

# Arbitrageurs' profits, LVR, and sandwich attacks: batch trading as an AMM design response.\*

Andrea Canidio<sup>†</sup> and Robin Fritsch<sup>‡</sup>

July 11, 2023

## Abstract

We consider an automated market maker (AMM) in which all trades are batched and executed at a price equal to the marginal price (i.e., the price of an arbitrarily small trade) after the batch trades. We show that such an AMM is a *function maximizing* AMM (or FM-AMM): for given prices, it trades to reach the highest possible value of a given function. Competition between arbitrageurs guarantees that an FM-AMM always trades at a fair, equilibrium price, and arbitrage profits (also known as LVR) are eliminated. Sandwich attacks are also eliminated because all trades occur at the exogenously-determined equilibrium price. We use Binance price data to simulate the lower bound to the return of providing liquidity to an FM-AMM and show that this bound is very close to the empirical returns of providing liquidity on Uniswap v3 (at least for the token pairs and the period we consider).

**Keywords:** Arbitrage profits, Loss-vs-Rebalancing (LVR), MEV, Sandwich attacks, AMM, Mechanism design, Batch trading

## 1 Introduction

Constant Function Automated Market Makers (CFAMMs) are the centerpiece of decentralized finance. Their popularity is largely due to their simplicity: the price at which a given CFAMM is willing to trade depends exclusively on the size of its liquidity pools. One important consequence is that trades occurring on the same

---

\*We are grateful to Felix Leupold and Martin Köppelmann for initial discussions on batch trading on AMM that led to the writing of this paper. We also thank Haris Angelidakis, Eric Budish, Agostino Capponi, Felix Henneke, Fernando Martinelli, Ciamac Moallemi, Andreas Park, and Anthony Lee Zhang for numerous comments and suggestions.

<sup>†</sup>Corresponding author; CoW Protocol; andrea@cow.fi

<sup>‡</sup>ETH Zurich and CoW Protocol; rfritsch@ethz.ch

CFAMM within the same block pay different prices depending on the order in which they are executed.

This design has two well-recognized flaws. First, liquidity providers (LPs) trade at a loss whenever there is a rebalancing event. More precisely, when the underlying value of the assets changes, the first informed arbitrageur who trades with the CFAMM earns a profit by aligning the CFAMM price with the new equilibrium price. These profits are at the expense of LPs, who suffer a “loss-vs-rebalancing” (LVR). Second, traders are routinely exploited by attackers, most commonly via sandwich attacks in which an attacker front-runs a victim’s swap with the same swap and then back-runs it with the opposite swap. Doing so allows the attacker to “buy cheap” and “sell expensive” while forcing the victim to trade at less favorable terms.

This paper proposes a novel AMM design that avoids both problems. In its simplest form, we propose that all trades that reach the AMM during a period are batched together and executed at a price equal to the new marginal price on the AMM – that is, the price of executing an arbitrarily small trade after the batch trades. We derive the trading function of such an AMM and show two interesting equivalences. First, this AMM is *function maximizing* because, for given prices, it maximizes the value of a given function subject to a budget constraint. For this reason, we call our design a function-maximizing AMM, or *FM-AMM*. Also, if the function is a standard Cobb-Duglas objective function (i.e., the weighted sum of two natural logs), then for given prices, the FM-AMM LPs run a passive investment strategy: absent trading fees, the total value of the two pools is shared between each pool according to some pre-specified weights. Finally, we show that an FM-AMM does not satisfy path independence: traders can obtain a better price by splitting their trades into smaller orders, which is why batching is required.

Our main contribution is to consider the behavior of such an AMM in the presence of arbitrageurs, who have private information relative to the equilibrium prices (determined, for example, on some very liquid off-chain location). Competition between arbitrageurs guarantees that the batch always trades at the equilibrium price, and arbitrage profits are eliminated. Intuitively, if this were not the case, some arbitrageurs would want to trade with the batch and, by doing so, would push the price on the batch in line with the equilibrium. This also eliminates all forms of MEV extraction, such as, for example, sandwich attacks: arbitrageurs will always act so to remove deviations from the equilibrium price, therefore making it impossible to manipulate the FM-AMM price. The benefit of contributing liquidity to an FM-AMM relative to a traditional CFAMM is that FM-AMM LPs earn the arbitrage profits generated by rebalancing the CFAMMs. Because these arbitrage profits are larger for more volatile prices (as they lead to more frequent and larger rebalancing, see Milionis et al., 2022 and Milionis et al., 2023), holding everything else equal, the benefit of providing liquidity to an FM-AMM relative to a CFAMM increases with

the price volatility.

We then use price data to simulate the return of providing liquidity on an FM-AMM, and compare the simulated return with that earned by liquidity providers on Uniswap v3 (currently the most important AMM). To do so, we consider an FM-AMM that does not charge fees for including an order on the batch, but only on the net amount that is then settled on the FM-AMM. Such FM-AMM earns fees from arbitrageurs but not from noise traders, because arbitrageurs always absorb trades from noise traders before they reach the FM-AMM. It is a valuable benchmark because we can use historical price data to compute the trade necessary to align the FM-AMM price with the new reference price, the resulting trading fees, and the evolution of the liquidity pools. Hence, our results do not rely on assumptions about the size and distribution of noise trades reaching the FM-AMM. Of course, the caveat is that the estimated return to providing liquidity to an FM-AMM is the lower bound of a more general case in which noise trades generate fees.

The first part of our empirical analysis compares the historical returns of providing liquidity to some Uniswap v3 pools to a counterfactual in which the same liquidity is contributed to our simulated FM-AMM, under the assumption that the FM-AMM rebalances at the same frequency and charges the same fee as the Uniswap v3 pool.<sup>1</sup> Because the FM-AMM always trades at the equilibrium price, the return on providing liquidity to the FM-AMM is determined by the variation in the price of the underlying assets (which can be fully hedged, see Milionis et al., 2022). The return on providing liquidity on Uniswap v3 also depends on the price variation, plus the fees earned from noise traders and minus arbitrage profits. Comparing the return of providing liquidity on the two AMMs allows us to establish whether, during a given period and for a given token pair, Uniswap LPs earned more in trading fees from noise traders than their loss to arbitrageurs.<sup>2</sup>

Our results are mixed: whether providing liquidity to our simulated FM-AMM generates higher returns than providing the same liquidity to Uniswap v3 depends on the token pair and the period we consider. However, these returns are similar: at the end of the 6-months period we consider, the differences in returns between an FM-AMM and Uniswap v3 across the three pools we study are -0.22% (for the ETH-USDT pool), 0.03% (for the BTC-USDT pool) and 0.11% (for the ETH-BTC pool).

---

<sup>1</sup> Note that Uniswap v3 is characterized by having *concentrated liquidity*: each LP provides liquidity over a price range and earns returns only if the price is within this range. In our comparison, we use the empirical distribution of liquidity and consider the return of an arbitrarily small non-concentrated liquidity position (i.e., a position over the entire price range  $[0, \infty]$ ). For the FM-AMM, we also assume a liquidity position that is non-concentrated. Whether or not the rest of the liquidity provided to the FM-AMM is concentrated (and how) is irrelevant to our results.

<sup>2</sup> Several authors studied whether providing liquidity on Uniswap is profitable, see Heimbach et al. (2021), Loesch et al. (2021), Heimbach et al. (2022). The main difference between these papers and ours is that we compare Uniswap LP returns to a different benchmark (here FM-AMM LP returns, in those papers, a holding strategy). In this respect, our strategy is similar to Milionis et al. (2022), which we discuss in more detail later.

Also, during the period we consider, the maximum difference in value between the two liquidity positions (relative to their initial values) is 0.30% (for the ETH-USDT pool), 0.14% (for the BTC-USDT pool), and 0.11% (for the ETH-BTC pool). We conclude that the lowest bound on the return to providing liquidity to an FM-AMM is similar to the empirical return to providing liquidity to Uniswap v3. Our result also shows that on Uniswap v3, fees from noise traders are approximately equal to arbitrageurs' profits.<sup>3</sup>

The remainder of the paper is organized as follows. We now discuss the relevant literature. In Section 2, we introduce the FM-AMM in its simplest form with a product function and zero fees. In Section 3, we discuss several extensions, including fees and the fact that an FM-AMM violates path dependence and hence requires batching. In Section 4 we consider the behavior of an FM-AMM in the equilibrium of a game with informed arbitrageurs and noise traders. Section 5 contains the empirical analysis. The last section concludes. All proofs and mathematical derivations missing from the text are in the appendix.

**Relevant literature.** Several authors argued that AMM's design allows informed arbitrageurs to profit at the expense of LPs. Aoyagi (2020), Capponi and Jia (2021), and Milionis et al. (2022) provide theoretical models that illustrate this possibility. In particular, Milionis et al. (2022) consider a continuous time model with zero fees and derive a closed-form formula to measure LPs returns and the cost they face when trading with informed arbitrageurs (which they call loss-vs-rebalancing or LVR). Milionis et al. (2023) extend this analysis to the case of discrete-time and strictly positive trading fees. They use the term *arbitrageur profits* to indicate LPs losses, a term we adopt because both our model and our empirical analysis are in discrete time and have fees. Aoyagi (2020) and Capponi and Jia (2021) draw the implication of this cost for liquidity provision.

