Truthcoin
Blockchain Prediction Markets

"Outcomes"

v2 – 10/15/2014

Paul Sztorc

This Presentation

Applications

Outcomes

Trading

Bitcoin
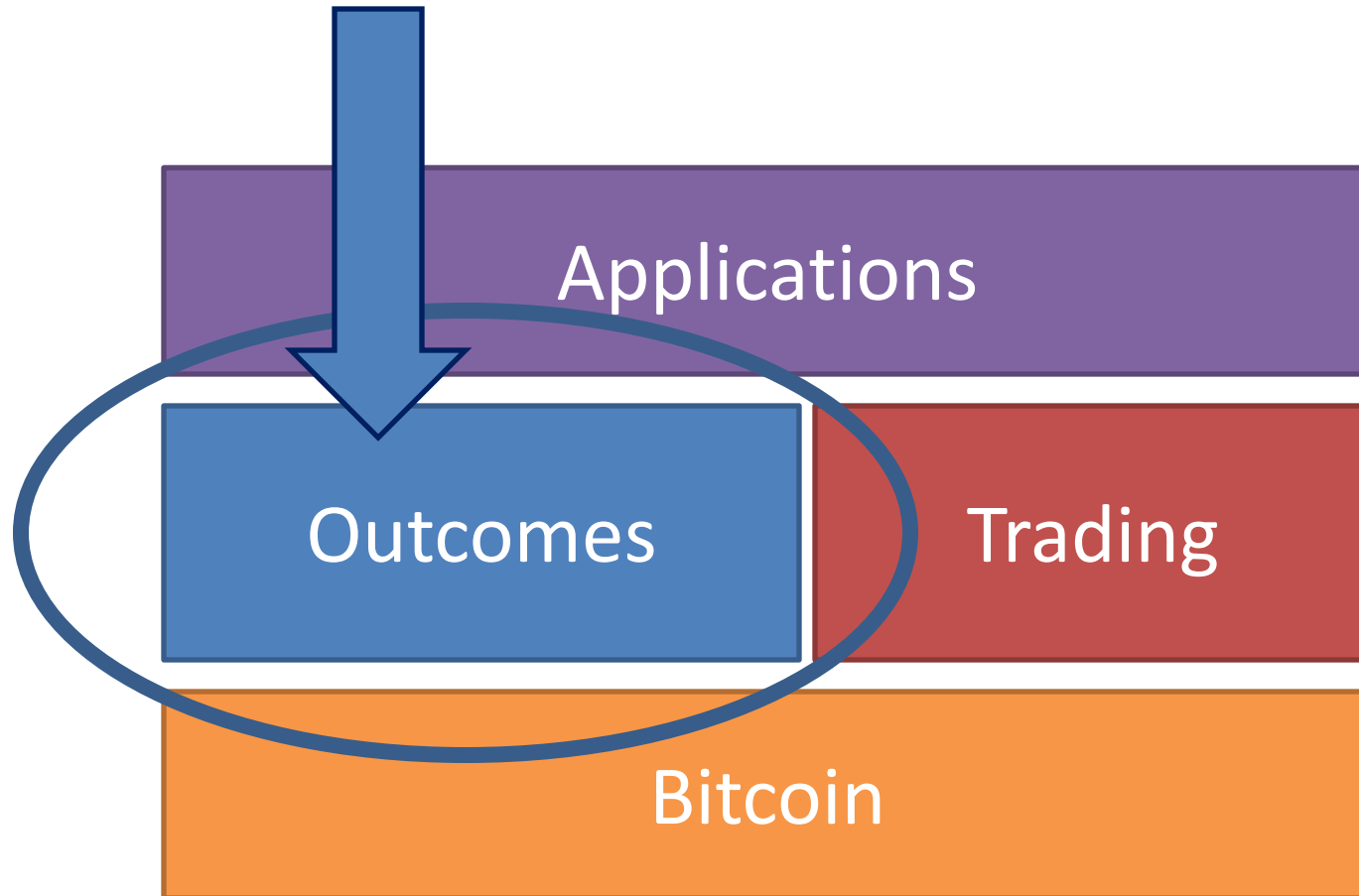
Talk Outline – 26 Slides

1. The Outcome Problem (Slides 4 – 8)
    1. The Goal, stated clearly.
    2. Competing Arbiters? Not 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.
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.
  - "The Powers That Be" / Crazy "Joker" types.

What won't work:
Competing Arbiters / Price-Feed-Providers

?

