Improved Stock Market Structure Using Cryptography [*]

Charanjit S. Jutla[1] and Barry Mishra[2]

[1]IBM T. J. Watson Research Center, Yorktown Heights, NY 10598, USA
[2]School of Business,Univ. of California, Riverside, CA, USA

Abstract

The stock markets have two primary functions, that of providing liquidity and price discovery. While the market micro-structure was mostly ignored or assumed to function ideally for the purpose of asset pricing, O'Hara (Journal of Finance, 2003) has established that both liquidity and price discovery affect asset pricing, and in particular asset returns. Easley and O'Hara (Journal of Finance 2004) have demonstrated that informed investors' private information is not reflected efficiently in price discovery. We argue that the periodic price discovery has both positive and negative consequences for asset returns. In particular, the inefficient reflection of investors' information during price discovery incentivizes them to conduct research. However, this requires that the auctioneer be ideal or fully trusted. In this work we propose using cryptography, and in particular multi-party secure computation, to setup a novel stock market structure that, to a large extent, removes the negative consequences of liquidity costs and periodic price discovery, as well as incentivizes investors to conduct research. Interestingly, the proposed market structure takes us back to the early days of stock markets, i.e. periodic call markets, but with the not so "trusted" auctioneer replaced by a decentralized set of parties where no individual party (or small coalition) gets to know the order book.

1 Introduction

The advent of bitcoin and other cryptocurrencies has highlighted the fact that cryptography can lead to disruptive technologies. In this work we propose that modern cryptography can also lead to enhanced stock markets that incentivizes investors to conduct independent research and thus lead to a better overall information structure surrounding a firm's stock. In a ground-breaking work, Easley and O'Hara [EO04] demonstrated a rational expectations equilibrium model that *incorporates private information* to show that the quantity and quality of information lowers market risk and hence affects asset prices. We will use the same model along with additional analysis of practical mechanisms such as clearing price double auctions (CPDA), to reinforce the importance of incentivizing independent research. Further, we propose the use of modern cryptography to replace

[*] This paper is a new version of the paper "Upending Stock Market Structure Using Secure Multi-Party Computation" [Jut15]. The main difference is a more finance oriented write-up and an analysis showing that despite public information about the volume of an auction, in addition to the clearing price information, the informed trader is still incentivized to conduct research.

open order books and/or real-world auctioneers with *ideal* auctioneers, so that the information garnered by costly independent research is not leaked to the market, and hence preserving the incentive to conduct such independent research. The ideal auctioneer is a distributed computing system, split between various entities (possibly including private banks/exchanges and regulators), so that no collusion of a subset of these entities can infer any useful information about the order book[1].

Cryptography: Secure Multi-Party Computation (MPC) Typically, the markets work by matching bids and asks submitted by various investors. Such clearing can be continuous or periodic, the latter usually performing a cumulative clearance. The matching and clearing are either performed by a single auctioneer (i.e. specialist in the case of NYSE) or by a distributed computation (for public order books as in the case of NASDAQ). Both matching and clearing can be viewed as computations, which can either be performed by hand or by a computer. The computation takes as input a set of bids and asks and computes a matching or a clearing price at which the trade takes place. The question arises as to how such a computation can be performed if the underlying bids and asks are *encrypted*. In other words, the auctioneer (or his computing system) does not see the bids and asks in the clear, and yet it has to produce a correct clearing price. *Secure multi-party computation* (MPC) [Yao86, GMW87, BGW88, CCD88] provides a solution to this problem if the auctioneer can be split into multiple independent auctioneers and they run a distributed computational protocol to compute the clearing price. As long as at least one of these multiple auctioneers remains honest and refuses to collude with the rest, the protocol preserves complete privacy of the submitted bids and asks. Thus, a traditional specialist (firm) can be replaced by, say, four or five firms, one of which could even be a regulatory agency, and they can run this MPC protocol to compute the clearing price. All investors can rest assured that their bids and asks (both size and price) remain hidden from the auctioneers, as long as one of the auctioneers remains honest. Over the years, MPC has become efficient enough that the volume encountered in a typical opening NYSE auction can easily be handled in real time. Similarly, the continuous trading can be replaced by repeated clearing price double auctions, say, repeated every five minutes.

Note that in our system, the clearing price and matching trades are revealed to the public, and thus both price and volume are revealed which is important for making markets. What remains hidden from the public as well as the auctioneers, even after the auction round is over, is the remaining bids and asks that were not matched. This then removes an often cited detriment to liquidity, i.e. timing mismatch, as investors can safely and securely leave large bids and asks in the bid-ask books (which can also be carried from one round to the next, or altered by the investor). Thus, our proposed solution not only helps incentivize independent research, but this in turn increases liquidity as investors have a less risky valuation of a stock *and* can securely leave large orders on the bid-ask books.

MPC has been used before in running clearing price auctions, notably in the sugar-beet auction in Denmark [BCD$^+$09]. However, this is the first work to give an economic and game-theoretic justification for such a transition to MPC. We hope that our work will lead to a more widespread use of MPC in commodity and stock markets.

Private Information in Rational Expectations Equilibrium Information about the economy is by nature decentralized. It is important to design mechanisms so that this information can be

[1] This should be contrasted with dark pools where a single firm runs the dark pool and has access to the order book via its software.

shared with others, who can then make better investment choices. Hayek [Hay45] argues that it is not just scientific knowledge, but private knowledge about arbitrage opportunities, as well as inefficiencies in commerce that are important to be shared, and to be *not* assumed a priori given to all as is commonly assumed in standard economic theory. From his arguments one can conclude that one function of the stock market is to garner this decentralized information into asset prices.

Taking a cue from Hayek's criticism of equilibrium theories of prices where all information is considered publicly known, Grossman and Stiglitz [GS80] further argue that the "efficient markets" hypothesis, i.e. that prices reflect all available information, implies that equilibrium does not exist or the market will vanish. In fact, using a Gaussian model of public and private information, they prove that if efficient markets hypothesis is true and prices reflect even the "informed" traders' private information, then the informed traders have no incentive to garner costly private information. Thus, assuming rationality, all traders will become "uninformed". But, this is also not an equilibrium, as clearly one trader can garner information, even at a fixed cost, and taking the "equilibrium" price as a given, increase his returns tremendously.

