On Decentralizing Prediction Markets & Order Books

Jeremy Clark, Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Andrew Miller, & Arvind Narayanan
Remove uncertainty about unknown events
<table>
<thead>
<tr>
<th>Politics</th>
<th>Sports</th>
<th>Weather</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market Share</td>
<td>Geo-politics</td>
<td>Product Completion</td>
</tr>
<tr>
<td>Scientific Discoveries</td>
<td>Sales</td>
<td>Awards</td>
</tr>
</tbody>
</table>
Prediction Markets
Prediction Markets

Obama
Romney
Johnson
Other

Winner: $10
Losers: $0
# Prediction Markets

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Price</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obama</td>
<td>$6.10</td>
<td>61%</td>
</tr>
<tr>
<td>Romney</td>
<td>$3.80</td>
<td>38%</td>
</tr>
<tr>
<td>Johnson</td>
<td>$0.09</td>
<td>0.9%</td>
</tr>
<tr>
<td>Other</td>
<td>$0.01</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

Winner: $10  
Losers: $0
Prediction Markets

Obama $6.10
Romney $3.80
Johnson $0.09
Other $0.01
### Prediction Markets

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obama</td>
<td>$6.10</td>
</tr>
<tr>
<td>Romney</td>
<td>$3.80</td>
</tr>
<tr>
<td>Johnson</td>
<td>$0.09</td>
</tr>
<tr>
<td>Other</td>
<td>$0.01</td>
</tr>
</tbody>
</table>

**Obama** - $6.10
## Prediction Markets

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obama</td>
<td>$6.10</td>
<td>$7.30</td>
</tr>
<tr>
<td>Romney</td>
<td>$3.80</td>
<td>$2.65</td>
</tr>
<tr>
<td>Johnson</td>
<td>$0.09</td>
<td>$0.04</td>
</tr>
<tr>
<td>Other</td>
<td>$0.01</td>
<td>$0.01</td>
</tr>
</tbody>
</table>

**Obama** $-6.10
### Prediction Markets

<table>
<thead>
<tr>
<th>Candidate</th>
<th>First Price</th>
<th>Second Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obama</td>
<td>$6.10</td>
<td>$7.30</td>
</tr>
<tr>
<td>Romney</td>
<td>$3.80</td>
<td>$2.65</td>
</tr>
<tr>
<td>Johnson</td>
<td>$0.09</td>
<td>$0.04</td>
</tr>
<tr>
<td>Other</td>
<td>$0.01</td>
<td>$0.01</td>
</tr>
</tbody>
</table>

- Obama: $6.10 + $7.30
# Prediction Markets

<table>
<thead>
<tr>
<th></th>
<th>Obama</th>
<th>Romney</th>
<th>Johnson</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>$6.10</td>
<td>$3.80</td>
<td>$0.09</td>
<td>$0.01</td>
</tr>
<tr>
<td>Value</td>
<td>$7.30</td>
<td>$2.65</td>
<td>$0.04</td>
<td>$0.01</td>
</tr>
</tbody>
</table>

\[-$6.10 + $7.30 = $1.20\]
Prediction Markets

<table>
<thead>
<tr>
<th></th>
<th>Obama</th>
<th>Romney</th>
<th>Johnson</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta$</td>
<td>$-6.10$</td>
<td>$+7.30$</td>
<td>$0.09$</td>
<td>$0.01$</td>
</tr>
</tbody>
</table>

Immediately Realized

$-6.10 + 7.30 = 1.20$
Prediction Markets

<table>
<thead>
<tr>
<th>Candidate</th>
<th>+6.10</th>
<th>+7.30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obama</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Romney</td>
<td>$3.80</td>
<td>$2.65</td>
</tr>
<tr>
<td>Johnson</td>
<td>$0.09</td>
<td>$0.04</td>
</tr>
<tr>
<td>Other</td>
<td>$0.01</td>
<td>$0.01</td>
</tr>
</tbody>
</table>

