A Rational Interpretation to the Automated Market Makers Design

Zhengge Zhou [1]

May 2024

Abstract

This paper establishes an economic microfoundation for the ad hoc Automated Market Makers (AMMs) mechanism design on decentralized exchanges (DEXs) in cryptocurrencies. First, we show that the current AMM mechanically pools the heterogeneity between liquidity providers (LPs), leading to an allocative inefficiency when accommodating the trading needs of DEX traders. Using a social planner problem, we subsequently characterize the optimal AMM that ensures efficient allocation for any group of heterogeneous LPs. This optimal AMM is structured as a geometric mean of LPs' utility preferences, with weights corresponding to their fractional ownership in the DEX. Finally, we implement this optimal AMM as an equilibrium in a Nash bargaining game among LPs and consider an extension where LPs are incentivized to truthfully report their preferences, thereby addressing concerns about private preference information in the implementation result.

Keywords: Decentralised Exchanges, Mechanism Design, Market Microstructure.

[1] 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.

This paper has greatly benefited from discussion with Andrea Andolfatto(discussant), Olga Klein, Roman Kozhan, Jesus Gorrin Leon, Kebin Ma, Rory Mullen, Ganesh Viswanath Natraj, Andreas Park, David Skeie, Fahad Saleh, Moris Strub, and Ruslan Sverchkov. I am grateful to seminar and workshop participants at the Gillmore Center monthly meeting seminar, the brownbag seminar of Warwick Business School, and the 2024 Lancaster-Manchester-Warwick Joint PhD Workshop on Quantitative Finance and Financial Technology.

1 Introduction

In traditional financial markets, plenty of trading protocols, ranging from auctions and limit order books to over-the-counter markets, have been successfully created and studied by both practitioners and academics. The diversity among these trading mechanisms is striking. However, a ubiquitous element unites these trading mechanisms: the presence of trusted centralised financial intermediaries who control and manage critical aspects of traders' accounts, including funds and identity information.

In sharp contrast, the emergence of blockchain technology creates the possibility for two parties to exchange crypto assets in a trustless and non-custodial fashion. By having numerous computer nodes act as information validators, the public blockchain network enables anonymous users to store, process, and transfer crypto assets in a decentralized manner. This approach, however, faces practical challenges due to the well-known blockchain scalability limitation. For instance, all unmatched limit orders must be stored, processed, and broadcast to the entire blockchain network, making it impractical for sizable trading activities on a public blockchain. Therefore, to facilitate trades on the blockchain, industrial practitioners created the Automated Market Maker (AMM) algorithmic system and built the first crypto-decentralised exchanges (DEXs) upon it in mid-2020 to provide market-making services. Nowadays, billions of dollars worth of trading activities take place on DEXs every day.

AMM has changed the landscape of financial markets for its genuinely novel market-making structure. On the liquidity supply side, it creates a liquidity pool by combining cryptos staked by liquidity providers (LPs). On the liquidity demand side, DEX-users or namely liquidity demanders (LDs) can instantly access the liquidity pool and trade against it or, to put it differently, LDs can swap out one type of crypto from the pool by swapping in other cryptos. AMM situated between LPs and LDs determines the exchange rate. Noticeably, any crypto holders in the network can become LPs by depositing their cryptos into the liquidity pool for trading fee income on a pro-rata basis.

Differing from precedent trading mechanisms in traditional financial markets, where prices or asset exchange rates are formed through the competition between market-makers via such as limit order books in equity markets or bilateral/multilateral bargaining in OTC markets, AMM in a DEX determines exchange rates by ensuring that the reserves of cryptos A and B in the pool remain invariant from pre-trade to post-trade[2]. Specifically, suppose the reserves of cryptos A and B in the liquidity pool x and y respectively, then the amount of crypto B, which we denote by Δy, the LD has to swap into the pool for swapping out any given Δx amounts of crypto A is determined by solving the following bonding curve condition:

$$u_{AMM}(x, y) = u_{AMM}(x - \Delta x, y + \Delta y),$$

[2] To ease notation, we consider the liquidity pool consist of pair of tokens. Generalizing our discussion into more than three types of tokens in a liquidity pool is straightforward.

where $u_{AMM} : \mathbb{R}^2 \to \mathbb{R}$ is often called a bonding curve function in the literature [3].

On the one hand, AMM, relying on this novel boding curve design, transforms DEX into a liquidity crowd-sourced platform, provides unsophisticated crypto holders opportunities to earn a market-making income, and offers LDs immediate access to the liquidity pool. On the other hand, as highlighted in the literature on DEXs, implementing a simplistic bonding curve design in the trading mechanism of DEXs exposes LPs to various risks such as arbitrage risk (Capponi and Jia 2021 [16]), front-running risk (Park 2021 [42]), adverse selection cost(Lehar and Parlour 2021 [36]; Aoyagi and Ito 2021 [6]), etc. In response, we see various practices in improving the design of the bonding curve. Leading design examples include Uniswap V2 with $u_{AMM}(x, y) = xy$, Uniswap V3 with $u_{AMM}(x, y) = (x + \alpha)(y + \beta)$, Balancer with $u_{AMM}(x, y) = x^w y^{1-w}$, and StableSwap with $u_{AMM}(x, y) = x + y$, among others.

However, thus far, no existing study has definitively answered what the "optimal" functional form of the bonding curve function u_{AMM} should be. More importantly, as an *ad hoc* design created by industrial practitioners, no existing study has ever provided a microfoundation for this simplistic but *ad hoc* bonding curve function. The absence of this economic interpretation raises many fundamental questions. For example, we observe that the bonding curve only depends on the aggregate crypto reserves in the pool, implying that, economically, the crypto deposited by each (potentially heterogeneous) LP is pooled. Or equivalently, the bonding curve overlooks the fundamental heterogeneities among LPs. This mechanical pooling practice, adopted by all current AMM trading algorithms, is equivalent to an allocation rule known as proportionally fair allocation (or pro-rata allocation). As we will show later in this paper, while LPs grouped in the DEX are heterogeneous in their preferences, this allocation rule leads to a trade allocative inefficiency in matching LPs and LDs in the AMM trading mechanism. With that said, we have some fundamental questions to be answered: Why do we need an AMM built upon a bonding curve that pools LPs' heterogeneity in DEXs? Does an optimal AMM enable efficient trade allocation to exist on a DEX, and if so, what will be the corresponding bonding curve $u^{\star}_{AMM}$ in this optimal AMM? Under what circumstances can we have this optimal AMM implementable as an equilibrium within a DEX? Addressing these questions above yields the main results of this paper.

We begin by showing that while LPs exhibit heterogeneity, a trade allocative efficiency exists resulting from the proportional allocation rule in the bonding curve design. Firstly, let us assume that each LP i is characterized by a utility preference function

[3] Note that, in practice, to incentivize LPs to stake cryptos A and B into the pool, LDs must pay not only the number of cryptos to the pool but also some additional units of crypto B as a trading fee. Thus, the actual AMM operation, incorporating the trading fee, is represented as:

$$u_{AMM}(x, y) = u_{AMM}(x - \Delta x, y + \gamma \Delta y), \gamma \in (0, 1]$$

where $\gamma \in (0, 1]$ and thus, $1 - \gamma \in [0, 1)$ represents the level of the trading fee paid by LD for exchanging Δx units of cryptos A against the pool.

$u_i(x, y)$, where (x, y) represents a bundle comprising x units of crypto A and y units of crypto B. For each feasible trade $(\Delta x, \Delta y)$, AMM will divide it into some smaller trades, $\{(\beta_i \Delta x, \beta_i \Delta y)\}_i$ with $\sum_i \beta_i = 1$, and allocate each LP i a trade $(\beta_i \Delta x, \beta_i \Delta y)$, where β_i is LP i's respective proportional ownership in the liquidity pool due to the propositional allocation principle adopted by the AMM algorithm. It now becomes evident that the current bonding curve algorithm, in conjunction with the propositional allocation rule, takes into account LPs' asymmetric liquidity ownership $\{\beta_i\}_i$ but overlooks the heterogeneities in LPs' utility preferences $\{u_i\}_i$. This simplistic algorithm, however, generates a suboptimal trading mechanism in the sense that a trade allocative inefficiency arises when LPs have heterogeneous preferences over how to absorb the trade request made by LD[4]. Essentially, current AMM algorithms worked in DEXs trade off the fundamental heterogeneities among LPs for absolute proportional allocation fairness.

The above suboptimality gives rise to a natural, important question: What is the optimal trade allocation in the DEX whose liquidity pool is grouped by heterogeneous LPs or to put it equivalently the optimal trading mechanism? To answer this, in this paper, we consider a social planner problem: Let us assume there exists a benevolent social planner with knowledge of LPs' preferences and their liquidity ownership in the DEX and the objective of this planner is to design such an allocation that minimises the trading cost of LDs subject to LPs' participation constraints. We find that in sharp contrast to the proportionally fair allocation mentioned above, the social planner not only just splits feasible trade $(\Delta x, \Delta y)$ made by LDs into smaller trades but also strictly follows LPs' participation constraints. The latter indeed contains information about LPs' heterogeneities in their liquidity ownership and their utility preferences. By solving this social planner problem, we successfully characterise the optimal trading mechanism for a DEX whose liquidity is contributed by a group of heterogeneous LPs.

Having obtained the optimal trading allocation for any given group of LPs, we then aim to take one step further and explore the conditions under which one can equate this socially optimal trading mechanism for a group of heterogeneous LPs to a trading mechanism for a single LP representative. We consider such an equivalence since if there exists a way to aggregate a group of heterogeneous LPs as a single LP representative, one can then naturally interpret the resulting preference function of this LP representative (if exists) as the bonding curve function we look for. This, therefore, rationalises the ad-hoc bonding curve design adopted by a DEX platform whose owners are a group of heterogeneous LPs. Indeed, as the second main result in this paper, we show later that under a mild condition, the resulting preference function of the LP representative exists and it reads as

$$u^{\star}_{AMM} := \Pi_{i=1}^{n} u_i^{\beta_i},$$

[4] However, it is noteworthy that in the trivial case in which LPs are homogeneous in their preference, say $u_i(x, y) \equiv u(x, y)$, the AMM trading mechanism which utilises u as its bonding curve function design is still efficient even under the propositional fair allocation rule.

where $\{u_i\}_{i=1}^n$ are utility preferences of LPs.

