Truthcoin

Blockchain Prediction Markets

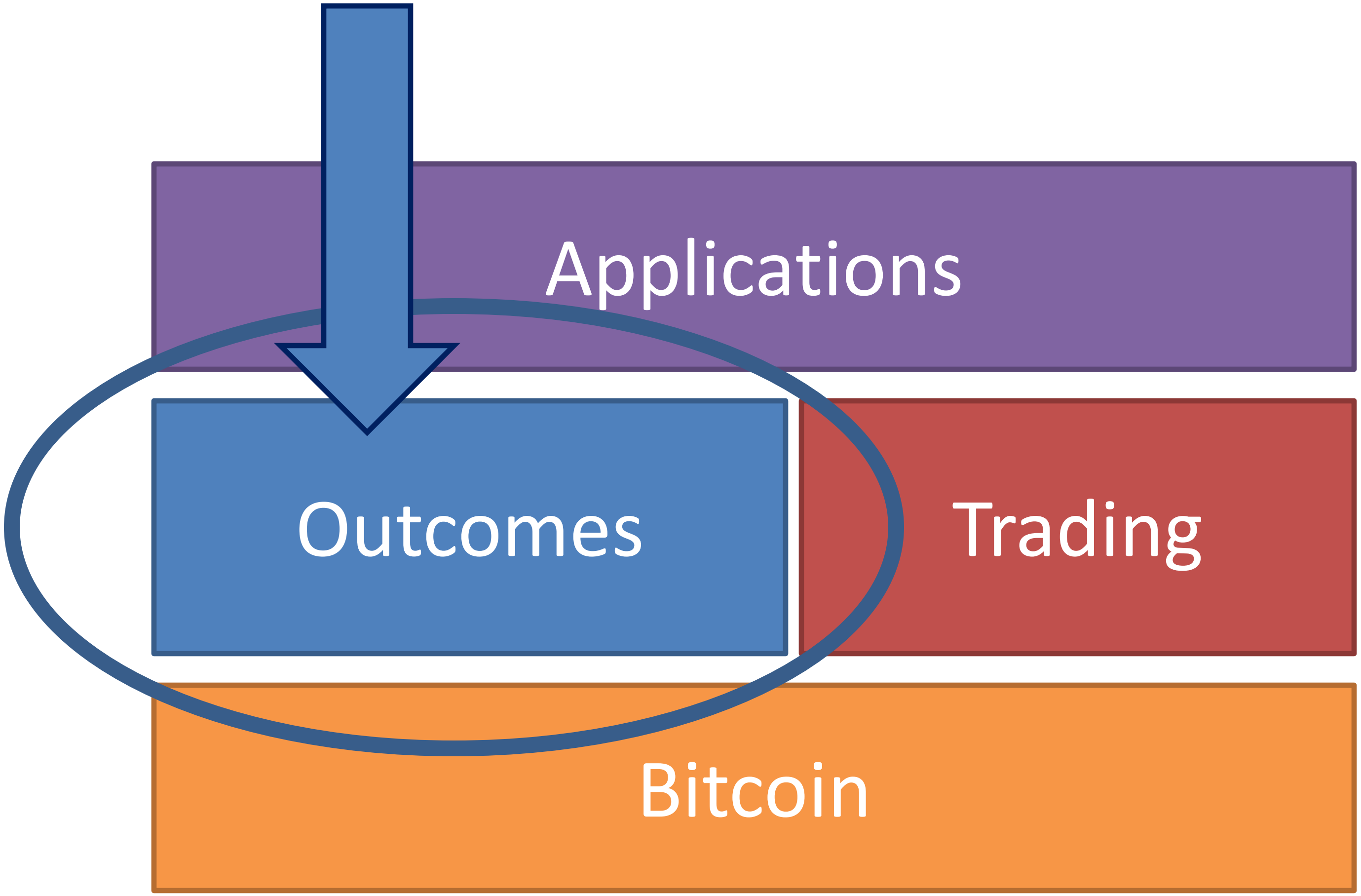
“Outcomes”

