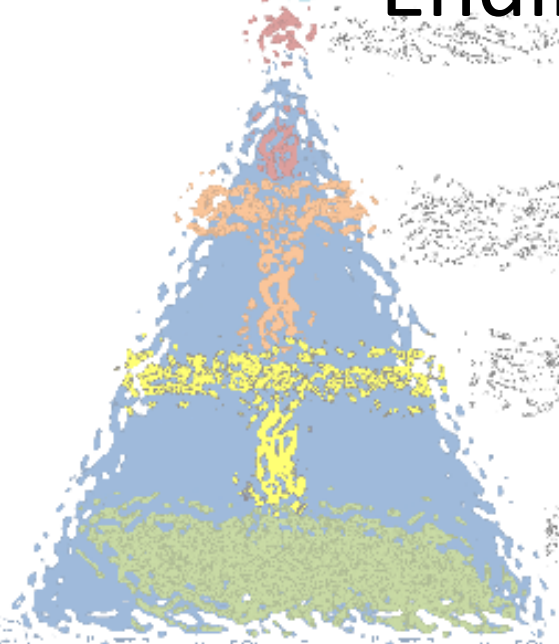
Introduction to Truthcoin

Prediction Markets for Bitcoin

"Ending the Age of Bullshit"



MIT Bitcoin Club

Jan 20th, 2015

Paul Sztorc

Agenda

1. Intro
2. Prediction-Market Hype / What Truthcoin Does
3. How Truthcoin Works*
4. *Questions

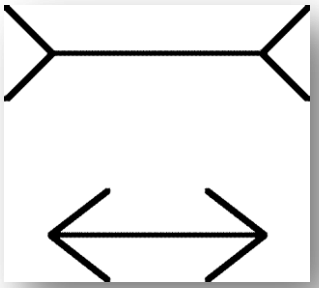
Presentation Goals: That you…

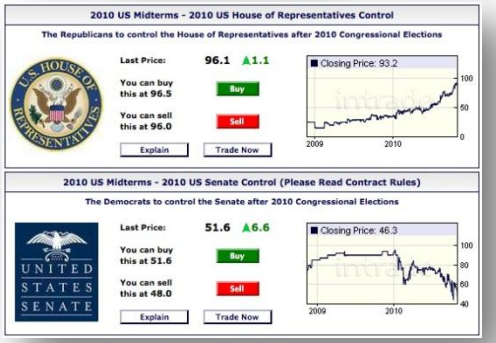
1. …**get excited** for upcoming software release.
2. …impress your friends by already knowing about this, when it comes out.
3. Join the forum (http://forum.truthcoin.info), read, ask questions, discuss, hang out.

Note: Will be a Bitcoin-sidechain, to use the features of this, you only need to buy anything or invest in anything else.

Who / Why

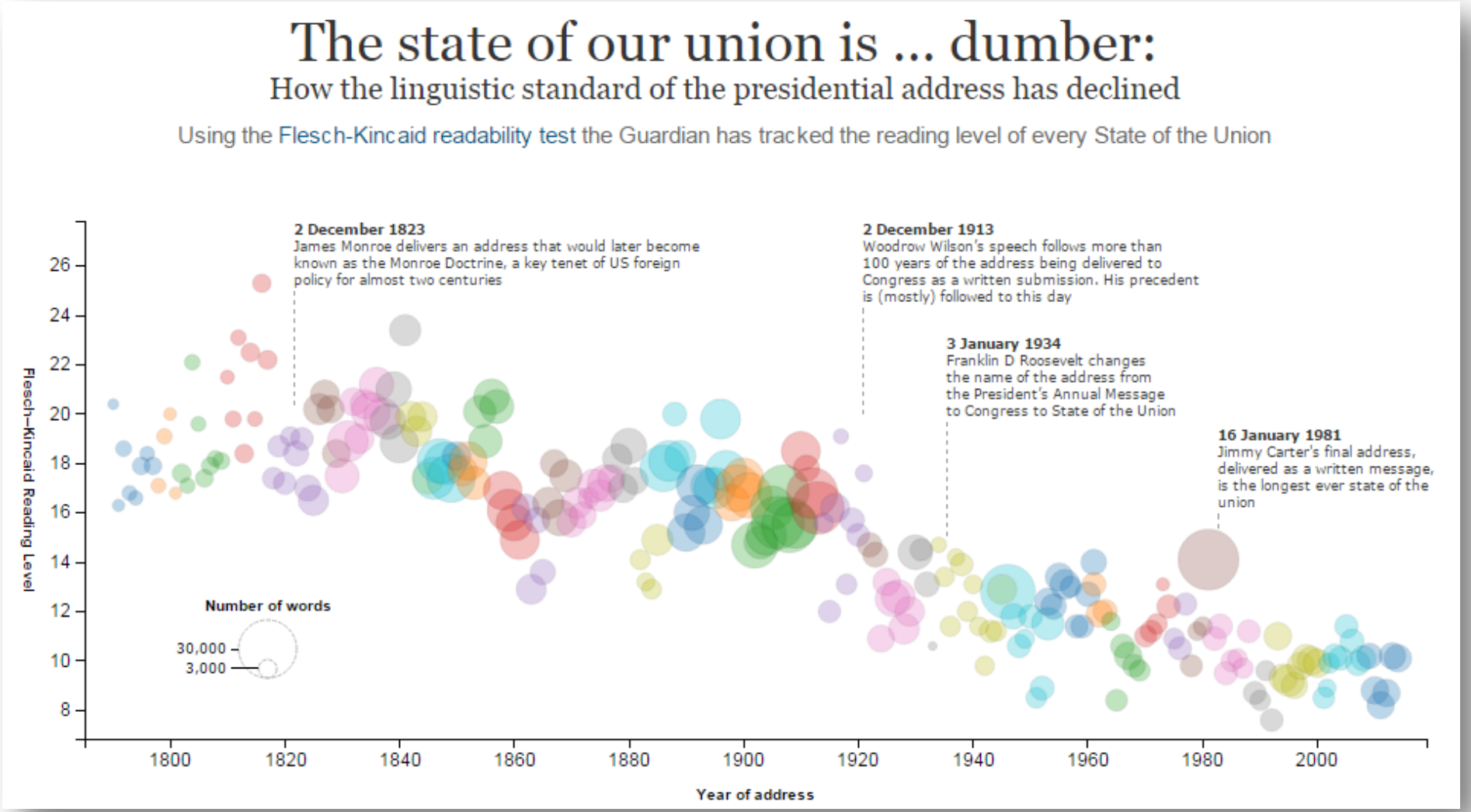
- Degrees (BA, MS-M, MBA) from CWRU in **economics**, **psychology**, **statistics** and **finance**.
- Researcher at Yale Economics Dept for 2 years.
- Consulting experience - Finance role.
- Lifelong interest in human biases and **prediction markets**.