Trader

Judge 1

Judge 2

Judge 3
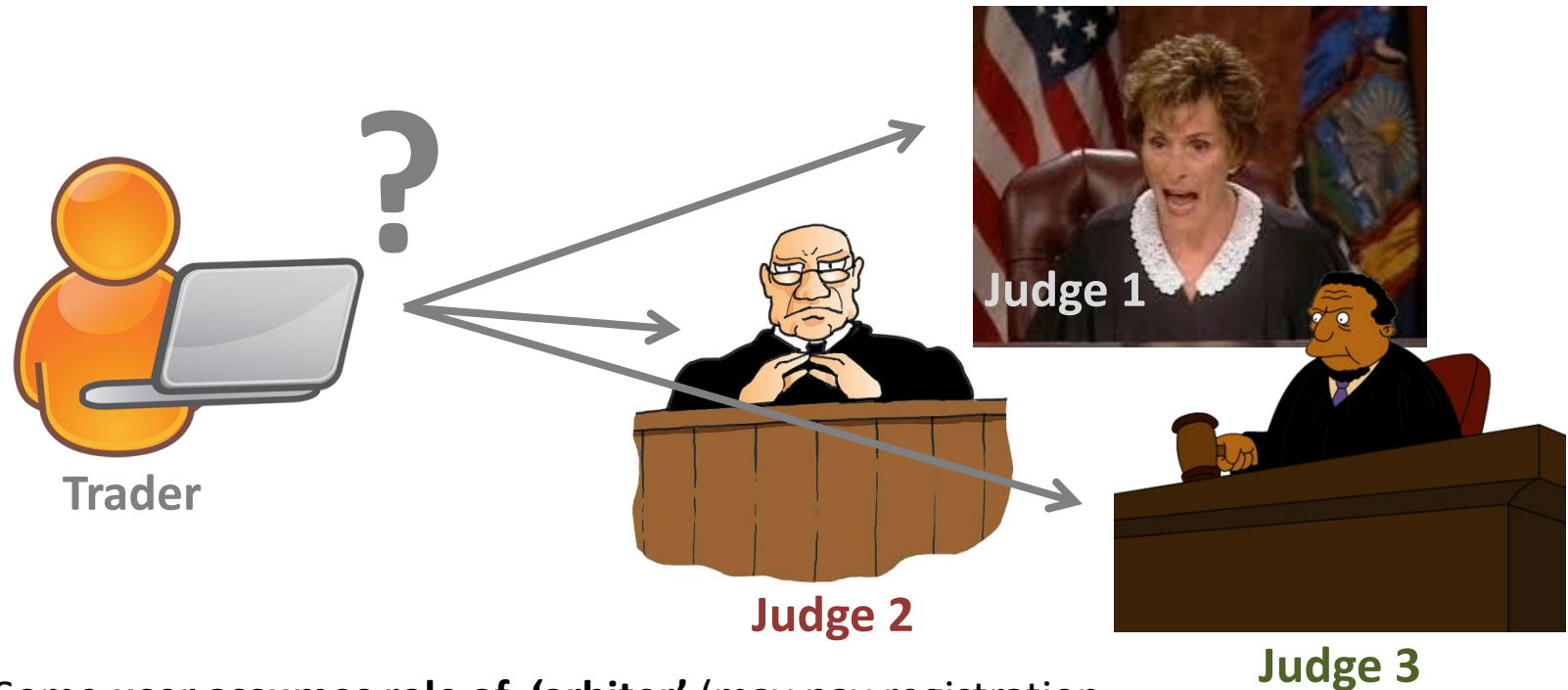
1. Some **user assumes role of 'arbiter'** (may pay registration fee, 'fidelity bond', or may be free, may involve off-chain marketing/legal …).
2. Arbiters collect **fees on an ongoing basis** per judgment, resolution, audit, or per day, feed, subscriber, etc.
3. Trader can choose arbiter: competitive marketplace provides **incentive to keep good reputation**. "Bad" agent = no longer chosen = **loses ongoing fees**.
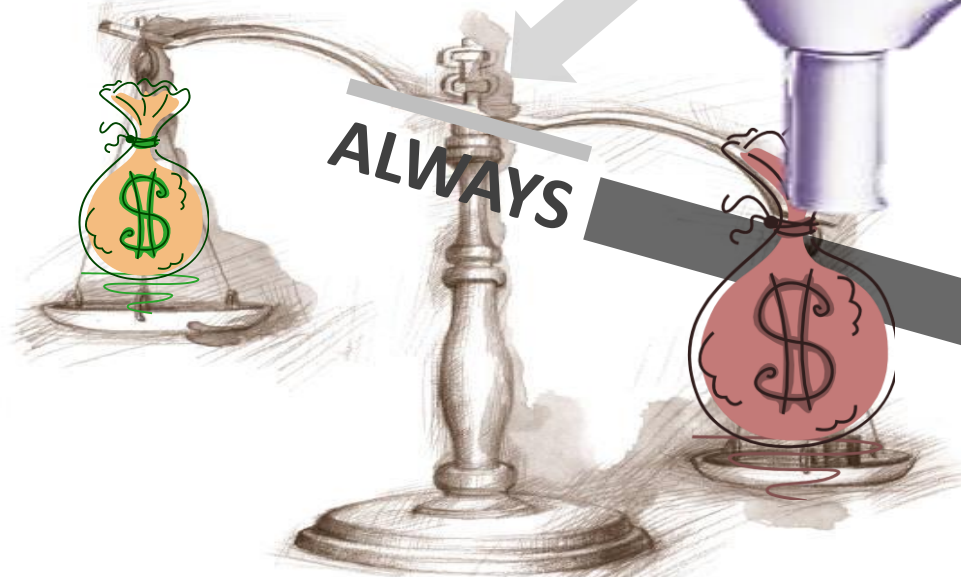
(I don't own these images).

5

The Competing Arbiters Assumption

2: Payoffs in Future

1: Attack Payoff Today

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)

ALWAYS

The Out

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

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!

- <u>Our reality</u> 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 <u>think we "know"</u> **<u>some facts</u>** ("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**.

"I'm unreliable."

10
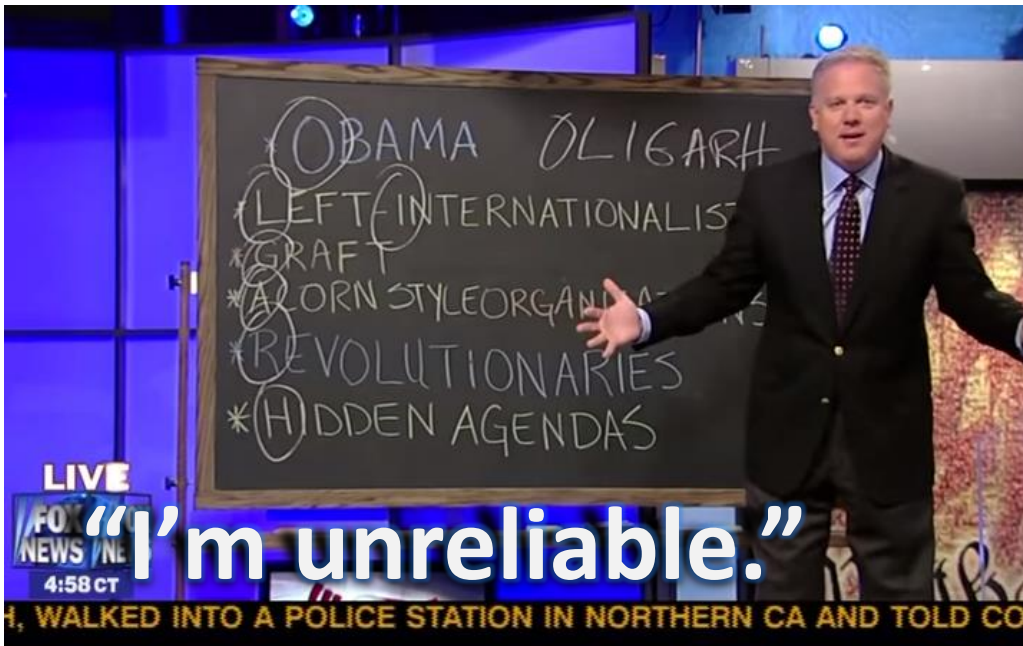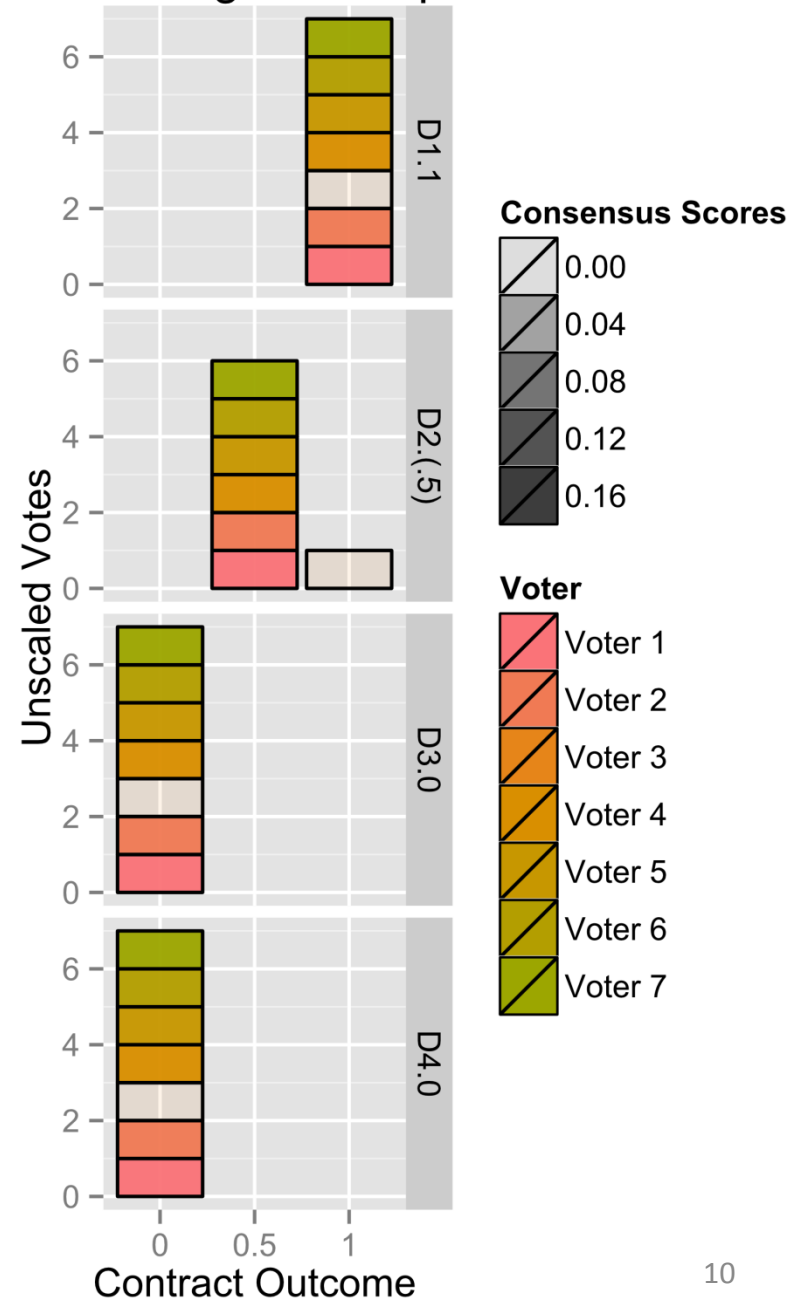
Singular Value Decomposition