v1 – 9/8/2014

Paul Sztorc

Yale Economics Department

This Presentation



Applications

Outcomes

Trading

Bitcoin

Talk Outline – 19 Slides

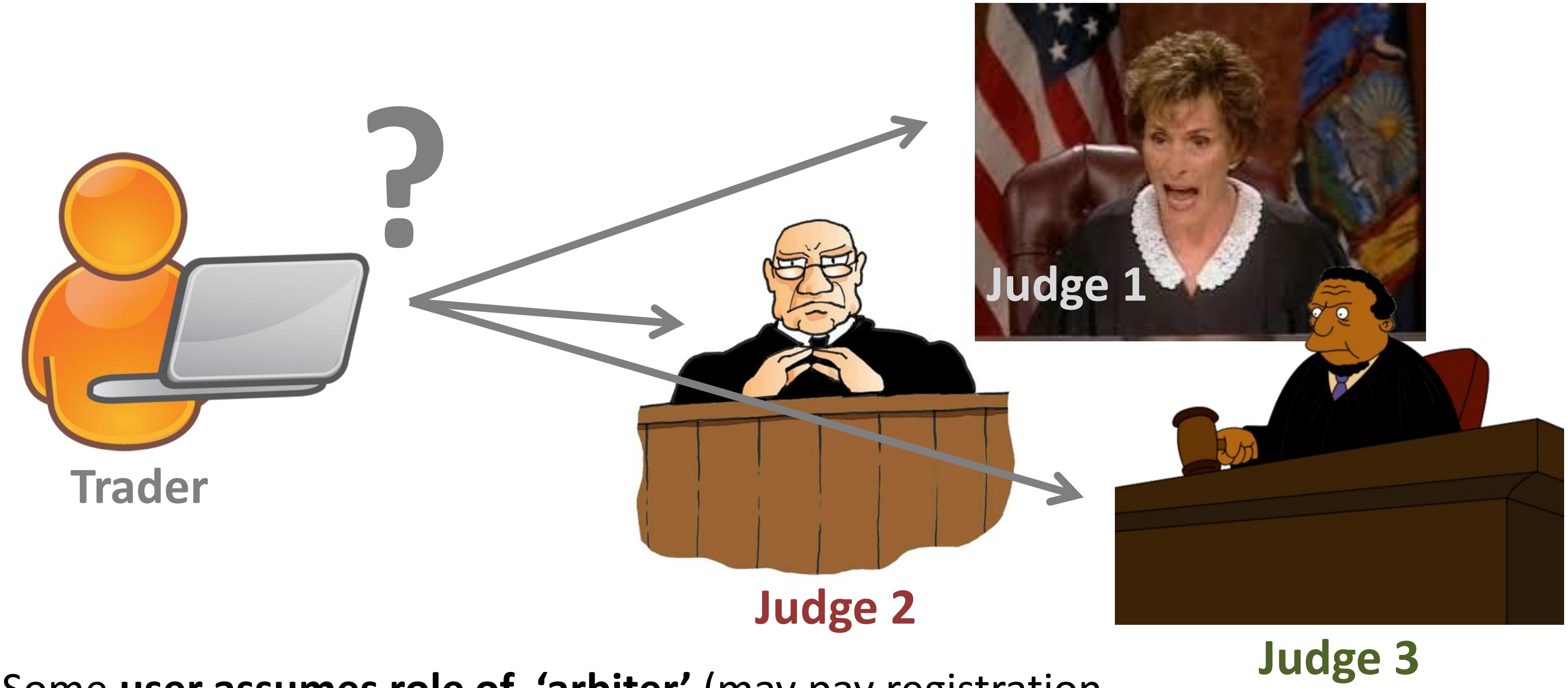
1. The Outcome Problem (Slides 4 – 8)
   1. The Goal, stated clearly.
   2. Competing Arbiters? Not convincing.
   3. The Assumption.
2. Can we do better? (Slides 9 – 13)
   1. Consistency – brought to you by SVD.
   2. Reputation – brought to you by financial econ.
3. Truthcoin Overview (14-19)
   1. The Big Graphic.
   2. Scalability via "Branching".
   3. The 51% ownership attack.

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.
  - “The Powers That Be” / Crazy “Joker” types.

What won’t work:

Competing Arbiters / Price-Feed-Providers



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

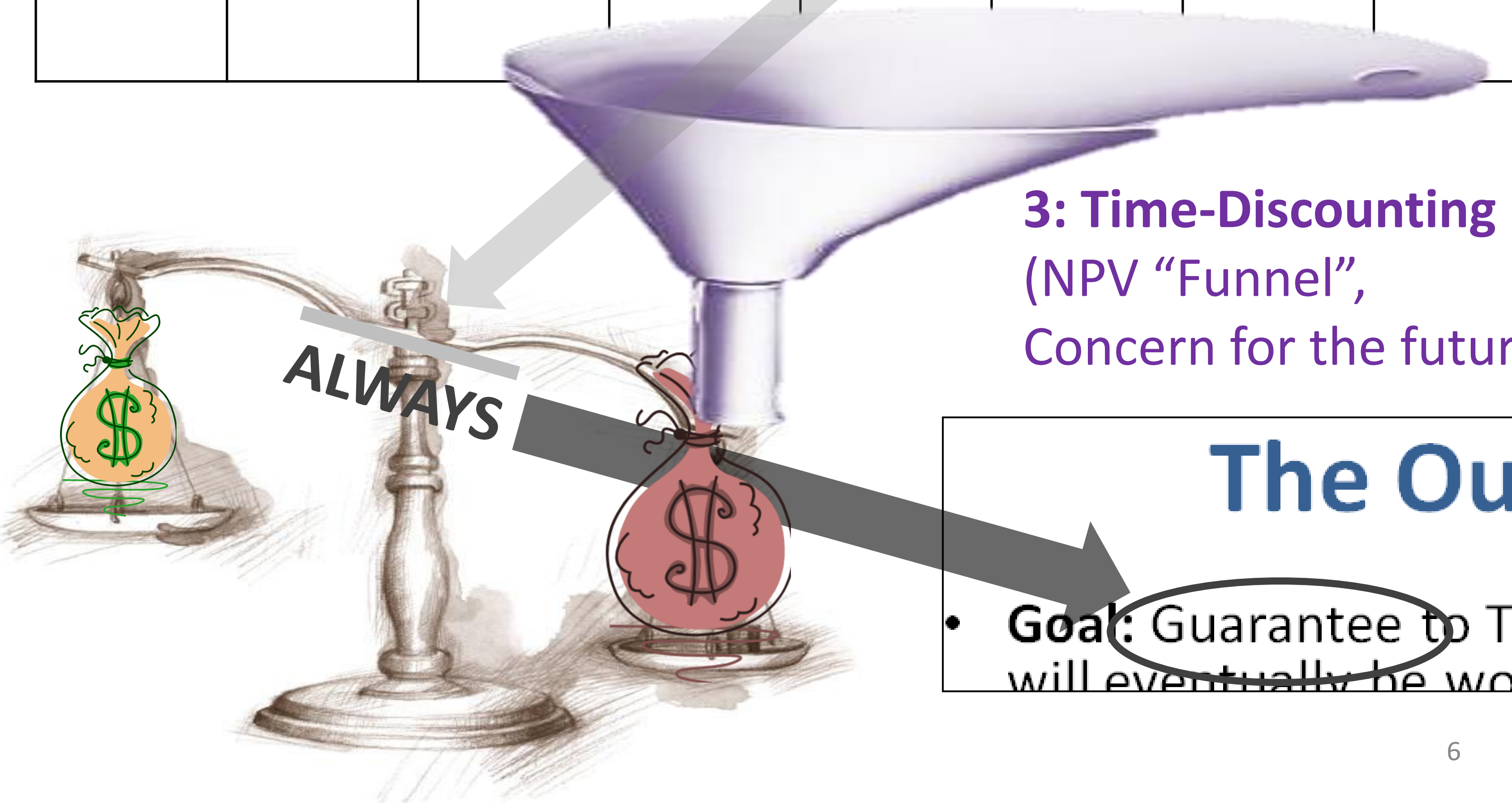
(I don’t own these images).

