Wharton
University of Pennsylvania
Initiative on Financial Policy & Regulation

The Evolution of Decentralized Exchange: Risks, Benefits, and Oversight

Campbell R. Harvey, Joel Hasbrouck, and Fahad Saleh

Abstract

A decentralized exchange or DEX is an application deployed on a blockchain that allows investors to exchange digital assets at pricing terms determined by a preset exchange rate formula. This technology has several unique features, including accessibility to all investors, transparency of pricing, and simultaneity of execution and settlement. Notably, trading via a DEX is feasible for any asset tokenized on a blockchain. In turn, given that assets such as stocks and bonds could be tokenized easily, it is particularly important to understand the risks posed by DEXs. This paper examines both the benefits and risks to investors from DEXs, explores the role of private and public liquidity pools and analyzes possible regulatory approaches.

Campbell R. Harvey is J. Paul Sticht Professor of Finance at Fuqua School of Business, Duke University.

Joel Hasbrouck is Kenneth G. Langone Professor of Business at the Stern School of Business, New York University.

Fahad Saleh is Associate Professor of Finance at the University of Florida.

The **Wharton Initiative on Financial Policy and Regulation** is directed by **Itay Goldstein**, the Joel S. Ehrenkranz Family Professor and Professor of Finance at The Wharton School of the University of Pennsylvania. It commissions white papers from leading and emerging experts on a range of topics on financial policy and regulation. For more, see https://wifpr.wharton.upenn.edu/

Wharton Initiative on Financial Policy and Regulation White Paper

The Evolution of Decentralized Exchange: Risks, Benefits, and Oversight*

Campbell R. Harvey† Joel Hasbrouck‡ Fahad Saleh§

Duke University and NBER *NYU Stern* *University of Florida*

Abstract

A decentralized exchange or DEX is an application deployed on a blockchain that allows investors to exchange digital assets at pricing terms determined by a preset exchange rate formula. This technology has several unique features, including accessibility to all investors, transparency of pricing, and simultaneity of execution and settlement. Notably, trading via a DEX is feasible for any asset tokenized on a blockchain. In turn, given that assets such as stocks and bonds could be tokenized easily, it is particularly important to understand the risks posed by DEXs. This paper examines both the benefits and risks to investors from DEXs, explores the role of private and public liquidity pools and analyzes possible regulatory approaches.

Keywords: *Decentralized exchange, DEX, Decentralized finance, DeFi, Centralized exchange, CEX, Smart contracts, Uniswap, Limit-order book, Front running, Sandwich attack, Just-In-Time liquidity, Trading fees, Slippage, Bid-ask spread, Liquidity, Proposer, Builder, Relayer, Private pools, DEX aggregator.*

JEL Classification: *G10, G23, G28*

*October 16, 2024. We thank Viktor Bunin, Lewis Cohen, Itay Goldstein, Yuliya Guseva, Max Harris, Trevor Kiviat, Evgeny Lyandres, Timothy Massad, Barnabé Monnot, Joey Santoro, Lee Schneider, Xin Wan, Aviv Yaish, David Yermack, Anthony Lee Zhang, and participants at the WIFPR Roundtable for valuable comments.

†email: cam.harvey@duke.edu

‡email: jh4@stern.nyu.edu

§email: fahad.saleh@ufl.edu

1 Introduction

A Decentralized Exchange (DEX) is an important financial innovation. In contrast to a centralized exchange, a DEX is accessible to all investors, provides transparent trading terms, and offers trade execution and settlement simultaneously. Nonetheless, irrespective of these advantages, a DEX entails a variety of novel risks for investors, and those risks must be understood prior to forming an appropriate regulatory policy. In this paper, we detail both DEX investor benefits as well as risks and thereafter discuss potential regulatory approaches.

Nakamoto (2008) introduced the idea of a decentralized peer-to-peer payment system with the Bitcoin blockchain. However, the Bitcoin blockchain does not allow for the deployment of DEXs. Rather, a key innovation in blockchain technology, largely attributable to Buterin (2014) and Wood (2014), was the introduction of the Ethereum blockchain. Ethereum provides the same functionality as the Bitcoin blockchain in terms of peer-to-peer transactions but also adds a further functionality: the ability to deploy a computer program onto the blockchain. These computer programs operating on a blockchain are known as *smart contracts*, the importance of which is that blockchain users can interact with these computer programs, thereby facilitating a rich set of user interactions.

One interaction made feasible by smart contracts is trading assets at transparent pricing terms. This interaction is facilitated through a DEX, which is a set of inter-related smart contracts that interact to facilitate trading. Any blockchain user can interact with a DEX by submitting an order with a trade size and a trading direction. The pricing terms of the trade are then determined mechanically and transparently by an algorithm encoded into a smart contract. The pricing algorithm is known as an *Automated Market Maker (AMM)*, and the mechanics of this algorithm are known publicly precisely because they are defined explicitly in a smart contract.[1]

A DEX generally consists of *liquidity pools* wherein each pool is defined by a set of assets across which it facilitates trading. Each pool can hold only a fixed set of assets, and trading is facilitated through a pool by allowing users to exchange some of the assets held by the pool for other assets held by the pool. As an example, a two-asset pool consisting of ETH

[1] Although the AMM pricing function is predetermined and transparent, the actual terms of trade are not finalized until the user's trade is added to the blockchain. The state of the AMM and blockchain at that point may differ from that observed by the user when the order was submitted. To protect against adverse price movements, the user may attach a limit price (or, equivalently, a *slippage tolerance*) that will prevent execution at a price that would breach the limit or tolerance. As with a traditional limit order, however, the user has essentially written an option that can be exercised at the discretion of anyone who possesses the ability to interact with it (as the order passes through the block-building process). Until the order has been added to the block, therefore, it is exposed to the risk of being picked off. A more restrictive limit price or slippage tolerance can provide more protection against this risk, but only by increasing the probability (and opportunity cost) of a failed execution attempt. We elaborate in Section 3.2.

and DAI is a pool that can hold only ETH and DAI. A user interacting with an ETH-DAI pool can purchase ETH for DAI by receiving ETH from the pool and providing DAI to the pool in return. Similarly, a user can sell ETH for DAI by receiving DAI from the pool and providing ETH to the pool in return. The specific amount of DAI (ETH) to be provided to the pool for receiving a given amount of ETH (DAI) is determined by an AMM.

In general, an AMM determines pricing terms by maintaining a particular invariant. The most common invariant is a *constant product* invariant where the product of the various asset holdings of the pool is held invariant before and after a trade. To give an example, for an ETH-DAI pool, a constant product AMM (CPAMM) maintains the product of ETH units and DAI units held by the pool as invariant across a trade. In particular, if there are initially x ETH units and y DAI units held by the pool, then the product of ETH units and DAI units must remain equal to $x \cdot y$ after any trade. If a user submits an order to buy δ_x units of ETH, that order reduces the ETH units held by the pool to $x - \delta_x$ and thereby requires an increase in DAI units to maintain the constant product invariant. Direct verification reveals that the user must add $\frac{x \cdot y}{x - \delta_x} - y$ DAI units to the pool because this addition increases the pool's DAI holding to $\frac{x \cdot y}{x - \delta_x}$ which thereby maintains the product of ETH units and DAI units at $(x - \delta_x) \cdot \frac{x \cdot y}{x - \delta_x} = x \cdot y$ after the trade. So, if there are initially $x = 5$ ETH units and $y = 20$ DAI units, then the constant product that must be maintained after a trade is $5 \cdot 20 = 100$. In turn, a trade to buy $\delta_x = 1$ ETH unit requires a payment of $\frac{x \cdot y}{x - \delta_x} = \frac{100}{5-1} - 20 = 5$ DAI units because the purchase of 1 ETH unit reduces the pool ETH holding to $5 - 1 = 4$ and providing 5 DAI units increases the pool DAI holding to $20 + 5 = 25$, thereby maintaining the constant product invariant of $100 = 4 \cdot 25$.

For a liquidity pool to function, the pool must acquire some inventory of the assets that characterize the pool. For example, an ETH-DAI pool must acquire both ETH inventory and DAI inventory; otherwise, such a pool could not facilitate exchanges of ETH for DAI or vice versa. A liquidity pool acquires its inventory from investors who obtain the assets separately (e.g., at a centralized exchange) and then provide those assets to the liquidity pool. This investor behavior is incentive compatible because each liquidity pool charges trading fees and passes those fees onto investors who provide the pool with inventory. Although investors providing inventory to a liquidity pool earn trading fees, they also incur a loss known as *Loss-Versus-Rebalancing* (LVR), which was first highlighted by Milionis, Moallemi, Roughgarden, and Zhang (2022) and is explained below. Ultimately, the liquidity provision for a liquidity pool is an equilibrium quantity, and it is determined as the level at which investors are indifferent between providing liquidity to the liquidity pool and investing their capital in other investment opportunities. For a formal economic analysis of equilibrium liquidity provision at a liquidity pool, see Capponi and Jia (2021), Lehar and Parlour (2021)

and Hasbrouck, Rivera, and Saleh (2023).

LVR is a loss experienced by investors providing inventory to a liquidity pool due to arbitrageurs trading at off-market prices against the liquidity pool. Liquidity pool pricing is determined by an AMM that implements a mechanical pricing rule. The AMM mechanical pricing rule does not directly incorporate public information so that prices implied by an AMM do not directly update upon the release of news. Rather, prices implied by the AMM change only as a function of the asset holdings of the associated liquidity pool, whereas the relative asset holdings change due to trading. In turn, upon the release of public information, arbitrageurs are able to trade against a liquidity pool at prices that do not reflect the new public information. This arbitrage trading then alters the asset holdings of the liquidity pool in such a way that the liquidity pool's price begins to incorporate the public information. The arbitrage trading ends only when the liquidity pool's price has adjusted sufficiently to eliminate further arbitrage opportunities. Importantly, investors who provide inventory to a liquidity pool become partial owners of the overall inventory at the liquidity pool. Therefore, such investors experience losses to the extent that the liquidity pool incurs trading losses through trades at off-market prices. Milionis et al. (2022) examine these losses, demonstrating that they increase with the volatility of the exchange rate between the assets in a two-asset liquidity pool. In turn, Hasbrouck, Rivera, and Saleh (2022) and Cao, Hemenway Falk, and Tsoukalas (2023) discuss the need for trading fees at a liquidity pool to be set such that they offset those losses.[2]

Trading via an AMM offers various advantages. First, due to the mechanical implementation of AMMs, terms of trade are highly transparent. The assets of the underlying liquidity pool are held directly by pool investors, and while these investors are exposed to market risk, the pool assets cannot be misappropriated. Second, settlement of AMM trades normally occurs on the blockchain within at most a few minutes. This contrasts with traditional markets, where settlements delays are often a day or more. These advantages have led to the consideration of AMMs as supplements for traditional markets. In the interbank foreign exchange market, the Bank for International Settlements' Project Mariana demonstrated the technical feasibility of AMMs for cross-border trading and settlement of wholesale central bank digital currencies (Bank for International Settlements, 2023). Malinova and Park (2023) suggest that AMMs could provide efficient trading of tokenized US equities, particularly for smaller firms. They also contend that, if applied to traditional markets, an AMM could significantly reduce trading costs by allowing passive investors to provide their asset

[2]A concept related to loss-versus-rebalancing is *impermanent loss* which refers to a loss relative to the value of the initial holding ("loss-versus-holding"). For a comprehensive discussion regarding impermanent loss, consult Capponi and Jia (2021).

holdings for the purpose of liquidity provision.

To clarify the innovative nature of DEXs, we first contrast DEXs with centralized exchanges in Section 2. Then, in Section 3, we explain the novel risks that investors face when interacting with DEXs. These novel risks may require regulation, but the nature of blockchain poses various hurdles to regulation. We clarify these hurdles and discuss possible regulatory approaches in Section 4. We then take a broader view in Section 5, exploring the general notion of decentralized exchange and how DEXs have contributed to decentralized exchange. We conclude with Section 6. Throughout, our analysis focuses on the Ethereum blockchain because it possesses the most DEX activity of all blockchains as measured by either total trading volume or total liquidity (see `https://defillama.com/protocols/Dexes`, date accessed: May 29, 2024). To be clear, DEX activity also occurs on other blockchains with different consensus protocols.

