Some notes on decentralized finance

Evan Chow

echow@alumni.princeton.edu

Version 0.1 (August 8, 2024)

These are my informal notes on decentralized finance and specifically on exchanges (DEXs), covering primarily the mechanisms governing the interaction of the entities.

Disclaimer: These come from readings, documentation, academic papers, ChatGPT, my own thoughts and notes, and more. Curated by myself and all corrections welcome.

1 DEX as a four-side marketplace

It seems to me DEXs such as Uniswap are can be regarded as **four-sided** marketplaces: the protocol developers, liquidity providers, traders, and miners. Of course there can be overlap between these.

1.1 Market participants

Each has the incentives and key metrics as follows.

- Protocol developers
  - **Fundamentally, they want to see growth and increasing value of the protocol.**
  - Actions: Develop the platform, release updates, fix bugs. Since they hold protocol tokens, they can vote for protocol changes, and also buy/sell those on secondary markets.
  - Incentives: token allocations (shares in the protocol which may appreciate), possibly protocol fees, grants and funding, bug bounties, other intangibles
  - Metrics: active developers, development activity, support and upgrades, community engagement
- Liquidity providers
  - **Fundamentally, they want to see returns to their liquidity.**
  - Actions: provide/withdraw liquidity, and in return get proportional cut of (staking rewards + ongoing stream of trading fees). Also hold protocol tokens for governance, purchase and resale.
  - Incentives: liquidity mining, staking rewards, tiered incentives, fee share, impermanent loss compensation

  - Metrics: TVL, revenue, active LPs, volume-to-liquidity, churn rate, impermanent loss metrics
- Traders
  - **Fundamentally, they want to see returns to their trades.**
  - Actions: exchange tokens on the protocol (or others) hoping to make a profit.
  - Incentives: reduced trading fees, loyalty programs, trading competitions, subsidies, referral programs
  - Metrics: PNL, trading volume, active traders, microstructural aspects (market depth, order flow toxicity, adverse selection of traders etc.)
- Miners OR validators
  - Miners (proof-of-work)
    - **Fundamentally, they want to see returns to their mining.**
    - Actions: verify and add to the blockchain transactions done by everyone else on the protocol: LPs (changes to liquidity), traders (exchanging tokens), and the protocol developers (upgrades). This is done via **mining**: whoever solves the longest chain of blocks the fastest –¿ gets to add that to the blockchain.
    - Incentives: gas fees from mining, block rewards (may include protocol token), other bonuses around uptime or participation in network upgrades etc.
    - Metrics: active miners, gas fees, transaction throughput (counts, monetary value, hash rates and processing times), competition (transaction ordering, forks).
  - Validators (proof-of-stake)
    - **Fundamentally, they want to see returns to their stakes.** (similar to LPs)
    - Actions: similar to miners, validate and add to the blockchain transactions done by everyone else. This is done via **staking**: validators lock up crypto (stake), and are randomly selected in proportion to their stake to validate
    - Incentives: similar to mining, plus governance via staking rewards
    - Metrics: similar to mining, plus slashing (e.g. downtime / being unavailable)

Note some may only consider this a 2- or 3-side marketplace, if the infrastructure-providing miners/validators (on the settlement layer) are simply fee absorbers and so can be considered part of ”operating costs” by the other parties. We will assume an automated-market making mechanism (AMM) set by the protocol developers.

2 The Uniswap objective function

In this section I restate the Uniswap framework for the objective function of a decentralized exchange protocol [4]. The three main entities are the protocol, LPs (liquidity providers), and traders (liquidity takers). Both the latter are considered users of the protocol. I clean up the notation a little bit.

2.1 Liquidity makers (LPs)

A liquidity provider (LP) aims to maximize **risk-adjusted return** (RAR), as a function of **incentives** (I), **operational costs of the LP** (OM), **the liquidity they provide** (L), and **risk to liquidity** (R).

$$RAR = \frac{I - O - L * R}{L} \tag{1}$$

By rebalancing due to arbitrage, this should be equal between the protocol and other venues, so that we have $RAR_{protocol} = RAR_{market} = RAR$. We assume **liquidity** (L) is a function $\mathcal{L}(.)$ of R, OC, and I, so that we have:

$$L = \mathcal{L}\left(\underline{R}, \underline{OC}, \overline{I}\right) \tag{2}$$

where $\underline{X}, \overline{X}$ informally indicate the sign of contribution to the function (first derivative). For instance, $\mathcal{L}(\underline{R})$ indicates $\mathcal{L} < 0$, assuming the derivative exists.
Note that the revenue from trading fees is reinvested by default.