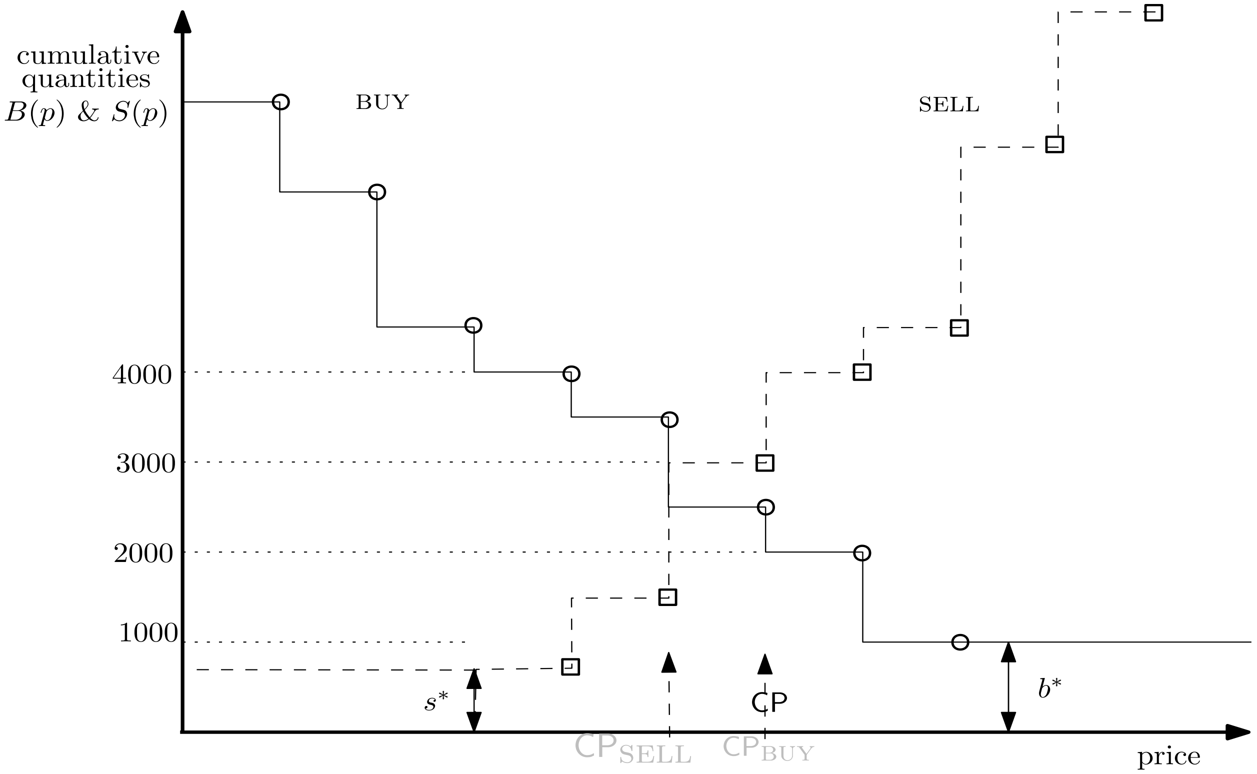
Building on [GS80], Easley and O'Hara [EO04] show that rational expectations equilibrium (or Walrasian equilibrium [LS06] in the capital assets pricing model (CAPM)) prices only partially reflect the informed traders knowledge about future prices, as long as the informed traders knowledge itself is Gaussian and they are risk-averse. This allows for the informed to continue to pay for costly research, as it allows them to be more competitive. Note, that in this rational expectations "pricing" model it is important that only prices, and distributions of various traders' information etc., be publicly known (and not the actual bid-ask price and size of the order).

Financial Reporting versus Independent Research Easley and O'Hara [EO04] actually demonstrated that asymmetry between public and private information about a firm *increases* the cost of capital of the firm, simply because the uninformed are disadvantaged and hence averse to investing in the firm at the same level as informed traders. However, the main motivation of [EO04] (and [O'H03]) was to address how the differing accounting and reporting standards *as well as* differing market micro-structure influence the information structure surrounding a firm's stock. So, while they correctly conclude that transparent financial reporting is beneficial for lowering the cost of capital, one cannot ignore the value of independent research brought to bear on a company's valuation[2]. Thus, both better reporting standards[3] as well as incentive to conduct independent research lead to a more informed market and, ultimately, better asset pricing. In this work we will show, using the same analysis as used by Easley and O'Hara, that information garnered by investors by independent research is not fully reflected in market prices and hence the incentive for independent research is enhanced by replacing the real world auctioneer by an ideal auctioneer implemented using MPC.

Clearing Price Double Auctions In this work, we show that a specific clearing price double auction mechanism that we describe (Fig. 1) incentivizes independent research even more than that inferred from rational expectations equilibrium. Further, when a large fraction of traders get informed, either by eventual public dissemination of information (e.g. after an earnings report) or by expending resources on research, then the clearing price converges to rational expectations

[2] As former SEC Chairman Arthur Levitt posited in a remark to the Economic Club of Washington (2000) that there exists a web of dysfunctional relationships including where analysts develop models to gauge a company's earnings but rely heavily on a company's guidance itself.

[3] For example, Reg FD related to full and fair disclosure of information to the public instead of selective disclosures.



equilibrium prices. Moreover, even though the informed are further incentivized, as long as their knowledge is Gaussian, the uniformed still get returns by trading on the public knowledge of the informed's knowledge imprecision.

The specific clearing price double auction is similar to the usual CPDAs, except for two specific differences: (a) the traders are allowed to submit market price buy or sell orders, and the clearing price is such that all market price orders (buy and sell) are cleared, (b) if the price at which supply and demand cross, the supply and demand are not equal, then the clearing price is chosen so that all supply below the clearing price is fully cleared and all demand above the clearing price is fully allotted. Note that (b) automatically implies full clearance of market orders. This still sets the price to be either the greatest price where demand is larger than supply, or the least price where supply is larger than demand (see Fig. 1).

The rest of the paper is organized as follows. In Section 2 we describe the specific CPDA auction we propose as stock market mechanism. The security model is discussed in Section 2.5 where we also show how blockchains can be used to audit malicious behavior of auctioneers participating in the MPC protocol. The rational expectations equilibrium analysis of Easley and O'Hara in presence of private information [EO04] is reviewed in Section 3. Finally, the effects of micro-structure of our CPDA are illustrated in Sections 3.1 and 3.1.1.

2 Stock Market Mechanism

We first describe the CPDA mechanism assuming an ideal functionality $\mathcal{F}$ or a single ideal auctioneer. In this description, the investors do not encrypt their inputs, as the ideal auctioneer is by definition trusted to not leak this information to anyone. Once the single ideal auctioneer is precisely described, especially as to what its inputs and outputs are and how the output is computed from the inputs, we can then move on to describe how the inputs are encrypted and how this ideal auctioneer can be replaced and implemented using MPC by a set of independent auctioneers.

An ideal functionality takes inputs from all the investors (or their brokers), computes the required function(s) and returns the specified outputs to the individual investors and public. No other information about the different investor's input is leaked to any of the investors or observers. Since our aim is to hide the investors' bid-ask size and price, especially those that were not matched or alloted, even in this ideal description we have to pay extra attention to whether partial fulfillment ratios can leak information about unallocated orders. For an example of the following CPDA mechanism, see Fig. 1.

- All brokers submit their clients' bids and asks as follows:

  Each broker is pre-assigned a broker ID, say BROKER-ID.

  Each client can make two kinds of bids and two kinds of asks. One of the two kinds in either case is *market price*.

  If it is not a market price bid or ask, the bid or ask is a list of pairs $\langle z_i, p_i \rangle$, where z_i is the quantity bid to buy at price p_i (or quantity z_i to sell with ask-ing price p_i). Each price shall be in (positive integer) cents.

  If it is market-price the list of pairs is a singleton with the pair $\langle z, * \rangle$.

  Thus, each client's order will be specified as (order-type = market/limit, buy/sell, list-of-pairs).

  A client can submit multiple orders.

  The broker assigns a random ID to each order (large enough to be unique), say ID, and submits (BROKER-ID, ID, order-type = market/limit, buy/sell, list-of-pairs).

- The ideal functionality $\mathcal{F}$ computes the following:

  1. $\mathcal{F}$ outputs the total number of buy and sell orders to the public.
  2. For each possible price p, $\mathcal{F}$ computes $b(p)$ as the sum of all z, where the sum is over all brokers and all of their orders marked BUY such that its corresponding list-of-pairs contains a pair $\langle z, p \rangle$.
  3. $\mathcal{F}$ also computes b^* as the sum of all z, where the sum is over all brokers and all of their orders marked BUY such that its corresponding list-of-pairs contains a pair $\langle z, * \rangle$.
  4. Similarly using the orders marked SELL, $\mathcal{F}$ computes $s(p)$ for each possible price p, as well as s^*.
  5. For each p, let $B(p) = b^* + \sum_{p' \geq p} b(p')$, and $S(p) = s^* + \sum_{p' \leq p} s(p')$.
  6. Next, $\mathcal{F}$ computes the least price p, denoted cp_{BUY}, such that $B(p) \leq S(p)$.
  7. $\mathcal{F}$ also computes the largest price p, denoted $\mathsf{cp}_{\text{SELL}}$, such that $B(p) \geq S(p)$.