A second important limitation of CFAMM is that they enable sandwich attacks (see Park, 2022). These attacks are quantitatively relevant. For example, Torres et al. (2021) collected on-chain data from the inception of Ethereum (July 30, 2015) until November 21, 2020 and estimated that sandwich attacks generated 13.9M USD in profits. Qin et al. (2022) consider a later period (from the 1st of December 2018 to the 5th of August 2021) and find that sandwich attacks generated 174.34M USD in profits. Our design eliminates these attacks. We are therefore related to the growing literature proposing mechanisms to prevent malicious re-ordering of

---

<sup>3</sup> Lehar and Parlour (2021) and Foley et al. (2022) argue that liquidity provision is strategic: the size of liquidity pools is smaller when arbitrageurs' profits are higher. The intuition is that when there is a rebalancing event, the loss to arbitrageurs *per unit of liquidity* is independent of the size of the liquidity pools. At the same time, the size of the liquidity pools determines the fraction of the revenues from noise traders earned by each unit of liquidity. Hence, the endogenous response of liquidity providers may explain why we find that fees from noise traders are approximately equal to arbitrageurs' profits.

transactions (of which sandwich attacks are an example), especially those that can be implemented at the smart-contract level (Breidenbach et al., 2018, Gans and Holden, 2022, Canidio and Danos, 2023, Ferreira and Parkes, 2023).<sup>4</sup>

Several initial discussions on designing “surplus maximizing” or “surplus capturing” AMMs occurred informally on blog and forum posts (see Leupold, 2022, Josojo, 2022, Della Penna, 2022). Goyal et al. (2022) provides an axiomatic derivation of the surplus-maximizing AMM. Relative to their work, our contribution is to place this new type of AMM in a context with arbitrageurs and other trading venues. Schlegel and Mamageishvili (2022) also study AMM from an axiomatic viewpoint. In particular, they discuss path independence, which FM-AMMs violate.

The intuition for our main result is closely related to Budish et al. (2015), who study the batching of trades in the context of traditional finance as a way to mitigate the high-frequency-trading (HFT) arms race and protect regular (or slow) traders. The main result is that batching trades force informed arbitrageurs to compete in price instead of speed, because the priority of execution within the batch is given based on price. The intuition in our model is similar, although competition between arbitrageurs on the batch is rather in quantity than in price: if the price on an FM-AMM differs from the equilibrium price, competing arbitrageurs will submit additional trades to exploit the available arbitrage opportunity, but by doing so, they push the price on the FM-AMM in line with the equilibrium.

We conclude by noting that an FM-AMM is also an oracle: it exploits competition between arbitrageurs to reveal on-chain the price at which these arbitrageurs can trade off-chain. It is, therefore, related to the problem of Oracle design (as discussed, for example, by Chainlink, 2020).

## 2 The function-maximizing AMM

In this section, we first introduce the main concepts of interest using a simple constant-product function (both for the CFAMM and the FM-AMM), no fees, and keeping formalities to the minimum. In the next section, we generalize our definitions and results and introduce additional elements.

As a preliminary step, we derive the trading function of a constant product AMM, the simplest and most common type of CFAMM. Suppose that there are only two tokens, ETH and DAI. A constant-product AMM (CPAMM) is willing to trade as long as the product of its liquidity pools remains constant (see Figure 1 for an illustration). Call  $Q^S$  and  $Q^E$  its initial liquidity pools in DAI and ETH, respectively, and  $p^{CPAMM}(x)$  the average price at which the CPAMM is willing to trade  $x$  ETH, where  $x > 0$  means that CPAMM is selling ETH while  $x < 0$

<sup>4</sup> Another strand of the literature studies how to prevent malicious re-ordering of transactions by modifying the infrastructure that underpins how transactions are sent. See, for example, Kelkar et al. (2020) and the literature review in Heimbach and Wattenhofer (2022).

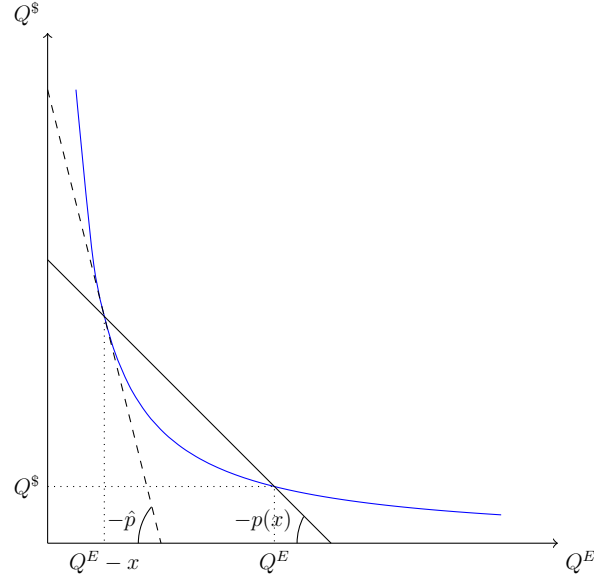


Fig. 1: Initially, the liquidity pools of the CPAMM are  $Q^S$  and  $Q^E$ . A trader then purchases  $x$  ETH at an average price  $p(x)$ . Note that, after the trade, the marginal price on the CPAMM (that is, the price for an arbitrarily small trade) is  $\hat{p} \neq p(x)$ .

means that the CPAMM is buying ETH. For the product of the liquidity pools to be constant, it must be that

$$Q^S \cdot Q^E = (Q^S + p^{CPAMM}(x)x)(Q^E - x)$$

or

$$p^{CPAMM}(x) = \frac{Q^S}{Q^E - x}.$$

Note that the marginal price of a CPAMM (i.e., the price to trade an arbitrarily small amount) is given by the ratio of the two liquidity pools. The key observation is that, in a CPAMM, a trader willing to trade  $x$  pays a price that is different from the marginal price after the trade. This is precisely the reason why arbitrageurs can exploit a CPAMM: an arbitrageur who trades with the CPAMM to bring its marginal price in line with some exogenously-determined equilibrium price does so at an advantageous price (and hence makes a profit at the expense of the CPAMM).

Instead, in the introduction, we defined an FM-AMM as an AMM in which, for every trade, the average price equals the marginal price after the trade (we may call this a *clearing-price-consistent AMM*). For ease of comparison with the CPAMM described earlier, suppose that the FM-AMM function is the product of the two liquidity pools, and hence, that its marginal price is the ratio of its liquidity pools.

The price function  $p(x)$  for buying  $x$  ETH on the FM-AMM is implicitly defined as

$$p(x) = \frac{Q^{\$} + x \cdot p(x)}{Q^E - x},$$

where the RHS of the above expression is the ratio of the two liquidity pools after the trade. Solving for  $p(x)$  yields:

$$p^{FM-AMM}(x) \equiv p(x) = \frac{Q^{\$}}{Q^E - 2x},$$

which implies that the FM-AMM marginal price is, indeed, the ratio of the liquidity pools. Hence, a given trade on the FM-AMM generates twice the price impact than the same trade on the traditional CPAMM (cf. the expression for  $p^{CPAMM}(x)$ ).

Interestingly, an FM-AMM can also be seen as a price-taking agent maximizing an objective function. If its objective function is the product of the two liquidity pools, then for a given price  $p$  the FM-AMM supplies  $x$  ETH by solving the following problem:

$$x^{FM-AMM}(p) = \operatorname{argmax}_x \{(Q^E - x)(Q^{\$} + p \cdot x)\}.$$

It is easy to check that the FM-AMM supply function is:

$$x^{FM-AMM}(p) = \frac{1}{2} \left( Q^E - \frac{Q^{\$}}{p} \right).$$

Hence, to purchase  $x$  ETH on the FM-AMM, the price needs to be, again:

$$p^{FM-AMM}(x) = \frac{Q^{\$}}{Q^E - 2x}.$$

It follows that, whereas a traditional CPAMM always trades along the same curve given by  $Q^{\$}Q^E$ , the FM-AMM trades as to be on the highest possible curve. With some approximation, we can therefore see an FM-AMM as a traditional CPAMM in which additional liquidity is added with each trade. See Figure 2 for an illustration.

A final observation is that the FM-AMM's trading function is equivalent to

$$p \cdot (Q^E - x^{FM-AMM}(p)) = Q^{\$} + p \cdot x^{FM-AMM}(p).$$

In other words, for a given  $p$ , the value of the two liquidity pools is equal after the trade. Therefore, the FM-AMM is trading to implement a passive investment strategy, in which the total value of the two pools is equally split between the two assets (that is, a passive investment strategy with weights  $1/2, 1/2$ ). It is easy to check that the FM-AMM can implement any passive investment strategy with fixed weights  $(\alpha, 1 - \alpha)$  by specifying the objective function as  $(Q^E)^{\alpha}(Q^{\$})^{1-\alpha}$  for an appropriate  $\alpha \in (0, 1)$ .

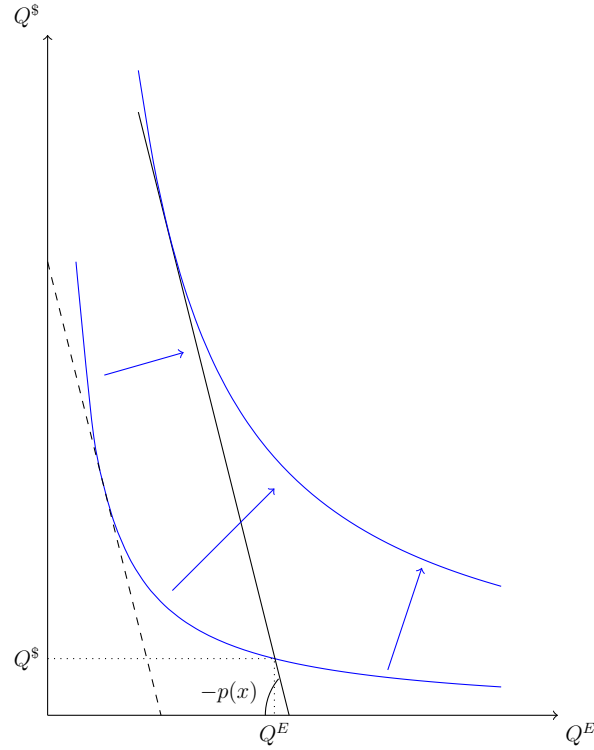


Fig. 2: On an FM-AMM, the price at which a given trade  $x$  is executed equals the marginal price after the trade is executed. This implies that an FM-AMM “moves up” the curve with each trade.