2.2 Liquidity takers (traders)

A trader aims to maximize the PnL of a trade of **value** V,[1]. This is accompanied by a **price execution** (P) cost consisting of a **trading fee** (F) and **slippage** (S). In short the trader aims to maximize the PnL of the trade:

$$PNL_{trade} = \mathcal{P}(V, \overbrace{F + S}^{P}) \tag{3}$$

Against a different venue, a trader chooses the venue with the highest expected PNL (imprecisely):

$$\mathbb{E}[PNL_{trade}] = PNL_{trade} - AltPNL_{trade} \tag{4}$$

which equals the difference in fees, since the trade values cancel out.
The goal of the trader is to maximize the PNL of all trades, minus some **fixed operating costs of the trader** (OT):

$$PNL_{overall} = \sum_{trade \in trades} PNL_{trade} - OT \tag{5}$$

2.2.1 Aggregating up to exchange.

The **volume on the exchange** (VOL) is a function of the above, specifically the trading costs (P=F+S) and the operating costs faced by the trader (OT):

$$VOL = \mathcal{V}(\overbrace{\underline{F + S}}^{P}, \underline{OT}) \tag{6}$$

[1]Let this be positive, so that "value" is captured by either buys or sells.

2.3 The protocol and its developers

2.3.1 Maximizing protocol value via its tokens

Both LPs and traders are users of the protocol and must use the protocol's particular "pool token" to participate, which is a token separate from those in the reserves.

- These pool tokens represent "shares" in the protocol reserves.
- LPs receive (burn) these pool tokens in order to provide (withdraw) liquidity to the protocol reserves. Moreover, LPs receive a cut of trading fees proportional to how many pool tokens (share of the pool) they hold.
- Traders do not usually receive or burn tokens.

These pool tokens, which are held by LPs, represent "shares" in the reserve and yield "dividends" (yields from trading activity). Similar to stocks, these offer value to the tokenholders (LPs) in several ways.

Value proposition 1 (Yields). The yield of the tokens can be analyzed via discounted future cash flow analysis. Let the **present value of a token** (PV) be the sum of **future cash flows** (FCF) according to some **discount rate** (r) over times $t = 1 \dots T$:

$$PV = \sum_{t=1}^{T} \frac{FCF_t}{(1+r)^t} \tag{7}$$

What is a future cash flow (cash flow at time t)? To the LP, it is the volume of trading multiplied by the unit trading fee of the protocol,[2] to obtain the total gain.

$$\begin{aligned}
FCT_t &= \overline{VOL_t} * \overline{F_{protocol}} && \text{future gain to LP} && (8)\\
&= \overline{\mathcal{V}(\underline{F+S}, \underline{OT})} * \overline{F_{protocol}} && \text{use volume on the exchange} && (9)\\
&\text{let slippage be inverse to liquidity: } S = \mathcal{S}(\underline{L}) && && (10)\\
&= \overline{\mathcal{V}(\underline{F + \mathcal{L}\left(\underline{R}, \underline{OC}, \overline{I}\right)}, \underline{OT})} * \overline{F_{protocol}} && \text{liquidity faced by LPs} && (11)\\
&= \overline{\mathcal{V}}(\underline{R}, \underline{OC}, \overline{I}, \underline{F}, \underline{OT}) * \overline{F}_{protocol} && \text{net directions of impact} && (12)
\end{aligned}$$

Value proposition 2 (Governance). The tokenholder also obtains the ability to vote on decisions made to the protocol. The importance of **governance** (G) is heuristically given as a function of **brand** (B), **market share** (M), and **size** (S):

$$G = \mathcal{G}\left(\overline{B}, \overline{M}, \overline{S}\right) \tag{13}$$

Value proposition 3 (Secondary market). This is only implied, but there is also a secondary market for buying-and-selling the protocol tokens.

[2] Compare with the fee F faced by the trader.