8. If $S(\mathsf{cp}_{\text{SELL}}) > B(\mathsf{cp}_{\text{BUY}})$, then clearing price $\mathsf{cp} = \mathsf{cp}_{\text{SELL}}$, otherwise $\mathsf{cp} = \mathsf{cp}_{\text{BUY}}$. Also, $\mathcal{F}$ outputs cp to the public.
9. All buy orders which are either market price or if their bidding price is greater than or equal to cp_{BUY} are given full allotment at price cp. $\mathcal{F}$ outputs all such bids, along with their BROKER-ID and ID to the respective brokers..
10. Similarly, all sell orders which are either market price or if their ask-ing price is less than or equal to $\mathsf{cp}_{\text{SELL}}$ are given full allotment at price cp. $\mathcal{F}$ outputs all such asks along with their BROKER-ID and ID to the respective brokers.
11. – If $\mathsf{cp} = \mathsf{cp}_{\text{BUY}}$, $\mathcal{F}$ sorts all sell orders with limit price cp_{BUY} by decreasing order size (i.e. z_i in the asks). Then it outputs the sell orders starting with the largest, as long as the sum total remains less than $B(\mathsf{cp}_{\text{BUY}}) - S(\mathsf{cp}_{\text{SELL}})$. The last sell order maybe partially filled, so that the sum total is exactly $B(\mathsf{cp}_{\text{BUY}}) - S(\mathsf{cp}_{\text{SELL}})$.
    - Else, $\mathcal{F}$ sorts all buy orders with limit price $\mathsf{cp}_{\text{SELL}}$ by decreasing order size (i.e. z_i in the bids). Then it outputs the buy orders starting with the largest, as long as the sum total remains less than $S(\mathsf{cp}_{\text{SELL}}) - B(\mathsf{cp}_{\text{BUY}})$. The last buy order maybe partially filled, so that the sum total is exactly $S(\mathsf{cp}_{\text{SELL}}) - B(\mathsf{cp}_{\text{BUY}})$.
12. $\mathcal{F}$ outputs the total volume of trades to the public.

Remark. The reason why the partial fulfillment in step 11 is prioritized by size of the order and not performed on a random basis is because if the partial fulfillment was based on randomization then a curious investor can learn the size of the gap $B(\mathsf{cp}_{\text{BUY}}) - S(\mathsf{cp}_{\text{SELL}})$ by submitting many different small orders and noting the fraction of those orders that get alloted. Then, comparing it with the total volume which is public information, he/she can infer $B(\mathsf{cp}_{\text{BUY}}) - S(\mathsf{cp}_{\text{SELL}})$. Hence, it is important to give precedence to larger orders at clearing price.

Readers not familiar with secure multi-party computation are referred to [BCD$^+$09] or [CHK$^+$12]. These works describe different, but now standard, ways of implementing the ideal functionality using a distributed set of parties. In particular, the former is built on [BGW88, CCD88] and the latter uses Rabin's Oblivious Transfer (OT) [JH85] and is built on [GMW87, NP05, IKNP03, LLXX05]. Both these protocols are in the semi-honest security model (see section 2.5 below), which means that the parties are assumed to not deviate from the protocol, but are allowed to collect any information they can from the execution of the protocol. In other words, assuming each party is participating in the secure multi-party computation protocol using a computer connected to the other computers via a network, then each party can observe and collect information from the memory of their computer during and after the execution of the protocol. Since the protocols are proved secure, this means that the parties do not manage to gather any additional information about the inputs of others by this semi-honest behavior, over and above what the ideal functionality will give them as output (e.g. the public outputs of $\mathcal{F}$). This should be contrasted with dark pools, where the firm running the dark pool can read the complete order book since it controls the software and the hardware and the order book is not encrypted or hidden from this firm.

Note that in the mechanism above, we assume that brokers run the protocol through $\mathcal{F}$. However, in the real world there can be a large number of brokers (from different countries, as well). Thus, to be practical, we will assume that some small subset of these brokers, say four, and a regulating authority such as the securities and exchange commission (SEC) actually run the protocol emulating and replacing $\mathcal{F}$. In standard cryptography parlance this would then be called a secure 5-PC (five-party computation). Recall, different known 5-PC protocols give different security guarantees against collusion. We recommend using a 5-pc protocol that requires all five parties to collude before they can get any useful information, especially if a watchdog agency is one of the five participating auctioneers.

The brokers would still need to encrypt their bids and asks (for all of their clients). For some versions of MPC, the brokers may instead be just required to implement splitting their inputs using known simple secret sharing techniques and then sending the shares (using a cryptographically secure channel, e.g. SSL) to the five parties implementing MPC (the secret sharing can be a basic additive splitting or of a threshold kind [Sha79]). At the end of the protocol, the five parties will all know the public output (as prescribed by $\mathcal{F}$), and they can publish it on a public bulletin-board, such as a permissioned blockchain. The actual process of doing the trade, i.e. which CUSIP numbered shares go to which broker can be done by some clearing agency (it may charge a small fees for its services).

2.1 How many CPDA sessions a day?

The number of CPDA auction sessions per day for each stock will depend on the time it takes to do the 5-PC. The opening session of each day usually commands the most attention, and it may have the most volume of inputs, and hence is likely to be more computation and communication intensive. However, most of the computation and communication in the MPC protocols can be done even before the investors' actual bid and ask orders arrive, as it mainly involves generating lots of correlated random numbers among the five auctioneers. The actual on-line computation (i.e. involving the orders) is expected to take less than a minute on modern processors (see e.g. recent results on performing an initial public offering using MPC [HBC$^+$19]). The other sessions may complete in even lesser time. One must also provide a gap of, say, about five minutes between rounds for all investors to digest the results of the previous auction round.

2.2 Low Volume Market Price

Usually during the main trading sessions, the fraction of trades at market price to those with limit is low enough that the above methodology is sound. However, a caveat can be introduced that if $\min\{s^*, b^*\}$ is more than $\min\{S(\mathsf{cp}), B(\mathsf{cp})\}$, the clearing price is reset to the clearing price of the previous session; in other words, in such a case the market price is just the clearing price of the previous session. If $B(\mathsf{cp}) < S(\mathsf{cp})$, then all market sell orders and sell order with limit price less than or equal to cp are executed, and only an appropriate subset of the buy orders are executed. Similarly, the same logic holds for the opposite case, i.e. $B(\mathsf{cp}) > S(\mathsf{cp})$.

Another possibility is to let the market price orders be in the clear, i.e. not encrypted, so that competitive forces can provide a better price if the non market-price volume is low.

2.3 Improved Liquidity

Since the limit bids and asks are now completely secret (other than what is disclosed from the output of $\mathcal{F}$), the main concern of the traders in submitting large bid and ask goes away. For example, a typical example often cited in the current stock market structure is that not all investors maybe present at the same time, even though they are willing to take opposite sides of the trade.

An investor A may want to sell 1000,000 shares of Apple stock today at current prices, whereas another investor B may want to buy 1000,000 shares at current prices, but only tomorrow due to some independent reasons (assuming no new drastic information is generated). In the current system, if a large sell order by A is put into the market, the prices immediately drop (this behavior of the market holds even in the NYSE specialist system [MC00]). In essence, investor A ends up paying the cost of liquidity to other intermediaries who serve as liquidity providers. However, in our system, if investor A is patient for a day or two, or sometimes even a few CPDA sessions, partial information leaked by outputs of $\mathcal{F}$ in different CPDA sessions, will still hide the remaining open orders of A. We model and analyze this behavior of our mechanism more rigorously in Section 3.1.1.

It has often been cited [BHR13] that high frequency trading (HFT) has improved liquidity in the DA markets. However, it has also come under severe criticism [Lew14] that the HFT traders may completely remove liquidity when the market is under stress. Moreover, the improved liquidity possibly comes at a higher liquidity cost, as all the bids and asks are open in the DA markets (note that once the bids and asks are in the open, the analysis of [EO04] which shows that informed traders have an incentive does not hold any more). Our mechanism, which is closer in spirit to the specialist system (without the concern of specialist leaking the order book), is expected to remedy these HFT front-running and high liquidity-cost concerns.