- http://www.youtube.com/watch?v=pAiVb7gWUrM
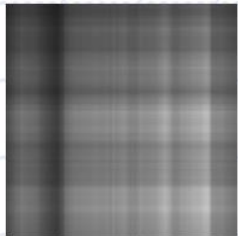- Point = Build **index of disagreement** with an abstract 'most-representative ballot' (not known in advance to any single voter). Cotinuous.
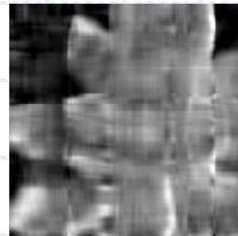
Original image

rank 1   rank 2   rank 4   rank 8   rank 16   rank 32

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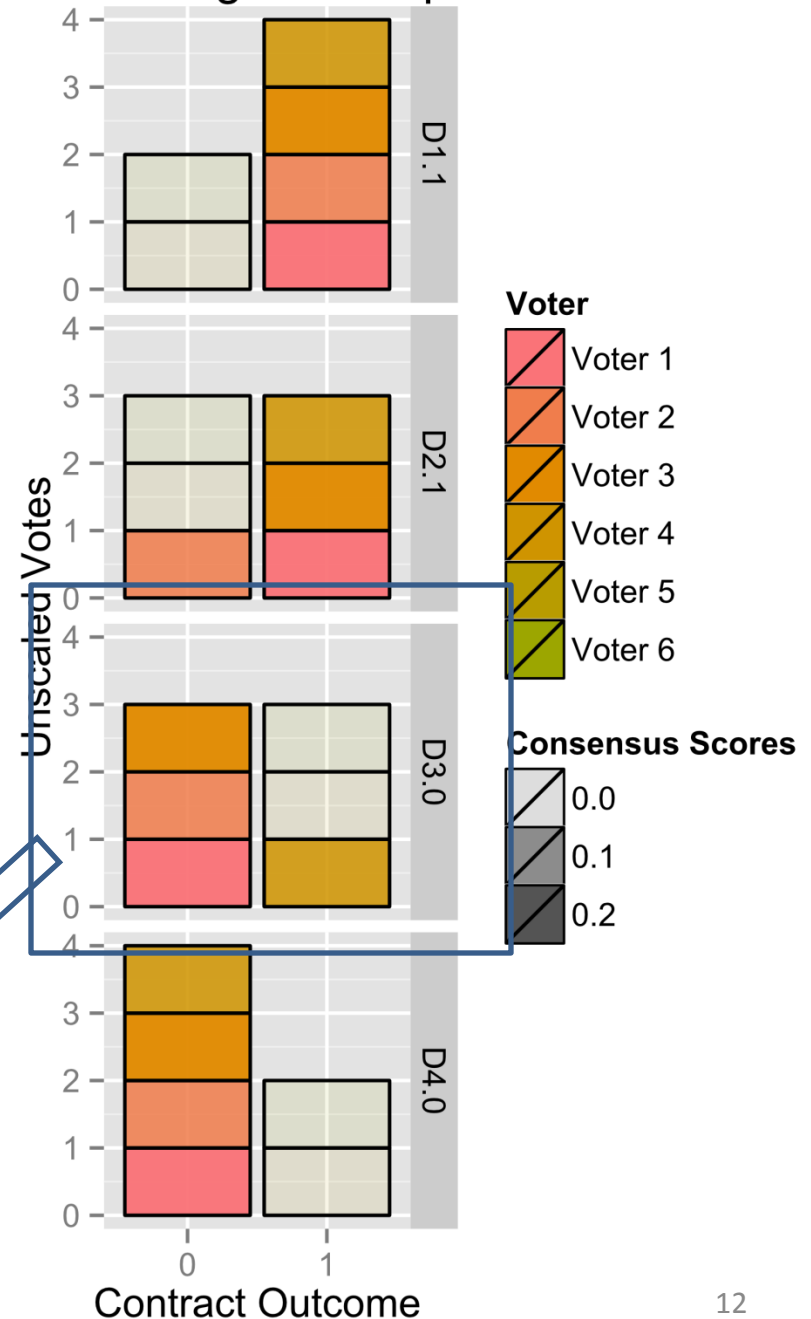
Example 2:

