Achieving Trust without Disclosure: Dark Pools and a Role for Secrecy-Preserving Verification

Achieving Trust without Disclosure: Dark Pools and a Role for Secrecy-Preserving Verification

(Invited Paper)

David C. Parkes
SEAS, Harvard University
33 Oxford Street
Cambridge, MA
parkes@eecs.harvard.edu

Christopher Thorpe
Harvard Innovation Lab
125 Western Ave.
Allston, MA 02163
cat@eecs.harvard.edu

Wei Li
Citigroup
Citibank Tower, 3 Garden Road, Central, Hong Kong
wei.x.li@ualberta.net

ABSTRACT

Can an exchange be "dark," so that orders are not displayed, while simultaneously trustworthy, so that the execution of trades and flow of information occur as promised? SEC actions against dark pools suggest cause for concern, and regulators seem to be moving towards requiring more disclosure. Yet there is a clear tension: trading order information is widely exploited. Therefore, institutional investors have a strong interest in keeping pre-trade information about large trades hidden. Secrecy-preserving proofs of correctness can be used to build trust without revealing unnecessary information. By performing operations on obfuscated representations of orders (perhaps encrypted or otherwise hidden), a *zero knowledge proof* can be provided, allowing anyone to verify correctness of trades. Crucially, this can be done without revealing any information beyond this correctness. This technology can be usefully applied to construct provably trustworthy dark pools. Additional practical protocols relax the definition of "zero knowledge" to reveal limited information, providing necessary transparency for efficient market operation while limiting information that can be exploited by observers. Coupled with Trusted Computing hardware, these protocols can provide an excellent balance of practicality with secrecy.

Categories and Subject Descriptors

D.2.4 [**Software engineering**]: Software/Program Verification—*Correctness proofs, validation*; K.4.1 [**Computers and Society**]: Privacy, Regulation; J.4 [**Social and Behavioral Sciences**]: Economics

General Terms

Algorithms, Economics, Legal Aspects, Verification

Keywords

Dark pool, Zero-Knowledge Proofs, Trust, Market design

1. INTRODUCTION

Recent years have brought a rising concern in regard to the trustworthiness of public stock exchanges, grabbing the public's attention through *Flash boys* [17]. As described there, limit orders are "front-run" by high frequency trading (HFT) algorithms, with a buy order that is placed by an institutional investor such as Fidelity on one exchange detected and HFTs "running ahead" or "front-running," and buying shares on other exchanges in anticipation of driving up the price and quickly selling back to this investor.

As stated in a 2015 memo written by the SEC Division of Trading and Markets [30]:

> *Institutional investors typically need to trade in large size. If the market can infer their trading intentions from their trading activities before the full size of their trading interest is executed, the likely result will be an unfavorable price move against the institutional investor ("price impact"). To minimize this price impact, institutional investors often seek to execute their orders by splitting them into many, smaller-sized "child" orders that are fed into the market over time.*

Indeed, national securities exchanges such as Nasdaq and BATS introduced special types of orders to provide HFTs with information on orders without any requirement to trade in return for this information.[1] A 2015 action of the U.S. Securities and Exchange Commission (SEC) [31] against the Direct Edge exchange (now part of BATS) states that trading clients had influence on the design of orders, and received special information about the way certain kinds of order types would work. According to Lewis [17], the location of BATS just outside the Lincoln tunnel from Manhattan also provides special value to HFTs, allowing them to gain information about new orders just ahead of other exchanges.

In short, HFTs have developed algorithms that detect large trades by monitoring market orders, and when they detect a likely large trade, they make exploiting trades ahead of the large trade.

[1]These are the flash and post-only order types associated with the so-called flash order controversy [38].

One response to concerns about the fairness of public securities exchanges and the trading behaviors of HFTs has been a further fragmentation of stock markets and the proliferation of *dark pools*. A dark pool is an *alternative trading system* (ATS), and regulated under a different set of rules than public exchanges (see the Appendix). The name dark pool refers to a trading system that generally does not display orders. Whether trading occurs on a public exchange or a dark pool, regulation requires that all trades are priced at or better than the best quoted bid and ask prices displayed on the national securities exchanges, referred to as the *National Best Bid and Offer* (NBBO). Dark pools typically price trades to be at the midpoint of the NBBO. For example, if the NBBO price spread is 20-20.02 (bid-ask) then the trade is executed at 20.01.[2] In this sense, dark pools provide volume discovery rather than price discovery, with the price being set in public exchanges.

Beyond hiding pre-trade order information, some dark pools try to limit who participates in the pool to passive, institutional investors who trade on stock price movements and not information, and who wouldn't be expected to trade based on order flow.[3] As much as a third of the volume executed in Nasdaq and NYSE stocks is now traded in dark pools and other off-exchange trading.[4]

As evidenced by actions brought by the SEC and others in recent years, this emergence of private exchanges is bringing with it new concerns about trust. See Table 1, and refer to the Appendix for some specific details. Some general concerns include:

- Orders not matched with "natural liquidity" on the other side of the dark pool as claimed (Pipeline)
- Order information shared improperly with other traders (Liquidnet, LavaFlow)
- Price set incorrectly (SIGMA X)
- HFTs able to gain useful information through trading or exploit order types (Barclays LX, UBS)

A group of fund managers (i.e., passive, institutional investors) plan to launch a new dark pool named Luminex later in 2015 [9], proposing to restrict participation, insist on a commitment to a minimum block size for trades and price at the midpoint of NBBO. We return to the design of the Luminex dark pool in Section 3.

Concerns about HFTs, and an interest in enabling better execution of large block trades for institutional investors, have also promoted renewed interest in batch auctions (that match orders synchronously, at a defined time). The London Stock Exchange and the NYSE plan to introduce a mid-day batch auction [14, 39]. Existing dark pools such as POSIT Match and Instinet execute orders in batch, for example once per day or at multiple intervals during the trading day [29]. In light of HFTs, Budish et al. [4, 5] analyze *frequent batch auctions* for use in place of a continuous limit order books in a public exchange. In such a design, all orders received during the same interval are treated as having arrived at the same time. A uniform price double auction is used to clear the market, at which point all orders are displayed.[5]

To summarize:

1. There are concerns about the predatory practices of HFTs in public securities exchanges, and especially with behavior such as front-running, that causes orders placed in one exchange to have a short-term price impact in other exchanges.
2. Dark pools were originally envisioned as a way to allow institutional investors to handle large block trades, trading amongst themselves at the broader market price and without interacting with fast, algorithmic trading algorithms looking to make short-term profits.
3. The opaqueness of dark pools leads to new concerns about trust, in regard to whether they will correctly match and price orders, whether or not active investors can still participate and gain an unfair advantage, and whether or not useful information might still flow to HFTs either as a side-effect of placing orders or through other information flows.

The need for institutional investors to have provably correct execution (and thus "best" execution, with best defined as is appropriate to the rules of the exchange as well as governing SEC regulation) has become stronger than ever. This is especially true for dark pools, since these have been short on transparency. This is becoming a challenge for market operators, such as banks and dealer-brokers, who are running these trading systems. In recent years, this requirement is extending from exchange traded products such as stocks to other products such as foreign exchanges, and thus there is likely to be an increasing interest in the techniques described in this paper.