2 Comparing DEXs and CEXs

We begin with a brief summary and comparison of the traditional centralized exchanges (CEXs) prominent in equities markets, CEXs in cryptoassets, and the newer decentralized exchanges (DEXs).

Many of today's CEXs were initially organized around physical trading floors. In a floor market, trading proceeds by open outcry. One floor trader makes an oral bid or offer (price and quantity). A trade occurs when a second trader sells into the first's bid or buys at the first's offer. The dialogue is formalized. For example, the CME (Chicago Mercantile Exchange) Rulebook (Rule 521, circa 2004) states, "A bid is made by stating the price first and quantity next (such as '38.50 on 2,' etc.) ... An offer is made by stating quantity first and price next (such as '2 at 38.50')." The rule continues, "When a trader desires to buy the going offer in the [market], he shall by outcry state 'buy it' ... [when] selling, the trader shall state 'sell it.'" The trade does not automatically occur simply because one member is bidding and another is offering at the same price. The two steps ("bidding"/"asking" and "sell it"/"buy it") are distinct; an execution requires both (Hasbrouck, 2023, chap. 3).

"Liquidity" often refers to immediacy, the option to convert a security into cash or the reverse without delay. In this sense, the trader making the bid or offer is considered the liquidity maker, or simply the "maker," and the second trader is the liquidity taker. In a floor market, maker and taker roles are not fixed. For example, a prospective buyer can take the lowest offer or they can make their own bid. They might start by making a bid priced below the lowest offer, possibly rebidding at progressively higher prices, and ultimately (if no one hits her bid) they might take the best offer or withdraw from the market. A planned

strategy can be modified on the fly. The maker/taker distinction persists in almost all markets.

A floor trader might trade as a principal (on their own account). Alternatively, they might act as an agent for an off-floor customer. In this case, the customer leaves an order specifying their intention. A limit order specifies direction (buy or sell), quantity, and a limit price (a lower limit for a sell order or an upper limit for a buy order). Upon receiving an order to buy "Buy 500 shares limit $10," a broker might call out "bid 10 for 500" (although they might first try lower prices). Since a limit order translates naturally into a bid or offer, it corresponds to a "maker" strategy. The main alternative, a market order, directs the broker to place priority on obtaining an execution, with price a secondary consideration. In this sense, a market order acts as a "taker". The correspondence between order type and maker/taker role is meaningful, but it should not be construed as equivalence because there are significant differences between an exchange member present on the floor and an off-floor customer. A floor trader observing the open-outcry process possesses information not available to off-floor participants. Furthermore, prior to the era of electronic communications, the off-floor customer acting through the on-floor broker could not easily switch maker/taker roles.

Late in the 19th century, the NYSE's floor procedures were augmented by the addition of specialists (official market makers). The specialist assumed the responsibility of ensuring that a listed stock always had a bid and an ask, bidding and offering on their own account in the event that no one else was willing to do so. This supported the NYSE's reputation as a reliable source of liquidity. In addition, the specialist maintained a book where other traders would leave their (and their customers') limit orders. This spared the customer's broker from the burden of constantly monitoring the trading process, watching and waiting for an opportunity to execute the order. The specialist assumed these responsibilities as well.[3]

The specialist stood literally and figuratively at the center of the market for an assigned stock. Their broad responsibility was the maintenance of a "fair and orderly market."[4] To this end, the specialist was subject to numerous affirmative and negative obligations. Some of these obligations, particularly the maintenance of a market presence, could be formidable. In compensation, the specialist enjoyed certain rights and privileges. For example, as agent for the limit order book, they knew its contents but were prohibited from revealing the contents

[3]The historical development of the specialist system and the operations of the U.S. equity market circa mid-20th century are described at length in the SEC's Special Study of the Securities Markets (U.S. Securities and Exchange Commission, 1963). An NYSE memo to members summarizes the rights and responsibilities of the specialist circa 1989, arguably the apex of specialists' importance (New York Stock Exchange, 1989).

[4]This is a touchstone phrase in U.S. market regulation. See, for example, the SEC's mission statement at https://www.sec.gov/about/mission).

to others (an important informational advantage). In modern times, when the specialist's post (desk) became the destination for orders conveyed to the exchange electronically, the specialist had the first opportunity to engage with this order flow.

Under the specialist system, almost any market participant could provide liquidity, at least in principle. A bid, for example, might originate from the specialist, another member on the floor, or from a limit buy order placed in the book by an off-floor customer. The market structure, however, generally favored the specialist and (to a lesser extent) floor traders over off-floor customers. Broadly speaking, up to about 1990, providing (making) liquidity was considered the purview of specialists and similar professionals, whereas the demand for (taking of) liquidity flowed from the public customers.[5] The fluidity and flexibility of maker/taker roles that characterized the early floor markets no longer existed.

Market structure changed dramatically in the 1990s. Limit order books became much more important, eventually dominating many markets, while the influence of specialists and similar market makers ebbed. The forces responsible for these changes were technological and regulatory. On the technological side, improvements in computing and communications led to experimentation with electronic markets. Most of these were organized as electronic limit order books, suggesting the attractiveness of this structure going forward, (U.S. Securities and Exchange Commission, 2000). On the regulatory front, the SEC took steps to promote the prompt display of customer limit orders.[6]

The advent of electronic markets and the SEC's order display requirements diminished the specialists' competitive presence. This decline was hastened, however, by two other developments. By way of explaining the first, we note a market's tick size puts a floor on its bid-ask spread, a strong determinant of market maker trading revenue. Since its founding in 1792, the NYSE tick had been one-eighth (of a dollar), that is, \$0.125 per share. In 1997, the U.S. Congress made an unusual direct intervention in market structure. The Common Cents Pricing Act mandated a reduction of the tick size to \$0.01. This change cut costs for off-floor traders but also reduced specialist profits. The second development comprised various enforcement actions against Nasdaq market makers and NYSE specialists.[7]

[5] A parallel dichotomy between makers and takers generally pervades most of the early canonical economic models of liquidity. Papers from Garman (1976) (with its title including the then-novel term "market microstructure"), through the inventory control models (following Stoll (1976)), the sequential trade models (such as Glosten and Milgrom (1985)), and the continuous auction models (Kyle (1985), and so forth) almost universally posit separate and distinctly different populations of liquidity providers and demanders.

[6] The SEC's Market 2000 study noted that "Questions have arisen as to whether specialists and [other] dealers in listed stocks are displaying limit orders entrusted to them. Specialists and dealers that do not represent limit orders in the quotations may not be displaying the real quotation spread," (U.S. Securities and Exchange Commission, 1994). The SEC later adopted strong order handling rules (U.S. Securities and Exchange Commission, 1996a).

[7] Nasdaq's difficulties followed from a series of academic studies that drew a connection between dealer

Public limit orders were additionally strengthened by the Order Protection Rule component of the SEC's Regulation NMS (National Market System), adopted in 2005 (U.S. Securities and Exchange Commission, 2005). This protection refers to situations known as trade-throughs. For example, if venue XYZ is bidding, say, $10 per share (perhaps from a customer limit order), no other venue can execute a trade priced below $10. That is, XYZ's $10 bid cannot be "traded through" (it is protected). This protection is subject to various restrictions: the protected order must be electronically accessible, visible, and priced at the top of its venue's book (see the discussion accompanying the rule).

The requirement of electronic accessibility removed protection of oral bids and offers, seemingly sealing the fate of the traditional floor markets. Yet one important feature of those early markets has reemerged, in a sense, relatively intact. The modern electronic limit order market provides traders of all types with the ability to quickly reprice orders or shift maker/taker roles. Standard order types can accomplish these tasks routinely, automatically, and at no cost.[8] This process is not as egalitarian as was once hoped (Mendelson and Peake, 1979). High frequency traders enjoy numerous and diverse first-mover advantages. All traders nevertheless enjoy broad opportunities for accessing or supplying liquidity.

Given the success of electronic limit order markets for traditional securities, it is not surprising that this structure is also used extensively for cryptoassets. Coinbase, Binance, and the now-defunct FTX all employ/employed limit order books. Although the traded assets may be implemented on a blockchain, however, the trading process itself is centralized and these markets are most emphatically CEXs. A decentralized exchange (DEX), however, is implemented via smart contracts on a blockchain. The implementation method is crucial to the CEX/DEX distinction, but there are other differences as well.

2.1 Contrasting CEXs and DEXs for Liquidity Demanders

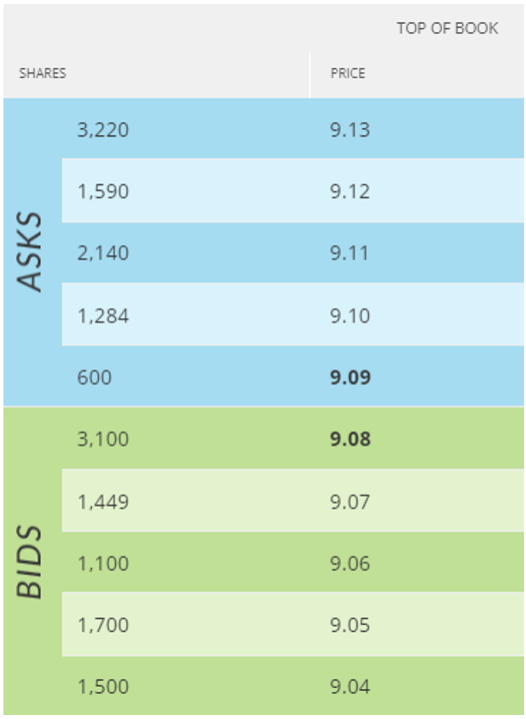
Both the DEX automated market maker (AMM, discussed in the introduction) and the CEX limit order book (LOB) supply liquidity. We therefore begin with an example demonstrating the potential for similar pricing schedules. That is, the two markets can look similar from

quoting practices and the possibility of collusion (Christie and Schultz, 1994; Christie, Harris, and Schultz, 1994; Christie and Schultz, 1995). The ensuing SEC investigation uncovered evidence of pervasive rule violations and mandated numerous reforms (U.S. Securities and Exchange Commission, 1996b). The NYSE cases involved patterns of violations from 1999 to 2003 involving five major specialist firms (U.S. Securities and Exchange Commission, 2004c). In 2008, the NYSE supplanted the specialists with designated market makers (DMMs). Like the specialist, a DMM is broadly charged with maintaining a fair and orderly market. Similarly, the DMM is required to bid and offer to ensure a liquid market. Other obligations have been softened, but the special rights and privileges enjoyed by the specialist have been sharply curtailed.

[8] A pegged order, for example, automatically updates its limit price relative to some reference level, such as the best bid or ask in the market. A discretionary limit order becomes marketable when the quote on the opposite side moves within a preset range.

the perspective of liquidity demanders (the takers). In the next section, we consider the perspectives of liquidity suppliers (the makers).

Figure 1: A Limit Order Book for Robinhood



Screenshot of the limit order book for Robinhood Markets Inc. (Nasdaq ticker symbol HOOD) displayed on CBOE's web site for the BZX Exchange on Tuesday, May 22, 2022, at approximately 1:10 PM ET.

