Optimal Automated Market Makers

Zhengge Zhou*

15th November 2024

Click here to the latest version

Abstract

Blockchain technology has enabled intermediary-free exchanges in which trades are facilitated by automated market-making (AMM) algorithms. This paper shows that: 1) *existing* AMM designs in practice cannot allocate trading needs of liquidity demanders among liquidity providers efficiently; 2) the optimal AMM design attaining efficient trading allocation is structured as a *weighted geometric average* over liquidity providers' preferences; 3) this optimal design emerges in equilibrium when intermediary-free exchanges operate as a decentralized autonomous organization.

Keywords: Blockchain technology, Automated Market Maker, Decentralized Autonomous Organization.

*Gillmore Center for Financial Technology, Warwick Business School, University of Warwick. Email: Zhengge.Zhou@warwick.ac.uk. Correspondence address: Warwick Business School, the University of Warwick, Coventry, CV4 7AL, the United Kingdom.

[1]This paper has greatly benefited from discussion with Andrea Andolfatto, Agostino Capponi, Maxi Guennewig, Florian Heider, Roman Kozhan, Jesus Gorrin Leon, Byung Hwa Lim, Evgeny Lyandres, Kebin Ma, Vincent Maurin, Albert J. Menkveld, Rory Mullen, Ganesh Viswanath Natraj, Leonid Kogan, Dirk Niepelt, Andreas Park, Fahad Saleh, David Skeie, Konstantin Sokolov, Ruslan Sverchkov and Jiawei Wang. I thank seminar, workshop, and conference participants at Gillmore Center, Warwick Business School, Economics of Financial Technology Conference, 2024 Lancaster-Manchester-Warwick PhD Workshop, 2024 FMA Asia Conference, APAD Conference, HEC Paris PhD Workshop, Tri-City Day-Ahead Workshop, CEPR Fintech and Digital Currencies RPN Workshop and 2024 FMA Annual Meeting for their valuable comments.

1 Introduction

A prevalent feature of many modern financial markets is the presence of institutional intermediaries who provide liquidity, transmit information, and facilitate market-making. However, the rise of blockchain technology has enabled the implementation of intermediary-free exchanges, where trades of tokenized assets between liquidity providers (LPs) and liquidity demanders (LDs) are governed by automated market-making (AMM) algorithms. Despite their widespread adoption — exemplified by existing blockchain-based decentralized exchanges that record daily trading volumes exceeding several billion dollars, these algorithmic AMM designs are ad hoc. They are initialised by practitioners in computer science and their economic microfoundation still remains unclear.

Given that, this paper studies the AMM design for intermediary-free exchanges from an economic normative perspective. Using a social planner problem, the paper defines an optimal AMM design for any intermediary-free exchange in its allocative efficiency — minimizing the trading costs for LDs while satisfying the participation constraints of LPs. Then the paper focuses on the implementation of this optimal AMM design such that it can emerge as an equlibrium outcome chosen by market participants on intermediary-free exchanges.

As demonstrated later in the paper, the optimal AMM design with efficient trading allocation exists and is characterized as a weighted geometric average of LP preferences, where the weights reflect each LP's relative liquidity contribution to the exchange. Furthermore, the paper establishes that this optimal design can emerge as an equilibrium bargaining solution if the intermediary-free exchange operates as a fully decentralized autonomous organization (DAO). Within this framework, LPs collectively manage the exchange, enabling them to negotiate the design of the AMM algorithm based on their preferences and bargaining powers. By setting LP bargaining powers in proportion to their liquidity contributions, the resulting equilibrium bargaining solution among LPs immediately implements the optimal AMM design.

This paper sits at the intersection of market microstructure and mechanism design. Prior literature has largely focused on two separate strands: (1) The design of optimal trading mechanisms for financial markets with the presence of institutional financial intermediaries, as explored in foundational works dated back to Myerson (1981), Vickrey (1961), Clarke (1971), and Groves (1973); and (2) the implications of adopting a given specific AMM design on the market quality of the blockchain-based decentralized exchanges (DEXs) — a special but most prominent type of intermediary-free exchanges built upon blockchain technology, as studied by Park (2021), Capponi and Jia (2021), Carre and Gabriel (2022), Aoyagi and Ito (2024), among others. This paper, however, is among the first to address the optimal AMM algorithm design for trades on intermediary-free exchanges. From an economic normative perspective, the desired AMM algorithm is no longer taken as given but becomes the equilibrium outcome in a general (trading) exchange environment without financial intermediaries. Of particular importance, the findings of this paper extend beyond blockchain-based DEXs to any intermediary-free trading environments.

The contributions of this paper are threefold: (1) It characterizes the optimal AMM design for trade on intermediary-free exchanges, where the maximum trading allocative efficiency between LPs and LDs is attained; (2) It provides the first possible economic microfoundation for the commonly used yet ad hoc AMM designs on current blockchain-based DEXs, revealing an inherent trade-off in the design of AMM algorithm: AMM programming simplicity versus trading allocative efficiency; (3) It presents that attaining optimal trading allocative efficiency for an intermediary-free exchange tightly depends on the condition that this exchange operates as a decentralized autonomous organization (DAO): the platform's design of this exchange has to be collectively managed by its LPs, whose respective governance powers are determined by their liquidity contribution to the exchange. Despite being adopted by most decentralized finance (DeFi) projects, this DAO governance feature is studied in this paper within a specific, fundamental economic framework for the first time.

In terms of model specification, this paper develops a two-period model to study the optimal AMM algorithm design for intermediary-free exchanges. In the first period $t = 1$, a group of potentially heterogeneous LPs determine an AMM algorithm to set exchange rates between tokenized assets, such as A and B, on the intermediary-free exchange. In period $t = 2$, a specific type of liquidity demander (LD) arrives at the exchange to fulfil her trading needs.

Building on this model setup, the paper first considers a social planner problem *à la* Holmström and Myerson (1983), a useful benchmark case where we can derive the (first-best) allocation for the trade between LPs and LDs on an intermediary-free exchange. The social planner's role in the context of intermediary-free exchange is to maximise trading efficiency, where she allocates LD's trading needs among LPs to minimise trading costs paid by the LD while satisfying LP participation constraints. Specifically, for each LD's trading need of size q in asset A, the notation of an optimal allocation $(q_i, \tau_i)_i$ is the one that minimizes $\sum_i \tau_i$—the token B transfer made by the LD—across all feasible allocations subject to (1) $\sum_i q_i = q$ (market clearing), ensuring that planner does not absorb any assets while matching LPs and LDs and (2) each LP i is willingly to absorb a trade fraction (q_i, τ_i), say exchanging q_i quantities of token A for τ_i quantities of token B and achieving at least her reservation utility (participation constraint).

The analysis of this benchmark case shows that optimal allocation exists, is unique, and binds LPs' participation constraints, highlighting that the optimal AMM design—when aimed at maximizing trading efficiency in the notation of our social planner problem—is tightly linked to LP heterogeneity. This finding stands in sharp contrast to most blockchain-based DEX practices[1], where their AMM designs allocate LD's trades among LPs strictly in proportion to LP's liquidity contributions to the DEX. While this proportional allocation rule greatly simplifies the programming complexity of the AMM algorithm, it also overlooks the economic heterogeneity among LPs, resulting in suboptimal trading efficiency on DEXs. Thus, the result of this benchmark problem reveals a fundamental

[1] The author thanks Evgeny Lyandres for noting that in the VirtuSwap protocol, LP revenue sharing can also depend on staking protocol tokens, not just liquidity contributions.

trade-off between programming simplicity and trading allocative efficiency in the design of the AMM algorithm, a trade-off that remains largely unexplored in the literature on intermediary-free exchange.

Having characterised the optimal allocation in trading efficiency, as an important industrial implication, this paper then studies its connection to existing single-function algorithm practices in the AMM design of blockchain-based DEXs[2]. This connection is particularly important for the future development of blockchain-based DEXs because it can answer which single-function algorithm, which we denote as $F^\star$, could attain the maximised trading allocation efficiency in the notation of our social planner problem.

For an illustration of this single-function AMM algorithm, suppose that a blockchain-based DEX populates a group of LPs with heterogeneous preferences $\{u_i\}_i$ and liquidity contributions $\{w_i\}_i$. Then this paper shows that the optimal $F^\star$, which attains our maximum trading allocation efficiency, is structured as $\prod_i u_i^{w_i}$, a weighted geometric mean of LP preferences with weights reflecting LPs' liquidity contributions. This functional form represents a Nash social welfare structure *à la* Nash (1950)[3]. We can, therefore, naturally interpret the optimal single-function algorithm for blockchain-based DEXs as a planner who aims for maximum Nash social welfare. Perhaps surprisingly, our result here not only yields a specific form of single-function algorithm that can be hard-coded into the AMM of DEXs for maximum trading efficiency but also, to the best of the author's knowledge, is the first that provides a clear economic rationale for this widespread yet ad hoc single-function-based algorithmic AMM design on blockchain-based DEXs.

The final main result of this paper implements the optimal AMM design derived from our social planner problem for trade on the intermediary-free exchange. In this implementation, LPs are regarded as the owners of the exchange, bargaining with each

[2]For any given DEX, there exists a one-to-one correspondence between its single-function algorithm $F^\star$ and the optimal trading allocation $\tau^\star(q) := \underset{\{q_i\}_i}{min}\{\sum_i \tau_i(q_i) | \sum_i q_i = q\}$ as the current AMM single-function algorithm design for blockchain-based DEX typically requires $F^\star(x - q, y + \tau^\star(q)) = F^\star(x, y)$.

[3]In the seminal work of Nash (1950), Nash derives a form of welfare function as a product of consumers' utilities, arising from axiomatic bargaining with weights determined by the consumers' corresponding bargaining power.

other over how to absorb and allocate the trading needs of LDs. The bargaining power of each LP is assumed to be proportional to her relative liquidity contribution to the exchange[4]. As a result, the equilibrium bargaining solution implements the same trading allocation derived from solving the social planner problem, thereby implementing the optimal AMM algorithm design defined for the intermediary-free exchange.

Instead of serving as a limitation, the assumption that LPs' bargaining power is proportional to their relative liquidity contributions is rather a fundamentally important property we want the implementation to hold. To fully appreciate this point, consider how our implementation framework closely follows the decision-making process within existing decentralized autonomous organizations (DAOs) — entities that operate without central leadership and are collectively managed by their members. For example, a blockchain-based DEX, as a typical DAO, has enabled its platform designs determined by its (governance) token holders through a decentralized "propose-then-vote" governance scheme. Under this decentralised governance, each token holder's voting power is given by the number of governance tokens she owns. Our bargaining framework, coupled with the bargaining powers of LPs proportional to liquidity contribution assumption, indeed precisely captures this DAO-type decision-making feature in reality. To the best of the author's scholarship, the implementation result in this paper seems to be the first that demonstrates the fundamental positive rationale behind "why decentralization matters in Decentralized Finance".

This paper also includes a key extension to address the concern on an important assumption in our implementation framework: the optimal AMM algorithm design for an intermediary-free exchange requires LPs' preference information to be publicly known, though the information of preference is typically privately known by each LP[5]. In this

[4] In each bargaining round, an LP i is selected as the proposer in a probability w_i. She can propose a trading allocation proposal for any given LD's trading need of size q. A feasible trading allocation proposal $(q_j, \tau_j)_j$ requires that 1) $\sum_j q_j = q$; 2) LP j absorbs q_j units of token A for token B transfer of size τ_j. Other LPs can accept or reject this proposal. If accepted, this allocation proposal is then hard-programmed into the AMM algorithm design of this intermediary-free exchange. If not accepted, LPs repeat the bargaining process until an allocation proposal is agreed upon by all LPs.

[5] There is no private information concern about liquidity contributions of LPs as the AMM algorithm records a complete history of LPs' token deposits and withdrawals.

extension, we ultimately prove that if LPs are required by the AMM algorithm to report their preferences (whether true or false) when staking tokens into the exchange, then truthfully reporting their preferences becomes a dominant strategy for all LPs. This result effectively resolves the concern around privately known preference information.

The rest of this paper proceeds as follows. Section 2 reviews the literature. Section 3 presents the model. In section 4, a social planner problem that defines the optimal allocation for trade on the intermediary-free exchange is studied. Section 5 studies the connection of single-function algorithm $F^\star$ in the AMM practice of existing blockchain-based DEX to our optimal trading allocation. Section 6 implements the optimal AMM design as an equilibrium. Section 7 provides two important implications by studying this optimal AMM design. Section 8 addresses the privately known preference information concern in the implementation result. Relevant proofs and some additional discussion are provided in the Appendices.

2 Related Literature

This paper contributes to the rapidly expanding literature on blockchain and decentralized finance. Reviews by Chen et al. (2021), Harvey et al. (2021) and John et al. (2022) provide comprehensive insights. From the market quality perspective of DEXs, various studies contribute complementary findings. For instance, Park (2021) focuses on front-running risks to LPs, while Barbon and Ranaldo (2021) argues that DEXs exhibit lower liquidity and price inefficiency compared to centralized exchanges. Foley et al. (2023) question the empirical superiority of an algorithmic AMM as a market-making design, finding improved trading efficiency for specific asset characteristics. Lehar and Parlour (2021) and Aoyagi (2020) consider the case where LPs as passive investors are exposed to informed traders due to asymmetric information. Capponi and Jia (2021) show that the pre-coded AMM algorithm design at a DEX allows arbitrageurs to extract profit from LPs even in a public information environment. Our work here highlights the fundamental trading allocative inefficiency at the blockchain-based DEX due to the flawed, ad hoc design in their AMMs: pooling LPs' heterogeneities for algorithmic simplicity.

Noticeably, Capponi and Jia (2021) find that the curvature of the AMM single-function algorithm is a key characteristic that can be carefully designed for maximum social welfare. Carre and Gabriel (2022) and Rivera et al. (2023) study the optimally programmable interest rate rule in a decentralised lending platform. Rather than taking the AMM algorithm design as given in these studies, this paper studies the optimal design of AMM from an economically normative viewpoint: It begins with a social planner problem and then defines the first-best AMM algorithm design straightforwardly. As a result, the main findings of this paper are not only about the functional form of the optimal AMM algorithm design but also the economic microfoundation to this *ad hoc* AMM algorithm design, addressing a significant gap in the literature on DEXs. Another important paper is Fabi and Prat (2022) where they interpret AMM design via consumer theory. Rather than taking LPs homogeneous in preference and studying the optimal AMM algorithm design being aligned with this homogeneous preference as in Fabi and Prat (2022), the paper here allows the LPs to be generally heterogeneous. Furthermore, we implement the optimal AMM algorithm design in equilibrium, yielding an important implication for future industrial development on intermediary-free exchanges.

There also exist some interesting studies on the "optimal" AMM algorithm designs from the perspectives of financial engineering and computer science. Leading examples include Angeris et al. (2021), Bichuch and Feinstein (2022), Schlegel et al. (2022), Goyal et al. (2023) and Angeris et al. (2023). These papers focus on finding a mathematical axiomatic framework to encompass and generalize the geometric properties of the AMM single-function algorithm. Taking Angeris et al. (2021) as an example, they find that a concave, nonnegative, nondecreasing, and homothetic payoff function for LPs is "equivalent" to deploying a concave, nonnegative, nondecreasing, and homothetic AMM algorithm function on DEXs[6]. Our work here, however, studies the optimal AMM algo-

[6]Technically speaking, the "equivalence" here means that LP's payoff function and the single-function algorithm in AMM's design are Fenchel conjugates of each other.

rithm design from the economic normative perspective and in a general intermediary-free exchange environment.

The implementation result of this paper contributes to the literature on how blockchain technology-backed protocols achieve decentralised consensus. Noticeable contributions in this direction in Bitcoin's protocol include such as Abadi and Brunnermeier (2018), Biais et al. (2019), Leshno and Strack (2020) and Cong et al. (2021). However, DEXs are built on open-source smart contracts systems such as Ethereum and Tezos in the sense that the consensus of any platform design is facilitated through a decentralised manner: communication and collaboration between community members such as LPs in the context of DEX[7].

