SoK (Systemization of Knowledge)

Yield Aggregators in DeFi (Decentralized Finance)

Jiahua (Java) Xu, Ph.D.

2022

Decentralized finance

DeFi A **rule-based** financial system that operates according to **protocols** composed of **smart contracts** on **blockchains**.

DeFi applications

- Decentralized exchanges (Xu et al. 2022)
  - UNISWAP Balancer Curve DODO
- Lending protocols (Xu and Vadgama 2022; Perez et al. 2021)
  - MAKER Compound AAVE
- Yield aggregators (Cousaert, Xu, and Matsui 2022)
  - yearn.finance Harvest Finance BREAD FOR THE PEOPLE Pickle Finance Bank Of Chain
- Token-based insurance solutions (Cousaert, Vadgama, and Xu 2022)
  - Nexus Mutual ETHERISC insure

Yield Aggregators

DeFi yield aggregators A DeFi yield aggregator is a decentralized fund manager that uses smart contracts to determine and execute investment strategies.

Where do yields come from

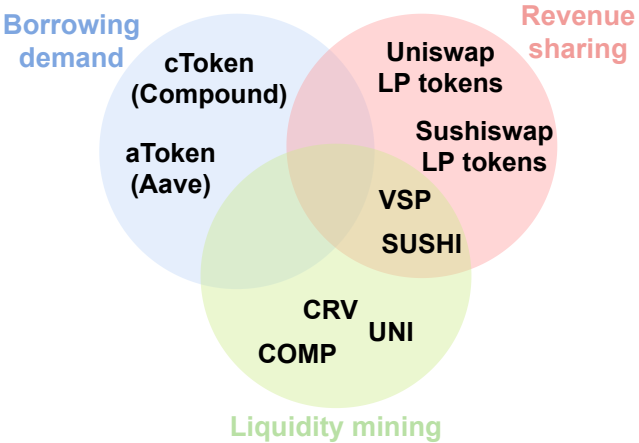

Figure 1: Yield sources

Yield farming process

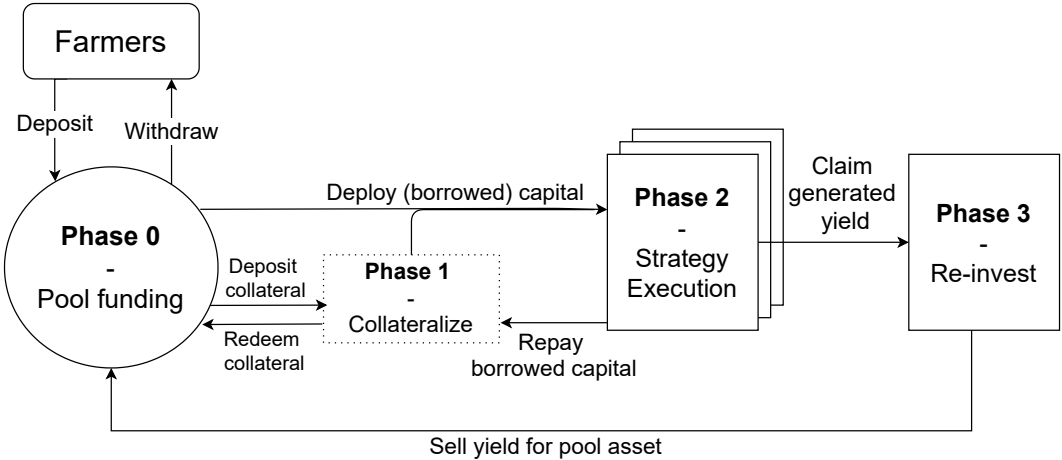

Figure 2: Stylized yield aggregator mechanism (Cousaert, Xu, and Matsui 2022)

