Trust without Disclosure:
Dark Pools and Secrecy-Preserving Proofs

David C. Parkes
Harvard University

Christopher Thorpe
(Harvard iLab)

Wei Li
Citigroup

• Based on a talk and paper I presented at The Third Conf. on Auctions, Market Mechanisms and Their Applications, Aug 8-9, 2015

• Regulatory action correct as of August 9th, 2015!

• Paper: see my publications page at http://econcs.seas.harvard.edu/
Dark Pools

- Restrict participation to institutional investors
- Don’t display orders
- Trade at broader market price
- Avoid interaction with HFTs

Buy 100,000 IBM

Sell 50,000 MSFT

... Trades

passive investors

active investors

... 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.

The Dream

• “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.”

Continued Market Fragmentation

Today U.S. stock market ~10 public exchanges, ~45 alternative trading systems, including dark pools. Market innovation!

Regulation Landscape

- Exchanges are public; ATSSs can be private
  - “fair access rule”
  - ATS can deny access if <=5% volume
- Orders can be displayed or non-displayed
- If public (or >5%): displayed orders -> CQS -> National Best Bid and Offer
  - “order protection rule”
- All trades must be inside NBBO
## Examples of Dark Pools

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Details</th>
<th>Avg trade size, midpoint NBBO</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipeline</td>
<td>CLOB</td>
<td>Min order size, partial display</td>
<td>~50,000, ?</td>
<td>'04-'12</td>
</tr>
<tr>
<td>Liquidnet</td>
<td>Negotiation</td>
<td>Price/volume via IM</td>
<td>38,000, 97%</td>
<td>'01-</td>
</tr>
<tr>
<td>Barclays LX</td>
<td>CLOB</td>
<td>Profiling</td>
<td>~200, 40%</td>
<td>'06-'15</td>
</tr>
<tr>
<td>Citi Lavaflow</td>
<td>CLOB</td>
<td>Allow display orders</td>
<td>~300, 10%</td>
<td>'06-'15</td>
</tr>
<tr>
<td>UBS dark pool</td>
<td>CLOB</td>
<td></td>
<td>~150, 60%</td>
<td>'08-</td>
</tr>
</tbody>
</table>

- Continuous Limit Order Book
- Provide “pegged orders” that execute at mid-NBBO

## Some Details

- [LiquidityMatrixTM](#) June 2015
Pipeline (‘04-’12)

- CLOB
- Minimum order size of 10,000, 25,000 or 100,000 shares depending on stock
- When order placed, symbol showed to all members, but not the side, price or size
- Allow orders pegged to mid-point NBBO

Liquidnet (‘01-present)

- Negotiation
- Installed on Order Management Systems on trading floors
- Two parties on opposite side invited to negotiate price and volume
- Negotiation via IM, anonymous
- ~38,000 avg block size, 97% at NBBO midpoint, “within seconds”
Barclays LX (‘08-present)

• CLOB

• Both limit and pegged orders
• Liquidity profiling: how “aggressive” is trader, based on price movement, size of trades
• Trader A can restrict the “liquidity profile” of a counterparty

• Small trade sizes; ~40% at mid-NBBO

Follow your dreams...

• “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 …”
## Regulator complaints

<table>
<thead>
<tr>
<th>Dark pool / ATS</th>
<th>Date of complaint</th>
<th>Complaint</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipeline</td>
<td>Oct’11</td>
<td>Majority of trades executed by subsidiary</td>
<td>$1m</td>
</tr>
<tr>
<td>Liquidnet</td>
<td>June’14</td>
<td>Pre-trade indications shared with trading desk</td>
<td>$2m</td>
</tr>
<tr>
<td>Citigroup</td>
<td>July’14</td>
<td>Non-displayed orders shared with affiliate</td>
<td></td>
</tr>
<tr>
<td>Barclays LX</td>
<td>June’14</td>
<td>Inconsistent profiling, no action taken, some profiles altered, HFTs given special access</td>
<td></td>
</tr>
<tr>
<td>UBS dark pool</td>
<td>Jan’15</td>
<td>Sub-penny order types to HFTs, selective access to profiling system</td>
<td>$14.4m</td>
</tr>
</tbody>
</table>
## Regulator complaints