Existing literature says little about how the decision is made by society members on the blockchain without centralised leadership. Exceptions include Aoyagi and Ito (2022) and Sockin and Xiong (2023). Aoyagi and Ito (2022) focus on the equilibrium trading fee as the key characteristic to be implemented between members on a decentralised platform. Sockin and Xiong (2023) examines whether decentralising ownership can be an innovation to resolve the conflict between platforms and their users. Han et al. (2023) points out the interest conflict between whale token holders and small token holders in DAOs. Our implementation result contributes to this literature by presenting a strict game-theoretical DAO governance framework for this decentralised "propose and vote" decision-making process and by providing a positive, fundamental answer to "why decentralization matters in Decentralized. Finance".

3 Model

This section presents an overview of the model for studying the optimal design of an automated market-making (AMM) algorithm in the intermediary-free exchange. Two types of assets, A and B, are traded at this intermediary-free exchange. Without loss of

[7] The details about how smart contracts system implements such "decentralised" platform feature can be found in, for examples, Warren and Bandeali (2017), Zhang et al. (2018) and Adams et al. (2021).

any generality, the value of asset A in terms of asset B, which we denote as $p > 0$, is common knowledge to all agents. Agents in this intermediary-free exchange economy are of two types: liquidity providers (LPs) and liquidity demanders (LDs).

LDs are the users or traders of this intermediary-free exchange. We assume they are exposed to liquidity shock θ, which has a commonly known distribution over $[\underline{\theta}, \overline{\theta}]$ with a CDF G. Upon realising a specific shock θ, this LD of type-θ is assumed to have a trading need of purchasing $q(\theta) > 0$ quantities of asset A from this intermediary-free exchange. To ease expository, only the buy side of asset A is presented here while the sell side can be analysed similarly.

Furthermore, we assume the net utility payoff obtained by this trader from purchasing asset A of size q following that

$$u(q;\theta) - \tau(q),$$

where $u(q;\theta)$ is the utility benefit from purchasing a size-q asset A and $\tau(q)$ is the respective transfer paid by this trader.

LPs are investors possessing some amount of capital which they can invest in either the intermediary-free exchange or an alternative investment. Investors are incentivized to lock their capitals into this intermediary-free exchange because being LPs entitles them to earn some expected amount of trading fees charged on the trading activities made by LDs. Notably, this liquidity provision payment, or the market-making service fee, is now available to retail investors. This is one key feature that distinguishes this intermediary-free exchange from traditional financial markets where market-making service as well as the associated service fee generally apply to institutional financial intermediaries only.

LPs are very likely to exhibit heterogeneity in their capital size as well as economic preferences. We assume that a group of investors lock their capital into the intermediary-free exchange and thus become the LPs. The relative liquidity (capital) contribution made by each LP i is assumed to be $w_i \in (0,1)$. Clearly, $\sum_{i=1}^{n} w_i = 1$.

As for preference of LP i, it is assumed to be represented by a general mapping u_i:

$$u_i : \mathbb{R}_+^2 \longrightarrow \mathbb{R}_+,$$

where the value of $u_i(x, y)$ represents the utility LP i can derive from holding a bundle of assets A and B, say (x, y), which represents x units of A and y units of B.

While we do not specify a particular context for the heterogeneity exhibited among LPs, their diverse preferences can be interpreted in terms of portfolio or consumption preferences. For example, Sockin and Xiong (2023) models that digital platform users with Cobb-Douglas utility preferences over two complementary tokens can derive some utility from consuming the bundle of two types of tokens. Importantly, we do not restrict LP preferences to the Cobb-Douglas utility class as in Sockin and Xiong (2023) but generalize them to homothetic preferences, as outlined below.

Assumption 1 (homothetic preference): *Throughout the paper, preferences of LPs, $\{u_i\}_i$, are assumed to be homothetic: $u_i(\lambda(x, y)) = \lambda u_i(x, y)$ for any $i \in I, \lambda \geq 0$.*

Homothetic preference is not overly restrictive. For example, the family of preferences with constant elasticity of substitution including Leontief, Cobb-Douglas, and linear preferences are all homothetic[8]. In addition, most AMM algorithm designs adopted by *existing* blockchain-based DEXs are structured as homothetic. Leading examples include $u(x, y) = x + y$ on mStable; $u(x, y) = x^{\frac{1}{2}} y^{\frac{1}{2}}$ on Uniswap-V2, $u(x, y) = x^w y^{1-w}$ on Balancer, $u(x, y) = C(x + y) + x^{\frac{1}{2}} y^{\frac{1}{2}}$ on StableSwap and Saber, among many others.

One important exception is the AMM algorithm design on Uniswap–V3. With the additional concentrated liquidity feature in place, the resulting AMM algorithm on Uniswap-V3 is structured as $u(x, y; x_0, y_0) = (x+x_0)(y+y_0)$, which is not homothetic. However, we

[8] We call a preference a CES preference with an elasticity of substitution $\sigma \in \mathbb{R}_{++} \backslash 1$ if it follows: $u(\mathbf{x}) = \left(\sum_i (a_i x_i)^{\frac{\sigma-1}{\sigma}}\right)^{\frac{\sigma}{\sigma-1}} \quad \forall \mathbf{x} \in \mathbb{R}_+^n \quad and \quad \mathbf{a} = \{a_i\}_i \in \mathbb{R}_{++}^n$. CES preferences are homothetic and they are extensively studied in the literature. Leontief, Cobb-Douglas, and linear preferences are indeed the limit of a CES preference with σ converging to $0, 1$ and $+\infty$, respectively. For example, taking log for both sides of CES preference $u(x_1, x_2) = (a_1 x_1^\gamma + a_2 x_2^\gamma)^{\frac{1}{\gamma}}$ and then considering its limit with $\gamma \to 0$ yields that $u(x_1, x_2) = x_1^{a_1} x_2^{a_2}$ — a Cobb-Douglas preference.

can decompose this Uniswap-V3 AMM algorithm as an AMM algorithm (with homotheticity) in Uniswap-V2-type plus some independent price range constraints[9]. Therefore, the insight we derived in this paper under this homothetic property can still extend to the AMM design of Uniswap-V3.

The AMM algorithm design that fully governs the trade between LPs and LDs on an intermediary-free exchange consists of two key algorithmic components:

- The first algorithmic component has to record the number of assets (bundles) staked by LPs into this exchange, say $\{x_i, y_i\}_i$. Such an algorithmic (market structure) component is known as *liquidity pool* in the literature of blockchain-based DEXs. We directly borrow this language for convenience. The novelty of this liquidity pool market structure allows LDs to trade against the pooled liquidity in the exchange straightforwardly, thereby eliminating the need for financial intermediaries to act as market makers.

- The second algorithmic component is needed to allocate the trade request made by the external LD among internal LPs so that each LP absorbs a fraction of this trade. We call this component *AMM algorithm.*

Therefore, a design of the AMM algorithm for trade on an intermediary-free exchange is indeed equivalent to the trading allocation rule that splits the trade needs of LDs among the group of LPs. Technically, an AMM algorithm can be represented by a vector-valued mapping in the following sense:

$$F\Big(\cdot; \{x_i, y_i\}_i, \{u_i\}_i\Big) : \mathbb{R} \to \mathbb{R}^{2n}, \text{where } F\Big(\Delta x; \{x_i, y_i\}_i, \{u_i\}_i\Big) = \begin{bmatrix} (x_1 - \delta x_1, y_1 + \delta y_1) \\ \vdots \\ (x_n - \delta x_n, y_n + \delta y_n) \end{bmatrix}. \tag{1}$$

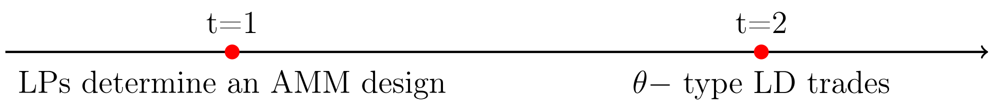
[9]This decomposition is unique. Uniswap-V2 AMM design plus some price range constraints replicate a particular Uniswap-V3-AMM design, and vice versa

In terms of economics, a given vector-valued mapping F designed for allocating trades on an intermediary-free exchange implies that: 1) the LD can pay $\Delta y := \sum_i \delta y_i$ in asset B for purchasing a quantity $\Delta x := \sum_i \delta x_i$ of asset A from the exchange (or from the group of LPs); and 2) each LP i absorbs a fraction δx_i of asset A trading needs for a payment δy_i in asset B in return.

Thus, when we say determining an AMM algorithm design for trade on an intermediary-free exchange, we mean that how a group of LPs with heterogeneous liquidity contributions $\{x_i, y_i\}_i$ and preferences $\{u_i\}_i$ reach an agreement in terms of allocating any feasible trade $(\Delta x, \Delta y)$ internally.

With this said, the optimal AMM design problem for trade on any intermediary exchanges turns out to be a trading allocation problem that can be studied in a simple two-period model as follows.

The model timeline is depicted below:



For any intermediary exchange populated by a group of heterogeneous LPs whose respective preferences and liquidity contributions are given by $\{u_i\}_i$ and $\{x_i, y_i\}_i$,

- LPs at $t = 1$ determine an AMM algorithm design. To put it differently, LPs have to agree upon a trading allocation solution ahead of the arrival of LDs (traders) in this intermediary-free exchange. As for how LPs reach an agreement upon an AMM design, we defer this discussion until section 6 of this paper. At this point, let us suppose they can implement an AMM design based on their heterogeneous interests.

- At $t = 2$, suppose the (single) LD experiences a liquidity shock θ, whereby she generates a need for purchasing asset A of size $q(\theta)$ to be fulfilled at this intermediary-free exchange.

In this model, we aim to address the AMM design problem faced by LPs at $t = 1$ given the (anticipated uncertain) trading needs of LDs at $t = 2$. This problem, in general, is mathematically extremely complicated, as LPs are allowed to exhibit heterogeneities in both preferences and liquidity contributions. However, we notice that this two-dimensional problem can be made much easier if accounting for the reality that any exchange in the economy also confronts competition from other trading platforms. By assuming inter-platform completion *à la* Bertrand, we can conjecture and verify later in the online appendix B that the payment in asset B charged by each intermediary-free exchange for absorbing a given size of asset A trade made by LDs is symmetric.

With this said it becomes evident that the optimal trading allocation or equivalently the optimal AMM design chosen by LPs at $t = 1$ should be the one(s) such that the LD at $t = 2$ pays some minimum trading cost, subject to LPs participation constraints. Indeed, we will characterise this minimum trading cost term via a social planner problem, to be defined more formally in the following section.

4 The optimal AMM design: A social planner problem

In this section, we consider a benchmark case where a social planner can allocate the trading needs of LDs among LPs for trading allocative efficiency, providing us with an economically meaningful notation in the optimal AMM design required for trade on an intermediary-free exchange.

It is noteworthy that instead of restricting them to specific parameters, liquidity contributions and preferences of LPs in our social planner problem are allowed to be generally heterogeneous. Consequently, the resulting trading allocative efficiency will reveal which market inefficiencies are unavoidable features of the primitive intermediary-free exchange environment and which are instead the symptoms of a flawed AMM design.

4.1 A social planner problem for an intermediary-free exchange

In our model timeline, the implementation of an intermediary-free exchange requires LPs to stake their capital first and then determine a trade allocation ahead of the arrival of LDs. This setting follows the social planner problem *à la* Holmström and Myerson (1983) where a benevolent social planner chooses a trading allocation that maximizes traders' utility *ex ante*.

Based on classical social planner notation, we can, therefore, define the optimal trading allocation for trade on an intermediary-free exchange by solving the social planner problem as follows.

$$\textbf{Planner's problem:} \quad \underset{\{q_i(\theta),\tau_i(\theta)\}_i}{Max} \quad u\left(\sum_i q_i(\theta), \theta\right) - \sum_i \tau_i(\theta)$$

$$\textit{subject to} \quad u_i\Big(x_i - q_i(\theta), y_i + \tau_i(\theta)\Big) \geq \pi_i(x_i, y_i) \quad \forall i \in 1, ..., I \tag{2}$$

$$\textit{and} \quad \sum_i q_i(\theta) = q(\theta). \tag{3}$$

Above, the first set of constraints represents participation constraints faced by LPs, whereby $\pi_i(x_i, y_i)$ represents the exogenously given reservation utility obtained by each LP i, which she would get if she did not participate; and the second constraint is the market clearing condition ensuring that social planner does not retain any asset in the process of matching LPs and LDs. Therefore, conditionally upon satisfying these two constraints, the planner has to choose a feasible allocation $\{q_i(\theta), \tau_i(\theta)\}_i$ to maximise the net utility payoff of LD for each possible realization of θ.

Notably, coding these allocation solutions $\{q_i(\theta), \tau_i(\theta)\}_i$ for all feasible θ into the AMM algorithm defines what we call the optimal AMM design immediately. In other words, this optimal trading allocation and the optimal AMM design are interchangeable in this paper.

Solving the above optimization problem is straightforward. We can show that the participation constraints of LPs always bind at the optimum. Intuitively, if this was not the case, keeping $\{q_i\}_i$ unchanged and slightly reducing some τ_i — the transfer made by LD in asset B — would immediately increase LD's trading payoff while still ensuring the satisfaction of LPs participation.

Lemma 1 (optimal trading allocation) *For any intermediary-free exchange populated by LPs with respective references and liquidity contributions given by $\{u_i\}_i$ and $\{x_i, y_i\}_i$, its optimal trading allocation $\{q_i, \tau_i(q_i)\}_i$ in the notation of our social planer problem is characterised by*

$$\tau(q) = \underset{\{q_i\}_i}{min}\left\{\sum_i \tau_i(q_i) : \sum_i q_i = q\right\}, \tag{4}$$

where each $\tau_i(\cdot)$ satisfies that

$$u_i\Big(x_i - q, y_i + \tau_i(q_i)\Big) = \pi_i(x_i, y_i). \tag{5}$$

Hereafter, we simplify the notation by suppressing θ to ease paper exposition[10]. For each feasible trade $(q, \tau(q))$ on the intermediary-free exchange, on the liquidity demand side, the LD's primary concern is the total trading cost $\tau(q)$ required to acquire q units of asset A from the liquidity pool. In contrast, on the liquidity supply side, each LP i focuses on a fraction of the trade (q_i, τ_i), associated with her post-trade utility if absorbing this fraction trade. Should the LD achieve higher payoffs elsewhere, they would select alternative platforms to fulfil trading needs, making the total trading payoff for the LD the core measure of allocative efficiency for trade on this intermediary-free exchange, given the participation of LPs.

Aim for efficient allocation for trade on the intermediary-free exchange, this social planner hereby selects an allocation $\{q_i, \tau_i\}_i$ per Lemma 1 to maximize LD's trading

[10] This does not impact the results due to the revelation principle, which implies that it is without loss of generality to assume the intermediary-free exchange post a direct revelation mechanism to which LD would truthfully reveal their types or sizes of trading needs.

payoff across all feasible allocations as defined by

- Binding LP Participation Constraint — $u_i(x_i - q_i, y_i + \tau_i) = \pi_i(x_i, y_i)$;
- Market Clearing Condition — $\sum_i q_i = q$.

Armed with the result in Lemma 1, one direct implication is that implementing an optimal trading allocation or AMM design for an intermediary-free exchange lies in satisfying the LPs' participation constraints. This simple yet intuitive result contrasts sharply with current AMM practices on existing blockchain-based DEXs. Indeed, these existing AMM practices follow an allocation rule known as the "proportional allocation principle." In this approach, only the LPs' liquidity contributions are considered when determining how to absorb and split the LD's trading needs among LPs. In other words, this proportional allocation mechanically pools away other dimensions of heterogeneity among LPs, particularly their utility preferences. A detailed discussion of the allocative inefficiency induced by the implementation of this proportional allocation rule on DEXs is provided in Appendix A.

