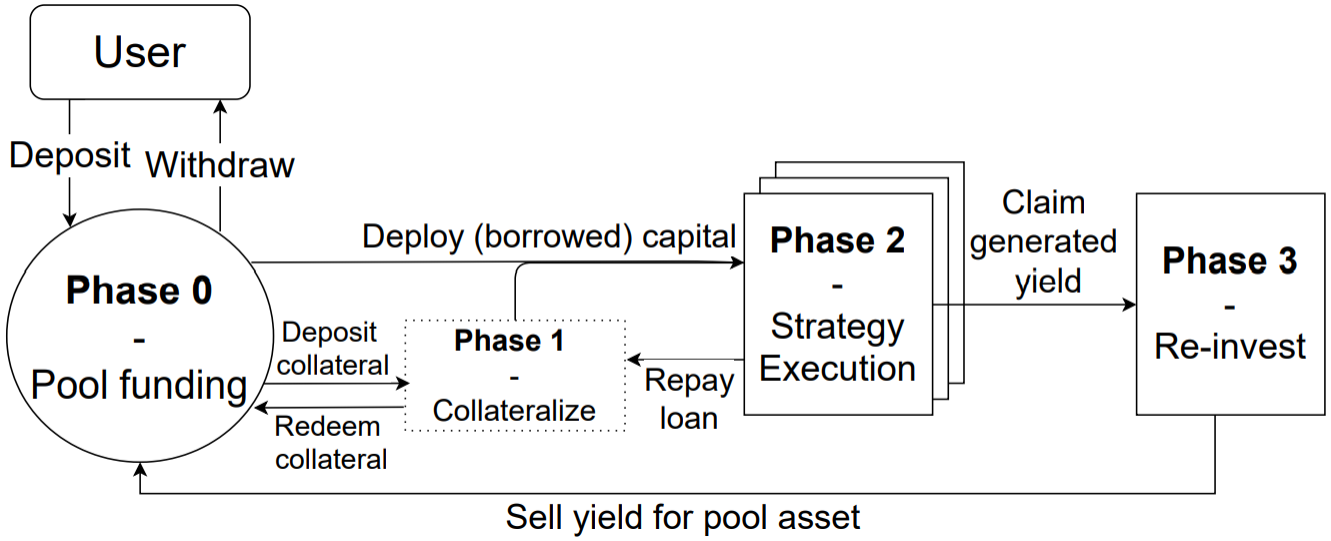
Protocol Workflow (Phase 0)



- A yield farming strategy* is proposed, created and deployed on blockchain.
- A pool is deployed in order to collect and disperse funds.

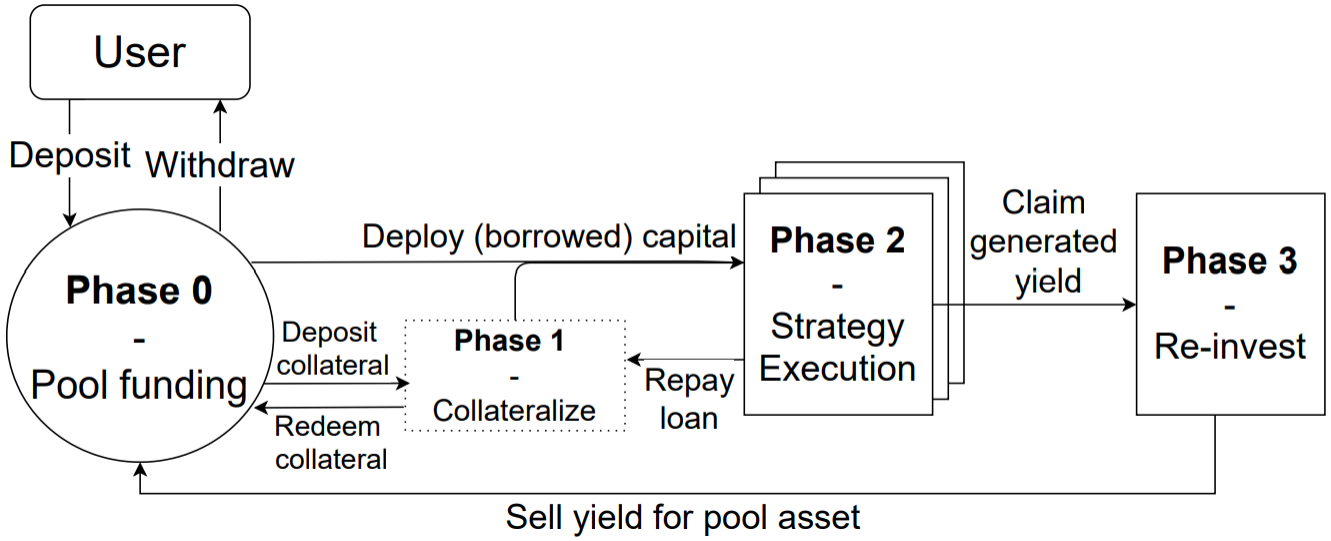
* In centralized protocols, only internal developers can create strategy; more decentralized protocols allow other to have a vote in strategy implementation.