The resulting $u^\star_{AMM}$ structures as a weighted product of the utility preference of LPs and the weight assigned to each LP i's preference u_i equals her respective liquidity ownership in the liquidity pool β_i [5]. To grasp some economic intuition on this result, one can consider two simple DEX environments. First, if LPs are homogeneous in their preference, say $u_i(x, y) \equiv u(x, y)$ (but ownership can be heterogeneous), then trivially but heuristically, the optimal bonding curve to be implemented in the DEX should be this homogeneous preference $u(x, y)$, independently of LPs' heterogeneous liquidity ownership, which is therefore confirmed by our $u^\star_{AMM}$ as $\sum_i \beta_i = 1$. Another simple but nontrivial example is to consider a liquidity pool grouped by a whale LP and a small LP. Intuitively, due to the imbalanced liquidity contribution to the pool, one should conjecture that the optimal bonding curve accommodates the preference of the whale LP mainly, rather than the small LP. Once again, our $u^\star_{AMM}$ with a weighted product structure confirms such a conjecture, as $u^\star_{AMM}$ always assigns a dominant weight on the preference of LP who has dominant liquidity ownership in the pool, say the whale LP in this example.

Given this optimal bonding curve design $u^\star_{AMM}$, the next question we address in this paper is how to implement it as an equilibrium in a game among LPs. By assuming that LPs can bargain and negotiate how to absorb and allocate the trade request made by outside DEX-users, i.e., liquidity demanders, we show that a non-cooperative Nash bargaining game among LPs implements the socially optimal allocation or to put it differently the optimal bonding curve functional $u^\star_{AMM}$. We choose this Nash bargaining game as our implementation modelling framework for two primary reasons. Firstly, in practice, the decision-making process in the community of a DEX closely resembles a "propose then vote" governance procedure, which is the exact game structure adopted by most Nash bargaining games.

Secondly, the concept of a weighted product of players' (LP's) preferences is not new but known as the Nash social welfare function in economic literature, originating from the remarkable work of Nash (1950)[40]. In this work, Nash characterized the equilibrium of a two-person bargaining game by considering the product of two agents' utility preferences. Subsequent literature on social choice problems built upon Nash's work has extended it into more general cases such as the N-person bargaining game. Heuristically, Nash social welfare function selects the social outcome by balancing society members' preferences and their "importance" to the society, say, equivalently, their bargaining powers. In our DEX community case, this importance/bargaining power of each LP is naturally represented by her liquidity ownership of the pool. This key observation provides insight into why the optimal bonding curve function $u^\star_{AMM}$ we derived has the weighted-product structure. As a result, we prove that the optimal bonding curve design in a DEX grouped

[5] Strictly speaking, we cannot multiply $\{u_i\}_{i=1}^n$ in the way as if they are real numbers. The rigorous definition of this weighted product is to comprehend the LP representative as an aggregate consumer, more details specified later in the paper.

by heterogeneous LPs can be implemented as an equilibrium in a bargaining game among LPs, where the bargaining power assigned to each LP equals her fractional ownership of the pool. Technically, the bargaining power reflects the probability of each LP being selected as the proposer in each round of the game. The higher the chance of being selected as proposer, the higher the expected utility payoff this LP can gain from the game, which, in turn, corresponds to the weight on her preference function.

In the first extension of this paper, we study the competition between multiple symmetric DEX trading platforms and prove the existence of a unique symmetric equilibrium under this oligopolistic competition model. In this equilibrium, DEX platforms are compelled to provide an efficient pricing schedule as they compete in a Bertrand-style manner of supplying liquidity for DEX traders. This finding may shed light on the DEX market fragmentation observed in cryptocurrencies, where LPs stake their liquidity across multiple liquidity pools and LDs trade against multiple liquidity pools. In the second extension of this paper, we address the concern regarding the public information assumption on the preference functions of LPs in the implementation result. Specifically, Nash bargaining game described in our implementation result relies on that preferences of LPs are public information. Unlike the ownership information that is observable in the DEX as they are just the number of cryptos staked by each LP to the total number in the liquidity pool, the information about the preference profile of LPs is impossible to learn for mechanism designers. Due to that, we show that adding a preference-reporting stage where each LP has to report her preference prior to entering the Nash bargaining game can resolve this concern. In this preference-reporting game, each LP's respective payoff is determined by the preference reported by herself as well as the preferences reported by other LPs. Having the objective of this preference-reporting as by maximising the Nash social welfare among LPs, we show that truthfully reporting preference is a dominant strategy for every LP in this game, which, therefore, resolves the concern about how to obtain LPs' preference profile information in our aforementioned implementation result.

The rest of this paper proceeds as follows. Section 2 reviews the literature, along with the contribution of this paper. Section 3 presents the basics of our DEX economic environment and the allocative inefficiency in the DEX trading platform due to the implementation of the current AMM mechanism design. In section 4, by studying a benchmark social planner problem, we first characterise the optimal trading mechanism at a DEX in the presence of a group of heterogeneous LPs. We subsequently show the existence of an optimal bonding curve design that replicates the aforementioned socially optimal trading mechanism. Section 5 proves that the optimal bonding curve design we derived in section 4 is implementable as a bargaining game equilibrium between LPs. Section 6 considers the competition between DEXs, explaining the liquidity fragmentation in the DEX economy. Section 7 deals with the public information concern on the preference of LPs in our implementation result. Section 8 concludes. Proofs omitted in the main part of the paper are provided in the Appendix.

2 Related Literature

This paper contributes to the rapidly expanding literature on blockchain and decentralized finance. Reviews by Chen, Cong, and Xiao (2021)[19], Harvey, Ramachandran, and Santoro (2021)[30] and John, Leonid and Saleh (2022)[33] provide comprehensive insights into the broader landscape. From the market quality perspective of DEXs, various studies contribute complementary findings. For instance, Park (2021)[42] focuses on front-running risks to liquidity providers, while Barbon and Ranoaldo (2021)[9] argue that DEXs exhibit lower liquidity and price inefficiency compared to centralized exchanges. Foley, O'Neil, and Putnins (2023)[24] question the empirical superiority of AMM bonding curve functions as a market design, finding improved trading efficiency for specific asset characteristics. Lehar and Parlour (2021)[36] and Aoyagi (2020)[5] consider the case where LPs as passive investors are exposed to informed traders due to asymmetric information. Capponi and Jia (2021)[16] show that the pre-coded bonding curve at a DEX allows arbitrageurs to extract profit from LPs even in a public information environment. Our work here highlights that even if in a public information environment without any arbitrageurs, the *ex-ante* pre-coded bonding curve smart contract itself can still cause inefficiency as it pools LPs' heterogeneity and misallocates asset between LPs.

Noticeably, Capponi and Jia (2021)[16] find that the curvature of the bonding curve function is a key characteristic to be designed at a DEX for achieving maximum social welfare. Carre and Gabriel (2022)[17] and Rivera, Saleh and Vandeweyer (2023)[43] study the optimally programmable interest rate rule in decentralised lending platform. In contrast to existing literature, our work takes a unique step by directly investigating the trading mechanism design problem from a social planner perspective, while all prior studies predominantly accept the algorithmic trading mechanism as given (say, bonding curve in DEX and utilization setting in DeFi lending protocol). Our work here provides an economic microfoundation for these *ad hoc* trading mechanisms. We explore the conditions under which a bonding-curve-based function can serve as an optimal trading mechanism at a DEX, addressing a significant gap in the current literature focused on DEX design.

We also find several studies that try to understand the "optimal" design of a bonding curve function at DEXs from financial engineering and computer science perspectives. Leading examples include Angeris, Evans and Chitra (2021)[4], Bichuch and Zachary (2022)[12], Schlegel et al. (2022)[45], Goyal et al. (2023)[25] and Angeris et al. (2023)[3]. The main focus of these papers is to find a mathematical axiomatic framework that can encompass and generalize the geometric properties in bonding curve functions. Taking Angeris, Evans and Chitra (2021)[4] as an example, they find that having a concave, nonnegative, nondecreasing, and homothetic payoff function to LPs is "equivalent" to setting a concave, nonnegative, nondecreasing, and homothetic bonding curve function at DEXs[6]. Due to the popularity of these properties in algorithm trading programs, we may

[6] Mathematically speaking, the "equivalence" here means that LP's payoff function and the bonding

not be too surprised that most of the well-known bonding curves have such nice properties as they are mainly created by blockchain practitioners as well. Our work here, however, studies the bonding curve optimality problem from a game theory perspective.

Due to the emergence of DEXs, the current financial market in cryptocurrencies has experienced market liquidity fragmentation, and relevant literature on this crypto platform competition is scarce but gradually expanding. Lehar and Parlour (2021)[36] develop a competition framework between a DEX (Uniswap which utilizes AMM) and a CEX (Binance which utilizes limit order books) and compare LPs' return on either of them. Aoyagi and Ito (2021)[6] study the platform choice decision made by informed traders, assuming a DEX and a CEX coexist in the economy. Hasbrouck, Rivera and Saleh (2022)[31] study the effect of increasing trading fees at a DEX on its equilibrium trading volume, provided the existence of a given competing CEX. Han, Huang, and Zhong (2022)[27] empirically study interactions between a DEX and a CEX and show that DEX can help reveal the consensus on the value of the cryptocurrency. Our model complements the above studies by developing a theoretical framework to analyse the platform competition problem incorporating oligopolistic DEXs, rather than a single DEX platform like other studies. This inter-DEX competition is crucial for determining the market quality in crypto and market participants' incentives. We show that confronted with oligopolistic DEXs, LPs will strategically multi-home their assets at different DEXs in our model. This will reduce each DEX's market depth but enable liquidity demanders to better diversify their trading needs. By expecting that, both LPs and liquidity demanders will multi-home at all DEXs, which creates the market segmentation endogenously. Such market fragmentation equilibrium could be welfare-improved in our model. This result is related to the branch of the broader literature on market fragmentation. Leading papers studying the implication of market fragmentation in traditional financial markets include Malamud and Rostek (2017)[38], Chen and Duffie (2020)[18], Babus and Parlatore (2022)[8], among a few.

The implementation result in 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)[1], Biais et al. (2019)[10], Leshno and Strack (2020)[37] and Cong, He and Li (2021)[21]. 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, say, communication and collaboration between community members such as LPs at a DEX[7]. Existing literature has little to say about how the decision is made by blockchain society members in a decentralised manner. Exceptions include Aoyagi and Ito (2022)[7], Sockin and Xiong (2023)[46] and Han et al. (2023). Aoyagi and Ito (2022)[7] focus on the equilibrium trading fee as the key characteristic to be im-

curve function are Fenchel conjugates of each other.

[7] The details of how smart contracts system implements such "decentralised" platform feature can be found in, for examples, Warren and Bandeali (2017)[48], Zhang et al. (2018)[49] and Adams et al. (2021)[2]

plemented between members in a decentralised platform. Sockin and Xiong (2023)[46] examine whether decentralising ownership can be an innovation to resolve the conflict between platforms and users. Han et al. (2023)[28] point out the interest conflict between the large ("whale") and small token holders in a decentralised autonomous organisation (DAO). Our implementation result contributes to this literature by suggesting an explicit negotiation and communication process, which not only resembles the typical "propose and vote" processes in most DAOs but also incorporates decentralised ownership. Furthermore, we provide this decentralised negotiation process with a rigorous game theoretical foundation (i.e., the asymmetric noncooperative Nash bargaining game).