Also, Lemma 1 demonstrates that achieving efficient allocation in trade on an intermediary-free exchange depends critically and collectively on the functional form of all LPs' preferences. However, we want to emphasize that deriving the explicit functional form of τ in (4) given (5) requires a computation over all feasible allocations. This is a challenging task unless the number of LPs is small. Developing practical algorithms that solve this optimal AMM design with good computational performance is crucial for the future development of intermediary-free exchanges including blockchain-based DEXs and it is yet to be studied. To summarise, Lemma 1 reveals a fundamental and unavoidable trade-off between coding simplicity and economic trading efficiency in designing an economically meaningful AMM algorithm for intermediary-free exchanges.

4.2 The optimal AMM design: a single-function representation

Built upon the optimal trading allocation in Lemma 1, we know that the pricing schedule τ faced by the LD in this intermediary-free exchange is given by

$$\tau(\cdot) : \mathbb{R} \to \mathbb{R}, \quad \text{where} \quad \tau(q) = \min_{\{q_i\}_i} \left\{ \sum_i \tau_i(q_i) : \sum_i q_i = q \right\}.$$

By taking this optimal pricing τ as given, we are now interested in whether there exists an associated single function u_{AMM} such that the following invariant property is preserved:

$$u_{AMM}(x - q, y + \tau(q)) = u_{AMM}(x, y). \tag{6}$$

The AMM design built upon a single-function u_{AMM}, along with its associated invariant property as specified above, is often referred to as bonding curve design in the literature on blockchain-based DEXs. With this said, characterising the optimal bonding curve design is thus of first-order importance. Indeed, we have observed many trials of different bonding curve designs on existing blockchain-based DEXs. Leading examples include $u_{AMM}(X, Y) = X \times Y$ on Uniswap-V2, $(X + a) \times (Y + b)$ on Uniswap-V3, $X^w \times Y^{1-w}$ on Balancer, $X + Y$ on StableSwap, and many others.

However, on the one hand, it appears that industrial practitioners as well as academics have not yet reached an agreement in terms of how to select or design an "optimal" bonding curve function u_{AMM}. On the other hand, by taking the bonding curve of Uniswap (the largest existing DEX by market share) as an example, say $u_{AMM}(x, y) = X \times Y$, we can easily derive that $\tau(q) = \frac{X \times Y}{X - q} - Y$. This pricing τ is ad hoc as $\tau(q)$ goes to infinite when q converges to X, which has neither precedent in traditional financial markets nor a clear economic microfoundation in the literature.

To the best of our knowledge, there is no existing study in the literature that can provide a plausible economic interpretation for this ad hoc bonding curve design. Our analysis here aims to address this gap, thereby providing an essential implication for the development of future bonding curve designs on DEXs.

Role of optimal AMM As mentioned earlier, the (optimal) AMM algorithm for the intermediary-free exchange acts as the role of the social planner, say allocating the LD's trade among LPs subject to their preferences and liquidity contributions. Then we ask: What if this social planner has a preference? It may, therefore, become not too surprising to see that the bonding curve function u_{AMM} generating the optimal pricing schedule τ would be structured as the planner's preference.

Nevertheless, characterising the social planner's preference is challenging as the optimal pricing schedule 4 has no explicit form. To proceed, we need well-defined economics in terms of this preference, as stated below.

Aggregated LP The role of the social planner in allocating trades among LPs at a decentralized exchange reminds us of the classical economics literature on aggregated consumers: How do individual budgets and consumption preferences determine the aggregated consumption decision? We show below that it is essentially helpful and intuitive to understand our social planner as an aggregated LP (consumer).

Formally, we can denote the liquidity contribution made by each LP i by its capital value, say

$$b_i := x_i + py_i,$$

where p is the price of asset A against asset B at the time LP i stake her asset bundle, (x_i, y_i), into the exchange.

Then for each feasible trade $(q, \tau(q))$, the participation constraint conditions for LPs to accept this aforementioned optimal allocation $\{q_i, \tau_i(q_i)\}_i$ in the language of consumer theory would turn out to be

$$u_i\Big(x_i(p, b_i) - q_i, y_i(p, b_i) + \tau_i(q_i)\Big) \geq u_i\Big(x_i(p, b_i), y_i(p, b_i)\Big) := \pi_i(p, b_i).$$

Above, $(x_i(p, b_i), y_i(p, b_i))$ is the most preferred bundle of assets for LP i given that her budget is b_i[11]. The term $\pi_i(p, b_i)$ measures the reservation utility LP i that she could obtain if did not participate in this trading but instead consumed her budget directly.

We now reach the point to formally define the preference of our social planner in the language of the aggregated LP.

Definition 1 (preference of social planner): *A function $u_{AMM} : \mathbb{R}^2_+ \to \mathbb{R}_+$ is referred to as the preference of our social planner if*

$$\Big(\boldsymbol{x}(p, \boldsymbol{b}), \boldsymbol{y}(p, \boldsymbol{b})\Big) = \Big(\sum_i x_i(p, b_i), \sum_i y_i(p, b_i)\Big), \tag{7}$$

where $\boldsymbol{b} := \sum_i b_i$. Here, $(x_i(p, b_i), y_i(p, b_i))$ is the most preferred bundle of assets of LP i under a budget b_i, while $\Big(\boldsymbol{x}(p, \boldsymbol{b}), \boldsymbol{y}(p, \boldsymbol{b})\Big)$ is the social planner's most preferred asset bundle under a budget given by $\boldsymbol{b}$.

Condition (7) in this definition is intuitive: the most preferred bundle of assets for the social planner (or the optimal AMM design) has to be consistent with the aggregation over the most preferred token bundles of all LPs in the DEX. This definition is general as the existence of u_{AMM} is allowed to behold for arbitrary $p > 0$, liquidity contributions $\{b_i\}_i$, and preferences $\{u_i\}_i$. It results in the structure of u_{AMM}, if exists, depending on the specific distribution among LPs' liquidity contributions and preferences. This is in sharp contrast to the classical preference aggregation approach in Gorman (1968) where changes in the distribution of budget contribution are required to have no impact on the aggregated preference.

Armed with this definition and letting w_i denote the relative liquidity contribution of

[11] Specifically, the most preferred bundle of assets for LP i with a budget b_i is defined as

$$\Big(x_i(p, b_i), y_i(p, b_i)\Big) = \underset{(x,y)\in\mathbf{R}^2_+ : px+y\le b_i}{argmax} \quad u_i(x, y).$$

Moreover, it is not hard to prove that for a given price p, LP i would choose the bundle of asset (x, y) consistent with $(x_i(p, b_i), y_i(p, b_i))$ while staking it into the exchange.

LP i to the exchange, say

$$w_i = \frac{b_i}{\mathbf{b}},$$

we can now formally characterise the preference of our social planner, which is, in other words, the bonding curve function associated with the optimal AMM design as stated in the following proposition.

Proposition 1 (optimal bonding curve function). *For an intermediary-free exchange populated with a group of LPs whose respective preferences and liquidity contributions are given by $\{u_i\}_i$ and $\{b_i\}_i$, the bonding curve function u_{AMM} associated with our optimal AMM design can be represented by*

$$u_{AMM}(x, y) = \max_{\{x_i, y_i\}_i} \left\{ \Pi_i \left(\frac{u_i(x_i, y_i)}{w_i} \right)^{w_i} \quad \middle| \quad \sum_i (x_i, y_i) = (x, y) \right\}. \tag{8}$$

The proof of Proposition 1 is straightforward as it follows the standard technique in the literature on aggregated consumers. Proposition 1 shows us that the preference of our social planner is structured as a weighted geometric mean of the individual preferences of LPs, with weights corresponding to each LP's relative liquidity contribution to the exchange. Additionally, the resulting value of u_{AMM} at any bundle point (x, y) is indeed equal to the maximal Nash social welfare with the maximum taken over all possible allocations $\{x_i, y_i\}_i$.

Nash's seminal work in Nash (1950) showed that a welfare function, structured as the product of individual utilities, naturally arises in axiomatic bargaining contexts, with each individual's weight in the function reflecting their bargaining power in the game. This product form, known as the Nash social welfare function, has become widely studied in economic theory. Viewing the optimal AMM design through the Nash social welfare lens (i.e., a normative economic perspective) seems to be the first in the literature. By doing so, it turns out to be natural to interpret the optimal AMM design as acting as a kind of "social planner" who is aiming for trading allocation efficiency. Further, it becomes evident to understand the functional form of the bonding curve function associated with the optimal AMM design as the preference of this social planner. Other applications and industrial implications built upon Proposition 1 are explored in Section 6 of this paper.

5 Implementing optimal AMM design under decentralised governance scheme

A key question that remains to be answered in this paper is whether the optimal allocation solution derived in Lemma 1 can emerge as an equilibrium outcome chosen by the market participants on the intermediary-free exchange, especially by LPs who stake their assets to the exchange *ex ante*.

Designing a reasonable, practical implementation framework among LPs requires a comprehensive understanding of the typical decision-making process within intermediary-free exchanges. As one of the most prominent decentralized autonomous organization (DAO) applications, blockchain-based DEXs feature decentralized governance in the sense that any platform design including this AMM algorithm design can be collectively managed by LPs through a decentralised decision-making process. Within this decentralized governance structure, LPs can vote on the platform design proposal with some governance rights proportional to the number of governance tokens they hold, see Han et al. (2023) for detailed DAO governance introduction.

This decentralised decision-making process thus suggests a Nash bargaining game designed among LPs to implement the optimal AMM design as the "propose then vote" structure reminds of the typical actions made by agents in a Nash bargaining game.

5.1 n-person Nash Bargaining Solution

Let us specify the n-person Nash bargaining problem and its solution concept for our intermediary-free exchange.

Suppose the number of assets in the post-trade liquidity pool is represented by $\mathcal{R} = (\mathbf{x}-q, \mathbf{y}+T(q))$ and LPs can now bargain over the division of this post-trade liquidity pool. We consider the division of this post-trade liquidity pool simply because the resulting division solution minus the initial liquidity contributions of LPs immediately measures how LPs allocate the LD's trade on the intermediary-free exchange among themselves.

The set of possible division agreements is

$$X = \left\{(x_i, y_i)_i \in \mathbb{R}_+^{2\times n} \quad | \quad \sum_i (x_i, y_i) = \mathcal{R} = (\mathbf{x} - q, \mathbf{y} + T(q))\right\}$$

where x_i and y_i are the respective amounts of assets A and B taken by LP i from the post-trade liquidity pool. Alternatively, we can have the feasible set of utilities for LPs as

$$V = \left\{(z_i)_i \in \mathbb{R}_+^n \quad | \quad \exists (x_i, y_i)_i \in X, \forall i, z_i \leq u_i(x_i, y_i)\right\}. \tag{9}$$

The disagreement point in this Nash bargaining problem is assumed to be $d = (d_i)_i = 0$ for simplicity[12]. Then the solution concept of this Nash bargaining problem $(V, \{u_i\}_i)$ is given as follows.

Definition 2 (Nash Bargaining Solution). *Let $(V, \{u_i\}_i, \beta)$ as the n-person Nash bargaining problem with the weight $\beta = (\beta_i)_i$ satisfying $\sum_i \beta_i = 1$ and $\beta_i > 0$. A payoff vector $z^\star(\beta) = \left\{z_i^\star(\beta)\right\}_i = \left\{u_i(x_i^\star, y_i^\star)\right\}_i \in V$ is called the Nash bargaining solution of*

[12]For Nash bargaining problem, disagreement point $d \in V$ is essential to ensure the existence of the solution, especially for the interior disagreement point d in V for the existence of non-trivial solution, see e.g. Kaneko and Nakamura (1979). So the more natural and intuitive way to define the disagreement point in this paper is taking $d = (d_i)_i = \Big(D_i(p, b_i)\Big)_i$, where $D_i(p, b_i)$ represents the maximum utility LP i can obtain if the bargaining is unsuccessful and LP i, consumes her budget b_i directly. However, this generalization only complicates our notation and has no impact on our results, since $d = 0$ and $d = \Big(D_i(p, b_i)\Big)_i$ are both interior points in V and play the same role in guaranteeing the existence of a non-trivial solution.

$(V, \{u_i\}_i, \theta)$ *if* $z^\star$ *solves the following optimization problem*

$$\max_{z=(z_i)_i \in V} \quad \Pi_i \left(\frac{z_i}{\beta_i}\right)^{\beta_i}$$

Or equivalently, we replace z_i *by* $u_i(x_i, y_i)$ *and then normalize the objective function by multiplying* $\Pi_i \left(\frac{1}{\beta_i}\right)^{\beta_i}$. *That is,*

$$\max_{(x_i,y_i)_i \in X} \quad \Pi_i \left(u_i(x_i, y_i)\right)^{\beta_i} \tag{10}$$

It is important to note that setting $\beta_i = \frac{1}{n}$ for all $i = 1, ..., n$ results in the symmetric Nash bargaining problem. This type of bargaining problem was first proposed by Nash (1950, 1953) for a two-person case and later extended by Hart and Mas-Colell (1996) for an n-person case. The asymmetric Nash bargaining problem was considered by Binmore et al. (1986) for the two-person case, where the asymmetry arises from different beliefs about the risk of negotiation breakdown. More recently, Okada (2010), Britz et al. (2010) and Kawamori (2014) have explored the solution concept of n-person asymmetric Nash bargaining problem and rationalized them under non-cooperative Nash bargaining games. In this paper, we connect our implementation work to this literature by modelling the decision-making process in a decentralised governed intermediary-free exchange as an n-person asymmetric Nash bargaining problem, where the asymmetry in bargaining power between LPs originates from their asymmetrical liquidity contributions to the exchange.

5.2 Bargaining procedure among LPs

The implementation objective is to establish a noncooperative bargaining game among LPs to yield an equilibrium that achieves the optimal trading allocation as defined in Lemma 1. An appropriate bargaining game framework should effectively capture the competition among LPs within the decision-making process of an intermediary-free exchange as well as the asymmetric bargaining powers between LPs due to their asymmetrical liquidity contributions to the exchange.

Let us begin with the specification of the desired decentralised decision-making process. Let $\rho \in (0, 1)$ be a fixed parameter. There are potential infinite rounds in the bargaining procedure under the decision-making process. For each round, we have two phases: the propose phase and the respond phase.

Propose Phase. One of the LPs will be chosen as the proposer at the beginning of each round $t = 1, 2, 3, ...$ The probability LP i becomes the proposer in each round is β_i. This selected LP proposes a feasible allocation vector $\{(x_i, y_i)\}_i$ in X or equivalently, a feasible utility payoff vector $z = (z_i)_i$ in V.

Respond Phase. All other LPs either accept or reject the proposal sequentially.[13]

- If all other LPs accept it, then this bargaining game ends and LPs obtain the respective allocated liquidities listed in this proposal $\{(x_i, y_i)\}_i$.
- Otherwise, the bargaining procedure moves to the next round. In this case, with probability ρ, the negotiation continues among LPs and the game repeats. That is, it goes back to the "propose phase". With probability $1 - \rho$, the game ends and all LPs get the liquidity allocation d_i specified in the predetermined disagreement point.

In the proposal phase, we directly assume that the probability of each LP i being selected as the proposer is β_i. In simpler terms, the higher the budget/liquidity contribution LP i has in the liquidity pool, the greater the chance of being chosen as the proposer in each round. The intuition behind this is straightforward. In our sequential bargaining game, there exists a risk of negotiation breakdown denoted by probability $1 - \rho$, possibly due to the intervention of some external factor. This breakdown threat is "equivalent" to LPs' attitude toward the time needed to reach a consensus, as detailed in Binmore

[13] The order of how other LPs respond to this proposal does not matter in our paper as only the allocation accepted by all LPs unanimously can be implemented.

et al. (1992)[14]. The larger the position LP i has in the liquidity pool, the riskier the game becomes for her to the next round. To compensate her for this extra risk, it is reasonable to offer LP i a relatively higher first-move opportunity in a decentralized platform.