	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.inf
o/index.php/topic,134.0.
html

Plot of Judgement Space
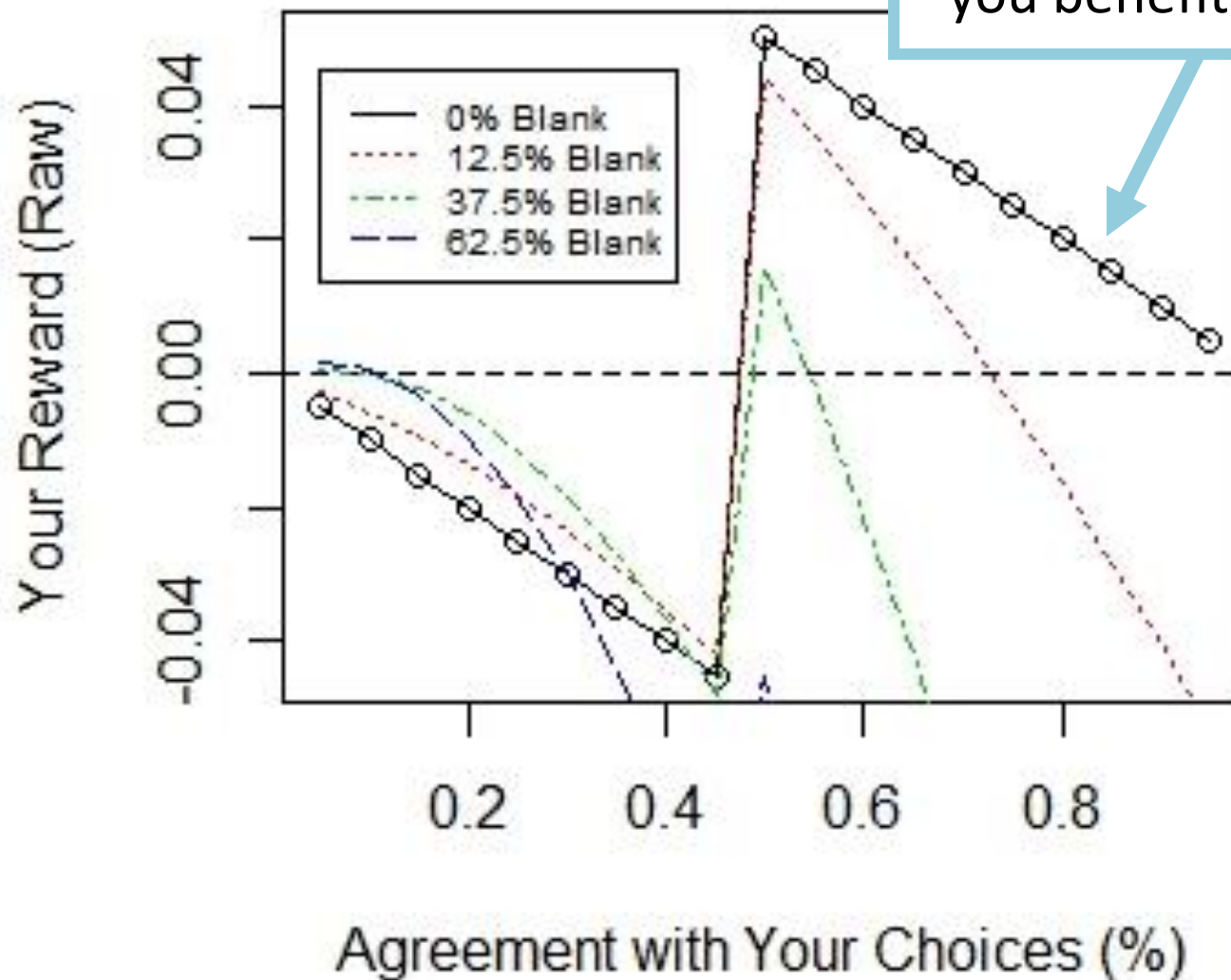
As others disagree with you, you benefit (up to a point)!

Your Reward (Raw)

- 0% Blank
- 12.5% Blank
- 37.5% Blank
- 62.5% Blank

Agreement with Your Choices (%)

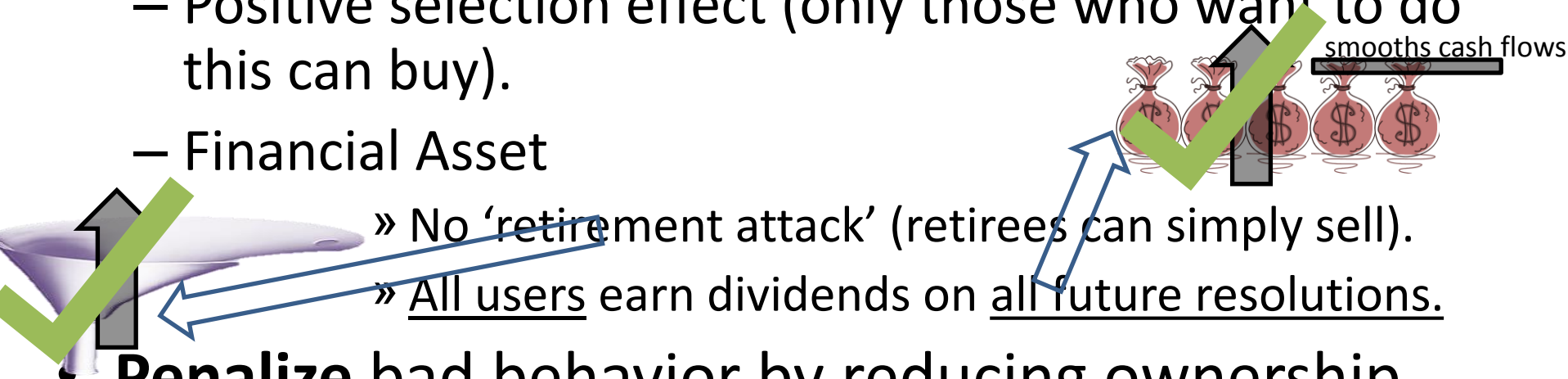**Result:** Cannot trust rival voters...no cartels or "voting pools".

