

# Fair Price Discovery with Decentralized Exchange

Yehuda Jay Berg  
jaybny@gmail.com

May 2021

## Abstract

## 1 Introduction

Ever since Satoshi solved peer to peer digital cash with the Bitcoin protocol, people have been trying to apply similar techniques to other hard problems. Peer to peer decentralized exchange (DEX), is one of the most difficult of these problems.

The purpose of an exchange in financial markets, is to first match buyers and sellers of financial assets at a *market* price, and then to provide settlement to mitigate any counterparty risk. Tradition electronic exchanges are designed with the goal of reaching a *price discovery* equilibrium [3]. Centralized exchanges (CEXs), employ continuous limit order books as a price discovery mechanism.

Due to well known centralized exchange hacks, coupled with the technical difficulty of decentralized limit order books, most DEXs are solely focused on the non-custodial settlement, rather than *price discovery*.

**Price discovery** is a social benefit and a key goal in the design of a market structure. In fact, the goal of the architecture of an exchange mechanism, is to attract as much liquidity needed to for price discovery. [3]

Price discovery is described in microstructure research as a search for an equilibrium price based on new external information. This new information is reflected in the traders orders, and is ultimately converted into a market price. [6]

Some even define an exchange as “any trading facility that has as its primary function the delivery of good price discovery” [3].

However, the price discovery function of an exchange typically receives insufficient attention in market structure discussions. This is largely attributable to the non-observability of equilibrium prices and, therefore, to the difficulty of quantifying the deviations of transaction prices from their equilibrium values [3]

price discovery is dynamic in nature, and an efficient price discovery process is characterized by the fast adjustment of market prices from the old equilibrium to the new equilibrium with the arrival of new information [7]

**Limit order books** and price discovery are tightly related. [6] [4]

To achieve price discovery exchanges offer two order types. Limit orders, and Market orders. All orders are sent to a centralized matching engine in the exchange servers.

Market orders have a quantity but no price.

1. "Buy 1 @ market" - an order to buy 1 unit of the asset at the market

Limit orders have a quantity and a price.

1. "Buy 1 @ 100" - an order to buy 1 unit of the asset at the market

**Continuous limit order books (CLOB)** are the market micro structure that leads to price discovery <sup>1</sup>. There are two order types. Limit orders, where you provide your own price, with the risk of waiting to be matched. And market-orders, where you get filled immediately in return for a possible worse price.

The interaction between market orders matching limit orders is continuous.

The state of a CLOB in a centralized exchange is shown to produce a price discovery equilibrium.

The design of CLOB evolved from previous exchanges, Futures trading pits in Chicago reached a price discovery.

For the purpose of price discovery, the match of buyers and seller needs to be atomic, otherwise one party can pull out of the deal.

---

<sup>1</sup>Other types of markets such as call auctions, and dealer markets, do not provide the robustness of limit orders for price discovery. [2]

## Evolution of Exchange

## The HFT Problem

## Blockchain DEX Problems

## MEV and Public Blockchains

## Front-Running and Permissioned Blockchains

## Transaction Ordering

## Why does it not work?

## New Blockchain Abstraction

**Limit order books** and price discovery are tightly related. [6] [4]

To achieve price discovery exchanges offer two order types. Limit orders, and Market orders. All orders are sent to a centralized matching engine in the exchange servers.

Market orders have a quantity but no price.

1. "Buy 1 @ market" - an order to buy 1 unit of the asset at the market

Limit orders have a quantity and a price.

1. "Buy 1 @ 100" - an order to buy 1 unit of the asset at the market

Price discovery happens by pooling liquidity from many buyers and many sellers.

Decentralized exchanges

To date most decentralized exchanges (DEXs) forgoes the traditional mechanism employed by traditional centralized exchanges (CEXs), namely limit order books (LOBs).

Many have attempted to design decentralized exchanges

Decentralized exchanges (DEX)

Ever since Satoshi solved peer to peer digital cash with Bitcoin, people have been trying to apply similar techniques to solve other hard problems. One such problem, peer to peer exchange, is one of the most difficult of these problems. An exchange is a financial market, where trading of securities occur. The purpose of an exchange is two fold; 1) for price discovery, 2) for counterparty settlement. Centralized Exchanges, have been well researched and developed in traditional finance for well over a century. They evolved from trading under a tree, to the Chicago trading pits, to electronic exchanges with continuous limit order books. Modern exchanges provide 24/7 trading, and offer co-location for the most prolific traders, high frequency trading bots. Other decentralized exchanges aim to bring traditional centralized exchanges into a peer to peer blockchain protocol. Due to early bitcoin exchange hacks most research has been focused on the settlement utility of exchange. We focus on the price discovery utility, an emergent property of real-time trading. We

present fair price discovery with decentralized exchange by solving the impossible task of consensus on total ordering of transactions to mitigate front-running.