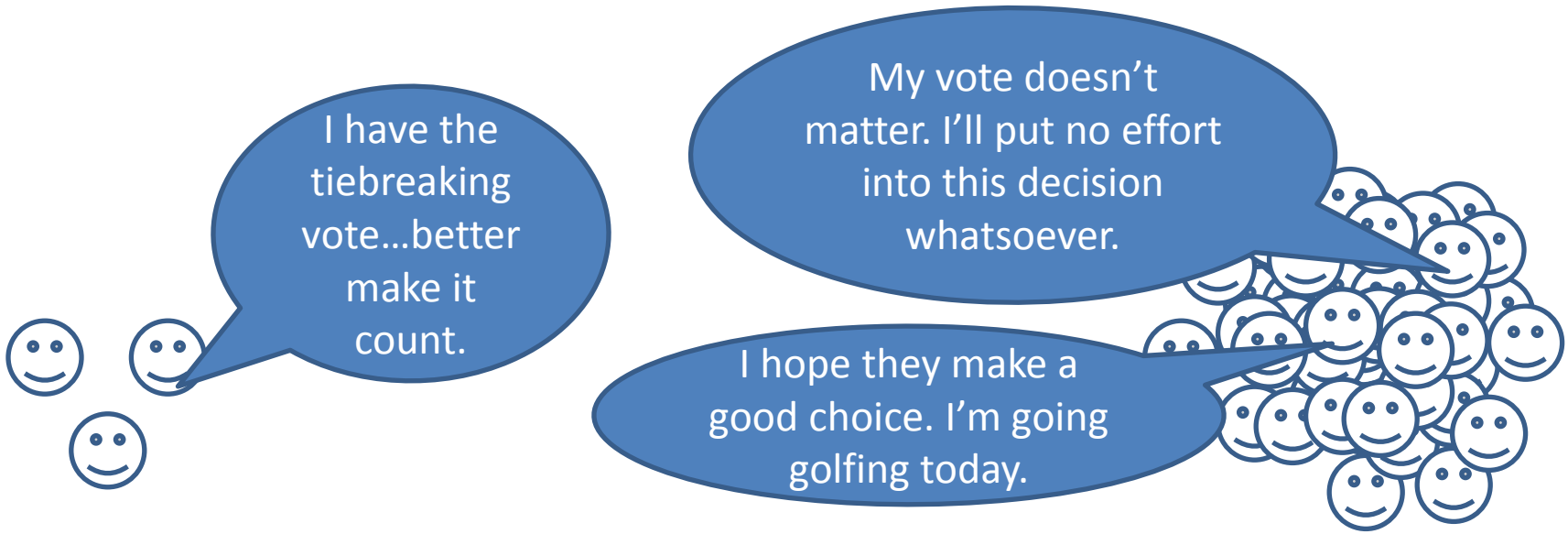


- I used to believe in **learning** and **sharing knowledge** <u>through discussion</u>. Now I think that's a waste of time.
- In fact, I feel it is immoral:
  - Talk is cheap (and you get what you pay for).
  - Encourages trust in experts/authority
  - Better to trust one's own experience, or, even better one's own skepticism (cautious people do "OK").

Our Age: The Age of Bullshit



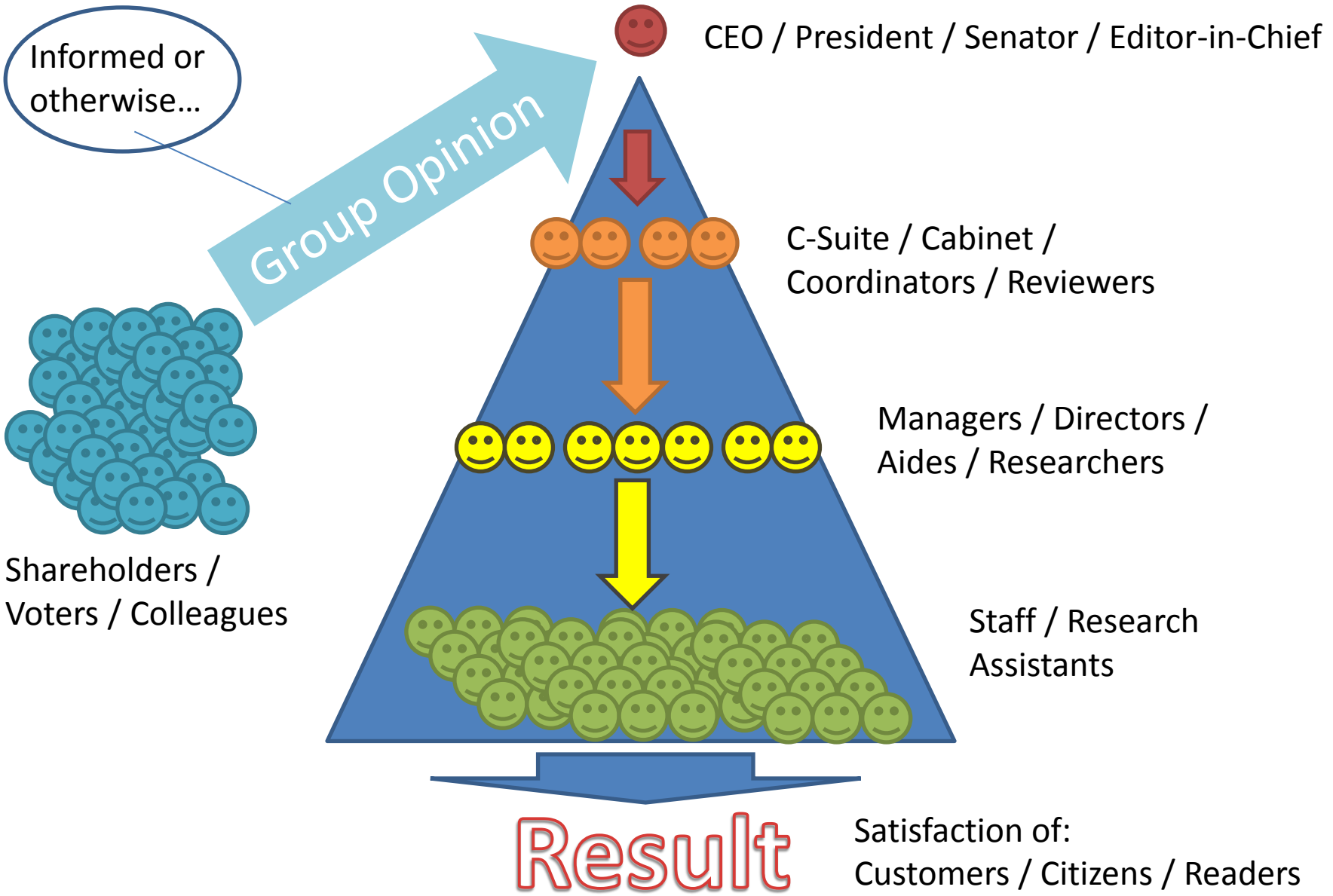
Why so bad? Scale. Ex: Voting



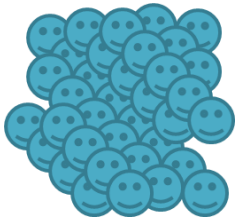
Group Size ↑ ⇨ **Benefit** if became informed. ↓
Cost to become informed. →
Power of group (tax revenue, military strength). ↑
⇨ Temptation to Corruption ↑

1. We are **choking on information**: too much on each plate, no reason to chew.
2. Too many **info-sources**, not enough **info-aggregation**.

Rot From Above: Who controls what?



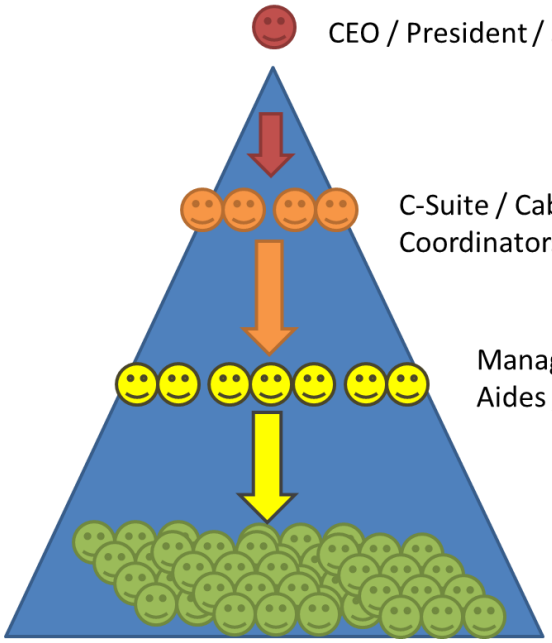
Ownership and Control: The Weakest Link



Shareholders / Voters / Colleagues

1. How to we **combine** the many preferences of this group into one request?
2. Do we each have to **monitor** the leader's work? If not, who do we trust (and why)?
3. If I don't like this leader, how do I find out if others agree? How do we **fire the leader**?

