TL;DR:

We discover that negative liquidity is possible and construct an AMM to access the negative domain by allowing the price to go negative. The invariant for a negative price happens to be the formula for a circle and the liquidity distribution happens to have a power law tail. You can interact with and compare it to an RMM here. Most interesting points are outlined below with link to paper at the end.

[

Screenshot 2023-12-14 at 2.05.07 AM

2294×1734 172 KB

](https://ethresear.ch/uploads/default/original/2X/2/2aa7f87f50d43b6ca8c3608ca6d021214a3693c2.jpeg)

Figure 1

:Two negatively priced assets can be exchanged between each other for a positive price. An impossible task in tradfi, requiring a fiat numeraire to act as an intermediary.

Summary:

Swapping and liquidity provision transactions of a Concentrated Circular Market Maker (CCMM

) are obfuscated using Fully Homomorphic Encryption (FHE) to mitigate MEV in the public mempool by combining game theory with the Kelly criterion. Liquidity of the CCMM is adjusted using a scale parameter and can be modified with a hook in Uniswap v4. We show how it is possible to enter the negative liquidity domain with the CCMM.

Negative Liquidity

If we look at a Constant Product Market Maker (CPMM) such as Uniswap, we can see that it happens to provide liquidity in the negative domain. Take the Uniswap Invariant with liquidity L

$xy=L^2$

introducing price p

as $p = y/x$

and $y = px$

$xpx=L^2$

solving for x

$x=\sqrt{\frac{L^2}{p}}$

note the appearance of a negative sign

$x=\pm\frac{L}{\sqrt{p}}$.

It's just difficult to access this negative liquidity in Uniswap due to the invariant being a hyperbola. By pressing the invariant against the axes, concentrating liquidity, and folding it on itself we can travel to the negative domain. A liquidity provider may become a liquidity taker with the following invariant where z

is a scale parameter

$(x-z)^2 +(y-z)^2 =z^2$.

We like to call it the DiracAMM (Paul Dirac discovered anti-matter with a similar trick by seeing that energy $\sqrt{E^2}$

could have a negative value in theenergy-momentum relation). One can program the invariant to not provide liquidity after touching the axes though, in which case its liquidity distribution L

happens to be the Student's-t distribution with degree of freedom df=2

, a special case of a power law tail where the law of large numbers has no predictive capacity on thevariance.

$L_{Student-t}(x) = \frac{1}{(1+x^2)^\frac{2}{3}}$

LP Payoffs

If price, following a power law, is allowed to flow into the negative, as is empirically observed with various assets, then the LP payoff function happens to resemble a collection of non-linear payoffs.

[

f4

3072×1536 396 KB

](https://ethresear.ch/uploads/default/original/2X/2/26bcfee31f3367d0f7f7c86d0e2508a53489be9b.jpeg)

But it's not necessary though for the underlying price to be negative for this AMM to be useful. Rather, one suggestion is to use the price of $0 as an offset from the current underlying price of, let's say $100 . A negative 1 price indicates a decline of the underlying from $100 to $99. If the CCMM has one asset that can not go negative, such as a stablecoin, then it can only have LP payoffs 2A2

and 2B2

, but by borrowing the LP position through a lending protocol one could mimic the payoffs of 2D2

and 2C2

respectively.

MEV approach with Kelly Criterion and FHE

Since a gain and a loss can be defined as an offset with a CCMM, we can combine it with the game theory behind rational MEV decision makers who follow the Kelly criterion, a strategy that ensures long-term optimal geometric growth

$f* = p - \frac{1-p}{b}$

where $f*$

represents a MEV extractor's portfolio allocation in a MEV attack with the probability of success p

and betting odds b

. By targeting Kelly-neutrality

we set a MEV extractor's Kelly betting amount f = 0

at an increased gas cost by rearranging for the following equality to hold

$p=\frac{1-p}{b}$.

We do so by introducing two encrypted boolean values (ebool) for swapping $B_{swap}=[0,1]$

and providing liquidity $B_{LP}=[0,1]$

going into the mempool. Where the boolean value can mean 1 for swap x for y and 0 for swap y for x (or remove and re-add liquidity for B_{LP}

). We can also encrypt the swap quantity dx

(or dy

) as euints, thereby making it unclear what the betting odds b

(gain and loss relationship) are.

$E(B_{swap/LP})=\frac{1-E(B_{swap/LP})}{\frac{E(Gain)}{E(Loss)}} = \frac{1-0.5}{\frac{x}{x}}=0.5$

Setting the expected value of a MEV extractor's Kelly bet $E(f*) = 0$. Targeting Kelly-neutrality could be a useful mechanism for MEV. We noticed that with FHE we can selectively target just the variables we want to obfuscate enough without having to encrypt everything and think that this approach could be useful to others looking into MEV.

Further work

An approach to avoid negative prices for the underlying could be to construct a passive wall of liquidity

, a liquidity fingerprint that asymmetrically increases non-linearly as price approaches zero, denting price impact. The super-heavy tailed distributions like the Log-Cauchy distribution with concentration parameter c

come to mind with liquidity fingerprint in price space being

$$L_{Log-Cauchy}(p) = \frac{1}{\pi p} \frac{c}{ln(p)^2+c^2}.$$

[

f44

1920×1920 236 KB

](https://ethresear.ch/uploads/default/original/2X/2/24b37c0e2b2d52fb38f2be8db48606f43be14827.jpeg)

This is a very interesting liquidity fingerprint because it captures what we see in crypto where some tokens stay where they are, the majority approach the zero bound, and a select few fly towards the right tail. One of the mathematical challenges here being that liquidity spikes to infinity at 0 though.

Our paper with more interesting details is on GitHub