1.1 Illustrative Challenges

Consider the following concrete examples of challenges faced by the operator of a dark pool in convincing participants about the trustworthiness of a market:

(I) in the context of the IEX dark pool (a continuous limit order book), prove that published "priority rules" in regard to time, price and quantity are being followed when matching bids and asks.

(II) in the context of a dark pool such as Barclays LX, which uses an algorithm to assign a level of "aggressiveness" to a trader in the pool, prove that the levels are correctly assigned, and that rules by which a participant can restrict the counter-party with which it trades are correctly applied.

(III) in the context of a frequent batch auction by BCS Inc., prove that orders are being correctly sealed until the end of a discrete time interval, that the set of orders is not modified at that time, and that the uniform price rule is correctly applied.

(IV) in the context of a dark pool such as that proposed by Luminex, prove that statements of interest and orders cannot be shared with other parties.

[2] Prominent dark pools such as Liquidnet, Barclays DirectEx, BIDS and IEX report more than seventy percent of their trades are done at the NBBO midpoint [40].

[3] Rather than restrict participants, another market design response is to delay all data flowing from a dark pool just enough to prevent HFTs from front-running orders. The IEX trading system interposes a 350 millisecond delay on all data through the use of a 38-mile coil of optical fiber. This allows its own computers to look for better prices on other exchanges before the HFTs respond.

[4] The volume executed in Nasdaq stocks increased from 29.4% to 2005 and 38.6% in 2014; the change in volume of NYSE stocks was from 13.0% in 2005 to 34.6% in 2014 [30]. This includes ATS volume as well as internalization, which occurs when banks and brokers match orders from clients against their own customers' trading flow.

[5] A theoretical model shows that a frequent batch auction reduces the value that HFTs can gain from speed, and suggests that this would lower the costs for passive investors [5]. Wah et al. [45, 44] adopt a computational approach to study the effect of adopting batch auctions. Their analysis suggests that batch auctions would attract sufficient volume in competition with continuous limit order books, with HFTs following passive traders to participate in batch auctions.

Dark pool / ATS	Date of action	Complaint	Penalty	Size of pool
Pipeline	October, 2011	Majority of trades executed by subsidiary of Pipeline	\$1 million	Closed
Liquidnet	June, 2014	Pre-trade indications of interest shared with trading desk	\$2 million	14th largest
Goldman SIGMA X	June, 2014	Price outside of NBBO	\$800,000	6th largest
Barclays LX	June, 2014	Inconsistent profiling of "aggressiveness" of traders, and application of this profile; catering to HFTs	Contested	9th largest
Citigroup LavaFlow	July, 2014	Share information on hidden orders with affiliated business unit	\$5 million	Closed
UBS dark pool	January, 2015	Sub-penny pricing via order types offered to HFTs, selective access to a system to protect against HFT counter-party	\$14.4 million	Largest

Table 1: Actions of regulatory authorities against dark pools and alternative trading systems. The rank of a dark pool by trading volume is for May 2015, and based on average daily volume statistics [40].

Now imagine providing these proofs of correctness in a way that does not reveal any information about orders past or present. This is the task to which secrecy-preserving proofs of correctness can be applied.

1.2 Outline

Rather than provide a technical treatment, the goal is to provide a brief survey of prior research into the use of secrecy-preserving proofs of correctness for building trustworthy markets. The discussion will emphasize practical aspects, and note some of the remaining difficulties. These are not around providing secrecy-preserving proofs of correctness, but around preventing an unscrupulous market operator from choosing to disclose additional information.

In Section 3, we connect the discussion back to the design of dark pools and trading systems, revisiting the proposed Luminex dark pool design and sketching out two complementary designs. We also circle back to the four challenges above, and suggest some additional benefits of cryptographic methods in regard to required disclosures to regulators.

The Appendix provides some details on the actions of the SEC and others against dark pools and ATSs in recent years, along with a brief summary of regulation of financial markets as it relates to the design of exchanges and trading systems.

2. SECRECY-PRESERVING PROOFS

Broadly speaking, there are two kinds of trust that we might like to establish through cryptographic methods:

Secrecy-preserving correctness: a market operator can prove to anyone that the market outputs (i.e., trades) are correct given the rules of the market and the inputs (i.e., orders), and do so without revealing any information about the inputs other than that implied by the outputs or as otherwise required (e.g. regulation, exchange rules, or market design).

Strong Secrecy: the market operator is unable to release any additional information about the inputs (i.e., orders) other than that implied by the outputs (i.e., trades) and other information disclosure required by regulators.

The first property is useful even without the second property, because it allows a market operator to establish correctness without revealing information about orders. The second property provides additional confidence that the operator of a market, who is known to be correctly executing trades based on orders, is not at the same time sharing information that could lead to price impact in other exchanges or provide an advantage to investors placing orders in this market.

Section 2.1 provides a brief overview of some required background in regard to cryptographic methods. Sections 2.2 and 2.3 focus on methods to establish secrecy-preserving correctness. Section 2.4 refers to methods to establish secrecy.

2.1 Preliminaries

Some of the constituent components for providing secrecy- preserving proofs of correctness are:

- An *electronic bulletin board* to which any trader or the market operator can post data. Posted data is time stamped and data cannot be erased.
- A *public key infrastructure* (PKI), providing a sound method of establishing and sharing public keys that can be used, amongst other things to generate the encryption $E(x)$ of a value x. This is the "ciphertext", while x is the "plaintext" x. Encryption requires that the value x can only be recovered from $E(x)$ by someone who has the corresponding private key.
- A *commitment* method, that is required to be information hiding and binding. If a commitment $COM(x)$ is made to value x, then this does not reveal any information about x, and it is binding, such that when a private key corresponding to the commitment is released the commitment releases value x and no other value.[6]
- A *time-lapse cryptography service* that provides a constant stream of public keys and commits to reconstruct and publish the associated secret decryption keys at pre-defined intervals [27, 28].
- A *homomorphic encryption scheme*, allowing computation to be performed on encrypted values such that the result is the encryption of an associated computation on the values themselves; e.g., computing $E(x_1)\cdot E(x_2)$ might correspond to $E(x_1+x_2)$. This allows anyone with access to $E(x_1)$ and $E(x_2)$ to verify output $y = x_1 + x_2$ by computing $E(y)$, and checking $E(x_1) \cdot E(x_2) = E(y)$. This does not reveal anything about x_1 and x_2 beyond "$x_1 + x_2 = y$."

The existence of a PKI is used for many of these components, including homomorphic encryption schemes [22] and time-lapse cryptography. A PKI also allows *digital signatures*; i.e., the ability to sign an input with a participant's private key so that anyone can validate the source of the input.

[6]Encryption schemes also satisfy hiding, and are typically binding. The crucial difference between commitment and encryption is that encryption requires that decryption can be achieved with some private key that applies independent of what is encrypted, while a commitment can be opened with a message-dependent key. This makes the design of commitment schemes easier than that of public-key encryption; see Dodis [8] for more information.

2.2 The Evaluator-Prover Model

The evaluator-prover (EP) model [23, 26] provides a useful framework for practical, secrecy-preserving proofs. Multiple players secretly submit input values $x_1, \ldots, x_n$ to the EP. The EP computes a function $y = f(x_1, \ldots, x_n)$, outputs the value y, and engages in a proof of the correctness of the result. The proof of correctness can be verified by anyone, and is sound (so that it is not possible to prove a false claim, except with very low probability.) An EP is *secrecy-preserving* if the proof does not reveal anything about the input except for the information implied by the output value.

