Constant Function Market Makers

Waylon Jepsen
Department of Computer Science, Colorado State University
Primitive Bits, 2022

Motivation

A collection of prominent financial exchanges have been built in distributed computing environments made available by blockchains.

- **Inspired by a desire for sovereignty and ownership**, contrasting risk acquired from trusted asset custodians [3].
- **Necessary monetary constraints on computation and storage in blockchains** [2] have driven CFMMs to be the dominant DEX architecture [1].
- Currently **accounting for more than $75B worth of assets**, the decentralized financial landscape should be taken seriously and requires rigorous study.

Order-Books as Constant Sum Markets

$\varphi := P_1 R_1 + P_2 R_2$

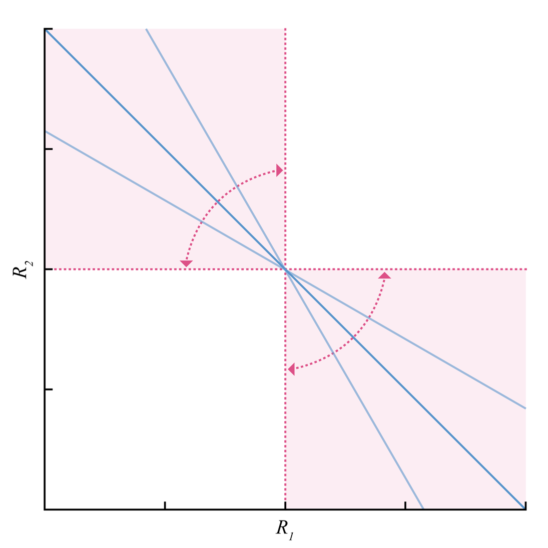

Figure 1: Constant Sum Trading Functions

Price: Slope of target line at a point

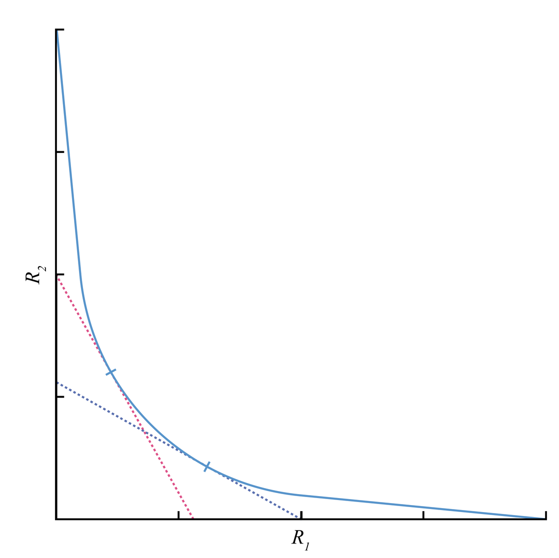

Figure 2: Constant Product Trading Function

- The ***gradient of the multivariate function*** gives information as a ***reported price***.
- An **Order-Book** can be thought of as an infinite combination of constant sum markets over all $P \in \mathbb{R}_+$ Such that the slope always monotonically decreasing and touches both axis.
- **Computational restrictions** of blockchains make this expensive.
- Construct a **single convex curve** instead, where the gradient at a point on the curve represents the exchange rate.

Transaction Ordering

- In the **Ethereum Blockchain** transactions are processed by miners of the network.
- An economic incentive exists to process transactions in **order of most profitable**.
- Because blocks have a finite amount of space, transaction priority is given to transactions with highest fees.

$k \in K$ s.t.
$|K| = h, k_h > k_{h-1} \ldots > k_0$

Block: n

$\mathbf{tx}_1$: fee: k_h
$\mathbf{tx}_2$: fee : k_{h-1}
$\mathbf{tx}_2$: fee : k_{h-2}
...

Figure 3: Preferential Transaction Ordering

If a block in the past has monetary value to be extracted (through reordering), and that value is greater than the computational cost of acquiring large influence over the network, then a consensus instability exist.