Consistency #2: Time
After someone lets you down, then stop trusting them!
(Reputation)
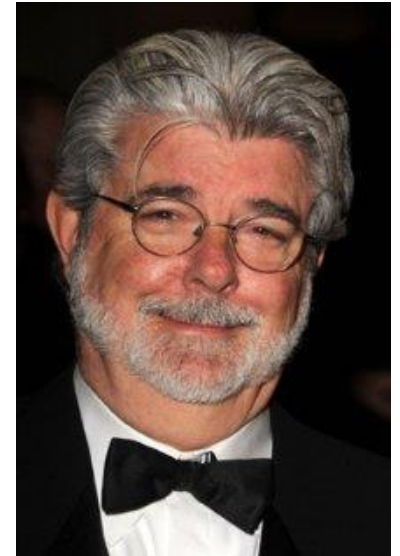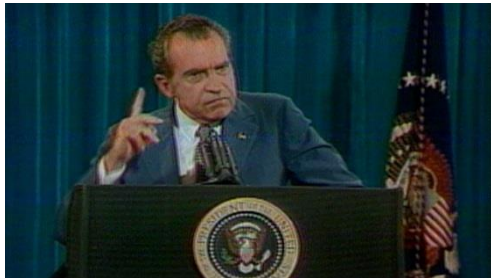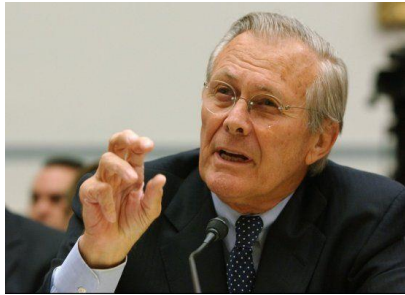
How to 'tie' people to a permanent reputation (as they are so-tied in real life)?

- **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.

  smooths cash flows

- **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

Main

Sports

Decisions

Markets

Authorship

Trades

Authorship

Authorship

Owners ("Cash") ("Bitcoin")

Scalability = "Branching"

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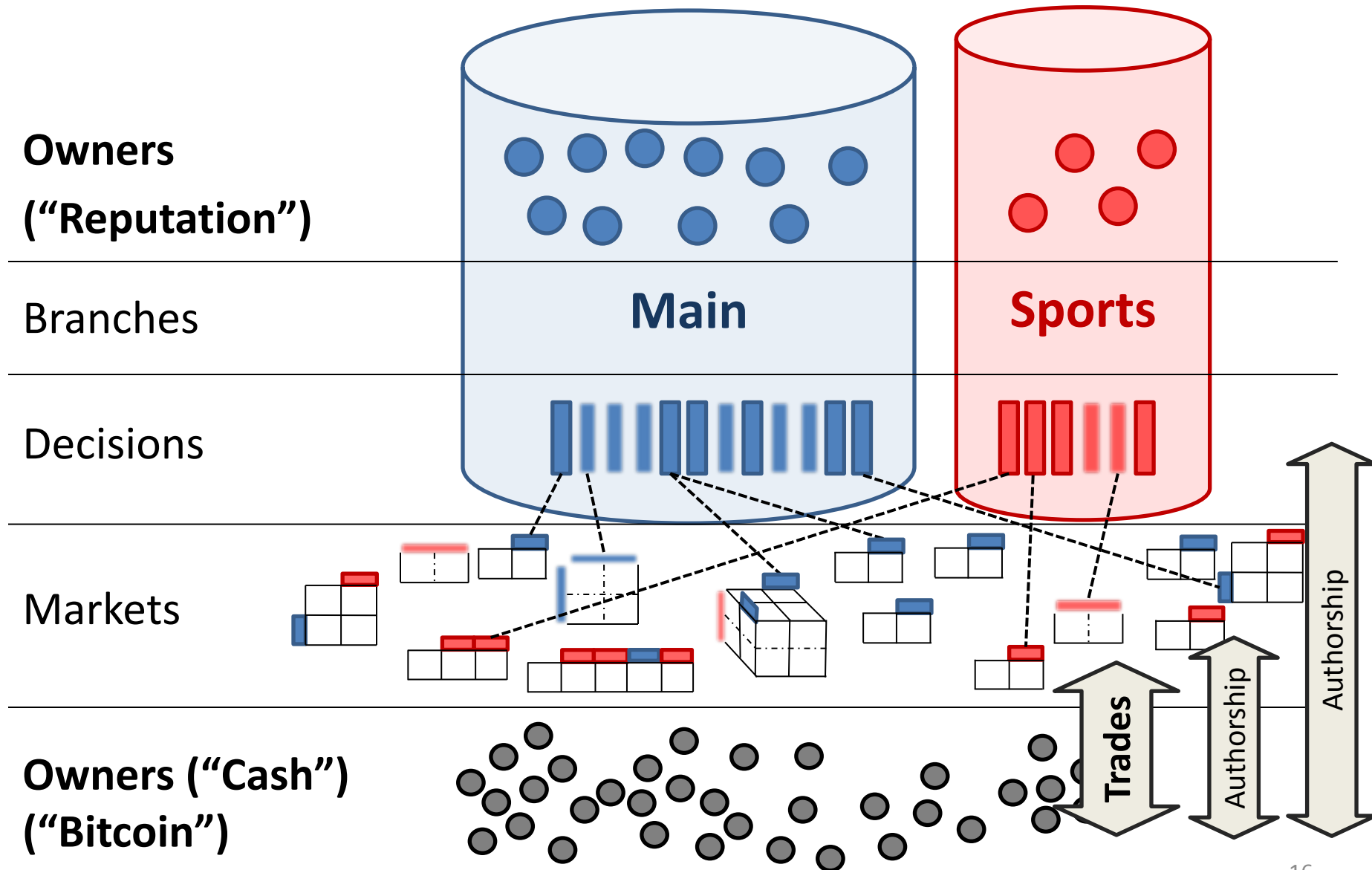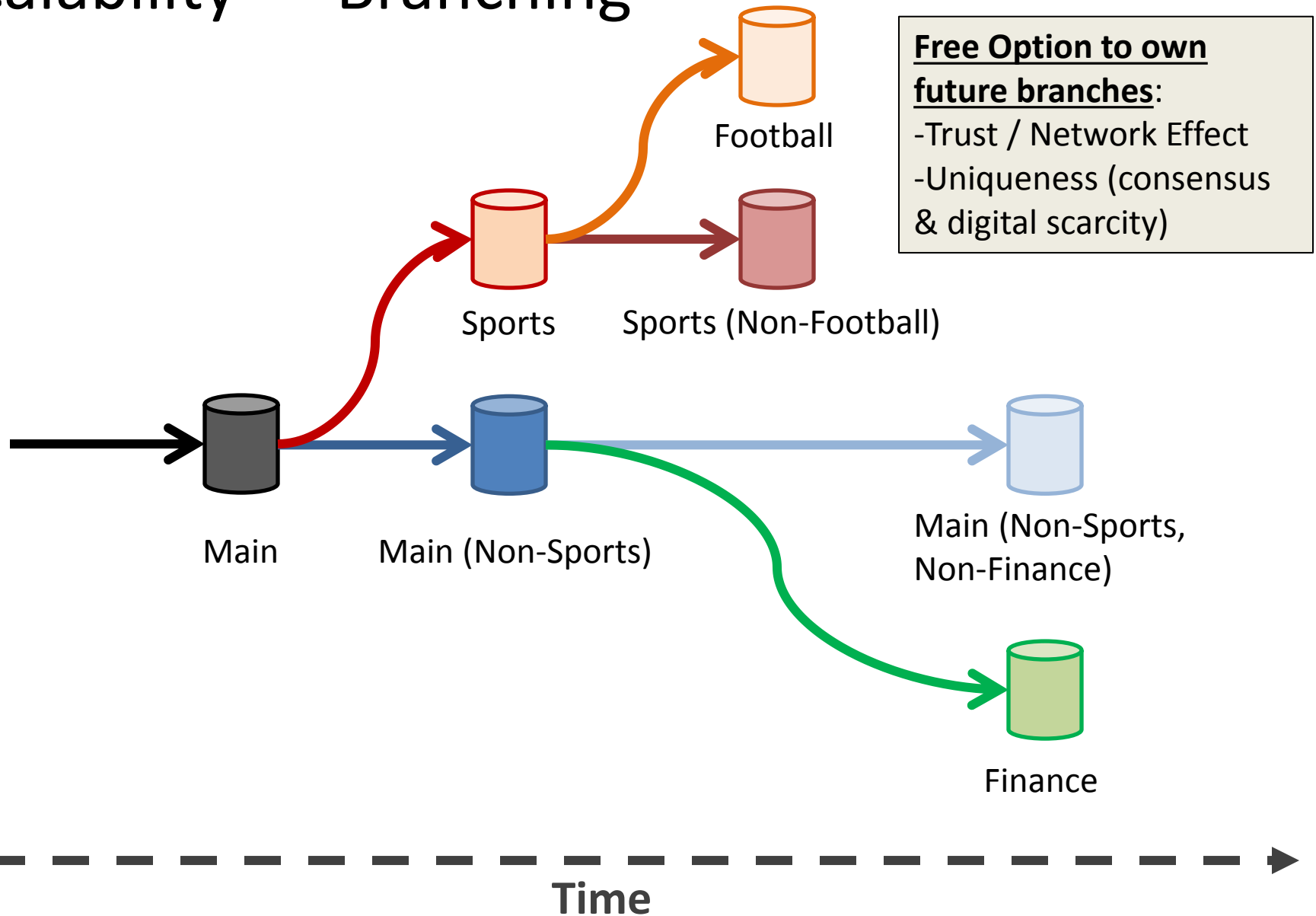
The 51% Voter-Attack is Much Harder