The Competing Arbiters Assumption

1: Attack Payoff Today

2: Payoffs in Future

Conform		💰	💰	💰	💰	💰	💰
Attack	💰						
TIME	Today	+ 1 Day	+ 2 Days	+ 3 Days	+ 4 Days	+ 5 Days	+ 6 Days

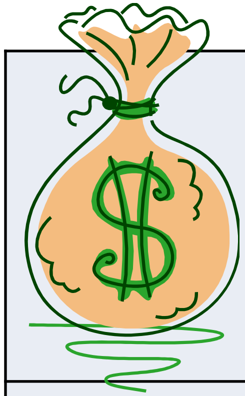


3: Time-Discounting
(NPV “Funnel”,
Concern for the future)

The Out

- **Goal:** Guarantee to Tra
will eventually be wort

Triple Uncertainty



- The **Attack Payoff Today** (we want low) can skyrocket:
  - As a **market becomes unexpectedly popular**.
  - Marketing / Hedged-"Chandelier Trades" by Arbiters themselves.
- No reliable way of estimating market's future popularity.

- The **Future Payoffs** (we want high) can collapse on news/**rumors** :
  - About **judge-industry-competitiveness** (more people joining the industry, higher-quality offerings). Econ theory -> "No Rent".
  - About the **future of the protocol** (more popular alternative coming out, critical vulnerability found).

- The **arbiter's concern for the future** (we want high) can decrease:
  - With capricious Arbiter preferences (we cannot guarantee to Traders that Arbiters have psychologically stable preferences).
  - Arbiter hacked / faux-hacked / diagnosed with terminal illness.
  - With Arbiter retirement-plans ("I've been doing this for a while, and I just don't want to do it anymore"). Arbiter dies -> ?

Will anything work?

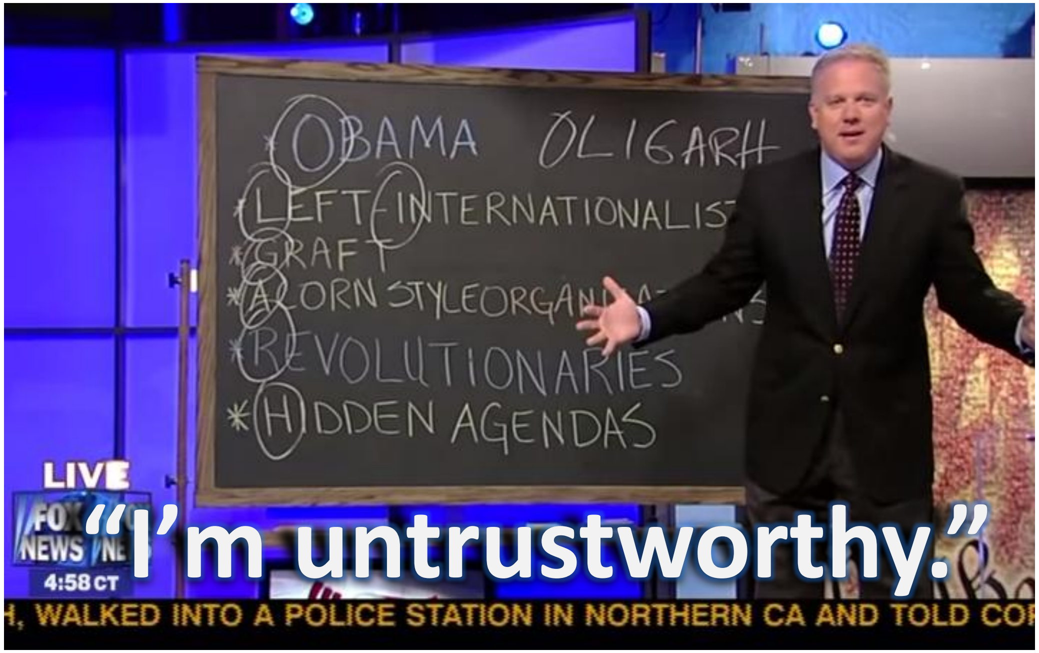
Don’t be discouraged…

…real people do it all the time!