Note that the EP model allows the EP to learn the input values. Because of this, the EP model provides secrecy-preserving correctness but without strong secrecy. The EP must operate the rules of the market correctly, given the inputs (i.e., determine the correct trades given the orders.)[7] But the EP could still choose to disclose information about orders, including pre-trade information.

To fix ideas, let's think about the EP model in the context of a batch auction that will clear at some time T. The trades determined at time T must correspond to the correct trades given the rules, and given the orders placed by time T. In addition, time-lapse cryptography can be used to prevent the EP knowing anything about the orders before time T. However, the EP is not prevented from sharing information about the orders after time period T.

Applications.

A number of applications of the EP model have been suggested, to a variety of auction designs and security market designs. See Table 2. These include multi-unit auctions, combinatorial auctions, clock auctions, batch auctions and a market with a continuous limit order books.

A typical operation of a trustworthy, sealed-bid auction runs as follows [23]:

1. Each bidder encrypts his or her bid with the auctioneer's public key and posts it to the bulletin board, as a commitment via time-lapse cryptography.

2. The time-lapse cryptography service opens the commitments to reveal the encrypted bids, and everyone can verify that the encrypted bids correspond to the commitments.

3. The auctioneer (privately) decrypts the bids using its private key, determines and posts the outcome of the auction (the winner, the payment) along with a proof of the correctness of the outcome to the bulletin board.

4. Anyone can verify the proof that the outcome is correct given the encrypted bids on the bulletin board.

Let's now turn to two applications that have been developed for securities markets.

Combinatorial batch auction [42]. Each trader submits an order that states an interest to trade a basket of trades. The submitted baskets are "crossed," with pricing at the midpoint of the NBBO. Any orders that aren't completely filled are combined to form a remainder basket. Anyone can verify that this remainder is determined correctly given the submitted orders. The right to trade this remainder basket in the broader market is auctioned off, with bidders in this auction able to request risk characteristics, for example the "skew" (difference between long and short trades), along with market sector and market cap information. The cost of trading the remainder basket would be shared amongst participants in the batch auction according to orders placed in the pool. By using on auction on the remainder, this design ensures that the information available to the EP after the auction is complete is of minimal value.[8]

Continuous limit order book [41]. This design maintains an encrypted order book and proves that all updates made to the book are correct given encrypted orders that arrive into the market. On this basis, a proof of correctness can be provided whenever a trade occurs. The designer can also choose which statistics to publish about the state of the order book, ranging from no statistics to information such as market depth, bid-ask spread, etc. The correctness of all such statistics can be proved to participants without revealing any more about the order book. The authors also point to the use of special purpose hardware, or methods to distribute inputs amongst a group of parties, as a way to achieve strong secrecy. This is a topic that we return to in Section 2.4.

2.3 Cryptographic approaches

Many papers have been written on zero-knowledge proofs since the seminal contributions of Goldwasser et al. [12] and Goldreich et al. [11]. The focus is on approaches that are designed to be practical in real-world settings, and especially on techniques that fit well with the EP model.

Table 3 provides a summary of progress in regard to the time required to verify the outcome of a sealed-bid, single item auction in the EP model. We also mention two approaches to attaining strong secrecy as well as correctness. Rather than verification, the output of these approaches is correct by design. Specifically— the computation is distributed to multiple parties, and as long as enough parties can be trusted not to collude then the output will be correct and no additional information can be learned by anyone about the inputs.

A decisive advantage of the EP model in financial markets is speed: the computation itself can be done on plaintext, and is thus unencumbered by the need to be necessarily correct (as in the case of the distributed approaches) or to prove correctness.[9] A proof of correctness can be generated after-the-fact, and even on demand. By way of contrast, the approaches of secure function evaluation and multi-party computation are likely to introduce too much latency because a complex, multi-round message passing protocol is required to perform computation on obfuscated inputs. For this reason, we restrict the following discussion to approaches that have been proposed in achieving secrecy-preserving proofs in the EP model.

Paillier encryption.

One approach uses the Paillier homomorphic encryption scheme [22].Given encryptions $E(x_1)$ and $E(x_2)$ of two values, x_1 and x_2, and a public constant a, anyone can compute the encryptions $E(x_1 + x_2)$, $E(x_1 + a)$ and $E(x_1 \cdot a)$ without learning

[7] A little more precisely, the market operator *could* deviate from the rules, but the market operator would with high likelihood be caught. Thus, as long as the penalties for incorrect operations are high enough, it is reasonable to believe that the market operator will follow the rules correctly.

[8] Similarly, when applied to a procurement auction or for the sale of wireless spectrum licenses, the first order concern is to complete the auction in a way that is correct and trustworthy. Any loss in secrecy after the auction closes cannot affect the outcome of the auction, and is reasonably considered a secondary concern.

[9] This point is also made by Thorpe and Willis, who point out that realtime decision making can be separated from asynchronous correctnes proofs [43].

Auction design	Application	Reference
Multi-unit auctions with second-price payments	Procurement	PRST [23]
Clock-proxy auction, including package bids, core payments, price feedback	Wireless spectrum	PRT [24]
Combinatorial batch auction, including auction to sell remainder basket	Securities	TP [42]
Continuous limit order book, configurable to reveal different statistics about order book	Securities	TP [41]
Multiple second-price auctions	Internet advertising	RMMY [25]

Table 2: Applications of the Evaluator-Prover model to secrecy-preserving proofs.

Crypto-scheme	Properties	Notes / Verification time	Reference
Secure two-party computation	Correctness, Strong secrecy	2 parties, garbled circuits†	NPS [19]
Secret sharing, secure multi-party computation	Correctness, Strong secrecy	˜4 trusted parties‡	HTK [13], BDJ+ [1]
Paillier encryption [22]	Correctness (EP model)	˜1 minute per bid	PRST [23]
Random representation (RR)	Correctness (EP model)	˜500 milliseconds per bid	RST [26]
RR, with hardware commitment device	Correctness (EP model)	˜0.02 milliseconds per bid	RMMY [25]

Table 3: Time to verify a proof (generally scales linearly in number of bids). Some of this timing information is 5+ years old and runtimes may be significantly shorter now as a result of advances in computing hardware. † Garbled circuit may be impractical [18]. ‡ Multi-party schemes may be impractical [19].

anything about x_1 or x_2.[10]

To convey the approach, and some details (about "help values" to provide semantic security[11]): suppose that $E(x_1)$ and $E(x_2)$ are posted to the bulletin board, and that the computation of interest is $x_1 + x_2$. The EP decrypts the inputs, and computes and posts output $y = x_1 + x_2$ to the bulletin board. Given this, anyone can use $d = E(x_1 + x_2) = E(x_1) \cdot E(x_2)$ to compute the encrypted value of the sum, and then confirm that $d = E(y)$.

The majority of the computational cost associated with Paillier encryption comes from modular exponentiations; see Thorpe and Parkes [42] for estimates of the time required to prove correctness for a combinatorial batch auction on 3,000 securities as well as some remarks about how to further speed up the approach.

Random representation.