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 (<u>all of which is lost</u> 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.
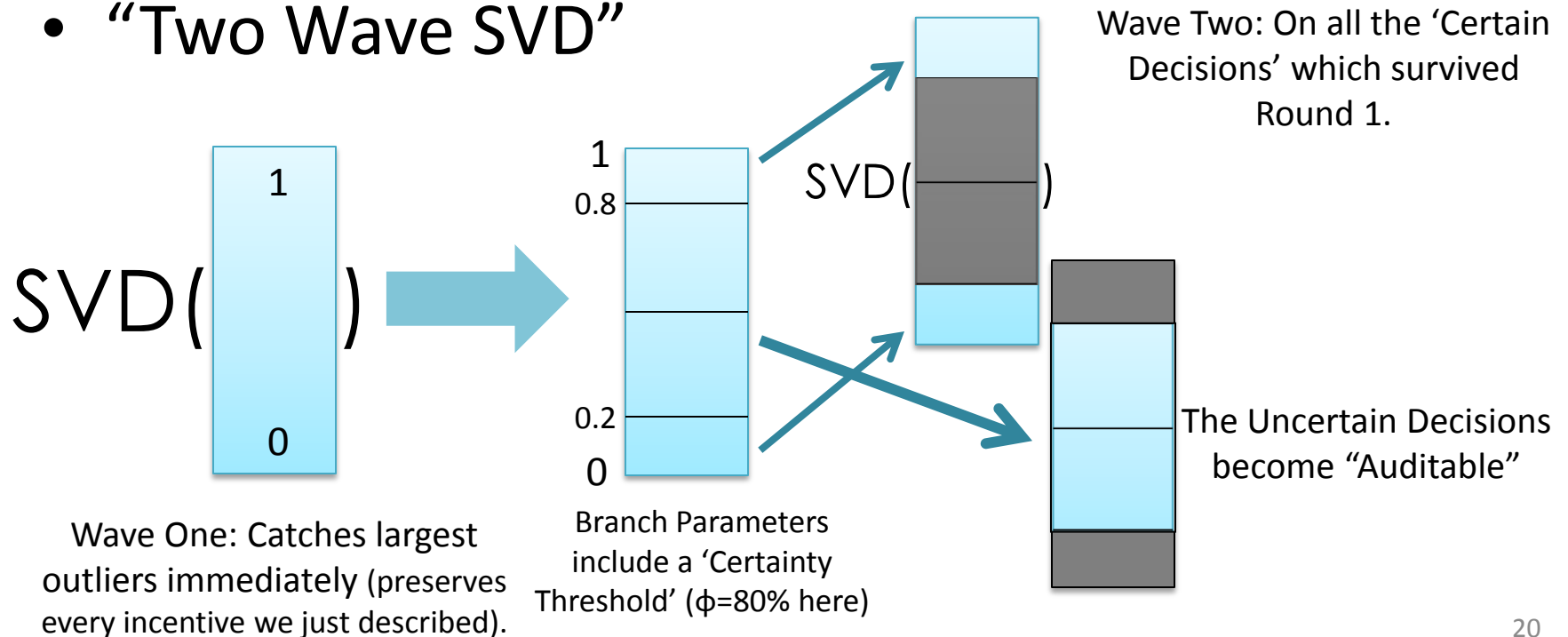   2. Previously, your 'investment' was low.

Going Beyond 50%

What if exceeds and

someone buys up >51% of the VoteCoins?

Could execute same 'lie attack', only larger (51/100th cheaper).

