Hyperledger Capital Markets

June 30, 2021 10 am EDT

AMM: Promise & Risk- A guided open discussion

by Kirthi K (Civitas Fintech) and Vipin Bharathan

https://zoom.us/my/hyperledger.community.backup?pwd=dkJKdHRlc3dNZEdKR1JYdW40R2pDUT09
Details: https://wiki.hyperledger.org/display/CMSIG/2021-06-30

Agenda

- Terminology
- Yield Farming
- AMM and Liquidity Pools
- The promise
- Case Studies
- How things can go wrong!

Terminology

Yield farming: Automated techniques for creating yield for digital assets (thru lending and market making).

Automated Market Maker (AMM): AMM is a type of decentralized exchange (DEX). AMM platforms allow digital assets to be traded automatically using a programmed liquidity pool bringing together buyers and sellers.

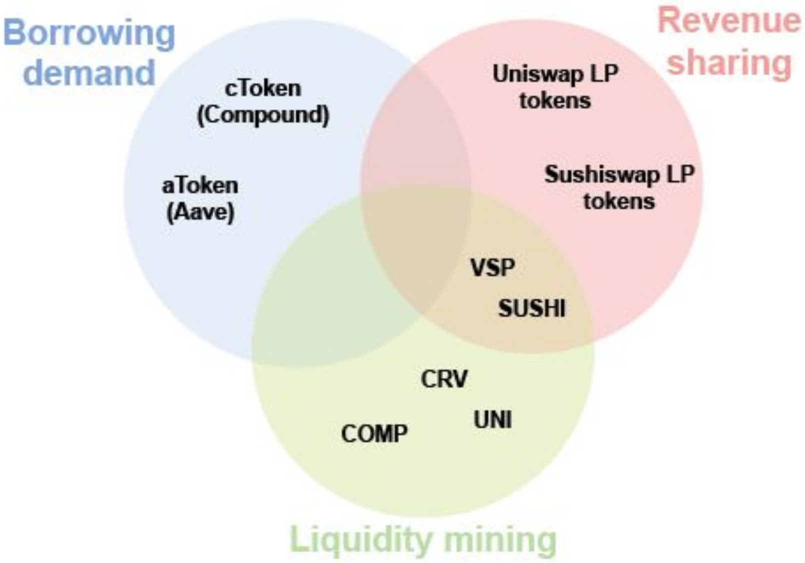
Total Value Locked (TVL): Metric for the size of DeFi market. Total value locked is the amount of capital that has been deposited. (as collateral or into a trading pool)

Liquidity pools: Liquidity refers to to the ease of converting one asset may to another without moving the price much. AMM platforms collect funds in a liquidity pool controlled by a smart contract. This can facilitate trading, lending, etc. Eg. Uniswap, Pancakeswap, SushiSwap.

Liquidity providers and LP tokens: Liquidity providers are incentivized by getting periodic returns. Part of the fees generated through trading within the pool may be used to pay liquidity providers. When liquidity providers contribute assets to a pool, the AMM platform can also automatically generate an LP token which can amplify their returns.

Flash loan: A loan that is made and returned within the timeframe it takes to create a new block on the blockchain.

Yield farming

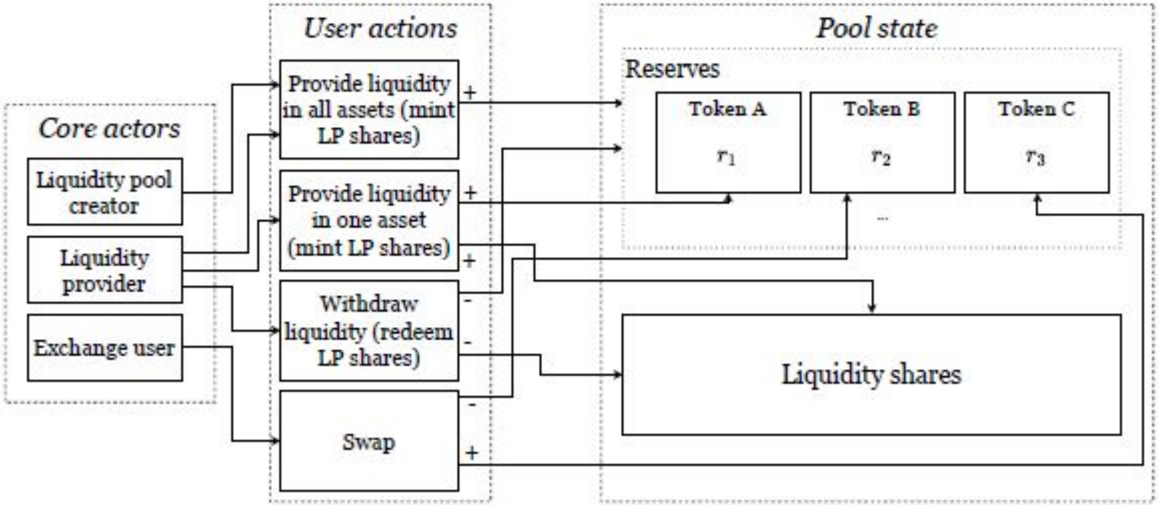


Yield farming Protocols

Protocols for loanable funds (PLF). PLFs enable lending and borrowing of on-chain assets, where the interest rate is set programmatically.