Developed by Rabin et al. [26, 25], and extending methods of Kilian [15] and Brassard et al. [3], the approach of *random representation* provides an approach that in comparison to homomorphic encryption is both faster and simpler to understand (which can help in gaining acceptance).[12] The approach provides a proof of correctness that is sound with high probability; i.e., a false claim will only be accepted with a negligible probability. All computation is performed on values in a field F_p for prime p, for example $p = 2^{128}$, and all arithmetic is done mod p. As is standard in the EP model, the computation is done by the evaluator on plaintext using any algorithmic approach.

The approach to providing a secrecy-preserving proof of correctness is to represent a value $x \in \{0, 1, \ldots, p-1\}$ as a pair of numbers $X_1 = (u_1, v_1)$, such that $u_1 \in F_p$ is randomly chosen and $(u_1 + v_1) \bmod p = x_1$. Let $val(X_1) = (u_1 + v_1) \bmod p$. All inputs are encoded this way (in what are sometimes referred to as "blobs"). Given this, properties can be proved about relationships between inputs and outputs for each coordinate separately, and secrecy is preserved by never revealing both coordinates.

For a concrete example, let $X_1 = (u_1, v_1)$ and $X_2 = (u_2, v_2)$ represent two input values (with plaintext values x_1 and x_2). Assume that a commitment to all four values is posted to the bulletin board, and that the computation of interest is $x_1 + x_2$. The EP opens the commitments, and computes and posts the output $y = val(X_1) + val(X_2)$ to the bulletin board. The output is correct if, and only if, there exists a value w such that:

$$u_1 + u_2 = y + w, \qquad \text{and} \tag{1}$$

$$v_1 + v_2 = -w. \tag{2}$$

The EP also posts value w to the bulletin board, and will now engage in an interactive proof to convince a verifier that y is correct. The verifier issues a random challenge $c \leftarrow \{1, 2\}$. Let's assume $c = 1$. The EP now reveals u_1 and u_2. If these values are consistent with the commitments, and (1) holds, then the verifier accepts the proof. Analogously, if the challenge is $c = 2$, then the EP reveals v_1 and v_2 and the verifier accepts the proof if these are consistent with the commitments and property (2) holds.

We make the following observations:

(i) the proof reveals nothing about $val(X_1)$ and $val(X_2)$ beyond what would be implied by correctness; and

(ii) if the claim is correct, then the verifier will always accept the proof, and if the claim is false, then the verifier will accept the proof with probability at most 1/2.

For (i), suppose without loss of generality that $c = 1$. Values u_1, u_2 and w are revealed. But nothing is revealed about v_1, and for any v_1 there exists some v_2 such that $v_1 + v_2 = -w$. Therefore, knowledge of u_1 reveals nothing about $val(X_1)$. A similar argument for v_2 shows that nothing is revealed about $val(X_2)$.

For (ii), the interesting case is when the claim is not true. But then at least one of (1) and (2) must be false, and so a random challenge will discover the problem with probability at least 1/2.

In order to "amplify" this soundness, and ensure that a false claim will be caught with high probability, the EP can perform k, independent proofs. Simple analysis shows that the probability that

[10]For proofs of multiplication, and for inequality comparisons and interval membership proofs, the EP can use an interactive proof (i.e., a proof that involves the verifier issuing a random challenge to the EP). See Parkes et al. [23] for details.

[11]Given two plaintexts and their encryptions, semantic security requires that one cannot tell which ciphertext corresponds to which plaintext without being able to decrypt them.

[12]For example, the hiding property of the Paillier encryption scheme is based on a computational assumption named the "decisional composite residuosity assumption" [23]. In comparison, the properties of the random representation scheme follow from simple information-theoretic arguments.

the EP will not be caught when making a false claim is less than $1/2^k$.[13]

The random-representation approach extends to verify properties between input and output values that can be computed through a *straight line computation*. This is a computation on inputs $x_1, \ldots, x_n$ that corresponds to a sequence

$$\text{SLC} = x_1, \ldots, x_n, x_{n+1}, \ldots, x_L, \tag{3}$$

where for all $t > n$ there exist $j, k < t$ for which properties such as $x_t = x_j + x_k$ or $x_t = x_j \cdot x_k$ or $x_t = x_j$ hold, and where x_L is the output. By creating a random representation of all intermediate values, the challenge-and-respond proof structure extends to prove the correctness of a straight line computation. The approach also extends to prove inequality and interval membership properties between values (see Rabin et al. [25]).

It is worth emphasizing that the algorithmic approach to compute the output $f(x_1, \ldots, x_n)$ from the inputs is not restricted to straight-line computation. Rather, this can be done via any algorithmic approach. It is just the proof of correctness that must be performed through properties that can be straight-line computed (i.e., without branching). For example, the winner of an auction can be determined by finding the maximum of a set of bids. Suppose that bidder 1 is the winner. The proof would then establish $x_1 > x_j$ for all $j \neq 1$. The proof structures enabled by straight-line computation seem quite flexible can be applied to settings such as multi-unit and combinatorial auctions.

2.4 Strong Secrecy

Given the short-term price impact that can arise from information about orders, and because of parasitic practices such as front-running, providing a guarantee of strong secrecy may be important for trading systems.

How important this is in practice will depend on the specifics of the market design. For example, it will depend on the extent to which information that is available to an EP could be used in a way that is detrimental to investors who participate in the trading system. A design that includes an enforced delay in information flow, as in the IEX market, is already more robust against front-running by HFTs. A design that fills every order, and does so in a batch auction (as in Thorpe and Parkes [42]) for which pre-trade information is kept secret, leaves little actionable *a posteriori* information.

The importance of strong secrecy also depends on what information can already be discovered through trading. For example, a dark pool that admits HFTs and allows HFTs to trade with passive investors may already leak considerable information about large orders. If a pool is already leaky in this sense then strong secrecy doesn't add much of value!

We describe two approaches to addressing this challenge of strong secrecy. The first uses secure computing hardware and the second uses secure multi-party computation.

Trusted Computing.

One approach to achieving strong secrecy is to retain the EP model but adopt specialized hardware to prevent undesired information disclosure.

A *Trusted Computing* infrastructure, based on secure hardware and digitally signed software, and installed in a physically secure location with ongoing automated monitoring, can prevent the leaking of information [37]. Trusted Computing makes use of a secure processor, which is a closed device for which all outputs are publicly observable. A useful mental model is that of a "computer in a cage" with all outputs monitored.

Because the communication interfaces are monitored, communication can be restricted to information in allowed categories, such as (i) trades, (ii) proofs of correctness, or (iii) other information required by regulators or for compliance.[14] Secrecy-preserving correctness proofs complement this approach— we need not trust the computer to produce correct results, the proofs play this role.

Research into the use of Trusted Computing infrastructure to build markets that are both provably correct and provide strong secrecy is still in its infancy. For example, one concern is that information could still leak out even if the only data that is posted falls into an approved category. For example, there could be a "steganographic attack," where information is smuggled through covert channels (perhaps embedded in the use of spaces or fonts). This smuggling could also happen through appropriate choices of random values when constructing proofs, these values revealed during the verification process.[15]

Multi-party function evaluation.

A second approach to strong secrecy is to adopt methods from *secure multi-party computation*; see Harkavy et al. [13] and Bogetoft et al. [1]. At a high-level, these approaches tend to assume the existence of multiple, non-colluding computers that work collectively to operate the trading system. These computers comprise a distributed computational model for the trading system. It is important that these entities are each operated by a different business, because secrecy is only achieved when they can be trusted to work independently and not collude. Each trader distributes parts of his or her input (i.e., order) to each computer. As long as enough computers follow the protocol, it is not possible for any entity to learn the orders, and no information can be disclosed.