Yield farming process - Phase 2

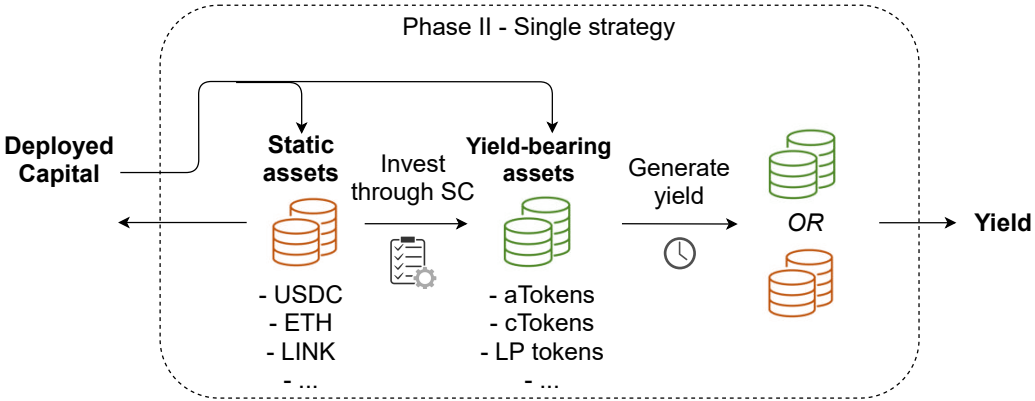

Figure 3: Execution process of a single strategy. SC = Smart Contract (Cousaert, Xu, and Matsui 2022)

Classic yield farming strategies – Simulation assumptions

- the transaction cost is neglected;
- the value of the yield aggregator W_t is measured in `DAI`; $W_0 = 1$;
- the aggregator supplies all funds in the pool to a yield-generating protocol—either a lending platform or an AMM, and the funds represent 1% of the protocol's total assets held at $t = 0$;
- the yield-generating protocol—either a lending platform or an AMM—distributes 0.01 governance token / day to its users proportionately to their stake;
- the governance token price remains constant during the simulation period;
- the lending platform has a fixed borrow APY of 10% and a collateral factor of 80%, meaning for each `DAI` deposited, the depositor is allowed to take 0.8 `DAI`'s worth of loan; at $t = 0$, 70% of the funds in the lending platform pool is lent out, and all other market participants' additional borrow and repay, as well as deposit and withdraw cancel each other out on an aggregate level during the simulated period;
- the AMM has a fixed exchange fee of 5% and applies a constant-product conservation function; the fee is charged by retaining 5% of the theoretical fee-free purchase quantity within the AMM pool.

Algorithm 1 Simple lending

1: **Deposit** assets in a lending protocol.
2: **Accrue** supply interest and **collect** native tokens over time.
3: **Withdraw** deposits with accrued supply interest.

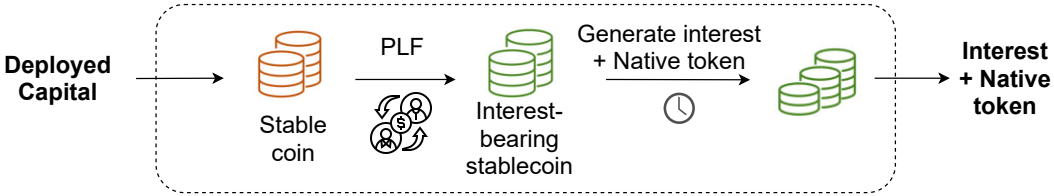

Figure 4: Simple lending

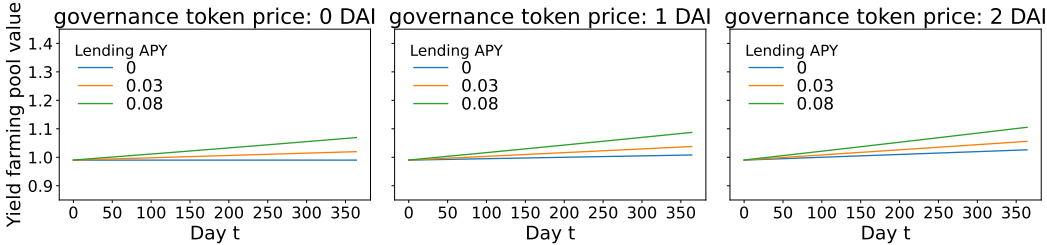

Figure 5: Simple lending

Algorithm 2 Leveraged borrow

1: **Deposit** assets in a lending protocol
2: **Borrow** assets with the deposits as collateral.
3: **Deposit** borrowed assets.
4: **Repeat** steps 2–3 multiple times.
5: **Accrue** interest and **collect** native tokens over time.
6: **Swap** the native tokens into the assets borrowed.
7: **Repay** loans with accrued borrow interest.
8: **Withdraw** deposits with accrued supply interest when needed.