Preventing the >51% Attack: 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"

SVD( )

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

Branch Parameters include a 'Certainty Threshold' (ϕ=80% here)

1
0.8
0.2
0

SVD( )

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

The Uncertain Decisions become "Auditable"

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).
3. More general: Vote on Ballots from multiple Branches and Time Periods.
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).
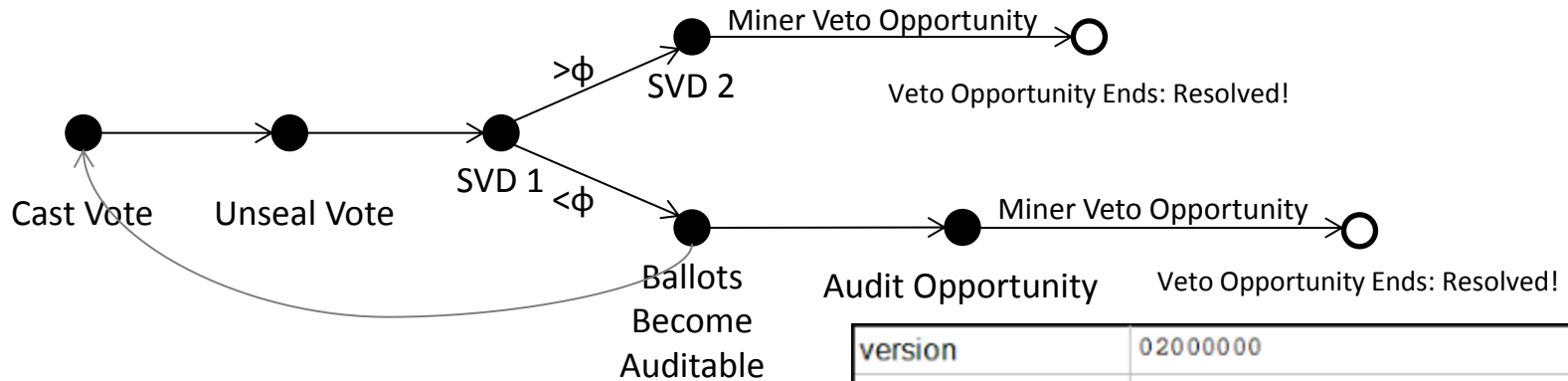

Cash Branch

Owners ("Cash")
("Bitcoin")
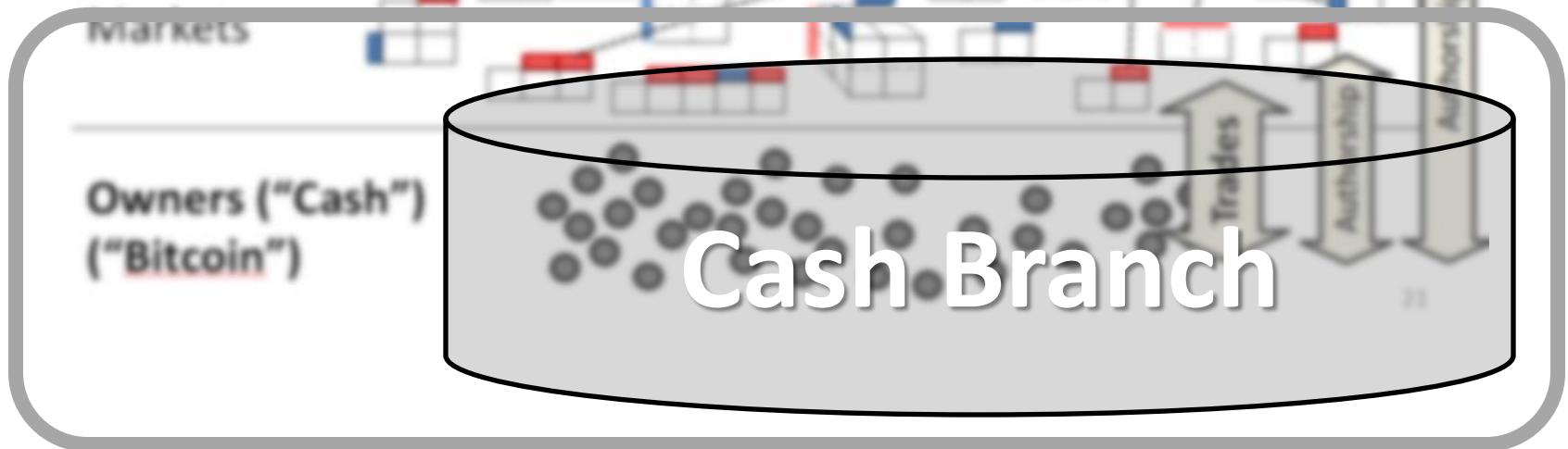
Result: By 'sticking it out', an honest minority of Voters can earn a superior return (50% instead of <50% [by definition, they are a minority]).

Miner Veto Seals the Deal

- 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' (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 <u>even more inconvenient</u> for liar-Voters, by using a Miner Veto.

Preventing the >φ Attack

Cast Vote — Unseal Vote — SVD 1

>φ SVD 2 — Miner Veto Opportunity

Veto Opportunity Ends: Resolved!

<φ Ballots Become Auditable — Audit Opportunity — Miner Veto Opportunity

Veto Opportunity Ends: Resolved!

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c817010000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833