2.4 Improved Incentives for Information Gathering

We also show in Section 3.1.2 that our mechanism incentivizes the informed trader even more than as predicted by the Walrasian equilibrium analysis of [EO04]. Moreover, the uninformed traders continue to get returns as the indepedent research is not perfect. Further, eventually all information becomes more or less public, e.g. after an earnings report, and the playing field is leveled for rational traders. Thus, the uninformed (but rational) traders continue to be in the market and be the usual source of liquidity.

2.5 Security Model: Semi-Honest vs Malicious Adversary

While secure multi-party computation can also be achieved under malicious adversarial behavior, e.g. by using verifiable secret sharing [CGMA85, JMN10], in the stock market setting this may not be required if all the participants are required to save all their computations, i.e. inner workings of the protocol and involved random numbers, in a permissioned blockchain in an encrypted form and and release the encryption keys to the public after a month or so. The SEC (or the public, for that matter) can audit the saved computations and check if all computations were performed according to protocol. Note, in our economic modeling we do not require that the bidding strategies of the traders are secret. In fact, these strategies, and even all distributions are assumed to be public knowledge. Thus, if the transcripts are released after a reasonable amount of time, this causes no harm to the incentive of conducting independent research in our system.

3 Modeling Research Advantage in Rational Expectations Equilibrium

Since double auctions are notoriously difficult to analyze, we will make some simplifying assumptions. We will assume, as in [EO04], that the seller(s) have a supply of stocks to sell, which follows a normal distribution.

Each buyer has a choice of investments which can either be cash, or one of the n risky stocks. Let's say at the beginning of a day when the buyer needs to make an investment choice, it is public knowledge that the value of the k-th stock in the future (or next day), denoted by random variable v_k, will follow a normal distribution with mean $\bar{v}_k$ and precision ρ_k. This, of course, is a base case distribution. Some traders may have proprietary research that could change their future valuation of each stock. For simplicity, we will assume that such *informed traders* obtain the same signal s_k, and the probability distribution of s_k is itself a normal distribution with mean v_k and precision γ_k conditioned on the future valuation of the stock being v_k. Thus, s_k more or less predicts v_k with precision γ_k (in other words, γ_k can be seen as measuring the historical accuracy of their research about the k-th stock). In fact as observed in [EO04], conditioned on the signal s_k, the distribution of v_k can be calculated by Bayes rule to be a normal distribution with mean $\bar{v}_k\rho_k + s_k\gamma_k$ and precision $\rho_k + \gamma_k$.

We will also assume that each buyer (investor) T_j has an exponential utility function with risk-aversion coefficient δ_j. In other words, the buyer's utility function u_j is the following function of wealth w_j: $u_j(w_j) = (1 - e^{-\delta_j w_j})/\delta_j$. It is safe to assume that big institutions are more risk-neutral, meaning their δ is close to zero, whereas individual investors will tend to have a large δ.

For any buyer T_j with risk-aversion coefficient δ_j, and initial wealth w_j, suppose T_j buys $x_{j,k}$ quantity of the k-th stock at price p_k. Then, the cash d_j it has left is $w_j - \sum x_{j,k}p_k$. Thus, their future wealth Ψ_j is $d_j + \sum x_{j,k}v_k$, which is same as

$$w_j + \sum_k (v_k - p_k) \cdot x_{j,k}$$

Now, suppose that the buyers know the price they have to pay for the k-th stock, e.g. price in rational expectations equilibrium. Then, their future utility can be maximized w.r.t. each of the quantities $x_{j,k}$. For the buyers who receive a signal for the k-th stock, we can also condition on the signal being s_k. In either case, i.e. whether they receive a signal or not, the distribution of v_k remains normal with a mean and precision known to the buyer. As mentioned earlier, if they do receive a signal s_k, then the conditional distribution of v_k is still normal with mean $\bar{v}_k\rho_k + s_k\gamma_k$ and precision $\rho_k + \gamma_k$.

It can be shown (see e.g. [EO04]) that if the utility function of T_j is of the above exponential form with risk-aversion coefficient δ_j, then it suffices to maximize $\mathrm{E}[\Psi_j] - (\delta_j/2) \cdot \mathrm{Var}[\Psi_j]$. It is not difficult to see that maximum is achieved at

$$x_{j,k} = \frac{\bar{v}_{j,k} - p_k}{\delta_j (\rho_{j,k})^{-1}} \tag{1}$$

where $\bar{v}_{j,k}$ and $\rho_{j,k}$ are the (conditional) expectation and variance resp. of v_k (conditioned on the signal s_k for the buyers who receive signal s_k).

With this analysis, [EO04] conclude that if *all* traders receive the signal, and assuming all of them have the same δ, and further if there is a per capita supply y_k of the k-th stock, then since in rational expectations equilibrium supply equals demand, we get that

$$p_k = \frac{\bar{v}_k \cdot \rho_k + s_k \cdot \gamma_k - \delta \cdot y_k}{\rho_k + \gamma_k}.$$

However, the situation gets more interesting if only a faction μ_k of traders get the signal for the k-th stock. In the rational expectations equilibrium model, the uninformed buyers (i.e. those who do not receive the signal) can conjecture the signal from the price p_k as long as the distribution of the signal is public knowledge. In particular, [EO04] show that in case $\mu_k > 0$ then conditioned on the price p_k, the uninformed buyers can compute a random variable θ which is distributed normally with mean v_k (not to be confused with $\bar{v}_k$) and precision ρ_θ given by

$$\left[\gamma_k^{-1} + \left(\frac{\delta}{\mu_k \gamma_k}\right)^2\right]^{-1} \tag{2}$$

Note that if δ is zero, as is the case for risk-neutral buyers, then this is the same distribution as that of the signal, and hence the price completely reveals whatever advantage the informed buyers get from the signal. On the other hand, if δ is non-zero, then the price is only partially revealing to the uninformed in equilibrium, and there remains an advantage to the informed. However, in the next section we show that the sealed bid clearing price auction as described above allows for the informed to retain an advantage even when they are risk-neutral.

3.1 Effects of Micro-Structure of Price Discovery on Asset Returns

While the analysis above was done assuming rational expectations equilibrium without regard to the mechanism which may be required to achieve such an equilibrium, we now focus on practical mechanisms and analyze the effects on returns for both informed and uninformed traders.

The main goal is to show that sealed-bid and sealed-ask clearing price double auctions of the particular form as described above have the property that (a) the average return of an informed investor is higher than in the basic rational expectations equilibrium analysis, and (b) if all investors are equally informed then the clearing price rapidly converges to the rational expectations equilibrium price.

Actually, the property (b) has been well-studied in the individual private belief model, and it is shown in [SW89] that if the number of traders is large then they converge to bidding truthfully, i.e. in accordance with their private valuation. Also see [KN04], where it is shown that discrete bidding strategies (as opposed to continuous bidding functions) make the clearing price auction efficient.

So focusing on (a), we first remark that rewarding an investor who has put costly effort into researching a stock is not just important from an equilibrium perspective, but one can reasonably argue that such an equilibrium tends to incentivize research and hence more efficient utilization of capital. Further, the uninformed also continue to have positive returns, since the signal that the informed receive is not absolutely precise. Thus, the uninformed remain in the game, and hence provide liquidity. Finally, when the information becomes public, e.g. after an earnings report, the playing field is leveled and the uninformed get even higher returns.

3.1.1 Price Discovery under Common Public Information

We first focus on the case where no buyer (or seller) receives a signal (and it is common knowledge), and the distribution of the future price v is public knowledge to be a normal distribution with mean $\bar{v}$ and precision ρ. All buyers and sellers are assumed to have the same risk-aversion coefficient δ. For simplicity of exposition, we will assume that there are exactly n buyers and exactly n sellers. Moreover, each investor has only risk-free cash as an alternative. The buyers will be assumed to own no stock, and the sellers will be assumed to own on average per-capita stock of z (random variable) shares (say, z_j for the j-th seller). Also, for simplicity, we will assume that the CPDA has infinite precision, i.e. bids, asks and the clearing price can be arbitrary real numbers.