An exchange is a financial market, where trading of securities occur. The pupose of an exchange is two fold. 1) for price discovery, 2) for counter party settlement..

Centralized Exchanges (CEX), have been well researched and developed in traditional finaince for well over a century. [exchage cite] They evoled from trading under a tree, the Chicago trading pits, to electroic exchanges with continuous limit order books. Modern exchanges provide 24/7 trading, and offer co-location for the most prolific traders, High Freaquency Trading (HFT) bots.

Decentralized exchange (DEX), aims to bring tradition centralized exchanges into a peer to peer blockchain protocol. Due to early bitcoin CEX hacks, most DEXs have been focused on the settlement utility of exchange. As price discovery is an emergent property of the real-time trading and difficult to research.

We present a DEX with focus on providing price discovery. Our solution, Fair Price Disovery (FPD)

## 2 Introduction2

Ever since bitcoin solved peer to peer digital cash was possible, poeple have been trying to apply similar technoques to solve other hard problems. One such problem, peer to peer exchange, is one of the most difficult of these problems.

An exchange is a financial market, where trading of securities occur. The pupose of an exchange is two fold. 1) for price discovery, 2) for counter party settlement..

Centralized Exchanges (CEX), have been well researched and developed in traditional finaince for well over a century. [exchage cite] They evoled from trading under a tree, the Chicago trading pits, to electroic exchanges with continuous limit order books. Modern exchanges provide 24/7 trading, and offer co-location for the most prolific traders, High Freaquency Trading (HFT) bots.

Decentralized exchange (DEX), aims to bring tradition centralized exchanges into a peer to peer blockchain protocol. Due to early bitcoin CEX hacks, most DEXs have been focused on the settlement utility of exchange. As price discovery is an emergent property of the real-time trading and difficult to research.

The word "central" is part of the common definitio of an exchange. "A central place where buying and sellers come to finf price and execute trades.

The pupose of exchange is two fold. 1 - for price disoverry [cite] 2 - for counter party settlement

Due to early bitcoin exchange hacks, Decentrized Exchange or (DEX), has been mostly focused on the non-custodial side for the settlement utility.

We focusing on the real public service of an Exchange, the price discovery utility. We design price discovery within a DEX, with a pupose of "Fair Price Discovery".

With, Fair Price Discovery (FPD), as our goal. We focus on a mechanism designed exchange, for reaching equilibrium which produces price.

Taking inspiration from Rational Protocol Design analysis of Bitcoin, and looking back to the original Bitcoin white-paper.

examining the state of the art in price-discovery, High Frequency Market Making, and electronic exchange matching engines

Since Bitcoin showed us how peer to peer electronic cash was possible, we have re-searching if and how peer-to-peer exchange was possible.

Exchanges are a critical part of the financial markets.

Ecological balance otherwise the order-driven market can collapse Transparency is an important feature

first to win is most important

## Price Discovery

Price discovery as a key goal in the design of the market structure. In fact, the goal of the architecture of an exchange mechanism, is to attract as much liquidity needed to for price discovery. [3]

Price discovery is described in microstructure research as a search for an equilibrium price, from new external information. This new information is reflected in the traders orders, and is ultimately converted into a market price. [6]

price discovery is dynamic in nature, and an efficient price discovery process is characterized by the fast adjustment of market prices from the old equilibrium to the new equilibrium with the arrival of new information [7]

From a definitional perspective, any trading facility that has as its primary function the delivery of good price discovery can, de facto at least, be considered an exchange. Unfortunately, however, the price discovery function of an exchange typically receives insufficient attention in market structure discussions. This is largely attributable to the non-observability of equilibrium prices and, therefore, to the difficulty of quantifying the deviations of transaction prices from their equilibrium values [3]

**Limit order books** and price discovery are tightly related. [6] [4]

To achieve price discovery exchanges offer two order types. Limit orders, and Market orders. All orders are sent to a centralized matching engine in the exchange servers.