2.3.2 Cost-benefit approach to assessing proposals

A proposal to change the protocol must be evaluated via cost-benefit analysis. The **net benefit** (NB), which is the sum of **benefits** (Benefits) and **costs** (Costs), must be positive.

$$NB = Benefits - Costs \tag{14}$$

Funding proposals often occurs via the protocol tokens. To fund a proposal, one must estimate the **cost** of the proposal, which is notionally the product of the **quantity of tokens spent** (TS) and the **market price** (MP) of the tokens, which is a spot exchange rate.[3] Thus, the cost is in the units of a non-protocol-token numeraire.

$$Costs = MP * TS \tag{15}$$

Overall, how do we specify the net benefit? We can specify this in several ways, depending if we consider the benefit to be the stream of future cash flows and governance value.

$$\Delta NB_{FCF} = \Delta PV - Costs \quad \text{stream of future cash flows w/stationary fixed costs} \tag{16}$$

$$\Delta NB_{gov} = \Delta G - Costs \quad \text{governance} \tag{17}$$

$$\Delta NB_{overall} = \Delta PV + \Delta G - Costs \quad \text{overall} \tag{18}$$

Intuitively, we consider the net benefit today to be our expected stream of benefits (present value + governance), minus today's costs. □

2.4 Miners

This is not mentioned, but it is also worth thinking about the incentives for miners / validators. Miners should have something similar to liquidity providers:

$$Benefit_{miner} = I(M) - OP(M) \tag{19}$$

where for some level of **mining activity** (M), they obtain **incentives** (I) which include gas fees (or for validators - staking rewards), minus **operating costs** (OP).

3 State representation of a DEX protocol

This adapts the framework of [5] which can be used to model AMM protocols such as Uniswap (V2-V3), Balancer, Curve and more. This focuses on the **mechanisms** of exchange rather than the incentives. Denote times $t \in \mathcal{T} = \{1 \dots T\}$ and tokens $k \in \mathcal{K} = \{1 \dots K\}$.

[3] Note this does not include price impact on the spend

3.1 System states

The state(s) of the protocol is given by the **market data** at any given time t. This includes, for each token k and quantity $r_k \in \mathbb{R}_+$. In addition, there is a conservation function invariant[4] $\mathcal{C} \in \mathcal{R}_+$, and other protocol hyperparameters Ω.

$$\mathcal{X} = (\{r_k\}_k; \mathcal{C}, \Omega) \tag{20}$$

Spot prices (exchange rates) are implicit because in the decentralized AMMs we consider, they are derived directly from the relative reserves balances. For instance, in Uniswap the spot price, trading x for 1 unit of y, is given by (r_x/r_y).

There is a state transition function encoded in the protocol so that $\mathcal{X}_t \to_a^f \mathcal{X}_{t+\Delta}$, for some admissible action $a \in \mathcal{A}$ as to trigger the state transition function f.

3.2 The conservation function

Concisely denote a conservation function $Z : \mathbb{R}^k \times \mathbb{R}_+ \to \mathbb{R}_+$ maintains an invariant relation between a function $C : \mathbb{R}_+^k \to \mathbb{R}$ of the reserve quantities $\{r_k\}_k$ and the conservation constant $\mathcal{C}$.

$$Z(\{r_k\}_k; \mathcal{C}) = C(\{r_k\}_k) - \mathcal{C} = 0 \qquad \textbf{the conservation function} \tag{21}$$

Both $C(.)$ and $\mathcal{C}$ can be thought of in terms of "total wealth of the system," hence why conservation-preserving liquidity contribution increases both terms. (See the actions of the LPS below.)
For example, in UniSwap we only have $k = 2$ and so we have:

$$Z^{Uniswap}(\{r_k\}_k; \mathcal{C}) = r_1 r_2 - k = 0 \tag{22}$$

which corresponds to the famous $xy = k$ equation. (Note the signs for below.)

3.3 From reserves to spot prices

Spot prices are given by the instantaneous ratio between reserves. Consider exchanging token i for token j ($i, j \in \mathcal{K}$). The price of token j in terms of i is given by how many i I need to contribute for 1 "unit" of j, so that its derivative goes on the bottom.

$$P_{ij}(\{r_k\}_k; \mathcal{C}) = \frac{\partial Z/\partial r_j}{\partial Z/\partial r_i} = \frac{\partial Z}{\partial r_j} \cdot \frac{\partial r_i}{\partial Z} = \frac{\partial r_i}{\partial r_j} \tag{23}$$

In the constant-product Uniswap/Balancer framework we simply obtain the ratio r_i/r_j (directly how much i wrt. 1 unit of j). This can be obtained by taking the total derivative:

$$\frac{\partial}{\partial r_j}\left[r_i r_j - k\right] = r_i * 1 + \frac{\partial r_i}{\partial r_j} * j = 0 \tag{24}$$

$$\Rightarrow \frac{\partial r_i}{\partial r_j} = -\frac{r_i}{r_j} \equiv \frac{r_i}{r_j} \tag{25}$$

where we have removed the negative sign since we have positive prices.

