Truthcoin
Blockchain Prediction Markets

“Outcomes”
v2 – 10/15/2014
Paul Sztorc
This Presentation

Applications

Outcomes

Trading

Bitcoin
Talk Outline – 26 Slides

1. The Outcome Problem (Slides 4 – 8)
   1. The Goal, stated clearly.
   2. Competing Arbiters? Not even close to good enough.
   3. The Assumption.

2. How can we do better? (Slides 9 – 13)
   1. Consistency – brought to you by SVD.
   2. Reputation – brought to you by financial econ.

3. Truthcoin Overview (14-19)
   1. The Big Graphic.
   2. Scalability via “Branching”.
   3. The 51% ownership attack.

4. Going Beyond (19-26)
   1. Auditing Branches (Two-Wave SVD)
   2. Vetoing Bad Votes
   3. Semi-Trusted “Branch Insurance”
The Outcome Problem

• **Goal:** Guarantee to Traders that their ‘event derivatives’ will eventually be worth their promised value.

• **Resources:**
  – Reports from users, aggregated (“votes”).
  – Some $ to pay the reporters (“voters”).

• **Problems:**
  – Completely self-determined (reliable data must be only a function of the reports). Decentralization = no “special users”.
  – Laziness: (No one will vote unless they have to).
  – ‘Virtual Voters’ likely pseudonymous, can’t be sued, shamed, or whacked. No 9 month waiting period.

• **Special Problems:**
  – Half of all trades will be ‘losers’: these traders have an inherent reason-to-lie.
  – “Retiring users” have an inherent reason-to-lie.
Existing Proposal (Which Won’t Work): Competing Arbiters / Price-Feed-Providers

1. Some **user assumes role of ‘arbiter’** (may pay registration fee, ‘fidelity bond’, or may be free, may involve off-chain marketing/legal ...).
2. Arbiters collect **fees on an ongoing basis** per judgment, resolution, audit, or per day, feed, subscriber, etc.
3. Trader can choose arbiter: competitive marketplace provides **incentive to keep good reputation**. “Bad” agent = no longer chosen = **loses ongoing fees**.

(I don’t own these images).
The Competing Arbiters Assumption

1: Attack Payoff Today

<table>
<thead>
<tr>
<th>Conform</th>
<th>Attack</th>
<th>TIME</th>
<th>+ 1 Day</th>
<th>+ 2 Days</th>
<th>+ 3 Days</th>
<th>+ 4 Days</th>
<th>+ 5 Days</th>
<th>+ 6 Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>$</td>
<td>Today</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2: Payoffs in Future

The Competing Arbiters Assumption

3: Time-Discounting
(NPV "Funnel", Concern for the future)

The Outcome

- **Goal:** Guarantee to Track will eventually be worth
### Triple Uncertainty

<table>
<thead>
<tr>
<th>• The <strong>Attack Payoff Today</strong> (we want low) can skyrocket:</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ As a <em>market becomes unexpectedly popular</em>.</td>
</tr>
<tr>
<td>▪ Marketing / Hedged-”Chandelier Trades” by Arbiters themselves.</td>
</tr>
<tr>
<td>▪ No reliable way of estimating market’s future popularity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>• The <strong>Future Payoffs</strong> (we want high) can collapse on news/<em>rumors</em> :</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ About <em>judge-industry-competitiveness</em> (more people joining the industry, higher-quality offerings). Econ theory -&gt; “No Rent”.</td>
</tr>
<tr>
<td>▪ About the <em>future of the protocol</em> (more popular alternative coming out, critical vulnerability found).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>• The <strong>arbiter’s concern for the future</strong> (we want high) can decrease:</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ With capricious Arbiter preferences (we cannot guarantee to Traders that Arbiters have psychologically stable preferences).</td>
</tr>
<tr>
<td>▪ Arbiter hacked / faux-hacked / diagnosed with terminal illness.</td>
</tr>
<tr>
<td>▪ With Arbiter <em>retirement-plans</em> (“I’ve been doing this for a while, and I just don’t want to do it anymore”). Arbiter dies -&gt; ?</td>
</tr>
</tbody>
</table>
Will anything work?

Don’t be discouraged...
...real people do it all the time!

• Our reality is completely self-determined.

• And real people are:
  – Liars who constantly misrepresent themselves.
  – Hypocrites who aren’t self-aware enough to have a reputation to lose (politicians: no shame).
  – Lazy (not voting on important things unless they have to). Threshold for “public consciousness”.

• Yet, we still think we “know” some facts (“Was Mitt Romney elected president in 2012?”, ‘Google-able’ facts)

• Notice: After the fact = Much easier.
How Do We Do It?

- Experience “reports” on many things from many people in real-time (‘Ballot’).
- Constantly evaluate logical consistency of the person.
Singular Value Decomposition

- [http://www.youtube.com/watch?v=pAiVb7gWUrM](http://www.youtube.com/watch?v=pAiVb7gWUrM)
- Point = Build **index of disagreement** with an abstract ‘most-representative ballot’ (not known in advance to any single voter). Continuous.