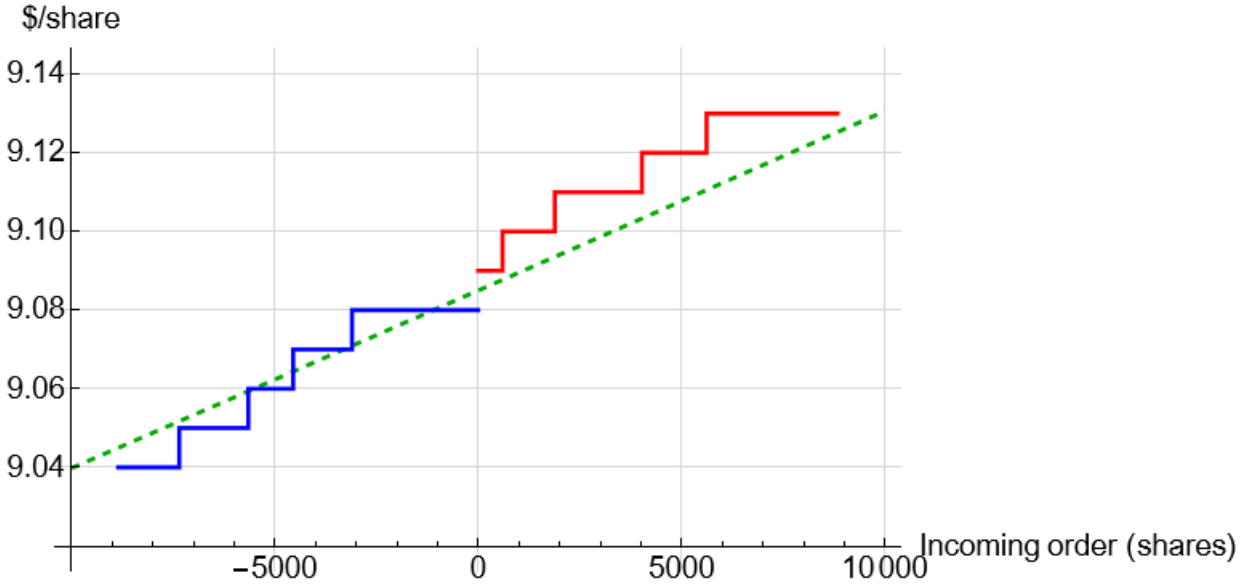
Figure 1 depicts the top levels of limit order book on the CBOE's BZX stock exchange for Robinhood Markets Inc. at one instant on Tuesday, May 22, 2022.

The book is organized in price-time priority. For example, on the bid side of the book, the best bid is the highest, \$9.08. At this price, 3,100 shares are sought, possibly representing multiple limit orders. If there are multiple orders at the same price, time priority applies (first come, first served).[9]

Figure 2 depicts the corresponding price-quantity schedule. For example, an incoming order to buy 1,000 shares with limit price \$9.13 would execute against the higher priority ask price of \$9.09, trading 600 shares but leaving 400 shares remaining. These 400 remaining shares would then trade at \$9.10 where there are 1,284 shares available. If the 1,284 shares

[9]The screenshot displays only the first five price levels on the bid and offer side, and only on the BZX exchange. There may be non-displayed orders and orders priced outside of the first five levels. The display is not consolidated: additional depth may exist at other exchanges. During regular trading hours, the book is publicly available, with data slightly delayed, at https://www.cboe.com/us/equities/.

Figure 2: Price schedule implied by the Robinhood limit order book



Cumulative supply and demand functions implied by prices and quantities in the Robinhood book depicted in Figure 1, expressed as a function of the incoming marketable order size (signed negative for a customer sale, and positive for a purchase). The dashed line is the pricing schedule corresponding to a hypothetical automated market maker (AMM). Following the example in Section 1, the inventory of shares is $y = 2M$ shares, and the inventory of cash is $x = \$9.085 \times 2M$. The initial price is set to the bid-ask midpoint, and the inventory of shares is selected to approximate the slope of the book.

offered at \$9.10 represent multiple orders, they would be executed in time priority based on order submission and not on a pro-rata basis. Similarly, a second incoming buy order for, say, 1,110 shares would first take the remaining 884 shares at \$9.10, followed by 216 shares at \$9.11.

The dashed green line in the figure represents the schedule generated by a hypothetical AMM. The AMM schedule represents a continuous approximation of the book. The close resemblance of the prices schedules suggests that for liquidity demanders, the CEX and AMM/DEX can be nearly equivalent. This equivalence does not extend, however, to liquidity suppliers.

2.2 Contrasting CEXs and DEXs for Liquidity Providers

DEX/AMM liquidity supply differ in many respects from CEX limit order books. The orders resting in the CEX limit order book retain their separate identities, and are executed in price-time priority. In contrast, executions against a DEX liquidity pool are handled pro

rata against all relevant liquidity providers in a homogeneous fashion. In a DEX, among liquidity providers, there is no time priority. Liquidity providers are treated identically whether they are the first investors contributing to the pool or the last.

Additionally, while liquidity provision is one-way on a CEX, it is two-directional in the DEX AMM. On a CEX, a resting limit sell order provides liquidity to incoming buyers only. In contrast, a DEX liquidity provider is potentially a counterparty to either buyers or sellers (or both). The liquidity provider invests in the pool without knowing the direction of the incoming orders.

A final difference between CEX and DEX liquidity provision concerns the persistence of the liquidity-provision obligation. On a CEX limit order book, once a resting limit order is executed, it no longer exists. There is no further presence or obligation. In contrast, on a DEX, after any execution, liquidity does not disappear but rather is converted to the other side of the market. In turn, the liquidity provision obligation on a DEX persists even after a trade execution. For example, a buy of ETH against DAI at an ETH-DAI pool reduces ETH liquidity but increases DAI liquidity since the buy entails the DEX giving ETH but receiving DAI. The additional DAI holding becomes available to serve as liquidity for future ETH sell orders and thus the liquidity providers supplying the initial ETH remain obliged to provide liquidity albeit on the opposite side of the market.

2.3 Custody and Settlement

In traditional finance, "the trade" is but the first step toward the transfer of legal ownership of the payment and the security. The transfer is complete only when the trade is settled, which may require several days to plan and complete. Furthermore, for reasons of safety, ease of record-keeping and so forth, most investors do not directly hold their traditional assets (physically or electronically), preferring instead to use a custodian. Blockchains offer the possibility of simplifying both custody and settlement. Firstly, cryptoassets can be directly and securely held in wallets. Secondly, if trade and settlement both occur on the blockchain, there is a sense in which they are equivalent and simultaneous. From this perspective, DEXs are an attempt to realize this simplicity.

2.3.1 Traditional Assets

Ownership of an asset conveys rights to income, control and exchange. A shareholder exercises these rights when they collect a dividend, vote for a slate of directors, or transfer ownership. Because these processes may require specialized attention and expertise, the owner may delegate them to a custodian. For a retail investor, the custodian would typically

be their broker.[10] An investment fund managed on behalf of others (such as a mutual fund or pension fund) will usually have a custodian distinct from the investment manager and also separate from the brokers that execute the fund's trades.[11]

Morris (2022) describes settlement in U.S. equity and bond markets. A trade transfers security ownership (and generally custody). Historically, this required movement of the physical share certificate and/or registering the new owner on the books of the issuer. In more recent times, paper certificates were dematerialized and replaced with electronic records of ownership. In the United States, these records are centrally held at the Depository Trust and Clearing Corporation (DTCC). The DTCC normally registers shares in the name of a custodian, or, in the case of a retail account, the investor's broker. Settlement timing generally follows market conventions. Until recently the US stock market settled two days after the trade ("T+2"), but on Tuesday, May 28, 2024 settlement changed to T+1.[12,13]

2.3.2 Cryptoasset CEXs

Establishing an account on a CEX that intermediates cryptoassets usually requires that the customer deposit the cryptoasset and/or fiat with the exchange. The customer's trades on the CEX are settled against this account. In this arrangement, the exchange is acting as the custodian, but one that may not be subject to the same oversight as a custodian for a traditional asset. Withdrawals and transfers from the account may be subject to high fees, delay, and inconvenience. Finally, unlike a US retail brokerage account, the CEX account is not covered by SIPC protection.

[10] For investor protection, assets held in custody are segregated from the business assets of the broker. U.S. retail customer holdings are also protected (up to $500,000) by the Small Investor Protection Corporation (SIPC, similar to the FDIC for banks). SIPC protection extends to the customer assets but not losses due to change in market value. Suppose a customer buys 1,000 shares of a stock at a market price of $100. If the market price subsequently declines to $90, SIPC does not cover the $10,000 loss. If the investor's shares are surreptitiously transferred without the investor's knowledge or authorization, though, the value of the shares ($90,000) would be covered.

[11] An institutional custodian will also assist in arranging loans of securities, management of collateral, settlement of foreign securities, and exchange of foreign currencies (Loader, 2019).

[12] Technically, settlement is negotiable. A buyer and seller might agree to settle immediately or perhaps ten days hence, but this must be agreed upon prior to the trade. A bid, ask, or the acceptance of a bid or ask is understood to be for standard settlement. For anything else, the trader (or their broker) would have to search beforehand for an amenable counterparty. Or, to take a post-trade perspective, it might be thought that once the necessary information was shared and confirmed, settlement could proceed immediately, possibly prior to the market convention. In fact, suppose that, in the current $T+1$ environment, a buyer and seller have confirmed the terms immediately after the trade (on day $T+0$). If the seller were to suggest settling on $T+0$ the buyer would have to make payment one day early (thereby losing one day's interest). If the buyer were to suggest settling on $T+0$, the seller would lose any dividend paid on day $T+0$. In short, it is unlikely that both parties would be agreeable to an accelerated settlement.

[13] We omit here a discussion of clearing. Clearing comprises various precursors to settlement, such as: confirming the identities of the buyer and seller (or their custodians), confirming the terms of trade, and making arrangements for payment.

2.3.3 DEXs

A DEX is restricted to intermediate assets settled directly on the blockchain on which that DEX is deployed. This restriction is what enables a DEX to generate trade settlement simultaneous to trade execution. The computer program that defines a DEX liquidity pool usually entails a swap function that a user can execute in order to trade. The swap function directly re-assigns ownership of the assets being exchanged to the new owners thereby achieving trade execution and settlement simultaneously.[14]

To understand this point, we offer an example. If Alice wants to buy 1 ETH from a DEX on the Ethereum blockchain, she must first identify an asset settled on the Ethereum blockchain that she would like to provide in return to receive the 1 ETH. Alice cannot make her purchase in U.S. dollars because the currency is not settled on the Ethereum blockchain. In practice, Alice would typically opt to use a stablecoin for her purchase. Alice could pay for her 1 ETH with the DAI stablecoin. Then, to execute such a purchase, Alice would need to swap DAI for ETH from an ETH-DAI liquidity pool where the execution would entail Alice explicitly executing the swap function for the ETH-DAI pool. In response, the ETH-DAI pool would price Alice's trade based on its AMM as discussed earlier. Suppose that the ETH-DAI pool prices Alice's purchase of 1 ETH at 3000 DAI. In that case, ignoring fees, the resulting swap function execution would simultaneously transfer 3000 DAI into the ETH-DAI liquidity pool while transferring 1 ETH to Alice. The swap function execution alters ownership of the relevant assets and thus settlement is simultaneous to trade execution.

When trading with a DEX, there are no intermediaries. The trader receives not only ownership but also custody of the asset being purchased immediately and also loses custody of the asset being used for the purchase immediately. In our example, Alice possesses custody and ownership of the 3000 DAI only before her trade execution and receives custody and ownership of the 1 ETH when her trade is executed.

[14] We refer to trade settlement as the first time at which the assets being exchanged have transferred based on the canonical chain of the blockchain implementing the transfer. To provide more technical precision within the specific context of the Ethereum blockchain, our notion of the canonical chain refers to the chain selected by the LMD-GHOST protocol. A more conservative definition of trade settlement would entail requiring that the assets being exchanged have transferred according to a chain that has achieved some notion of "finalization" (e.g., via Casper FFG in Ethereum's case). However, that stricter definition generally implies a settlement delay of less than 20 minutes while introducing unnecessary technical complexity. For the sake of exposition, we avoid discussions regarding finalization. The interested reader may consult John, Monnot, Mueller, Saleh, and Schwarz-Schilling (2024) for comprehensive details regarding finalization and other technical details of the Ethereum protocol.

2.4 Order Priority on CEXs vs. DEXs

CEX limit order books are arranged in price-time priority: orders are ranked first on price and then on time of submission. Arriving orders are handled on a first-come, first-served basis. Within its own system, a CEX can enforce these priorities. When there are multiple CEXs, maintenance of priorities requires more coordination (as mandated, for example, in US Reg NMS), price priority is maintained, but time priority is less certain.