### 3 Additional considerations

#### 3.1 Generalization of definitions and results

We now generalize our results. First of all, an AMM is an entity that accepts or rejects trades based on a pre-set rule. Such rule can be derived from the AMMs liquidity pools  $(Q^S, Q^E) \in \mathbb{R}_+^2$  and the AMM function  $\Psi : \mathbb{R}_+^2 \rightarrow \mathbb{R}$ . We assume that the AMM function is continuous, it is such that  $\Psi(Q^S, 0) = \Psi(0, Q^E) = \Psi(0, 0)$  for all  $Q^S, Q^E$ , that it is strictly increasing in both its arguments whenever  $Q^S > 0$  and  $Q^E > 0$ , and that it is strictly quasiconcave. The difference between different types of AMMs is how the function  $\Psi(\cdot, \cdot)$  and the liquidity pools  $(Q^S, Q^E)$  determine what trades will be accepted and rejected by the AMM.

**Definition 1** (Constant Function Automated Market Maker). For given liquidity pools  $(Q^S, Q^E)$  and function  $\Psi : \mathbb{R}_+^2 \rightarrow \mathbb{R}$ , a constant function automated market maker (CFAMM) is willing to trade  $x$  for  $y = p(x)x$  if and only if

$$\Psi(Q^S + p(x)x, Q^E - x) = \Psi(Q^S, Q^E).$$



Our first goal is to define an AMM that is *clearing-price-consistent* in the sense that, for every trade, the average price of the trade equals the marginal price after the trade.

**Definition 2** (Clearing-Price Consistent AMM). For given liquidity pools  $(Q^S, Q^E)$  and function  $\Psi : \mathbb{R}_+^2 \rightarrow \mathbb{R}$ , let

$$p_\Psi^{\text{margin}}(Q^S, Q^E) = \frac{\frac{\partial \Psi(Q^S, Q^E)}{\partial Q^E}}{\frac{\partial \Psi(Q^S, Q^E)}{\partial Q^S}}$$

be the marginal price of the AMM for reserves  $Q^S, Q^E$ . A clearing-price consistent AMM is willing to trade  $x$  for  $y = p(x)x$  if and only if

$$p(x) = p_\Psi^{\text{margin}}(Q^S + p(x)x, Q^E - x). \quad (1)$$

Note that, given our assumptions on  $\Psi(.,.)$ , whenever  $Q^S > 0$  and  $Q^E > 0$ , the marginal price is strictly increasing in the first argument and strictly decreasing in the second argument, converges to zero as  $Q^E \rightarrow \infty$  or  $Q^S \rightarrow 0$ , and to infinity as  $Q^E \rightarrow 0$  or  $Q^S \rightarrow \infty$ .

Second, we define a *function-maximizing AMM (FM-AMM)* that maximizes the objective function instead of keeping it constant:

**Definition 3** (Function-Maximizing AMM). For given liquidity pools  $(Q^S, Q^E)$  and function  $\Psi : \mathbb{R}_+^2 \rightarrow \mathbb{R}$ , a function-maximizing AMM is willing to trade  $x$  for  $y = p(x) \cdot x$  if and only if  $p(x) = x^{-1}(p)$ , where

$$x(p) := \operatorname{argmax}_x \{ \Psi(Q^S + p \cdot x, Q^E - x) \}. \quad (2)$$

The next proposition establishes the equivalence between clearing-price-consistent and function-maximizing AMMs.

**Proposition 1.** *For given liquidity pools  $(Q^S, Q^E)$  and function  $\Psi : \mathbb{R}_+^2 \rightarrow \mathbb{R}$ , an AMM is function maximizing if and only if it is clearing-price consistent.*

*Proof.* Under our assumptions, solving (2) is equivalent to satisfying the first-order condition, which is equivalent to (1).  $\square$

### 3.2 Path-dependence (or why batching trades is necessary)

CFAMMs (without fees) are *path-independent*: splitting a trade into multiple parts and executing them sequentially does not change the average price of the trade. This property does not hold for an FM-AMM because traders can get better prices by splitting their trade. In fact, they can get approximately the same price as on the

corresponding CFAMM by splitting their trade into arbitrarily small parts. This is why an FM-AMM's trading function can be implemented only if trades are batched.

To see this, note that a trade on the FM-AMM with product function changes the reserves as follows:

$$(Q^{\$}, Q^E) \rightarrow \left( Q^{\$} \left( \frac{Q^E - x}{Q^E - 2x} \right), Q^E - x \right)$$

By instead splitting the trade into smaller parts  $\sum_{i=1}^n x_i = x$  and executing them sequentially, the reserves of the FM-AMM will change to

$$\left( Q^{\$} \prod_{i=1}^n \frac{(Q^E - \sum_{j=1}^{i-1} x_j) - x_i}{(Q^E - \sum_{j=1}^{i-1} x_j) - 2x_i}, Q^E - \sum_{i=1}^n x_i \right).$$

Setting  $x_i = \frac{1}{n}x$  and letting  $n \rightarrow \infty$  leads to the DAI reserves after the trade being

$$\lim_{n \rightarrow \infty} Q^{\$} \frac{Q^E - \frac{1}{n}x}{Q^E - \frac{n+1}{n}x} = Q^{\$} \frac{Q^E}{Q^E - x}$$

This term exactly equals the DAI reserve of a CPAMM after these trades. Hence, to have an FM-AMM, it is necessary to prevent splitting orders by imposing the batching of trades.

### 3.3 Fees

An important design choice is the fee structure. An FM-AMM can charge fees in at least two ways: a fee could be charged for including a trade on the batch, and an additional one could be charged on the trades not netted out on the batch and hence are settled on the FM-AMM. The difference between the two fees is that some of the trades may be netted already on the batch without ever reaching the FM-AMM. In what follows, we assume that the fee for inclusion in the batch is zero, while there could be a strictly positive fee on trades settled on the FM-AMM. Theoretically, this is the simplest case and the one we will consider in the empirical analysis. The reason is that fees earned from noise traders are zero, and we will not need to make any assumption concerning the frequency and distribution of these trades. But our results continue to hold when there are positive fees for inclusion in the batch.

The FM-AMM also needs to decide on which currency to charge the fee. For ease of comparison with Uniswap (the most important and liquid CFAMM), we assume that fees are specified in the sell tokens (i.e., the input token from the AMM perspective). Hence, if there is a fee  $\tau$  then an order for  $x$  ETH that is settled on the FM-AMM pays  $x \cdot p^{FM-AMM}(x) / (1 - \tau)$  DAI, while a sell order for  $x$  ETH that is settled on the FM-AMM receives  $x(1 - \tau) \cdot p^{FM-AMM}(x(1 - \tau))$  DAI. We can

therefore define the *effective price* as

$$\tilde{p}(x, \tau) \equiv \begin{cases} \frac{p^{FM-AMM}(x)}{1-\tau} = \frac{Q^s}{(1-\tau)(Q^E-2x)} & \text{if } x > 0 \\ (1-\tau) \cdot p^{FM-AMM}(x(1-\tau)) = \frac{Q^s}{\frac{Q^E}{(1-\tau)}-2x} & \text{if } x < 0 \\ \left[ \frac{Q^s(1-\tau)}{Q^E}, \frac{Q^s}{(1-\tau)Q^E} \right] & \text{if } x = 0 \end{cases} \quad (3)$$

We interpret the terms  $Q^E/(1-\tau)$  and  $Q^s/(1-\tau)$  as the FM-AMM's *effective reserves*. Hence, the fee causes the FM-AMM to behave as if it had more of the token that traders want to sell to the FM-AMM. Also, a positive-fee FM-AMM remains a function maximizing AMM, but the objective of the maximization depends on the sign of the trade. That is  $\tilde{p}(x, \tau) = x^{-1}(p, \tau)$  and

$$x(p, \tau) = \operatorname{argmax}_x \{U(x, p, \tau)\}$$

where

$$U(x, p, \tau) = \begin{cases} (Q^E - x) \cdot \left( \frac{Q^s}{1-\tau} + p \cdot x \right) & \text{if } x > 0 \\ \left( \frac{Q^E}{1-\tau} - x \right) \cdot (Q^s + p \cdot x) & \text{if } x < 0 \\ Q^E \cdot Q^s & \text{if } x = 0 \end{cases} \quad (4)$$

See Figure 3.

There is a range of effective prices at which the FM-AMM will not want to trade, and the size of this range is increasing in  $\tau$ . This is important whenever the trades on the batch are fully netted out within the batch. In this case, we assume that the FM-AMM price is such that the traders' net demand is zero.

A final observation is that the fee  $\tau$  also affects the elasticity of the effective price to the size of the trade  $|x|$ . The reason is that only the fraction of the trade not paid as a fee generates a price impact. Hence, a higher fee implies a smaller price impact.

### 3.4 Other design choices: enforcing batching and frequency of rebalancing

Implementing an FM-AMM requires making several additional design choices. Here we briefly discuss two: how to enforce the batching of trades and the frequency of rebalancing of the FM-AMM.

In what follows, we will assume that the FM-AMM enforces batching by collecting intentions to trade off-chain and settling them on-chain at regular intervals, with all trades settled simultaneously facing the same prices.<sup>5</sup> However, there could

<sup>5</sup> This process is modeled around CoW Protocol ([www.cow.fi](http://www.cow.fi)). CoW Protocol collects intentions to trade off-chain, which are then executed as a batch. CoW Protocol enforces uniform clearing prices so that all traders in the same batch face the same prices.