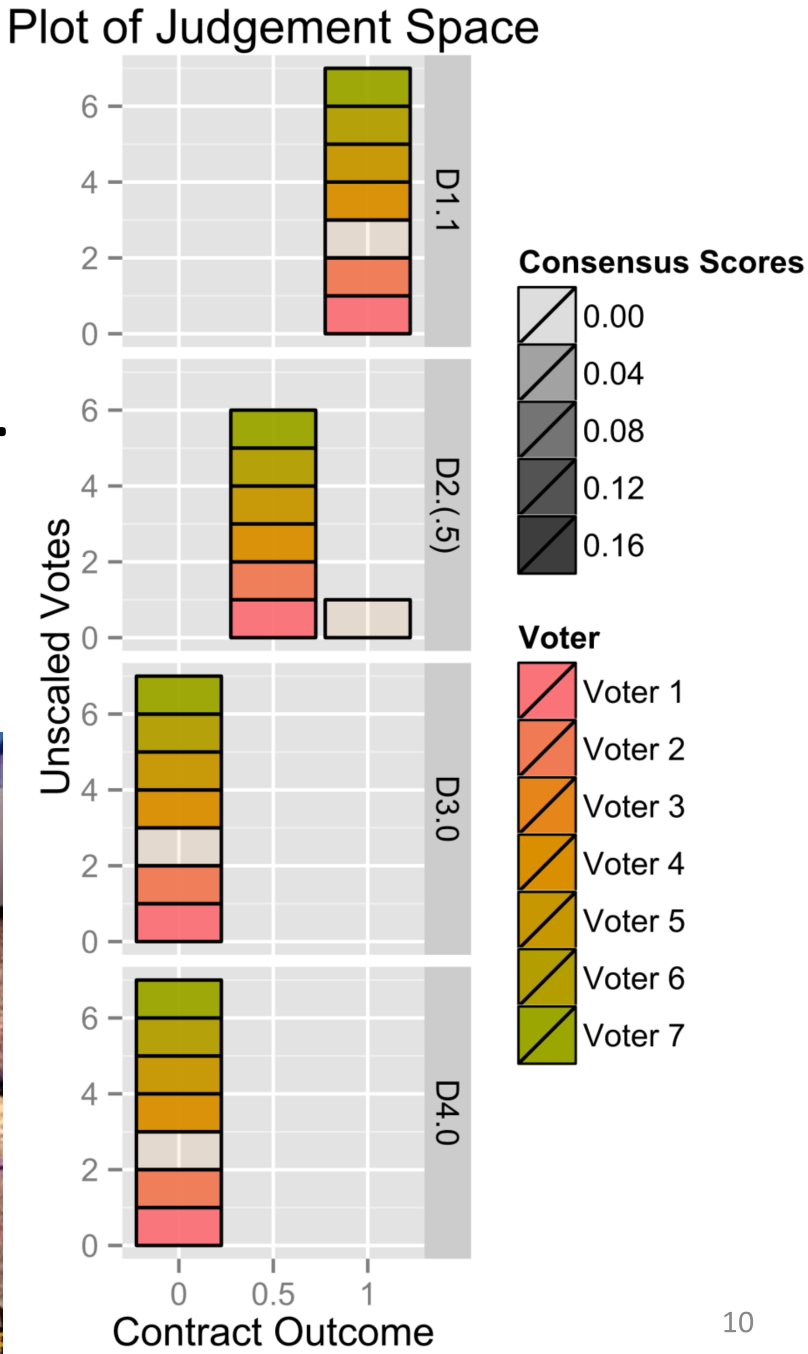
- Our reality is completely **self-determined**.
- And real people are:
  - **Liars** who constantly misrepresent themselves.
  - **Hypocrites** who aren’t self-aware enough to have a reputation to lose (politicians: no shame).
  - **Lazy** (not voting on important things unless they have to). Threshold 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 **<u>many things</u>** from **<u>many people</u>** in real-time (‘Ballot’).
- Constantly evaluate logical consistency **<u>of the person</u>**.

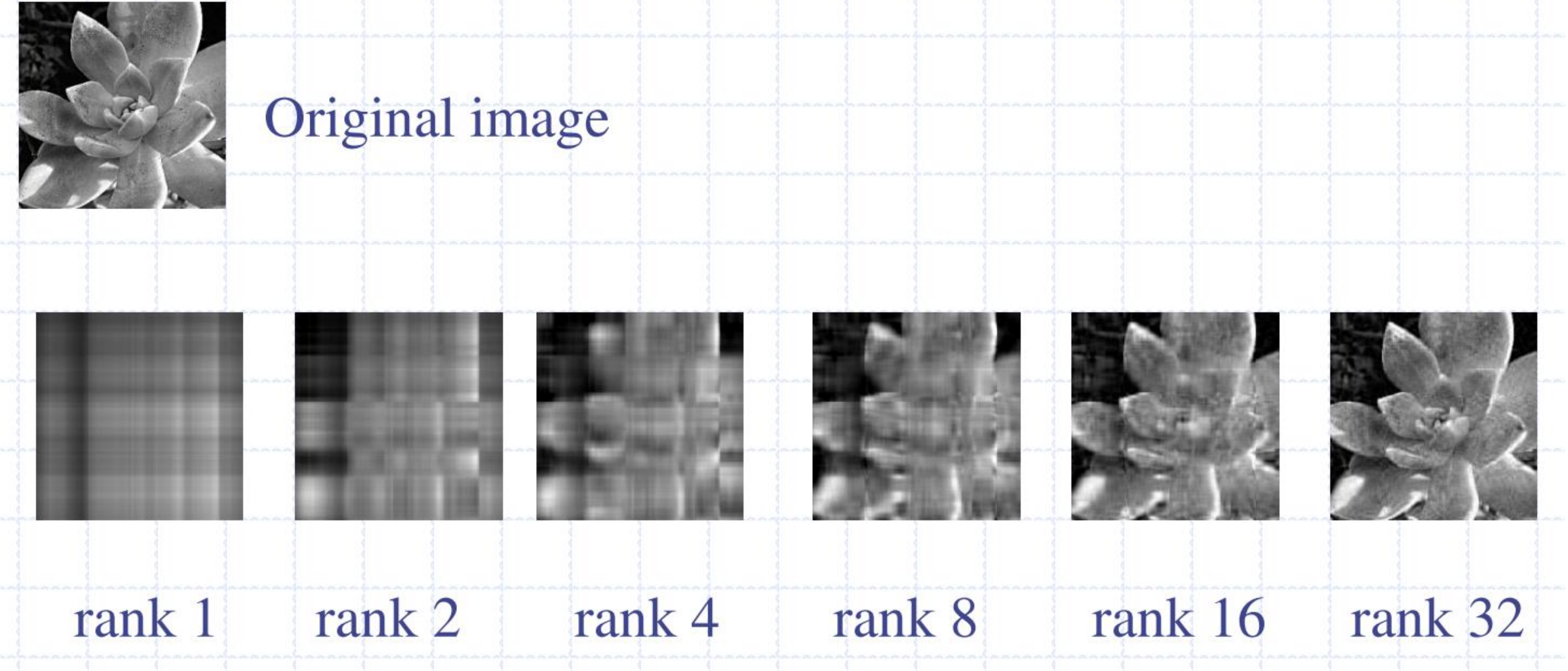


“I’m untrustworthy.”