Bad



Can easily…
…make requests.
…observe work/results.
…fire insubordinates.

Good

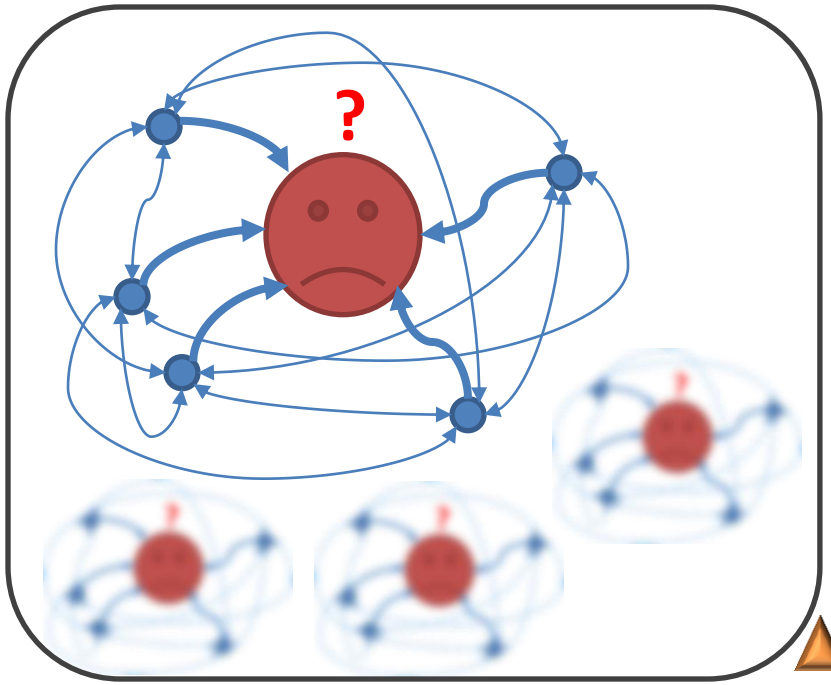
Truthcoin enables **Prediction Markets** to Aggregate Info

- For the Public: **Reliable** and **Common** Information

It's right.

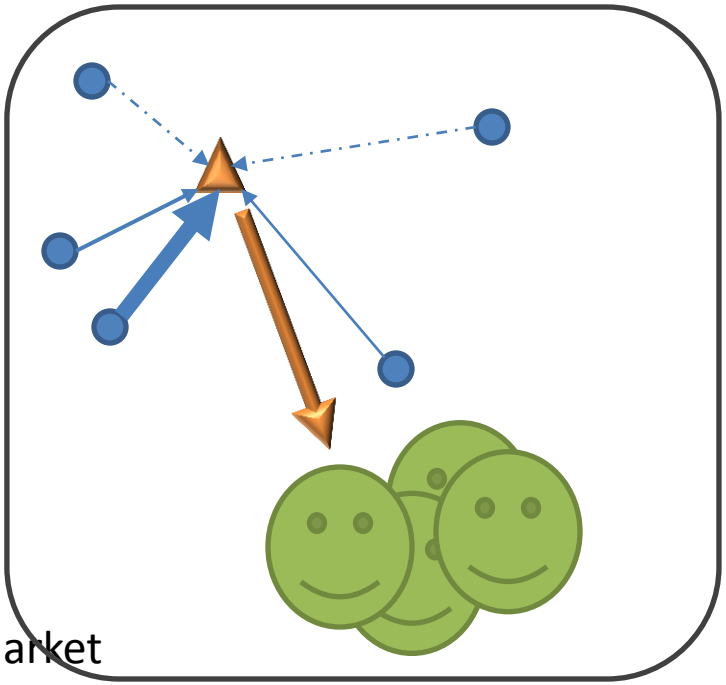
It's broadcast to everyone (and everyone knows that everyone got it).

For example: **no more bullshit about climate change (either way)**.



= Info Source

= Prediction Market



1. PMs: ‘stock market’ for a special kind of derivative.

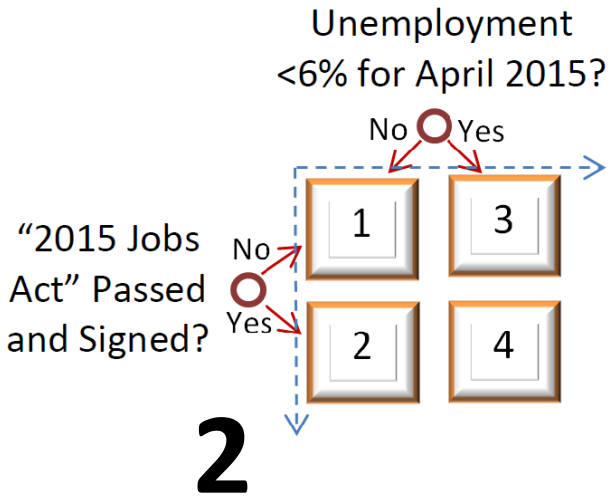
Below: **event derivative** (InTrade.com) on 2012 global warming