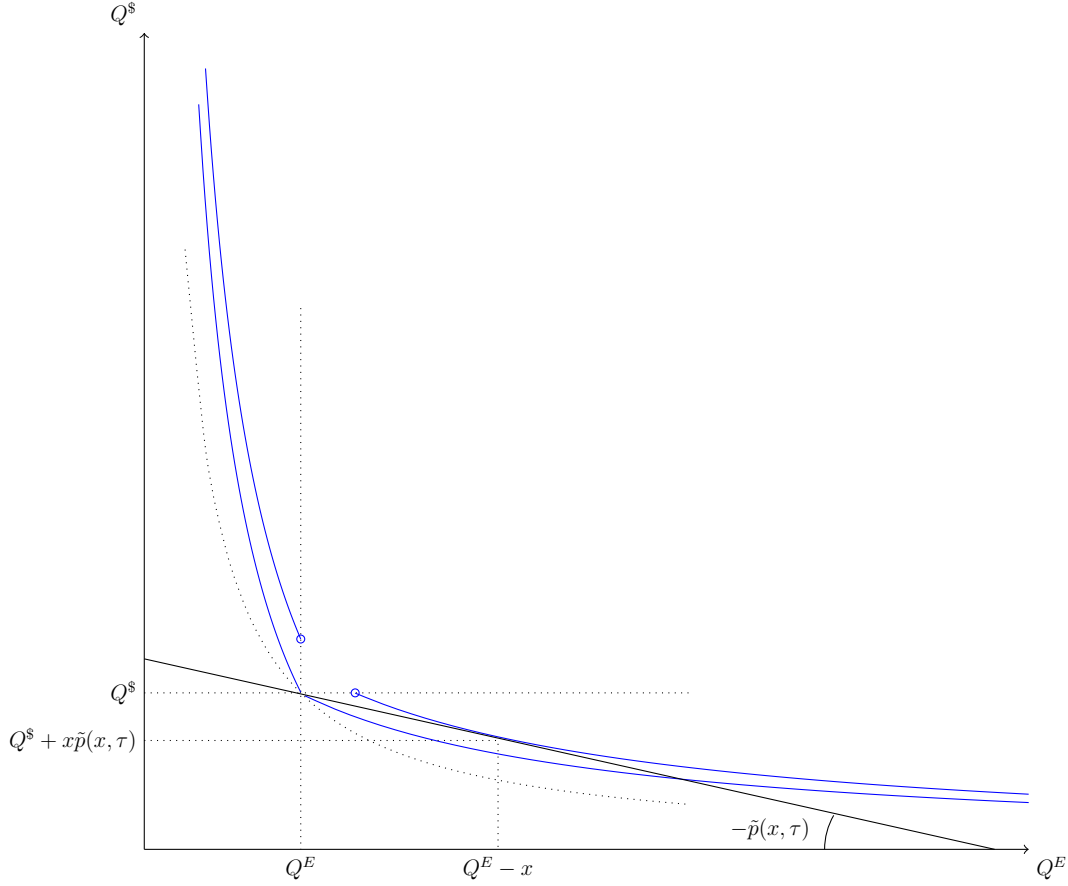


Fig. 3: A positive-fee FM-AMM moves up the curve: effective price for given trade  $x < 0$  (in blue, the FM-AMM level curves for given  $Q^S$  and  $Q^E$ ).

be other ways to enforce batching, for example, by leveraging proposer-builder separation (or PBS). In PBS, block builders (entities that assemble transactions in a block that are then forwarded to a proposer for inclusion in the blockchain) could compute the net trades that will reach the FM-AMM during that block. Builders will then include a message announcing this value at the beginning of the block, which the FM-AMM uses to compute the price at which all trades will be executed. If the proposer's announcement turns out to be correct at the end of the block, the FM-AMM will reward the builder (punishments can also be introduced if the block builder report is incorrect, see Leupold, 2022).

The frequency of rebalancing is a design choice because of path dependence. For example, an FM-AMM earns more when it settles one large batch instead of two smaller batches trading in the same direction. In this case, therefore, less frequent batches may be beneficial. However, settling a single large batch, in which opposite trade demands net out, may generate little or no trade (and hence little or no benefit

to the FM-AMM), while settling two smaller batches trading in opposite directions moves the FM-AMM “up the curve” each time. In this case, more frequent batches are more beneficial. In the theoretical analysis, to easily compare an FM-AMM with a traditional CPAMMs, we will assume that the FM-AMM rebalances each block. However, in the empirical analysis, we will compare the performance of an FM-AMM at different rebalancing intervals.

## 4 The model

Equipped with the full description of an FM-AMM, we can now study its behavior in an environment with traders and arbitrageurs. We limit our analysis to the product function.

The game comprises  $n$  noise traders, each wanting to trade  $a_i$  units of ETH. We adopt the convention that if  $a_i > 0$  trader  $i$  wants to buy ETH, while if  $a_i < 0$  trader  $i$  wants to sell ETH. Call  $A = \sum_i a_i$  the aggregate demand for ETH from noise traders, assumed small relative to the FM-AMM liquidity pools  $Q^E$  and  $Q^S$ .<sup>6</sup> Next to traders, a large number of cash-abundant, competing arbitrageurs, who can trade as part of the batch and on some external trading venue, assumed much larger and more liquid than the combination of our  $n$  traders and the FM-AMM. The equilibrium price for ETH on this external trading venue is  $p^*$  and is unaffected by trades on the FM-AMM. Arbitrageurs aim to profit from price differences between the FM-AMM and the external trading venues. Arbitrage opportunities will be intertemporal (over short intervals). Hence, for ease of derivations, we assume that arbitrageurs do not discount the future.

The timing of the game is discrete. Even periods are when on-chain transactions occur. Even periods are, therefore, better interpreted as different blocks. Odd periods are when off-chain events occur. In these periods, first, the equilibrium price  $p^*$  may change, and then traders/arbitrageurs can submit trades for inclusion in the batch.

We are now ready to derive our main proposition.

**Proposition 2.** *Suppose that, at the end of an even period, the pools of the FM-AMM are  $Q^E$  and  $Q^S$ . In the equilibrium of the subsequent odd period, after  $p^*$  is realized, noise traders will collectively submit trade  $A$  to the batch, and arbitrageurs will collectively submit trade  $y(p^*)$  such that  $\tilde{p}(A + y(p^*), \tau) = p^*$ .*

The proof of the proposition distinguishes between two cases. The first is  $p^* > \frac{Q^S}{(1-\tau)Q^E}$  or  $p^* < \frac{(1-\tau)Q^S}{Q^E}$ , so that  $A + y(p^*) \neq 0$ . There is positive trade on the FM-AMM in equilibrium, and the FM-AMM unique effective price is exactly the

---

<sup>6</sup> In practice, we assume that trading  $A$  on the FM-AMM has a negligible price impact. Else, we should treat orders from noise traders as limit orders. In this case, all our results continue to hold at the cost of additional notation.

equilibrium price  $p^*$ . In this case, we say that there was a rebalancing event. The second case is  $p^* \in [\frac{Q^S}{(1-\tau)Q^E}, \frac{(1-\tau)Q^S}{Q^E}]$ , in which case there is no trade settled on the FM-AMM, and  $p^*$  is one of the possible effective prices. Note, however, that  $p^*$  is the only price at which arbitrageurs are indifferent and  $y(p^*) = -A$  (i.e., at any other price  $[\frac{Q^S}{(1-\tau)Q^E}, \frac{(1-\tau)Q^S}{Q^E}]$  there is an unmet demand or supply for ETH).

Hence, if the equilibrium price is sufficiently far from the FM-AMM marginal price  $\frac{Q^S}{Q^E}$ , the FM-AMM will be rebalanced so that its effective price equals the new equilibrium price. Otherwise, no trade is settled on the FM-AMM (that is, all trades are netted out already on the batch). In either case, the effective price on the FM-AMM is  $p^*$  and the amount settled on the FM-AMM is independent of the trades from noise traders. The key intuition is that all arbitrageurs can submit trades on the batch. Hence, there is no equilibrium in which there is an exploitable arbitrage opportunity; otherwise, some arbitrageurs will want to submit additional trades on the batch. Arbitrage opportunities are absent whenever  $\tilde{p}(A + y(p^*), \tau) = p^*$ , which is the unique equilibrium.

The revenues earned in fees are contributed to the FM-AMM liquidity pools. It follows that the FM-AMM earns the effective price on every trade. Knowing this, we can easily derive the evolution of the liquidity pools:

**Corollary 1.** *If  $A + y(p^*) \neq 0$ , then the liquidity pools after the rebalancing are  $Q^E - (A + y(p^*))$  and  $Q^S + p^* \cdot (A + y(p^*))$ . Otherwise, the liquidity pools are again  $Q^E$  and  $Q^S$ .*

The key observation is that the FM-AMM always trades at the equilibrium price, even though its trading function does not depend on such price. Again, this is a consequence of the competition between arbitrageurs, who will add trades to the batch until the FM-AMM effective price equals the equilibrium price. Note also that, even if the price at which the FM-AMM trades is always  $p^*$  and is independent of the fee, the probability of trading and the trade size depends on the fee. More precisely, higher fees decrease the probability of a rebalancing event but increase the trade needed to rebalance the FM-AMM (i.e., it increases the equilibrium  $A + y(p^*)$ ). This is because higher fees imply that the effective price is less elastic to the trade size, and hence larger trades are required to move the effective price to the new equilibrium.