We claim that the following strategies for the buyers and sellers converges to a (bayesian) Nash equilibrium, as n tends to infinity.

- For each price $p < \bar{v}$, each buyer puts in an order to buy ρ/δ shares of stock at limit price p.
- At each price $p > \bar{v} - z_j \cdot \delta/\rho$, j-th seller puts in an order to sell ρ/δ shares of stock at limit price p. Also, for prices $p < \bar{v} - z_j \cdot \delta/\rho$, the j-th seller becomes a buyer and puts in an order to buy ρ/δ shares at limit price p.

Theorem 1 *Let there be n buyers and n sellers. Then, as n tends to infinity, the above strategies constitute a bayesian Nash equilibrium for the CPDA mechanism described in Section 2. The strategies are also truthful.*

Proof: If there are n buyers and n sellers with these strategies[4], the net demand for the stock at price p is

$$B(p) - S(p) = n \cdot (\bar{v} - p) \cdot \rho/\delta \ - \ (n \cdot z - n \cdot (\bar{v} - p) \cdot \rho/\delta)\,.$$

Thus, the clearing price p^* is $p^* = \bar{v} - \rho^{-1}\delta \cdot z/2$. At this price, the j-th buyer gets exactly $z/2$ shares. Note that since the buyer's utility function is CARA, and all random variables follow normal distribution, the buyer's utility is an increasing monotonic function of the standard mean-variance expression, i.e. $\mathrm{E}[\Psi_j] - (\delta/2) \cdot \mathrm{Var}[\Psi_j]$, where, as in Section 3, Ψ_j is j-th buyer's future wealth. Then, ignoring the cash position of the j-th buyer, the above mean-variance expression is easily calculated to be $z^2\rho^{-1}\delta/8$.

We now show that this is "almost" a bayesian Nash equilibrium, in the sense that if n tends to infinity, then it converges to a Nash equilibrium. For finite n, an investor can improve upon his "equilibrium" strategy by only a factor of $1/(1 + 1/2n)$. This is commensurate with [SW89] where they only considered CPDA with each agent bidding or offering exactly one item.

Suppose, all agents but one fix their strategy to be as described above. We will only consider the case where the exceptional agent is a buyer (the other case is symmetric and analyzed similarly). The exceptional agent choses an alternate strategy of demanding a cumulative $D(p)$ stock at price p. For comparison, the "equilibrium" strategy above sets $D(p) = (\bar{v} - p) \cdot \rho/\delta$, for $p < \bar{v}$, and zero everywhere else. The total demand for the stock at price p is now

$$\begin{aligned} B(p) - S(p) &= n \cdot (\bar{v} - p) \cdot \rho/\delta \ - (\bar{v} - p) \cdot \rho/\delta + D(p) \ - \ (n \cdot z - n \cdot (\bar{v} - p) \cdot \rho/\delta) \\ &= (2n - 1) \cdot (\bar{v} - p) \cdot \rho/\delta \ + D(p) \ - \ n \cdot z \\ &= (2n - 1) \cdot \rho/\delta \cdot \big(\bar{v} \ - \ n/(2n - 1) \cdot z \cdot \rho^{-1}\delta \ - (p - D(p)\rho^{-1}\delta/(2n - 1))\big) \end{aligned}$$

Thus, the clearing price p^{**} satisfies

$$p^{**} - D(p^{**}) \cdot \rho^{-1}\delta/(2n - 1) \ = \ \bar{v} \ - \ n/(2n - 1) \cdot z \cdot \rho^{-1}\delta \tag{3}$$

Note that as n tends to infinity, this is same as the clearing price p^* computed earlier where all agents used the prescribed strategy. We need to compare if the exceptional buyer's (say, j-th buyer) utility can be improved upon with the alternative strategy $D(p)$. At the above price p^{**}, the j-th

[4] We will also assume that the number of buyers is large enough that budget constraints of individual buyers does not come into play.

buyer gets full allotment $D(p^{**})$, and hence the above mean-variance expression difference from "equilibrium" expression is (after some simple manipulation and using (3))

$$(z \cdot 2n/(2n-1) - D(p^{**}) \cdot (2n+1)/(2n-1)) \cdot \rho^{-1}\delta/2 \cdot D(p^{**}) \; - \; z^2 \cdot \rho^{-1}\delta/8$$

Taking the derivative of this w.r.t. $D(p^{**})$ shows that the maximum is achieved at $D(p^{**}) = z/2 \cdot 2n/(2n+1)$. Thus, with n tending to infinity, this approaches the equilibrium quantity, and hence we obtain a Nash equilibrium in the limit. For finite n, it can be shown that the exceptional buyer can follow the strategy $D(p)$ of bidding $(2n-1)/2n \cdot \rho/\delta$ shares at each limit price p with $p < (2n-1)/2n \cdot \bar{v}$ to get $D(p^{**}) = z/2 \cdot 2n/(2n+1)$. This only differs from the limiting Nash equilibrium strategy by a factor of $1/(1+1/2n)$.

□

3.1.2 Price Discovery under Mixed Private and Public Information

The situation gets interesting when only a fraction of investors receive a pointed signal about the future stock price(s). Recall that in such a scenario, in the rational expectations equilibrium setting above (section 3), the price is only partially revealing to the uninformed buyers. We will now illustrate that in the CPDA considered in this work, that the informed are even more incentivized to gather information than suggested by the rational expectations equilibrium and are incentivized even if they are risk neutral). Moreover, the uninformed also continue to get a positive return on their investment.

Again, for simplicity of exposition we will assume that all the n buyers are uninformed and own no stock, n_1 of the sellers are uninformed, and $n_2 = n - n_1$ sellers are informed and get a signal s from a normal distribution with mean v (the actual future price) and precision γ. The sellers, on average, own per capita stock of z. We will now show that as n tends to infinity, the following strategies form a bayesian Nash equilibrium.

- The j-th uninformed seller, who own z_j stock, behaves as in previous sub-section, i.e. at each price $p > \bar{v} - z_j \cdot \delta/\rho$, j-th seller puts in an order to sell ρ/δ shares of stock at limit price p. Also, for prices $p < \bar{v} - z_j \cdot \delta/\rho$, the j-th uninformed seller becomes a buyer and puts in an order to buy ρ/δ shares at limit price p.

- The informed, who receive a signal s, can be shown to believe that the future price follows a conditional distribution that is a normal distribution with mean $\bar{v}_{|s} = (\rho \cdot \bar{v} + \gamma \cdot s)/(\rho + \gamma)$ and precision $\rho + \gamma$ [EO04]. Thus, the informed seller, who owns z_j of stock, does the following: for each price $p > \bar{v}_{|s} - z_j \cdot \delta/(\rho+\gamma)$, the informed seller puts in an order to sell $(\rho+\gamma)/\delta$ shares of stock at limit price p. Also, for $p < \bar{v}_{|s} - z_j \cdot \delta/(\rho+\gamma)$, this agent becomes a buyer, and puts in an order to buy $(\rho+\gamma)/\delta$ shares of stock at limit price p.

- The n uninformed buyers, who own no stock, do the following: for each price $p < \bar{v}$, each uninformed buyer puts in an order to buy ρ/δ shares of stock at limit price p.