Climate Change: PM vs Talk

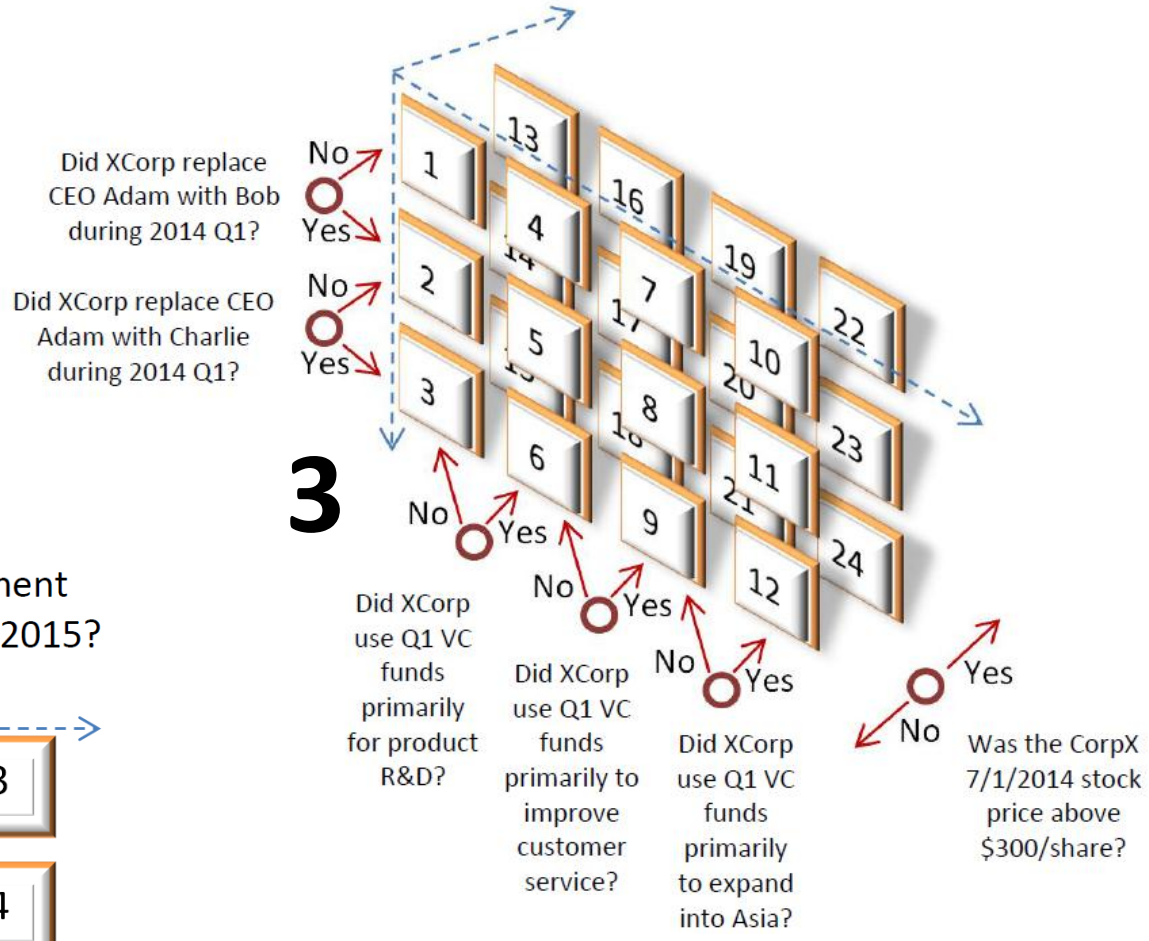
- Talk: Why even bother becoming informed?
  - Hard to learn this stuff (and I only have so much time)
  - How am I supposed to convince others?
  - Why résumés *must* be short (info-processing costs).
  - Minimal-info strategies (join a tribe/"political party").
- PM forces a clear definition.
- Prices are **constantly** and **unanimously** acceptable. At all times, everyone agrees with the price (if not, they can profitably trade).
- Note: Suppose climate change were false. The "reliability" and "broadcast" problems are much worse.

Prediction Market Magic: More Than One Dimension

1

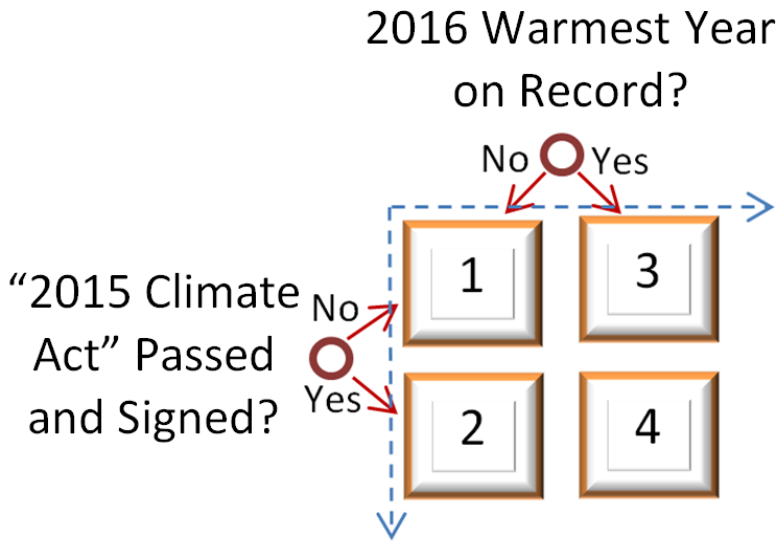


2



3

More Dimensions: More Forecasts, AND More **Relationships**



Joint, Marginal, and Conditional Probabilities

MSRs Bayesian Net

	No	Yes	
No	0.35	0.05	0.40
Yes	0.15	0.45	0.60
	0.50	0.50	1.00

	No	Yes	
No	0.15	0.45	0.60
Yes	0.35	0.05	0.40
	0.50	0.50	1.00

	No	Yes	
No	0.25	0.25	0.50
Yes	0.25	0.25	0.50
	0.50	0.50	1.00

The Point: Probabilities are not only: "Will X happen?"…
…they are also: "Would Y influence X?"

Multidimensional Governance

- Applications
  - "Which CEO *would most increase* **our stock price**?"
  - "Which President *would most decrease* **unemployment**?"
  - "Which FED Policy *would most increase* **GDP**?"
  - "Which law *would most decrease* **violent crime**?"
- So much more:
  - Betting "in" USD / DJIA / etc.
  - Provision of Public Goods (without taxes)

If Prediction Markets are so great, why don't we already use them everywhere?

- We do, privately (Best Buy, GE, Google, IBM, Intel, Siemens, Yahoo!, etc.)…
- Why not for **public** orgs/decisions…?

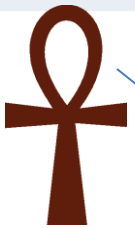
PM Problems

1. Agency Cost
    1. New info: find **replacements for inefficient leaders**.
    2. Who tries this experiment first? What if competitors don't? ("Norming", Need **globally accessible** set of new rules).
    3. Where allowed, would not be needed.
2. Public Awkwardness / Old Taboos
    1. Resembles vulgar gambling (history of **banned finance**).
    2. "I know that my vote doesn't count, but you don't have to be rude about it." Re: **Unpopular election-betting**.
    3. **Regulatory** response to (Irish) company. PAM vs Wyden.
3. Counterparty Risk
    1. The age-old betting problem: "**Will this guy pay up**?"
    2. Value-Storage as a **single point of failure** / Fall of InTrade
    3. Will the admin **censor** PMs (that I like)?

Sound familiar…?

Protocol (Decentralized)	Centralized Non-Protocol
Spoken English	Shakespeare's Globe Theatre, The Library of Alexandria, MLA Citation Format, Walt Whitman, J.K. Rowling.
Rules to American Football	The NFL, ESPN, The Buffalo Bills.
Bluetooth	A Set of Stereo Speakers, The iPhone 6, A Car Radio Equipped with Bluetooth
Bitcoin	VISA, PayPal, SWIFT, Western Union, Airline Miles, Amazon Coins, e-Gold, Liberty Reserve.

Protocols are Immortal



Ankh – Egyptian Symbol of Eternal Life

Protocols are self-replicating "informational viruses" (like memes) which can easily outlive their creator!