Automated Market Makers (AMM) AMMs provide liquidity from liquidity providers by pooling funds, asset prices are set via a *conservation function*. *Liquidity providers* receive liquidity provider (LP) tokens for their liquidity contribution. *Traders*, swap an input (what to be spent) for an output (what to be received). The exchange rate between the assets is deterministic. The liquidity providers are incentivized using the **Liquidity incentivizing protocol** which can create new tokens, used for staking and have independent value.

AMM Mechanism



Promise

- Decentralized through automation
- Non-custodial
- Openly auditable protocols
- Composability - Defi Stack
- Other people’s code can offer automation advantages (a passive approach)
- Automated strategy can maximise yield
- Pooling transactions make individual execution costs (gas) smaller

Risks

Liquidity risk. In PLFs, as the Utilization rate U approaches 1 Liquidity risk increases. Lenders can have difficulty getting their funds out when U is close to 1.

Liquidation risk. When the value of the collateral falls below a pre-determined liquidation threshold, the borrower receives the collateral minus penalty. Borrowing using stablecoins as collateral decreases this risk.

Composability risks. Risks of complex strategies can be unknown due to crypto-economic complexity and technical weaknesses

Bugs in smart contracts can cause loss of funds.

Recentralization risks Pool operators control smart contracts using admin keys

Interacting smart contracts risk. While two contracts may be secure in isolation, the combination of them may not.

Rewards and Costs in AMM

- Liquidity reward
- Staking reward
- Governance right
- Security reward

- Explicit costs
  - Liquidity withdrawal penalty
  - Swap fee
  - Gas fee
- Implicit costs
  - Slippage
  - Divergent Loss

Conservation function and prices

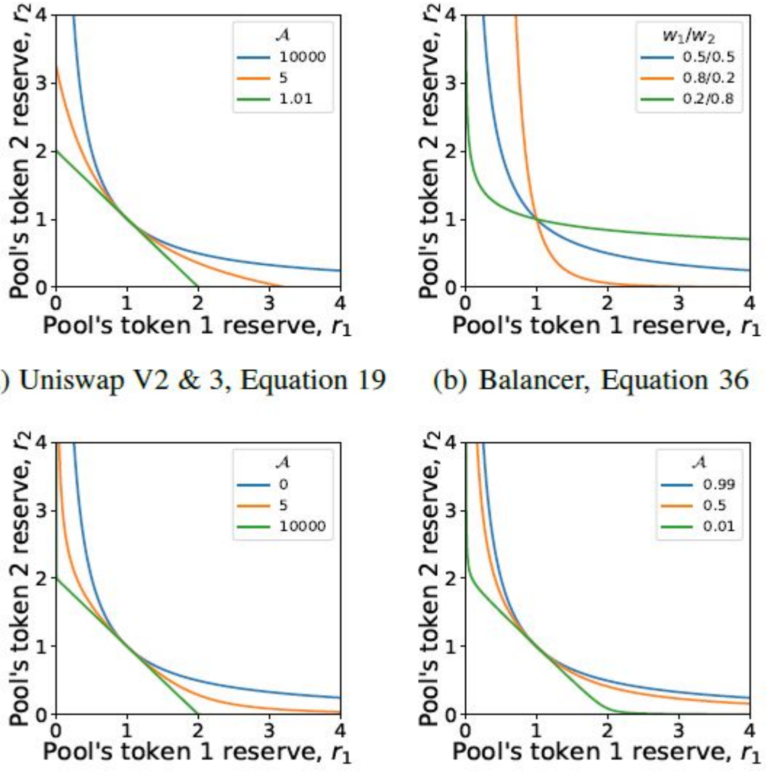
State Changes through pure liquidity changes and pure swaps

Liquidity change ({rk}k=1,...,n, {pk}k=1,...,n, C, Ω) −→({rk}k=1,...,n, {pk}k=1,...,n, C’, Ω)

Swap ({rk}k=1,...,n, {pk}k=1,...,n, C, Ω) −→({rk}k=1,...,n, {p’k}k=1,...,n, C, Ω)

Conservation functions (Bonding Curve)

Constant Sum
Constant Product
Oracle Price



(a) Uniswap V2 & 3, Equation 19

(b) Balancer, Equation 36

(c) Curve, Equation 44

(d) DODO, Equation 50

AMM Attacks

- Oracle Attack (Flash Loan Funded)
- Rug Pull
- Front Running
- Back Running
- Sandwich Attack
- Vampire Attack

References

1. SoK: Yield Aggregators in DeFi
2. SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols
3. Anatomy of a flash loan attack
4. Crypto’s weimar moment