Singular Value Decomposition

- 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). Cotinuous.

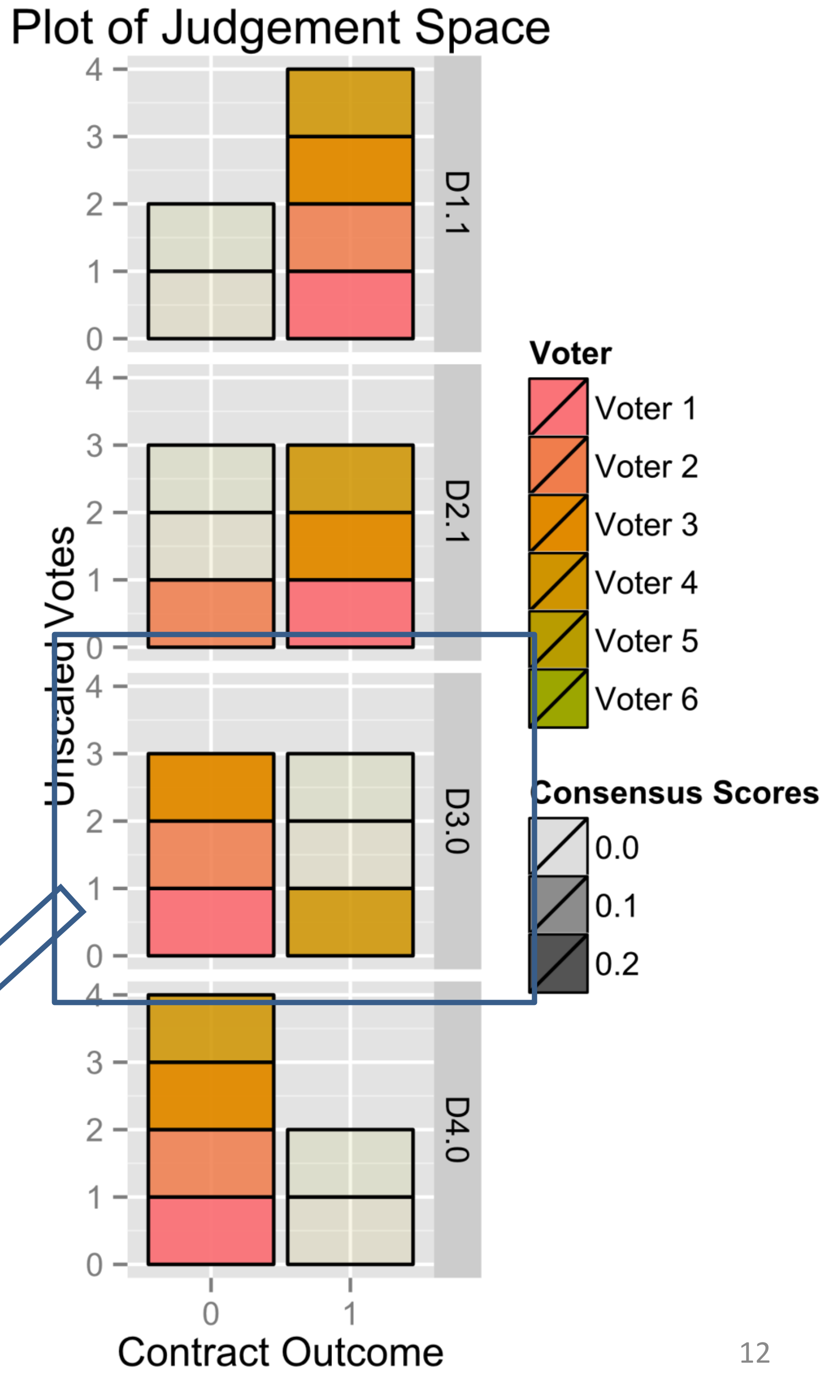


- http://www8.tfe.umu.se/courses/systemteknik/Media_signal_processing/04/presentations/MSP_P3-3.pdf

Example 2:

	D1	D2	D3	D4
Voter 1	1	1	0	0
Voter 2	1	0	0	0
Voter 3	1	1	0	0
Voter 4	1	1	1	0
Voter 5	0	0	1	1
Voter 6	0	0	1	1
Total	**4 - 2**	**3 - 3**	**3 - 3**	**2 - 4**

Demo:
http://forum.truthcoin.info/index.php/topic,134.0.html



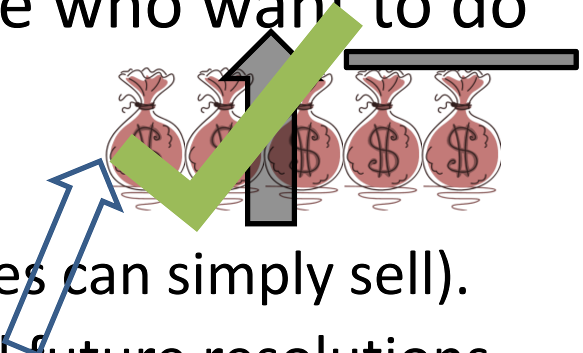
Consistency #2: Reputation

After someone lets you down, then stop trusting them!