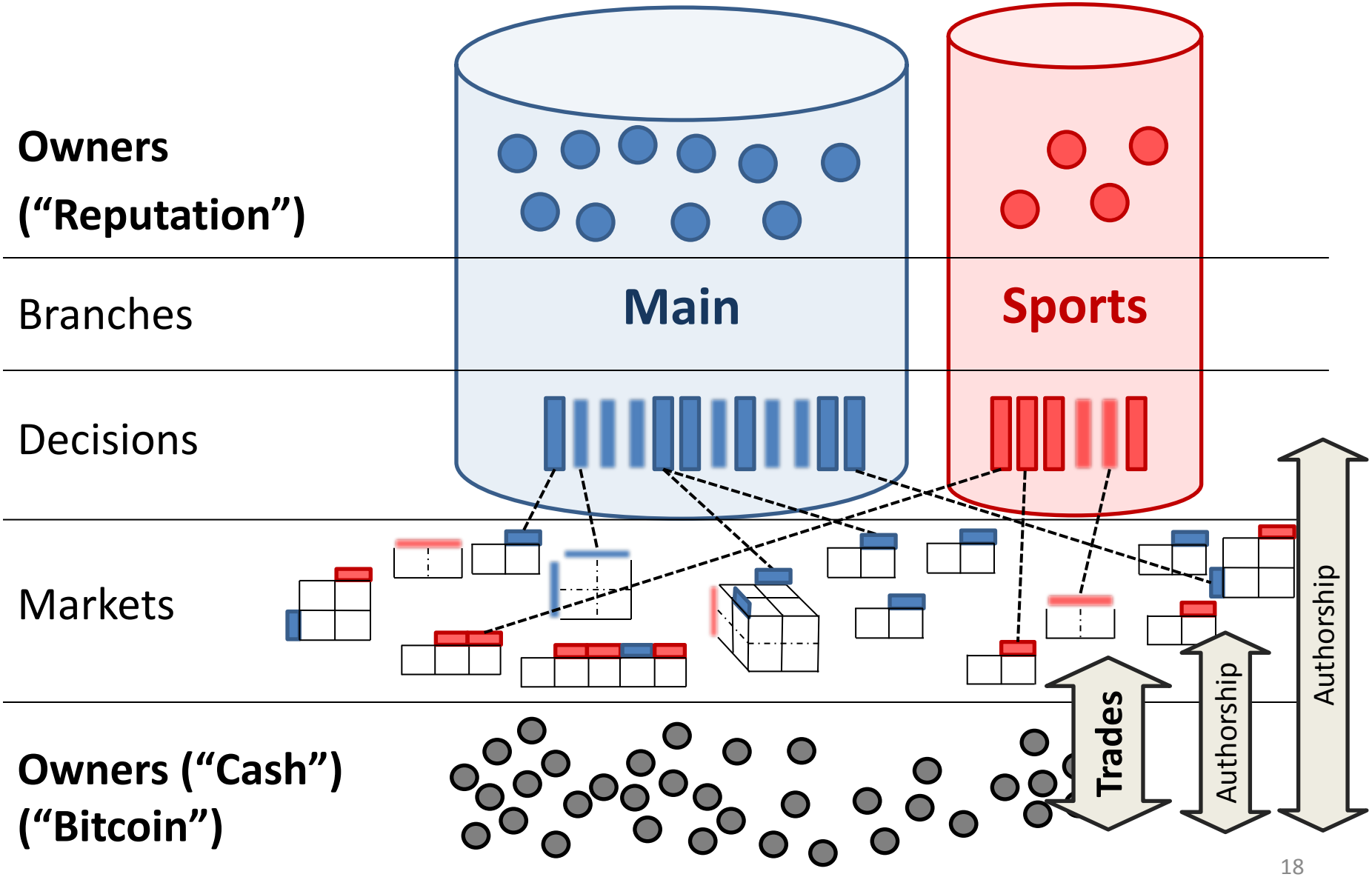
Benefits of Immortality:

1. Will still be around to pay you back (cannot be killed, cannot go out of business).
2. Tamper/Censorship-Resistant (contracts enforced as signed).
3. No middlemen (self-sustaining, less overhead, lower cost).

So How Does The Protocol Work?

Many Other (Better) Resources:
Whitepaper / Code / Demo / Forum / FAQs
www.truthcoin.info

Truthcoin Graphic: Two Coin Types



Timeline (on one Branch)

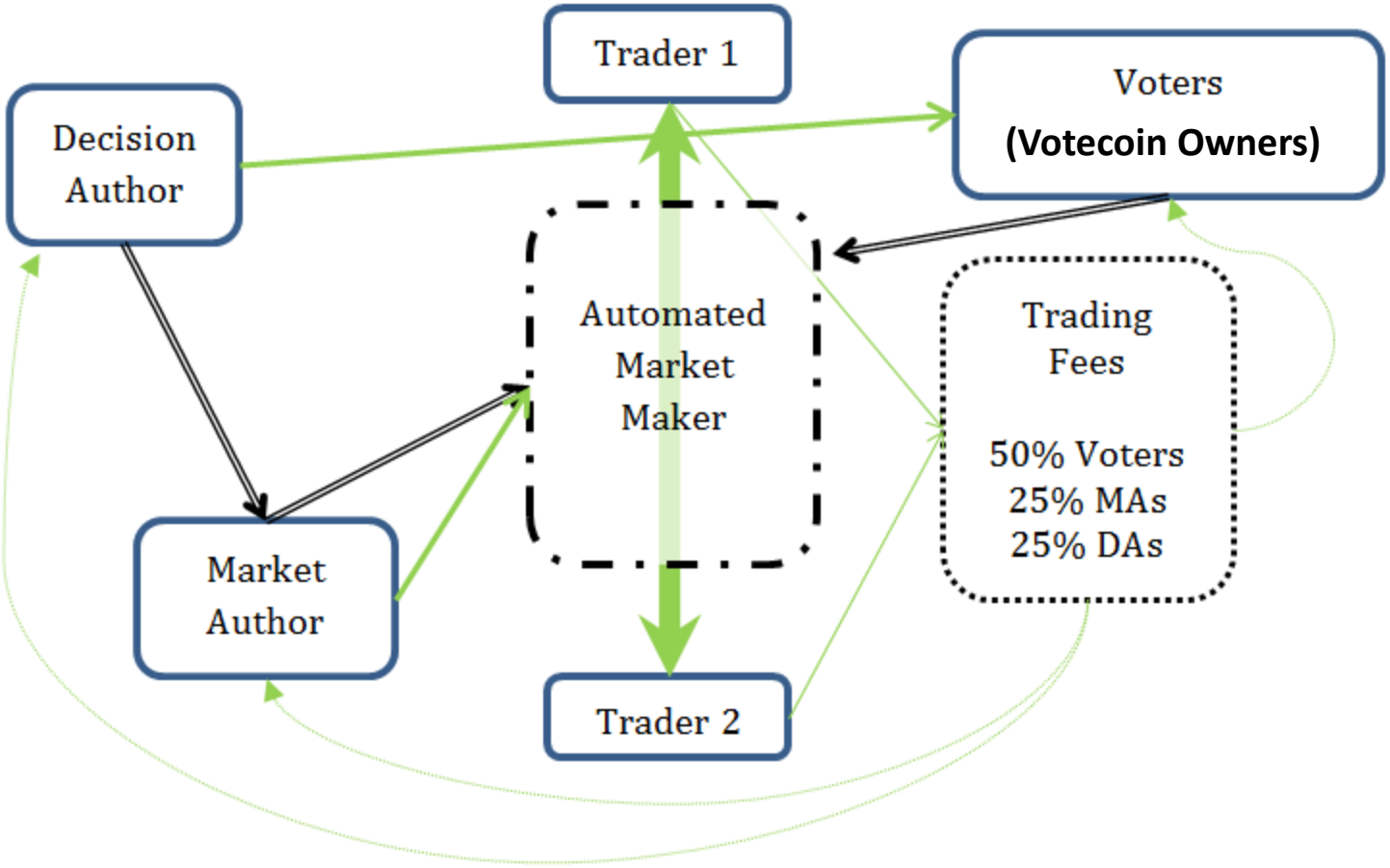


Figure 6. The flow of costs (green solid), revenues (green dashed), and information (black double) among various agents (blue solid) and accounts (black dashed). The horizontal axis corresponds to time, and line widths correspond to expected magnitudes, with the exception of revenues (whose magnitudes are a function of trading volume).