Theorem 2 *As n tends to infinity, and n_2 remaining finite, the above strategies constitute a bayesian NASH equilbrium for the CPDA mechanism described in Section 2. The strategies are also truthful.*

Proof: Consider the case that $s > \bar{v}$ (the other case is similarly handled). In that case, the net demand for the stock $B(p) - S(p)$ at price p, for $\bar{v} \leq p < \bar{v}_{|s}$, is given by

$$-\ (n \cdot z - n_1 \cdot (\bar{v} - p) \cdot \rho/\delta - (n - n_1) \cdot ((\rho \cdot \bar{v} + \gamma \cdot s)/(\rho + \gamma) - p) \cdot (\rho + \gamma)/\delta)\,,$$

and is given by

$$n \cdot (\bar{v} - p) \cdot \rho/\delta\ -\ (n \cdot z - n_1 \cdot (\bar{v} - p) \cdot \rho/\delta - (n - n_1) \cdot ((\rho \cdot \bar{v} + \gamma \cdot s)/(\rho + \gamma) - p) \cdot (\rho + \gamma)/\delta)\,,$$

for $p < \bar{v}$. Thus, if all agents follow the prescribed strategies, the clearing price is

$$p^* = \frac{(n - n_1) \cdot \gamma \cdot s + n \cdot \rho \cdot \bar{v} - n \cdot \delta \cdot z}{n \cdot \rho + (n - n_1) \cdot \gamma}, \tag{4}$$

if $s > \bar{v} + n/(n - n_1) \cdot z\delta/\gamma$, else

$$p^* = \frac{(n - n_1) \cdot \gamma \cdot s + 2n \cdot \rho \cdot \bar{v} - n \cdot \delta \cdot z}{2n \cdot \rho + (n - n_1) \cdot \gamma}. \tag{5}$$

In the latter case, $p^* < \bar{v}$ (and $s < \bar{v} + n/(n - n_1) \cdot z\delta/\gamma$), and even the uninformed buyers get an allotment. For simplicity, we will now focus on the this second case. Now, given the information, the informed and the uninformed have a different future distribution of the stocks price. While for the uninformed, the future price distribution remains normal with mean $\bar{v}$ and precision ρ, using Bayes principle, it can be seen that having received the signal s, the informed's conditional distribution of the future price of the stock is normal with mean

$$\bar{v}_{|s} = \frac{\rho\bar{v} + \gamma \cdot s}{\rho + \gamma}$$

and precision $\rho+\gamma$. Thus, the mean-variance expression of the uninformed's utility, having obtained their allocation or sale at price p^* above (4), and taking into account their previous ownwership of stock, is given by

$$\frac{(\bar{v} - p^*)^2}{2\delta\rho^{-1}}.$$

The informed's ownership w after the CPDA will be

$$(\bar{v}_{|s} - p^*) \cdot (\rho + \gamma)/\delta. \tag{6}$$

So, the informed's mean-variance expression is given by

$$\begin{aligned}
&\mathrm{E}[(v - p^*) \cdot w \mid s] - \delta/2 \cdot \mathrm{Var}[(v - p^*) \cdot w \mid s] \\
&= (\bar{v}_{|s} - p^*) \cdot w - \delta/2 \cdot (\rho + \gamma) \cdot w^2 \\
&= (\bar{v}_{|s} - p^*) \cdot (\bar{v}_{|s} - p^*) \cdot (\rho + \gamma)/\delta - \delta/2 \cdot (\rho + \gamma)^{-1} \cdot (\bar{v}_{|s} - p^*)^2 \cdot (\rho + \gamma)^2/\delta^2 \\
&= 1/2 \cdot (\bar{v}_{|s} - p^*)^2 \cdot (\rho + \gamma)/\delta \\
&= 1/2 \cdot w^2 \cdot (\rho + \gamma)^{-1}\delta
\end{aligned} \tag{7}$$

As in Section 3.1.1, now we consider the case where all the strategies are fixed, except for one informed seller/buyer, who instead uses a different ownership (post-CPDA) function $D(p)$. In other words, if he/she already owns z_j of stock, then his/her demand is $D(p) - z_j$. In that case $B(p) - S(p)$, for $\bar{v} \leq p$ is given by

$$\begin{aligned} B(p) - S(p) &= n \cdot (\bar{v} - p) \cdot \rho/\delta + D(p) \\ &\quad - \ (n \cdot z - n_1 \cdot (\bar{v} - p) \cdot \rho/\delta - (n - n_1 - 1) \cdot ((\rho \cdot \bar{v} + \gamma \cdot s)/(\rho + \gamma) - p) \cdot (\rho + \gamma)/\delta) \\ &= (n - n_1 - 1) \cdot (\rho \cdot \bar{v} + \gamma \cdot s)/\delta \ - \ (n \cdot z - (n + n_1) \cdot \bar{v} \cdot \rho/\delta) \\ &\quad - p \cdot \rho/\delta \cdot (2n - 1) - p \cdot \gamma/\delta \cdot (n - n_1 - 1) + D(p), \end{aligned}$$

and hence the clearing price p^{**} satisfies

$$p^{**} \cdot (2n-1) + p^{**} \cdot (n-n_1-1) \cdot \rho^{-1}\gamma - D(p^{**}) \cdot \rho^{-1}\delta = (2n-1) \cdot \bar{v} + (n-n_1-1) \cdot \rho^{-1}\gamma \cdot s \ - \ n \cdot z \cdot \rho^{-1}\delta \quad (8)$$

Now, the mean-variance expression of this exceptional informed investor is given by

$$\left(\bar{v}_{|s} - p^{**}\right) \cdot D(p^{**}) - \delta/2 \cdot (\rho + \gamma)^{-1} \cdot D(p^{**})^2.$$

Using (8) and taking the derivative of the above w.r.t. $D(p^{**})$, we find that the maximum is obtained at $D(p^{**})$ satisfying

$$\begin{aligned} &\bar{v}_{|s} - \frac{(2n - 1) \cdot \rho \cdot \bar{v} + (n - n_1 - 1) \cdot \gamma \cdot s - n \cdot \delta \cdot z}{(2n - 1) \cdot \rho + (n - n_1 - 1) \cdot \gamma} \\ &\quad = D(p^{**}) \cdot \left(\frac{2\delta}{(2n - 1) \cdot \rho + (n - n_1 - 1) \cdot \gamma} + \frac{\delta}{\rho + \gamma} \right) \end{aligned}$$

With n tending to infinity, even if $n_2 = (n - n_1)$ remains finite (i.e. the number of informed investors remains finite or tiny), the above gives

$$D(p^{**}) = \left(\bar{v}_{|s} - \frac{2n \cdot \rho \cdot \bar{v} + (n - n_1) \cdot \gamma \cdot s - n \cdot \delta \cdot z}{2n \cdot \rho + (n - n_1) \cdot \gamma} \right) \cdot (\rho + \gamma)/\delta,$$

which is same as informed's stock ownership at equilibrium given by (6) noting that equilibrium clearing price p^* is given by (4). Then, by (7), the informed's mean-variance expression is also the same as in equilibrium. Thus in the limit, when n tends to infinite, and even if the number n_2 of informed investors remains finite or tiny, the above set of strategies constitute a bayesian Nash equilibrium.

□

Note that when $s < \bar{v} + n/(n - n_1) \cdot z\delta/\gamma$, we have $p^* < \bar{v}$, and the uninformed buyers also get an allocation, and their future utility is positive. Thus, even though the informed get a pointed signal from their research, as long as it is not grossly lopsided, the uninformed get a price which is below the mean future price, and hence their future utility is positive.