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
MAD MAIL
Should I be worried about Bear Stearns (BSC) in terms of liquidity and get my money out of there?

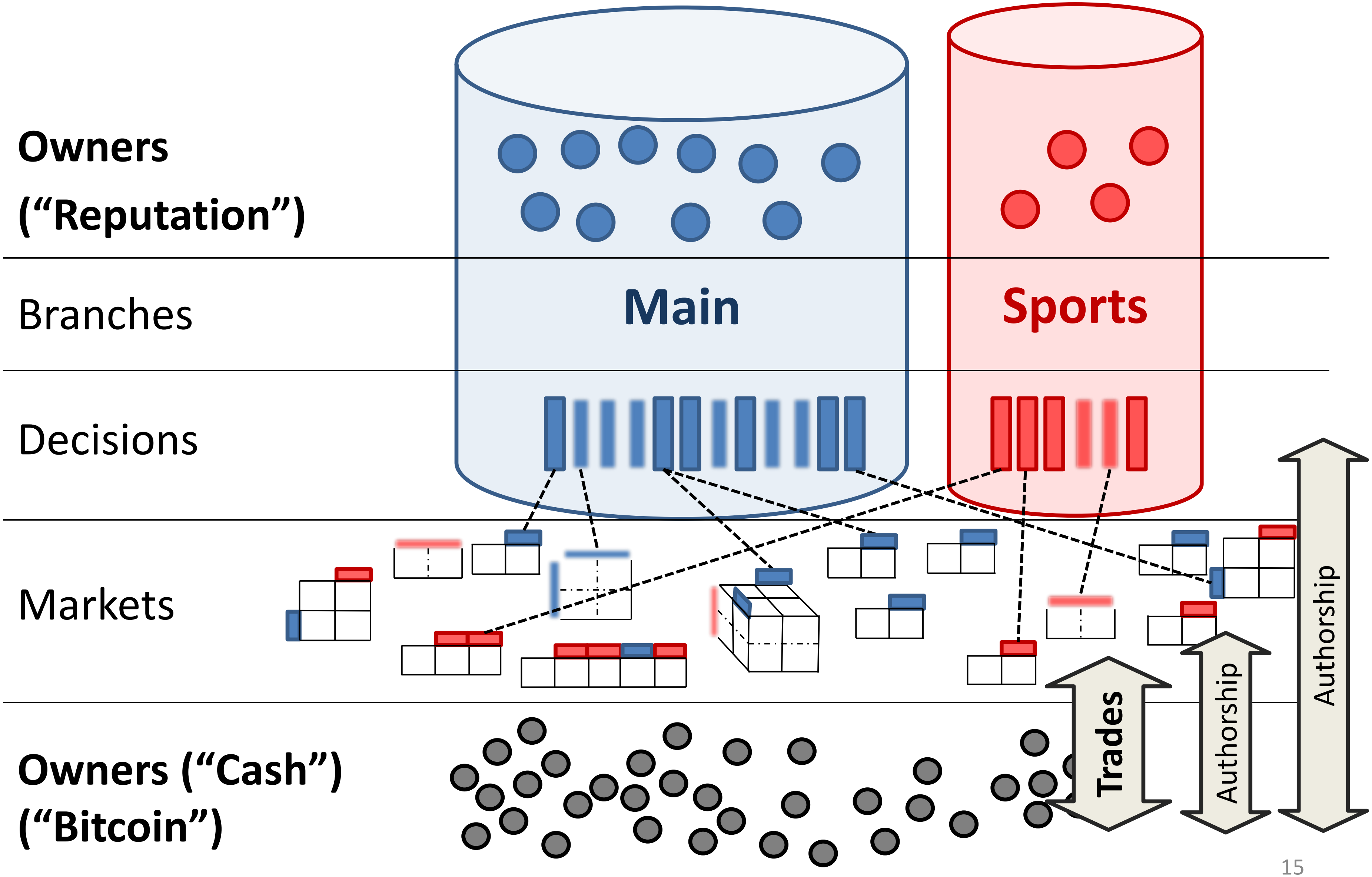
How to ‘tie’ people to a permanent reputation (as they are so-tied in real life)?

- **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”)