<table>
<thead>
<tr>
<th>Dark pool / ATS</th>
<th>Date of complaint</th>
<th>Complaint</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipeline</td>
<td>Oct’11</td>
<td>Majority of trades executed by subsidiary</td>
<td>$1m</td>
</tr>
<tr>
<td>Liquidnet</td>
<td>June’14</td>
<td>Pre-trade indications shared with trading desk</td>
<td>$2m</td>
</tr>
<tr>
<td>Barclays LX</td>
<td>June’14</td>
<td>Inconsistent profiling, no action taken, some profiles altered, HFTs given special access</td>
<td>Contested</td>
</tr>
<tr>
<td>Citigroup Lavaflow</td>
<td>July’14</td>
<td>Non-displayed orders shared with affiliate</td>
<td>$5m</td>
</tr>
</tbody>
</table>
### Regulator complaints

<table>
<thead>
<tr>
<th>Dark pool / ATS</th>
<th>Date of complaint</th>
<th>Complaint</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipeline</td>
<td>Oct’11</td>
<td>Majority of trades executed by subsidiary</td>
<td>$1m</td>
</tr>
<tr>
<td>Liquidnet</td>
<td>June’14</td>
<td>Pre-trade indications shared with trading desk</td>
<td>$2m</td>
</tr>
<tr>
<td>Barclays LX</td>
<td>June’14</td>
<td>Inconsistent profiling, no action taken, some profiles altered, HFTs given special access</td>
<td>Contested</td>
</tr>
<tr>
<td>Citigroup Lavaflow</td>
<td>July’14</td>
<td>Non-displayed orders shared with affiliate</td>
<td>$5m</td>
</tr>
<tr>
<td>UBS dark pool</td>
<td>Jan’15</td>
<td>HFTs allowed sub-penny orders, selective access to profiling system</td>
<td>$14.4m</td>
</tr>
</tbody>
</table>

### Some Responses

- **IEX Market** (insert a 0.00035 second delay to limit HFT’s ability to respond)
Responses –IEX market

• CLOB
• 350 microsec delay on data; 38-mile coil of optical fiber.
• IEX gets pricing in other exchanges before HFTs can respond.
• Moving towards a public exchange, displayed orders.

Some Responses

• IEX Market (insert a 0.0007 second delay to limit HFT’s ability to respond)
• Frequent batch auctions (Budish et al., QJE 2015)
Some Responses

• IEX Market (insert a 0.0007 second delay to limit HFT’s ability to respond)
• Frequent batch auctions (Budish et al., QJE 2015)
• Luminex Dark Pool
  – “By the buy side, for the buy side”, led by Fidelity
  – Bids convey volume, price at midpoint NBBO
  – Interim CEO goal “build trust among users through transparent trading rules and protocols…”

Review

• Concerns about predatory practices in exchanges.
• Dark pools envisioned as a way for “sheep” to trade amongst themselves, hide information.
• But their very opaqueness has led to new concerns, to regulatory actions.

How to design a trustworthy, dark pool?
Example Challenges

• Could we prove the following:
  – Correctly follow priority rules when clearing orders?
  – Orders are sealed until end of interval, not modified, and priced correctly?
  – Correctly compute “aggressiveness” labels, apply filter?

Cryptography for proving correctness.
Cryptography for hiding.

Using computation to establish trust.

Prove outcome is correct given the inputs without revealing any more about the inputs
Evaluator-Prover Model

Alice posts $\text{Com}(\text{buy})$

Bob posts $\text{Com}(\text{sell})$

AU receives orders

Computes trades

Posts trades

Zero-knowledge proof: Prove trades correct given orders without revealing additional info about orders.

Commitments:
- Information-theoretically hiding
- Computationally binding: no $x' \neq x$ s.t. $\text{Com}(x') = \text{Com}(x)$

(1 of 2) Time-Lapse Cryptography

Alice posts $E_{\text{TLC}}[E_{\text{AU}}(x_1)]$

Bob posts $E_{\text{TLC}}[E_{\text{AU}}(x_2)]$

AU receives $x_1, x_2$

Evaluates $z = f(x_1, x_2)$

Posts $z$

Proves correctness.