In our Nash bargaining model, it is assumed that LPs have perfect information regarding all historical actions taken by other LPs. This assumption is quite strong. Nevertheless, in the context of a blockchain-based platform, such as decentralized exchanges (DEXs) operating on public blockchains, this concern is significantly mitigated. Public blockchains, like Ethereum, inherently leverage blockchain technology to ensure transparency in trade activities and governance structures and often make the underlying code open-source. This transparency framework allows all participants to easily access and verify the historical actions taken by other LPs, thus supporting the model's public information assumption effectively.

5.3 Stationary Subgame Perfect Equilibrium

Denoted by $G(\rho, \beta)$, the above bargaining model incorporates the negotiation breakdown probability $1-\rho$ and the probability distribution $\beta = \{\beta_i\}_i$, determining which LP is the proposer in each round. For each LP i, a strategy is represented as a sequence of actions, as follows:

$$\sigma_i = \{\sigma_i^t\}_{t=1}^{\infty},$$

where σ_i^t is a mapping that prescribes the $t-$th round strategy of LP i, say,

$$\sigma_i^t = \begin{cases} \textit{a proposal } z_i^t = (z_i^t)_i \in V, \textit{ if LP } i \textit{ is the proposer;} \\ \textit{a response function assigns "accept" or "reject" to others' proposals, otherwise.} \end{cases}$$

[14] For simplicity, we skip the discussion regarding how to micro-found the Nash bargaining solution from assuming asymmetric discount rates to LPs' future payoff. But there does exist a way to do so. In short, identical results hold if alternatively, we assume LP i, who contributes β_i fractional liquidity to the liquidity pool, discounts her future payoff with the rate $r_i = \frac{1}{\beta_i}$.

Following the literature on noncooperative multi-person sequential bargaining games, we only study the stationary subgame perfect equilibrium (SSPE) denoted as $\sigma^\star = (\sigma_1^\star, .., \sigma_n^\star)$ in the game $G(\rho, \beta)$. Focusing on SSPE is intentional, as it greatly simplifies the set of strategies for each LP. Additionally, restricting our attention to SSPE can help us avoid the equilibria multiplicity problem in a dynamic game. We define SSPE in the conventional manner, whereby the strategy of each LP in the t-th round depends solely on the history within that round t. We sum up the outcomes of our implementation results in the following proposition.

Proposition 2 (Implementation of Nash Bargaining Solution). *For each $\rho \in [0, 1)$, the noncooperative bargaining game $G(\rho, \beta)$ exists an SSPE $\sigma^\star(\rho, \beta)$. Denote by $z^\star(\rho, \beta)$ the respective expected utility payoff vector of LPs in this SSPE. Then, as $\rho \to 1$, say, the probability of negotiation breakdown $1 - \rho \to 0$, $z^\star(\rho, \beta)$ converges to $z^\star(\beta)$, the asymmetric Nash bargaining solution of $(V, \{u_i\}_i, \beta)$.*

The rigorous proof is provided in Appendix A, where we establish the existence of SSPE and construct the SSPE strategy for each LP. Leveraging the fixed point theorem facilitates a straightforward proof. Regarding the equilibrium strategy, we adhere to the standard methodology found in the literature on sequential bargaining games for the two-person case, extending it to the N-person scenario. Specifically, the equilibrium strategy of LP i is given by that: If selected to be the proposer, she will propose the allocation to maximize her residual while offering other LPs their respective continuation utility payoffs; however, if she is selected as the responder, she will always "accept" the proposal made by other LPs if the offered allocation ensures her a utility no less than her expected continuation utility, and "reject" otherwise. As $\rho \to 1$ (i.e., the negotiation breakdown probability caused by external intervention approaches zero), LPs in an SSPE will converge to offer the same allocation vector in their strategies. It can be verified that this allocation vector indeed serves as the solution to the Nash bargaining problem.

We wish to emphasize that, to the best of our knowledge, no existing study has provided a specific framework akin to ours for comprehending the decision-making process in DAOs, including what we study here for how a group of LPs determine an AMM algorithm design in an intermediary-free exchange. Our bargaining framework seems to be the first effort in the literature to rationalize the decentralized governance scheme in DAOs from a game theoretical perspective, bridging the traditional economic literature on bargaining games with the decentralised decision-making process in DAOs — a novel organizational structure that runs as "smart contracts" on the blockchain. We hope our approach can serve as a valuable tool or benchmark for future studies seeking to understand the crucial trade-off between decentralization and welfare (efficiency) within DAOs.

To conclude, we establish an economic microfoundation for the novel decision-making process for a decentralised-governed intermediary-free exchange *à la* DAOs in the practice. Our sequential bargaining framework effectively captures the decentralised governance feature of DAOs in which any new platform designs require the submission of some proposals and the validation of these proposals is contingent on obtaining sufficient votes from other LPs through timely voting. Leveraging this bargaining implementation framework, we find that the allocative efficiency achieved in the optimal AMM design can be implemented as an equilibrium among LPs, where their bargaining power is determined by their respective liquidity contributions to the exchange, adhering the "one token, one right" DAO principle.

6 Applications

The optimal AMM design result in Proposition 1 introduces two important applications: 1) a potential economic rationale for the wide-adopted constant product market maker designs on blockchain-based DEXs, and 2) the connection of our optimal AMM design to the efficient allocation frontier in portfolio choice theory.

6.1 Constant Product Market Makers

Most AMM designs on existing DEXs follow the constant product market makers (CPMM) functional design in which u_{AMM} is formed as

$$u_{AMM}(x, y) = x^w y^{1-w}, \quad w \in (0, 1).$$

For instance, Uniswap, the largest DEX by its market share, selects $w = \frac{1}{2}$. Another leading DEX platform Balancer chooses the parameter w to w and $1 - w$ proportions LP's wealth locked in the liquidity pool invested on token A and token B, respectively.

As mentioned earlier, AMM algorithms, including this specific CPMM design, are ad hoc: they have neither any precedent in traditional financial markets nor any economic rationale in the existing literature on DEXs. We, however, show below that the CPMM bonding curve design can result from the optimal AMM design in Proposition 1 under some simple yet intuitive economic environment.

To start, suppose LPs are single-minded agents and their preferences are of the following two types,

$$\text{type-1: } u_1(x, y) = x; \quad \text{type-2: } u_2(x, y) = y.$$

The market composition of these LPs in the DEX is assumed to be n_1 quantities of type-1 and n_2 quantities of LPs of type-2. Furthermore, LPs have made an identical contribution to the liquidity pool:

$$b_1 = ... = b_i = ...b_n = b > 0,$$

where $n = n_1 + n_2$ is the total number of LPs. Then for any given price of token A against token B, say $p > 0$, we can compute the respective reservation utilities of a type-1 LP and a type-2 LP as follows:

$$\pi_1 = \frac{b}{p} \quad \text{and} \quad \pi_2 = b. \tag{11}$$

This defines the reservation utilities of type-1 and type-2 LPs if they manage their funds independently and trade with LDs separately.

Instead of managing wealth independently, LPs now have contributed their wealth into a single liquidity pool together to attract the trading needs of external LDs, with the pricing managed by an optimal AMM algorithm in the spirit of our social planner. Having said that, the social planner would allocate $\frac{n_1}{n_1+n_2}$ fractional funds contained in the liquidity pool to hold token A, as LPs make identical liquidity contributions and n_1 LPs out of the total $n = n_1 + n_2$ LPs are of type-1. Note that this investment strategy is independent of the market price $p > 0$ as LPs are single-minded in this setup.

Therefore, we conjecture and verify below that the optimal AMM algorithm acting as a social planner would exhibit a Cobb-Douglas preference u_{AMM} in the following manner with a parameter λ to be determined:

$$u_{AMM}(x, y) = x^{\lambda} y^{1-\lambda}.$$

By integrating the economic interests as well as the liquidity contribution of both types of LPs into social planners' decision-making, we further conjecture that

$$\lambda = \frac{\sum_{k=1}^{n_1} b_k}{\sum_{i=1}^{n_1+n_2} b_i} = \frac{n_1 b}{n_1 b + n_2 b} = \frac{n_1}{n_1 + n_2}.$$

Hence, λ reflects the fractional funds invested by the AMM algorithm on token A.

Using Proposition 1, we can verify the above conjecture by solving the following optimization problem:

$$\begin{aligned} \max_{x,y} \quad & u_{AMM}(x, y) = x^{\frac{n_1}{n_1+n_2}} y^{\frac{n_2}{n_1+n_2}} \\ \textit{subject to} \quad & px + y \leq \sum_{i=1}^{n_1+n_2} b = (n_1 + n_2)b. \end{aligned}$$

Consequently, this problem admits a unique solution as follows:

$$x^{\star} = n_1 \times \frac{b}{p} = n_1 \times \pi_1 \quad and \quad y^{\star} = n_2 \times b = n_2 \times \pi_2$$

This result is consistent with the exact maximal utilities earned by LPs if they construct their most preferred bundle of tokens independently, as specified in (11).

Thus the CPMM-based AMM trading mechanism on DEXs, to some extent, can be explained as a weighted "average" over the most preferred tokens portfolio owned by LPs. Additionally, our Proposition 1 shows that there exists an economically well-defined way to compute this "weighted average": understanding the AMM algorithm as the social planner who cares about Nash social welfare among the groups of heterogeneous LPs. Our study here, therefore, provides the first economic microfoundation for the ad hoc CPMM-based trading mechanism designs in the literature on DEXs.

6.2 Efficient Portfolio Frontier

In this subsection, we present an alternative interpretation of the ad hoc AMM-based trading mechanism on DEXs by discussing its connection with the efficient frontier in modern portfolio theory.

Set of admissible trades To start, we find that the participation constraint of each LP in our social planner problem naturally defines a set of admissible trades associated with each LP i, which we denote as $\hat{S}_i(x_i, y_i)$ and are given by

$$\hat{S}_i(x_i, y_i) = \Big\{(q_i, \tau_i(q_i)) : u_i(x_i - q_i, y_i + \tau_i(q_i)) \geq \pi_i(x_i, y_i)\Big\}. \tag{12}$$

We now turn to the characterization of the set of admissible trades supported by a group of heterogeneous LPs on a DEX. This step is natural given that DEX is a liquidity crowd-sourced platform, collectively owned and managed by a group of LP members.

Connection to our social planner problem In the language of this set of admissible trades, we see that for each trade $(q, \tau(q))$, it is admissible only if there exists at least one decomposition $\{q_i, \tau_i(q_i)\}_i$ such that

$$\sum_i (q_i, \tau_i(q_i)) = (q, \tau(q)) \quad and \quad (q_i, \tau_i(q_i)) \in \hat{S}_i(x_i, y_i)$$

As may be expected, this decomposition is tightly linked with our earlier social planner problem, where a social planner aims to find an optimal allocation $\{q_i, \tau_i\}_i$ to minimise the trading cost of LDs subject to LPs' participation constraints.

To see this connection clear, we first recall that the optimal pricing schedule τ in the social planner problem replicates a corresponding optimal AMM algorithm u_{AMM} due to the one-to-one correspondence between u_{AMM} and τ as below,

$$u_{AMM}(x - q, y + \tau(q)) = u_{AMM}(x, y).$$

Then if we interpret the above relation in our language of admissible trade set, we immediately notice that the following set of admissible trades $\hat{S}_{AMM}(x, y)$ has its boundary denoted as $\partial\hat{S}_{AMM}$ that defines our desired optimal pricing schedule τ,

$$\hat{S}_{AMM}(x, y) = \{(q, \tau(q)) : u_{AMM}(x - q, y + \tau(q)) \geq u_{AMM}(x, y)\}.$$

In summary, the discussion above shows that the optimal AMM algorithm u_{AMM} can be characterised via either the set $\hat{S}_{AMM}$ in the language of the set of admissible trades or the optimal pricing schedule τ in the context of the social planner problem. In other words, characterising the set of admissible trades $\hat{S}_{AMM}$ first and then deriving the optimal pricing schedule τ through the boundary $\partial\hat{S}_{AMM}$ can be seen as an alternative approach to studying the optimal AMM design u_{AMM} for the DEX, as compared to the earlier analysis in the social planner problem where we derive the optimal pricing schedule τ first and then define its associated optimal AMM design u_{AMM}.

A candidate set of admissible traders for the DEX We now turn to find a "well-defined" $\hat{S}_{AMM}$ with its boundary $\partial\hat{S}_{AMM}$ defines the desired optimal pricing schedule τ we have found in our social planner problem.

Given the set of admissible trades definition for each LP in (12) and the fact that DEX is collectively owned by all LPs, we can simply aggregate LPs' sets of admissible traders and have a straightforward yet economically meaningful candidate set as follows:

$$S(x, y) := \hat{S}_1(x_1, y_1) + \hat{S}_2(x_2, y_2) + ... + \hat{S}_n(x_n, y_n). \tag{13}$$

This sum over sets of admissible trades is in the sense of a so-called Minkowski sum. Technically, a Minkowski sum of two sets A_1 and A_2 is defined by:

$$A_1 + A_2 = \{(x_1 + x_2, y_1 + y_2) : (x_1, y_1) \in A_1 \quad \text{and} \quad (x_2, y_2) \in A_2\}.$$

For an economic illustration of this Minkowski sum, suppose that two LPs collectively own a DEX and their sets of admissible trades are given by

$$\hat{S}_1 = \{(0, 0), (1, 2)\} \ \textit{and} \ \hat{S}_2 = \{(0, 0), (1, 3), (2, 7)\},$$

respectively. We can then compute their Minkowski sum and get

$$S := \hat{S}_1 + \hat{S}_2 = \{(0, 0), (1, 2), (1, 3), (2, 5), (2, 7), (3, 9)\}.$$

This set S contains all possible trades that could happen at this DEX. Taking the element $(2, 5) \in S$ as an example, this trade is admissible at this DEX due to its representation $(1, 2) + (1, 3)$, which means that LP1 and LP2 are required to absorb trades $(1, 2)$ and $(1, 3)$, respectively. This is admissible given that LP1 and LP2 collectively manage the DEX and $(1, 2) \in \hat{S}_1$ and $(1, 3) \in \hat{S}_2$.

We find that $\hat{S}_1(p, b_1) \cup \hat{S}_2(p, b_2) = \{(0, 0), (1, 2), (1, 3), (2, 7) \subsetneq S := \hat{S}_1(p, b_1) + \hat{S}_2(p, b_2)\}$. This implies that a larger set of admissible trades is obtained on this DEX if they can allocate the LD's trade between them, as opposed to trades independently on the DEX platform. Since trading with LDs separately and independently yields the set of admissible trades given by $\hat{S}_1(p, b_1) \cup \hat{S}_2(p, b_2)$, a subset of the Minkowski sum $S := \hat{S}_1 + \hat{S}_2$, where the trade arising from LDs can be allocated between LP 1 and LP 2 accordingly as long as the participation constraints of LPs are satisfied[15].

However, the Minkowski sum over LPs' sets of admissible trades would generate some unreachable points such as $(2, 7)$—an inefficient capital allocation in the context of our social planner problem. We call it unreachable as the Minkowski sum contains a point $(2, 5)$ strictly preferred by LDs. Recall that each element $(q, \tau(q))$ in the set of admissible trades represents that the LD can trade $\tau(q)$ quantities of token B for q quantities of token A. Thus, from the perspective of LD, the admissible trade $(2, 7)$ is strictly dominated by $(2, 5)$, as choosing the latter allows her to pay less while trading out an identical 2 units of token A from the DEX.