[4] Note, this may be multiple.

3.4 Actions of agents

We focus on liquidity providers and traders.

Liquidity providers (LPs) can add or withdraw liquidity in a proportion-preserving amount across all reserves, so that the relative proportions are preserved. This corresponds to an outward (inward) movement of the reserves frontier. Their set of admissible actions can be summarized as selecting $a^{LP} \in \mathcal{R}_+$ such that the proportions are preserved:

$$(\{r_k, p_k\}_k; \mathcal{C}, \Omega) \to \left(\{a^{LP} * r_k, p_k\}_k; \mathcal{C}, \Omega\right) \tag{26}$$

Traders can exchange one token for another, subject to the conservation law and noting they will receive a quantity and price determined by the protocol.

$$(\{r_k, p_k\}_k; \mathcal{C}, \Omega) \to (\{r'_k, p'_k\}_k; \mathcal{C}, \Omega) \tag{27}$$

We do not cover objective functions here, nor the actions of protocol developers and miners.

3.5 Mechanics of a Uniswap trade ($k = 2$).

Suppose there are two tokens x and y, and you want to exchange $\Delta x > 0$ ("principal") in order to get some amount $\Delta y > 0$ ("proceeds"). Of course, you know the protocol, so all this will be transparent to you.

3.5.1 Trade calculation analysis.

Pre-trade, spot price of y. As above, this is given by x/y, since we are interested in how much x we need to exchange to get for 1 "unit" of y.

Post-trade, proceeds. The conservation law implies, for some constant $K > 0$:

$$xy = (x + \Delta x)(y - \Delta y) = K \tag{28}$$

Solve for the proceeds Δy:

$$xy = xy + \Delta xy - x\Delta y - \Delta x\Delta y \tag{29}$$

$$\Rightarrow \Delta xy = x\Delta y + \Delta x\Delta y \tag{30}$$

$$\Rightarrow \Delta y = \frac{\Delta xy}{(x + \Delta x)} \qquad \textbf{proceeds} \tag{31}$$

Post-trade, price. Similar to the spot calculation we obtain:

$$\frac{\partial}{\partial y}\left[(x+\Delta x)(y-\Delta y)\right] = \frac{\partial}{\partial y}\left[xy + \Delta xy - x\Delta y - \Delta x\Delta y\right] \tag{32}$$

$$= \left(x + \frac{\partial x}{\partial y}y\right) + \Delta x - \frac{\partial x}{\partial y}\Delta y = 0 \tag{33}$$

$$= (x+\Delta x) + \frac{\partial x}{\partial y}(y-\Delta y) = 0 \tag{34}$$

$$\Rightarrow \frac{\partial x}{\partial y} = -\frac{x+\Delta x}{y-\Delta y} \equiv \frac{x+\Delta x}{y-\Delta y} \qquad \textbf{execution price} \tag{35}$$

Note since $\Delta x, \Delta y > 0$, this implies that the execution price (how much you have to pay for a unit of y) is more expensive than spot, by construction:

$$0 \leq \underbrace{\frac{x}{y}}_{spot} \leq \frac{x}{y-\Delta y} \leq \underbrace{\frac{x+\Delta x}{y-\Delta y}}_{execution} \tag{36}$$

Calculating slippage. Slippage in units is given by the absolute or percentage difference of execution (higher) vs. spot (lower).

Impermanent (divergence) loss. This can be calculated via several steps, which may/may not have an analytical solution. Note this only calculates the impermanent loss for a small change in one token.

- First, calculate the base value of the tokens held in the pool, for tokens $j \in \mathcal{K}$ and where the prices are standardized against some numeraire token i.

$$V = \sum_j p_{ij} r_j \tag{37}$$

- Calculate the value if some token o appreciates by some $\delta \in (0,1)$ and is held outside the pool.

$$V_H = \sum_{j \neq o} p_{ij} r_j + (p_{io} r_o)(1+\delta) \tag{38}$$

$$\text{with } o\text{'s pool amount in the sum: } (p_{io} r_o)(1) \tag{39}$$

$$= V + (p_{io} r_o)\delta \tag{40}$$

  Here you can stop if you only care about this market value.