![Original image](http://www8.tfe.umu.se/courses/systemteknik/Media_signal_processing/04/presentations/MSP_P3-3.pdf)

- [http://www8.tfe.umu.se/courses/systemteknik/Media_signal_processing/04/presentations/MSP_P3-3.pdf](http://www8.tfe.umu.se/courses/systemteknik/Media_signal_processing/04/presentations/MSP_P3-3.pdf)
Example 2:

<table>
<thead>
<tr>
<th></th>
<th>D1</th>
<th>D2</th>
<th>D3</th>
<th>D4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voter 1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Voter 2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Voter 3</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Voter 4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Voter 5</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Voter 6</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

As others disagree with you, you benefit (up to a point)!

Result: Cannot trust rival voters...no cartels or “voting pools”.
Consistency #2: Time

After someone lets you down, then stop trusting them!

(Reputation)
How to ‘tie’ people to a permanent reputation (as they are so-tied in real life)?

• **Allow** them to become owners in an abstract corporation.
  – Must ‘buy in’ (prevents Sybil attacks).
  – Positive selection effect (only those who want to do this can buy).
  – Financial Asset
    » No ‘retirement attack’ (retirees can simply sell).
    » All users earn dividends on all future resolutions.

• **Penalize** bad behavior by reducing ownership.
  – Non-conformity (measured via SVD-consensus)
  – Laziness (failure to vote on-time, every-time).
Truthcoin Graphic: Two Coin Types

Owners ("Reputation")

Branches

Decisions

Markets

Owners ("Cash") ("Bitcoin")

Trades

Authorship
Scalability = “Branching”

Free Option to own future branches:
- Trust / Network Effect
- Uniqueness (consensus & digital scarcity)
The 51% Voter-Attack is Much Harder

1. **YOU (individually) need 50%** (a mere “coalition of >50%” will not work, as you can’t trust them).

2. Now you must ‘buy up’ **the marketcap** of the entire Branch (not just pay off one person).
   1. Requires additional investment (**all of which is lost** post-attack).
   2. Opportunity cost of attack is tied to the profitability of the Branch (previously, lots of ‘luck’ re: gaining rep, chancing to referee a popular market).

3. Attackers **LOSE** the reputation you bought (**ie the opportunity cost of selling**).
   1. Previously, you lost only your established reputation.
   2. Previously, your ‘investment’ was low.
   3. Strong resistance to the (otherwise fatal) “exit scam”.

18
What if an Attack exceeds Conform and someone buys up >51% of the VoteCoins?

Could execute same ‘lie attack’, only worse (51/100th cheaper)!

To SVD, we add:

[1] Audit

- Real-World Logic: When people can’t agree on something, they do not go with “51%”, instead they say something like “we really aren’t sure”.

- “Two Wave SVD”

Wave One: Catches largest outliers immediately (preserves every incentive we just described).

Wave Two: On all the ‘Certain Decisions’ which survived Round 1.

The Uncertain Decisions become “Auditable”.

Branch Parameters include a ‘Certainty Threshold’ ($\phi=80\%$ here).
1. Per **Audit Period** (6 Months or so), anyone can cast a vote with their available cash (cash not invested in a market).

2. These votes are on the top 5 most representative Ballots from each ‘Auditable Ballot’ (not on the Auditable Decisions themselves, this substantially reduces the workload of the auditors).


4. You always get your cash back (no penalty for not voting).

5. Winners in SVD get the half Trading Fees for that round (the other half go to the winning Branch VTC owners), proportional to their agreement (as usual).

**Result:** By ‘sticking it out’, an honest minority of Voters can earn a superior return (50% instead of <50% [by definition, they are a minority]).

• So far, we have a situation where:
  – Voters would like to collaborate and attack, but fear being double-crossed by double-agent Voters.
  – Honest Voters have recourse for ‘sticking it out’ (not only overall, but especially on a Decision-by-Decision basis).
  – Therefore, Voters are unlikely to trust each others (even if they can prove they are a majority).

• Let’s **amplify** Voter mistrust by making life **even more inconvenient** for liar-Voters, by using a Miner Veto.
Preventing the $\phi$ Attack

- **50% “Ballot Veto”**
  - Ballot / Audit Ignored
  - Try again next period
  - (Miners can already hard-fork, this is simply a failsafe).

- **(And/Or) 95% “Branch-Veto”**
  - Branch’s future Decisions can be moved to a different Branch (by their Author).
**[3] Miner Override**

- We need to stop anyone from owing **51%** of something... *sound familiar?*
- Outsource the task of Voting completely to Miners.
- High instability, extra special effort required, but Miners should always find it to be worthwhile, even profitable. (Comparable to reacting to a software bug / hard fork).
- Costs everyone big...attackers most of all.

<table>
<thead>
<tr>
<th>Source of Forecast-Correction</th>
<th>Network Capacity</th>
<th>Expected Throughput (Usage)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traders</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Voters</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Auditors</td>
<td>Very Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>Miners</td>
<td>Extremely Low</td>
<td>Extremely Low</td>
</tr>
</tbody>
</table>
Truthcoin Graphic: Two Coin Types

Owners
("Reputation")

Branches

Decisions

Markets

Owners ("Cash")
("Bitcoin")

Thank You!