3 Basics

In this paper, we analyse a trading mechanism design problem at a cryptocurrency decentralised exchange (DEX). For simplicity, the crypto tokens traded at this DEX are tokens A and B. Moreover, without loss of generality, we let token A have an intrinsic value of $p \in \mathbb{R}_+$ against token B, a common knowledge known by all agents in the market[8].

Market structure The market structure of a DEX trading platform typically consists of three main components: the liquidity pool, liquidity providers (LPs), and DEX traders. The liquidity pool, positioned between DEX traders and LPs, contains tokens staked by LPs who are on the liquidity supply side of the DEX. They are incentivized to deposit tokens into the liquidity pool primarily for the trading fees charged on the trading activities carried out by DEX traders. Consequently, DEX traders are situated on the liquidity demand side of the DEX platform and we refer to DEX traders as liquidity demanders (LDs) for expository convenience. The novelty of this DEX market structure lies in the presence of the liquidity pool, which allows any token holders in the network to trade instantly, eliminating the prevalent search friction in traditional financial markets where matching trading partners is required.

Market participants. As for the specific types of DEX market participants (LPs and LDs), formally, we have:

1. LPs indexed by $i \in I$ are investors who can participate in any DEXs and become the fractional owner of the liquidity pool by staking some crypto there;
2. The LD is a trader who wants to fulfil her trading needs at the DEX.

The trading motivations of DEX traders are exogenously given here. We assume there is a signal θ privately received by each LD and such a signal directly determines a

[8] It is noteworthy that the DEX in practice, e.g. Uniswap 3, can contain more than one liquidity pool for the trading related to each pair of cryptos A and B. This design enables each pool associated with a specific level of trading fee. The main focus of this paper, however, is the trading mechanism design. Therefore, for simplicity, we only consider the DEX platform whose structure is restricted to one pool.

token-A purchasing need $q(\theta)$. For simplicity, let us assume that $\dot{q}(\theta){>}0$. Possible ways to endogenize this signal can be either from the margin call of LD's customers or some hedging requirements. Then one can naturally interpret θ as the inventory holding of the LD[9].θ is privately observed by the LD but has a commonly known distribution over $[\underline{\theta}, \overline{\theta}]$ with a CDF F. We parameterise the type of LD based on her signal θ.

Preference functions. Next, let us specify the heterogeneity between LPs at the DEX platform. As one of the most fundamental (and the cleanest) ways, we directly assume that LPs are heterogeneous in their preference function u, a mapping defined as follows:

$$u : \mathbb{R}_+^2 \longrightarrow \mathbb{R}_+.$$

By interpreting (x, y) as a tokens bundle consisting of x units of crypto A and y units of crypto B, we then naturally have the value $u(x, y)$ as the level of utility an agent can derive from consuming this bundle of tokens. This modelling device, based on agents' preferences, is also adopted by Sockin and Xiong (2023), where the authors assume that digital platform users, with a Cobb-Douglas utility preference over two complementary tokens, can derive utility from consuming token bundles. Such an economic intuition applies to our setting as well, leading to heterogeneous LPs and LDs finding it maybe profitable to interact with each other via a liquidity pool, whether by staking or swapping tokens.

In sharp contrast to Sockin and Xiong (2023), we do not impose a specific Cobb-Douglas utility preference in this paper. Instead, we assume that the utility preferences of LPs are given by $\{u_i\}_{i\in I}$, where $\{u_i\}_{i\in I}$ are allowed to be potentially heterogeneous. Regarding the utility preferences of LDs, as mentioned earlier, each LD has a signal-related trading need $q(\theta)$. To capture the impact of this signal θ on her trading at the DEX, we assume that a θ-type LD can derive a utility benefit from purchasing $q(\theta)$ shares of crypto A given by $u(q; \theta)$.

Trading mechanism design variable. Having introduced the preferences of LPs and LDs, we now turn to the specification of the current DEX trading mechanism designs in practice. Unlike market makers in traditional financial markets where they compete in posting pricing schedules, in the current DEX practices, LPs participating in any DEX platform have to accept a pre-determined DEX pricing—the Automated Market Maker mechanism (AMM). Denoting by $\mathcal{R} = (x, y)$ the liquidity pool whose respective reserves on crypto A and B are x and y, we can then represent a typical AMM trading mechanism by a real-valued mapping whose domain is the token reserves in the liquidity pool:

$$u_{AMM} : \mathcal{R} \subseteq \mathbb{R}_+^2 \to \mathbb{R}_+.$$

[9] For more details about the role of this signal, readers can go to section 6 of this paper where we explicitly model signal θ as the inventory holding of LDs.

In this AMM mechanism or u_{AMM}, it proceeds any token-A purchasing trade Δx made by the LD if the amount of token B paid by the LD, which we denote as Δy, satisfies the following rule:

$$u_{AMM}(x - \Delta x, y + \Delta y) = u_{AMM}(x, y). \tag{1}$$

Given that, in this paper, we also refer to the AMM as a bonding curve, another popular term used in the literature on DEXs. Moreover, it is not hard to see that any AMM mechanism design u_{AMM} as specified above is equivalent to some pricing schedule T as defined below:

$$T : \mathbb{R}_+ \to \mathbb{R}_+,$$

where $T(\cdot)$ states that a trader can swap out $q := \Delta x$ shares of crypto A from the liquidity pool in the DEX if at least $T(q) := \Delta y$ shares of crypto B are swapped into this pool.

Note that our pricing schedule $T(\cdot)$ representation is general. For instance, the limit order books trading mechanism in centralised equity exchanges can be written as

$$T(q) = \int_0^q t(z)dz,$$

where $t(z)$ is the marginal money cost of purchasing the zth unit of an asset. Another example is an Over-the-Counter (OTC) market where dealers compete to provide liquidity to traders. It is evident that a dealer with a preference function $u(x, y)$ will be willing to trade q shares of asset A with a trader only if the money (asset B) transfer $T(q)$ paid by the trader satisfies that $u(x - q, y + \Delta(q)) \geq u(x, y)$. Consequently, we see that the quote $\Delta(q)$ provided by the dealer effectively functions as a pricing schedule $T(q) := \Delta(q)$.

Mechanism design problem in the DEX The DEX mechanism design problem in each DEX platform is twofold.

First, confronted with the liquidity provision competition from other platforms, including both other DEXs and centralized exchanges (CEXs), LPs in each DEX platform have to determine a pricing schedule design that offers competitive pricing for upcoming DEX traders. During this process, LPs also face heterogeneous participation constraints due to their preference heterogeneity. Taking these two factors into account naturally defines the mechanism design problem faced by LPs in a DEX: they have to design a pricing schedule at an ex-ante stage to maximise LD's trading payoff. Such a mechanism design problem in the context of DEX indeed follows the spirit of the optimal trading mechanism problem defined in Biais et al. (2000)[11] and Holmström and Myerson (1983) [32]: a social planner has to choose an optimal trading mechanism to maximize traders' utility at an ex-ante stage, subject to marker maker's participation constraints. We, therefore, can define a similar social planner problem for LPs as their papers, interpreting LPs in the DEX as passive market makers. Consequently, we characterise the optimal pricing schedule, resulting from the solution of our planner problem, which archives the allocative efficiency in matching LDs and LPs on the DEX.

Second, the DEX platform—one of the most successful decentralized autonomous organizations (DAOs)—operates without a central leadership and is collectively managed by its members (LPs), who hold economic rights proportional to their staked liquidity in the liquidity pool. This decentralized decision-making process in the DEX governance scheme makes the implementation of the optimal trading mechanism solution derived from the aforementioned social planner problem non-trivial, especially when accounting for the potential preference heterogeneity among LPs. To this end, we introduce a bargaining framework into the DEX governance scheme, allowing LPs with heterogeneous preferences and asymmetric liquidity pool ownership to propose and vote on the trading mechanism to be implemented on the platform. Having the bargaining power of each LP precisely equal to her liquidity ownership in the liquidity pool, we show that our optimal trading mechanism defined by the social planner problem is implementable as an equilibrium between LPs.

We conclude this section by noting that the current AMM mechanism on most DEXs, as an *ad hoc* industrial practice, relies on the bonding curve design (1). However, this design may not ultimately lead to $T^\star$, the socially optimal mechanism achieving a trading allocative efficiency. The main rationale behind this conjecture is due to the observation that, in order to maintain algorithmic simplicity in the bonding curve design, the AMM allocates each trade between LDs and LPs in a proportional allocation principle. However, this principle only focuses on the asymmetry between LPs in their liquidity ownership in the liquidity pool but mechanically pools their heterogeneity in preference, thereby yielding a trade allocative inefficiency. This key observation raises an important, unanswered question: what is the cost of pooling LPs for the sake of a simplistic AMM/bonding curve algorithm? Therefore, before presenting the optimal pricing schedule $T^\star$ and its implementation result, we have to answer this question first and begin the analysis in the next subsection by investigating the exact role of this proportional allocation principle in executing trades at DEXs.

3.1 The Proportional Allocation Principle in DEX Platforms

As mentioned earlier, a 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[10].

Trivially, the ownership vector $\{\beta_i\}_i$ satisfies $\sum_{i=1}^{n} \beta_i = 1$. Beyond this, it plays an essential role in the DEX ecosystem with automated market making. For instance, given the ownership vector $\{\beta_i\}_i$,

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 have to be $\beta_i x$ and $\beta_i y$, respectively.

Bonding curve design (1) results in the DEX pricing as well as the trading fees paid by LDs as a function of the market depth of the liquidity pool, namely the total number of tokens in the liquidity pool. Given this and the typical DAO feature of the DEX platform, it works well to adopt the proportional allocation principle in distributing the trading fees paid by DEX traders among LPs, say the owners of the platform. 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 DEX traders.

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) may generate inefficiency, particularly concerning when LPs exhibit heterogeneity in their preferences. In the subsequent discussion, let us delve deeper into these potential inefficiencies and their implications in the DEX platform.

3.2 Trading Allocative Inefficiency in AMM Mechanism

In stark contrast to market makers in traditional financial markets, who engage in strategic competition to provide liquidity, LPs on DEX platforms take on a passive role. 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

[10] 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.

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:

$$u_{AMM}(x-q, y+T(q)) = u_{AMM}(x, y). \tag{2}$$

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:

$$u_i(x_i - \beta_i q, y_i + \beta_i T(q)) \geq \pi_i(x_i, y_i). \tag{3}$$

Upon inspection of (3), 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.