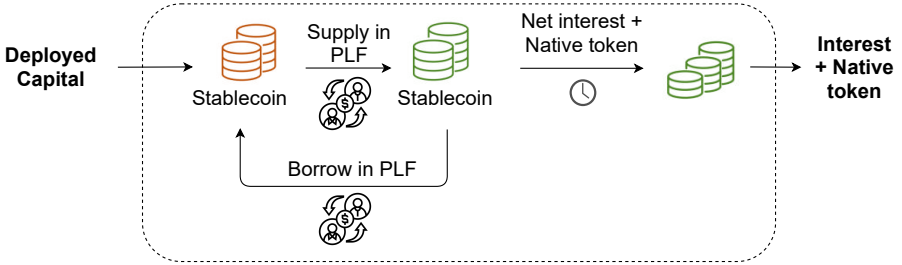

Figure 6: Leveraged borrow

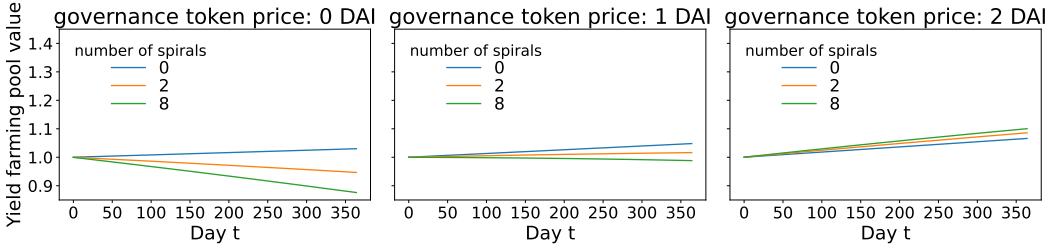

Figure 7: Leveraged borrow

Algorithm 3 Liquidity provision

1: **Provide** assets as liquidity in an AMM pool.
2: **Collect** native tokens over time.
3: **Withdraw** liquidity.