Protocol Workflow (Phase 1)



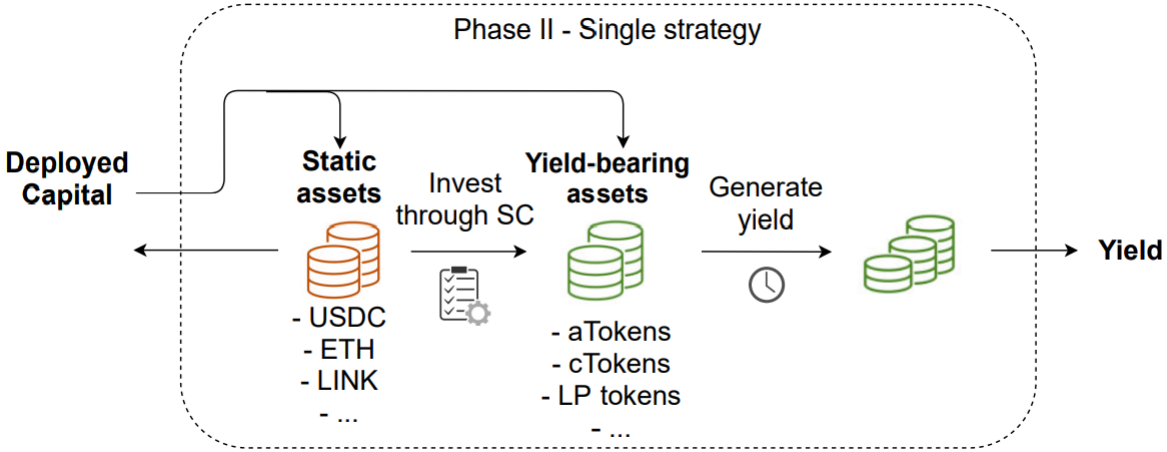
- Use funds pooled in Phase 0 as collateral to borrow another asset through lending platforms (usually stable coins).
- Can be skipped if pooled asset already satisfies the asset type requirement.

Protocol Workflow (Phase 2)



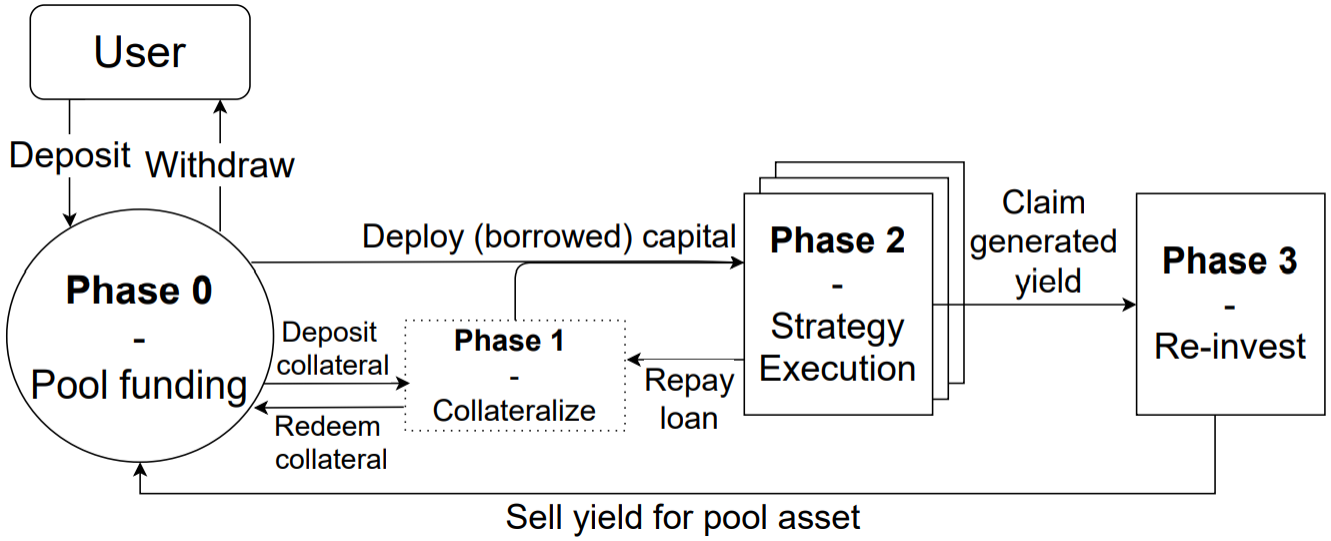
- Funds from Phase 0 and/or Phase 1 are deployed to generate yield, by following the pre-programmed strategy.
- Output is the yield.