In sharp contrast to CEX ordering, the ordering of DEX executions is determined by the sequence in which these executions are posted on the blockchain ledger. Executions are finalized only when they are included in a block. All executions within a block are priced sequentially so that ordering within a block has practical implications. If one execution receives priority on a block relative to another execution, then the first execution on the block affects the asset holding of the liquidity pool before the second execution on the block. In turn, due to AMM pricing, the price of each execution depends on the asset holding directly before the execution. Therefore the order of executions *within a block* affects the pricing of each execution. This leads to various risks from profit-seeking entities. We explore those risks in detail in Section 3.2.

The ordering of executions within a block is ultimately at the discretion of whichever entity received the authority to post that block (the proposer). The proposer in turn relies on another entity (a builder) to build the block (see Section 4.4), and the builder usually determines block order so as to extract maximum value for themselves. The last quantity is known as Maximal Extractable Value (MEV). This extraction of value by the builder arises largely through priority fees whereby users pay a higher fee to the entity building the block to receive priority execution within the block relative to other users (see Daian, Goldfeder, Kell, Li, Zhao, Bentov, Breidenbach, and Juels 2020). This type of prioritization is distinct from prioritization across blocks, a phenomenon that arises also in simpler blockchains such as Bitcoin (see John, O'Hara, and Saleh 2022).

The referenced pay-for-priority mechanism might resemble practices of high frequency traders (HFTs) in existing CEXs. In both cases, intermediaries are paying for speed. Beyond that though, there are many substantive differences. Most importantly, the expenditures of HFTs represent fixed-cost investments in technology that the traders hope will enable them to make higher trading profits on average (over a large population of stocks and over time). The bidding for priority execution on a block, though, is essentially order-by-order. The order-by-order auctions are likely to be more efficient than averaged mechanisms, but only in the narrow sense of maximally extracting value from users from the the more numerous

liquidity traders.[15]

3 Risks

A variety of novel risks arise for DEX users relative to CEX users. Some of these risks apply generally for users of any smart contract, whereas other risks apply specifically to DEX users. We detail the former in Section 3.1 and the latter in Section 3.2.

3.1 Risks for Smart Contract Users

A DEX is a set of inter-related smart contracts where a smart contract is a computer program deployed on a blockchain. DEXs are generally deployed on blockchains that are both *public* and *permissionless*. Each of those features implies novel risks.

3.1.1 Risks Due to Public Nature of Blockchain

A blockchain is deemed public if any individual can read the contents of the blockchain. Most blockchains, including most blockchains with DEXs, are public. As a consequence, risks for public blockchains are also risks for DEXs.

The key problem arising from the public nature of blockchain for DEXs is that the computer programs that define the DEX are public and thus their code is known to even profit-seeking hackers.[16] There are potentially hundreds of hackers simultaneously examining DEX computer programs for vulnerabilities in order to steal user funds. To date, several hacks have led to non-trivial losses fore DEX users (see, e.g., MarsNext 2023 and Haqshanas 2023).[17] A mitigating factor is the community of white-hat hackers, individuals who examine the code to find vulnerabilities and then propose code modifications to resolve any vulnerabilities that are found. Notably, just as profit-seeking hackers are able to exploit

[15] Ernst, Spatt, and Sun (2022) note the contrast between order-by-order and averaged pricing in their analysis of a recent SEC proposal for handling retail orders.

[16] As a technical aside, the DEX code is not necessarily publicly available in the format that it is initially written (i.e., source code). Rather, the initial source code is compiled to bytecode before being released to the public blockchain network. This caveat notwithstanding, major DEXs (e.g., Uniswap) generally release their source code publicly (e.g., on `www.etherscan.io`). Moreover, that source code is usually verified against the publicly available bytecode to confirm that it is the source code for the DEX.

[17] A DEX hack can arise due to portions of the associated smart contract code unintentionally including opportunities for profit-seeking attackers to drain funds associated with the smart contract. A common example of such a code vulnerability is the re-entrancy bug whereby a user is able to withdraw their funds but "re-enter" the code infinitely, making the same withdrawal request each time as though the user had never withdrawn their funds initially. In this way, the user can drain all funds of the smart contract. The interested reader may consult Liu, Liu, Cao, Chen, Chen, and Roscoe (2018) for details.

vulnerabilities due to the public nature of the blockchain, white-hat hackers are also able to mitigate the problem precisely because of the blockchain's public nature.

From a theoretical perspective, such hacks could be overcome with perfect code-writing for smart contracts. However, such a standard for code writing is practically unrealistic. Due to the volume of code involved in any sophisticated computer program, most if not all such programs will likely possess vulnerabilities overlooked by the code writers. Thus, the crucial difference between the public blockchain context and a traditional centralized system context is the extent to which hackers have access to the underlying code. From an economic perspective, the ease of access to the code in the public blockchain context reduces the cost of a hacker attack and thereby increases the risk of a hacker attack in equilibrium.

3.1.2 Risks Due to Permissionless Nature of Blockchain

A blockchain is deemed permissionless if an agent requires no special permission to interact with it. Most prominent blockchains, including most blockchains with DEXs, are permissionless. In turn, risks for permissionless blockchains are also risks for DEXs.

A key feature of a permissionless blockchain is that user identities are not managed by a centralized entity. That an individual requires no permission to interact with the blockchain means that any individual can create an identity understood by the blockchain without approval from any centralized authority. In practice, identities within permissionless blockchains are generated through cryptographic systems in a manner that is not only independent of centralized entities but also independent of any particular blockchain. The Ethereum blockchain, for example, relies on a cryptographic system known as the Elliptic Curve Digital Signature Algorithm (ECDSA), that not only operates independently of Ethereum but also predates all modern blockchains (see Johnson, Menezes, and Vanstone 2001).

Since blockchain user identities exist independently of any centralized entity, those user identities must be managed directly by users. This is an advantage in that users maintain direct custody of any assets held on the blockchain. However, it also introduces a novel risk because mismanagement of a user identity could ldead to a financial loss that cannot be corrected by any centralized authority. Cryptographic systems involve a *private key* that functions as a password for the user identity; a user can misplace their private key which would cause them to lose access to their blockchain identity and thus all assets held under that identity. In a traditional centralized context, the same user could reset their password through their centralized intermediary. However, in the context of a DEX, a user providing inventory to the DEX would lose all associated financial claims if they misplace their private key because the user would no longer be able to demonstrate that they are the user who

provided the inventory. Furthermore, in this case, with no centralized entity that could reset the private key, the user's loss from misplacing their private key would be irreversible.[18]

Custody is a significant risk and is the reason why many choose to interact with centralized exchanges like Coinbase, Gemini or Kraken where custody is delegated. Indeed, custody also explains the popularity of the cryptoasset ETFs where the purchaser does not need to worry about managing private keys. However, there are many ways to reduce custody risk in the absence of a centralized entity. One popular method is "key splitting", by which a key is divided into three or more pieces. Any two pieces can be used to reconstitute the original private key. A user might delegate one piece to a custodian. Even if the custodian is hacked, the single piece is useless. The user might keep the other two pieces. If one is lost, reconstituting the key with the custodian's piece is straightforward.

3.2 Risks for DEX Users

An especially salient risk for DEX users is front-running, an activity that occurs frequently and regularly on DEXs without any intervention from governments.[19] On a DEX front-running might arise from three considerations: (1) blockchains update only at discrete time intervals, (2) many actions submitted to a blockchain are publicly observable when not yet posted to the blockchain, and (3) actions posted to a blockchain are not typically posted with time priority. An action being posted to a blockchain only at discrete time intervals and that action being publicly visible while pending implies that a blockchain user can observe that action prior to it being posted to the blockchain. Then, since actions are not posted to the blockchain with time priority, a user can take a consequent action after observing a prior action in such a way that her consequent action is processed prior to the earlier action - i.e., a user can front-run an earlier action. In practice, front-running can pose risks for both traders and liquidity providers. We discuss front-running related to trading in Section 3.2.1 and front-running relating to liquidity provision in Section 3.2.2.

To provide detail on actions being posted to a blockchain, it is important to understand

[18]The relationship between a user's public identity and their private key is publicly known and there exists an algorithm to recover a user's private key from their public identity. However, the referenced algorithm for recovering a user's private key is practically infeasible given modern technology. Although advances in quantum computing will likely make the process of recovering ECDSA private keys feasible, quantum-resistant cryptographic systems are also likely to arise. This research is usually called post-quantum cryptography or PQC.

[19]In one recent case, an SEC complaint defines front-running as "trading ahead of large, nonpublic orders of market participants to benefit from the market impact of those large orders," (U.S. Securities and Exchange Commission, 2022a). More generally, the legality of the activity may turn on the nature of the relationships (Linehan, Heath, and Shulkin, 2021). For example, should a block-builder be considered an agent for the trading parties, or is the relationship "arms-length?" An agency duty normally prohibits front-running; an arms-length separation might afford greater leeway.

that a blockchain is a distributed system that involves many nodes. Moreover, updates to the blockchain are allowed only at certain times, and the authority to update at a particular time is generally allocated on a probabilistic basis to a single node (see John et al. 2024). In turn, to receive the fastest possible service time, a user submitting an action would prefer the action be received by all nodes in the network, ensuring that the action is known to the node that can next update the blockchain. To achieve timeliness, blockchain nodes follow a *gossip* protocol whereby nodes rebroadcast actions to a random set of other nodes, until the action is disseminated to all nodes in the network. A user seeking to have their action posted to the blockchain generally submits that action to only a few nodes (sometimes only one) and the action is eventually observed by the full network due to the gossip protocol. Crucially, an action received by a node cannot be posted immediately to the blockchain. For that reason, until a pending action is posted to the blockchain, it is stored locally by each node in a structure known as a *memory pool*. Once a node observes a block, that node removes the actions within the observed block from their memory pool.

3.2.1 Trader Front-Running Risk: "Sandwich Attacks"

As discussed in Section 2.4, an order to trade is executed only when it is included in an update of the underlying blockchain. In turn, an order to trade can be front-run by an order submitted later in time so long as the later order is included on the blockchain with a higher priority than the earlier order. Prior to being included in an update to the blockchain, an order can be publicly visible. As a consequence, an order later in time can be constructed so that it receives priority over the initial order thereby front-running the earlier order.

For a concrete example, we describe front-running a trading order submitted to a DEX on the Ethereum blockchain. First, the Ethereum blockchain updates only at regular intervals of 12 seconds. In turn, if a blockchain user, Alice, submits a trading order one second after the most recent Ethereum update, then her order cannot be posted to the Ethereum blockchain for another 11 seconds, although her order would be publicly visible for those 11 seconds. Thus, during those 11 seconds, another user, Bob, could submit a trading order for the same liquidity pool and in such a way that Bob's order receives priority over Alice's order in terms of the sequence of the orders being posted to the Ethereum blockchain. This course of action would constitute Bob front-running Alice.

Under certain conditions, front-running a trade can be conducted such that it is always profitable (see, e.g., Park 2023). This is important because if any blockchain user can conduct a front-run and front-running is profitable, then front-running is an inevitable outcome for a submitted DEX order. Indeed, front-running can always be made profitable in the specific case of a DEX with a CPAMM and no fees. So, if Alice places an order to buy $\delta_x > 0$ ETH

units from an ETH-DAI liquidity pool with a CPAMM, then, absent fees, it will *always* be profitable for Bob to execute a version of front-running known as a "sandwich" attack.