Assumption 1 (homothetic preference). *For each LP $i \in I$, her utility preference function u_i is homothetic. That is, $u_i(\lambda(x, y)) = \lambda u_i(x, y)$ for any $\lambda \geq 0$.*

This homothetic preference is not restrictive, especially when considering the family of preference with constant elasticity of substitution (CES). We call a preference a CES preference with an elasticity of substitution $\sigma \in \mathbb{R}_{++}\backslash 1$ if it follows:

$$u(\mathbf{x}) = \left(\sum_i (a_i x_i)^{\frac{\sigma-1}{\sigma}} \right)^{\frac{\sigma}{\sigma-1}} \quad \forall \mathbf{x} \in \mathbb{R}^n_+ \quad and \quad \mathbf{a} = \{a_i\}_i \in \mathbb{R}^n_{++}. \tag{4}$$

Utility preferences in CES family are homothetic and they are extensively studied in the literature. Leading examples include Leontief, Cobb-Douglas, and linear preferences[11].

Moreover, it is noteworthy that most bonding curve designs in practice are homothetic. For instance, $u(x, y) = x + y$ design in mStable is linear; Uniswap V2 with $u(x, y) = x^{\frac{1}{2}} y^{\frac{1}{2}}$ and Balancer with $u(x, y) = x^w y^{1-w}$ both follow a Cobb-Douglas preference; StableSwap and Saber with $u(x, y) = C(x + y) + x^{\frac{1}{2}} y^{\frac{1}{2}}$ can be viewed as a combination of linear preference and Cobb-Douglas preference. All these bonding curve designs are homothetic functions.

Of particular importance, one should note that even though the bonding curve design in Uniswap V3, such as $u(x, y; x_0, y_0) = (x+x_0)(y+y_0)$, does not directly follow the homothetic property, it can be decomposed into a bonding curve in the form used in Uniswap V2, namely $u^*(x, y) = xy$, plus an independent price range constraint. It is not difficult to verify that this decomposition is unique. Conversely, a Uniswap V2 AMM, whose bonding curve is homothetic, plus some independent price range constraints, also uniquely replicate a specific AMM design in Uniswap V3. Due to this one-to-one correspondence, we can then view LPs in Uniswap V3 together with their participation constraints as if they were in Uniswap V2 and they faced participation constraints in the form of (2) plus some independent price range constraint. Having said that, we see the main insights derived in this paper based on homothetic bonding curve designs, including that in Uniswap V2 platform, naturally extended to Uniswap V3 platform.

Lemma 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*

$$u_{AMM}(x - q, y + T(q)) = u_{AMM}(x, y) \Longrightarrow u_i(x_i - \beta_i q, y_i + \beta_i T(q)) \geq \pi_i(x_i, y_i) \;\; \forall i, \tag{5}$$

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

[11] They are the limiting cases of the CES preferences as σ goes to $0, 1$ and $+\infty$, respectively. As an illustration, let us consider the limiting case as σ goes to 1. Suppose $u(x_1, x_2) = (a_1 x_1^\gamma + a_2 x_2^\gamma)^{\frac{1}{\gamma}}$. Taking log for both sides yields that $log\, u(x_1, x_2) = \frac{1}{\gamma} log\, (a_1 x_1^\gamma + a_2 x_2^\gamma)$. Therefore, by applying the l'Hôpital's rule and taking $\gamma \to 0$ (i.e. $\sigma \to 1$), we can see $u(x_1, x_2) = x_1^{a_1} x_2^{a_2}$, a Cobb-Douglas utility function.

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 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.

3.3 Liquidity Withdrawal Inefficiency in AMM Mechanism

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 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[12]. Suppose now that both LP1 and LP2 decide to 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 ones. However, one should note that this process would incur additional trading costs and other sources of risk not modelled here.

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

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)[16] argue 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)[16], 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.

4 Optimal Trading Mechanism at a DEX

In this section, using a social planner problem, we first specify the exact trading allocative efficiency in the context of the DEX trading platform. Based on that, we derive the optimal trading mechanism at the DEX. Note that when we refer to an optimal trading mechanism at the DEX, we mean a mechanism that matches LPs and LDs efficiently (more details to follow). Lastly, by interpreting the bonding curve as the preference function of an LP representative, we characterize the optimal bonding curve design which replicates our optimal trading mechanism in the social planner problem.

4.1 Ex Ante Efficiency: A Social Planner Problem

To establish a DEX trading platform, LPs must design a hard-coded trading mechanism and stake their liquidity ahead of the arrival of LDs. We, therefore, consider the optimal trading mechanism definition in the spirit of Holmström and Myerson (1983): a benevolent social planner chooses an optimal trading mechanism that maximizes traders' utility at an *ex-ante* stage. To the best of our scholarship, such a social planner problem is the most straightforward way to define allocative efficiency for trading mechanisms. The objective of this planner is to maximize the LD's trading payoff, as this LD would otherwise choose other platforms where they could achieve a higher trading payoff.

Specifically, we can denote by

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

the net utility payoff a θ-type LD obtains from fulfilling her privately known trading need $q(\theta)$ against a trading mechanism $\{q(\cdot), \tau(\cdot)\}$, where $q(\theta)$ and $\tau(\theta)$ are the respective quantities of crypto A and the transfer of crypto B made by this θ-type LD trader at the DEX.

Contingent on the future realization of θ, at an *ex-ante* stage, the optimal trading mechanism chosen by the social planner has to be the solution for the optimization problem below:

$$\textbf{Planner's problem:} \quad \underset{\{q(\cdot),\tau(\cdot)\}}{Max} \quad \int_{\underline{\theta}}^{\overline{\theta}} \Big[u(q,\theta) - \tau(\theta)\Big] dF(\theta) \tag{6}$$

$$\textit{subject to} \quad \int_{\underline{\theta}}^{\overline{\theta}} u_i\Big(x_i - q_i(\theta), y_i + \tau_i(\theta)\Big) dF(\theta) \geq \pi_i \quad \forall i \in 1, ..., I \tag{7}$$

$$\textit{and} \quad \sum_i q_i(\theta) = q(\theta); \quad \sum_i \tau_i(\theta) = \tau(\theta). \tag{8}$$

Above, the first part of the constraints is the *ex-ante* participation constraints of LPs as in the last section, whereas the second part is the market clearing condition ensuring that the social planner (or the trading mechanism) does not retain any token after the trading between LPs and DEX traders.

Note that in practice, the DEX trader also has to pay a small amount of additional token B, denoted by $\gamma\tau_i(\theta)$, as the trading fee for each LP i. This fee serves as the key incentive for crypto holders in the network to stake liquidity into the AMM pool. The fee is initially added to the liquidity pool but is subsequently transferred to the wallets of the LPs. Following the literature, such as Lehar and Parlour (2021)[36], we assume that this trading fee is paid directly to LPs, thereby simplifying our notational exposition.

Solving this planner's problem is straightforward. We can show later in Proposition 1 that participation constraints of LPs are binding at the optimum since it is a necessary condition for the existence of an efficient trading allocation. Formally, we characterize and state below the optimal trading mechanism, denoted by $\tau(q)$, for a DEX platform in the following proposition.

Proposition 1 (optimal trading mechanism). *For a group of LPs whose preferences are given by $\{u_i\}_i$, the optimal trading mechanism $\tau(q)$ that maximises the LD's trading payoff is characterised by*

$$\tau(q) \equiv \min_{\{q_i\}_i} \left\{ \sum_i \tau_i(q_i) : \sum_i q_i = q \right\}, \tag{9}$$

where $\{\tau_i(\cdot)\}_i$ satisfy that

$$u_i\Big(x_i - q, y_i + \tau_i(q)\Big) = \pi_i \quad \forall i.$$

Upon inspection of (9), it becomes evident that the efficiency of a trading mechanism at the DEX centres around its allocative efficiency that accommodates the trading needs of DEX traders between LPs. The metric for assessing the allocation efficiency of a trading mechanism is the total trading cost paid by DEX traders subject to the participation constraints of LPs. Specifically, on the liquidity-demanding side, the LD is primarily concerned with the aggregated transfer she needs to pay for swapping out q units of token A from the pool, denoted as $\tau(q) := \sum_i \tau_i(q_i)$. On the liquidity-supplying side, however, each LP absorbs only one fraction of the trade, exchanging q_i shares of token A with the LD for $\tau_i(q_i)$ shares of token B as the return.

Focusing on minimizing the trading cost of LD requires the planner to design an allocation $\{q_i\}_i$ over all feasible allocations such that $\sum q_i = q$ and that the participation constraints of LPs are binding. Given this set of feasible allocations, the optimal bundle of transfers $\{\tau_i(q_i)\}$ achieving a minimal $\sum_i \tau_i(q_i)$ defines the efficient allocation for this trading q. Repeating this process for all admissible $q \in [0, x)$ defines the optimal mechanism, thereby solving our social planner problem for a DEX trading platform. It is noteworthy that one key factor in designing the above optimal mechanism lies in ensuring LPs' binding participation constraints. This is indeed in sharp contrast to the popular AMM algorithm design, which absorbs and allocates trades between LPs only according to their liquidity contributions. It now becomes evident that AMM violates the optimality factor associated with LPs' binding participation constraints, thereby leading to the AMM mechanism being suboptimal in its trading allocative efficiency, as indicated by the main result in our Lemma 1.

Let us now conclude this section with some remarks on our optimal trading mechanism (9). First of all, although we have identified the optimal trading mechanism, its relationship to the popular bonding curve design in DEX trading platforms is still unclear at this stage. DEX practitioners opt for implementing a bonding curve design to govern the trades on the liquidity pool for its simple functional form u_{AMM}. In sharp contrast, our social planner problem points out that to compete with other DEXs by maximizing the trading payoff of LDs, DEXs have to determine an optimal pricing schedule $\tau(q)$ as in (9). This $\tau(\cdot)$, however, may not necessarily be consistent with any pricing schedule $\Delta y(\Delta x)$ implied in any bonding curve design $u_{AMM}(x - \Delta x, y + \Delta y) = u_{AMM}(x, y)$. A natural, important question then emerges: What is the underlying relationship between the optimal pricing schedule $\tau(q)$ derived from a social planner problem and the ad hoc bonding curve design in our DEX practices? This question unfolds in two parts. First, given a group of LPs with preferences $\{u_i\}_i$ and liquidity contributions $(x_i, y_i)_i$, we seek to determine the exact functional form of $\tau(\cdot)$ in the sense of our social planner problem (9). Secondly, we want to see the possibility of finding a bonding curve design $u_{AMM}(\cdot, \cdot)$ such that, if it is utilized at the DEX, it indeed generates a pricing schedule that is exactly the $\tau(\cdot)$ given above.

4.2 Optimal Bonding Curve Function

The market structure of the liquidity pool transforms DEXs into a liquidity crowd-sourced system. LPs contribute their funds to the liquidity pool, enabling outside trades (i.e., LDs) to exchange assets without relying on a centralized order book. Based on this market structure, the group of LPs in a DEX has to determine a pricing schedule or trading mechanism, accepted by the entire LPs community and accounting for the presence of heterogeneity between LPs, at an ex-ante stage. This setup reminds us of a classical question in aggregate consumer studies in economics literature: How do individual budgets and preferences determine the aggregate consumption decision?