Protocol Workflow (Phase 2)



- Funds from Phase 0 and/or Phase 1 are deployed to generate yield, by following the pre-programmed strategy.
- Output is the yield.

Protocol Workflow (Phase 3)

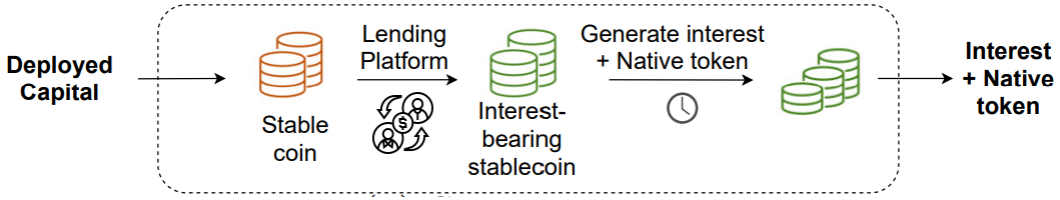


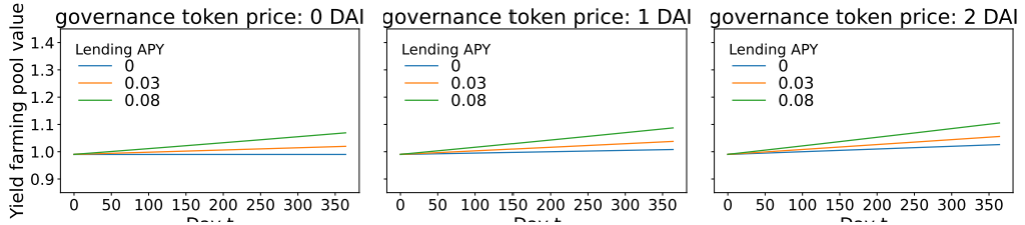
- Get the generated yield back to the original fund.
- Yield will be exchanged (via DEX) for the original asset and return to Phase 0*.

* Yield can also be deposited in Phase 1 as collateral or re-invested directly in Phase 2.

Common Strategies

- Simple lending: With this strategy, the aggregator earns yield through lending interest and governance tokens distributed by the lending platform.