As discussed earlier, these kinds of secure multi-party computation approaches are likely impractical for financial exchanges because of the latency involved in computation. Computation involves a large number of rounds of message passing between the distributed machines, introducing latency (something hard to tolerate in the context of financial markets). Moreover, an outside observer must trust that the rules of the protocol are being correctly followed, and cannot independently verify this. Finally, the computational model of multiple, independent entities operating the distributed trading system does not typically fit well with business models; a possible exception is the Luminex dark pool, which will be co-sponsored by a number of market participants to which its operation could be distributed.[16]

[13] In particular, multiple random representations of the inputs are generated (and verified to be equal to each other), and then the verifier issues k independent challenges. Because the verifier will only accept the proof if every challenge succeeds, the probability bound follows [26]. A recent extension allows the prover to supply any required number of proofs to multiple verifiers, by creating more copies of the input on the fly as required [25].

[14] This third kind of data can be encrypted (e.g., with the public key of a regulator), and itself be subject to a proof of correctness, in order to verify that it is correctly computed on the basis of orders placed and trades executed.

[15] In regard to this concern, Rabin et al. [26] propose to use an independent secure co-processor RANDOM with a physical random number generator that acts as a universal source of randomness.

[16] Di Crescenzo [7] describes an approach where each trader participates in a secure, two-party computation with a single market operator. However the market operator is assumed to be "honest but curious," meaning that it would like to learn the inputs but will run any program honestly. This does not seem very realistic.

3. CONNECTING TO DARK POOLS

In this section, we provide a high-level description of three stylized dark pool designs, any of which would benefit from secrecy-preserving proofs of correctness in building trust.

3.1 Continuous, Block trades only

The design of the proposed Luminex dark pool could be instantiated within the EP model (see challenge **I**, above):

1. A trader can submit an order at any time to buy or sell a stock, along with an "auto-execute amount" and a maximum quantity. These orders are posted to a bulletin board in a "sealed" form (eg., using homomorphic encryption or random-representations.)
2. The EP privately receives the inputs.
3. Any time there is a match (a buy and sell order on the same stock), the EP will execute a trade. First, if the orders suggest that a larger trade is possible, each counter-party is given a specified delay (e.g., 20 seconds) to privately report a quantity between its auto-execute amount and its max. These quantities are sealed and posted to a bulletin board. Time-lapse cryptography can keep information sealed during the time interval.
4. The EP executes the trade at the midpoint of the NBBO (or the volume-weighted average NBBO price if a delay was incurred), and at the maximum possible quantity given the reports.
5. The EP publishes a proof of correctness (i.e., that the two orders should match according to the priority rule, that the quantity traded is correct, etc.).

Some details would need to be worked out in regard to how to handle priority rules. But supposing a quantity-time rule then this would require that an order selected to match is either strictly larger than all other orders, or that there is no larger order and that this order arrived no later than any other orders of the same size. Proving these kinds if inequality relationships on inputs is familiar from proving the correctness of the outcome of an auction (e.g., for a second-price auction with bids $x_1, \ldots, x_n$, that $x_1 > x_j$ $(j \neq 1)$ and $x_2 \geq x_j$ $(j \neq 1)$).

The proposed design of the Luminex dark pool includes a minimum block size for any trade, and traders must commit to trade at least this quantity in the event of a match. This is to make it more difficult for information to leak to HFTs through trading. Placing orders to gain information about the order book becomes more costly— an algorithm would need to buy (or sell) a large number of stocks in order to learn about another order.

3.2 Continuous, with Counter-party awareness

A lingering question is whether there will ever be enough contraside interest amongst a dark pool that is restricted to only include institutional investors, many of whom are tracking the same stock indexes. According to Levine [16] the "dream of many institutional investors, and ... the story that every dark pool wants to tell" is:

> *"You can trade stocks without interacting with professional traders who expect to make money in the short term by interacting with institutional order flow. You can have a market that is just institutions trading with institutions, with no short-term profit-seekers hanging around taking their share.*

Levine continues:

> *"But there's a problem, which is that it doesn't work very well. When you just put institutional investors in a pool that excludes high-frequency traders, they have a hard time trading with each other. There's not, it turns out, all that much natural liquidity."*

This helps to rationalize the design of the Barclays LX dark pool, and suggests a second, stylized design. Like the LX pool, this design allows both active and passive investors, but tries to provide some transparency as to trading styles. In particular, the LX pool is designed to allow an investor to know something about how "aggressive" a counter-party is, and choose who they want to match against (and thus which kinds of traders may gain information about their order).

Responding to challenge **II**, we also note that the design of the LX pool fits well with the EP model: secrecy-preserving proofs of correctness can be used to prove that a publicly available computation is used correctly to assign an "aggressiveness" label to a trader, and that rules are used correctly for matching, all the while without revealing information about the label itself or the history of orders or trades of an individual.

3.3 Frequent Batch, Passive and Active

It's worth taking a step back, and asking what trust is enabled by using secrecy-preserving proofs of correctness, without strong secrecy, in a market that uses a continuous limit order book. True, the market operator can only follow the published rules in deciding on trades to execute. Proofs of correctness allow this kind of trust to be established. But nothing prevents a market operator at any time once an order has been placed, and before the order has traded, from leaking information about this order. The distinction between "before" and "after," present in a sealed-bid auction, is completely blurred in an asynchronous, continuous trading environment. It is good that a market operator does not need to reveal information to establish proofs of correctness. But without strong secrecy, a market operator cannot commit not to leak pre-trade information.

A third, stylized design is use a frequent batch auction. In contrast to the design of Budish et al. [5], the design would complete all trades at the mid-point of the NBBO. The design would insist on pegged orders from institutional investors (to trade at the midpoint of NBBO), coupled with auto-execute quantities (as in the Luminex design). The design could choose to allow limit orders and smaller quantities from active investors, seeking to promote additional liquidity.[17] Rather than disclose orders at the end of the time interval, a secrecy-preserving proof of correctness can be provided at the completion of every batch (challenge **III**).

In addition to the benefits outlined by Budish et al. [5], including lower cost of providing liquidity and mitigating the advantage gained by fast traders over slow traders, the use of batch auctions over continuous limit books provides more for cryptographic methods to do. By providing a clear "before" and "after" distinction, the auction takes on the flavor of a sealed-bid auction and bids placed during the time interval between batches can be kept secret from all participants, including the market operator, using time-lapse cryptography. By also including an enforced delay of information flow (IEX style), the routing algorithms used by the pool in meeting the "order protection" regulation (see the Appendix) can reach other exchanges before information about orders can be used by HFTs.

[17]The intent here is not to be overly prescriptive, but to suggest a combination of features that could be useful in enabling a well-functioning dark pool.

3.4 Discussion

In regard to strong secrecy (challenge **IV**), and proving that statements of interest or orders cannot be shared with other parties, the most promising direction is to adopt Trusted Computing. This would replace the EP with a *Secure Processor Evaluator-Prover* (SPEP) [26], and a computer that is not only able to prove the correctness of its outputs given its inputs but also able to commit to only reveal allowable information (such as a record of executed trades, proofs of correctness.) Given the importance of fair and well-functioning financial markets and the resources that can be brought to bear in this industry sector this topic is worthy of ongoing research and development.