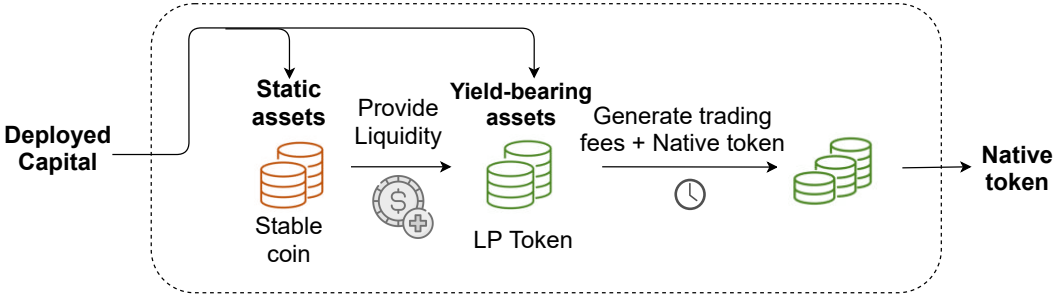

Figure 8: Liquidity provision

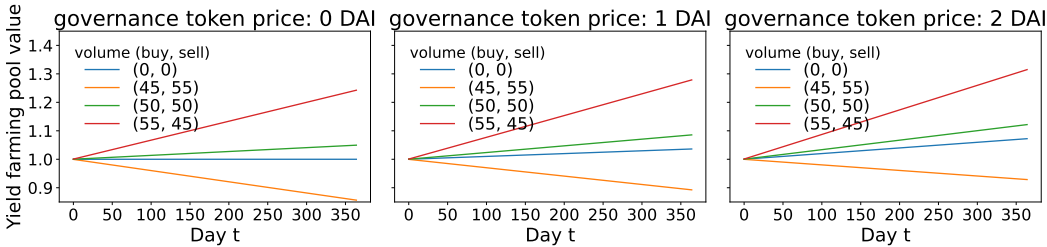

Figure 9: Liquidity provision

Classic yield farming strategies

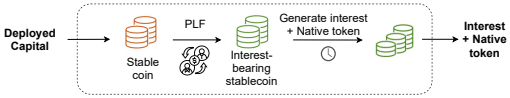

Figure 10: Simple lending

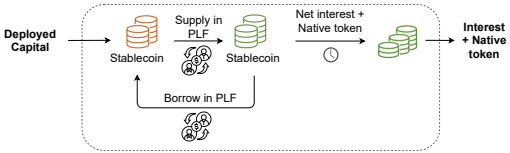

Figure 11: Leveraged borrow

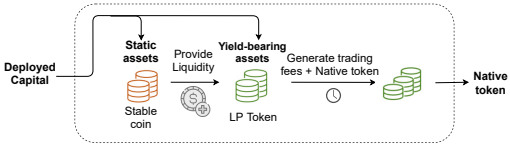

Figure 12: Liquidity provision

Risks

- Lending and borrowing risks
  - Liquidity risk
  - Liquidation risk
- Composability risks
  - Individual smart contract risk
  - Composing multiple smart contracts risk
- APY instability
  - Divergence loss
  - Low trading activity
  - Price fluctuations in liquidity incentives (governance token)
  - Uncertainty on yield sustainability

Existing yield farming protocols

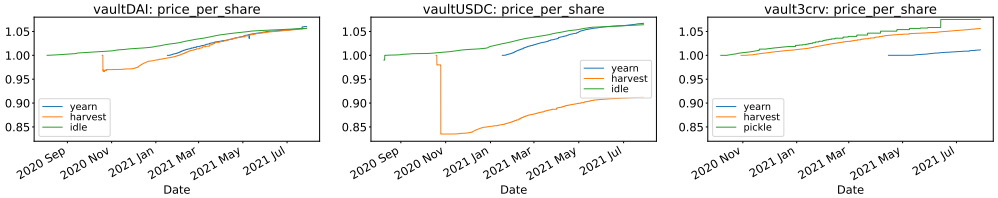

Figure 13: Price per share of Yearn, Harvest, Pickle

On 26th October, a flash loan attack occured on Harvest.

Emerging yield farming protocols

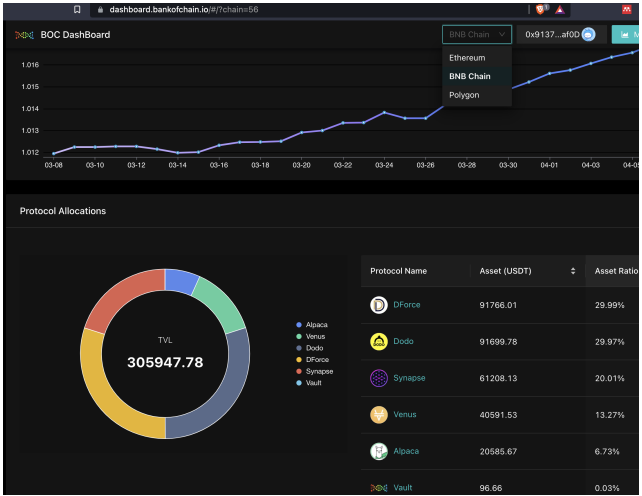

Figure 14: Bank Of Chain, a smart multi-chain yield optimizer that provides long-term "risk-free" return (Bank Of Chain 2022)

Thank you!

Contact

Jiahua (Java) Xu

UCL Centre for Blockchain Technologies

66-72 Gower Street

jiahua.xu@ucl.ac.uk

References I

Bank Of Chain. 2022. "Bank Of Chain." https://bankofchain.io/.

Cousaert, Simon, Nikhil Vadgama, and Jiahua Xu. 2022. "Token-based Insurance Solutions on Blockchain." In *Blockchains and the Token Economy: Theory and Practice*. https://arxiv.org/abs/2109.07902v1.

Cousaert, Simon, Jiahua Xu, and Toshiko Matsui. 2022. "SoK: Yield Aggregators in DeFi." In *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. http://arxiv.org/abs/2105.13891.

Perez, Daniel, Sam M. Werner, Jiahua Xu, and Benjamin Livshits. 2021. "Liquidations: DeFi on a Knife-Edge." In *Financial Cryptography and Data Security*, 12675 LNCS:457–76. Springer. https://doi.org/10.1007/978-3-662-64331-0_24.

Xu, Jiahua, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. 2022. "SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols." http://arxiv.org/abs/2103.12732.

Xu, Jiahua, and Nikhil Vadgama. 2022. "From Banks to DeFi: the Evolution of the Lending Market." In *Enabling the Internet of Value: How Blockchain Connects Global Businesses*, 53–66. https://doi.org/10.1007/978-3-030-78184-2_6.