In the context of DEXs, to some extent, we can interpret the bonding curve function in the AMM trading mechanism as the utility preference function of a hypothetical LP representative (i.e., a single aggregate consumer in the literature on aggregating consumers). LPs (individual consumers) trust this representative (aggregate consumers) and stake their cryptos into the liquidity pool (aggregate budgets) so that she can represent them in trading with outside LDs (making consumption decisions). From the perspective of this representative, she needs to learn LPs' utility preferences, represent them in trades with LDs, and eventually return the post-trade liquidity pool to LPs. Therefore, we should expect that the utility preference of this LP representative must account for the heterogeneity between LPs' preferences and ownership of the pool. Indeed we can show shortly that a "well-defined" LP representative has her preference function structured as a weighted product of LPs' utility preferences, with weights reflecting LPs' fractional ownership of the liquidity pool.

To start, suppose that the liquidity contributed by each LP i to the liquidity pool is valued $b_i > 0$ (in USD) and the price of crypto A against crypto B is $p > 0$. If LP i chooses to consume her budget directly, her most preferred bundle of cryptos, which we denote as $D_i(\mathbf{p}, b_i)$, is given by

$$D_i(\mathbf{p}, b_i) := \Big(x_i(\mathbf{p}, b_i), y_i(\mathbf{p}, b_i)\Big) = \underset{(x,y)\in\mathbf{R}^2_+ : px+y\leq b_i}{argmax} \quad u_i(x, y), \tag{10}$$

where $\mathbf{p} = (p, 1)$ denotes the price vector of cryptos A and B.

For each trade request $(q, T(q))$ made by outside LD, LP i, as a fractional owner of the liquidity pool, at the *ex-ante* stage, will only be willing to accept the trade allocation $\{q_i, T_i(q_i)\}_i$ (which is specified in the trading mechanism) if

$$u_i\Big(x_i(\mathbf{p}, b_i) - q_i, y_i(\mathbf{p}, b_i) + T_i(q_i)\Big) \geq u_i\Big(x_i(\mathbf{p}, b_i), y_i(\mathbf{p}, b_i)\Big) := \pi_i(\mathbf{p}, b_i),$$

where $\pi_i(\mathbf{p}, b_i)$ represents the reservation utility LP i could obtain if she does not participate in the DEX but consumes her budget directly. Recall that the above condition is just the participation constraint of LP i in our social planner problem. Based on the above condition, one can see that the trades allowed by LP i, which we denote by the set of admissible trades of LP i, is given as follows,

$$\hat{S}_i(\mathbf{p}, b_i) = \Big\{(q_i, T_i(q_i)) : u_i(x_i - q_i, y_i + T_i(q_i)) \geq \pi_i(\mathbf{p}, b_i)\Big\}, \tag{11}$$

where equality is achieved when there is sufficient competition between LPs within a DEX or across DEXs for liquidity provision service.

By using the form of admissible trade set (11) and considering the DEX as a liquidity crowd-sourced platform, we now turn our attention to characterizing the set of admissible trades supported by a liquidity pool (or a group of heterogeneous LPs). In principle, the trading mechanism must allow for any trade request $(q, T(q))$ made by an LD, provided there exists a trade allocation $q_i, T_i(q_i)_i$ such that $\sum_i(q_i, T_i(q_i)) = (q, T(q))$ and $(q_i, T_i(q_i))$ satisfies the participation constraint of LP i. Stated differently, each $(q_i, T_i(q_i))$ should belong to $\hat{S}_i(\mathbf{p}, b_i)$, the admissible trades set supported by LP i. Building upon this observation, a natural and straightforward definition of the set of admissible trades supported by a group of LPs is given by:

$$\hat{S}(\mathbf{p}, \mathbf{b}) := \hat{S}_1(\mathbf{p}, b_1) + \hat{S}_2(\mathbf{p}, b_2) + ... + \hat{S}_n(\mathbf{p}, b_n), \tag{12}$$

where $\mathbf{b} := \sum_i b_i$, $\hat{S}_i(\mathbf{p}, b_i)$ represents the set of admissible trade supported by LP i, and the summation between two sets defined here represents the Minkowski sum over sets.

In mathematics, the Minkowski sum of two sets, A_1 and A_2, is defined as follows:

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

Applying this definition to our set of admissible trades definition, an element $(q, T(q))$ belonging to $\hat{S}(\mathbf{p}, \mathbf{b})$ implies that there exists at least one trade allocation $\{q_i, T_i(q_i)\}_i$

such that $(q_i, T_i(q_i)) \in \hat{S}_i(\mathbf{p}, b_i)$. In practical terms, the trading mechanism in the DEX will break down a trade request $(q, T(q))$ made by the LD into n smaller trading requests $(q_i, T_i(q_i)) \in \hat{S}_i(\mathbf{p}, b_i)$ according to LPs' preferences. Each LP i absorbs a trade $(q_i, T_i(q_i))$ so that she can engage in a trade with the LD, exchanging q_i units of crypto A for receiving $T_i(q_i)$ units of crypto B, and this trade $(q_i, T_i(q_i))$ has to satisfy her participation constraint, say belonging to $\hat{S}(\mathbf{p}, b_i)$.

However, we want to emphasise that we cannot simply aggregate (in the Minkowski sum sense) individual sets of admissible trades for the aggregate set of admissible trades supported by the DEX. As one will see in the following illustrative example, the Minkowski sum set $\hat{S}(\mathbf{p}, \mathbf{b})$ would contain elements that are never reachable in real trading activities in a DEX.

Example 2. Suppose that we have two LPs that group the DEX and their sets of admissible trades are given by

$$\hat{S}_1(\mathbf{p}, b_1) = \{(0,0),(1,2)\} \ \ \textit{and} \ \ \hat{S}_2(\mathbf{p}, b_2) = \{(0,0).(1,3),(2,7)\},$$

respectively. We can compute the Minkowski sum over these two sets of admissible trades as follows.

$$\hat{S}_1(\mathbf{p}, b_1) + \hat{S}_2(\mathbf{p}, b_2) = \{(0,0),(1,2),(1,3),(2,5),(2,7),(3,9)\}.$$

On the positive side, $\hat{S}(\mathbf{p}, \mathbf{b}) = \hat{S}_1(\mathbf{p}, b_1) + \hat{S}_2(\mathbf{p}, b_2) \supsetneq \hat{S}_1(\mathbf{p}, b_1) \cup \hat{S}_2(\mathbf{p}, b_2)$. That is, from the perspective of LDs, compared to trading with this group of LPs independently, the Minkowski sum enlarges the set of admissible trades in this DEX. Furthermore, one should note that the size of Minkowski's sum would grow dramatically while any of $\{S_i(\mathbf{p}, b_1)\}_i$ becomes large. However, on the negative side, defining the set of admissible trades on a group of LPs under the Minkowski sum operation will generate unreachable or redundant points such as point $(2,7)$ in our example. Point $(2,7)$ is unreachable as we already have $(2,5)$ contained in $\hat{S}(\mathbf{p}, \mathbf{b})$. Recall that a point $(q, T(q))$ in the set of admissible trades $\hat{S}(\mathbf{p}, \mathbf{b})$ represents that LD can swap out q shares of asset A for the liquidity pool by transferring a $T(q)$ shares of asset B. Therefore, the admissible trade $(2,7)$ is strictly dominated by the trade $(2,5)$ and only the latter would be chosen by LD.

These unreachable points reflect the fact that confronted with the competition between LPs or among oligopolistic DEXs for liquidity provision services, LDs who want to minimise their trading cost will never make a feasible trade request that would be dominated by other elements in $\hat{S}(\mathbf{p}, \mathbf{b})$. In other words, the competitive landscape between LPs (or among DEXs) would lead to each DEX posting the efficient frontier in $\hat{S}(\mathbf{p}, \mathbf{b})$). Mathematically, it implies that the realised set of admissible trades posted by each DEX would correspond to the boundary of $\hat{S}(\mathbf{p}, \mathbf{b})$, i.e., $\partial\hat{S}(\mathbf{p}, \mathbf{b})$. Consequently, it is may not hard to anticipate that $\partial\hat{S}(\mathbf{p}, \mathbf{b})$ would read as a geometric "mean" over $\{\partial\hat{S}(\mathbf{p}, b_i)\}_i$. The key question here is to have a well-defined mean over two sets. Graphically, suppose for example that we have only two LPs within the DEX and assume that LP 1 and LP 2 own β_1 and $\beta_2 = 1 - \beta_1$ fractions of the pool, respectively. Then the optimal bonding curve chosen by these two LPs cooperatively would be given by $F_{aggregate}(x, y) = k$, the red dashed curve depicted below:

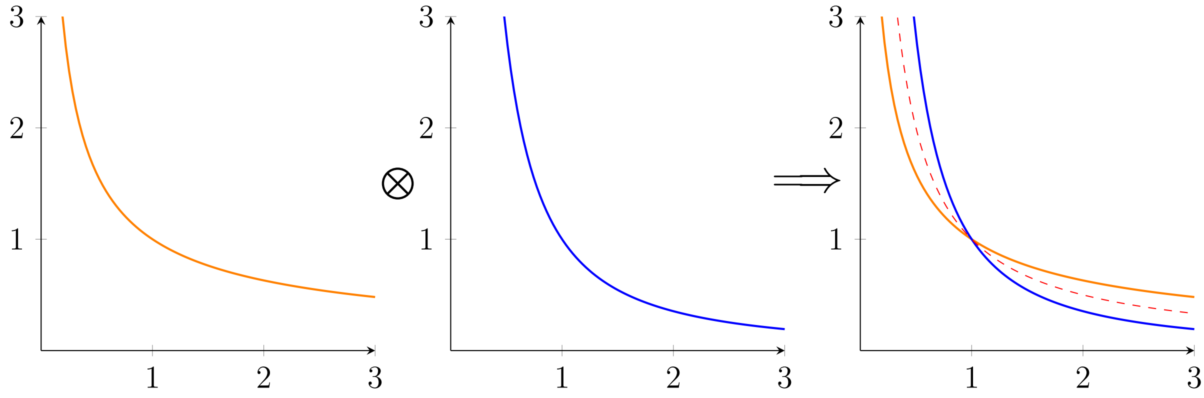

Figure 1: Here, we select $u_1(x, y) = x^{\frac{2}{5}}y^{\frac{3}{5}}$, $u_1(x, y) = x^{\frac{3}{5}}y^{\frac{2}{5}}$ and $\beta_1 = \beta_2 = \frac{1}{2}$ to illustrate their geometric mean.