To conclude, we discuss how the FM-AMM performs in the presence of risk. Consider the end of an odd period. At that point in time, the future equilibrium price  $p^*$  is a random variable with  $E[p^*] = p_0^*$ . In a traditional CFAMM, we know from the literature that arbitrage profits increase in the volatility of the price (see Milionis et al., 2022, and Milionis et al., 2023), which implies that the expected value of future LP holdings is lower when future prices are more volatile. The previous corollary shows that CF-AMM trades at the fair equilibrium price at every realization of  $p^*$ , and the expected value of its liquidity pools is  $p_0 Q^S + Q^E$ . Hence,

with respect to the value of the pools, CFAMMs are risk averse while FM-AMMs are risk neutral. At the same time, we discussed earlier how a CFAMM always trades to stay on the same function, while an FM-AMM trades to increase the value of its function. The next proposition shows that this increase is larger the more risk there is. Hence, with respect to the value of the function, a CFAMM is risk neutral (i.e. it always stays on the same function), while an FM-AMM is risk-loving.

**Proposition 3** (FM-AMM is risk loving). *Consider two probability distributions of the equilibrium price,  $F(p) : R^+ \rightarrow [0, 1]$  and  $G(p) : R^+ \rightarrow [0, 1]$  having equal mean  $p_0^*$ . Assume that  $F()$  is a mean-preserving spread of  $G()$ , that is, it is possible to write*

$$p_f^* = p_g^* + \epsilon$$

*where  $p_f^* \sim F()$ ,  $p_g^* \sim G()$  and  $\epsilon$  is a shock with  $E[\epsilon|p_g^*] = 0$ . Then, in expectation, the FM-AMM reaches a higher function under distribution  $F()$  than under distribution  $G()$ , that is*

$$E_F[U(A + y(p^*), p^*, \tau)] \geq E_G[U(A + y(p^*), p^*, \tau)]$$

*The inequality is strict if the probability of a rebalancing under distribution  $F()$  is strictly positive.*

The proposition compares the expected value of the function under two distributions of the future price, where one distribution is a mean-preserving spread of the other. This ranking of distributions captures an intuitive notion of risk because one distribution can be derived from the other by adding some noise. If one distribution is a mean-preserving spread more than the other, the first distribution has a higher variance. Note, however, that not all distributions can be ranked using mean-preserving spreads. It is, however, usually the case that if both distributions belong to the same family (i.e., both normal), then ranking based on mean-preserving spreads coincides with the ranking based on variance.

## 5 Empirical analysis

We complement our theoretical analysis by estimating the returns of providing liquidity to an FM-AMM. We do so by considering a counterfactual in which an FM-AMM existed during a specific period. We use Binance price data (together with our theoretical results) to simulate how arbitrageurs would have rebalanced our simulated FM-AMM. Importantly, because we consider an FM-AMM with a zero fee for inclusion in a batch, our FM-AMM generates no fees from noise traders. (Equivalently, we could also assume that the FM-AMM does not receive any noise trading volume and is only rebalanced by arbitrageurs.) Hence, the estimated LP returns should be considered a lower bound to the possible returns generated by an FM-AMM that also earns revenues from noise traders.

We then compare the return of providing liquidity to our simulated FM-AMM to the empirical returns of providing liquidity to the corresponding Uniswap v3 pool. If the Uniswap v3 pool and the FM-AMM rebalance at the same frequency and has the same fee, then the comparison between these returns and the simulated FM-AMM returns establishes whether, on the Uniswap v3 pool we consider, arbitrageurs' profits exceed or fall short of the revenues generated by noise traders.<sup>7</sup> We then consider how the return of FM-AMM LP changes with its rebalancing interval and fee.

## 5.1 Details of the empirical analysis

We retrieve price data from Binance from October 2022 to March 2023 for several trading pairs. We then use the result of Proposition 2 to simulate an FM-AMM pool rebalanced to the Binance price in regular intervals of different frequencies (namely once every  $12s = 1$  block, 1 min, 5 min, 1h, and 1 day). These rebalancing trades determine the evolution of the FM-AMM pools and the return of its liquidity providers. We repeat the same exercise for different fees charged by the FM-AMM, namely 0.0%, 0.05%, 0.3%, and 1.0%.

To calculate the return on a liquidity position in a Uniswap v3 pool, we consider three pools for which we also have Binance price data: WETH-USDT (with fee 0.05%), WBTC-USDT (with fee 0.3%), and WBTC-WETH (with fee 0.05%).<sup>8</sup> In each case, we simulate the return of a small full-range position. We then query the amount of fees the pool earned in a given block and the amount of liquidity that is “in range” at the end of the same block.<sup>9</sup> We then use the size of the simulated liquidity position in range to calculate the fees it earns.

Our method is based on two assumptions. First, we assume that the simulated liquidity position is too small to affect price slippage, the volume of trades, and the incentive to provide liquidity by other LPs. We also implicitly assume that the liquidity in the range is constant during a block. This last assumption introduces some non-systematic inaccuracies in our estimation. For example, if within a block,

---

<sup>7</sup> Milionis et al. (2022) perform a similar analysis: they consider a continuous-time model in which arbitrageurs pay no fee and derive a formula for the return of providing liquidity to Uniswap. They then use their formula to study empirically whether fees from noise traders exceed or fall short of arbitrageurs' profits on the ETH-USDC Uniswap v2 pool. The main difference with our analysis is that the theoretical model we use for our empirical decomposition is already in discrete time and has fees (in this sense, it is related to Milionis et al. (2023)). In any case, Milionis et al. (2022) find that the losses to arbitrageurs are smaller than the revenues earned from noise traders, which is consistent with our results.

<sup>8</sup> Note that, whereas most Binance prices are expressed in *USDT*, this stablecoin is not widely used in Uniswap v3: at the time of writing, if we exclude stablecoin-to-stablecoin pairs, the two pools we consider are the only pools with USDT in the top 30 Uniswap v3 pools.

<sup>9</sup> We use the Uniswap v3 subgraph to query the data. <https://thegraph.com/hosted-service/subgraph/uniswap/uniswap-v3>



first some fees are collected and then some additional liquidity is introduced, our method attributes a fraction of these fees to the new liquidity even if, in reality, it did not earn any. If, instead, first some fees are collected and then some liquidity is withdrawn, our method does not attribute any of the fees to the liquidity that was withdrawn, while in reality it did earn some fees. Similarly, if a price changes tick, our method shares all fees collected in a block among the liquidity available in the last tick, whereas, in reality, some of the fees are shared among the liquidity available at the initial tick.<sup>10</sup>

Finally, our results do not depend on the size of the initial liquidity position. On Uniswap v3, a larger initial position earns proportionally more fees, but its ROI is the same. Similarly, on an FM-AMM, the size of the rebalancing trade scales proportionally with the available liquidity so that, again, its ROI is independent of its initial size. Also, for both Uniswap v3 and the FM-AMM, we consider a liquidity position that is non-concentrated (i.e., a position over the entire price range  $[0, \infty]$ ). If both positions are concentrated in the same (symmetrical) way, both Uniswap v3 fees and FM-AMM returns increase by the same factor as long as the price does not go out of range. So the comparison does not change, and the full-range comparison already constitutes a general comparison.

## 5.2 Results

**Arbitrageurs' profits vs. Uniswap fees** Figure 4 shows the evolution of the simulated liquidity position on three different Uniswap v3 pools over 6 months (October 2022 - March 2023)<sup>11</sup>, together with the hypothetical return of providing the same liquidity to an FM-AMM with fee equal to the fee of the Uniswap v3 pool we are comparing to, and rebalancing every block. Note that for ETH-USDT and BTC-USDT, the numeraire is USDT, while for the ETH-BTC, the numeraire is BTC. Moreover, note that the returns of both the FM-AMM and Uniswap v3 are plotted relative to the value of the liquidity position (i.e. a zero-fee Uniswap v3 liquidity position).

The results are mixed: for ETH-BTC, arbitrage profits are larger than Uniswap v3 fees over the whole period; hence contributing liquidity to our simulated FM-AMM would have generated larger returns. For ETH-USDT the result is reversed: fees on Uniswap v3 compensate for the loss to arbitrageurs, and contributing liquidity to our simulated FM-AMM would have generated lower returns. For BTC-USDT, the two are about the same.

A comparison of monthly returns can also be found in Table 1. Note that the

<sup>10</sup> Besides being non-systematic, the inaccuracies introduced are likely to be extremely small. For the ETH-USDT pool, we calculate that the difference between assuming liquidity to be constant over *two* blocks instead of over one block is 0.0002% over 6 months. We expect the inaccuracies from assuming the liquidity to be constant over one block to be of the same magnitude.

<sup>11</sup> More precisely, between blocks 15,648,998 and 16,950,010.