Vote Matrix

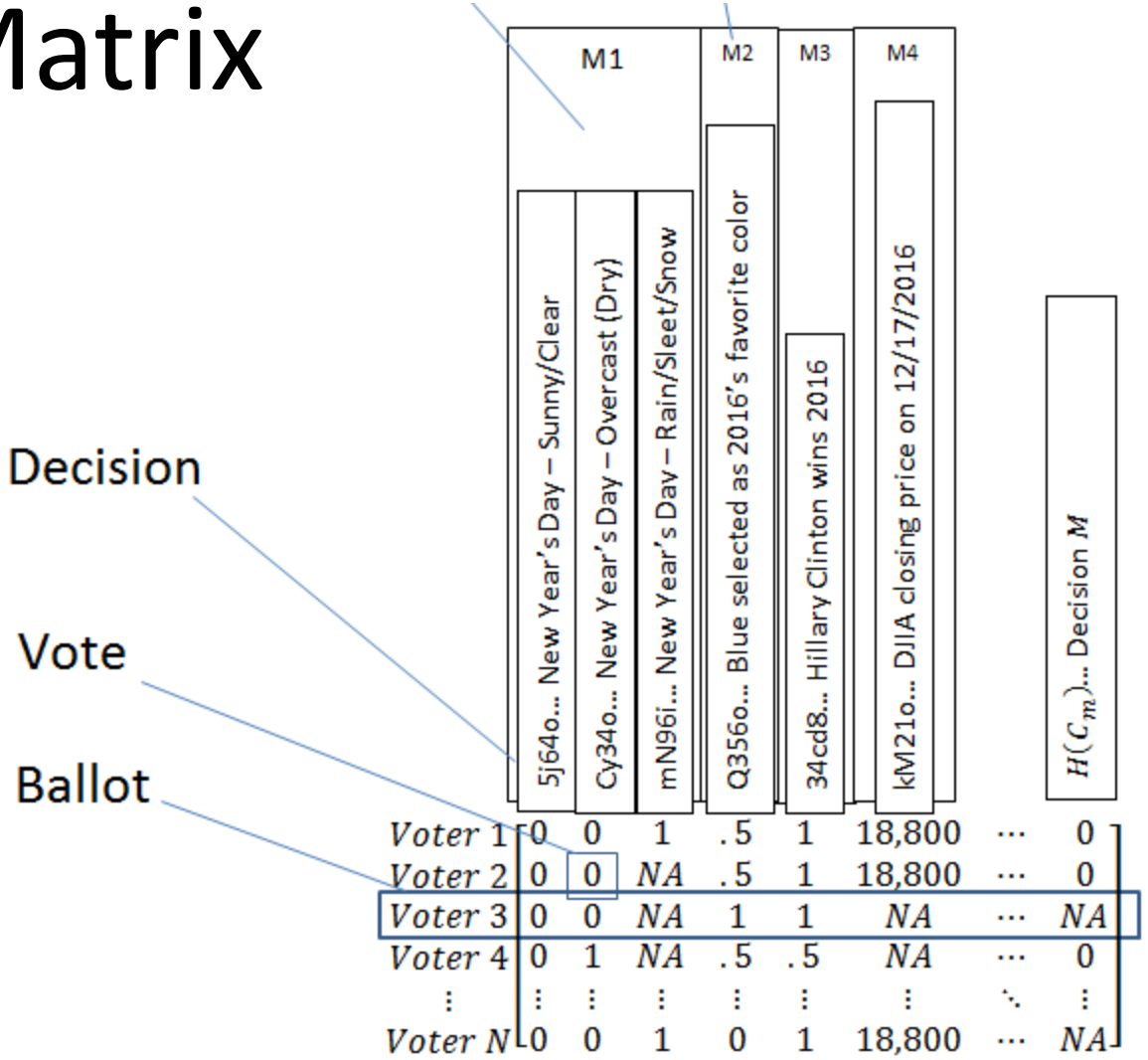
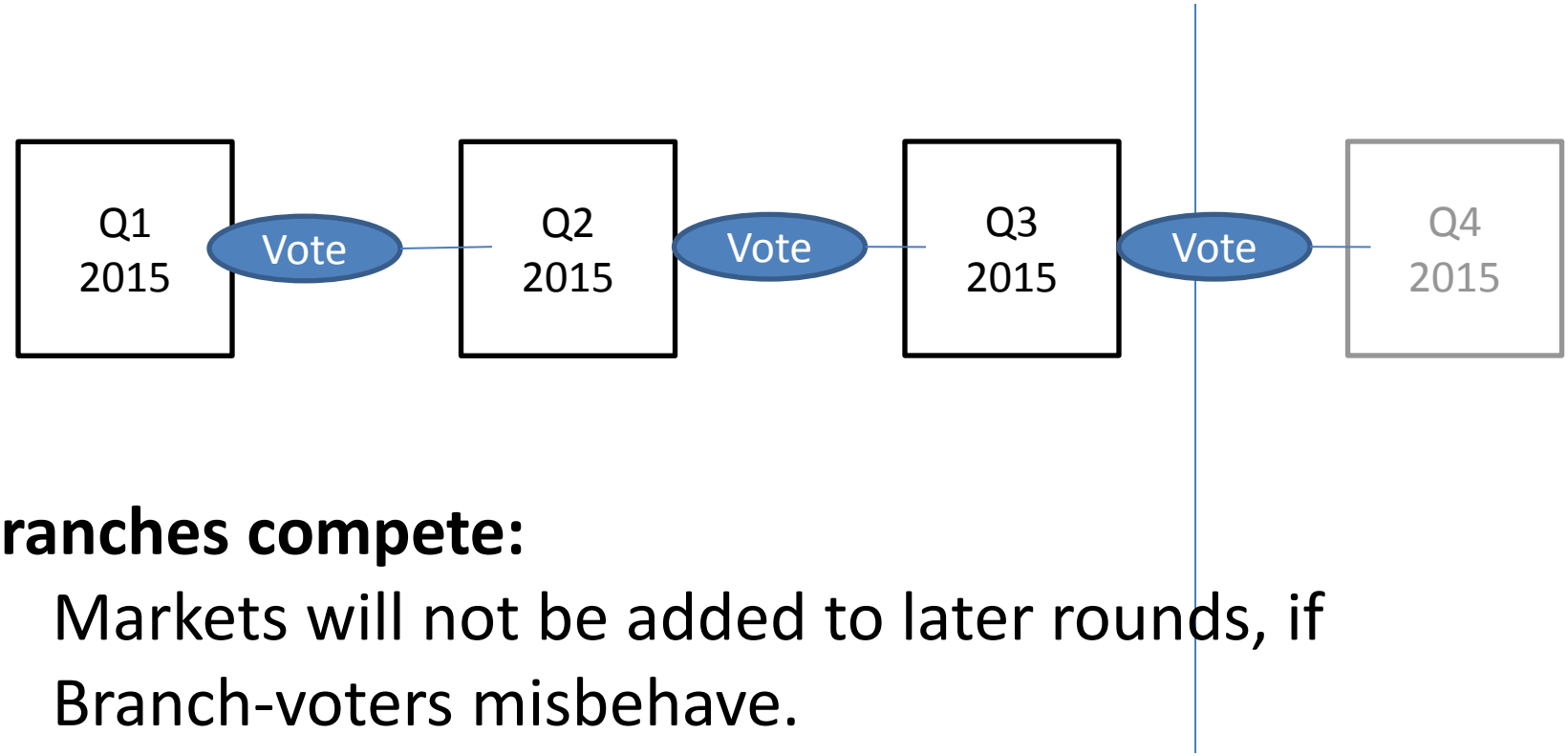


Figure 3. A hypothetical January 2017 Vote Matrix, with annotations. This Vote Matrix would be for a Branch at least general enough to contain Decisions on US weather, politics, and financial indices.