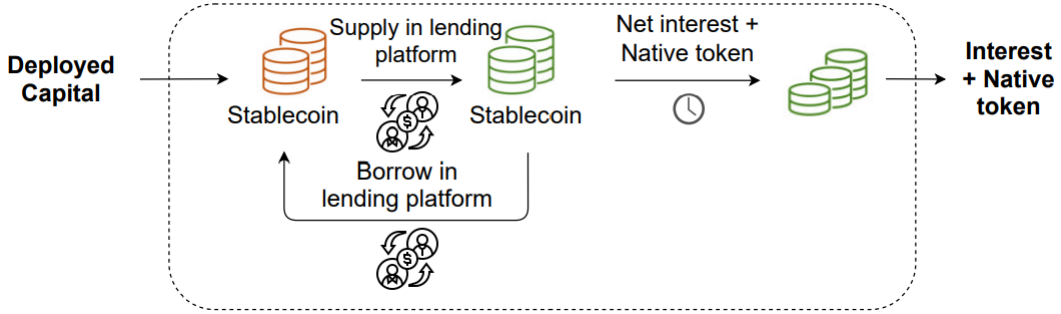


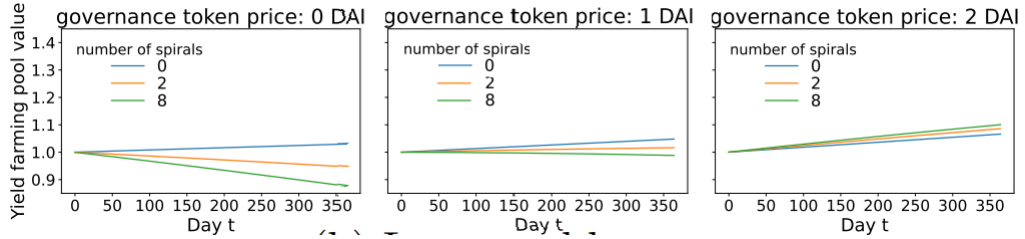


- The simple lending strategy is a low-risk one, and losses usually do not occur.

Common Strategies

- Governance tokens are rewarded to both lenders and borrowers (e.g., Compound).
- Leveraged borrow: maximize the amount of governance tokens received by the lending platform through leveraging spirals.

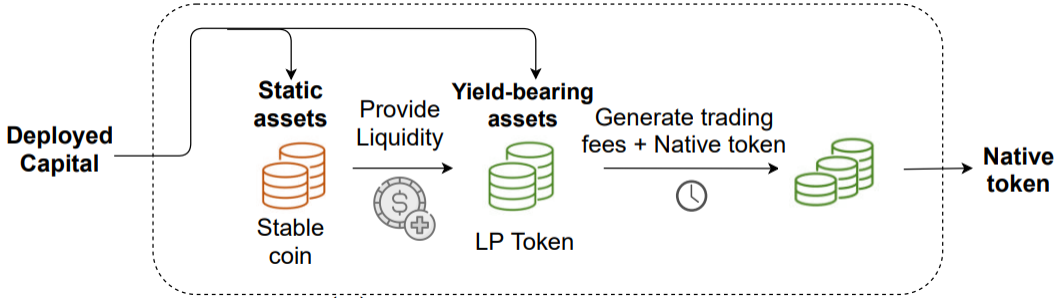


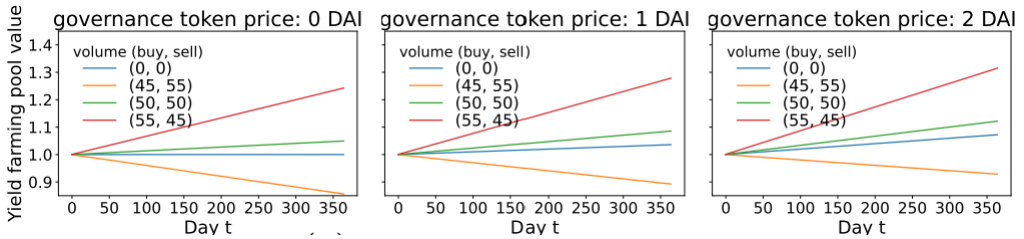


- A high degree of leverage (measured by the number of spirals) can amplify both the profit as well as the loss.

Common Strategies

- Liquidity provision: the aggregator supplies funds to an AMM in order to profit from both trading fees and governance tokens rewarded by the AMM.