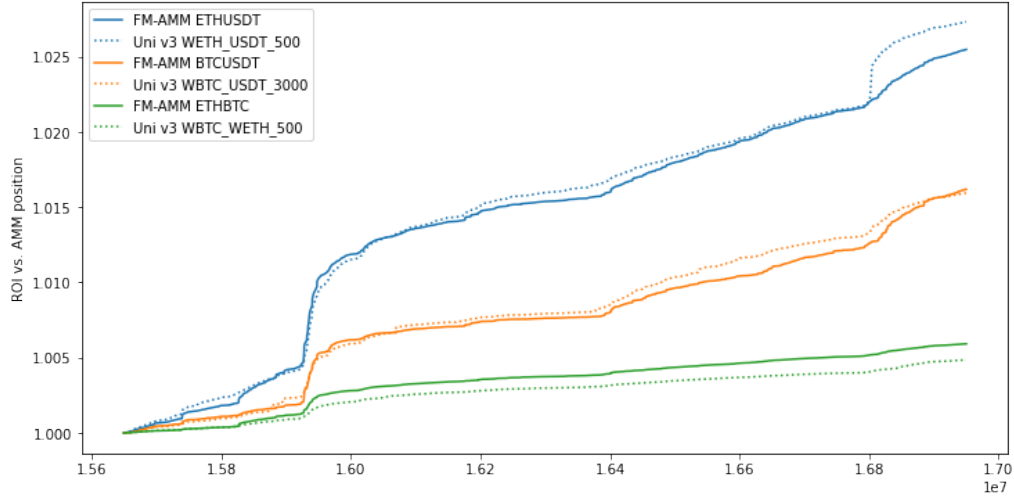


Fig. 4: Comparison over 6 months (October 2022 - March 2023): simulated returns to providing liquidity to an FM-AMM vs. historical trading fees on Uniswap v3, both relative to the value of the liquidity position.

table shows relative returns, i.e., the changes in the value of the liquidity position relative to holding the starting value of the position fully in the numeraire outside an AMM. Again, which AMM provides a higher ROI depends on the pair and the period.

	Oct 22	Nov 22	Dec 22	Jan 23	Feb 23	Mar 23
ETH-USDT FM-AMM	9.13%	-7.99%	-3.84%	<b>15.66%</b>	<b>0.96%</b>	6.90%
ETH-USDT Uni v3 Fees	<b>9.23%</b>	<b>-7.83%</b>	<b>-3.81%</b>	<b>15.66%</b>	0.92%	<b>7.17%</b>
BTC-USDT FM-AMM	<b>3.04%</b>	-8.00%	<b>-1.79%</b>	18.73%	0.15%	11.39%
BTC-USDT Uni v3 Fees	2.77%	<b>-7.61%</b>	-2.02%	<b>18.76%</b>	<b>0.16%</b>	<b>11.43%</b>
ETH-BTC FM-AMM	5.81%	<b>-0.25%</b>	-2.15%	<b>-2.59%</b>	<b>0.80%</b>	<b>-3.94%</b>
ETH-BTC Uni v3 Fees	<b>5.83%</b>	-0.30%	<b>-2.09%</b>	-2.62%	0.68%	-4.00%

Tab. 1: Comparison of relative monthly returns on an FM-AMM vs. on a regular AMM (using historical trading fees on Uniswap v3). The bold numbers indicate the higher return each month.

We conclude by arguing that the difference in returns between the two AMMs is small. The difference in the total return at the end of the 6 months we consider is: -0.22% (for the ETH-USDT pair), 0.03% (for the BTC-USDT pair) and 0.11% (for the ETH-BTC pair). Furthermore, by looking at the evolution of the two liquidity positions (as in Figure 4), we calculate the maximum difference in value between the two liquidity positions (expressed in percentage of the initial liquidity

position). This measure can be interpreted as a “relative maximum drawdown” and is 0.30% (for the ETH-USDT pair), 0.14% (for the BTC-USDT pair) and 0.12% (for the ETH-BTC pair). We interpret these results as showing that the simulated FM-AMM and Uniswap v3 generate similar returns.

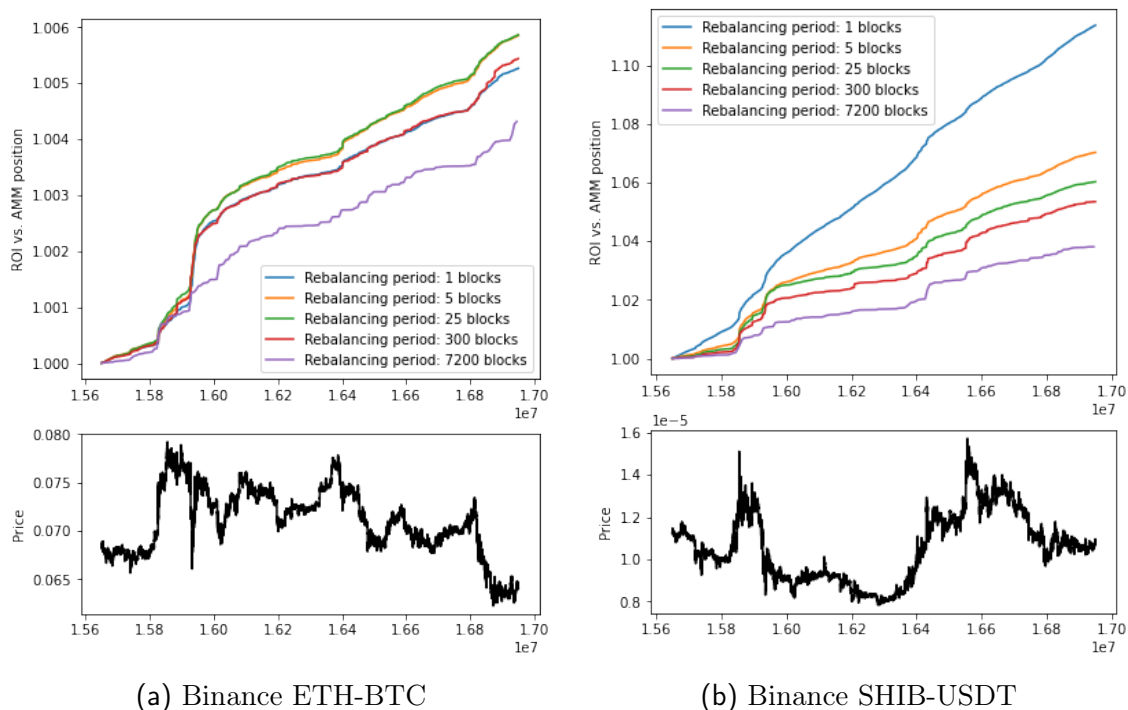


Fig. 5: Return on providing liquidity to an FM-AMM, for different rebalancing periods: 1 block (12s), 5 blocks (1 min), 25 blocks (5 mins), 300 blocks (1h), 7200 blocks (1 day)

**FM-AMM rebalancing frequency and fees** The return on the simulated FM-AMM is the lower bound to the possible return of an FM-AMM for several reasons. As already mentioned, the simulated FM-AMM does not earn revenues from noise traders by design. In addition, the simulated FM-AMM has the same fee and rebalancing interval as the corresponding Uniswap pool. Here we explore whether choosing a different fee or rebalancing interval would have generated higher returns for FM-AMM LPs.

We start with the rebalancing frequency. In Figure 5a, we report two examples, one in which the fastest rebalancing interval (1 block) generates the highest return and one in which this is not the case. In Appendix B we repeat the exercise for other token pairs. In most cases, the shortest rebalancing interval generates the largest returns, although for some pairs this is not the case. For example, for the

pair ETH-BTC, a rebalancing period of 25 blocks (5 mins) would have generated the highest returns.

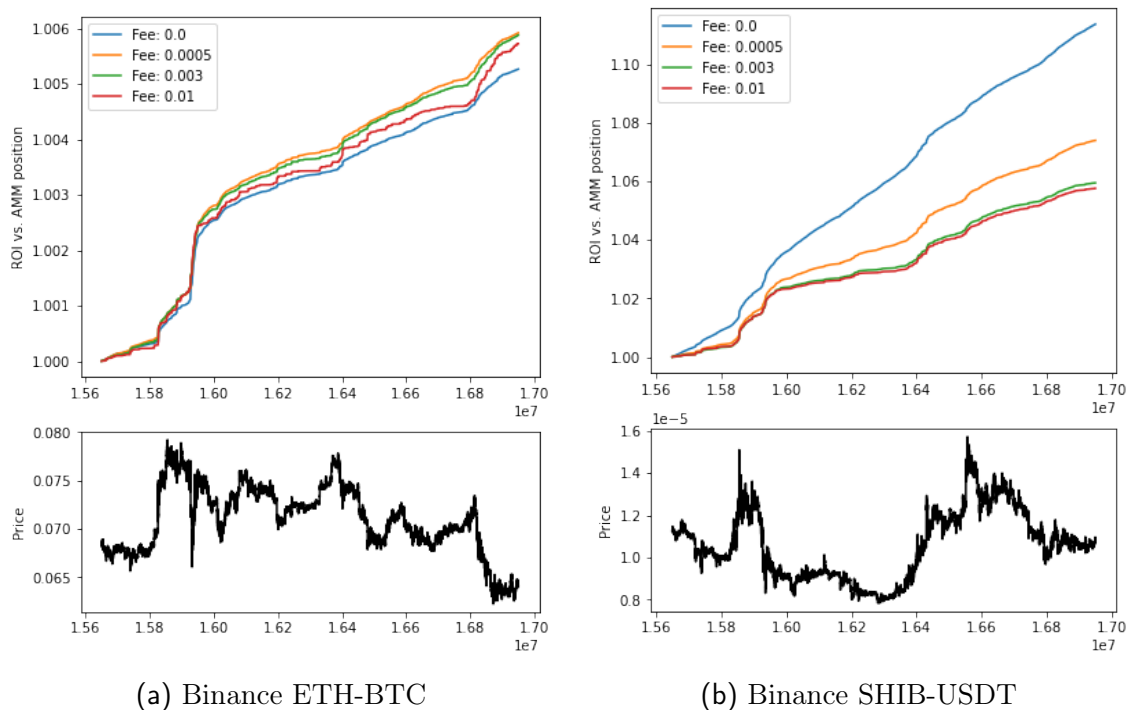


Fig. 6: Return on providing liquidity to an FM-AMM, for different fees: 0.0%, 0.05%, 0.3%, 1.0%

Concerning the fee, remember that its value affects whether arbitrageurs rebalance the pool, with higher fees implying a lower probability that the pools will be rebalanced. Furthermore, the fee also affects the size of the rebalancing trade, with higher fees implying larger rebalancing trades (which always occur at the new equilibrium price). Figure 6 shows two examples, one in which a fee of zero is optimal and another in which a strictly positive fee is optimal (see Appendix B for additional token pairs). In line with the previous result, we find that, in most cases, the optimal choice is a zero fee, which implies more frequent rebalancing. Again, there are exceptions, though, where LP returns on an FM-AMM would have been highest for a larger-than-zero fee.