Another use of cryptographic technology is for *provably correct disclosure* in meeting regulatory requirements. For example, a dark pool can publish and prove the correctness of aggregate volume statistics without disclosing any information about order flow. This can be useful in promoting stronger regulation without compromising proprietary information corresponding to strategies [9]. Regulators may also be interested in a proof that traders are not using the prohibited practice of "spoofing" [36]. Navigant [20] suggest that it is hard for regulators to monitor this because of the lack of transparency in dark pools.[18]

Another suggested application users cryptographic methods to provide a trustworthy trading system that supports rule-based trading, with participants submitting general trading rules rather than orders to buy and sell [43]. In addition to leveling the playing field between various parties, with all rules executed on the basis of the current market price (e.g., from NBBO at each "tick" of the exchange), this may allow the exchange or regulators to examine systemic risks or simulate various scenarios on the market.

4. CONCLUSIONS

Market design is unnecessarily encumbered by concerns about trust. Are published information flows and order processing rules being faithfully followed? Good actors who want to build well functioning markets are hampered by problems of adverse selection. It is difficult to credibly commit to operating a dark pool that does not leak information, does not provide advantages to some subset of traders, and does not facilitate trades through affiliated businesses.

The interim CEO of Luminex has stated that his goal is "*to build trust among users* through transparent trading rules and protocols and efficient execution" (emphasis added) [6]. Yet the straightforward meaning of transparency is at odds with what institutional investors find interesting about dark pools. Investors don't want anyone to literally be able to see everything that is happening in the dark pool. Secrecy-preserving proofs of correctness can provide both trust and transparency. A market operator can prove that rules are being correctly implemented without revealing information about orders that investors would prefer to remain hidden. With ongoing research and development, strong secrecy can also be provided, so that the market operator is completely prevented from revealing pre-trade information about orders.

[18]Spoofing is the name given to the behavior of artificially placing a large order outside the bid-ask spread and then canceling it, expecting that information will leak out to HFTs who will trade and move the price slightly but on the basis of misleading information. For example, an investor with a large block of securities may place a large buy order, driving up the price. The order can be canceled, with the investor instead selling smaller portions of the security.

Notes and Acknowledgments

Thanks to Michael Rabin, without whom this work wouldn't be possible. Parkes and Thorpe have authored patents related to some of the ideas presented in this paper.[19]

Appendix

A1. Actions by Regulators against Dark Pool Operators

Pipeline.

In October 2011, the SEC charged the Pipeline dark pool with violating regulations by misrepresenting the way in which trades were being executed [35].[20] Pipeline stated that it operated a market that matched customer orders with those from other customers, and prevented the disclosures of pre-trade information. But according to the SEC, Pipeline failed to disclose that upwards of 80% of the shares traded where bought or sold by a wholly owned subsidiary of Pipeline. This subsidiary had special access to data about trading activity in order to more accurately predict the side and limit price of customer orders, and would also place and then cancel large orders to assess interest. It would then buy shares in other markets and seek to sell in the dark pool, or otherwise sell short and seek to buy in the dark pool. Without acknowledging guilt, Pipeline agreed to settle the SEC's charges and pay a $1 million penalty.

Liquidnet.

In June 2014, the SEC charged Liquidnet, Inc. with violating ATS regulations by not protecting the confidentiality of pre-trade data [34]. Liquidnet operates a dark pool for large block trades and represented to its members that it would keep their trading information confidential and allow them to trade with maximum anonymity and minimum information leakage.[21] According to the SEC, the "Ships Passing alert" tool notified Liquidnet's trading desk (which

[19]David C. Parkes, Michael O. Rabin, Stuart M. Shieber, and Christopher A. Thorpe. Practical Secrecy-Preserving, Verifiably Correct and Trustworthy Auctions. U.S. Patent 8,024,274.
Michael O. Rabin and Christopher A. Thorpe, Method and apparatus for time-lapse cryptography U.S. Patent 8,526,621.
Christopher A. Thorpe and David C. Parkes. Zero-knowledge proofs in large trades US Patent application 2009/0177591.
David C. Parkes and Christopher A. Thorpe. Zero-Knowledge Proofs in Large Trades. October 2008. U.S. Patent Application 2009/0177591.
Michael O. Rabin, Rocco A. Servedio, Christopher Thorpe. Highly efficient secrecy-preserving proofs of correctness of computation U.S. Patent Application 2009/0327141

[20]Pipeline was launched in 2004, using software originally developed by Fidelity. The system imposed a minimum order size of 10,000, 25,000 or 100,000 shares depending on the stock. When an order was placed the stock symbol would be displayed to all members, but without indicating the side, price or size. If two customers entered market orders for the same stock on opposite sides the trade would be executed at the midpoint of the NBBO at the time of the trade. It changed its name to Aritas in January 2012, and closed in May 2012.

[21]The Liquidnet dark pool has electronic access to a member's order management system and looks for matches among members interested in buying and selling the same stock. The potential buyers are invited to negotiate with each other, anonymously, through the Liquidnet system [34]. Once negotiations begin, typically they are completed within seconds [2] and the vast majority of trades occur at the NBBO midpoint. Liquidnet controls participation by monitoring the propensity of participants to complete a trade once matched.

it operated, in addition to its dark pool) when there were missed execution opportunities based on member indications. Another tool, "Internal InfraRed" provided information on the indicated interest and number of shares that Liquidnet members were interested in buying or selling to employees in a business unit. Without acknowledging guilt, Liquidnet agreed to settle the SEC's charges and pay a $2 million penalty.

Goldman Sachs SIGMA X.

In June 2014, the Financial Industry Regulatory Authority (FINRA), an independent regulator for securities firms in the U.S., charged that the Goldman Sachs SIGMA X dark pool executed nearly 400,000 trades between July 29, 2011, and August 9, 2011 at a price inferior to the best price on public exchanges [10].[22] Without acknowledging guilt, Goldman Sachs agreed to settle FINRA's charges and pay a $800,000 penalty.

Barclays LX.

In June 2014, the U.S. State of New York charged that Barclays defrauded and deceived participants in its LX dark pool, at the time the second-largest dark pool by volume [21].[23] According to the complaint, while Barclays was telling investors it monitored the dark pool to keep the market free from HFTs minimize the likelihood that HFTs would act as counterparties, Barclays was catering to HFTs rather than protecting them. Barclays represented that its "Liquidity Profiling" tool would monitor every trade in the dark pool and grade traders by how "aggressive" their trading activity was ("0" aggressive, "5" passive), and allow members to decline to trade with some grades. But the Attorney General charges that Barclays (i) did not remove aggressive traders from the market, (ii) altered the profiles of traders from within Barclays such as Barclays Capital Making to make them a "4" despite being evaluated as a "0" or a "1", (iii) did not apply profiling to many orders, and (iv) provided HFTs with special access to servers to gain a speed advantage. Barclays contests the suit.

Citigroup LavaFlow.

In July 2014, the SEC charged that Citigroup's LavaFlow trading system failed to protect confidential member data, allowing an affiliate to gain access to help determine where to route orders [33].[24] According to the SEC, LavaFlow also provided non-displayed orders, promising that pre-trade information on these orders would remain hidden. LavaFlow allowed a subsidiary to use a system named "ColorBook" to gain access to information about these non-displayed orders, using the information to decide how to route orders for its own customers. Without acknowledging guilt, Citigroup agreed to settle the SEC's charges and pay a $5 million penalty.