Adding Decisions in Big, Distant Groups



Branches compete:

- Markets will not be added to later rounds, if Branch-voters misbehave.
- Fancy use of PMs allows far off events to be insured against themselves – Authors can withdraw the “cash cow” at any time.

Groups And Their Incentives

Role	Pays	Rewarded With
Decision-Author	Listing Fee (Large)	25% of Trading Fees, for Market which used this Decision
Market-Author	Market Fee (Small) + Liquidity Subsidy	25% of Trading Fees, for Market which used this Decision
Voters	Time Spent Voting + Votecoins at Risk + Opportunity Cost of Attacking the market-resolution process	50% of Trading Fees, for Market which used this Decision Additional Votecoins (greater ownership/ responsibility) if correct other Voter's mistakes. Ability to cash-out good reputation at any time.

Why Vote Honestly?

See Supporting Material for More Details

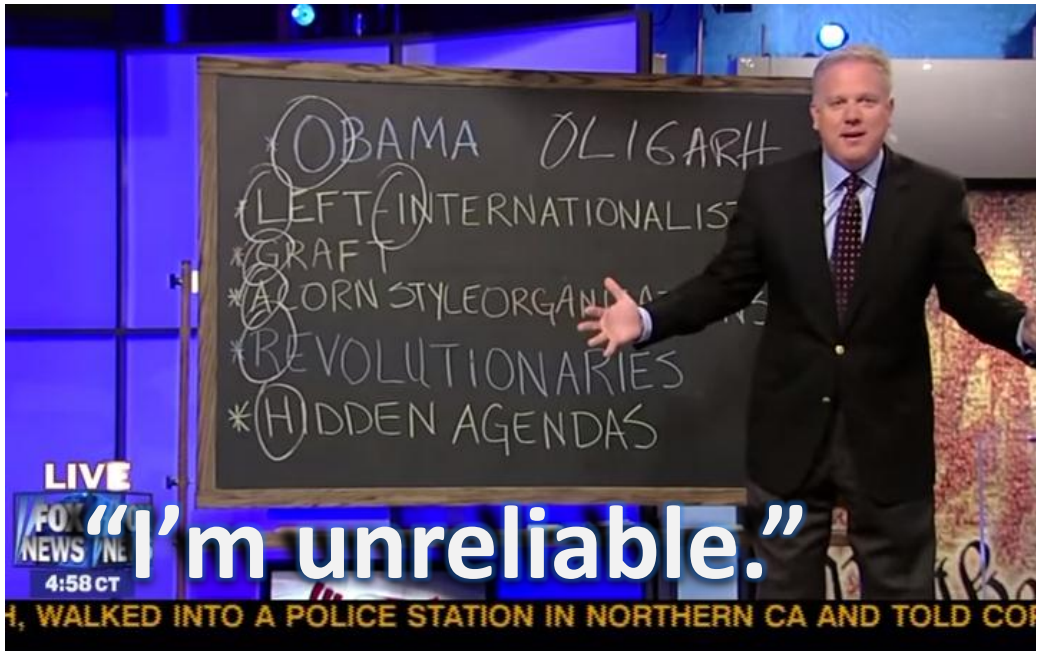
1. Mechanism Design (Ownership and Control)
    1. Voters 'buy in', simulating perjury / real-world reputation at stake. What they bought is worth little if it produces no value.
    2. Trades are mutually beneficial, even with fees (risk-pooling, insurance, recreation, etc). This produces overflow value which can be captured and repaid to Voters.
2. Truth-Heuristics for Keeping Voters In Line
    1. SVD / Eigentrust / Bayesian Truth Serum as a way of approximating "truth" (Bayes' Rule, Scientific Method, logical consistency, etc).

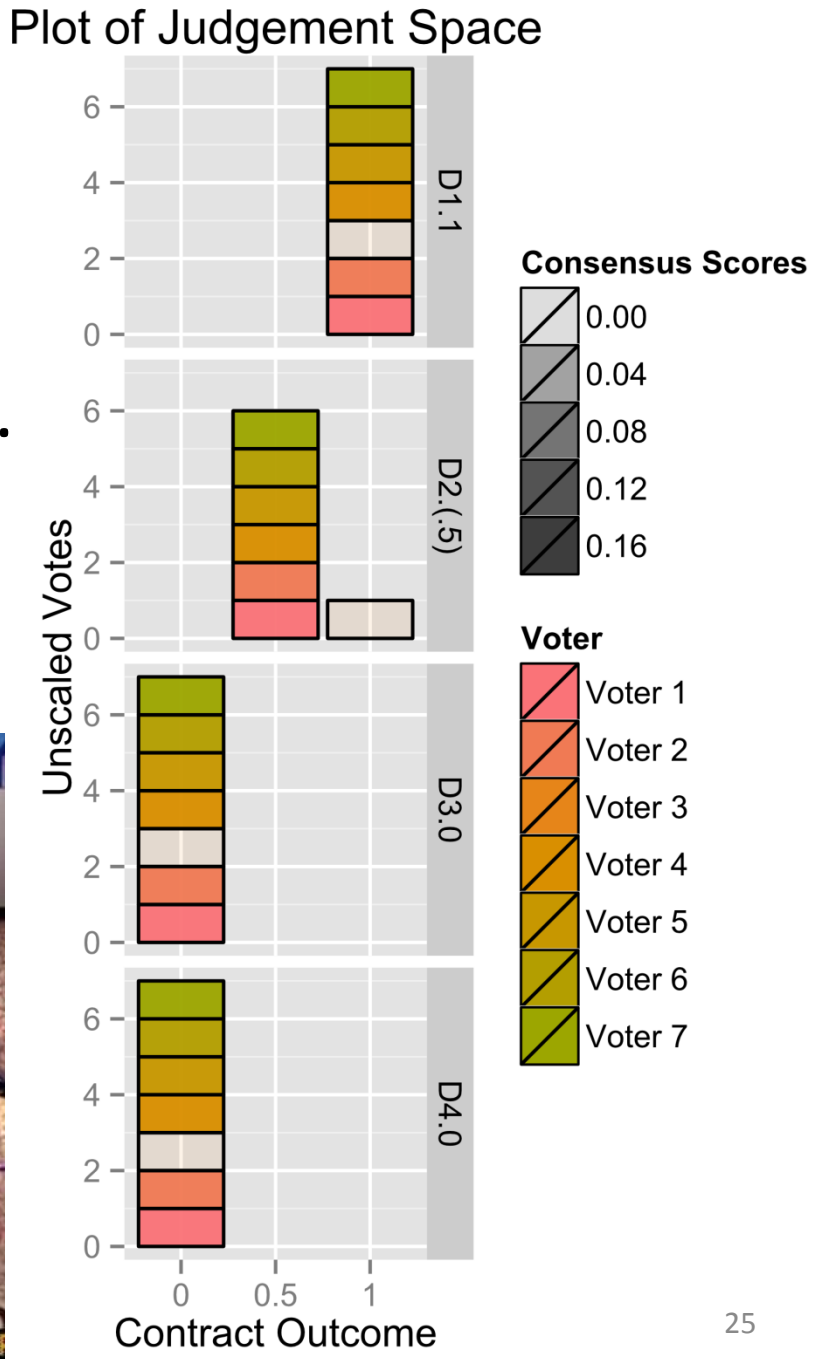
Mechanism: how to ‘tie’ people to a permanent reputation (as in real life)?

- **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). This neutralizes the opportunity cost to attack.
    - 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).

The SVD Penalty

- Experience "reports" on **many things** from **many people** in real-time ('Ballot').
- Constantly evaluate logical consistency **of the person**.