Eliminating these unreachable trades in our candidate Minkowski sum $S(x, y)$ immediately defines the efficient frontier and we claim that this efficient frontier is indeed the boundary of Minkowski sum $S(x, y)$, say $\partial S(x, y)$. To understand this result, one should note that for any element $(q, \tau(q)) \in \partial S(x, y)$, it implies that there is no other admissible trade $(q, \tau'(q)) \in S(x, y)$ such that the LD can trade out q quantities of token A but with a strictly smaller transfer in token B, say $\tau'(q) < \tau(q)$. Otherwise, it violates the definition of $\partial S(x, y)$—the boundary of $S(x, y)$.

For a graphical illustration of our efficient frontier. Suppose there are two LPs on the DEX and their liquidity contributions to the DEX are given by β_1 and $\beta_2 = 1 - \beta_1$, respectively. Then the (normalised) optimal AMM function chosen by these two LPs would be a bonding curve $u_{AMM}(x, y) = 1$ (red-dashed curve) lies between the bonding curve $u_1(x, y) = 1$ (orange curve) and the bonding curve $u_2(x, y) = 1$ (blue curve).

Compared to selecting any other (admissible trades) points in the interior area covered by the red dashed curve, there always exists a dominant (admissible trade) point to be

[15] Indeed, size of this Minkowski sum would grow dramatically once any of $\{S_i(x_i, y_i)\}_i$ is large.

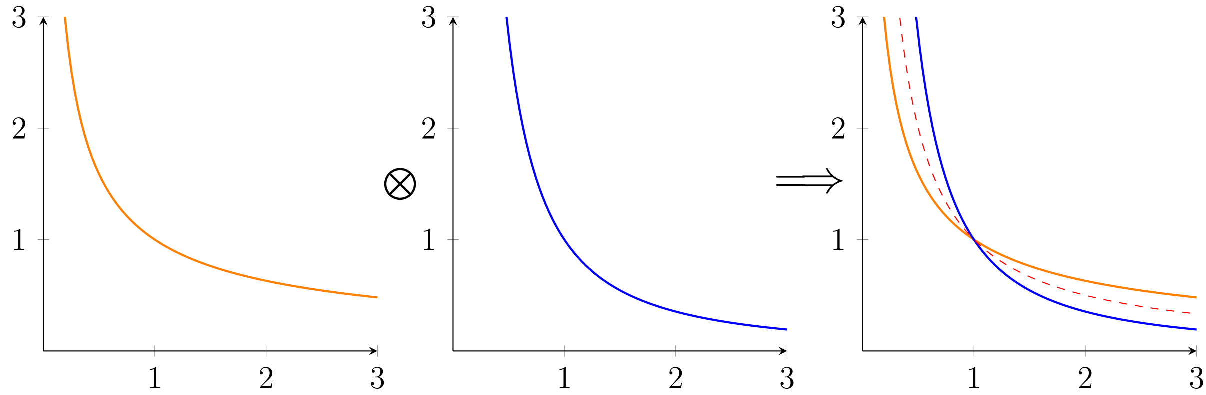


Figure 1: A equally weighted geometric mean of bonding curves where $u_1(x, y) = x^{\frac{2}{5}}y^{\frac{3}{5}}$, $u_2(x, y) = x^{\frac{3}{5}}y^{\frac{2}{5}}$ and $\beta_1 = \beta_2 = \frac{1}{2}$.

selected on the red dashed curve, where LD can trade out an identical quantity of token A but with a smaller token B transfer. Thus this red-dashed curve represents the efficient frontier. This efficient frontier uniquely pins down a pricing schedule τ, which is indeed the one we have characterised in our social planner problem.

7 Extension: truthfully reporting preferences

In this section, we address one major concern regarding the implementation result we derived in the last section.

Specifically, our implementation framework relies on achieving equilibrium through a Nash bargaining game where the preferences of LPs are public information to the mechanism designer. To see this, recall that optimal AMM follows a weighted geometric mean over LPs' preferences. Although the liquidity contribution information about the number of cryptos staked by LPs is publicly observable to the AMM algorithm, each LP's preference is privately observed. Moreover, LPs' preference is assumed to be homothetic in this paper, a large set of functions, whereby almost impossible for mechanism designers to infer and elicit LPs' preferences. Given that, a straightforward, practical approach to acquiring this preference information is to ask LPs to report it. Then a natural, important emerges: How can the AMM mechanism incentivize LPs to report their utility preferences truthfully?

To address this question, we extend the original implementation by augmenting a (algorithmic) component where LPs have to report their (true or false) preferences while staking assets into the liquidity pool. As a result, we show that truthfully reporting preference is a dominant strategy for every LP in this extended implementation. We want to emphasise that this preference reporting setting is not restrictive, since the leading DEX platform, Uniswap V4, has planned to introduce a large set of flexibility and customization options to be selected by their platform participants including customising most preferred AMM algorithm, a detailed description can be found from the white paper for Uniswap V4.

7.1 A typical VCG mechanism for DEX platforms

Incentivising agents to truthfully report their preferences brings to mind the classical Vickrey–Clarke–Groves (VCG) mechanism, introduced by Vickrey (1961), Clarke (1971), and Groves (1973). One key feature of the VCG mechanism is that agents find truthfully reporting valuations for possible outcomes to be a dominant strategy, where the sum of agents' utilities is maximised in equilibrium. In contrast to aiming for maximum utilitarian welfare (utilitarian social welfare), the objective of our implementation here is to maximise the Nash social welfare (a weighted sum of agents' utilities). Our extended implementation has to highlight this distinction under the context of intermediary-free exchanges.

Before proceeding with the main results, it is helpful to provide a summary of what a typical VCG mechanism would look like.

VCG mechanism for utilitarian social welfare. Let $X = \{(x_i, y_i)_i | \sum_i (x_i, y_i) = (x_0, y_0)\}$ denote the set of feasible allocation outcomes over the post-trade liquidity pool (x_0, y_0). As usual, let $(\beta_i)_i$, where $\sum_i \beta_i = 1$, represent the liquidity ownership of LPs within the pool. Then the valuation of each LP over any possible pool allocation outcome can be captured by a preference function:

$$u_i : X \to \mathbb{R}_+, \quad \text{where} \quad u_i(x) = u_i(x_i, y_i) \quad \text{and} \quad x = (x_i, y_i)_i \in X.$$

In a typical VCG mechanism setup, it is assumed that agents have quasilinear utility. For example, if the outcome allocation is $x \in X$ and LP i can receive a corresponding payment $p_i(x)$ (either positive or negative) under this outcome, then her eventual utility payoff will be:

$$\hat{u}_i(x) = u_i(x) + p_i(x).$$

Goal of VCG mechanism. The goal of the VCG mechanism is to select the outcome $x^\star$ such that the utilitarian social welfare of LPs is maximised. That is,

$$x^\star := x^\star\Big(\{u_i\}_i\Big) \in \underset{x \in X}{argmax} \ \sum_i \beta_i u_i(x).$$

A typical VCG mechanism. Following the VCG mechanism literature, we construct a standardized VCG mechanism in the following way:

1. The mechanism asks all LPs within the liquidity pool to report their utility preferences over each possible bundle of assets, say, $u_i(x)$ for $i = 1, ..., I$ and $x \in X$.
2. According to the utility preferences reported by LPs, the mechanism computes the $x^\star\Big(\{u_i\}_i\Big) \in \underset{x \in X}{argmax} \ \sum_i \beta_i u_i(x)$.
3. The mechanism pays LP i a weighted payment p_i that equals the sum of weighted utilities of all other LP j. That is,

$$p_i = \frac{1}{\beta_i} \sum_{j \neq i} \beta_j u_j(x^\star). \tag{14}$$

Examining step 3 in the above mechanism, one may notice that the interest of each LP

i aligns exactly with the interest of this mechanism designer, i.e., the maximum of the weighted sum of utilities of all LPs. Since each LP i in this mechanism eventually receives the utility:

$$\hat{u}_i := u_i(x^\star) + p_i = u_i(x^\star) + \frac{1}{\beta_i}\sum_{j\neq i}\beta_j u_j(x^\star),$$

where $u_i(x^\star)$ is the utility she obtains from the allocation defined in $x^\star$ and p_i is the total value/utilities she obtains from step 3 in the mechanism. Multiplying the above member i's utility by β_i yields that

$$\beta_i\hat{u}_i = \beta_i u_i(x^\star) + \beta_i p_i = \beta_i u_i(x^\star) + \sum_{j\neq i}\beta_j u_j(x^\star) = \sum_{k=1}^{n}\beta_i u_i(x^\star),$$

where the right-hand side is exactly the goal of this mechanism. Hence, LPs in this mechanism are incentivized to play the strategy that helps the society/mechanism designer achieve its utilitarian goal. Accordingly, LPs are incentivized to truthfully report their preferences.

7.2 A DEX-type-VCG mechanism

As emphasized earlier in Proposition 1, the social planner in our intermediary-free exchange has its welfare function structured as a Nash social welfare, which is a weighted product of LPs' utilities, instead of the weighted sum case in the VCG mechanism. Therefore, we have to modify the above standardised VCG mechanism solution to accommodate this change.

Surprisingly and intuitively, simply following the same three steps in the classical VCG mechanism but changing the sum operational there to a multiply operational can immediately implement the Nash social welfare. Let us name this new mechanism a DEX-type-VCG mechanism and specify its structure as below.

Goal of DEX-type-VCG mechanism First of all, let us denote X the set of possible allocation outcomes and $u_i(x)$ the valuation/utility of member i for each allocation outcome $x \in X$ in the same manner as above. However, the goal of our DEX-type-VCG mechanism here changes to select the outcome $x^\star$ that maximises the Nash social welfare of the society, say, the weighted product of utilities of LPs

$$x^\star\Big(\{u_i\}_i\Big) \in \underset{x \in X}{argmax}\ \Pi_i u_i(x)^{\beta_i}.$$

DEX-type-VCG mechanism for Nash social welfare The second difference between our DEX-type-VCG mechanism to classical VCG mechanisms lies in that given a final allocation output $x^\star = (x_i^\star, y_i^\star)_i$, this DEX-type-VCG mechanism only allocates LP i a fraction $f_i(x^\star)$ of her bundle $(x_i^\star, y_i^\star)$. Specifically, given the final allocation $x^\star$, LP i's eventual utility in DEX-type-VCG mechanism is given by

$$\hat{u}_i(x^\star) = f_i(x^\star) u_i(x_i^\star, y_i^\star).$$

Next, we need to specify how to construct a suitable $f_i(\cdot)$, and why our DEX-type-VCG mechanism motivates LPs to truthfully report their preferences, thereby achieving a Nash social welfare.

The DEX-type-VCG mechanism. Analogously, we construct the mechanism and show its solution in three steps.

1'. The mechanism asks LPs grouped in the liquidity pool to report their utility preferences over each possible bundle of assets, say, $u_i(x)$ for $i = 1, ..., I$ and $x \in X$.

2'. According to the utility preferences reported from LPs, the mechanism computes the $x^\star\Big(\{u_i\}_i\Big) \in \underset{x \in X}{argmax}\ \Pi_i u_i(x)^{\beta_i}$.

3'. The mechanism allocates each LP i a weighted fractional $(x_i^\star, y_i^\star)$, where the weight

f_i is given by

$$f_i = \left(\Pi_{j \neq i} u_j(x^\star)^{\beta_j}\right)^{\frac{1}{\beta_i}}. \tag{15}$$

As a result, we obtain the following proposition.

Proposition 3 (truthfully reporting) *Given the DEX-type-VCG mechanism as specified above,*

(I.) each LP $i \in I$ is incentivized to truthfully report her preference u_i as reporting true preference in step 1' is a dominant strategy.

(II.) This mechanism implements its goal, say, a weighted Nash social welfare among LPs for a weight vector $(\beta_i)_i$.

In our DEX-type VCG mechanism, each LP finds that truthfully reporting her preference is a dominant strategy. This property enables the augmentation of the benchmark implementation by mandating that LPs disclose their preferences when staking assets into the liquidity pool. Put differently, our extended implementation framework based on this DEX-type VCG mechanism effectively addresses the concern of privately known preferences in the original implementation result.

8 Conclusion

In this paper, we identify that the AMM designs currently used by intermediary-free exchanges, particularly blockchain-based DEXs, fall short in terms of trading efficiency, particularly in minimizing the trading costs for LDs while ensuring LPs' participation in the exchange. By examining a social planner's optimization problem, we derive the conditions necessary for an optimal trading allocation on an intermediary-free exchange. Our findings reveal the importance of incorporating LP heterogeneity, both in liquidity contributions and in individual preferences, when designing AMM algorithms for intermediary-free exchanges.

Moreover, we show that the algorithmic structure of our optimal AMM design for intermediary-free exchanges is given by a weighted geometric mean of LP preferences, with each LP's weight proportionate to her liquidity contribution to the exchange. Finally, we propose a decentralized governance scheme among LPs based on a Nash bargaining framework, which implements the optimal AMM design as an equilibrium bargaining outcome.

Future research could explore several promising extensions. For example, how might the optimal AMM design adjust to scenarios with asymmetric information about asset fundamentals? Another interesting question is how the implementation framework may evolve if a pivotal or dominant LP emerges within the LP community.

9 Appendix A: Inefficiency in existing AMMs

In this section, we discuss the difference between our optimal AMM trading mechanism derived in the main paper and the existing AMMs in practice.

DEX follows the typical DAO feature, ensuring that each LP can exercise some governance control over the liquidity pool entirely determined by her liquidity ownership to the pool. Specifically, suppose each LP $i \in \{1, ..., n\}$ stakes a bundle of tokens A and B (x_i, y_i) into the liquidity pool. According to the 'one token, one right' principle (i.e., the proportional allocation principle) in DAOs, the respective fractional ownership LP i has over this liquidity pool is then calculated as follows:

$$\beta_i := \frac{px_i + y_i}{\sum_{j=1}^{n}(px_j + y_j)},$$

where $p > 0$ is the commonly known value of crypto A against crypto B[16]. Trivially, $\sum_i \beta_i = 1$.

Ownership vector $\{\beta_i\}_i$ plays essential roles in the existing DEX ecosystem with automated market making. For instance,

1. each LP i receives a β_i fraction of the trading fees paid by LDs;
2. LP i has to absorb the fraction $\beta_i q$ and to receive a payment of $\beta_i T(q)$ in return when the feasible trade made by the LD at the DEX is $(q, T(q))$;
3. denoting $\mathcal{R} = (x, y)$ as the state of the token reserve in the liquidity pool, the maximum amounts of tokens A and B can be withdrawn by the LP i from the pool are $\beta_i x$ and $\beta_i y$, respectively.

Bonding curve design results in the DEX pricing as well as the trading fees paid by LDs being a function of the market depth. Thus only the total number of tokens in the

[16] Having the intrinsic value notion p is convenient but may not be the best language here. For intuition, we can follow the literature on DEXs and CEXs and interpret p as the price of crypto A against crypto B in the CEX, whose pricing is typically assumed to be more efficient. Loosely speaking, p is the marginal 'no-arbitrage' price of token A against token B.

liquidity pool matters for the fee payment on the DEX rather than the distribution of LPs' preference in the liquidity pool. This implies adopting the proportional allocation principle in distributing the trading fees paid by DEX traders among LPs, say the owners of the platform, is plausible: each LP i holding a fraction β_i of economic rights in the liquidity pool should receive an exact β_i fraction of the fees paid by LDs.

However, extending this proportional allocation principle in matching LDs and LPs at the DEX (i.e., point 2 above) and in withdrawing liquidity from the pools (i.e., point 3 above) could be suboptimal, and therefore generate inefficiency, particularly when LPs exhibit heterogeneity in great extents.