UBS dark pool.

In January 2015, the SEC charged that UBS created secret order types in its dark pool to allow HFTs to exploit investors, without disclosing this to participants [32]. Orders could be placed fractionally above or below other orders, violating regulation designed to prevent orders from executing before others based on economically insignificant sub-penny differences. These order types were marketed almost exclusively to HFTs, according to the SEC. The SEC also charges that UBS failed to disclose a system to prevent an order executing against aggressive traders, making this available only for orders executed by UBS's own trading algorithms. Without acknowledging guilt, UBS agreed to settle the SEC's charges and pay a $14.4 million penalty.

A2. U.S. Regulatory Landscape

Securities Exchange Act (1934).

The SEC is charged with facilitating the establishment of a national market system that promotes five objectives: (1) economically efficient execution of securities transactions, (2) fair competition among broker-dealers, among exchange markets, and between exchange markets and non-exchange markets; (3) price transparency; (4) best execution of investor orders; and (5) an opportunity, consistent with economic efficiency and best execution, for investor orders to meet without the participation of a dealer.

National securities exchanges.

Regulated markets that include Nasdaq, the New York Stock Exchange (NYSE), NYSE Arca, BATS Exchange and Nasdaq OMX BX. Two defining features of a national securities exchange are:

(a) they have to be open to anyone to trade

(b) if orders are displayed to traders (orders need not be displayed) then the best prices must be published to the consolidated quotation stream.

Alternative trading systems (ATS) .

An ATS provides a marketplace for buyers and sellers of securities, but is regulated differently from a public exchange. An ATS is private, has members, and can discriminate who comes into the trading system. In addition, an exemption (see Reg ATS, below) allows orders to be displayed to members without going to the consolidated quotation stream. ATSs include electronic crossing networks (ECNs) and dark pools. ECNs offer various order types including both displayed and undisplayed order types. Dark pools generally provide just non-displayed order types.

Regulation NMS (2007).

Reg NMS is a set of rules that applies to trading in any National Market System (NMS) stock, which generally means any exchange-listed security. Reg NMS applies to both public exchanges and ATSs. Components of Reg NMS include:

(a) A fair access provision. If trade volume in a stock is greater than 5%, then a trading system cannot deny access based on potential trading strategies of an applicant.[25]

(b) Order protection (or "trade through") rule. A public exchange with displayed orders has what are called "protected" orders and the best bid and ask most be distributed to the consolidated quotation stream.[26] All other markets have to respect the best published prices: no trade can occur on a NMS stock during regular trading

[22] The Goldman Sachs SIGMA X dark pool was launched in 2006 and facilitates block trades. Today it is the sixth largest ATS by volume [40].

[23] The Barclays LX dark pool provides two types of interactions. Members can post a limit order or place a market or pegged order. LX provides Liquidity Profiling using metrics to determine whether an order flow is aggressive, based on the movement of price after trades and the size of trades. Members can specify which grades are acceptable for a counter-party in a trade.

[24] Lava Flow was an electronic crossing network (ECN), providing much of the same functionality as public exchanges, including both displayed and non-displayed orders. Citigroup closed LavaFlow system on January 30, 2015. Citigroup continues to operate Citi Cross, Citi Liquifi and Citi Match.

[25] Liquidnet gained a 20% exemption.

[26] A public exchange does not need to display orders. For example, a frequent batch auction with an undisplayed order type would not need to publish orders.

hours at a price that is outside the best publicly displayed price.[27]

The main exception to this is provided by an *Intermarket Sweep Order* (ISO). Such an order can be executed immediately, without checking for prices in other public exchanges. In this case, the responsibility for ensuring order protection is held by the initiator of the order, who should send a limit order at the current best displayed price to all markets simultaneously to ensure compliance.[28]

Consolidated quotation stream.

Public exchanges must publish best displayed bids and asks to a consolidated quotation stream. ATSs must also do this for orders displayed to their subscribes when the volume that is traded in the stock is above 5% of total volume. This live stream is consolidated by the Security Information Processor (SIP), currently operated by the Nasdaq. The SIP is used to define the NBBO at any point in time. It is with regard to the NBBO that the order protection rule of reg NMS is defined.

Regulation ATS (2002).

Reg ATS is a set of rules that regulate ATSs, allowing them to operate under a different legal framework from national securities exchanges. In particular, an ATS can discriminate who comes into the system, for example based on trading behavior. An ATS must still meet the fair access and order protection provisions of Reg NMS. Components of Reg ATS include:

(a) Display/execute exemption. If the trading volume in a stock is below 5% of national volume, then there is an exemption from the requirement to publicly distribute the best bid and ask quote to the consolidated quotation stream.[29] (An ATS that does not display orders to its own members does not need to distribute best bid and ask quotes even if its trading volume is greater than 5%.)

(b) an ATS must establish safeguards and procedures to protect members' confidential trading information.

Post-trade information.

SEC rules require that post-trade information be reported to a Financial Industry Regulatory Authority (FINRA) trade reporting facility once trades have executed, and typically within 30 seconds of the trade. This information is then disseminated to the market.

FINRA Trade Data Disclosure Requirements (2014).

ATSs are required to report their aggregate weekly volume of transactions and number of trades by security (in part, this is to enable regulators to check for trading volume thresholds in regard to Reg ATS).

Regulation Systems Compliance (2015).

The Reg SCI rules apply to national securities exchanges and ATSs and generally obligate market operators to implement and enforce policies and procedures related to capacity, integrity, resiliency, availability and security of their systems. In part, Reg SCI is designed to establish procedures that promote the maintenance of fair and orderly markets and ensures that they operate in a manner that complies with the Exchange Act.

[27]Dark pools such as Liquidnet that set the price based on manual negotiation using a messaging system have an exemption; in this case, the price at which trade occurs must be within the NBBO at some point in the last 20 seconds.

[28]For example, a dark pool can be compliant with the order protection rule by sending ISOs to execute against any better-priced, protected quotations, in all public exchanges at the same time as matching block orders within the pool.

[29]Liquidnet has received a 20% exemption.

5. REFERENCES

[1] P. Bogetoft, I. Damgård, T. Jakobsen, K. Nielsen, J. Pagter, and T. Toft. A practical implementation of secure auctions based on multiparty integer computation. In *Proc. 10th International Conference on Financial Cryptography and Data Security (FC 2006)*, 2006.

[2] L. Boni, D. C. Brown, and J. C. Leach. Dark pool exclusivity matters. Technical report, Leeds School of Business, U. Colorado, 2012.

[3] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37:156–189, 1988.

[4] E. Budish, P. Cramton, and J. Shim. Implementation details for frequent batch auctions. *American Economic Review*, 104:418–424, 2015.

[5] E. Budish, P. Cramton, and J. Shim. The High-Frequency Trading Arms Race: Frequent Batch Auctions as a Market Design Response. Technical report, University of Chicago Booth School of Business, June 4, 2015.

[6] J. Detrixhe and S. Mamudi. Fidelity-BlackRock group unveils dark pool for stock trades. *Bloomberg news*, January 20, 2015. `http://www.bloomberg.com/news/articles/2015-01-20/fidelity-blackrock-group-prepares-dark-pool-for-big-stock-trades` Accessed on July 14, 2015.