Market orders have a quantity but no price.

1. "Buy 1 @ market" - an order to buy 1 unit of the asset at the market

Limit orders have a quantity and a price.

1. "Buy 1 @ 100" - an order to buy 1 unit of the asset at the market

**Continuous limit order books (CLOB)** are the market micro structure that leads to price discovery <sup>2</sup>. There are two order types. Limit orders, where you provide your own price, with the risk of waiting to be matched. And market-orders, where you get filled immediately in return for a possible worse price.

Directional liquidity traders - use market orders Market Makers - use limit orders

HFT-bandit

**Adverse Selection** Show HFT Alpha Show how market-orders are the cryponite

## Perfect Alpha and the High Frequency Trading (HFT) arms race

We define *Perfect Alpha* as recurring risk-less real-time arbitrage with positive EV. Believe it or not, *Perfect Alpha* is a product of centralized exchanges and continuous limit-order books.

**Theorem 1** *When 2 or more orders come in after your order, there exists a free arbitrage, provided 1) each order is for 1 share at a time, 2) you are first to act. Perfect Alpha exists in Continuous Limit Order books.*

1. HFT - "Buy 1 @ 100"
2. Bob - "Buy 1 @ 100"

qty	bid	ask	qty
2	100		

## 2.1 Decentralized Limit Order Books

make these problems much worse, by removing the one defensive market-order

## 2.2 Standard Blockchain Solutions

### 2.2.1 Permissionless

**Ethereum** smart contracts create MEV

---

<sup>2</sup>Other types of markets such as call auctions, and dealer markets, don't provide the robustness of limit orders for price discovery. [2]

MEV and front-running

Uniswap -

Total Ordering Consensus

### **2.2.2 Permissioned blockchains**

remove the issues with open blockchains, and uses BFT techniques

### **2.2.3 Why does bitcoin work**

Only when asking why? do we come with a new theory *Ration Design*

### **2.2.4 Why does it not work with Ethereum, Aequitas and BFT?**

The problem is abstractions. Solving generic solution with frameworks vs solving for a specific utility

## **3 A new blockchain abstraction**

Only when designing for a specific utility are we able to use designer intent vs adversarial motivations

1. First design with intent using Mechanism Design
2. Release the code and protocol
3. Test results from empirical evidence

We now have mechanism designed system that matched a rational design theory of decentralized exchange.

## **4 Fair Price Discovery**

## **5 Decentralized Limit Order Books**

We start with a closed network of exchange nodes, which each node has a matching-engine and maintains a CLOB, much like a centralized exchange.

The distributed network of nodes come to consensus on the total ordering of transactions. This is done in two steps:

1. *block-data* consensus is reached every N seconds on the full list of transactions from the mempool.
2. *block-order* consensus is reached via auction on each block, where the highest bidder gets to reorder the transactions in the *block-data*

From these two simple steps we have removed the advantage of HFT co-location, the need to front-run, and for *Miner Extracted Value*

**HFT Co-Location** is no longer possible as there is no single location for the matching engine. Furthermore, the notion of *being first* goes away, as all orders within the block are the same in regards to time. Also, since you can pay to *be first* after the fact, there is no longer justification of cost of the HFT arms race.

**Front-running** by *rushing* has no advantage, as the processing order is not determined by which transaction was seen first on the network.

**Miner Extracted Value** is no longer possible, as we come to consensus on the entire mempool, for each block. Recall, that *MEV* is defined as a miner choosing, ordering or adding new transactions into a block in a way that generates economic value. In our model, each block contains all the outstanding transactions, and the transactions in *block-data* are in no particular order for processing, until after the *block-order* auction.

Acknowledging the Condorcet paradox the impossibility of fair ordering [5]

In addition to a CLOB, each node also maintains the state of all accounts mapped to a *pub-key*

## 5.1 Centralized Fair Price Discovery

Starting with a centralized exchange we create a distributed limit order book to reach fair price discovery. Each exchange member will control its own matching-engine node and maintain an orderbook state.

**Create a network of known nodes** , with each node identified by an ip adress and a *pub-key* based address.

**Nodes crate new transactions** , and broadcast them to each node onthe network. Transactions propogate through the network via a gossip with each node identified by an ip adress and a *pub-key* based address.