Want: if AU modifies $x_1, x_2$, or deviates from $f$, then cannot prove correctness, will be caught.

TLC: Time-lapse cryptography service

(Rivest et al.'96, Rabin & Thorpe'06)
(2 of 2) Homomorphic Encryption

• Does not prevent incorrect behavior
• But proofs are sound: will be caught

• Real-time decisions vs proofs

• Applications developed past ~10 years:
  – procurement auctions, clock-proxy auction, CLOB, frequent batch auctions

Example: Blobs
(Kilian’92, Brassard et al. ’88, Rabin et al.’07, ’12)

\[ \mathbf{X}_i = (u_i, v_i) \text{ “blob”, } u_i \in \mathbb{F}_p, \ v_i = x_i - u_i \]

\[ \begin{align*}
  \mathbf{u}_1 &\quad \mathbf{u}_2 \\
  \mathbf{v}_1 &\quad \mathbf{v}_2
\end{align*} \]

\( \mathbf{X}_1 \)
\( \mathbf{X}_2 \)

AU computes \( z = x_1 + x_2 \)
Posts \( z \). Correct iff:
\( u_1 + v_1 + u_2 + v_2 = z \).
Equiv, exists \( w \) s.t.
(\( z = z + w \) (B) \( v_1 + v_2 = -w \))

1. Verifier issues random challenge: “1” or “2”
2. If “1”: AU reveals \( u_1 \) and \( u_2 \); Check (A)
   Similarly if “2”.

Posts \( w \).
Amplification

EP creates box of 300 matches, claims all are good.
V strikes one. Good!
What does V believe?
Take the statement "at least 2/3 are good."
If more than 1/3 bad, then would only pass test 1/3 of time.

Repeat 35x. Now would only falsely pass test at most $(1^3)^{35} < 10^{-6}$ of the time.

Amplification

Input\(^{(1)}\) : \(X_1^{(1)} \ldots X_n^{(1)}\)
\[\vdots \qquad \vdots\]
Input\(^{(K)}\) : \(X_1^{(K)} \ldots X_n^{(K)}\)

1: Post K commitments to same input
2: Post \(z\) and \(w^{(1)}, \ldots, w^{(K)}\).
3. Verifier issue K independent challenges
\[\Rightarrow\] If claim not true, prob. accept proof \(\leq (\frac{1}{2})^K\)
(Also need to prove inputs are equivalent)
Straight-Line Proofs

Dark pool compute the outcome.

Provides on-demand proofs of correctness of trades given orders.

Examples

• Frequent batch auctions (prove sealed-bid, not modified, uniform-price)
  – TLC to hide bids
  – Publish trades, generate proofs that orders correctly ranked and uniform-priced
Examples

• Frequent batch auctions (prove sealed-bid, not modified, uniform-price)
  – TLC to hide bids
  – Publish trades, generate proofs that orders correctly ranked and uniform-priced

• Barclays LX (prove correct in “aggressiveness” labels)
  – Classifier via SLC, prove correct grades associated (without revealing grades)
  – Prove restrictions followed in matching trades

Suggested Application: AdX

- Runs in ~0.2 sec
- Billions each day
- 100’s of bidders
- Google: publisher, advertiser, and AdX

Random representation scheme provides proofs on demand, ~secs to prove.
Conclusion

• Cryptography expands market design space
• Break onfounded between transparency + trust

• Correctly match buyers and sellers without revealing pre-trade order information

• Role for (practical) secrecy-preserving proofs of correctness.
Responses – IEX market

- CLOB
- 350 msec delay on data; 38-mile coil of optical fiber.
- Call-out to other exchanges before HFTs can respond.
- Moving towards a public exchange, displayed orders.

Responses – Freq Batch Auctions
(Budish, Cramton and Shim; Wah and Wellman)

- Clear every ~100 milliseconds
- All orders received during same interval treated as having arrived at same time
- Uniform price double auction, orders displayed at end of interval