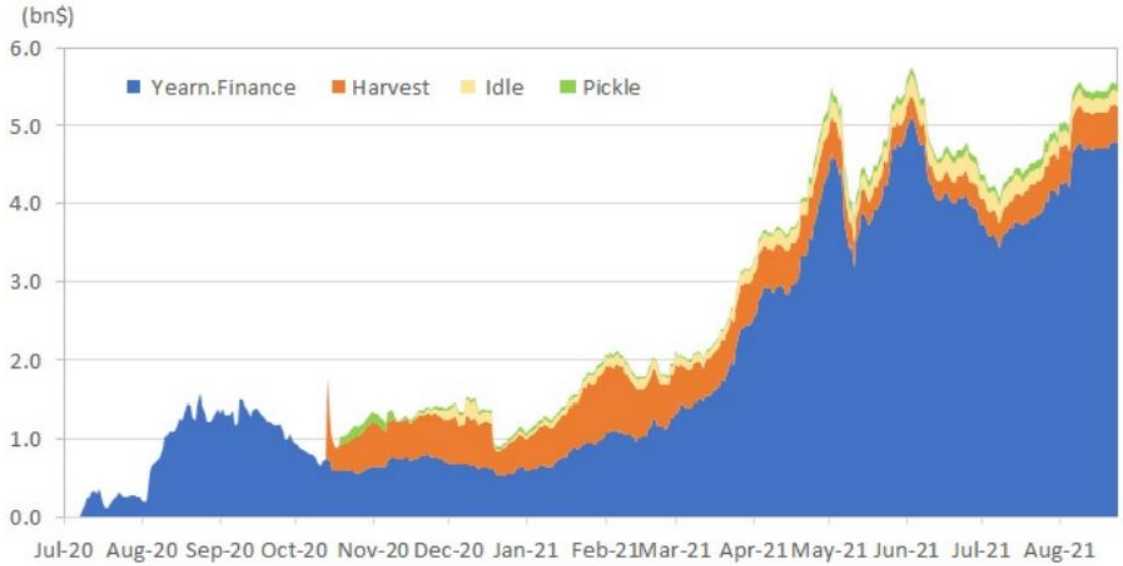




- Risks are associated with market movements of the assets within the AMM pool. Higher volatility of the AMM pool assets implies higher uncertainty in yield.

Major Yield Aggregators in DeFi

- Evolution of total value locked (TVL) for major protocols since July 2020.



Major Yield Aggregators in DeFi

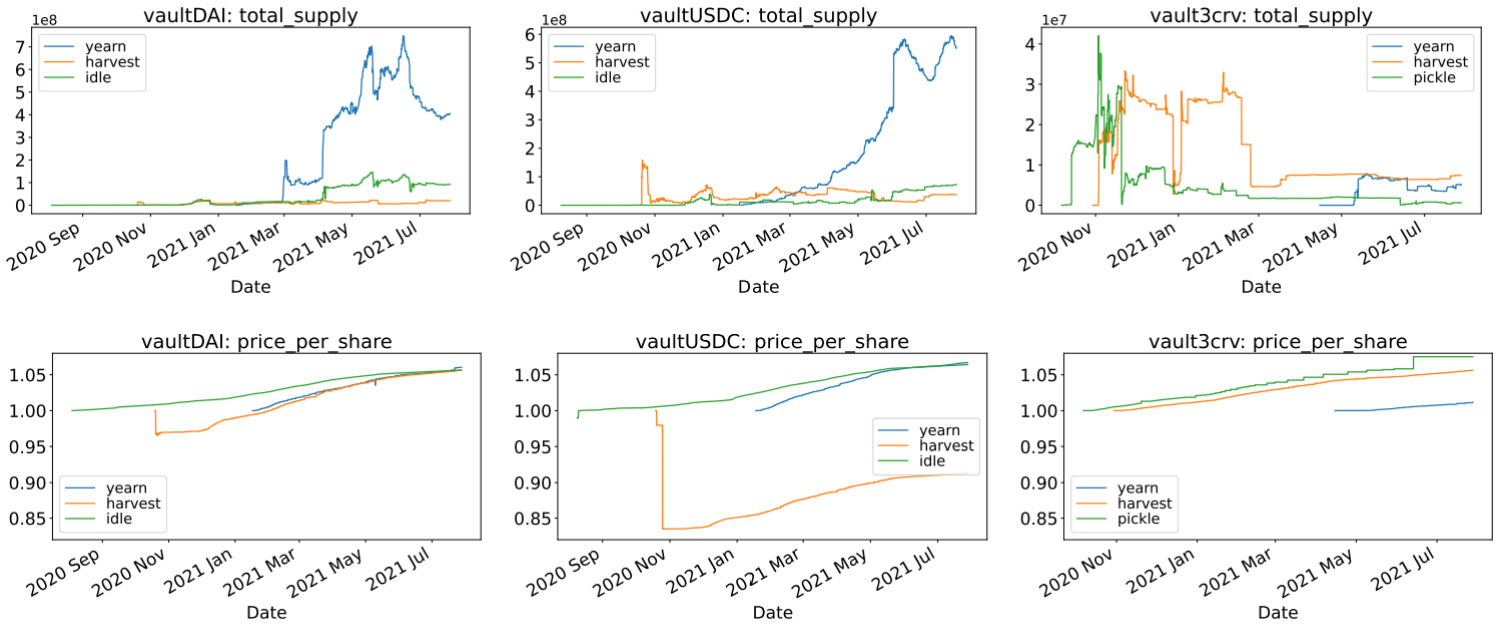
Table 1: Overview of major existing Yield Aggregators