[7] G. Di Crescenzo. Privacy for the stock market. In *Proc. 5th Int. Conf. on Financial Cryptography and Data Security (FC'01)*, pages 269–288, 2001.

[8] Y. Dodis. Introduction to Cryptography (Lecture 14, CSCI-GA.3210-001). `http://www.cs.nyu.edu/courses/spring12/CSCI-GA.3210-001/lect/lecture14.pdf`, Accessed on July 17, 2015.

[9] R. S. England. Can Dark Pool Luminex Unlock Enough Liquidity for Block Trades? *Institutional Investor*, May 29, 2015. `{http://www.institutionalinvestor.com/article/3458142/investors-endowments-and-foundations/can-dark-pool-luminex-unlock-enough-liquidity-for-block-trades.html#.VaViANbgq8Z}`,Accessed on July 14, 2015.

[10] FINRA. FINANCIAL INDUSTRY REGULATORY AUTHORITY LETTER OF ACCEPTANCE, WAIVER AND CONSENT NO.20110307615-01 RE: Goldman Sachs Execution & Clearing, L.P. *Financial Industry Regulatory Authority*, July 1, 2014.

[11] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their own validity, or all languages in NP have ZKP systems. *J. ACM*, 38:692–729, 1991.

[12] S. Goldwasser, S. Micali, and C. Racoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18:186–208, 1989.

[13] M. Harkavy, J. D. Tygar, and H. Kikuchi. Electronic auctions with private bids. In *Proc. Third USENIX Workshop on Electronic Commerce*, pages 61–74, 1998.

[14] B. Hope. NYSE Group planning midday auction for its stock markets. *The Wall Street Journal*, Jan. 2015.

[15] J. Kilian. A note on efficient zero-knowledge proofs and arguments. In *Proc. 24th Annual ACM STOC*, pages 723–732, 1992.

[16] M. Levine. Barclays not smart. *BloombergView*, June 25, 2014. http://www.bloombergview.com/articles/2014-06-26/barclays-not-smart, Accessed on July 18, 2015.

[17] M. M. Lewis. *Flash boys: A Wall Street revolt*. W. W. Norton & Co. (New York), 2014.

[18] H. Lipmaa, N. Asokan, and V. Niemi. Secure Vickrey auctions without threshold trust. In *Proc. 6th International Conference on Financial Cryptography and Data Security (FC 2002)*, pages 87–101, 2002.

[19] M. Naor, B. Pinkas, and R. Sumner. Privacy preserving auctions and mechanism design. In *Proc. First ACM Conf. on Electronic Commerce*, 1999.

[20] Navigant. Client alert: Dark pools and the new frontier of regulation. *Navigant Consulting*, 2015. {http://www.navigant.com/~/media/WWW/Site/Insights/Financial%20Services/2015/GIC_DarkPools_TL_0215%20FINAL.ashx},Accessed on July 17, 2015.

[21] NYAG. Initial Complaint against Barclays Capital, Inc. and Barclays PLC, Index No. 451391/2014. *New York State Attorney General*, June 25, 2014.

[22] P. Paillier. Public-key cryptosystems based on composite residuosity classes. In *Proc. EUROCRYPT '99*, pages 223–239, 1999.

[23] D. C. Parkes, M. O. Rabin, S. M. Shieber, and C. Thorpe. Practical secrecy-preserving, verifiably correct and trustworthy auctions. *Electronic Commerce Research and Applications*, 7:294–312, 2007.

[24] D. C. Parkes, M. O. Rabin, and C. Thorpe. Cryptographic combinatorial clock-proxy auctions. In *Proc. 13th International Conference on Financial Cryptography and Data Security (FC'09)*, pages 305–324, 2009.

[25] M. O. Rabin, Y. Mansour, S. Muthukrishnan, and M. Yung. Strictly-black-box zero-knowledge and efficient validation of financial transactions. In *Proc. 39th International Colloquium on Automata, Languages, and Programming (ICALP'12)*, pages 738–749, 2012.

[26] M. O. Rabin, R. A. Servedio, and C. Thorpe. Highly efficient secrecy-preserving proofs of correctness of computations and applications. In *Proc. 22nd IEEE Symposium on Logic in Computer Science (LICS'07)*, pages 63–76, 2007.

[27] M. O. Rabin and C. Thorpe. Time-lapse cryptography. Technical Report TR-22-06, Harvard John A. Paulson School of Engineering and Applied Sciences, 2006.

[28] R. L. Rivest, A. Shamir, and D. A. Wagner. Time-lock puzzles and timed release crypto, 1996.

[29] R. A. Schwartz, editor. *The electronic call auction: market mechanism and trading*. Springer (New York), 2001.

[30] SEC. Rule 611 of Regulation NMS. *SEC Division of Trading and Markets*, April 30, 2015.

[31] SEC. Order instituting administrative and cease-and-desist proceedings in the matter of EDGA Exchange, Inc., and EDGX Exchange, Inc. *Securities and Exchange Commission*, January 12, 2015.

[32] SEC. Administrative Proceeding in the Matter of UBS Securities, LLC. *Securities and Exchange Commission*, January 15, 2015.

[33] SEC. Administrative Proceeding in the Matter of LavaFlow, Inc. *Securities and Exchange Commission*, July 25, 2014.

[34] SEC. Administrative Proceeding in the Matter of Liquidnet, Inc. *Securities and Exchange Commission*, June 6, 2014.

[35] SEC. Administrative Proceeding in the Matter of Pipeline Trading Systems LLC. *Securities and Exchange Commission*, October 24, 2014.

[36] SEC. Administrative Proceeding in the Matter of Hold Brothers On-line Investment Services. *Securities and Exchange Commission*, September 25, 2012.

[37] S. W. Smith. *Trusted Computing Platforms: Design and Applications*. Springer, New York, 2005.

[38] J. Spicer. Direct Edge in crosshairs of "flash" orders debate. *Reuters*, July 27, 2009. {http://www.reuters.com/article/2009/07/27/us-exchanges-flashes-analysis-idUSTRE56Q4B320090727}, Accessed on July 13, 2015.

[39] P. Stafford. LSE to launch midday stock auction. *Financial Times*, November 2014.

[40] Tabb. Equities liquidity matrix. *Tabb Group*, June 2015. {http://tabbforum.com/liquidity-matrix/equities}, Accessed on July 13, 2015.

[41] C. Thorpe and D. C. Parkes. Cryptographic securities exchanges. In *Proc. 11th International Conference on Financial Cryptography and Data Security*, pages 163–178, February 2007.

[42] C. Thorpe and D. C. Parkes. Cryptographic combinatorial securities exchanges. In *Proc. 13th International Conference on Financial Cryptography and Data Security (FC'09)*, pages 285–304, 2009.

[43] C. Thorpe and S. R. Willis. Cryptographic rule-based trading (short paper). In *Proc. 16th Int. Conf. on Financial Cryptography and Data Security (FC'12)*, pages 65–72, 2012.

[44] E. Wah, D. R. Hurd, and M. P. Wellman. Strategic Market Choice: Frequent Call Markets vs. Continuous Double Auctions for Fast and Slow Traders. In *AAAI'15*, 2015.

[45] E. Wah and M. P. Wellman. Latency arbitrage, market fragmentation, and efficiency: A two-market model. In *Proc. 14th ACM Conference on Electronic Commerce*, pages 855–872, 2013.