-$2.70 = $2.65 + $0.04 + $0.01
## Prediction Markets

<table>
<thead>
<tr>
<th></th>
<th>Obama</th>
<th>Romney</th>
<th>Johnson</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$6.10</td>
<td>$3.80</td>
<td>$0.09</td>
<td>$0.01</td>
</tr>
<tr>
<td>Weighted Average</td>
<td>$7.30</td>
<td>$2.65</td>
<td>$0.04</td>
<td>$0.01</td>
</tr>
<tr>
<td>Prediction</td>
<td>$6.40</td>
<td>$3.53</td>
<td>$0.06</td>
<td>$0.01</td>
</tr>
</tbody>
</table>

Net Loss: -$2.70
## Prediction Markets

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Obama</th>
<th>Romney</th>
<th>Johnson</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$6.10</td>
<td>$3.80</td>
<td>$0.09</td>
<td>$0.01</td>
</tr>
<tr>
<td></td>
<td>$7.30</td>
<td>$2.65</td>
<td>$0.04</td>
<td>$0.01</td>
</tr>
<tr>
<td></td>
<td>$6.40</td>
<td>$3.53</td>
<td>$0.06</td>
<td>$0.01</td>
</tr>
</tbody>
</table>

-\$2.70 + \$3.60 = \$0.90
# Prediction Markets

<table>
<thead>
<tr>
<th></th>
<th>Obama</th>
<th>Romney</th>
<th>Johnson</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prediction</td>
<td>$6.10</td>
<td>$3.80</td>
<td>$0.09</td>
<td>$0.01</td>
</tr>
<tr>
<td>Value</td>
<td>$7.30</td>
<td>$2.65</td>
<td>$0.04</td>
<td>$0.01</td>
</tr>
<tr>
<td>Profit</td>
<td>$6.40</td>
<td>$3.53</td>
<td>$0.06</td>
<td>$0.01</td>
</tr>
</tbody>
</table>

- $2.70
# Prediction Markets

<table>
<thead>
<tr>
<th></th>
<th>Obama</th>
<th>Romney</th>
<th>Johnson</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prediction</td>
<td>$6.10</td>
<td>$3.80</td>
<td>$0.09</td>
<td>$0.01</td>
</tr>
<tr>
<td>Trading</td>
<td>$7.30</td>
<td>$2.65</td>
<td>$0.04</td>
<td>$0.01</td>
</tr>
<tr>
<td>Earnings</td>
<td>$6.40</td>
<td>$3.53</td>
<td>$0.06</td>
<td>$0.01</td>
</tr>
</tbody>
</table>

- $2.70  -$6.40

- Romney
- Johnson
- Other
- Obama
Prediction Markets

<table>
<thead>
<tr>
<th></th>
<th>Romney</th>
<th>Obama</th>
<th>Romney</th>
<th>Obama</th>
<th>Romney</th>
<th>Obama</th>
</tr>
</thead>
<tbody>
<tr>
<td>Johnson</td>
<td>$0.09</td>
<td>$0.04</td>
<td>$0.06</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>$0.01</td>
<td>$0.01</td>
<td>$0.01</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

-$2.70 -$6.40 +$10.00 = $0.90
Decentralization
Decentralization

Centralized Market:
• Money escrowed
• Shares escrowed
• Proprietary markets
• Match orders
• Vendor lock-in
• Adjudicate outcome
• Go offline
• Potentially transparent
• High fees

Decentralized Market:
• Hold your own money
• Hold your own shares
• Choose any market
• Open order matching
• Use any exchange
• Trust agility
• Fault tolerant
• Transparent by design
• Low fees
Decentralization

Centralized Market:
• Money escrowed
• Shares escrowed
• Popular markets
• Match orders
• Exchange lock-in
• Adjudicate outcome
• Easily disrupted
• Transparent by choice
• High fees

Decentralized Market:
• Hold your own money
• Hold your own shares
• Choose any market
• Open order matching
• Use any exchange
• Trust agility
• Fault tolerant
• Transparent by design
• Low fees
Decentralization