The mean-variance expression of the future utility of the informed, as calculated above in the proof, is

$$\begin{aligned}
&1/2 \cdot w^2 \cdot (\rho+\gamma)^{-1}\delta \\
&= 1/2 \cdot \left((\bar{v}_{|s} - p^*) \cdot (\rho+\gamma)/\delta\right)^2 \cdot (\rho+\gamma)^{-1}\delta \\
&= 1/2 \cdot \left(\left(\bar{v}_{|s} - \frac{(n-n_1)\cdot\gamma\cdot s + 2n\cdot\rho\cdot\bar{v} - n\cdot z\cdot\delta}{2n\cdot\rho + (n-n_1)\cdot\gamma}\right) \cdot (\rho+\gamma)/\delta\right)^2 \cdot (\rho+\gamma)^{-1}\delta \\
&= 1/2 \cdot \left(\left(\frac{\rho\cdot\bar{v} + \gamma\cdot s}{\rho+\gamma} - \frac{(n-n_1)\cdot\gamma\cdot s + 2n\cdot\rho\cdot\bar{v} - n\cdot z\cdot\delta}{2n\cdot\rho + (n-n_1)\cdot\gamma}\right) \cdot (\rho+\gamma)/\delta\right)^2 \cdot (\rho+\gamma)^{-1}\delta \\
&= 1/2 \cdot \left(\rho\cdot\bar{v} + \gamma\cdot s - \frac{(n-n_1)\cdot\gamma\cdot s + 2n\cdot\rho\cdot\bar{v} - n\cdot z\cdot\delta}{2n\cdot\rho + (n-n_1)\cdot\gamma} \cdot (\rho+\gamma)\right)^2 \cdot (\rho+\gamma)^{-1}\delta^{-1}
\end{aligned}$$

The clearing price above is

$$p^* = \frac{(n-n_1)\cdot\gamma\cdot s + 2n\cdot\rho\cdot\bar{v} - n\cdot\delta\cdot z}{2n\cdot\rho + (n-n_1)\cdot\gamma}.$$

In contrast, [EO04] show that the rational expectations equilibrium price q^* is

$$q^* = \frac{((n-n_1)\cdot\gamma + (n+n_1)\cdot\rho_\theta)\cdot s + 2n\cdot\rho\cdot\bar{v} - n\cdot\delta\cdot z}{2n\cdot\rho + (n+n_1)\cdot\rho_\theta + (n-n_1)\cdot\gamma},$$

where ρ_θ is as given in 2, i.e. $\left[\gamma^{-1} + \left(\frac{2n\cdot\delta}{(n-n_1)\cdot\gamma}\right)^2\right]^{-1}$. Since we are considering the case where $s > \bar{v}$, i.e. the when the signal is higher than the future a priori mean value, we now show that p^* is less than q^*, and hence the informed get a better allocation and hence a better mean-variance expression than in the equilibrium setting. This is not surprising, as in equilibrium, the uninformed also get partial information about the signal as demonstrated in[EO04] (see Section 3). We just show that when δ is zero, i.e. the investors are risk neutral, then $p^* < q^*$ (recall, in the rational expectations equilibrium, if δ is zero, the informed get no advantage for their research). We have, with $\delta = 0$ and hence $\rho_\theta = \gamma$,

$$\begin{aligned}
p^* - q^* &= \frac{(n-n_1)\cdot\gamma\cdot s + 2n\cdot\rho\cdot\bar{v}}{2n\cdot\rho + (n-n_1)\cdot\gamma} - \frac{((n-n_1)\cdot\gamma + (n+n_1)\cdot\gamma)\cdot s + 2n\cdot\rho\cdot\bar{v}}{2n\cdot\rho + (n+n_1)\cdot\gamma + (n-n_1)\cdot\gamma} \\
&= \frac{(n-n_1)\cdot\gamma\cdot s + 2n\cdot\rho\cdot\bar{v}}{2n\cdot\rho + (n-n_1)\cdot\gamma} - \frac{(2n\cdot\gamma)\cdot s + 2n\cdot\rho\cdot\bar{v}}{2n\cdot\rho + 2n\cdot\gamma} \\
&= \frac{(n-n_1)\cdot\gamma\cdot s + 2n\cdot\rho\cdot\bar{v}}{2n\cdot\rho + (n-n_1)\cdot\gamma} - \frac{\gamma\cdot s + \rho\cdot\bar{v}}{\rho+\gamma} \\
&= \frac{((n-n_1)\cdot\gamma\cdot s + 2n\cdot\rho\cdot\bar{v})\cdot(\rho+\gamma) - (\gamma\cdot s + \rho\cdot\bar{v})\cdot(2n\cdot\rho + (n-n_1)\cdot\gamma)}{(2n\cdot\rho + (n-n_1)\cdot\gamma)\cdot(\rho+\gamma)} \\
&= \frac{(n+n_1)\cdot\gamma\rho\cdot(\bar{v} - s)}{(2n\cdot\rho + (n-n_1)\cdot\gamma)\cdot(\rho+\gamma)} \\
&< 0
\end{aligned}$$

3.1.3 Does the Volume of the CPDA reveal information?

While in the rational expectations equilibrium model, Easley and O'Hara [EO04] show that the equilibrium price reveals only partial information about the signal that the informed receive, their model does not disclose the volume of trade that happens at equilbrium. However, market mechanisms such as the one described in Section 2 do reveal both the clearing price and the volume of trade in each CPDA. The question naturally arises as to whether the additional volume information reveal more information to the uninformed as can be garnered from just the price. First of all, in the periodic CPDA version of the stock market, each individual round reveals additional information to the uninformed, since at the end of each round the uniformed have access to the clearing price, and also the volume of trade in that round. If one runs enough rounds of CPDA, it is expected to reach an equilibrium similar to the one modeled in [EO04] by Walras' intuitive tatonnement.

In this section, we take a finer look at the model in the previous sub-section 3.1.2, by considering the distribution of the stock held by investors in determining the volume of trade in an individual round of CPDA. Previously, we had assumed that on average the sellers hold per-capita stock of z shares (a random variable). We can model this better by assuming that the informed sellers individually own stock the size of which is sampled from a normal distribution with mean z_2 and variance η_2, and similarly the uninformed own stock which is sampled from a normal distribution with mean z_1 and variance η_1. The actual number of informed and uninformed that show up for a CPDA may not be known, whereas we have been treating n and n_1 as publicly known values. It is better modeled by assuming that z_1 and z_2 are random variables (possibly samped from a known normal distribution).

The volume of the CPDA is decided by individual ownership z_j, in the sense that if for the j-th informed seller, $p < \bar{v}_{|s} - z_j \cdot \delta/(\rho+\gamma)$, then the j-th informed seller becomes a buyer. Now, we look at the clearing price, and determine which of the informed sellers effectively became buyers as their ownership z_j was too small, i.e. $p^* < \bar{v}_{|s} - z_j \cdot \delta/(\rho+\gamma)$, or $z_j < (\bar{v}_{|s} - p^*) \cdot (\rho+\gamma)/\delta$. Similarly, the uninformed sellers become buyers if $z_j < (\bar{v} - p^*) \cdot \rho/\delta$. Now, the average ownership $\bar{w}$ conditioned on the ownership being less than $\bar{z}+\alpha$, when sampling from a normal distribution with mean $\bar{w}$ and precision η is $\bar{z} - \frac{1}{\sqrt{2\pi\eta}} \cdot e^{-\eta^2\alpha^2/2}$. Thus, given that there are n_1 uninformed sellers, and $(n-n_1)$ informed sellers, the average ownership $\bar{w}_b$ of sellers-turned-buyers is (assuming both $(\bar{v}_{|s} - p^*) \cdot (\rho+\gamma)/\delta$ and $(\bar{v} - p^*) \cdot \rho/\delta$ is more than z_1 and z_2– other cases are handled similarly)

$$\frac{n_1}{n} z_1 + \frac{n-n_1}{n} z_2 - \frac{n_1}{n \cdot \sqrt{2\pi}\eta_1} \cdot e^{-\eta_1^2((\bar{v}-p^*)\cdot\rho/\delta - z_1)^2/2} - \frac{n-n_1}{n \cdot \sqrt{2\pi}\eta_2} \cdot e^{-\eta_2^2((\bar{v}_{|s}-p^*)\cdot(\rho+\gamma)/\delta - z_2)^2/2}$$

Similarly, the average ownershup $\bar{w}$ conditioned on the ownership being more than $\bar{z}+\alpha$ is $\bar{z} + \frac{1}{\sqrt{2\pi\eta}} \cdot e^{-\eta^2\alpha^2/2}$, and hence the average ownership $\bar{w}_s$ of sellers-staying-sellers is

$$\frac{n_1}{n} z_1 + \frac{n-n_1}{n} z_2 + \frac{n_1}{n \cdot \sqrt{2\pi}\eta_1} \cdot e^{-\eta_1^2((\bar{v}-p^*)\cdot\rho/\delta - z_1)^2/2} - \frac{n-n_1}{n \cdot \sqrt{2\pi}\eta_2} \cdot e^{-\eta_2^2((\bar{v}_{|s}-p^*)\cdot(\rho+\gamma)/\delta - z_2)^2/2}$$

Thus, the (clearing) volume $B(p^*)$ $(= S(p^*))$ is

$$n \cdot (\bar{v} - p^*) \cdot \rho/\delta + n_1 \cdot z_1 + (n-n_1) \cdot z_2 - \frac{n_1}{\sqrt{2\pi}\eta_1} \cdot e^{-\eta_1^2((\bar{v}-p^*)\cdot\rho/\delta - z_1)^2/2} - \frac{n-n_1}{\sqrt{2\pi}\eta_2} \cdot e^{-\eta_2^2((\bar{v}_{|s}-p^*)\cdot(\rho+\gamma)/\delta - z_2)^2/2}.$$

Thus, while p^* is a linear combination of the secret signal s and the random variable $z = \frac{n_1}{n} z_1 + \frac{n-n_1}{n} z_2$, the volume is a more complex function of s, z_1, z_2. Thus, if the CPDA result reveals s and the volume, the information about s revealed is only partial (as we have three unknowns and two known expressions).