## 6 Conclusion

In this paper, we study the design of AMM when trades are batched. Such an AMM does not need to satisfy path independence, which implies that the design space is larger than without batching. In particular, it is possible to design a function maximizing AMM (FM-AMM) which, for given prices, always trades to be on the highest

possible value of a given function. At the same time, batching creates competition between informed arbitrageurs. As a result of this competition, the price at which the FM-AMM trades is always equal to the equilibrium price (assumed determined on some very liquid location and exogenous to the FM-AMM). Hence, whereas in a traditional CFAMM, arbitrageurs earn profits at the expense of liquidity providers, in an FM-AMM these profits remain with the LPs. At the same time, sandwich attacks are eliminated because all trades within the same batch occur at the same price, equal to the exogenously-determined equilibrium price. We empirically estimate a lower bound to the return of providing liquidity to an FM-AMM and show that, at least for the token pairs and the period we consider, such a lower bound is very close to the empirical returns of providing liquidity on Uniswap v3.

A final observation is that an FM-AMM eliminates adverse selection by creating competition among multiple informed arbitrageurs. However, if there is a single, informed trader, then this trader can still enjoy information rents and trade at an advantage against FM-AMM LPs. A partial remedy is to set appropriate trading fees. Studying this problem is left for future work.

## A Mathematical derivations

*Proof of Proposition 2.* To start, note that if either  $p^* > \frac{Q^S}{(1-\tau)Q^E}$  or  $p^* < \frac{(1-\tau)Q^S}{Q^E}$ , then for  $y(p^*)$  such that  $\tilde{p}(A + y(p^*), \tau) = p^*$  we have  $A + y(p^*) \neq 0$ . Therefore, there is trade settled on the FM-AMM, and the price at which all traders trade is uniquely determined. If instead  $p^* \in [\frac{Q^S}{(1-\tau)Q^E}, \frac{(1-\tau)Q^S}{Q^E}]$ , then  $p^*$  can be the equilibrium price on the FM-AMM only if  $A + y(p^*) = 0$ , that is, no trade reaches the FM-AMM. In this case,  $\tilde{p}(0, \tau) = p^*$  is one of the possible equilibrium prices from the FM-AMM's viewpoint.

First, suppose that  $p^* > \frac{Q^S}{(1-\tau)Q^E}$  or  $p^* < \frac{(1-\tau)Q^S}{Q^E}$ , so that for  $y(p^*)$  such that  $\tilde{p}(A + y(p^*), \tau) = p^*$  we have  $A + y(p^*) \neq 0$ . The fact that  $y(p^*)$  is the unique equilibrium is easily established by contradiction: suppose the equilibrium is  $y'$  with  $\tilde{p}(A + y', \tau) \neq p^*$ , and that  $x \neq A + y'$ . Then by the fact that  $\tilde{p}(A + y', \tau)$  is locally continuous, an arbitrageur could submit an additional trade  $z$  such that  $\tilde{p}(A + y' + z, \tau) \neq p^*$  and earn strictly positive profits, which implies that  $y'$  is not an equilibrium. It is also easy to establish that  $y$  such that  $\tilde{p}(A + y(p^*), \tau) = p^*$  is an equilibrium, as no arbitrageur has any incentive to deviate.

Suppose now that  $p^* \in [\frac{Q^S}{(1-\tau)Q^E}, \frac{(1-\tau)Q^S}{Q^E}]$ . Also, here, it is easy to see that the only equilibrium is  $y = -A$  and  $\tilde{p}(0, \tau) = p^*$ , because this is the only case in which there are no arbitrage opportunities to exploit, and hence there is no excess demand or supply from arbitrageurs.  $\square$

*Proof of Proposition 3.* Remember that, for given prices, a positive-fee FM-AMM trades to maximize the objective function  $U(x, p, \tau)$ , defined in (4). The first obser-

vation is that the value function  $V(p, \tau) = \max_x U(x, p, \tau)$  is convex in  $p$ , strictly so if there is strictly positive trade (i.e., if  $x(p, \tau) \equiv \operatorname{argmax}_x U(x, p, \tau) \neq 0$ ). To see this, use the envelope theorem to write:

$$\frac{\partial V(p, \tau)}{\partial p} = \begin{cases} (Q^E - x(p, \tau)) x(p, \tau) & \text{if } x(p, \tau) > 0 \\ \left(\frac{Q^E}{1-\tau} - x(p, \tau)\right) x(p, \tau) & \text{if } x(p, \tau) < 0 \\ 0 & \text{if } x(p, \tau) = 0 \end{cases}$$

so that

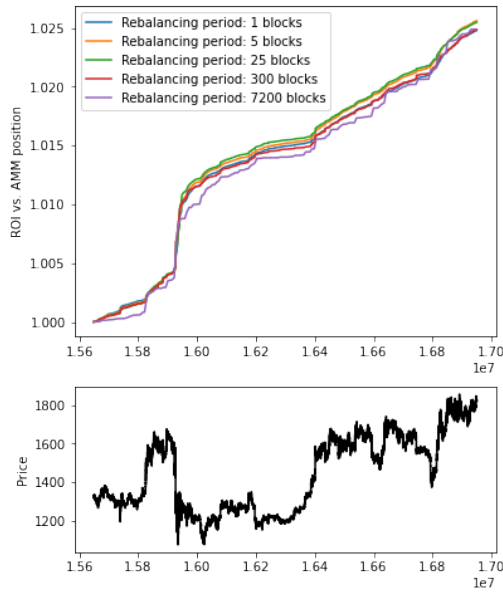
$$\frac{\partial^2 V(p, \tau)}{\partial p^2} = \begin{cases} \frac{\partial x(p, \tau)}{\partial p} (Q^E - 2x(p, \tau)) & \text{if } x(p, \tau) > 0 \\ \frac{\partial x(p, \tau)}{\partial p} \left(\frac{Q^E}{1-\tau} - 2x(p, \tau)\right) & \text{if } x(p, \tau) < 0 \\ 0 & \text{if } x(p, \tau) = 0 \end{cases}$$

Because  $p$  and  $x$  are strict complements in the objective function, by Topkis's theorem,  $\frac{\partial x(p, \tau)}{\partial p} > 0$  whenever  $x(p, \tau) \neq 0$ . Finally, the FM-AMM always trades so that  $(Q^E - 2x(p, \tau)) > 0$  and  $\left(\frac{Q^E}{1-\tau} - 2x(p, \tau)\right) > 0$ . It follows that  $V(p, \tau)$  is strictly convex in  $p$  whenever  $x(p, \tau) \neq 0$ . Because  $F()$  is a mean-preserving spread of  $G()$ , then

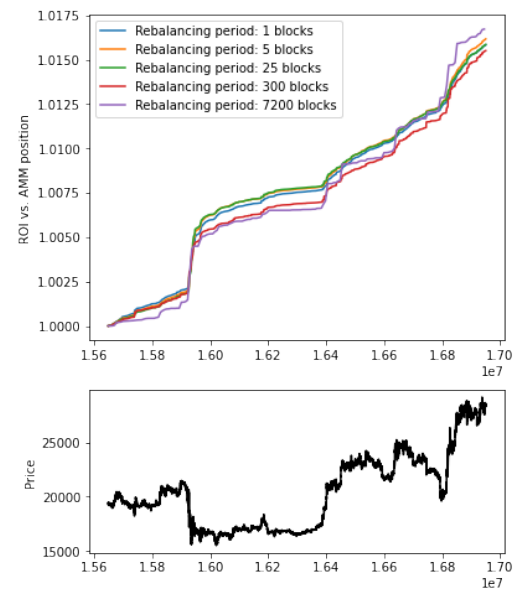
$$E_F[V(p, \tau)] \geq E_G[V(p, \tau)]$$

with strict inequality as long as  $x(p, \tau) > 0$  for some realization of  $p$ .  $\square$