Taken all the above discussions together, it implies that to compete with other DEXs, the set of admissible trades allowed by each DEX, which we denote by $S_{AMM}(\mathbf{p}, b)$, has to be:

$$S_{AMM}(\mathbf{p}, \mathbf{b}) = \Big\{(q, T(q)) : u_{AMM}(x - q, y + T(q)) \geq u_{AMM}(x, y)\Big\}, \tag{13}$$

where $\mathbf{b} := \sum_i b_i$ and u_{AMM} (if exists) is the bonding curve function or from the LP's perspective, the utility preference of the representative.

Using (13), one may notice that designing an optimal trading mechanism in the DEX $T(\cdot)$ would be equivalent to specifying the set of admissible trades $\hat{S}_{AMM}(\mathbf{p}, \mathbf{b})$ or determining the utility preference of the LP representative u_{AMM}. In essence, representation (13) develops a method that reduces the challenging problem of designing an optimal trading mechanism on a liquidity pool to simply computing the aggregate preference over a group of heterogeneous LPs. Moreover, one will see that this representation of aggregate preferences can refine the Minkowski sum by eliminating those unreachable points we discussed above. Formally, we have the following sufficient condition for the existence of an aggregate preference u_{AMM} over any group of homothetic preferences $\{u_i\}_{i=1}^n$.

Assumption 2. *Denoted by $\{u_i\}_i$ and $\{b_i\}_i$ the respective LPs' utility preference profile and liquidity contribution profile in the DEX, a well-defined LP representative has the utility preference u_{AMM} such that her most preferred bundle of cryptos equals the* *aggregation of LPs' individually most preferred bundles of cryptos. Specifically,*

$$\Big(\boldsymbol{x}(\boldsymbol{p},\boldsymbol{b}),\boldsymbol{y}(\boldsymbol{p},\boldsymbol{b})\Big)=\Big(\sum_i x_i(\boldsymbol{p},b_i),\sum_i y_i(\boldsymbol{p},b_i)\Big),\tag{14}$$

where for each $i\in\{1,...,I\}$, $\Big(x_i(\boldsymbol{p},b_i),y_i(\boldsymbol{p},b_i)\Big)$ defined in (10) represents the most preferred bundles of crypto of LP i, and

$$\Big(\boldsymbol{x}(\boldsymbol{p},\boldsymbol{b}),\boldsymbol{y}(\boldsymbol{p},\boldsymbol{b})\Big):=\underset{(x,y)\in\mathbf{R}^2_+:px+y\leq\boldsymbol{b}}{argmax}\quad u_{AMM}(x,y)$$

represents the most preferred bundles of assets of LP representative.

Several remarks are provided below in order. Firstly, it's important to recognize that one can interpret the bonding curve function in the DEX as the utility preference of a single "aggregate" representative, who can represent individual LPs to consume or exchange cryptos with LDs, only if the trust issue between this representative and individual LPs can be resolved perfectly. Indeed, facilitating trades in a trustless manner is the exact key advantage of DEXs due to its backbone blockchain technology. In sharp contrast to the traditional financial markets where individual agents require an institutional reason to trust a principal/platform, the trading mechanism utilised by DEXs is a hard-coded algorithm on the blockchain. Once coded, it becomes public, deterministic, decentralized, and beyond the unilateral control of any single LP, resulting in trustless trading feasible on DEXs.

Also, it's essential to note that the condition (14) above is required to behold for arbitrary $\mathbf{p}$ and $\{b_i\}_i$. However, inspecting (14) offers very limited insights into the specific functional form of an optimal u_{AMM}. To grasp more intuitions, let us consider an interesting example and derive the corresponding u_{AMM} below.

Example 3 Suppose that LPs are all single-minded agents and the utility preference function of each LP is either

$$u_i(x_1,x_2)=x_1\quad or\quad x_2.$$

Moreover, for simplicity, we assume LPs have an identical budget, $b>0$. Thus, for any given price vector $\mathbf{p}=(p,1)$, the reservation utilities of a type-1 LP and a type-2 LP will be

$$\hat{u}_1=\frac{b}{p}\quad\text{and}\quad\hat{u}_2=b,$$

respectively.

Instead of managing their budgets independently, suppose all LPs pool their funds into a single liquidity pool, managed by an LP representative. What will be the consumption plan made by this LP representative then? To answer, suppose that there are n_1 LPs of type-1 and n_2 LPs of type-2. We know that independent of market prices, a type-1 LP always allocates the entire budget to purchasing crypto A. Consequently, it is reasonable to infer that the LP representative would allocate the combined budgets of all type-1 LPs, denoted as $\sum_{k=1}^{n_1} b_{i_i} = n_1 b$, towards acquiring crypto A, mirroring the investment strategy of type-1 LPs regardless of the price vector $\mathbf{p}$. A similar rationale applies to the investment behaviours of type-2 LPs. Integrating the interests of both types of LPs into the decision-making framework of the LP representative, we conjecture that LP representative exhibits a Cobb-Douglas preference, say $u_{AMM}(x_1, x_2) = x_1^{\lambda} x_2^{1-\lambda}$, where $\lambda = \frac{\sum_{k=1}^{n_1} b_{i_i}}{\sum_i b_i} = \frac{n_1}{n_1+n_2}$. This proportion λ reflects the budgetary emphasis placed on crypto A by type-1 LPs relative to the total budget. The validity of this conjecture can be easily verified by solving an optimization problem given below:

$$\begin{aligned} \underset{(x_1,x_2)}{Max} \quad & u_{AMM}(x_1, x_2) = x_1^{\frac{n_1}{n_1+n_2}} x_2^{\frac{n_1}{n_1+n_2}} \\ \textit{subject to} \quad & p x_1 + x_2 \leq \sum_{i=1} b = (n_1 + n_2) b. \end{aligned}$$

Therefore, to well represent a population of n_1 type-1 LPs and $n - n_1$ type-2 LPs to exchange assets with external liquidity demanders, the representative LP should behave as an agent with Cobb-Douglas preference function given by $u_{AMM}(x_1, x_2) = x_1^{\frac{n_1}{n_1+n_2}} x_2^{\frac{n_2}{n_1+n_2}}$. For general cases beyond single-minded LPs, we have the following characterization.

Proposition 2 (optimal u_{AMM}). *For a group of LPs who have homothetic preference profile $\{u_i\}_i$ and budget profile $\{b_i\}_i$, the aggregate preference u_{AMM} satisfying condition (14) exists, and it reads as*

$$u_{AMM}(\boldsymbol{x}, \boldsymbol{y}) = \underset{\{x_i, y_i\}_i}{Max} \left\{ \Pi_i \left(\frac{u_i(x_i, y_i)}{\beta_i} \right)^{\beta_i} \;\middle|\; \sum_i (x_i, y_i) = (\boldsymbol{x}, \boldsymbol{y}) \right\}, \tag{15}$$

where $\beta_i = \frac{b_i}{\sum_i b_i}$ is the fractional ownership of each LP i for the liquidity pool.[13] *Moreover, based on this optimal aggregate preference u_{AMM}, we can characterise the optimal pricing schedule $T(\cdot)$ and the optimal set of admissible trades in the following sense:*

$$S_{AMM}\left(\boldsymbol{p}, \boldsymbol{b}\right) = \Big\{ (q, T(q)) : u_{AMM}(\boldsymbol{x} - q, \boldsymbol{y} + T(q)) = u_{AMM}(\boldsymbol{x}, \boldsymbol{y}) \Big\}. \tag{16}$$

The proof of this lemma is omitted here as it is an application of the results established by Eisenberg (1961)[22] for any population of consumers with homothetic preferences, or Eisenberg and Gale (1959)[23] in the context of probabilistic forecast aggregation.

[13] For notation simplicity, in Lemma 1, we take $(x_i, y_i) := (x_i(\mathbf{p}, b_i), x_i(\mathbf{p}, b_i))$, $\mathbf{b} = \sum_i b_i$ and $(\mathbf{x}, \mathbf{y}) := (\mathbf{x}(\mathbf{p}, \mathbf{b}), \mathbf{y}(\mathbf{p}, \mathbf{b}))$

Inspecting the form of the aggregate preference u_{AMM} in (15), one can observe a resemblance to the maximal weighted Nash social welfare. For those familiar with the remarkable work of Nash (1950)[40], in this work Nash introduces a social welfare function that equals the product of each player's utilities to characterize the equilibrium outcome in axiomatic bargaining games. Generalizing Nash's work leads to the concept of weighted Nash social welfare, where the weight assigned to each consumer's utility is her relative budget. The Nash welfare concept provides a key insight into the optimality of our bonding curve function u_{AMM}: Rather than following the ad hoc proportional fair allocation where only LPs' liquidity ownership is considered, our asset allocation rule implied in the functional form of u_{AMM} is superior as it allocates assets to LPs based on both their respective ownership to the liquidity pool and their heterogeneous preferences over cryptos A and B.

To assess the efficiency of our optimal u_{AMM}, including its trade allocative efficiency and liquidity withdrawal efficiency, let us assume that the state of liquidity pool updates from (x, y) to $(x-q, y+\tau(q))$ after some trading activities at this DEX. We know that LP representative with preference u_{AMM} would design her set of admissible trade as follows

$$\begin{aligned}S_{AMM} &= \Big\{(q,\tau(q)): \quad u_{AMM}(x-q, y+\tau(q)) \geq u_{AMM}(x,y) := k\Big\},\\ &= \Big\{((q,\tau(q)): \quad \underset{\{x_i,y_i\}_i}{Max}\ \Pi_i \left(\frac{u_i(x_i,y_i)}{\beta_i}\right)^{\beta_i} \geq k \quad \textit{subject to}\\ &\sum_i (q_i,\tau_i(q_i)) = (q,\tau(q)) \ \ \textit{and} \ \sum_i (x_i,y_i) = (x-q, y+\tau(q))\Big\}. \end{aligned} \tag{17}$$

The existence of u_{AMM} in (15) implies the existence of an optimal allocation $(x_i^\star, y_i^\star)_i$ that maximises the weighted product of LPs' utilities in (17), thereby achieving liquidity withdrawal efficiency. By using $(x_i^\star, y_i^\star)_i$, we can derive the trade allocation among LPs, denoted as $q_i^\star := x_i - x_i^\star$ and $\tau_i^\star(q_i) := y_i^\star - y_i$. Now, let us turn attention to checking whether the trade allocation $\{q_i^\star, \tau_i^\star\}_i$ satisfy LPs' participation constraints. Recall that u_{AMM} in Lemma 1 is a weighted Nash social welfare function, and therefore Pareto efficient, as established by Eisenberg and Gale (1959)[23] or Kaneko and Nakamura (1979)[34]. This implies that

$$u_{AMM}(x-q, y+\tau(q)) \geq u_{AMM}(x,y) \implies u_i(x_i - q_i^\star, y_i + \tau_i^\star(q_i) = u_i(x_i^\star, y_i^\star) \geq u_i(x_i, y_i)$$

for every i, thereby stratifying the participation constraints and achieving trade allocative efficiency[14].