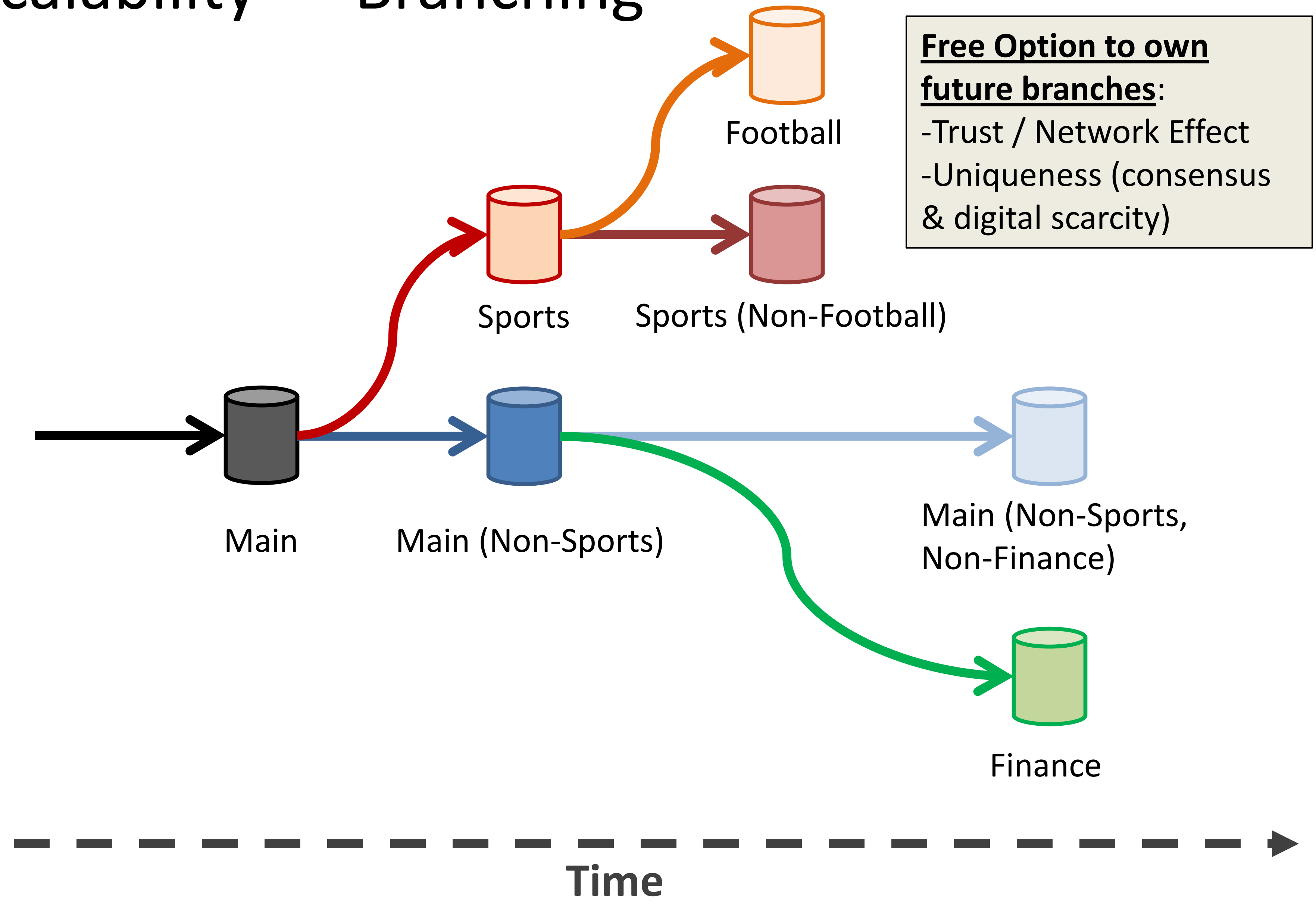
Branches

Decisions

Markets

Owners (“Cash”) (“Bitcoin”)

Scalability = “Branching”



Free Option to own future branches:
-Trust / Network Effect
-Uniqueness (consensus & digital scarcity)