Independent Actors of CFMMs

$\varphi_{Uniswap} := R_1 R_2$

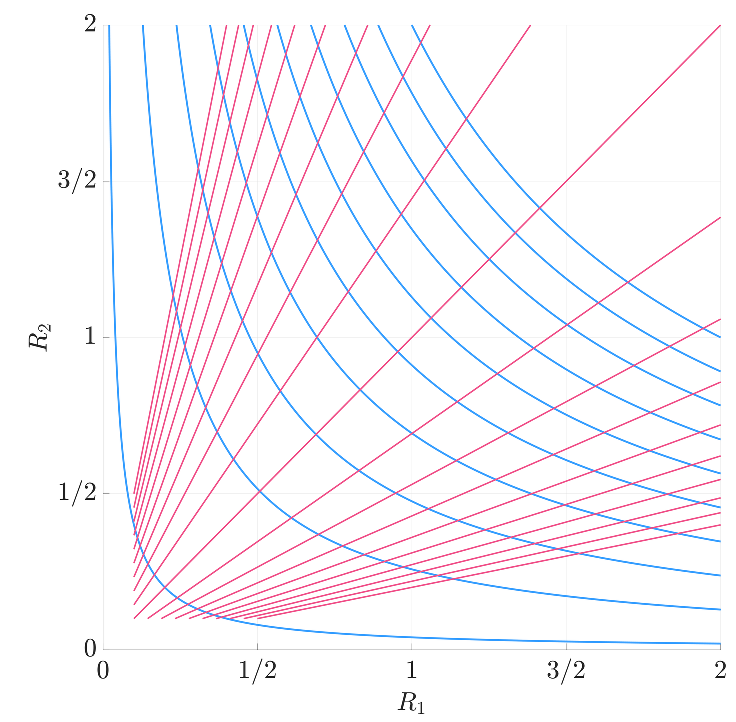

Figure 4: Contrast of Liquidity Providers and Traders on a Constant Product Market

$\varphi_{rmm} := -K\Phi(\Phi^{-1}(1-R_1) - \sigma\sqrt{\tau}) + R_2$

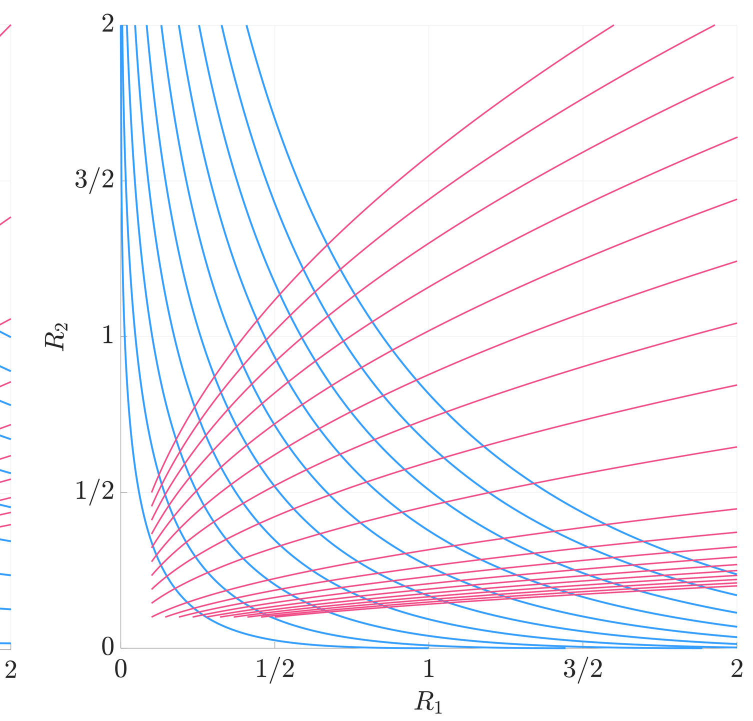

Figure 5: Contrast of Liquidity Providers and Traders on RMM-01

- Trades taken by **liquidity providers** shift the curves along the pink curves.
- Trades taken by **swappers** shift the price along the blue curves.