9.1 Trading allocative inefficiency in existing AMMs

In stark contrast to market makers in traditional financial markets, who engage in strategic competition to provide liquidity, LPs on DEX platforms are passive. LPs must adhere to the predetermined AMM algorithm when staking tokens into the pool. The AMM algorithm, designed for algorithmic simplicity, relies on two main components: a bonding curve and a proportional allocation rule. The former component designs that DEX pricing becomes a function with respect to the aggregated number of tokens in the liquidity pool, independent of the specific liquidity contribution made by each LP individual, while the latter component mechanically allocates the trading between LPs according to their liquidity ownership in the pool. Despite incorporating the asymmetric liquidity contribution factor, the trading allocation process due to the AMM nullifies all other dimensional heterogeneities among LPs. In turn, as we will show soon, it gives rise to trading allocative inefficiency on the DEX in matching LDs and LPs. Heuristically speaking, by mechanically pooling LPs' preferences, AMM at DEX platforms indeed trades off its allocative efficiency for algorithmic simplicity.

To illustrate the trading allocation inefficiency produced by AMM algorithm in the DEX, let us suppose that the LD submit a trade $(q, T(q))$ meeting the bonding curve design:

$$u_{AMM}(x-q, y+T(q)) = u_{AMM}(x, y). \tag{16}$$

Consequently, the AMM algorithm then automatically proceeds with this trading against the liquidity pool. During this process and with the proportional allocation rule in place, AMM forces the wallet of LP i in the liquidity pool to absorb a fraction $\beta_i q$ in exchange for a payment of $\beta_i T(q)$. Here, as before, we let $\{\beta_i\}$ the liquidity ownership of LPs in this liquidity pool.

Now, let us denote by $\pi_i(x_i, y_i)$ the reservation utility of LP i, which she would obtain if did not participate in the DEX but instead consumed the bundle of tokens (x_i, y_i) directly. With the proportional allocation design in place in AMM, we immediately derive the participation constraint of LPs in the DEX given by:

$$u_i(x_i - \beta_i q, y_i + \beta_i T(q)) \geq \pi_i(x_i, y_i). \tag{17}$$

Upon inspection of (17), we notice that this system of participation constraints above explicitly depends on the profile of LPs' preferences $\{u_i\}_i$. Moreover, such a key observation implies that the following statement (i.e., a necessary condition) has to be satisfied if the AMM allows the allocative efficiency at the DEX platform:

$$u_{AMM}(x-q, y+T(q)) = u_{AMM}(x, y) \Longrightarrow u_i(x_i - \beta_i q, y_i + \beta_i T(q)) \geq \pi_i(x_i, y_i) \ \ \forall i.$$

Trivially, the degenerate case where $u_i \equiv u_{AMM}$ immediately confirms the validity of the above statement. In this case, LPs have identical preferences, and the implemented bonding curve design in the AMM precisely aligns with that preference. As for the general cases where LPs exhibit heterogeneity in preference, we can prove later in lemma 1 that the above statement never holds at the DEX. Before that, we require a mild assumption on the preference of LPs for model tractability.

Lemma A-1 (trade allocative inefficiency in AMMs). *Given the proportional allocation rule designed in the AMM, there does not exist a bonding curve u_{AMM} satisfying*

$$u_{AMM}(x - q, y + T(q)) = u_{AMM}(x, y) \Longrightarrow u_i(x_i - \beta_i q, y_i + \beta_i T(q)) \geq \pi_i(x_i, y_i) \ \forall i, \quad (18)$$

if there exist at least two heterogeneous LPs in the DEX.

The detailed proof for this lemma is provided in the Appendix. There, we demonstrate that given the absolute fairness consideration in the AMM design (i.e., the proportional allocation principle), any bonding curve that ensures trading allocative efficiency would generally violate the participation constraints of some LPs. The exception to this is when LPs are homogeneous in their preferences.

Based on our Lemma 1, we document one fundamental trade-off in the current design of AMMs: prioritizing its algorithmic simplicity over the economic interests of LPs. Due to that, instead of separating LPs based on their preferences, AMM at the current DEX trading platforms only focuses on the liquidity ownership difference between LPs and mechanically pooling all other heterogeneities among them. As a result, this pooling effect yields the trading allocative inefficiency in the DEX trading platform while matching LPs and LDs.

Although the heterogeneity among LPs modelled in this paper primarily centres on utility preferences, other dimensions of heterogeneity may also contribute to the trade allocative inefficiency in DEXs. During the writing of this paper, the largest DEX platforms—Uniswap V3 and V4—have introduced more preference-associated options for LPs to choose from while staking liquidity into the pool. These platform changes including personalized price ranges and trading fees all fall under the category of LPs' preferences which indeed share a similar spirit as the utility preference modelling device in our paper. Hence, even though these platform changes account for the heterogeneity among LPs in an indirect, exogenous way, we may expect that they would ultimately help the AMM move closer to achieving allocative efficiency. In sharp contrast to these changes in practice, notably, our paper models the heterogeneity among LPs in their utility preference straightforwardly.

9.2 Liquidity withdrawal inefficiency in existing AMMs

Having characterized the AMM allocative inefficiency in matching LPs and LDs, we now turn to another source of inefficiency in the current AMM design — liquidity withdrawal inefficiency. Similar to the trade allocation inefficiency case, we will demonstrate below, using a simple yet non-trivial example, that this new source of inefficiency arises from the fundamental trade-off inherent in current AMM mechanism practices: prioritizing algorithmic simplicity over the economic interests of LPs.

Example A-1. Consider a liquidity pool within a DEX exclusively owned by two LPs, each characterized by a single-minded preference for tokens A and B. Specifically, the preferences of LP1 and LP2 are represented by the following two utility functions, respectively:

$$u_1(x, y) = x, \quad u_2(x, y) = y.$$

Assume both LPs stake an identical amount of liquidity into the pool:

$$(x_1, y_1) = (2a, 2b) \quad \text{and} \quad (x_2, y_2) = (2a, 2b).$$

We now have the liquidity pool established by these two LPs and its initial state can be denoted as $\mathcal{R}_0 = (4a, 4b)$. The bonding curve designed in the AMM trading mechanism on this liquidity pool follows that of Uniswap V2, a bonding curve defined by the product formula:

$$u_{AMM}(x, y) = xy.$$

Let us assume that the state of the liquidity pool changes to $\mathcal{R}_1 = (2a, 8b)$ after some trading activities at the DEX[17]. Suppose now that both LP1 and LP2 decide to

[17]Given the bonding curve design $u_{AMM}(x, y) = xy$, the marginal price of token A against token B

withdraw their liquidities from the pool and discontinue the DEX platform. According to the proportional allocation principle in the design of AMM, both LPs are entitled to half liquidity ownership in the pool $\mathcal{R}_1$ given that they contributed equally in establishing the initial liquidity pool $\mathcal{R}_0$. With this said, we can see that both LPs receive:

$$\frac{1}{2}\mathcal{R}_1 = (a, 4b)\,,$$

which evenly split the liquidity pool. Such an allocation, however, does not align with the preferences of LP1 and LP2, who would prefer to receive only one type of tokens in the pool rather than a mix of them.

By taking the preferences of LPs into account, a quick inspection of the liquidity pool $\mathcal{R}_1$ immediately provides a strictly Pareto-dominated allocation compared to the aforementioned proportional allocation. That is: LP1 takes all of token A, while LP2 takes all of token B. Such an alternative allocation then results in the following utility payoffs for the LPs upon their withdrawal:

$$\widetilde{u}_1(2a, 0) = 2a > u_1(a, 4b) = a; \qquad \widetilde{u}_2(0, 8b) = 8b > u_2(a, 4b) = 4b,$$

where the terms on the right-hand side of these inequalities represent the respective utility payoffs received by LPs under the proportional allocation solution. Of course, even though the proportional allocation is unfavourable for both LPs, they could hold onto their preferred type of token and trade the other type on trading platforms for preferred

under state $\mathcal{R}_0$ is $\frac{b}{a}$. This marginal price changes to $\frac{4b}{a}$ in state $\mathcal{R}_1$. Therefore, this state change in the token reserves of the liquidity pool can be interpreted as a fundamental price innovation shock for token A, moving from $\frac{b}{a}$ to $\frac{4b}{a}$. In the presence of high-frequency traders (HFTs) who closely monitor pricing in the DEX market, any DEX mispricing due to such a shock presents an arbitrage opportunity. These HFTs will engage in arbitrage trading to exploit the price discrepancy, which will immediately adjust the marginal price of token A against token B on the DEX trading platform from its pre-shock level to the post-shock level.

The liquidity staked by LPs in the liquidity pool, therefore, faces adverse selection due to the presence of these arbitrage traders. Specifically, arbitrage trading exploits the price differences at the expense of the liquidity providers. As shown later in our example, the proportional allocation rule designed in the AMM further exacerbates this adverse selection cost. This happens because the rule forces LPs to withdraw their liquidity in a fixed proportion, disregarding the new market conditions and the specific preferences of the LPs.

ones. However, one should note that this process would incur additional trading costs and other sources of risk not modelled here.

The welfare loss incurred by LP1 and LP2 when they withdraw tokens from the liquidity pool as we showed in this paper complements the understanding of "impermanent loss" in the literature. The term "impermanent loss" refers to the situation where the utility payoff gained by LPs from staking tokens in the liquidity pool is lower than what they would have earned by simply holding or directly consuming the tokens. The conventional understanding of "impermanent loss" posits that the value loss on the staked tokens resulting from arbitrage is temporary and diminishes when the token price at the DEX returns to its initial value. However, Capponi and Jia (2021) argues that this widely accepted conception of "impermanent loss" does not fully capture LPs' opportunity costs of depositing cryptos in the pool. Our paper thereby shares a similar economic intuition as their paper. In sharp to other studies in the literature on DEXs, including Capponi and Jia (2021), where the proportional fair allocation rule is taken as given, our approach starts from the fundamental participation constraint of LPs, which therefore determines the efficient allocation at the DEX in the cleanest way.

Thus far, we have identified two sources of allocative inefficiency in current AMM designs: trade allocative inefficiency and liquidity withdrawal inefficiency, as demonstrated by our results in Example 1 and Lemma 1. These inefficiencies primarily arise from the intentional ad-hoc design in AMMs, which prioritises algorithmic simplicity over the underlying heterogeneity between LPs. This fundamental trade-off leads to an incompatibility between the economic interests of heterogeneous LPs and the proportional allocation rule in AMMs, which has to mechanically pool LPs. Given the decentralized nature of DEX governance, where all LPs are both owners and managers of the platform, we may want to insist that no LP should have the incentive to compromise their welfare for the sake of an algorithmic simplistic trading mechanism design at the DEX. With that said, let us set aside the AMM design in the current DEX practice and focus on the characterization of an optimal trading mechanism at a DEX in the following section, particularly for the DEX established by a group of LPs with heterogeneous preferences.

10 Appendix B: competition between DEX platforms

In our discussion thus far, we have focused on the competition among LPs within one specific DEX, constituting what we term intra-DEX competition. This perspective holds assuming that LDs always trade on one particular DEX. However, what if there exists platform competition from other DEXs, and how does this competition shape the behaviour of market participants?

The competition between DEXs, termed inter-DEX competition, has its economic importance and interests. In reality, we observe the existence of oligopolistic DEXs. They compete for liquidity provision business, resulting in a segmentation of trading activities across various trading exchanges. Exploring this inter-DEX competition may shed light on the strategic behaviours of LDs, the rationale behind LPs participating in multiple DEXs, and the effects on market segmentation. Therefore, this section models the inter-DEX competition by assuming the presence of multiple DEXs in the economy.

10.1 Model

To study the strategic behaviours of LD, as before, we represent the utility benefit a θ-type LD can derive from purchasing q shares of crypto A by $u(q;\theta)$. Having learned the private information θ and pricing schedules $\{T_i(q)\}_{i=1,2,..,I}$ posted by DEXs, this θ-type LD chooses an optimal trade vector $\{q_i\}_{i=1,2,...,I}$ by solving

$$\underset{\{q_i\}_{i=1,...,I}}{Max} \quad u(q,\theta) - \sum_{i=1}^{I} T_i(q_i)$$

where $q = \sum_{i=1}^{I} q_i$. The optimal trade vector will be a function of θ and the posted pricing schedules $\{T_i(\cdot)\}_{i=1,2,...,I}$. This optimization problem could be mathematically extremely complex. For tractability, we make the following assumption.

Assumption 3 (mean-variance structure) *We assume that $u(q,\theta)$ follows a mean-variance structure, say,*

$$u(q,\theta) = -\frac{\lambda}{2}(\theta - q)^2 - (-\frac{\lambda}{2}\theta^2) \tag{19}$$
$$= \lambda\theta q - \frac{\lambda}{2}q^2,$$

where the first term on the right-hand side represents LD's utility from trading against DEXs and the second term measures the reservation utility of LD.

The above preference form can be found in many papers on market microstructure such as Sannikov et al. (2016), Chen and Duffie (2021) and Rostek and Yoon (2021), among many others. One possible heuristic explanation for this preference form is that LD enters the market with a positive level of inventory in the risky crypto asset A, say a privately known θ. λ measures her risk capacity. Any retaining post-trade inventory in risky crypto A incurs a quadratic holding cost to LD. Therefore, a privately observed θ reflects LD's trading needs[18].

The game and its timeline. The inter-DEX competition game has its extensive form outlined as follows:

0. At $t = 0$, we assume that there exist $J \geq 2$ DEXs in the market. For simplicity, we let DEXs be symmetrical in the sense that they have an identical liquidity pool.

1. In the first period ($t = 1$), LPs arrive and simultaneously decide on which liquidity pools to participate in. They have the flexibility to choose one, multiple, all, or none of any liquidity pools to stake liquidity.

2. In the second period ($t = 2$), LPs within each DEX $j \in J$ engage in a decentralized decision-making process, the Nash bargaining framework introduced in the previous section, to determine which pricing schedule $T_j(\cdot)$ to implement.

[18] An alternative classic explanation for this mean-variance structured preference is that LD has CARA utility and the risky asset value follows Gaussian distribution, see this setup, for example, in Biais et al. (2000).

3. In the third period ($t = 3$), nature selects a $\theta-$type LD. This LD subsequently trades against DEXs by choosing an optimal bundle of trades $\{q_j\}_{j\in J}$ to maximize her net utility payoff.

4. Finally, LPs withdraw their cryptos from DEXs for consumption.

We will study the Nash pure strategy equilibrium in this game, provided that the design-making process made by each DEX at $t = 2$ follows an N-persons Nash bargaining game. At equilibrium, LPs make crypto staking decisions at $t = 1$ that are the best response to the strategies of the other LPs given the strategic behaviours of LD at $t = 3$.

10.2 The Equilibrium Analysis

Let us start our analysis via backwards induction. For a given set of pricing schedules $\{T_j(\cdot)\}_j$ posted by J DEX platforms, from the point of view of a $\theta-$type LD, she needs to decide how to allocate her trade among these DEXs by maximising her utility payoff. More specifically, LD's problem is to choose a vector of trades $\{q_j\}_{j=1}^J$ by solving the following optimization problem.