## 5.2 Preliminaries

Order book transactions are like advertisements. Sender wants to broadcast intent. Intent of others seeing your transactions eliminates the commit/reveal strategies

1. Full transparency - no commit-reveal
2. Remove rent-seeking co-location
3. Acknowledge impossibility of total-ordering Consensus
4. Make front-running explicit, but limited to reordering - no inserting new orders

Centralized matching gives market-order privacy in return for co-location issues  
Decentralized matching removes co-location advantage in return for loss of market-order privacy

**Covert Adversaries** we learn that just being able to show cheating can reduce it.

## 5.3 On-Chain Solution

We focus on solving for decentralized matching engine that results in price discovery. Note, an on-chain solution with assets controlled by the protocol eliminates the centralized custody and settlement issues.

Goal is to eliminate front-running when there is consensus on order, and allow explicit front-running where total order consensus is not possible.

Step1: Hybrid blockchain, acts permissioned with BFT consensus by each node selecting quorum slices ( Stellar ) Step2: Node selects quorums based on reputation and trading activity. Bigger trading operations with good uptime, and heavy volume, will be selected by many. Step3: Reach consensus on mempool on past 5 seconds. Step4: Pay to re-order blocks by bribing bitcoin miners, or paying centralized exchange operator or burning coins.

### 5.3.1 Order transaction types

- limit and market and cancels.

Buy 1 at 100 Sell 1 at 101 Sell 1 at market Cancel order

Separating consensus on the orders from the state and result of those orders.

Order-book is deterministic based on the set of transactions and the ordering of those transactions

As a new on-chain protocol, with no dependence on smart-contracts or layer 1 like Ethereum. The state and code is contained within the node.

Node maintains a matching-engine and the state of the market in real-time. Nodes gossip they ordering in the background - this is not used for consensus but for preventing covert adversaries Node reach quorum with slices on mempool Nodes use results of auction, for reordering block

Node maintains multiple states by looping over all permutations. Most permutation will not change the state. When a permutation changes state the node will compare results and put a value on the results - and enter auction when needed.

Honest nodes will agree to default to actual real-time "true" orderings.

**Example Honest Front-running** Limit order cancelled immediately after getting filled by a market-order

**Example Dis-Honest Front-running** Limit order inserted with a higher price to standing limit-order to front-run the fills, due to new market move

In this example, the adversary will try to get a new order in at the end of the time-block. Note: doing this immediately becomes honest front-running

Difference between honest and dis-honest front-running, is when

**Example2 Dis-Honest Front-running** Limit order cancelled immediately after getting filled by a market-order, but gossiping the cancel before gossiping the market order.

### 5.3.2 Designer intended result

is a decentralized matching engine where no front-running occurs in real-time.

No advantage to real-time front-runnings Disadvantage by losing honest reputation, where nodes will not sure to add you to their quorum slice.

### 5.3.3 note

note how we don't have liveness or consistency or censorship resistance guarantees, as those are concepts for the design of protocols with different utilities. As we are seeking the utility of Fair Price Discovery from a decentralized on-chain blockchain matching engine exchange protocol.

## 6 Results

[1]

## References

- [1] Jing Chen and Silvio Micali. ALGORAND. <https://arxiv.org/pdf/1607.01341.pdf>, 2017.
- [2] Thierry Foucault, Ohad Kadan, and Eugene Kandel. Limit order book as a market for liquidity. Post-print, HAL, 2005.
- [3] Reto Francioni and Robert A. Schwartz. *Equity Markets in Transition The Value Chain, Price Discovery, Regulation, and Beyond*. Springer International Publishing, 2017.
- [4] Kenneth French and Richard Roll. Stock return variances: The arrival of information and the reaction of traders. *Journal of Financial Economics*, 17(1):5–26, 1986.
- [5] Mahimna Kelkar, Fan Zhang, Steven Goldfeder, and Ari Juels. Order-fairness for byzantine consensus. In *Advances in Cryptology – CRYPTO 2020*, pages 451–480. Springer International Publishing, 2020.
- [6] Andrew Lo, A. Craig MacKinlay, and June Zhang. Econometric models of limit-order executions. NBER Working Papers 6257, National Bureau of Economic Research, Inc, 1997.
- [7] Bingcheng Yan and Eric Zivot. The dynamics of price discovery. Working Papers UWEC-2005-01-R, University of Washington, Department of Economics, 2007.