In a "sandwich" attack, Bob not only submits an order that receives priority ahead of Alice's order (front-running) but also submits an order that is executed directly after Alice's order (back-running), thereby sandwiching Alice's order between two orders. For a CPAMM with no fees (liquidity or gas), it is always profitable for Bob to execute a sandwich attack whereby he front-runs Alice's order to buy δ_x ETH units with an identical order to buy δ_x ETH units and then back-runs Alice's order with an exactly off-setting order to sell δ_x ETH units. The CPAMM ensures that the ETH-DAI price decreases with ETH units held by the pool and increases with DAI units held by the pool.[20] In turn, Bob's front-run order to buy δ_x ETH units increases the ETH-DAI price for Alice's trade but then Bob's back-run order to sell δ_x ETH units receives the same elevated ETH-DAI price of Alice's order because Bob's back-run trade exactly offsets Alice's order. Bob's order to buy δ_x ETH units would face some ETH-DAI price P_0 whereas Alice's following order to buy δ_x ETH units would face an ETH-DAI price $P_1 > P_0$ because it is processed after Bob's order to buy δ_x ETH and because Bob's order reduces the liquidity pool's ETH holding while increasing the liquidity pool's DAI holding. Then, since Bob's order to sell δ_x ETH units exactly offsets Alice's buy order of δ_x ETH units, it incurs the same price as Alice's trade, $P_1 > P_0$. Consequently, absent fees, Bob receives a guaranteed strictly positive profit of $(P_1 - P_0) \cdot \delta_x > 0$ from the described sandwich attack.

In response to concerns regarding front-running of trading orders, a class of intermediaries called *private pools* has developed. A private pool is a known intermediary that accepts orders and posts those orders to the blockchain while ensuring the orders will not be front-run.[21] Capponi, Jia, and Wang (2023a) put forth a comprehensive economic analysis of private pools and find that although private pools can ameliorate front-running trading risk, they do not fully resolve the risk in equilibrium. By submitting orders through a private pool, execution risk arises because the private pool is not a centralized entity in control of the blockchain and thus the private pool may not be able to post to the blockchain in a timely manner. Capponi et al. (2023a) demonstrate that, in equilibrium, some users prefer to bear the front-running risk from submitting an order to the blockchain network directly rather than bearing the execution risk from a private pool.

[20] Recall that the ETH-DAI price is given explicitly by $\frac{y}{x-\delta_x}$ where $y > 0$ denotes the DAI units held by the pool and $x > 0$ denotes the ETH units held by the pool. By direct verification, the ETH-DAI price, $\frac{y}{x-\delta_x}$ increases in the DAI units, y, (i.e., $\frac{\partial}{\partial y}[\frac{y}{x-\delta_x}] = \frac{1}{x-\delta_x} > 0$) and decreases in the ETH units, x (i.e., $\frac{\partial}{\partial x}[\frac{y}{x-\delta_x}] = -\frac{y}{(x-\delta_x)^2} < 0$).

[21] There is circumstantial evidence that private pools exploit private order flow for profit (see Yaish, Dotan, Qin, Zohar, and Gervais 2023).

3.2.2 Liquidity Provider Front-Running Risk: Just-In-Time Liquidity

Within the context of blockchain, front-running extends beyond a user constructing a trading order that receives priority in terms of posting to the blockchain over a trading order submitted earlier. In particular, front-running can entail a user taking an action to provide liquidity such that the liquidity provision receives priority over a trading order submitted earlier in time. This type of front-running, Just-In-Time (JIT) Liquidity, and it is detrimental to other liquidity providers (see Capponi, Jia, and Zhu 2023b).

When a trading order is submitted, the order becomes public even though it is not posted to the blockchain immediately. Then, while the trading order is pending, another user can observe this order and front-run it by taking an action to provide liquidity such that the liquidity provision action is posted to the blockchain directly before the trading order. In such a case, the liquidity provision action entails providing inventory to the specific liquidity pool against which the trading order is executed. The purpose of this type of front-running is for the front-running user to accrue trading fee revenues while avoiding the risks faced by other liquidity providers. Since liquidity providers at a liquidity pool are owners of the inventory at the liquidity pool, they incur the price risk associated with fluctuations in the price of their inventory. The front-running user largely avoids this price risk by providing liquidity specifically for a single trade and then withdrawing liquidity immediately thereafter. This type of liquidity provision not only directly front-runs a trading order with a liquidity provision action but also directly back-runs the same trading order with a liquidity withdrawal action that removes all the liquidity provided earlier. Thus, the front-running user's liquidity is used only for the trading order and is otherwise insulated from price risk. Most liquidity providers are passive liquidity providers and leave their inventory at a liquidity pool for a long period. As such, liquidity provision front-running, or JIT liquidity, reduces the accrued fee revenue of most liquidity providers.

4 Challenges of Regulation

Investor protection of DEX traders and DEX liquidity providers is a legitimate concern for regulators. Traders and liquidity providers at a DEX face various risks from other profit-seeking DEX users. In turn, it would be ideal for regulation to ameliorate those risks. Nonetheless, any such regulatory policy, should be sensitive to the specific challenges for regulation in the blockchain context. To that end, we describe the most fundamental of those challenges. Our key point is that a DEX *cannot* be regulated as a centralized exchange

due to the specific institutional details of blockchain technology.[22]

We discuss separately challenges arising from regulating DEX users and from regulating DEXs in Section 4.1 and Section 4.2 respectively. Then, in Section 4.4, we discuss the challenges associated with regulating the entities that post orders to the blockchain.

4.1 Regulating DEX Users

The fundamental constraint to regulating a DEX user, whether a trader or a liquidity provider, is that access to a DEX does not require on-boarding and thus identifiable information regarding a DEX user is not generally available. In turn, there are non-trivial difficulties associated with imposing sanctions on a DEX user. For a user, interacting with a DEX requires only an identity recognizable by the blockchain on which the DEX is deployed. Moreover, as discussed in Section 3.1.2, an identity on a particular blockchain is not specific to that blockchain or even to blockchains more generally. Rather, blockchain identities are generated through cryptographic systems that are entirely independent of blockchain technology. Importantly, identities within a cryptographic system can be generated by an individual through isolated mathematical computations thereby making detection of generating such identities impossible in general. Then, since blockchain identities cannot be detected perfectly and since DEX users are known only through their blockchain identities, regulating DEX users is difficult because identifiable information regarding a user is not generally available. As a caveat, regulators may be able to uncover DEX user identities through blockchain forensic analysis (see, e.g., Cong, Harvey, Rabetti, and Wu 2023), but the need for such analysis represents a substantial increase in regulatory costs relative to a centralized exchange. Indeed, it is an open question as to whether such heightened costs render regulating DEX users directly unrealistic.

One approach to address the lack of identifiable information for a DEX user is for the DEX code to implement white-listing. In particular, the DEX code could theoretically restrict access to the DEX's trading functions to only those users who have undergone identity verification. While this solution may seem appealing, it nonetheless possesses a fundamental problem in that it assumes the existence of a centralized entity that will provide the identity verification service. A DEX is ultimately just computer code deployed on a blockchain and any entity can deploy such code without remaining available to support the application thereafter. We discuss this point in more detail in Section 4.2 because it relates to regulating

[22]This point has also been made more generally for decentralized finance applications by the International Monetary Fund (IMF): "In these contexts, the lack of intermediaries means that traditional AML/CFT regulation, in which AML/CFT requirements are imposed on the private sector and compliance is monitored by supervisors, cannot be applied" (International Monetary Fund, 2023).

the DEX itself.

4.2 Regulating DEXs

Given the difficulties of regulating DEX users in general, a regulator may prefer to regulate the DEX itself. This approach, however, reveals two problems. The first which also arises in the previous white-listing discussion, is that this approach assumes the existence of a centralized entity that may not exist. The second is that, even if such a centralized entity does exist, then imposing regulation on this entity may cause the entity to suspend its operation which would then increase DEX user risks.

Regarding the first problem, again, any entity can deploy a DEX to a blockchain. The DEX smart contract code distributed by software development companies rarely creates a legal relationship between the code and the developer (Cohen, Strong, Lewin, and Chen, 2022). In particular, the developer is generally under no legal obligation to support the code, although they usually do so at least initially. Moreover, as a further complication, an entity deploying a DEX need not identify itself since deploying a DEX requires only possessing an identity recognizable by the particular blockchain. As mentioned in Section 4.1, such an identity can be generated through isolated mathematical computations thereby implying that an entity can, without providing any traceable information, deploy a DEX and then cease to operate. The ease of DEX creation and absence of traceability may facilitate manipulative strategies that rely on undisclosed coordination of security issuance and the appearance of liquidity and investor interest. A DEX might be created and populated, for example, with the fraudulent intent of depicting price and volume growth in an otherwise worthless cryptoasset.[23] More generally, any regulatory policy that relies upon the existence of a centralized entity to verify identities is, by construction, limited.[24]

As for the second problem, even in DEX deployments that feature a centralized entity supporting the DEX, regulation of that centralized entity may not be optimal. In particular, onerous regulations could lead such an entity to cease operation, a course of action that would then exacerbate risks for DEX users. A well-meaning entity would typically directly address some of the risks discussed earlier (e.g., revising code to mitigate hacks) thereby

[23]Regulation of market makers in traditional settings discourages such coordination. FINRA Rule 5250 (a) states that, subject to certain exceptions, "No member or person associated with a member shall accept any payment or other consideration, directly or indirectly, from an issuer of a security, or any affiliate or promoter thereof, for publishing a quotation, acting as market maker in a security, or submitting an application in connection therewith," (https://www.finra.org/rules-guidance/rulebooks/finra-rules/5250).

[24]As an aside, actions on a blockchain (e.g., deploying a DEX) generally require paying fees in terms of the unit of account of the blockchain (e.g., ETH for Ethereum). In turn, a DEX deployment on Ethereum would require first acquiring ETH, and that transaction could ease the task of tracing the user deploying the DEX.

implying that the absence of such an entity would amplify DEX user risks. More concretely, a lab often supports a given DEX (e.g., Uniswap Labs for the Uniswap DEX), but the DEX code nonetheless exists independently of the supporting lab. Excess regulation could drive the lab to suspend its operations, but that would not interfere with the investors' ability to trade with the DEX through its code.

The SEC seems to favor direct enforcement actions against the DEXs. On April 10, 2024, the SEC delivered a Wells Notice to Uniswap Labs. While the content of the Wells Notice is not public, Uniswap Labs has stated that it will fight saying "this is the latest political effort to target even the best actors in crypto like Uniswap and Coinbase." Uniswap Labs has released a lengthy response to the Wells Notice (see https://blog.uniswap.org/wells-notice-response.pdf). Trading volumes on Uniswap were approximately $10 billion per week before Uniswap Labs received a Wells Notice and similar trading volumes have persisted since. Uniswap had approximately $5 billion of liquidity in its liquidity pools prior to Uniswap Labs receiving the Wells Notice and still maintains over $5 billion of liquidity as of May 30, 2024.

4.3 Regulating Market Places

U.S. securities exchanges and alternative trading systems (ATSs, a less-restrictive classification) are regulated by the SEC. In the 1934 Securities and Exchange Act, the original (and still current) text states, "[The] term 'exchange' means any organization, association, or group of persons, whether incorporated or unincorporated, which constitutes, maintains, or provides a market place or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange as that term is generally understood, and includes the market place and the market facilities maintained by such exchange," (15 U.S.C. § 78c(a)(1); full text available at https://www.law.cornell.edu/uscode/text/15/78c).

The SEC's current position on the applicability of this definition to DEXs is interwoven with recent rule proposals on non-crypto markets. As of this writing, the most recent discussion is (U.S. Securities and Exchange Commission, 2023, the "Reopening Release").[25]

[25] In 2020 the SEC released a rule proposal concerning alternative trading systems (ATSs) (U.S. Securities and Exchange Commission, 2020). The proposal included a Concept Release (essentially a broad overview) that discussed the bond market, noting in particular the diversity of trading protocols and variation in the regulation of trading platforms and requesting comment on approaches to regulatory harmonization. Based in part on the received comments, the SEC released in 2022 a new proposal (U.S. Securities and Exchange Commission, 2022b) that considered the definitions of exchanges and ATSs as they might apply to "U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities". Some of the comments received on the 2022 proposal sought information about how the proposed rules might apply to trading systems for cryptoasset securities. The 2023 Reopening Release supplemented the 2022 proposal

Section II.B of the Reopening Release ("Exchange Activity ... Using 'DeFi' systems") summarizes the SEC's views, the positions expressed in comment letters, and the SEC's responses. Our general concern regarding the absence of a centralized entity that might be regulated appears in some of the letters.