To conclude this section, we have characterized the optimal bonding curve function u_{AMM} in a DEX built by heterogeneous LPs. This optimal u_{AMM} is structured as a

[14] Indeed, LPs' participation constraints are automatically satisfied under the allocation rule implied in u_{AMM}, since the set of admissible trades given by S_{AMM} in (16) is a subset of the original Minkowski sum $\hat{S}_{AMM}(\mathbf{p}, \mathbf{b})$, and we note that all trades contained therein already are participation constrained

weighted product of LPs' preferences, with weights reflecting their fractional ownership of the liquidity pool. Its functional form aligns well with the economic intuition found in the aggregate consumer literature, which motivates us to interpret u_{AMM} as the preference of an LP representative within the DEX. However, it is essential to note that a clear micro foundation for this optimal u_{AMM} is currently lacking. Specifically, it remains unclear why LPs grouped in a DEX would unanimously agree to accept a bonding curve function structured as a weighted product of their preferences. Addressing this gap raises an interesting and important question: How can we implement the optimal bonding curve u_{AMM} as an equilibrium among LPs? Addressing this question will be our central focus in the next section.

5 Implementing Optimal Trading Mechanism

Up to this point, we have characterized the optimal trading mechanism in a DEX with heterogeneous LPs and explored its various representations. These representations include the optimal pricing schedule in the social planner problem ($\tau(q)$), the optimal bonding curve function (u_{AMM}), and the set of admissible trades for LP representative (S_{AMM}). However, a crucial question remains: Can any of these equivalent representations be implemented as an outcome in the practical decision-making process of DEXs? Alternatively, from a game theoretical perspective, is it feasible to implement our optimal trading mechanism as an equilibrium among LPs in DEXs? Answering this implementation question requires a comprehensive understanding of the typical decision-making process in DEXs. As one of the most prominent decentralized autonomous organization (DAO) applications, DEXs feature decentralized governance. This means that the DEX is collectively owned and managed by LPs through decision-making and economic rights derived from their liquidity contribution to the DEX. For instance, Uniswap, the largest DEX, empowers LPs to vote on proposals via the Ethereum blockchain to decide on any new platform design, referring to Han et al. (2023)[28] for a deeper DAO governance introduction.

Beyond the decision-making process in real DEXs practices, we also rely on a twofold economic intuition for determining our specific implementing framework: On the one hand, upon examining the set of admissible trades S_{AMM}, we observe that optimally allocating a given trade request $(q, \tau(q))$ among LPs in a DEX is equivalent to optimally allocating the post-trade liquidity pool among them. This equivalence arises due to the transformation of pool states from (x, y) to $(x - q, y + \tau(q))$ following a trade. So, we conceptualize the problem of dividing the post-trade pool allocation among LPs as a bargaining game. On the other hand, as mentioned in the last section, the optimal post-trade allocation solution outlined in Lemma 1 involves maximizing the weighted product utilities of LPs. This weighted product of utilities resembles a typical Nash social welfare, often rationalized by a bargaining game in the literature. Therefore, these two observations collectively inspire us to consider a Nash bargaining game over heterogeneous LPs for the implementation of our optimal bonding curve function u_{AMM}.

5.1 N-person Nash Bargaining Solution

To start, let us specify the definition of an N-person Nash bargaining problem and its solution concept. Suppose the post-trade liquidity pool is $\mathcal{R} = (\mathbf{x} - q, \mathbf{y} + T(q))$ and n LPs bargain over the division of this post-trade liquidity pool. Then the set of possible agreements is

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

where x_i and y_i are the respective amounts of cryptos A and B in the liquidity pool staked by LP i. Alternatively, we can have the feasible set of utilities as

$$V = \Big\{ (z_i)_i \in \mathbb{R}_+^n \quad | \quad \exists (x_i, y_i)_i \in X, \forall i, z_i \leq u_i(x_i, y_i) \Big\}. \tag{18}$$

For simplicity, we assume that the disagreement point in our Nash bargaining problem is denoted as $d = (d_i)_i = 0$[15]. For each Nash bargaining problem $(V, \{u_i\}_i)$, we define its solution as follows.

Definition 1 (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 $z^\star(\beta) = \big\{z_i^\star(\beta)\big\}_i = \big\{u_i(x_i^\star, y_i^\star)\big\}_i \in V$ is called the Nash bargaining solution of $(V, \{u_i\}_i, \theta)$ if $z^\star$ solves the following optimization problem*

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

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,

$$\underset{(x_i, y_i)_i \in X}{max} \quad \Pi_i \left(u_i(x_i, y_i)\right)^{\beta_i} \tag{19}$$

[15] 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)[34]. So the more natural and intuitive way to define the disagreement point in this paper is taking $d = (d_i)_i = \Big(D_i(\mathbf{p}, b_i)\Big)_i$ where $D_i(\mathbf{p}, b_i)$ 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 $d = \Big(D_i(\mathbf{p}, b_i)\Big)_i$ are both interior points in V and play the same role in guaranteeing the existence of a non-trivial solution.

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 problem was first proposed by Nash (1950, 1953)[40, 39] for a two-person case and later extended by Hart and Mas-Colell (1996)[29] for an n-person case. In contrast, the asymmetric Nash bargaining problem was considered by Binmore, Rubinstein, and Wolinsky (1986)[14] for the two-person case, where game asymmetry arises from different beliefs about the risk of negotiation breakdown. More recently, several studies, including Okada (2010)[41], Britz et al.(2010)[15], and Kawamori (2014)[35], have explored solution concepts in n-person asymmetric Nash bargaining problems and rationalized their solutions by presenting some non-cooperative game foundations. In this paper, we connect our implementation work to this literature by modelling the decision-making process in a decentralised governed DEX as an n-person asymmetric Nash bargaining problem, where the asymmetry in bargaining power between LPs originates from their asymmetrical liquidity contributions to the liquidity pool.

5.2 Bargaining Procedure in the Community of LPs

With Definition 1 at our disposal, a clear similarity emerges between the optimal post-trade allocation outlined in Lemma 1 and the Nash bargaining solution concept. Consequently, it becomes equivalent to establishing a noncooperative bargaining game between LPs, aiming to yield a Nash bargaining solution that precisely mirrors the optimal post-trade allocation solution. The next step is to identify an appropriate and specific Nash bargaining game framework: This framework should effectively capture the competition among LPs in the decision-making process of a DEX, characterized by decentralized governance. Moreover, it must account for the asymmetric bargaining powers between LPs, resulting from their asymmetrical liquidity contributions to the pool.

To start, let $\rho \in (0, 1)$ be a fixed parameter. There are potential infinite rounds in this bargaining procedure. 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.[16]

- 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

[16] 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.

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, Osborne, and Rubinstein (1992)[13][17]. 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, LPs have perfect information about the historical actions made by all LPs. One should note that this public information assumption is very strong. However, this concern is mitigated in the context of a public blockchain-based platform, such as DEXs. This is because, DEXs, running on Ethereum and leveraging blockchain technology, guarantee transparency in trade activities, and governance schemes, and even expose the underlying code to the public.

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,

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

Following the literature on noncooperative multi-person sequential bargaining games, we only study the stationary subgame perfect equilibrium (SSPE) denoted as $\sigma^\star =$

[17] 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 $r_i = \frac{1}{\beta_i}$.

$(\sigma_1^\star, .., \sigma_n^\star)$ 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 3 (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 the Appendix, 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.

As emphasized earlier, the optimal u_{AMM} is characterized as a weighted product of LPs' utility preferences, with each LP's weight aligning with her liquidity contribution to the pool. Through the lens of our implementation result in this proposition, the emergence of asymmetric bargaining powers among LPs within a DEX platform becomes evident, which is entirely driven by their asymmetrical liquidity ownership in the pool. This asymmetrical liquidity ownership determines their respective probability of being chosen as the proposer in every bargaining round.

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 how a group of LPs determines the trading mechanism design in DEX. 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 N-person 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 for future studies seeking to understand the crucial trade-off between decentralized governance and welfare efficiency in DAOs.

To conclude, we establish an economic microfoundation for the novel decision-making process in DEXs, a typical DAO 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 made by LPs, 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 our optimal bonding curve u_{AMM} can be implemented as an equilibrium among LPs, where their bargaining power is determined by their respective liquidity ownership in the pool, adhering the "one token, one right" DAO principle.

6 Extension One: Oligopolistic DEXs

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 LD opts to trade on this particular DEX. However, what if there exists liquidity provision 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.

6.1 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 $q = \sum_{i=1}^{I} q_i$. Clearly, 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. *We assume that $u(q, \theta)$ follows a mean-variance structure, say,*

$$u(q, \theta) = -\frac{\lambda}{2}(\theta - q)^2 - (-\frac{\lambda}{2}\theta^2) \\ = \lambda\theta q - \frac{\lambda}{2}q^2, \tag{20}$$

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 and Skrzypacz (2016), Chen and Duffie (2021)[18] and Rostek and Yoon (2021)[44], 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.

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 $t = 3$.

[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, Martmort, and Rochet (2000)[11].

6.2 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.

$$\textbf{LD's problem:} \quad \underset{\{q_j\}_{j=1}^J}{Max} \; u(q(\theta),\theta) - \sum_j T_j(q_j(\theta)) = \lambda\theta q - \frac{\lambda}{2}q^2 - \sum_j T_j(q_j(\theta))$$
$$\textit{subject to} \quad q_1(\theta) + q_2(\theta) + ... + q_J(\theta) = q(\theta), \tag{21}$$

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

$$\textbf{[IC condition:]} \quad \theta \in \underset{\hat{\theta}}{Argmax}\left(\lambda\theta q(\hat{\theta}) - \frac{\lambda}{2}q(\hat{\theta})^2 - \sum_j T_j(q_j(\hat{\theta}))\right). \tag{22}$$

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:

$$\textbf{[PC condition:]} \quad \pi(\theta) \geq \pi_{-k}(\theta), \tag{23}$$

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

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

[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 $T^{''} \geq 0$.

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:

$$\textbf{DEX k's Problem:} \quad \underset{T_k(\cdot)}{Max} \; B_k(T_1, ..., T_J) \tag{24}$$
$$:= \int_{\underline{\theta}}^{\bar{\theta}} \left\{ \left[u^k_{AMM}\Big(\bar{x} - q_k(\theta), \bar{y} + T_k(q_k(\theta))\Big) - u^k_{AMM}(\bar{x}, \bar{y}) \right] + \gamma T_k(q_k(\theta)) \right\} dF(\theta),$$

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. *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 size-q trade made by an 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

$$\textbf{DEX k's Problem:} \quad \underset{T_k(\cdot)}{\text{Max}} \; B_k(T_k, T_{-k}) = \int_{\underline{\theta}}^{\bar{\theta}} 2\gamma T_k\Big(q_k(\theta) : T_{-k}\Big)\, dF(\theta), \tag{25}$$

where the term involving the utility increment in (24) 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 by 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 $\{F_1, ..., F_J\}$. In fact, 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, Martmort, and Rochet (2000) [11]. 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, Martmort, and Rochet (2000) [11], 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 (25), 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, Martmort, and Rochet (2000) [11].