		Phase 0 Supported Pool Assets			Phase 2 Strategies								
Protocol		**Single Asset**	**LP Token**	**Multiple Assets**	**SL[1]**	**LB[2]**	**LP[3]**	**Pool name**	**# of pools**	**Gov. token**	**MCap* (mm$)**	**TVL (mm$)**	**Token holders**
Idle Finance	[25]	●	○	○	●	○	○	Pool	10	IDLE	118.3	187.8	3,595
Pickle Finance	[42]	○	●	○	○	○	●	pJar	19	PICKLE	19.1	101.9	6,799
Harvest Finance	[20]	●	●	○	●	○	●	Vault	53	FARM	168.3	481.1	10,142
Yearn Vaults	[60]	●	●	○	●	●	●	Vault	50	YFI	1,520.8	4,787.7	40,089
Vesper	[52]	●	○	○	●	○	○	Grow Pool	4	VSP	136.0	439.8	5,996
Rari Capital Earn	[46]	●	○	●	●	○	○	Pool	3	RGT	157.5	196.9	9,559

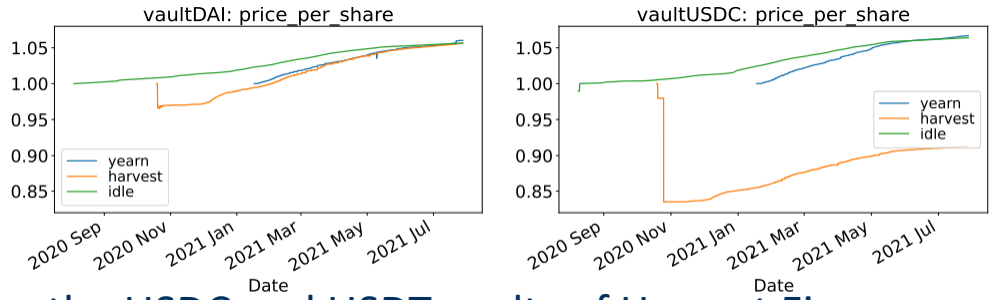
Data fetched on 5 September 2021. In phase 0, some protocols only accept single assets, others accept LP tokens and others accept more than one ERC20 token. Some protocols provide more than one category of vaults. In phase 1, some protocols focus on lending strategies, other focus on leveraged borrowing or liquidity provision strategies. Some protocols employ multiple strategy groups.
1 = Simple Lending, 2 = Leveraged Borrowing, 3 = Liquidity provision
* Fully diluted market cap - theoretical market cap which is calculated by assuming all the tokens were already in circulating supply.

THE UNIVERSITY of EDINBURGH
informatics

Major Yield Aggregators in DeFi (Empirical Data)



Flash Loan Attacks on Harvest Finance



- An attacker stole funds from the USDC and USDT vaults of Harvest Finance on 26th Oct 2020.
- A total value of $33.8M was stolen, accounting for 3.2%* of the protocol TVL.

We made an engineering mistake, we own up to it. Thousands of people are acting as collateral damage, so we humbly request the attacker to return funds to the deployer, where it will be distributed back to the users in its entirety.

755 8

Harvest Finance
1.3K Followers

* https://medium.com/harvest-finance/harvest-flashloan-economic-attack-post-mortem-3cf900d65217

Flash Loan Attacks on Harvest Finance

- The following mechanics of the Harvest protocol allowed for executing such an attack:
  - Harvest's investment strategies calculate the real-time value of assets invested in the underlying real-time protocols. The vaults use the value of the assets to calculate the number of shares to be issued to the user depositing the funds. They also use the value of the assets when users remove funds from the vaults to calculate the payout that a user should receive upon exit.
  - The assets inside some of the vaults (including USDC and USDT) are deposited into shared pools of underlying DeFi protocols (such as the Y pool on Curve.fi). The assets inside such pools are subject to market effects such as impermanent loss, arbitrage, and slippage. Thus, their value can be manipulated via market trades with a large volume.