In response the SEC notes that although many current exchanges are operated by a single organization, the statutory definition of an exchange does not require the existence of a single entity: a group of persons suffices. Specifically:

> The group of persons that constitutes, maintains, or provides a market place or facilities for bringing together buyers and sellers of securities or performs with respect to securities the functions commonly performed by a stock exchange, and is thus an exchange, would collectively have the responsibility for compliance with federal securities laws. A group of persons must consider how they will comply with the Exchange Act registration requirements given their activities, which can include, but are not limited to, designating a member of the group, to register the group or forming an organization to register as an exchange or, to operate as an ATS, registering as a broker-dealer and becoming a member of Financial Industry Regulatory Authority ("FINRA") to ensure compliance. (U.S. Securities and Exchange Commission, 2023, p. 26)

Although this passage authoritatively asserts the necessity of regulation, the question of feasibility remains unsettled.

The National Market System for U.S. equities comprises multiple exchanges and numerous ATSs that are subject to different regulatory obligations. A broker receiving a customer order usually has considerable flexibility in where they route the order (exchange, ATS, or dealer). The broker's agency duty of best execution nevertheless imposes a responsibility to monitor and evaluate the consequences of their choices. Crypto market structure might evolve along similar lines to construct a landscape of CEXs, DEXs, and other venues. Broker monitoring of order handling and execution outcomes might substitute in part for more direct regulation.

---

with a discussion of crypto markets (including decentralized developments) and where these markets might fall under the proposed regulatory framework (U.S. Securities and Exchange Commission, 2023). To clarify one aspect of the discussion, the 2022 proposal contains numerous references to a new term, "Communication Protocol Systems" (upper case). The fact sheet for the proposal describes these as "[trading] systems that offer the use of non-firm trading interest and provide protocols to bring together buyers and sellers of securities." A reference early in the proposal notes that they "... perform similar market place functions of bringing together buyers and sellers as registered exchanges and ATSs." These descriptions suggested possible consideration of a new regulatory classification, and references to "Communication Protocol Systems" appear widely in subsequent comment letters and various non-SEC material. The SEC dropped the term, however, in the Reopening Release, in favor of the more generic "communications protocols" (lower case).

4.4 Regulating Block Proposers

A potential alternative approach to regulating DEX activity is to regulate posting to the underlying blockchain more generally. In theory, such regulation could be imposed on *block proposers*, the entities with the authority to add blocks to the blockchain. However, block proposers generally do not construct blocks, relying instead on entities known as *block builders* (Heimbach, Kiffer, Ferreira Torres, and Wattenhofer 2023). Moreover, the interaction between block builders and block proposers is intermediated by entities known as *relays*. Regulators may consider regulating any or all of these three types of entities involved in block production.

For context on block production, the Ethereum blockchain partitions time into 12 second periods known as *slots*. For each slot, a single entity is selected as a block proposer according to a selection protocol known as *Proof-of-Stake* (see Saleh 2021). Proof-of-Stake requires that only one block per slot can be added to the blockchain and grants a monopoly right to the selected block proposer as the only entity with the authority to add that block. In practice, the selected block proposer does not construct the block and instead sells their block creation monopoly right to a block builder in a competitive bidding process.[26] Block builders participate in the competitive bidding process because each block builder specializes in creating blocks that specifically transfer value to that block builder. These value transfers are known broadly as *Maximal Extractable Value* (MEV) where examples of MEV include front-running (see Section 3.2.1) and voluntary fees paid for priority processing within a block. The value is transferred to a specific block builder only if that block builder's block is added to the blockchain and thus block builders are willing to engage in a competitive bidding process to have their blocks included in the blockchain (see Schwarz-Schilling, Saleh, Thiery, Pan, Shah, and Monnot 2023). A recent estimate indicates MEV of approximately $846 million per year and attributes roughly $216 million of that to sandwich attacks.[27] MEV has generally increased over time and thus the estimated magnitudes may significantly understate MEV going forward.

Whichever block is added to the blockchain in a given slot must involve a cryptographic signature from the block proposer selected in that slot by the Proof-of-Stake protocol. This cryptographic signature requirement is the enforcement mechanism for the block proposer

[26] The auction process can be viewed in real time at https://payload.de/data/.

[27] Our MEV estimates rely on data from www.libmev.com as of June 5, 2024. As of June 5, 2024, https://www.libmev.com/ reports MEV of 20,163 ETH over the past 30 days. Then, taking an estimate of 3500 USD per ETH, the approximate annual MEV is 20,163 ETH/ month × 12 months/ year × $ 3500/ ETH = $ 846 million/ year. With regard to the estimate of MEV due to sandwich attacks, www.libmev.com reports $ 18 million for the past 30 days from June 5, 2024, indicating an annual rate of $ 18 million/ month × 12 months/ year = $216 million.

having a monopoly right to add a block in a selected slot. In turn, the process of a block builder buying the block proposer's monopoly block creation right is not straight-forward and requires a mediator, a role fulfilled by a relay. If a block builder provides blocks directly to a block proposer, then the block proposer could steal the MEV that the block builder had transferred to themselves in the block builder's block. This is because the block proposer could simply construct a block identical to that of the block builder but replace any action involving the block builder with an identical action involving the block proposer. For example, the block proposer could set themselves as the fee recipient for all transactions within the block whereas the builder typically sets themselves as the fee recipient. In this way, the block proposer would accrue all the MEV received by the block builder in the block produced by the block builder, but the block builder would receive nothing because the block proposer would construct their own block rather than use the block builder's block.

A relay resolves this problem by receiving blocks from block builders and then passing onto the block proposer only the block headers and the block builder bids.[28] A block header summarizes the block content but does not directly reveal the block's content. As a consequence, the block proposer must select a winning bid without observing the winning block's content. More formally, the block proposer selects a winning bid by signing the associated block header and sending that signed block header to the relay. The act of the block proposer signing a block header allows the relay to combine the block header with the block content and then release it to the full blockchain network to be added to the blockchain. In particular, the block proposer's signature transfers their monopoly right to the particular block and thus the block proposer cannot propose a distinct block after signing a block header without facing a penalty (see John et al. 2024 for details). The block builder's bid is typically paid as a transaction on the block builder's block so that the block proposer is paid once the block builder's block is added to the blockchain.[29]

From a practical perspective, how to sanction block proposers, block builders or relays is unclear since none of these entities are required to provide identifiable information to participate in the block creation process. To that end, while the US Treasury Department's Office of Foreign Assets Control (OFAC) maintains a list of sanctioned Ethereum identities, those sanctioned identities can still have their actions posted on the Ethereum blockchain in practice. Heimbach et al. (2023) find that the share of blocks produced by non-OFAC

[28] In theory, a relay could defraud either the block builder or the block proposer. For that reason, block builders and block proposers interact only with relays whom they trust.

[29] To provide more context on payoffs, block proposers receive the winning block builder's bid and *block rewards* with the latter being seigniorage revenues from newly created units of Ethereum's native asset, ether. As a contrast, block builders receive any MEV that they extract (through priority fees or actions such as front-running) minus the bid paid to the block proposer.

compliant relays has increased over the past few years to approximately 50% in March 2023. Heimbach et al. (2023) also find that some relays that claim OFAC-compliance nevertheless occasionally produce blocks that violate OFAC sanctions. In fact, the proportion of Ethereum blocks including activity by OFAC-sanctioned Ethereum identities exceeds 1%. Wahrstätter, Ernstberger, Yaish, Zhou, Qin, Tsuchiya, Steinhorst, Svetinovic, Christin, Barczentewicz, et al. (2023) find that 46% of block builders are OFAC compliant, but this level of OFAC compliance is not effective at censoring transactions. In particular, transactions by OFAC sanctioned entities are only delayed but not censored.

4.5 The Settlement Process: Regulatory Parallels from Traditional Markets

Starting from a set of trades that have been submitted for inclusion in a block, builders, relays, proposers, and other entities (described in section 5.2.2) interact to determine the order in which the submissions will be processed as the block is assembled and, as soon as the block is proposed and accepted, settled. Different orderings can effectively change the identities of the participants trading and settling in a given slot. Relative to participants' expectations when their trades were submitted, these reorderings can break or reprice their trades. Social welfare can increase or decrease. The addition of the new block represents a market clearing (not necessarily with a single or unique price). Builders might bring to this clearing additional participants or determine matchings with higher trade surpluses, increasing total welfare. Some agents, though, might (via sandwich attacks, front-running, and so forth) interject themselves as intermediaries that extract for themselves not just newly-created surpluses but pre-existing surpluses as well.

These tensions are not unique to crypto markets, but exist in traditional markets as well. The main difference is that the reorderings, displacements, and so forth occur earlier in the trading process through practices known as interpositioning, spoofing, and triggering.

Interpositioning involves a "stepping between" a natural buyer and seller to extract rents. An SEC enforcement case against an NYSE specialist (U.S. Securities and Exchange Commission, 2004a) explains:

> To illustrate: if market orders were present on both sides of the market and simultaneously visible on the [limit order book], and the quote constituted a bid for $25.00 (purchase price) and an ask of $25.01 (sale price), the specialist was obligated to pair the market orders at $25.00 or $25.01. Instead, the specialist improperly interpositioned [their] dealer account by buying from the sellers at $25.00, and then selling to the buyers at $25.01 and capturing the one-cent spread.

The specialist in this case is analogous to a builder since they are aware of the orders and the state of the market and can propose an alternative that enriches themselves.

Spoofing involves making a spurious bid or offer often with the intent of establishing a reference price for a subsequent trade. In one such case (U.S. Securities and Exchange Commission, 2004b), the SEC noted,

> ***'s conduct, known in the industry as "spoofing," is illustrated by the following example:
>
> - 12:27:11 - *** placed an order to sell short 100 shares of the target security at $15.80 ... The order lowered the [market ask] price from $16.16 to $15.80;
> - 12:27:13 - *** entered a limit order to *buy* [emphasis ours] 500 shares of the target security at a price of $15.80, and the order was immediately executed [by a market-maker who guaranteed execution at the market ask].
> - 12:27:28 - *** cancelled his sell order.
>
> By improperly altering the public quote to obtain a better execution price for the buy order, *** was unjustly enriched in the amount of $180 [= ($16.16 − $15.80) × 500 shares]

This example lacks an exact correspondence on a DEX, because DEXs don't have bids and asks. Moving the reference price to obtain favorable executions on subsequent orders, however, is the essence of a sandwich attack.

The final instance, triggering, involves a special type of order. "Stop" orders submitted to a market are flagged so that their display and execution will be delayed until the last-sale price passes through some preset threshold (the stop price). If there are many such orders in the same direction and with stop prices close together, the triggering of one order may cause a trade that triggers another, and so on, cascading and generating a strong price. In the foreign exchange market, "[the UK Financial Conduct Authority] found that traders were sharing details about their [customers'] stop-loss orders with traders at other firms. Both would then trade in a manner designed to change the spot FX rate, and thus trigger the stop-loss order," (Kuhn and Bushnell, undated). As in the other cases, knowledge of a set of orders together with the ability to interject one's own orders can affect outcomes.

In these examples, the malefactors generated something analogous to MEV. They would presumably surrender some portion of the gains to ensure that their transactions would be settled on their terms. The resulting outcomes might be - in a narrow sense, at least - informationally efficient and pareto optimal. Yet in all cases, the practices are viewed as fraudulent.

5 Evolution of Decentralized Exchange

DEXs represent the most recent evolution in the more general concept of peer-to-peer exchange. In a general sense, a decentralized exchange of assets is any peer-to-peer transfer of assets without an intermediary. Barter is an example of peer-to-peer exchange. Any modern exchange of an asset for physical fiat currency is another form of peer-to-peer exchange.[30] In this section we examine the broader concept of decentralized exchange and discuss the role played by DEXs in the evolution of this concept.