4 Implications and Conclusion

In this work we have considered the possibility of replacing full trust in a single auctioneer in a stock market by a collection of auctioneers employing a cryptographic protocol. The cryptographic protocol, known as secure multi-party computation, is well studied in the field of cryptography, and guarantees the privacy of the investors' bids and asks as long as not all of the auctioneers collude. Thus, even if a single auctioneer refuses to join in a collusion, the other colluding auctioneers learn nothing other than the legitimate output of the auction. The output of the auction is the clearing price and the volume. We have argued, using economic and game-theoretic modeling, that not only does this enhanced trust in the privacy of the auction incentivize independent research in the underlying stock, it also improves liquidity in the market as investors can leave large limit orders on the order books without the concern of their private information leaking out. The enhanced trust may also help reverse the trend towards NASDAQ style open order books, as that trend is possibly a result of skepticism in the benevolence of specialist auctioneers. To quote T. Cason and D. Friedman [CF97], "the benevolent auctioneer is at best an endangered species" (for empirical studies on negative specialist behavior, see [MC00, Ben06]). The need for sealed bid-ask mechanisms is further amplified by our result, enhancing an earlier result of [SW89], that shows the sealed bid-ask clearing price double auction to rapidly converge (as the number of investors participating in the CPDA become large) to truthful behavior of investors in the usual CAPM (capital assets pricing) model extended by the Easley-O'Hara model of private information [EO04].

From a real world impact perspective, one can even have an independent regulator as one of the auctioneers, and thus practically removing any chance of full collusion among the auctioneers. The secret randomness used in the protocol can be saved in a block chain to be revealed later for public audit, thus enhancing trust in the system. The proposed mechanism and cryptographic protocol will not only incentivize independent research in the stock, thus enabling a better information structure around the stock, but also circumvent front running and obviate the need for dark pools.

References

[BCD$^+$09] Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas P. Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, Michael I. Schwartzbach, and Tomas Toft. Secure multiparty computation goes live. In *Financial Cryptography and Data Security, 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers*, pages 325–343, 2009. 1, 2

[Ben06] Sigridur Benediktsdottir. An empirical analysis of specialist trading behavior at the new york stock exchange. *FRB International Finance Discussion Paper*, (876), 2006. 4

[BGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *20th ACM STOC*, pages 1–10. ACM Press, May 1988. 1, 2

[BHR13] Jonathan Brogaard, Terrence Hendershott, and Ryan Riordan. High frequency trading and price discovery. Working Paper Series 1602, European Central Bank, 2013. 2.3

[CCD88] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In *20th ACM STOC*, pages 11–19. ACM Press, May 1988. 1, 2

[CF97] Timothy N Cason and Daniel Friedman. Price formation in single call markets. *Econometrica: Journal of the Econometric Society*, pages 311–345, 1997. 4

[CGMA85] Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults (extended abstract). In *26th FOCS*, pages 383–395. IEEE Computer Society Press, October 1985. 2.5

[CHK$^+$12] Seung Geol Choi, Kyung-Wook Hwang, Jonathan Katz, Tal Malkin, and Dan Rubenstein. Secure multi-party computation of Boolean circuits with applications to privacy in on-line marketplaces. In Orr Dunkelman, editor, *CT-RSA 2012*, volume 7178 of *LNCS*, pages 416–432. Springer, Heidelberg, February / March 2012. 2

[EO04] David Easley and Maureen O'Hara. Information and the cost of capital. *The Journal of Finance*, 59(4):1553–1583, 2004. 1, 2.3, 2.4, 3, 3, 3.1.2, 3.1.2, 3.1.3, 4

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th ACM STOC*, pages 218–229. ACM Press, May 1987. 1, 2

[GS80] Sanford J Grossman and Joseph E Stiglitz. On the impossibility of informationally efficient markets. *The American Economic Review*, pages 393–408, 1980. 1

[Hay45] F. A. Hayek. The use of knowledge in society. *American Economic Review*, 35(4), 1945. 1

[HBC$^+$19] Tzipora Halevi, Fabrice Benhamouda, Angelo De Caro, Shai Halevi, Charanjit S. Jutla, Yacov Manevich, and Qi Zhang. Initial public offering (IPO) on permissioned blockchain using secure multiparty computation. In *IEEE International Conference on Blockchain, Blockchain 2019, Atlanta, GA, USA, July 14-17, 2019*, pages 91–98. IEEE, 2019. 2.1

[IKNP03] Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. Extending oblivious transfers efficiently. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 145–161. Springer, Heidelberg, August 2003. 2

[JH85] M.O. Rabin J. Halpern. A logic to reason about likehood. In *Proc. 15th ACM STOC*, pages 363–365, 1985. 2

[JMN10] Thomas P. Jakobsen, Marc X. Makkes, and Janus Dam Nielsen. Efficient implementation of the Orlandi protocol. In Jianying Zhou and Moti Yung, editors, *ACNS 10*, volume 6123 of *LNCS*, pages 255–272. Springer, Heidelberg, June 2010. 2.5

[Jut15] Charanjit S. Jutla. Upending stock market structure using secure multi-party computation. *IACR Cryptol. ePrint Arch.*, page 550, 2015. ∗

[KN04] Ilan Kremer and Kjell G Nyborg. Underpricing and market power in uniform price auctions. *Review of Financial Studies*, 17(3):849–877, 2004. 3.1

[Lew14] M. Lewis. *Flash Boys: A Wall Street Revolt.* Penguin, UK, 2014. 2.3

[LLXX05] Bao Li, Hongda Li, Guangwu Xu, and Haixia Xu. Efficient reduction of 1 out of n oblivious transfers in random oracle model. Cryptology ePrint Archive, Report 2005/279, 2005. `http://eprint.iacr.org/2005/279`. 2

[LS06] Jonathan Levin and Ilya Segal. General equilibrium, 2006. `http://web.stanford.edu/~jdlevin/teaching.html`. 1

[MC00] A. Madhavan and M. Cheng. Price discovery in auction markets: A look inside the black box. *The Review of Financial Studies*, 13(3):627–658, 2000. 2.3, 4

[NP05] Moni Naor and Benny Pinkas. Computationally secure oblivious transfer. *Journal of Cryptology*, 18(1):1–35, January 2005. 2

[O'H03] Maureen O'Hara. Presidential address: Liquidity and price discovery. *The Journal of Finance*, 58(4), 2003. 1

[Sha79] A. Shamir. How to share a secret. *Comm. ACM*, 22(11):612–613, 1979. 2

[SW89] Mark A. Satterthwaite and Steven R. Williams. The rate of convergence to efficiency in the buyer's bid double auction as the market becomes large. *The Review of Economic Studies*, 56(4):pp. 477–498, Oct., 1989. 3.1, 3.1.1, 4

[Yao86] Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In *27th FOCS*, pages 162–167. IEEE Computer Society Press, October 1986. 1