Properties and Definitions

- A CFMM is an n-*asset pool* $\mathbb{R}^n_+$, and a ***trading function*** φ such that $\varphi : \mathbb{R}^n_+ \to \mathbb{R}$ Given any $\mathbf{R}$, the value $\varphi(\mathbf{R}) = k$ is called the ***invariant***.
- The reserves of n assets $\boldsymbol{R} \in \mathbb{R}^n_+$ is called an ***n-asset liquidity pool*** where for every $i \in \{1,\ldots,n\}$, the quantity R_i represents the quantity of asset i in the pool.
- Let $\boldsymbol{\Delta}, \boldsymbol{\Lambda} \in \mathbb{R}^n_+$ and be the ***tendered*** and ***received*** basket, respectively. We refer to the tuple, $(\boldsymbol{\Delta}, \boldsymbol{\Lambda}) \in \mathbb{R}^n_+ \times \mathbb{R}^n_+$, as a ***proposed trade***.
- Let $(\boldsymbol{\Delta}, \boldsymbol{\Lambda}) \neq 0$, then this trade is a ***valid swap*** if $\varphi(R + \gamma\boldsymbol{\Delta} - \boldsymbol{\Lambda}) = \varphi(R)$ where $\gamma \in [0,1]$ denotes the swap fee accrued by the liquidity providers.
- Given a CFMM the ***price vector*** is $\boldsymbol{P} := \nabla\varphi$, the ***reported price*** of asset i is $p_i := \dfrac{P_i}{P_n}$, and the ***value of the reserves*** is $V := \dfrac{1}{P_n}\boldsymbol{P}^T\boldsymbol{R}$.

Time Varying CFMM: RMM-01

$\varphi_{rmm} := -K\Phi(\Phi^{-1}(1-R_1) - \sigma\sqrt{\tau}) + R_2$

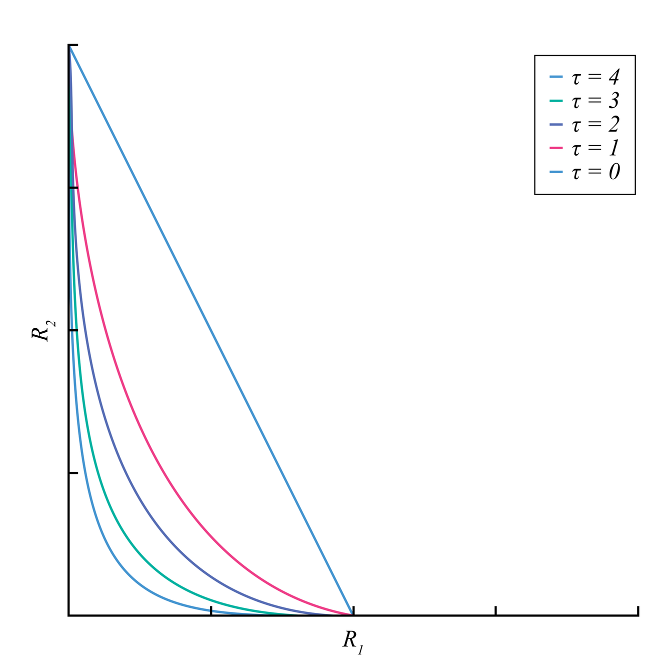

Figure 6: RMM-01 Varying over τ

- Some CFMMs change over time.
- An example is the RMM-01 Curve replicating the payoff of a covered call to liquidity providers
- RMM-01 approaches a single price as $\sigma\sqrt{\tau} -> 0$.
- Changes price impact of trades over time.
- Optimal arbitrage dependes on $\sigma\sqrt{\tau}$.