5.1 From Decentralized Exchange to DEXs

The simplest form of decentralized exchange is a peer-to-peer cash payment. While a peer-to-peer cash payment may be desirable because it does not require an intermediary, it is nonetheless inefficient for large value transfers and therefore impractical for many payments. Holding cash involves an opportunity cost of investment and also an inconvenience of needing to store the physical cash. These costs increase with the value being transferred and thus large cash payments are not practical.

Ultimately, the appeal of peer-to-peer decentralized exchange coupled with the impracticality of using physical cash for such exchange motivated the creation of the Bitcoin blockchain (Nakamoto, 2008). To that end, the Bitcoin blockchain facilitates digital peer-to-peer payments thereby offering a practical method for large decentralized value transfers. Bitcoin facilitates such peer-to-peer payments by creating an asset that settles directly on the Bitcoin blockchain, BTC, and by allowing users to transfer this asset peer-to-peer without an intermediary. Any amount of value therefore can be transferred peer-to-peer over the Bitcoin blockchain so long as the value is sent in the form of BTC.

While Bitcoin made an important first step by facilitating decentralized peer-to-peer payments, it did not enable a two-legged decentralized exchange of assets in which a user both sends and receives an asset. While Bitcoin enables a user to send value, it does not allow the user to send value in return for another asset of value. Rather, this type of decentralized exchange is the innovation characterizing DEXs. DEXs permit a user to acquire any asset settled on a blockchain in return for a payment in terms of any other asset settled on a blockchain. DEXs implement the exchange without an intermediary and thus the exchange is decentralized.

While DEXs do not involve intermediaries, they nonetheless do not implement direct peer-to-peer exchanges. A DEX liquidity pool is a smart contract, and DEX trades occur at the liquidity pool because users deposits liquidity at the smart contract and traders then

[30] See Harvey, Ramachandran, and Santoro (2021) for a historical perspective on decentralized exchange.

swap assets with the smart contract (e.g., ETH for DAI). Thus, DEX is facilitated through peer-to-smart contract exchanges and not through direct peer-to-peer exchanges. Smart contracts have no discretion to act and simply execute their defining code logic. As such, while DEX trades involve no intermediary and are decentralized exchanges, they are not peer-to-peer.

5.2 Evolution of DEXs

DEXs are not a static technology. In fact, DEXs have evolved significantly since their inception. On one hand, the design of individual DEXs have advanced. On the other hand, the ecosystem of DEXs has also evolved with interactions among DEXs. We will consider each of these points in turn.

5.2.1 Evolution of DEX Design

Our discussion of the evolution of DEX design focuses on the most prominent DEX, Uniswap. Uniswap's first prominent deployment, Uniswap v2, is a simple construction, featuring a single liquidity pool for each asset pair and a constant product AMM for pricing within each liquidity pool. Furthermore, Uniswap v2 features *uniform liquidity provision*. This means that any liquidity provided to a liquidity pool is used uniformly for all trades at that liquidity pool irrespective of the execution price. In contrast, Uniswap's subsequent deployment, Uniswap v3, allows for *concentrated liquidity provision*, whereby a liquidity provider may specify that the assets they provide would be used only for trades executed within specific price ranges (Hasbrouck et al., 2023). The motivation behind allowing for concentrated liquidity is that Uniswap v2's uniform liquidity effectively dispersed liquidity across all price levels, even price levels unlikely to be reached. Still, Uniswap v3's concentrated liquidity explicitly enables liquidity providers to focus their liquidity near current prices, thereby facilitating higher effective liquidity for trading even when liquidity providers invest an identical total level of capital.

Uniswap has recently launched Uniswap X, a web interface that seeks to facilitate better pricing for traders. Uniswap X combines a *router* with the opportunity for market-makers to fill each order. A router is software that seeks to determine the lowest cost execution for a trade across many liquidity pools, and Uniswap X's router specifically seeks the lowest cost execution across all Uniswap liquidity pools (both v2 and v3). In contrast, the process that involves market makers begins with a Request For Quote (RFQ) from a whitelisted set of market makers. The most competitive quote from the RFQ is compared to the lowest cost execution through Uniswap liquidity pools determined by the router. If the router

execution cost is lower than the RFQ's most competitive quote, then the order is executed directly through the pools specified by the router. Otherwise, a competitive descending price auction process is triggered in which the prices descend block by block over the course of the auction. This descending price auction relates to the RFQ only because the descending prices associated with each block are determined by the RFQ results. The auction is competitive because any market maker (even those not white-listed) can seek to fill the order on any block during the auction so long as the order has not already been filled. Since any market maker can fill the order, multiple market makers may seek to fill the order on the same block. The auction price descends block-by-block so that the execution price is fixed for a given block. In turn, multiple market makers competing to fill on the same block do not compete on price; rather, they compete for priority within the block by offering higher fees to the block builder with only the market-maker receiving the highest priority within the block filling the order. The block-by-block descending price auction has a block limit (effectively a time limit), and the order is left unfilled if no market-maker meets the required fixed price for any block during the auction. If the descending price auction fails, the trader may re-start the process by querying the Uniswap X interface again.

Uniswap is planning a new deployment, Uniswap v4. Uniswap 4's primary innovation is the incorporation of *hooks*, which are custom smart contracts that allow for code logic that conforms to a pre-specified interface.[31] Each liquidity pool would be associated with a single hook smart contract. Then, when trading through a particular pool at Uniswap v4, the code logic to be executed would be partly from the code within the pool's hook smart contract and partly from Uniswap v4's core smart contracts. Ultimately, hooks would enable a higher level of customization than prior DEX deployments. Some notable ideas for hooks include White-listing and MEV internalization. White-listing refers to maintaining a list of pre-approved user identities and allowing trades only submitted by user identities from the pre-approved list. MEV internalization refers to attempts to monetize profits from exploitative activities (e.g., front-running) and to distribute those profits back to traders. In fact, Flashbots has already implemented a version of MEV internalization, "MEV-Share", that allows for some redistribution of the MEV to the users.

MEV-Share is a modest beginning, while the functionality of Uniswap v4's hooks may facilitate further MEV internalization. The functionality of Uniswap v4's hooks may allow traders to be compensated for their losses from MEV beyond backruns and without the involvement of an intermediary (e.g., Flashbots). Additionally, if the MEV extraction is sufficiently competitive, then traders may be able to recoup almost all their losses.

[31] The code interface, IHook, is available at https://github.com/Uniswap/v4-core/blob/1dda6f5095e88a82a6249089fbc827a4a12abcf5/src/interfaces/IHooks.sol.

5.2.2 Interaction Across DEXs

Our analysis thus far has focused upon a single liquidity pool at a single DEX in isolation. But there are many DEXs in practice, and these DEXs frequently involve overlapping liquidity pools. For example, multiple ETH-DAI liquidity pools are spread across DEXs. This redundancy of liquidity pools across DEXs implies that the lowest trading cost might be achieved by trading across multiple DEXs simultaneously. An advantage of blockchain technology is that multiple legs of a trade can be executed simultaneously and atomically even if the legs of the trade are at different DEXs. In fact, as a consequence, entities called *aggregators* have arisen to facilitate trading across DEXs.[32] , DEX aggregators provide pricing by determining the lowest cost execution across various sources. The specific sources consulted by DEX aggregators generally fall into two categories: routers and market makers. Routers corresponds to a software and seek the minimal cost execution through specific liquidity pools. In contrast, market-makers correspond to users who compete to provide liquidity on a trade-by-trade basis through an RFQ process.

There are several fundamental difficulties in designing a DEX aggregator. First, each router considers only a subset of available liquidity pools so that each router's pricing is likely sub-optimal relative to the lowest cost execution across all liquidity pools. Second, even if all liquidity pools were considered by a single router, the mathematical problem of determining the lowest cost execution across an arbitrary set of liquidity pools is non-trivial due to the heterogeneity in the pricing of different liquidity pools. Third, the set of market-makers consulted for the RFQ process are a subset of all possible liquidity providers, and thus the RFQ process may not reflect pricing from a fully competitive liquidity provision market. Finally, there are also concerns about market makers providing competitive quotes and then opting not to fill the order, resulting in trade failures.

Although theoretically possible, a router cannot realistically incorporate all liquidity pools on a blockchain. The permissionless nature of blockchain (see Section 3.1.2) implies that any user can deploy a new DEX at any time and new liquidity pools within new DEXs at any time. Furthermore, smart contracts characterizing a DEX are not easily distinguishable from other smart contracts. Thus, any router seeking to incorporate all liquidity pools would have to be constantly revised to capture all DEXs and, even if a router were revised regularly, it might overlook some DEXs.

[32] A related set of entities that have arisen are *solvers*. Solvers aggregate across aggregators. For the sake of brevity, we do not discuss solvers in detail.

6 Conclusion

Decentralized exchanges represent an important innovation in finance. In particular, they enable asset swaps at transparent pricing terms with simultaneous trade settlement and trade execution. Anyone with a wallet can trade on a DEX almost instantly. There is no registration and no need to establish an "account" at a DEX. The DEXs are also interconnected, so a user can buy on one DEX and sell on another in the same transaction. Liquidity is relatively constant and available 24-7. Holders of assets can earn extra funds by providing their assets to DEX liquidity pools.

DEXs also involve a variety of novel risks. Given the algorithmic pricing function, prices do not immediately jump when new information arises leading to arbitrage among CEXs and DEXs. That said, in equilibrium, the fees that liquidity providers earn should exceed losses due to this sniping. More seriously, due to the nature of consensus in the Ethereum blockchain, pending transactions are visible to anyone. Those constructing the blocks of transactions can insert trades just before a larger order to front run the order.

There is no straightforward strategy for a national regulator. DEX is a global technology. A regulator could limit or prohibit access to a DEX in a particular country, but trading would proceed in other countries. One approach would be to sanction the users of DEX - but this goes against the initial motivation for exchange regulation. The original statutes were designed to protect users - not to sanction them. Another unproductive strategy is to focus on the DEX itself. This makes little sense because a DEX is an immutable algorithm deployed to a blockchain. While it might be possible to sanction the creator of the DEX, due to the nature of the technology, a DEX can be deployed by a (nearly) anonymous address. Often there is a "lab" entity associated with a DEX, (*e.g., Uniswap Labs) so another strategy is to try to regulate the lab entity. However, this too has multiple issues. First, the lab does not control the existing DEXs. Second, this approach might increase risk for users since the lab often serves useful function deploying updated algorithms that patch bugs and thereby ameliorating user risk. Yet another approach would be to try to regulate the block builders. Given the global nature of the technology, this seems infeasible.

One potential regulatory strategy is to let this innovation play out in a Safe Harbor or Regulatory Sandbox environment. There are already indications that some of the negative outgrowths, in particular, front running, may be naturally mitigated. The basic idea is to allow the front running but to give those that are front run a rebate. With the competitive efficiency, this rebate should eventually cover almost all of the loss. The remaining loss is just an additional (small) cost of trading. Layer 2 technologies with a first-in, first-out strategy may also mitigate the front running. Finally, researchers are exploring technologies

that enforce verifiable rules regarding the ordering of transactions (Ferreira, Venturyne, and Parkes, 2023).

The recent evolution of trading has incorporated a combination of DEX and other venues such as private pools. Traders will have many options as to where to execute: a centralized exchange, DEX, a request for quote market, or some combination. In the future, centralized exchanges will likely utilize DEXs as well as their order books to provide the best possible prices for their customers. This offers an intriguing possibility: the existing regulatory oversight of centralized exchanges might create an indirect way to conduct oversight of decentralized exchanges. For example, a centralized exchange utilizing a DEX may conduct due diligence on all assets purchased from the DEX to ensure that such assets are appropriate for the centralized exchange customers.

The decentralized nature of this technology poses another risk: DEX trading is available to anyone, even OFAC-sanctioned entities. While some block builders may avoid sanctioned addresses, this only delays the trading of sanctioned entities so long as some builders accept transactions from sanctioned addresses. Further, even if all block builders refused to include transactions from sanctioned addresses, those that are sanctioned could create new addresses that are not in the registry yet. This is a vexing problem with no obvious solution.