LD's problem:
$$\underset{\{q_j\}_{j=1}^J}{Max}\ u(q(\theta),\theta) - \sum_j T_j(q_j(\theta)) = \lambda\theta q - \frac{\lambda}{2}q^2 - \sum_j T_j(q_j(\theta))$$
$$\textit{subject to}\quad q_1(\theta) + q_2(\theta) + ... + q_J(\theta) = q(\theta), \tag{20}$$

where $q(\theta)$ represents the size of LD's trade, associated with a privately observed signal θ that arises from margin calls or hedging motivation. As pricing schedules posted by DEXs are convex[19], optimization problem (20) exhibits a unique optimal allocation for each $q(\theta)$. Moreover, given that θ is privately observed, from the mechanism designer's perspective, each DEX has to design a pricing schedule such that LD is willing to reveal

[19] To see the convexity of $T(q)$, we first note that for any bonding curve $u_{AMM}(x - q, y + T(q)) = k$, $T(q)$ is increasing in q as $u_{AMM}(x, y)$ is increasing in x and y. Second, taking the second derivative of $u_{AMM}(x - q, y + T(q)) = k$ in q immediately yields $T^{''} \geq 0$.

her true θ. Therefore, the incentive compatibility condition (IC) for LD requires that

$$\textbf{[IC condition:]} \quad \theta \in \underset{\hat{\theta}}{Argmax}\Bigg(\lambda\theta q(\hat{\theta}) - \frac{\lambda}{2}q(\hat{\theta})^2 - \sum_j T_j(q_j(\hat{\theta}))\Bigg). \tag{21}$$

To ease notation, we represent the corresponding information rent by $\pi(\theta)$:

$$\pi(\theta) = \underset{\{q_j\}_j, \sum_j q_j(\theta)=q(\theta)}{Max}\left(\lambda\theta q - \frac{\lambda}{2}q^2 - \sum_j T_j(q_j(\theta))\right).$$

Beyond the incentive compatibility condition, under oligopolistic screening competition between DEXs, DEX k also needs to ensure the participation constraint (PC) of LD holds for trading in DEX k:

$$\textbf{[PC condition:]} \quad \pi(\theta) \geq \pi_{-k}(\theta), \tag{22}$$

where $\pi_{-k}(\theta)$ represents the payoff LD obtained if she does not trade in $k-$th DEX but other DEXs instead. That is,

$$\pi_{-k}(\theta) := \underset{\{q_j\}_{j\neq k}: \sum_{j\neq k} q_j(\theta)=q(\theta)}{Max}\left(u(q_{-k}(\theta),\theta) - \sum_{j\neq k} T_j(q_j(\theta))\right).$$

Let us now turn our attention to the optimization problem faced by the group of LPs within DEX k, or equivalently representative k. Given the pricing schedules posted by other DEX competitors, which as usual denoted by $T_{-k} := \{T_1, ..., T_{k-1}, T_{k+1}, ...T_J\}$, the problem of DEX k is to design her best response strategy $T_k(\cdot; T_{-k})$ to maximise the following expected payoff:

$$\textbf{DEX k's Problem:} \quad \underset{T_k(\cdot)}{Max} \; B_k(T_1, ..., T_J) \tag{23}$$

$$:= \int_{\underline{\theta}}^{\overline{\theta}} \left\{\left[u^k_{AMM}\Big(\bar{x} - q_k(\theta), \bar{y} + T_k(q_k(\theta))\Big) - u^k_{AMM}(\bar{x}, \bar{y})\right] + \gamma T_k(q_k(\theta))\right\} dF(\theta),$$

where the first integral component is the post-trade utility of DEX k and the second term is the respective received trading fee for a given fee rate $\gamma \in (0, 1)$.

In general, the above problem yields a fixed-point argument condition with the variable involving pricing schedule functions, making it extremely complex. To make this problem solvable, we need one last assumption.

Assumption 4 (presence of arbitrageurs) *There exists a group of opportunistic traders in the market who monitor the DEXs closely and exploit the trading of LDs.*

Specifically, opportunistic traders can be viewed as high-frequency value arbitrageurs. These traders closely monitor DEXs, seizing any arbitrage opportunities arising from price movements around the fair value of cryptos. In the presence of opportunistic traders, each trade of size q requested by the LD is subsequently followed by a reverse trade of size $-q$ initiated by these opportunistic traders. This sequence happens because an LD's trade in one direction creates arbitrage opportunities for opportunistic traders to profit from trading in the opposite direction. As a result, the objective function for representative k changes to

$$\textbf{DEX k's Problem:} \quad \underset{T_k(\cdot)}{\text{Max}}\ B_k(T_k, T_{-k}) = \int_{\underline{\theta}}^{\overline{\theta}} 2\gamma T_k\Big(q_k(\theta) : T_{-k}\Big)\, dF(\theta), \tag{24}$$

where the term involving the utility increment in (23) disappears and there exists a multiplicative factor of 2 in front of the trading fee income, reflecting the fact that any trade made by an LD will be reversed by opportunistic traders in DEXs.

Inspecting the optimization problem faced by each DEX, we can denote the best response of DEX k to the strategies of her competing DEXs by $F_k(T_{-k})$. Then finding a Nash equilibrium in this oligopolistic inter-DEX competition game will correspond to the fixed points in the mapping $\{F_1, ..., F_J\}$. The computation can be greatly simplified by considering the following fact: Given the symmetric structure of the initial liquidity pools at $t = 0$, the set of strategies for each LP $t = 1$ will be either randomly choose a single pool to participate in or evenly distribute their cryptos across all initial pools. Both strategies have an equivalent effect in terms of the resulting aggregate liquidity and ownership structure within every DEX in equilibrium. Therefore, without loss of generality, we can consider the latter case for simplicity. Based on this, one can postulate (and verify later) the existence of a unique symmetric equilibrium: LPs within each DEX $j \in J$ collectively adopt a symmetric pricing schedule design $T_j := T^{\star}$. This result is formally stated in the following proposition.

Proposition 4 (Existence and Uniqueness). *Under assumption 4, there exists a unique equilibrium in this oligopolistic inter-DEX competition game. This equilibrium is symmetric in the sense that all DEXs design an identical pricing schedule. That is,* $T_1^{\star} = ... = T_J^{\star} \equiv T^{\star}$.

The proof of this proposition closely follows the roadmap to that of Biais et al. (2000). They analyze an oligopolistic screening game among n risk-neutral market-makers offering convex price schedules simultaneously and noncooperatively. They establish the existence of a unique symmetric equilibrium, demonstrating that the equilibrium pricing schedule does not restore *ex-ante* efficiency due to the adverse selection in a *common value* environment where market-makers are neither informed about traders' hedging needs nor the fair value of the trading asset. Our result here shares qualitative similarities but exhibits a key distinction since the adverse selection in our paper arises from the privately observed trading needs of the LD, a *private value environment*) only. Therefore, the equilibrium pricing schedule can yield an *ex-ante* efficient, say $u_{AMM}(\mathbf{x}-q, \mathbf{y}+T^{\star}(q)) = u_{AMM}(\mathbf{x}, \mathbf{y})$.

Additionally, instead of assuming risk-neutral market makers straightforwardly as in Biais et al. (2000), the utility preference u_{AMM} in this paper is more general, a weighted product of LPs' preferences. Although the objective function of LPs within each DEX turns out to be risk-neutral, see in (24), the fundamental goes to the presence of opportunistic traders in the market and the DAO structure of the DEX platform. Moreover, our equilibrium pricing schedule sells tokens at their marginal cost, no longer a constant as in Biais et al. (2000).

In conclusion, this section models an inter-DEX competition among symmetric DEXs, characterized by an oligopolistic competition reminiscent of Bertrand competition, where each DEX, in equilibrium, sells assets at its marginal cost. The key insight driving this outcome is that when her competitors are offering a break-even pricing schedule $T^{\star}(\cdot)$, the optimal pricing schedule can be offered by DEX k is the break-even pricing schedule $T^{\star}(\cdot)$. DEX k cannot increase her price without risking a loss of her market share. Interestingly, the marginal cost charged by each DEX for each unit of crypto A in this model departs from the constant pricing in traditional Bertrand competition. Instead, it takes the form of a weighted average of the marginal prices charged by individual LPs. This weighted pricing reflects the exact impact of diverse preferences as well as the asymmetric liquidity ownership of LPs on how to settle down an ex-ante mechanical pricing algorithm in the DEX.

11 Appendix C: Proofs

11.1 Proof of Lemma A-1

Proof. To start, suppose the bonding curve function utilised by the AMM is $u_{AMM}(\cdot,\cdot)$. Then the optimality of $u_{AMM}(\cdot,\cdot)$ in its trade allocative efficiency yields one following necessary condition as stated below:

$$u_{AMM}(x-q, y+\tau(q)) = u_{AMM}(x,y) \quad \Longrightarrow \quad u_i\left(x_i - \beta_i q, y_i + \beta_i \tau(q)\right) \geq \pi_i \;\; \forall i, \tag{25}$$

where $(x,y) = (\sum_i x_i, \sum_i y_i)$ and π_i is the reservation utility of LP i if she did not stake her tokens in the liquidity pool.

Let us prove this lemma by constructing a contradiction. Suppose that (25) holds for a general profile of preference $\{u_i\}_i$ and that all LPs stake an identical crypto bundle into the liquidity pool. This implies $(x_i, y_i) = (x_j, y_j)$ for any $i, j \in \{1, ..., n\}$. In other words,

$(x_i, y_i) = \frac{1}{n}(x, y)$ and LPs have identical liquidity ownership at the DEX, say $\beta_i = \beta_j = \frac{1}{n}$. Provided that the pricing schedule implied in the bonding curve design u_{AMM} is $\tau(\cdot)$, we then write the participation constraints of LPs in this DEX platform in the following way:

$$u_i(x_i, y_i) = u_i\Big(x_i - \beta_i q, y_i + \beta_i \tau(q)\Big) = \frac{1}{n} u_i\Big(x - q, y + \tau(q)\Big) \geq \pi_i, \tag{26}$$

where we apply the homotheticity of u_i and $\beta_i = \frac{1}{n}$ while deriving the last equality. Multiplying the left hand sides of (26) by a factor n and then rearranging its order yields that

$$u_i\Big(x - q, y + \tau(q)\Big) = n u_i(x_i, y_i) = u_i\Big(n x_i, n y_i\Big) = u_i(x, y) \quad \forall i, \tag{27}$$

where all equalities above hold because of the homotheticity of u_i and that $(x_i, y_i) = \frac{1}{n}(x, y)$.

Recall that bonding curve design requires that

$$u_{AMM}(x - q, y + \tau(q)) = u_{AMM}(x, y). \tag{28}$$

Taking all the results above together immediately leads to a contradiction. Notably, conditions (27) and (28) hold for any $x, y, q, T(q)$. However, the former condition (27) depends on u_i, whereas the latter condition (28) is independent of u_i. The only way to ensure their equivalence is if the degenerate case holds where $u_i \equiv u_{AMM}$. This contradicts our assumption that there exists at least one pair of LPs who are heterogeneous in their preferences. Proof completes. □

11.2 Proof of lemma 1

Proof. Substituting the market clearing condition back into the objective function of social planner, we immediately notice that the optimal mechanism candidate $\{q(\cdot), \tau(\cdot)\}$

or the allocation $\{q_i(\cdot), \tau_i(\cdot)\}_i$ has to minimise the cost of trading for any given trading quantity $q(\theta)$. That is,

$$\underset{\{\tau_i(\cdot)\}}{Min} \quad \int_{\underline{\theta}}^{\overline{\theta}} \sum_i \tau_i(\theta) dG(\theta)$$

subject to participation constraint of LPs. Solving this optimisation problem is essentially equivalent to finding the efficient allocation $\{\tau_i(\cdot)\}$ in which LT achieves the minimum trading cost (or maximum net trading payoff). Inspecting the participation constraint of LPs, we can claim that the optimal allocation corresponds to the case in which all participant constraints are binding. To illustrate, suppose for example that there exists at least one $i \in \{1, ..., I\}$ such that

$$\int_{\underline{\theta}}^{\overline{\theta}} u_i \left(x_i - q_i(\theta), y_i + \tau_i(\theta)\right) dG(\theta) > \pi_i,$$

Then the social planner could reduce transfer $\tau_i(\theta)$ by a small amount and turn this inequality to be equality. This would obtain a smaller trading cost for LD and produce a more efficient allocation. Therefore, any allocation other than the one that binds all participation constraints would be strictly dominated.

Therefore, at the optimum, we have

$$u_i \left(x_i - q_i(\theta), y_i + \gamma \tau_i(\theta)\right) = \pi_i, \quad \forall \theta \in [\underline{\theta}, \overline{\theta}] \quad and \quad i \in \{1, ..., I\},$$

where we get rid of the integration over θ as participation constraints of LPs are always binding for any given distribution function F. Using this fact we can have that the transfer $\tau_i(q_i(\theta))$ each LP i receives in the efficient allocation as follows,

$$\tau_i\Big(q_i(\theta); x_i, y_i, u_i\Big) \quad or\ simply \quad \tau_i(q_i).$$

Above, we use the condition that $\dot{q}(\theta) > 0$ to ensure the simplification over τ_i is well-defined. Having characterised the form of the pricing schedule for each LP i above, we can now compute the optimal pricing schedule $\tau(q)$ which maximises the net trading payoff of LDs:

$$\tau(q) \equiv \underset{\{q_i\}_i}{min}\left\{\sum_i \tau_i(q_i) : \sum_i q_i = q\right\}.$$

Extending the above analysis to the other side of the market where $q < 0$ is analogous. For conciseness, we only focus on one side of the market for which LD purchases crypto A, say $q > 0$.

□

11.3 Proof of Proposition 2

Proof. **Existence** Let us start the proof from the equilibrium existence. Suppose the expected allocation vector contained in the SSPE strategy of game $G(\rho, \beta)$ is $z = (z_1, z_2, ..., z_n)$. Then $z \in V$ due to that z is a convex combination of $z_1, z_2, .., z_n$ and the set of feasible utilities V is convex.

On the one hand, if member i is chosen to be the proposer at round 1, she can propose an allocation vector $x_i = (x_i^1, x_i^2, ..., x_i^n) \in V$ that will be accepted by others. If this is the case, she needs to propose the allocation vector by considering the optimization problem.

$$\underset{x_i=(x_i^1,x_i^2,...,x_i^n)\in V}{Max} x_i^i \ \textit{subject to} \ x_i^j \geq \rho z_j + (1-\rho)0 = \rho z_j \ \ \forall j \neq i.$$ [20]

It is easy to see that the set of constraints is bounded, closed, convex, and not empty. Therefore, we can denote $f_i^\star(\rho z_{-i})$ as the maximum value of x_i^i by solving the above optimization problem, where z_{-i} is defined as usual, say, $z = (z_i, z_{-i})$. On the other hand, rather than proposing the allocation vector that is accepted by others, remark that proposer i can propose an unacceptable proposal. In this case, her expected payoff will be ρz_i. Combining these two cases yields the expected payoff of member i in the SSPE as $\beta_i\ max\{f_i^\star(\rho z_{-i}), \rho z_i\} + (1-\beta_i)(\rho z_i)$. For each $z = (z_1, z_2, ..., z_n) \in V$, we can define a function $g_i^\rho(z)$ by

$$g_i^\rho(z) = \beta_i\ max\{f_i^\star(\rho z_{-i}), \rho z_i\} + (1-\beta_i)(\rho z_i),\ \ \forall i.$$

As a result, $g(z) := (g_i^\rho(z))_{i\in N}$ is a correspondence from V to V. By using facts that V is compact and convex and Brouwer's fixed point theorem, we immediately get that there exists a fixed point $z^\star(\rho) \in V$ such that $\forall i \in \{1, 2, ..., n\}$ we have $g_i^\rho(z^\star(\rho)) = z^\star(\rho)$. So, we complete the proof of existence part.

Equilibrium Strategy From the proof above, we can easily construct an SSPE strategy profile $\sigma^\star(\rho) = (\sigma_1^\star(\rho), \sigma_2^\star(\rho), ..., \sigma_n^\star(\rho))$ in the game $G(\rho, \beta)$ as follows, for every member $i \in N$,

I. if becomes the proposer, then proposes the allocation vector that solves the above optimization problem.

II. if becomes the responder, then accepts any proposal x_j^i if and only if $x_j^i \geq \rho z_j^\star$.

In an SSPE, no proposer in any round would have the incentive to propose an unacceptable allocation proposal as there exists a negotiation breakdown risk (time cost). Similarly, no responder has the incentive to reject a proposal if it offers her a payoff that equals her continuation value from rejecting such a proposal. Consequently, in every SSPE of $G(\rho, \beta)$, any selected proposer i in each round will propose $x_i^\star$ such that it solves

$$\underset{x_i=(x_i^1, x_i^2, ..., x_i^n)\in V}{Max} x_i^i\ \ subject\ to\ x_i^j \geq \rho z_j^\star\ \ \forall j \neq i.$$

This proposal $x_i^\star$ will be accepted by all other members.