Maximal Extractable Value

A number of fascinating phenomena analogous to high frequency trading in traditional finance has arisen from the design of these markets. Commonly referred to as *Maximal Extractable Value (MEV).*

- **Arbitrage:** Profit generated from pricing discrepancies. Arbitrage is widely considered as a positive phenomena as it increases market efficiency.
- **Liquidations:** Profit from liquidating under-collateralized loans. While at a cost of the lender, a necessary mechanism to prevent bad debt.
- **Sandwiches:** As a consequence of *price impact,* a necessary trade-off from CFMMs. Dictated by the graph of the curvature of the trading function. This is at the cost of the users

Modeling Trades on CFMMs

$\varphi_{Uniswap} := (R_1 + \gamma\Delta)(R_2 - \Lambda)$

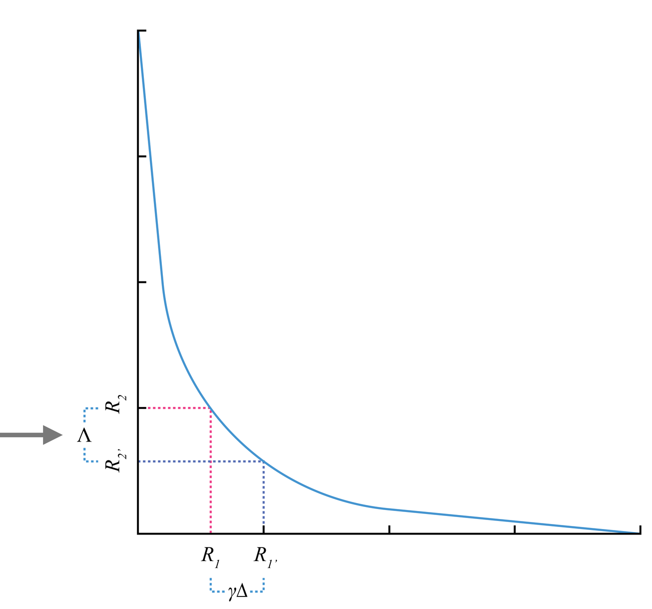

Figure 7: Constant Product Trade

$\varphi := P_1(R_1 + \gamma\Delta) + P_2(R_2 - \Lambda)$

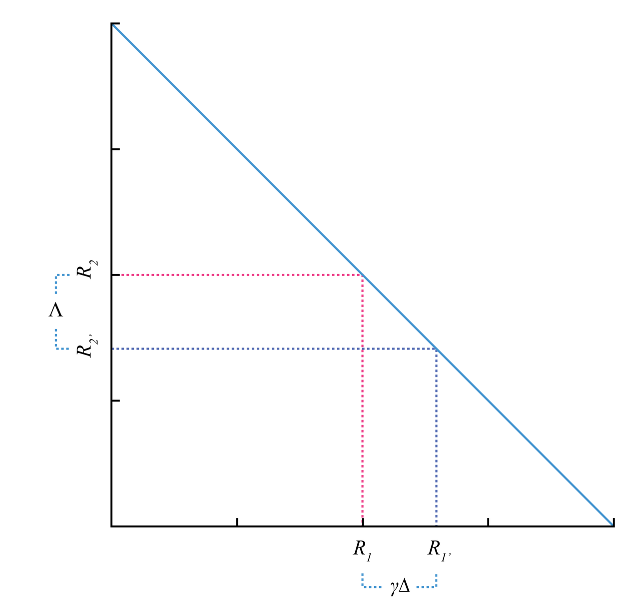

Figure 8: Constant Sum Trade

- Here we can see a ***valid swap*** on both a Constant Product and a Constant Sum CFMM.
- Notice the swap on the Constant Sum CFMM doesn't change the price but it does on the Constant Product CFMM.

Open Research Questions and Impact

- Can we construct **MEV aware design principles** to mitigate negative implications?
- **What risk can we eliminate** by removing asset custodians?
- **Understand, account for, and secure** 75B worth of assets in this ecosystem
- How does **change in consensus architecture** impact this phenomena?

"Trust Math not People"

References

[1] Guillermo Angeris, Akshay Agrawal, Alex Evans, Tarun Chitra, and Stephen Boyd. Constant Function Market Makers: Multi-Asset Trades via Convex Optimization. page 31, July 2021.

[2] Campbell R Harvey, Ashwin Ramachandran, and Joey Santoro. 2021. DeFi and the Future of Finance. John Wiley & Sons.

[3] Tim Roughgarden. Transaction fee mechanism design for the ethereum blockchain: An economic analysis of eip-1559. arXiv preprint arXiv:2012.00854, 2020.