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.

7 Extension Two: Reporting Preferences Truthfully

Let us now address one of the major concerns regarding our implementation result. Recall that our implementation in section 5 relies on achieving equilibrium through a Nash bargaining game where the utility preferences profile of LPs has to be assumed as publicly available for mechanism designers. Specifically, one can see that the optimal bonding curve design, say the weighted product of LPs' preferences, in our Proposition 2 is entirely determined by two sets of information: the preferences profile of LPs $\{u_i\}_i$ and the exact amounts of cryptos A and B deposited by each LP $\{(x_i, y_i)\}_k$. The latter information about the number of cryptos deposited by LPs is public in the DEX platform, whereas the former LP's preference information is privately observed. Moreover, the domain of LPs' preference function could be very general in mathematics, making inferring and eliciting this preference information almost impossible for mechanism designers.

Given that, we believe an alternative but also more practical approach to acquiring this preference information is to ask LPs to report their preferences directly. Then, a natural, important question arises: How do the mechanism designers incentivize LPs to report their utility preferences truthfully? This will be the central focus of this section.

To address this question, we extend our implementation result by introducing a partial allocation mechanism, serving as the pre-bargaining stage in the aforementioned Nash bargaining game. In practice, this preference information collection process implies that LPs are required to simultaneously report their preferences over bundles of cryptos or equivalently their utility preference functions when staking cryptos into the DEX. We demonstrate and prove later in this section that truthfully reporting preference would be a dominant strategy for every LP in our pre-bargaining stage.

Incentivising agents to truthfully report their preferences brings to mind the classical Vickrey–Clarke–Groves (VCG) mechanism, introduced by Vickrey (1961) [47], Clarke (1971) [20], and Groves (1973) [26]. The key features of the VCG mechanism include the fact that truthfully reporting valuations for possible outcomes is the dominant strategy for all agents, and it achieves the socially optimal utilitarian solution by maximizing the sum of agents' utilities. However, in contrast to the classical VCG mechanism, which aims to achieve utilitarian welfare (the sum of agents' utilities), our objective here is to attain Nash social welfare (a weighted sum of agents' utilities). To highlight this distinction, let's first provide a summary of what a typical VCG mechanism would look like in the context of our DEX allocation problem.

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 this 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,

$$p_i = \frac{1}{\beta_i} \sum_{j \neq i} \beta_j u_j(x^\star). \tag{26}$$

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.

As mentioned earlier, the social welfare function in the DEX should be the Nash social welfare, a weighted product of LPs' utility, 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, one will see that what we only need to do is just follow the same steps but change every sum operational in the VCG mechanism to a product operational correspondingly. Let us name this new mechanism a partial allocation mechanism and illustrate its structure specifically below.

Goal of our partial allocation 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 partial allocation 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

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

The partial allocation mechanism for Nash social welfare. The second difference of our partial allocation mechanism to the typical VCG mechanism is that if the final allocation output is $x^\star = (x_i^\star, y_i^\star)_i$, this mechanism only gives 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 this mechanism will be

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

Next, we need to specify how to construct a suitable $f_i(\cdot)$, and why our partial allocation mechanism motivates LPs to truthfully report their utility preferences, achieving the Nash social welfare goal.

The partial allocation 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

$$f_i = \Big(\Pi_{j \neq i} u_j(x^\star)^{\beta_j}\Big)^{\frac{1}{\beta_i}}. \tag{27}$$

Armed with this partial allocation mechanism, we have the following proposition.

Proposition 5 (Truthfully Reporting). *In the partial allocation mechanism 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, weighted Nash social welfare among LPs with the weight vector $(\beta_i)_i$.

Proof. Let us begin with the proof for part (II) where we can apply a similar argument as the above VCG mechanism case and show that steps 1'-3' here indeed implement Nash social welfare with the weights $\{\beta_i\}_i$.

The trick is in step 3'. Suppose that the final allocation implied in the Nash social welfare function is $x^\star$, then the total utility payoff of LP i in this partial allocation mechanism is

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

Taking a power of β_i on both sides yields that

$$\Big(\hat{u}_i(x^\star)\Big)^{\beta_i} = \Big[\Big(\Pi_{j \neq i} u_j(x^\star)^{\beta_j}\Big)^{\frac{1}{\beta_i}} u_i(x^\star)\Big]^{\beta_i} = \Pi_i u_i(x^\star)^{\beta_i}, \tag{28}$$

where the very left-hand side is the goal of our partial allocation mechanism, say, the weighted Nash social welfare of the DEX society. Hence, each LP has her interests aligned with those of the Nash social welfare planner. So the weighted Nash social welfare of the society will be achieved If LPs are incentivized to truthfully report 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, in step 2', denoted by the final allocation output by partial allocation mechanism $x^\star_T$ if LP i truthfully reports her preference, or $x^\star_F$ otherwise. Correspondingly, step 3' returns the fraction $f_T(x^\star_T)$ if LP i truthfully reports, or fraction $f_F(x^\star_F)$ otherwise.

To prove truthfully reporting her preference as a dominant strategy, what we need to show is that

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

Using the definition of f_T and f_F, our problem therefore reads as

$$u_i(x^\star_T)^{\beta_i}\Pi_{j\neq i}\bar{u}_j(x^\star_T)^{\beta_j} \geq u_i(x^\star_F)^{\beta_i}\Pi_{j\neq i}\bar{u}_j(x^\star_F)^{\beta_j}. \tag{29}$$

Verifying this inequality is immediately due to that $x^\star_T$ is defined as the maximiser to the weighted product of the corresponding reported preferences of LPs in step 2'. That is,

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

where remark that any LP $j \neq i$ is allowed to report any preference $\hat{u}_j$ that may differ from her true one u_j. As a result, reporting her true preference is a dominant strategy for every LP. Proof completes. □

8 Conclusion

Taking an oligopolistic competition framework between DEXs and adopting a decentralised governance scheme within each DEX, this paper has established an economic microfoundation for the prevalent *ad hoc* bonding-curve-based AMM trading mechanism. The consideration of heterogeneity among LPs, specifically through utility preference and liquidity contribution dimensions, has shown the potential sub-optimality associated with the simplistic bonding curve algorithms at DEXs, at the cost of trade allocation efficiency.

Through the study of a social planner problem, this paper has revealed the necessity of an optimal trading mechanism at a DEX that accounts for the asymmetry in LPs' liquidity contribution and their diverse utility preferences. Assuming homothetic preferences among LPs, we have proved that an optimal bonding curve design can be realized, structured as a weighted product of LPs' utility preference functions, with weights reflecting their fractional ownership in the DEX. Furthermore, we have developed a specific decentralised governance process a là N-person Nash bargaining game for implementing this optimal bonding curve design at a DEX.

Several important extensions remain to be pursued for future research. For instance, on the liquidity-demand side, what implications arise if prospective liquidity demanders are informed of the fundamental value of risky cryptos? How might the optimal pricing schedule be affected in the presence of more than one liquidity demander for each transaction (or block in reality)? On the liquidity-supply side, how might our implementation findings be altered in the presence of a pivotal or dictatorial LP within the DEX community? Lastly, how does competition unfold when we have asymmetric oligopolistic DEXs?

9 Appendix

9.1 Proof for Lemma 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:

$$u_{AMM}(x-q, y+\tau(q)) = u_{AMM}(x,y) \quad \Longrightarrow \quad u_i(x_i - \beta_i q, y_i + \beta_i \tau(q)) \geq \pi_i \ \ \forall i, \tag{30}$$

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 (30) 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:

$$u_i(x_i, y_i) = u_i\Big(x_i - \beta_i q, y_i + \beta_i \tau(q)\Big) = \frac{1}{n} u_i\Big(x - q, y + \tau(q)\Big) \geq \pi_i, \tag{31}$$

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 (31) by a factor n and then rearranging its order yields that

$$u_i\Big(x - q, y + \tau(q)\Big) = n u_i(x_i, y_i) = u_i\Big(nx_i, ny_i\Big) = u_i(x,y) \quad \forall i, \tag{32}$$

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

$$u_{AMM}(x-q, y+\tau(q)) = u_{AMM}(x,y). \tag{33}$$

Taking all the results above together immediately leads to a contradiction. Notably, conditions (32) and (33) hold for any $x, y, q, T(q)$. However, the former condition (32) depends on u_i, whereas the latter condition (33) 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. □

9.2 Proof of Proposition 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,

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

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

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

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

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

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:

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

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 $q > 0$.

□

9.3 Proof for Proposition 3

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.

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

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 together 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

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

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

$$\lim_{\rho \to 1} \ x_i(\rho) = z^\star = \lim_{\rho \to 1} \ x_j(\rho). \tag{34}$$

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

$$\frac{z_i^\star}{\beta_i}F_i(z^\star) = \frac{z_j^\star}{\beta_i}F_j(z^\star) \tag{35}$$

for any $i, j \in \{1, 2, ..., n\}$, where we derive the above equality by relying on the fact in (34), say, for any k, $\lim\limits_{\rho \to 1} \; x_i(\rho) = z^\star$.

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

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

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 (35), 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. □

References

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

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

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

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

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

[6] Jun Aoyagi and Yuki Ito. Coexisting exchange platforms: Limit order books and automated market makers. *Available at SSRN 3808755*, 2021.

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

[8] Ana Babus and Cecilia Parlatore. Strategic fragmented markets. *Journal of Financial Economics*, 145(3):876–908, 2022.

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

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

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

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

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

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

[15] 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.

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

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

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

[19] 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.

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

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

[22] Edmund Eisenberg. Aggregation of utility functions. *Management Science*, 7(4):337–350, 1961.

[23] Edmund Eisenberg and David Gale. Consensus of subjective probabilities: The pari-mutuel method. *The Annals of Mathematical Statistics*, 30(1):165–168, 1959.

[24] 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.

[25] 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.

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

[27] Jianlei Han, Shiyang Huang, and Zhuo Zhong. Trust in defi: an empirical study of the decentralized exchange. *Available at SSRN 3896461*, 2022.

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

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

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

[31] Joel Hasbrouck, Thomas J Rivera, and Fahad Saleh. The need for fees at a dex: How increases in fees can increase dex trading volume. *Available at SSRN*, 2022.

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

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

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

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

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

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

[38] Semyon Malamud and Marzena Rostek. Decentralized exchange. *American Economic Review*, 107(11):3320–3362, 2017.

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

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

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

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

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

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

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

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

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

[48] 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.

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