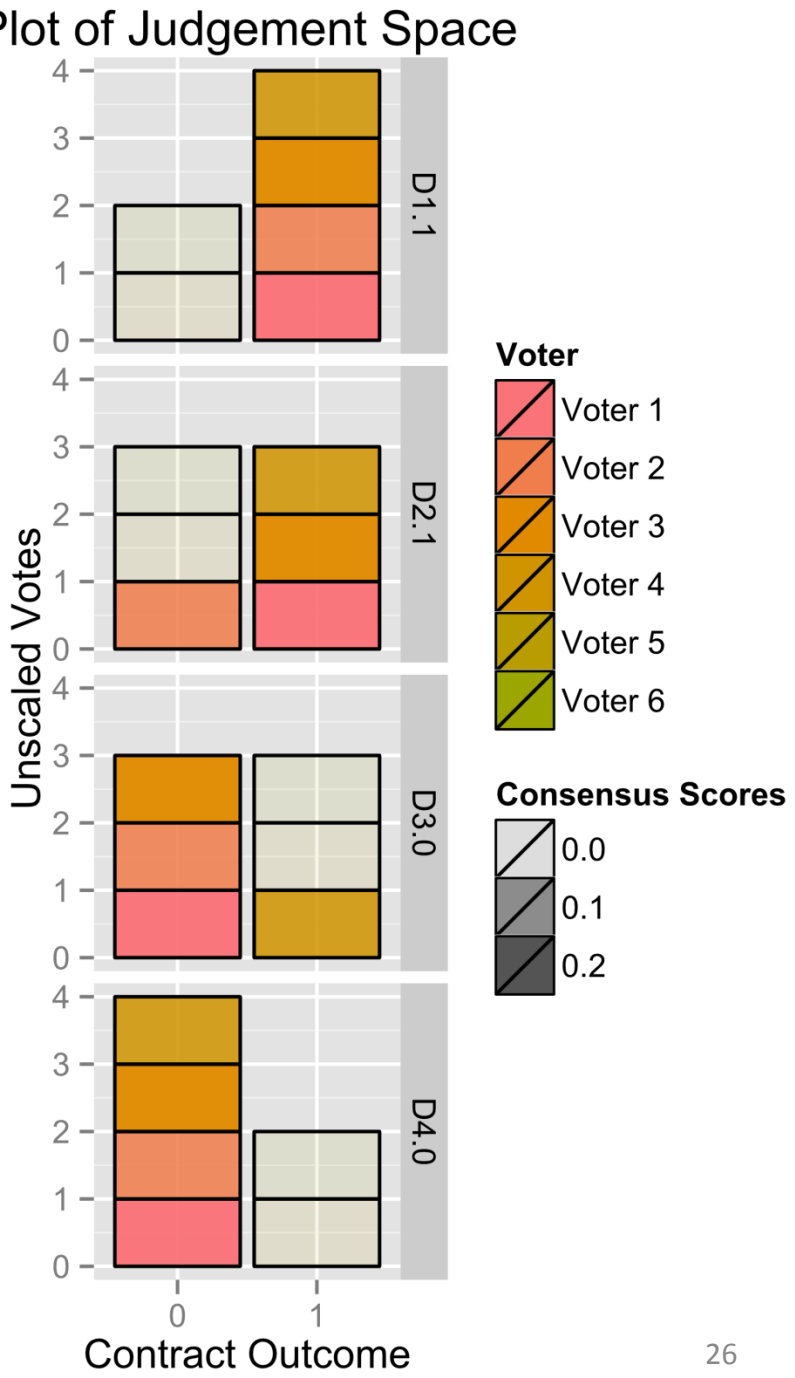




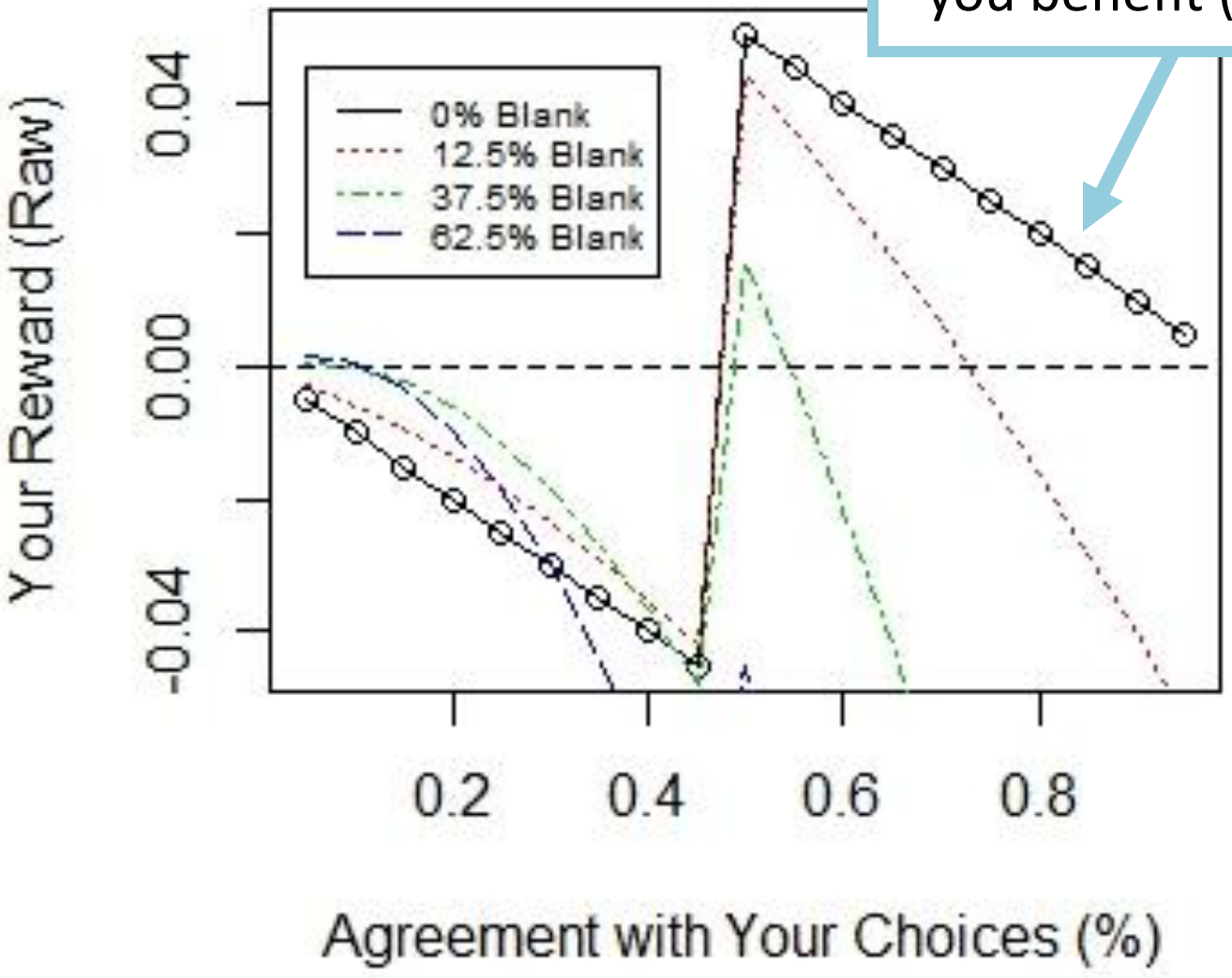
Example 2:

	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



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



Result: Cannot trust rival voters…no cartels or "voting pools".

Questions