Flash Loan Attacks on Harvest Finance

- The attacker deployed a contract through which they carried out the entire attack.
- The attacker sourced a large amount of USDT (18,308,555.417594) and USDC (50,000,000) from Uniswap into the attacking contract.
- Repeat for multiple times:
  - In Y pool@Curve.fi, convert USDT to USDC → decrease price of shares at Harvest
  - Depost USDC into Harvest's USDC vault → receiving more shares (fUSDC)
  - In Y pool@Curve.fi, convert USDC to USDC → increase price of shares at Harvest
  - Withdraw from Harvest's USDC vault trading all fUSDC shares back → Profit (in USDC)
- Eventually, the attacker transferred 13,000,000 USDC and 11,000,000 USDT from the attacking contract.

Attacks on Pickle Finance

- An attacker swipes $20M in ‘evil jar’ exploit.
- The attacker swapped funds between a malicious copycat contract* (the same interface of traditional jars but do bad things) and the cDAI jar.
- This hack was possible after several design issues within the Pickle contracts.

* https://etherscan.io/address/0x6186e99d9cfb05e1fdf1b442178806e81da21dd8#code

Benefits & Potential Risks

- Benefits of using yield aggregators:
  - Yield farmers do not have to actively compose their own strategy, but they can make use of the workflows invented by other users.
  - Cross-protocol transactions are happening through a smart contract. Capital shifts are done automatically, removing the need for the user to transfer funds manually between protocols.
  - Because funds are pooled in a strategy contract, the gas costs are socialized, resulting in fewer and thus lower interaction costs.

- Risks of Using yield aggregators include lending and borrowing risks, composability risks and APY instability.

Benefits & Potential Risks (Lending and Borrowing Risks)

- Yield farming strategies might use lending and borrowing transactions as part of creating yield. Both come with risks.
- Liquidity risk
  - The utilization rate U (totalAmountBorrowed/totalLiquidity) is close to 1.
  - Nearly all funds supplied in a pool are being borrowed.
  - If many lenders withdraw at the same time, a certain amount of them will have to wait until some of the borrowers have paid back their outstanding loans.
- Liquidation risk
  - Happens when the value of the collateral falls below a pre-determined liquidation threshold.
  - The deposited collateral is no longer deemed valuable enough to cover the amount of the loan that was taken.
  - The lending protocol automatically places for sale in the market at a discount with the proceeds used for loan repayment.

Benefits & Potential Risks (Composability Risks)

- The composability factor of DeFi is what makes yield farming possible in the first place by allowing for complex, interconnected financial protocols.
- Even if contracts are secure on an individual level, the combination of multiple smart contracts may not.
- The effect of failure in one of the core components can cause a ripple effect throughout the whole ecosystem.
- Using a yield aggregator, the risk not only lies in smart contract risks of that aggregator, but also in all of the underlying protocols in lower layers.

Benefits & Potential Risks (APY Instability)

- Market forces can lead to instabilities in the returns, making the advertised APYs unreliable. This decreases the user experience.
- Potential reasons:
  - Volatile lending returns: interacting with a lending protocol can affect the utilization ratio.
  - Divergence loss* (impermanent loss): a commonly known risk of providing liquidity in AMM caused by price volatility of the assets that were used to obtain LP tokens.
  - Low trading activity: low activity in a liquidity pool results in lower trading fees, decreasing APY.
  - Price fluctuations in liquidity incentives.

* Xu, J., Paruch, K., Cousaert, S.: SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols (3 2021), https://arxiv.org/abs/2103.12732

Bibliography

1. Cousaert, Simon, Jiahua Xu and Toshiko Matsui. “SoK: Yield Aggregators in DeFi.” (2021).
2. Xu, J., Paruch, K., Cousaert, S.: SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols (3 2021), http://arxiv.org/abs/2103.12732
3. Idle Finance: Idle Finance Documentation (2021), https://developers.idle.finance/
4. Harvest Finance: Harvest Finance (2021), https://harvest.finance/
5. Pickle Finance: Emission Schedule - Pickle Finance Docs (2021), https://docs.pickle.finance/faqs/emissions
6. Yearn Finance: yearn.finance (2021), https://yearn.finance/