Equilibrium Payoff in SSPE Armed with the observation described above, we immediately get that in any SSPE with payoff vector $z(\rho) = (z_1^\rho, ..., z_n(\rho))$, every member receives the payoff $f_i^\star(\rho z(\rho)_{-i})$ if she is the proposer, and gets $\rho z_i(\rho)$ if she is a responder.

Notice that the probability of each member i selected as the propose is β_i, and therefore, the expected payoff to each $i \in \{1, 2, ..., n\}$ in this SSPE with payoff vector $z(\rho) = (z_1^\rho, ..., z_n(\rho))$ satisfies that

$$z_i(\rho) = \beta_i f_i^\star(\rho z_{-i}(\rho)) + (1 - \beta_i)(\rho z_i(\rho)).$$

Therefore, we have that in any SSPE, the expected payoff $z^\star(\rho)$ is given by

$$z_i^\star(\rho) = \beta_i f_i^\star(\rho z_{-i}^\star(\rho)) + (1 - \beta_i)(\rho z_i^\star(\rho)) \quad \forall i \in \{1, 2, ..., n\}.$$

It implies that

$$f_i^\star(\rho z_{-i}^\star(\rho)) = \frac{1-\rho}{\beta_i} z_i^\star(\rho) + \rho z_i^\star(\rho).$$

As $\rho \to 1$, we immediately get

$$f_i^\star(z_{-i}^\star) = z_i^\star.$$

Denote by $x_i(\rho) = (\rho z_1^\star(\rho), ..., f_i^\star(z_{-i}^\star), ..., \rho z_n^\star(\rho))$ the payoff vector proposed by every member i who is selected as the propose in any SSPE of $G(\rho, \beta)$. Clearly, the above relation implies that

$$\lim_{\rho \to 1} x_i(\rho) = z^\star = \lim_{\rho \to 1} x_j(\rho). \tag{29}$$

That is, the proposals proposed by all members in any SSPE converge to the same $z^\star : (z_i^\star)_i$.

Nash Bargaining Solution Let us now establish the equivalence between the SSPE with $\rho \to 1$ and the Nash bargaining solution.

It is not hard to see that the set of feasible utilities V is closed, bounded, convex, smooth and nonlevel due to the assumption that utility preference functions $\{u_i\}_i$ are continuous, concave and differentiable. Therefore, there exists a continuous, concave and differential function F such that $F(x) = 0$ for any $x \in \partial V \cap \mathbb{R}^n_+$ and $F(x) \leq 0$ for any $x \in V^o \cap \mathbb{R}^n_+$, where V^o is the interior of V.

Any SSPE payoff vector $x_i(\rho)$ proposed by every member i in game $G(\rho, \beta)$ must belong to $\partial V \cap \mathbb{R}^n_+$. Otherwise, it would be not Pareto efficient and there will exist a Pareto-improved vector that increases all member's payoffs. So any member $j \neq i$ will reject this payoff allocation proposal $x_i(\rho)$, which is the desired contradiction. Consequently, for any two $i, j \in \{1, 2, ..., n\}$, it follows that $F(x_i(\rho)) = F(x_j(\rho)) = 0$, where $x_i(\rho)$ and $x_j(\rho)$ are the respective payoff vectors proposed by members i and j in an SSPE if they are selected as the proposer in round 1. By using the Taylor's Theorem, we see that there exists at least one $0 < t < 1$ such that

$$
\begin{aligned}
&0 = F(x_i(\rho)) - F(x_j(\rho)) = \sum_i F_i(tx_i(\rho) + (1-t)x_j(\rho))(x_i^k(\rho) - x_j^k(\rho)) \\
&= [f_i^\star(\rho z_{-i}^\star(\rho)) - \rho z_i^\star(\rho)]F_i(tx_i(\rho) + (1-t)x_j(\rho)) - [f_j^\star(\rho z_{-j}^\star(\rho)) - \rho z_j^\star(\rho)]F_j(tx_i(\rho) + (1-t)x_j(\rho)) \\
&= (1-\rho)\frac{z_i^\star(\rho)}{\beta_i}F_i(tx_i(\rho) + (1-t)x_j(\rho)) - (1-\rho)\frac{z_j^\star(\rho)}{\beta_j}F_j(tx_i(\rho) + (1-t)x_j(\rho)),
\end{aligned}
$$

where F_i is the partial derivative to the $k-th$ coordinate. We can multiply $\frac{1}{1-\rho}$ on both sides of the above equation and then take $\rho \to 1$. It yields that

$$\frac{z_i^\star}{\beta_i}F_i(z^\star) = \frac{z_j^\star}{\beta_i}F_j(z^\star) \tag{30}$$

for any $i, j \in \{1, 2, ..., n\}$, where we derive the above equality by relying on the fact in (29), say, for any k, $\underset{\rho\to 1}{lim}\ x_i(\rho) = z^\star$.

As the last step, let us derive the Kuhn-Tucker condition of the optimization problem for the Nash bargaining solution of (V, β). The computation is straightforward and it reads as

$$\frac{\beta_i}{z_i^\star}\Pi_i(z_i^\star)^{\beta_i} - \lambda F_i(z^\star) = 0, \quad \forall i \in \{1, ..., n\},$$
$$and \quad F(z^\star) = 0,$$

where λ is the respective Lagrange multiplier. Remark that we have proved a moment ago that any SSPE $z^\star = (z_1^\star, z_2^\star, ..., z_n^\star) \in V$ satisfies the conditions of $F(z^\star) = 0$ and (30), which indeed also fulfil the above Kuhn-Tucker condition of the optimization problem for the Nash bargaining solution of (V, β). So, as $\rho \to 1$, the respective SSPE $z^\star$ defines the solution of our original Nash bargaining problem. Proof completes. □

11.4 Proof of Proposition 3

Proof. We begin with the proof associated with part (II) by showing that steps 1'-3' here indeed implement a weighted Nash social welfare with the weights given by $\{\beta_i\}_i$.

The trick is in step 3'. Suppose that the final allocation $x^\star$ maximises the weighted Nash social welfare function, then the total utility payoff obtained by each LP i in this EX-type-VCG mechanism will be given by

$$\hat{u}_i(x^\star) = f_i(x^\star)u_i(x^\star) = \Big(\Pi_{j\neq i}u_j(x^\star)^{\beta_j}\Big)^{\frac{1}{\beta_i}}u_i(x^\star).$$

Taking a power of β_i on both sides yields that

$$\Big(\hat{u}_i(x^\star)\Big)^{\beta_i} = \Big[\Big(\Pi_{j\neq i}u_j(x^\star)^{\beta_j}\Big)^{\frac{1}{\beta_i}}u_i(x^\star)\Big]^{\beta_i} = \Pi_i u_i(x^\star)^{\beta_i}, \tag{31}$$

where the very left-hand side is the goal of our EX-type-VCG mechanism, say, the weighted Nash social welfare of the DEX society. Hence, each LP has its interests aligned with the mechanism designer or the social planner whose objective is to maximise the weighted Nash social welfare. This implies that the maximum of our weighted Nash social welfare would be attained if LPs truthfully reported their preferences.

To verify that reporting preference truthfully is a dominant strategy, let us assume that other LPs $j \in I, j \neq i$ report their preferences in step 1' as $\bar{u}_j$ (note that these preferences reported by LPs $j \neq i$ may differ from their true ones). Then the LP i has the option of either reporting her true preference or reporting a false one. Accordingly, denoted by $x^\star_T$ the final allocation generated by our DEX-type-VCG under the case where LP i truthfully reports her preference in step 2', and $x^\star_F$ otherwise.

Given that, step 3' returns a fraction $f_T(x^\star_T)$ in the case LP i truthfully reports, or a fraction $f_F(x^\star_F)$ otherwise.

To prove truthfully reporting her preference is a dominant strategy for every LP i, what we need to show is that

$$f_T(x^\star_T)u_i(x^\star_T) \geq f_F(x^\star_F)u_i(x^\star_F) \ \ \textit{or equivalently,} \ \ \Big(f_T(x^\star_T)u_i(x^\star_T)\Big)^{\beta_i} \geq \Big(f_F(x^\star_F)u_i(x^\star_F)\Big)^{\beta_i}.$$

Using the definition of f_T and f_F, what we need to prove is then the following relation,

$$u_i(x^\star_T)^{\beta_i}\Pi_{j\neq i}\bar{u}_j(x^\star_T)^{\beta_j} \geq u_i(x^\star_F)^{\beta_i}\Pi_{j\neq i}\bar{u}_j(x^\star_F)^{\beta_j}. \tag{32}$$

However, this inequality holds immediately, as $x^\star_T$ is defined as the maximiser to the weighted product of the correspondingly reported preferences of LPs in step 2'. That is,

$$x^\star_T \in \underset{x\in X}{argmax} \ \ u_i(x)^{\beta_i}\Pi^n_{j\neq i}\bar{u}_j(x)^{\beta_j}.$$

Remarkably, this condition holds even if any one of LPs $j \neq i$ reports a preference $\hat{u}_j$ that may differ from her true one u_j. Proof completes. □

References

Joseph Abadi and Markus Brunnermeier. Blockchain economics. Technical report, National Bureau of Economic Research, 2018.

Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. Uniswap v3 core. *Tech. rep., Uniswap, Tech. Rep.*, 2021.

Guillermo Angeris, Alex Evans, and Tarun Chitra. Replicating monotonic payoffs without oracles. *arXiv preprint arXiv:2111.13740*, 2021.

Guillermo Angeris, Tarun Chitra, Theo Diamandis, Alex Evans, and Kshitij Kulkarni. The geometry of constant function market makers. *arXiv preprint arXiv:2308.08066*, 2023.

Jun Aoyagi. Liquidity provision by automated market makers. *Available at SSRN 3674178*, 2020.

Jun Aoyagi and Yuki Ito. Competing daos. *Available at SSRN*, 2022.

Jun Aoyagi and Yuki Ito. Coexisting exchange platforms: Limit order books and automated market makers. *Journal of Political Economy Microeconomics*, 2024.

Andrea Barbon and Angelo Ranaldo. On the quality of cryptocurrency markets: Centralized versus decentralized exchanges. *arXiv preprint arXiv:2112.07386*, 2021.

Bruno Biais, David Martimort, and Jean-Charles Rochet. Competing mechanisms in a common value environment. *Econometrica*, 68(4):799–837, 2000.

Bruno Biais, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta. The blockchain folk theorem. *The Review of Financial Studies*, 32(5):1662–1715, 2019.

Maxim Bichuch and Zachary Feinstein. Axioms for automated market makers: A mathematical framework in fintech and decentralized finance. *arXiv preprint arXiv:2210.01227*, 2022.

Ken Binmore, Ariel Rubinstein, and Asher Wolinsky. The nash bargaining solution in economic modelling. *The RAND Journal of Economics*, pages 176–188, 1986.

Ken Binmore, Martin J Osborne, and Ariel Rubinstein. Noncooperative models of bargaining. *Handbook of game theory with economic applications*, 1:179–225, 1992.

Volker Britz, P Jean-Jacques Herings, and Arkadi Predtetchinski. Non-cooperative support for the asymmetric nash bargaining solution. *Journal of Economic Theory*, 145 (5):1951–1967, 2010.

Agostino Capponi and Ruizhe Jia. The adoption of blockchain-based decentralized exchanges. *arXiv preprint arXiv:2103.08842*, 2021.

Sylvain Carre and Franck Gabriel. Security and credit in proof-of-stake defi protocols. *Available at SSRN 4307207*, 2022.

Daniel Chen and Darrell Duffie. Market fragmentation. *American Economic Review*, 111 (7):2247–2274, 2021.

Long Chen, Lin William Cong, and Yizhou Xiao. A brief introduction to blockchain economics. In *Information for Efficient Decision Making: Big Data, Blockchain and Relevance*, pages 1–40. World Scientific, 2021.

Edward H Clarke. Multipart pricing of public goods. *Public choice*, pages 17–33, 1971.

Lin William Cong, Zhiguo He, and Jiasun Li. Decentralized mining in centralized pools. *The Review of Financial Studies*, 34(3):1191–1235, 2021.

Michele Fabi and Julien Prat. The economics of constant function market makers. Technical report, Mimeo, 2022.

Sean Foley, Peter O'Neill, and Tālis J Putniņš. A better market design? applying 'automated market makers' to traditional financial markets. *Applying 'Automated Market Makers' to Traditional Financial Markets (May 26, 2023)*, 2023.

William M Gorman. The structure of utility functions. *The Review of Economic Studies*, 35(4):367–390, 1968.

Mohak Goyal, Geoffrey Ramseyer, Ashish Goel, and David Mazières. Finding the right curve: Optimal design of constant function market makers. In *Proceedings of the 24th ACM Conference on Economics and Computation*, pages 783–812, 2023.

Theodore Groves. Incentives in teams. *Econometrica: Journal of the Econometric Society*, pages 617–631, 1973.

Jungsuk Han, Jongsub Lee, and Tao Li. Dao governance. *Available at SSRN 4346581*, 2023.

Sergiu Hart and Andreu Mas-Colell. Bargaining and value. *Econometrica: Journal of the Econometric Society*, pages 357–380, 1996.

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

Bengt Holmström and Roger B Myerson. Efficient and durable decision rules with incomplete information. *Econometrica: Journal of the Econometric Society*, pages 1799–1819, 1983.

Kose John, Leonid Kogan, and Fahad Saleh. Smart contracts and decentralized finance. *Available at SSRN*, 2022.

Mamoru Kaneko and Kenjiro Nakamura. The nash social welfare function. *Econometrica: Journal of the Econometric Society*, pages 423–435, 1979.

Tomohiko Kawamori. A noncooperative foundation of the asymmetric nash bargaining solution. *Journal of Mathematical Economics*, 52:12–15, 2014.

Alfred Lehar and Christine A Parlour. Decentralized exchanges. *Available at SSRN 3905316*, 2021.

Jacob D Leshno and Philipp Strack. Bitcoin: An axiomatic approach and an impossibility theorem. *American Economic Review: Insights*, 2(3):269–286, 2020.

Roger B Myerson. Optimal auction design. *Mathematics of operations research*, 6(1): 58–73, 1981.

John Nash. Two-person cooperative games. *Econometrica: Journal of the Econometric Society*, pages 128–140, 1953.

John F Nash. The bargaining problem. *Econometrica: Journal of the econometric society*, pages 155–162, 1950.

Akira Okada. The nash bargaining solution in general n-person cooperative games. *Journal of Economic Theory*, 145(6):2356–2379, 2010.

Andreas Park. The conceptual flaws of constant product automated market making. *Available at SSRN*, 3805750, 2021.

Thomas J Rivera, Fahad Saleh, and Quentin Vandeweyer. Equilibrium in a defi lending market. *Available at SSRN 4389890*, 2023.

Marzena Rostek and Ji Hee Yoon. Exchange design and efficiency. *Econometrica*, 89(6): 2887–2928, 2021.

Yuliy Sannikov, Andrzej Skrzypacz, et al. Dynamic trading: price inertia and front-running. *Preprint*, 2016.

Jan Christoph Schlegel, Mateusz Kwaśnicki, and Akaki Mamageishvili. Axioms for constant function market makers. *Available at SSRN*, 2022.

Michael Sockin and Wei Xiong. Decentralization through tokenization. *The Journal of Finance*, 78(1):247–299, 2023.

William Vickrey. Counterspeculation, auctions, and competitive sealed tenders. *The Journal of Finance*, 16(1):8–37, 1961.

Will Warren and Amir Bandeali. 0x: An open protocol for decentralized exchange on the ethereum blockchain. *URl: https://github. com/0xProject/whitepaper*, pages 04–18, 2017.

Yi Zhang, Xiaohong Chen, and Daejun Park. Formal specification of constant product (xy= k) market maker model and implementation. *White paper*, 2018.