Bitcoin
Bitcoin

$K_A$  $K_B$
**Bitcoin**

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>K</td>
<td>K</td>
<td>10 BTC</td>
</tr>
<tr>
<td>K</td>
<td>K</td>
<td>5 BTC</td>
</tr>
<tr>
<td>K</td>
<td>K</td>
<td>18 BTC</td>
</tr>
</tbody>
</table>

Ledger

K_A

K_B
Bitcoin

\( K_A \xrightarrow{\text{Sig}_A(5 \text{ BTC})} K_B \)

Ledger

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>K</td>
<td>K</td>
<td>10 BTC</td>
</tr>
<tr>
<td>K</td>
<td>K</td>
<td>5 BTC</td>
</tr>
<tr>
<td>K</td>
<td>K</td>
<td>18 BTC</td>
</tr>
<tr>
<td>K</td>
<td>K</td>
<td>5 BTC</td>
</tr>
</tbody>
</table>
Design Decisions

Underlying digital currency & block chain
- Extend Bitcoin
- Altcoin (XFT)
- Colored Coins
Design Decisions

How to Declare a Winner:
• Machine-readable feed
• Trusted (human) arbiter
• Miners vote
• Users vote
Design Decisions

How to Declare a Winner:
- Machine-readable feed
- Trusted (human) arbiter
- Miners vote
- Users vote

Threats:
- Wrong decision -> profitable
- No decision -> DoS
Design Decisions

How to Declare a Winner:
- Machine-readable feed
- Trusted (human) arbiter
- Miners vote
- Users vote

Arbiters:
- Choose who you trust (agility)
- Low barrier to entry
- History & external reputation
- Trustworthiness built into price
Design

New Operations (Simplified)

- OpenMarket() Description & Arbiter, signed by arbiter
- CloseMarket() Outcome, signed by arbiter
Design

New Operations (Simplified)

- **OpenMarket()** Description & Arbiter, signed by arbiter
- **CloseMarket()** Outcome, signed by arbiter

- **BuyPortfolio()** Convert 1 XFT into complete set of shares, signed by currency holder
- **SellPortfolio()** Convert complete set for 1 XFT, signed by share holder
Design

New Operations (Simplified)

- **OpenMarket()** Description & Arbiter, signed by arbiter
- **CloseMarket()** Outcome, signed by arbiter

- **BuyPortfolio()** Convert 1 XFT into complete set of shares, signed by currency holder
- **SellPortfolio()** Convert complete set for 1 XFT, signed by share holder

- **Exchange()** Exchange shares for XFT between two parties, signed by both parties
Design

Transaction: T9238

In-1: {5 XFT, (T_{3829:Out-2})}

In-2: {10 M_{ID:S_{ID}}, (T_{4950:Out-1})}

In-3: {4 XFT = 2 M_{ID:S_{ID}}, (T_{6743:Out-1}), (T_{CloseMarket})}

Out-1: {6 XFT, K_{Out-1}}

Out-2: {2.9990 XFT, K_{Out-2}}

Out-3: {10 M_{ID:S_{ID}}, K_{Out-3}}

Sign_{In-1}, Sign_{In-2}, Sign_{In-3}

Payment
Change
Shares
Order Book

Most common: continuous, price-time priority

Broadcast orders to Bitcoin-style network:

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders
Order Book

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders

The best we can + support external exchanges
Order Book

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders

Broadcast to all known neighbours
Order Book

• Nodes drop competitive orders
• No way to establish time
• Blockchain: updated in batches
• Miners drop competitive orders
• Miners front-run well-priced orders

Call Market: Market opens, orders pile up, randomly close market, match orders

Matching: Lowest ask matched to highest bid until no more matching possible
Order Book

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders

Miners keep spread: spreads can replace fees & miners can execute at best price (added perk)
Discussion

Design landscape, not a specific proposal

Regulatory issues: not attempting regulatory avoidance

Platform for other financial exchanges

Not suitable for forecasts about underlying currency
Questions?

@PulpSpy
@josephbonneau
@EdFelten
@realjoshkroll
@socrates1024
@random_walker