- Now calculate the equivalent value if the gain is implemented within the pool, so that the reserves are rebalanced respecting the protocol. This consists of $n-1$ equations, plus the conservation law, for n unknowns $\{r'_k\}_k$ that yield the prices.

$$\forall j : (1+\delta) = \frac{p'_{jo}}{p_{jo}} \qquad p'_{jo} \text{ a function of new states } \{r'_k\}_k, \{p'_k\}_k \tag{41}$$

$$Z(\{r'_k\}_k; \mathcal{C}) = 0 \tag{42}$$

After solving these, calculate the equivalent pool value:

$$V_{pool} = \sum_j p'_{ij} r'_j \tag{43}$$

- Lastly, the impermanent loss is given by the percentage difference:

$$IL = \frac{V_H}{V_{pool}} - 1 \tag{44}$$

3.5.2 Case study: comparative statics between counterparties

Assuming we are using Uniswap (x, y), let's say a trader correctly predicts an upward price movement: for $t \to t + h$, the movement is $p_t < p_{t+h}$, and so the trader buys q and then later sells q. How does this affect all parties?

- The trader makes profit $(p_{t+h} - p_t)q$, paying transaction costs (s_t, s_{t+h}) respectively.
- Transaction fee = protocol fee + gas fee. Protocol fees go to the LPs and maybe the protocol.
- The protocol earns protocol fees.
- The miner earns gas fees.
- What about the liquidity providers? They suffer a little due to impermanent loss (the market maker counterparty risk) but also earn part of the protocol fees. For the first part:
  - Initial state: $(x, y) : xy = k > 0$, with price of y given simply by the ratio:

$$p_y = \frac{x}{y} \tag{45}$$

  - At time t: trader buys q of x to purchase y. This means the new reserves are $(x+q, y-\Delta y)$ where from before we have:

$$\Delta y = \frac{\Delta x y}{x + \Delta x} = \frac{qy}{x + q} \tag{46}$$

  - Hence the new price of y is now:

$$p'_y = \frac{x+q}{y - \Delta y} = \frac{x+q}{y - \frac{qy}{x+q}} = \frac{(x+q)(x+q)}{y(x+q) - qy} = \frac{(x+q)^2}{xy} \tag{47}$$

  - Now consider p, the ratio of the new price of y to the old:

$$p = \frac{p'_y}{p_y} = \frac{(x+q)^2}{xy} \cdot \left(\frac{y}{x}\right) = \frac{(x+q)^2}{x^2} > 0 \tag{48}$$

    At this point it is helpful to recall that because we have put in an additional amount $q > 0$, and there is now more x in the pool, we therefore see the price of y get more expensive. Thus $p > 0$.

– For Uniswap, the impermanent loss formula for this movement from $p_y \to kp_y, k > 0$ is given by:

$$IL(k) = \frac{2\sqrt{k}}{1+k} - 1 \qquad \textbf{impermanent loss,}\ k > 0 \tag{49}$$

This is always nonpositive (LPs lose notational value) and bounded between [-1, 0].

– Computing the impermanent loss with $k := p$ we obtain:

$$IL = \frac{2\sqrt{(x+q)^2/x^2}}{1+(x+q)^2/x^2} - 1 = \frac{2(x+q)/x}{1+(x+q)^2/x^2} - 1 \tag{50}$$

$$= \frac{2z}{1+z^2} - 1 \qquad \text{set } z = 1 + (q/x) \tag{51}$$

$$= \frac{2(1+q/x)}{1+(1+(q/x))^2} - 1 \tag{52}$$

$$\text{multiply out:} \tag{53}$$

$$\Rightarrow IL = \frac{2(x+q)}{x+2q+q^2} - 1 = \frac{x-q^2}{x+2q+q^2} \tag{54}$$

So since we always have $x, q > 0$, whether the liquidity providers suffer impermanent loss (loss = positive) depends on the traded amount.

- If the trader puts in only a little bit of q, so that $q^2 < x$, the impermanent loss will be positive and so the liquidity providers will **lose notional value.**
- Vice-versa if the trader puts in too much: the impermanent loss will be positive and so liquidity providers will **gain notational value**.

Why is this? As above: trading activity can counteract the impermanent loss (always negative), so that the LPs can sometimes gain net value when the ratio becomes favorable.