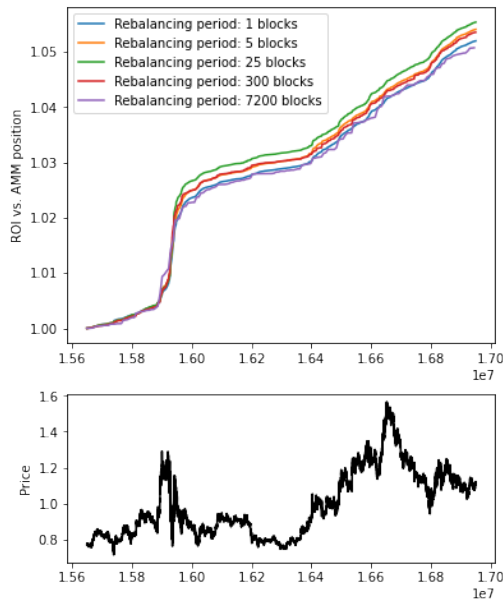
## B Extra figures



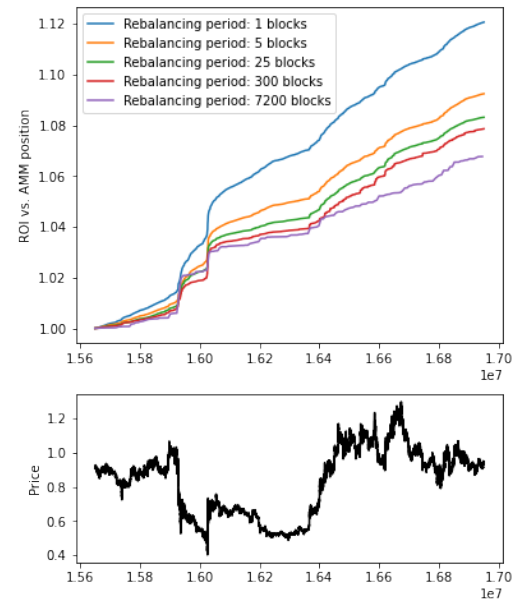
(a) Binance ETH-USDT



(b) Binance BTC-USDT

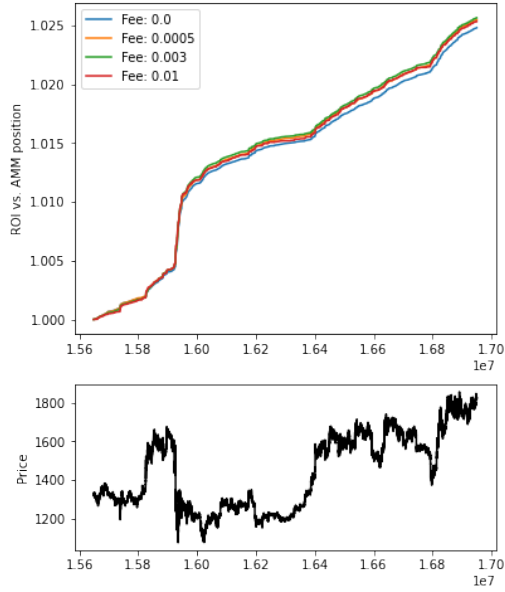


(c) Binance MATIC-USDT

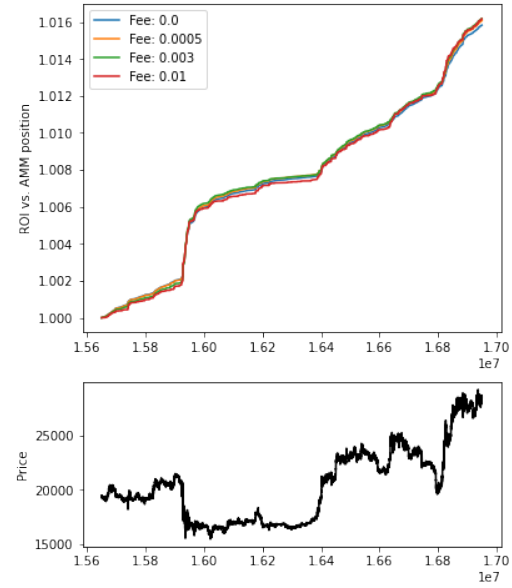


(d) Binance CRV-USDT

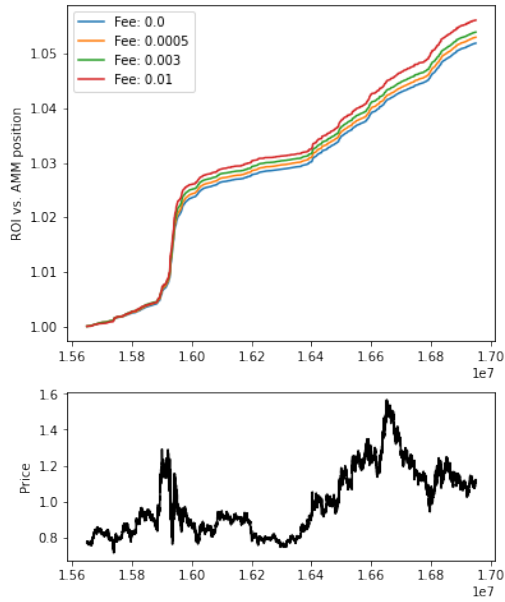
Fig. 7: Return on providing liquidity to an FM-AMM, for different rebalancing periods: 1 block (12s), 5 blocks (1 min), 25 blocks (5 mins), 300 blocks (1h), 7200 blocks (1 day)



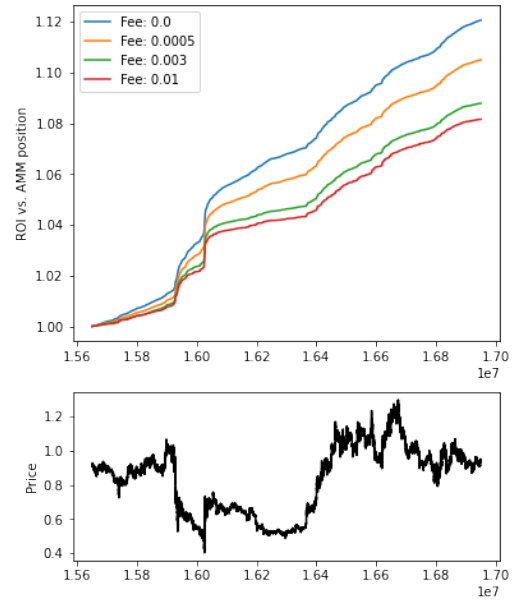
(a) Binance ETH-USDT



(b) Binance BTC-USDT



(c) Binance MATIC-USDT



(d) Binance CRV-USDT

Fig. 8: Return on providing liquidity to an FM-AMM, for different fees: 0.0%, 0.05%, 0.3%, 1.0%



## References

- Aoyagi, J. (2020). Liquidity provision by automated market makers. *working paper*.
- Breidenbach, L., P. Daian, F. Tramèr, and A. Juels (2018). Enter the hydra: Towards principled bug bounties and {Exploit-Resistant} smart contracts. In *27th USENIX Security Symposium (USENIX Security 18)*, pp. 1335–1352.
- Budish, E., P. Cramton, and J. Shim (2015). The high-frequency trading arms race: Frequent batch auctions as a market design response. *The Quarterly Journal of Economics* 130(4), 1547–1621.
- Canidio, A. and V. Danos (2023). Commitment against front running attacks. *arXiv preprint arXiv:2301.13785*.
- Capponi, A. and R. Jia (2021). The adoption of blockchain-based decentralized exchanges. *arXiv preprint arXiv:2103.08842*.
- Chainlink (2020). What is the blockchain oracle problem? Retrieved from <https://chain.link/education-hub/oracle-problem> on May 24, 2023. Online forum post.
- Della Penna, N. (2022, September 1). Mev minimizing amm (minmev amm). Retrieved from <https://ethresear.ch/t/mev-minimizing-amm-minmev-amm/13775> on May 24, 2023. Online forum post.
- Ferreira, M. V. X. and D. C. Parkes (2023). Credible decentralized exchange design via verifiable sequencing rules.
- Foley, S., P. O’Neill, and T. Putnins (2022). Can markets be fully automated? evidence from an automated market maker. Technical report, Working Paper, Macquarie University.
- Gans, J. S. and R. T. Holden (2022). A solomonic solution to ownership disputes: An application to blockchain front-running. Technical report, National Bureau of Economic Research.
- Goyal, M., G. Ramseyer, A. Goel, and D. Mazières (2022). Batch exchanges with constant function market makers: Axioms, equilibria, and computation. *arXiv preprint arXiv:2210.04929*.
- Heimbach, L., E. Schertenleib, and R. Wattenhofer (2022). Risks and returns of uniswap v3 liquidity providers. *arXiv preprint arXiv:2205.08904*.
- Heimbach, L., Y. Wang, and R. Wattenhofer (2021). Behavior of liquidity providers in decentralized exchanges.

- Heimbach, L. and R. Wattenhofer (2022). Sok: Preventing transaction reordering manipulations in decentralized finance. *arXiv preprint arXiv:2203.11520*.
- Josojo (2022, August 4). Mev capturing amm (mcamm). Retrieved from <https://ethresear.ch/t/mev-capturing-amm-mcamm/13336> on May 24, 2023. Online forum post.
- Kelkar, M., F. Zhang, S. Goldfeder, and A. Juels (2020). Order-fairness for byzantine consensus. Cryptology ePrint Archive, Paper 2020/269. <https://eprint.iacr.org/2020/269>.
- Lehar, A. and C. A. Parlour (2021). Decentralized exchanges. *working paper*.
- Leupold, F. (2022, November 1). Cow native amms (aka surplus capturing amms with single price clearing). Retrieved from <https://forum.cow.fi/t/cow-native-amms-aka-surplus-capturing-amms-with-single-price-clearing/1219/1> on May 24, 2023. Online forum post.
- Loesch, S., N. Hindman, M. B. Richardson, and N. Welch (2021). Impermanent loss in uniswap v3.
- Milionis, J., C. C. Moallemi, and T. Roughgarden (2023). Automated market making and arbitrage profits in the presence of fees. *arXiv preprint arXiv:2305.14604*.
- Milionis, J., C. C. Moallemi, T. Roughgarden, and A. L. Zhang (2022). Automated market making and loss-versus-rebalancing. *arXiv preprint arXiv:2208.06046*.
- Park, A. (2022). Conceptual flaws of decentralized automated market making. Technical report, Working paper, University of Toronto.
- Qin, K., L. Zhou, and A. Gervais (2022). Quantifying blockchain extractable value: How dark is the forest? In *2022 IEEE Symposium on Security and Privacy (SP)*, pp. 198–214. IEEE.
- Schlegel, J. C. and A. Mamageishvili (2022). Axioms for constant function amms. *arXiv preprint arXiv:2210.00048*.
- Torres, C. F., R. Camino, et al. (2021). Frontrunner jones and the raiders of the dark forest: An empirical study of frontrunning on the ethereum blockchain. In *30th USENIX Security Symposium (USENIX Security 21)*, pp. 1343–1359.