This space is progressing rapidly. We are seeing only one frame of a movie whose next scene has yet to be written. Most of the activity in the blockchain setting has been dominated by speculative traders. Satoshi Nakamoto's original vision of replacing the existing financial architecture with a new transaction mechanism has been supplanted by the so-called store of value role for crypto. However, there are signs that this is changing. Layer 2 technologies that vastly reduce the cost of trading provide a credible alternative transaction mechanism. Furthermore, we are seeing the gradual introduction of tokenized real world assets. Traditional financial institutions such as the $11 trillion asset manager, BlackRock, have fully embraced tokenization and have launched products in the space. While DEX might seem a relatively modest size today, increasing tokenization suggests a larger role for DEX in the future.

As with any new technology, DEX is not risk free. Regulators should reflect on the big picture: this technology promises to substantially reduce transactions costs which is a positive force for economic well being and growth. The technology also offers financial democracy - there are no distinctions between retail, institutional, banker, broker, or customer in decentralized finance - everyone is a peer. This may be a time to carefully monitor with a light rather than heavy hand. For example, some MEV issues are likely to naturally mitigate. Regulators should measure this progress. They also might want to leverage the existing regulatory oversight of centralized exchanges so that CEXs can carefully monitor

the subset of DEXs they deem useful for their customers.

References

Bank for International Settlements, 2023. Project Mariana: Cross-border exchange of wholesale CBDCs using automated market-makers (Final report). https://www.bis.org/publ/othp75.htm.

Buterin, V., 2014. A next-generation smart contract and decentralized application platform. Ethereum White Paper .

Cao, D., Hemenway Falk, B., Tsoukalas, G., 2023. Automated market makers and the value of adaptive fees. Available at SSRN .

Capponi, A., Jia, R., 2021. The adoption of blockchain-based decentralized exchanges. Columbia University Working Paper .

Capponi, A., Jia, R., Wang, Y., 2023a. Maximal extractable value and allocative inefficiencies in public blockchains. arXiv preprint arXiv:2202.05779 .

Capponi, A., Jia, R., Zhu, B., 2023b. The paradox of just-in-time liquidity in decentralized exchanges: More providers can sometimes mean less liquidity. Available at SSRN .

Christie, W. G., Harris, J. H., Schultz, P. H., 1994. Why did Nasdaq market makers stop avoiding odd-eighth quotes? Journal of Finance 49, 1841–60.

Christie, W. G., Schultz, P. H., 1994. Why do Nasdaq market makers avoid odd-eighth quotes? The Journal of Finance 49, 1813–1840.

Christie, W. G., Schultz, P. H., 1995. Policy watch: Did Nasdaq market makers implicitly collude? Journal of Economic Perspectives 9, 199–208.

Cohen, L., Strong, G., Lewin, F., Chen, S., 2022. The ineluctable modality of securities law: Why fungible crypto assets are not securities. Available at SSRN 4282385 .

Cong, L. W., Harvey, C. R., Rabetti, D., Wu, Z.-Y., 2023. An anatomy of crypto-enabled cybercrimes. Tech. rep., National Bureau of Economic Research.

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A., 2020. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. 2020 IEEE Symposium on Security and Privacy (SP) pp. 910–927.

Ernst, T., Spatt, C. S., Sun, J., 2022. Would order-by-order auctions be competitive?

Ferreira, X., Venturyne, M., Parkes, D. C., 2023. Credible decentralized exchange design via verifiable sequencing rules. In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, ACM, STOC '23.

Garman, M., 1976. Market microstructure. Journal of Financial Economics 3, 257–275.

Glosten, L. R., Milgrom, P. R., 1985. Bid, ask, and transaction prices in a specialist market with heterogeneously informed traders. Journal of Financial Economics 14, 71–100.

Haqshanas, R., 2023. SushiSwap Exchange Suffers Major $3.3 Million Smart Contract Hack – Here's What Happened. https://cryptonews.com/news/sushiswap-exchange-suffers-major-33-million-smart-contract-hack-heres-what-happened.htm, accessed: 2024-01-11.

Harvey, C. R., Ramachandran, A., Santoro, J., 2021. DeFi and the Future of Finance. John Wiley and Sons, Hoboken, NY.

Hasbrouck, J., 2023. Securities Trading: Principles and Procedures. Draft teaching notes at https://pages.stern.nyu.edu/~jhasbrou/STPP/STPPindex.html.

Hasbrouck, J., Rivera, T. J., Saleh, F., 2022. The need for fees at a DEX: How increases in fees can increase DEX trading volume https://ssrn.com/abstract=4192925.

Hasbrouck, J., Rivera, T. J., Saleh, F., 2023. An economic model of a decentralized exchange with concentrated liquidity https://ssrn.com/abstract=4529513.

Heimbach, L., Kiffer, L., Ferreira Torres, C., Wattenhofer, R., 2023. Ethereum's proposer-builder separation: Promises and realities. In: *Proceedings of the 2023 ACM on Internet Measurement Conference*, Association for Computing Machinery, New York, NY, USA, IMC '23, p. 406–420.

International Monetary Fund, 2023. Elements of Effective Policies for Crypto Assets. https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092.

John, K., Monnot, B., Mueller, P., Saleh, F., Schwarz-Schilling, C., 2024. Economics of ethereum.

John, K., O'Hara, M., Saleh, F., 2022. Bitcoin and beyond. Annual Review of Financial Economics 14, 95–115.

Johnson, D., Menezes, A., Vanstone, S., 2001. The elliptic curve digital signature algorithm (ecdsa). International journal of information security 1, 36–63.

Kuhn, C., Bushnell, T., undated. The fx remediation programme. https://www.hickmanandrose.co.uk/cms/documents/remediation_programme.pdf.

Kyle, A. S., 1985. Continuous auctions and insider trading. Econometrica 53, 1315–1336.

Lehar, A., Parlour, C. A., 2021. Decentralized exchanges. Available at SSRN 3905316 .

Linehan, P., Heath, W., Shulkin, J., 2021. The evolving line between legal and illegal trading and sales practices in the market intermediary and customer relationship. https://www.steptoe.com/a/web/215875/linehan-heath-shulkin.pdf.

Liu, C., Liu, H., Cao, Z., Chen, Z., Chen, B., Roscoe, B., 2018. Reguard: finding reentrancy bugs in smart contracts. In: *Proceedings of the 40th International Conference on Software Engineering: Companion Proceeedings*, Association for Computing Machinery, New York, NY, USA, ICSE '18, p. 65–68.

Loader, D., 2019. Clearing, Settlement, And Custody. Butterworth-Heinemann (Elsevier), Oxford, UK, third ed.

Malinova, K., Park, A., 2023. Learning from defi: Would automated market makers improve equity trading?

MarsNext, 2023. Kyberswap hacked for $46 million: A reentrancy attack drains #defi exchange. https://www.binance.com/en/feed/post/520751216026, accessed: 2024-01-11.

Mendelson, M., Peake, J. W., 1979. The ABCs of trading on a national market system. Financial Analysts Journal 35, 31–34 and 37–42, http://www.jstor.org/stable/4478272.

Milionis, J., Moallemi, C. C., Roughgarden, T., Zhang, A. L., 2022. Automated market making and loss-versus-rebalancing. arXiv preprint arXiv:2208.06046 .

Morris, V. B., 2022. Guide to clearance and settlement: An introduction to DTCC. https://www.dtcc.com/-/media/Files/Downloads/DTCC-Connection/DTCC-Interactive-Guide-to-Clearance-and-Settlement-2022.pdf.

Nakamoto, S., 2008. Bitcoin whitepaper. URL: https://bitcoin.org/bitcoin .

New York Stock Exchange, 1989. Memorandum to members: New specialist job description. Attachment to testimony of John J. Phelan, Jr., Chairman And Chief Executive Officer,

The New York Stock Exchange to The Senate Banking Committee Securities Subcommittee (May 18, 1989).

Park, A., 2023. The conceptual flaws of decentralized automated market making. Management Science 69, 6731–6751.

Saleh, F., 2021. Blockchain without waste: Proof-of-stake. The Review of financial studies 34, 1156–1190.

Schwarz-Schilling, C., Saleh, F., Thiery, T., Pan, J., Shah, N., Monnot, B., 2023. Time is money: Strategic timing games in proof-of-stake protocols. arXiv preprint arXiv:2305.09032 .

Stoll, H., 1976. Dealer inventory behavior: An empirical examination of Nasdaq stocks. Journal of Financial and Quantitative Analysis 11, 359–380.

U.S. Securities and Exchange Commission, 1963. Special Study of the Securities Markets. http://www.sechistorical.org/collection/papers/1960/1963_SS_Sec_Markets/.

U.S. Securities and Exchange Commission, 1994. Market 2000: An Examination of Current Equity Market Developments. https://www.sec.gov/divisions/marketreg/market2000.pdf.

U.S. Securities and Exchange Commission, 1996a. [release no. 34-37619a; file no. s7-30-95] final rule: Order execution obligations. /urlhttp://www.sec.gov/rules/final/37619a.txt .

U.S. Securities and Exchange Commission, 1996b. Report Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding the NASD and the Nasdaq Market. http://www.sec.gov/litigation/investreport/nasdaq21a.htm.

U.S. Securities and Exchange Commission, 2000. Special Study: Electronic Communications Networks and After-Hours Trading. https://www.sec.gov/news/studies/ecnafter.htm.

U.S. Securities and Exchange Commission, 2004a. In the Matter of: Spear, Leeds & Kellogg Specialists LLC, Release No. 49501 / March 30, 2004. https://www.sec.gov/litigation/admin/34-49501.

U.S. Securities and Exchange Commission, 2004b. Securities Exchange Act of 1934 Release No. 50046 (Administrative Proceeding File No. 3-11468). https://www.sec.gov/litigation/admin/34-50046.

U.S. Securities and Exchange Commission, 2004c. Settlement Reached With Five Specialist Firms for Violating Federal Securities Laws and NYSE Regulations. https://www.sec.gov/news/press/2004-42.htm.

U.S. Securities and Exchange Commission, 2005. Regulation NMS (Final Rule Release No. 34-51808; June 9, 2005). http://www.sec.gov/rules/final/34-51808.pdf.

U.S. Securities and Exchange Commission, 2020. [Release No. 34-90019; File No. S7-12-20] Regulation ATS for ATSs that Trade U.S. Government Securities, NMS Stock, and Other Securities; Regulation SCI for ATSs that Trade U.S. Treasury Securities and Agency Securities; and Electronic Corporate Bond and Municipal Securities Markets. https://www.sec.gov/files/rules/proposed/2020/34-90019.pdf.

U.S. Securities and Exchange Commission, 2022a. Complaint (Case 22-cv-10542) United States Securities and Exchange Commission v. Lawrence Billimek, and Alan Williams. https://www.sec.gov/files/litigation/complaints/2022/comp-pr2022-228.pdf.

U.S. Securities and Exchange Commission, 2022b. [Release No. 34-94062; File No. S7-02-22] Amendments Regarding the Definition of "Exchange" and Alternative Trading Systems (ATSs) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities. https://www.sec.gov/files/rules/proposed/2022/34-94062.pdf.

U.S. Securities and Exchange Commission, 2023. [Release No. 34-97309; File No. S7-02-22] Supplemental Information and Reopening of Comment Period for Amendments Regarding the Definition of "Exchange". https://www.sec.gov/files/rules/proposed/2023/34-97309.pdf.

Wahrstätter, A., Ernstberger, J., Yaish, A., Zhou, L., Qin, K., Tsuchiya, T., Steinhorst, S., Svetinovic, D., Christin, N., Barczentewicz, M., et al., 2023. Blockchain censorship. arXiv preprint arXiv:2305.18545 .

Wood, G., 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper 151, 1–32.

Yaish, A., Dotan, M., Qin, K., Zohar, A., Gervais, A., 2023. Suboptimality in defi. Cryptology ePrint Archive .