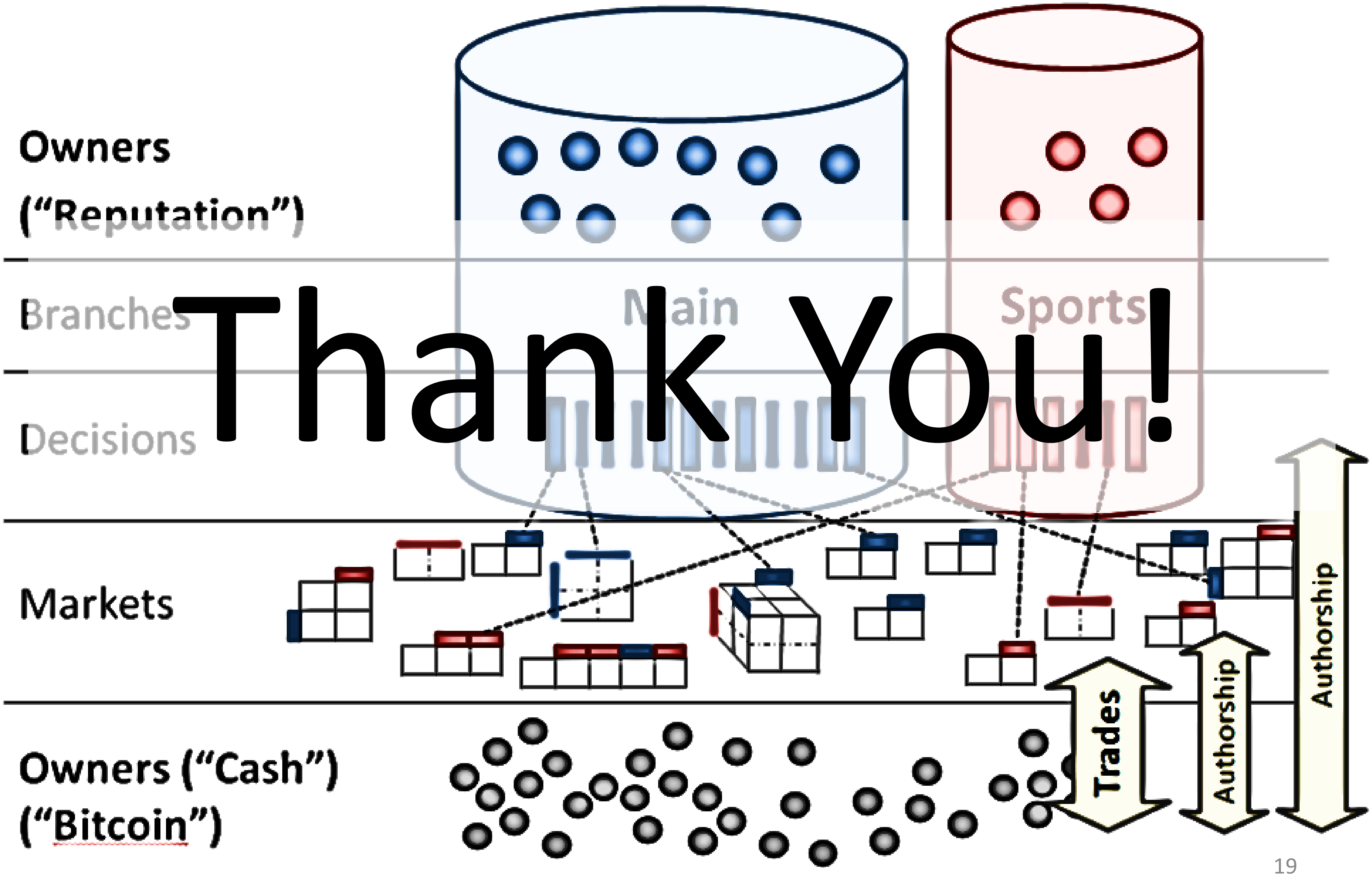
The 51% Voter-Attack

- The trick of this scheme is:
  - **YOU** really need 50% (“a coalition of >50%” won’t work, as you can’t trust them).
  - Now you must ‘buy up’ the marketcap of the entire branch, not just one market.
    - Lots of additional investment – all of which is lost post-attack.
    - Opportunity cost of attack is tied to the profitability of the network (previously, lots of ‘luck’ re: gaining rep, refereeing a popular market).
  - Now you LOSE the reputation you bought (ie the value of ALL the future markets, op. cost of selling).
    - Previously, you lost only your established reputation.
    - Previously, your ‘investment’ was low.

Current Status / Plans

- See forum.truthcoin.info, github.com/psztorc/Truthcoin
- Currently **no** organization / investors / foundation.
- Currently **are** several “volunteer-versions”, each with pros/cons, at various states of being.
- Release these versions for testing.
- Wait for sidechains/treechains (?).
  - …or *replace Bitcoin* *gasp*?
- Preserve ownership of the ‘VoteCoins’
  - value-add.
  - network-effect.
  - valuable-component.
  - Give ‘CashCoins’ to Bitcoin users to preserve econ network.

Truthcoin Graphic: Two Coin Types



Owners ("Reputation")

Branches

Decisions

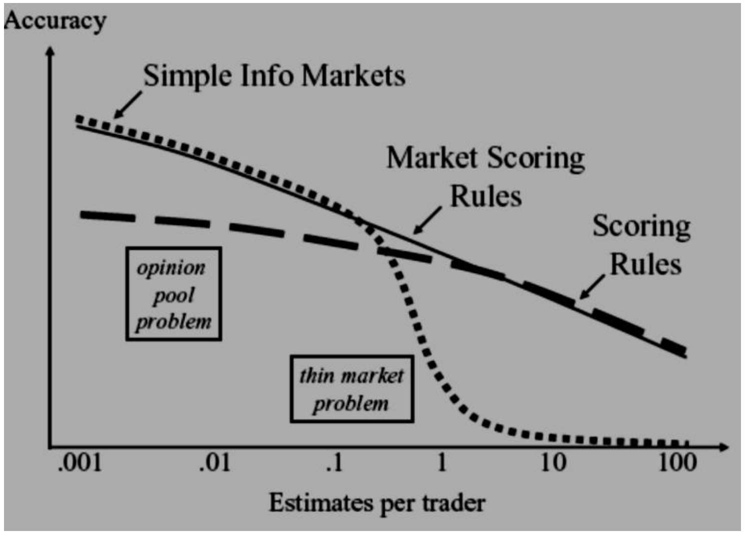
Markets

Owners ("Cash") ("Bitcoin")

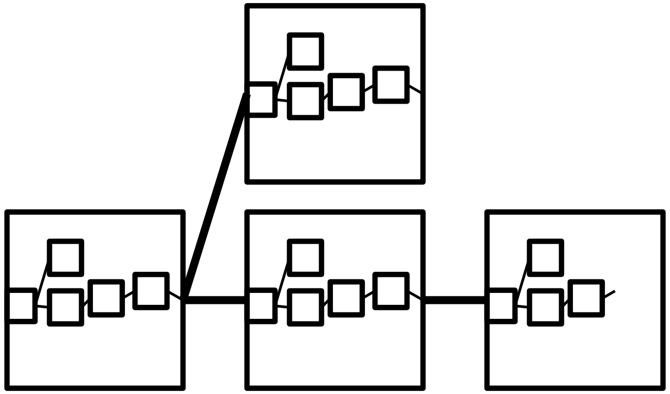
Thank You!

The Trading Slide

- Permanent Liquidity – Market Scoring Rules
  - No order books needed
  - Only one trader / trade needed.
  - One tx (“signed update”)



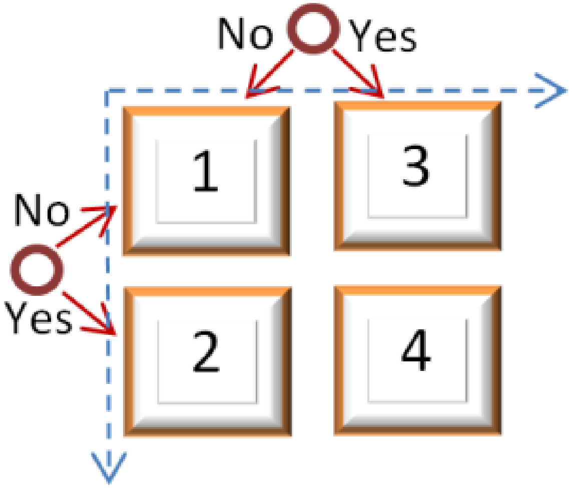
- Info Prize (donations)



- Trading at near-instant speed (within 10-minute blocks)

The Applications Slide

- Multidimensional Markets
  - Optimal Advice (“futarchy”)
  - Boost econ growth (CEOs)
  - Financing Public Goods



- Smart Contracts
  - (With Selling Disabled) = “Lockbox”
  - Public Goods without Coercion (T-DAC)
  - Focus On: the result, not the computation.