+

Ballot Vetos	
Audit Vetos	
Branch Vetos	

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

- Miner Branch-Veto
  - 95% Branch Veto = Branch's future decisions can move to a different Branch (with permission of Decision-Author).
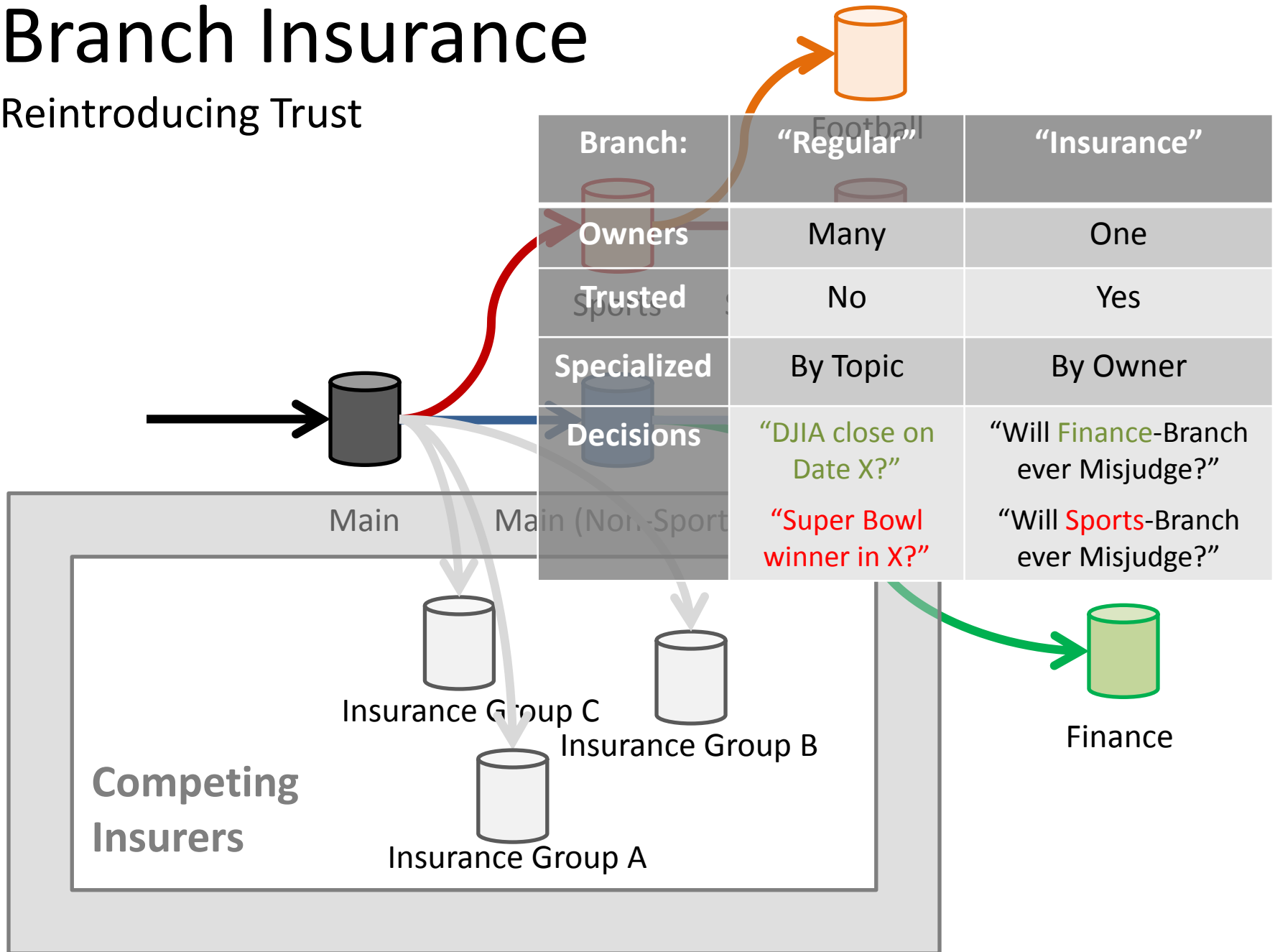
23

Can it get EVEN BETTER??

Branch Insurance

Reintroducing Trust

Branch:	"Regular"	"Insurance"
Owners	Many	One
Trusted	No	Yes
Specialized	By Topic	By Owner
Decisions	"DJIA close on Date X?" "Super Bowl winner in X?"	"Will Finance-Branch ever Misjudge?" "Will Sports-Branch ever Misjudge?"

Insurance Group C

Insurance Group B

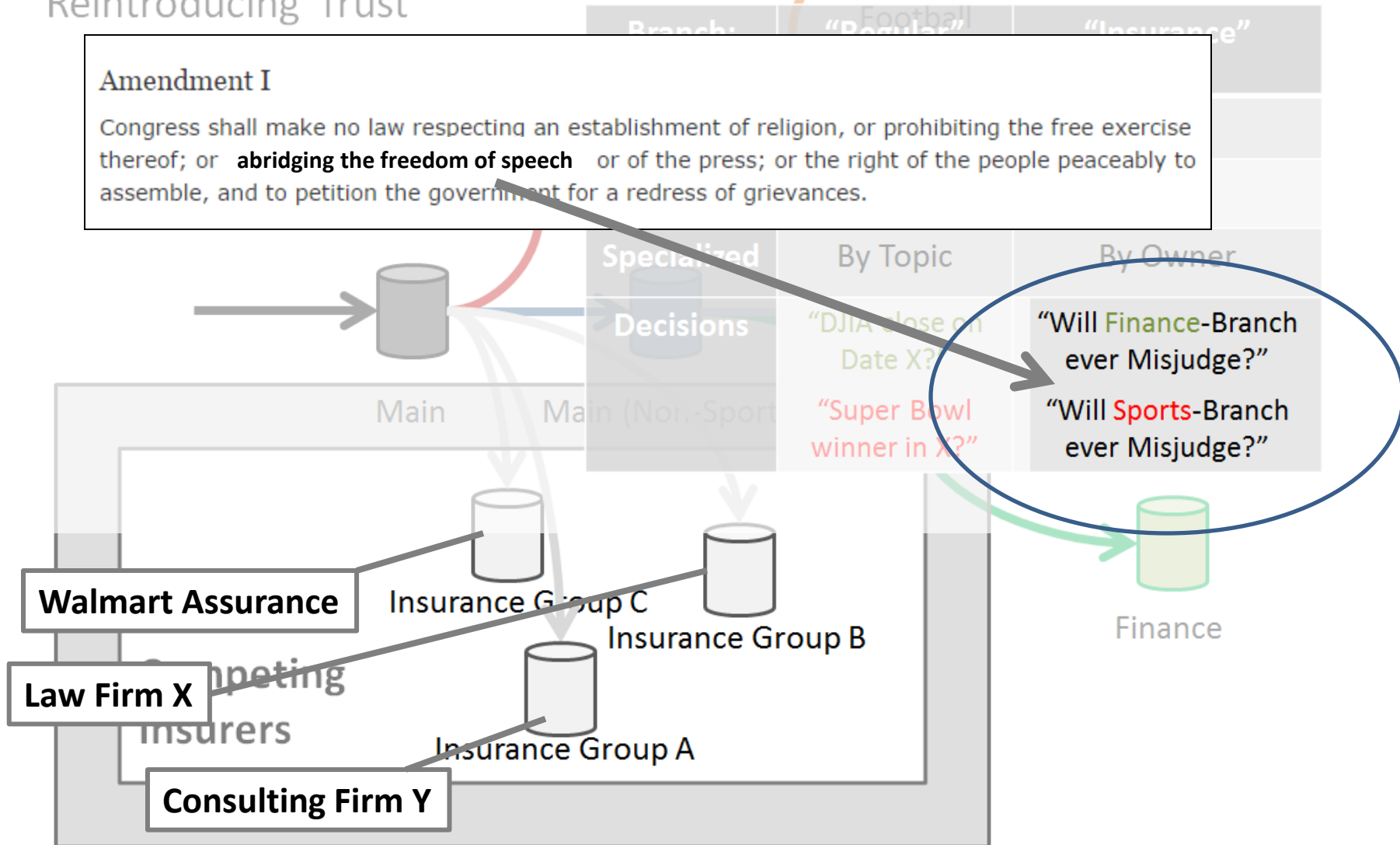Insurance Group A

Finance

Competing Insurers

New Business Opportunities
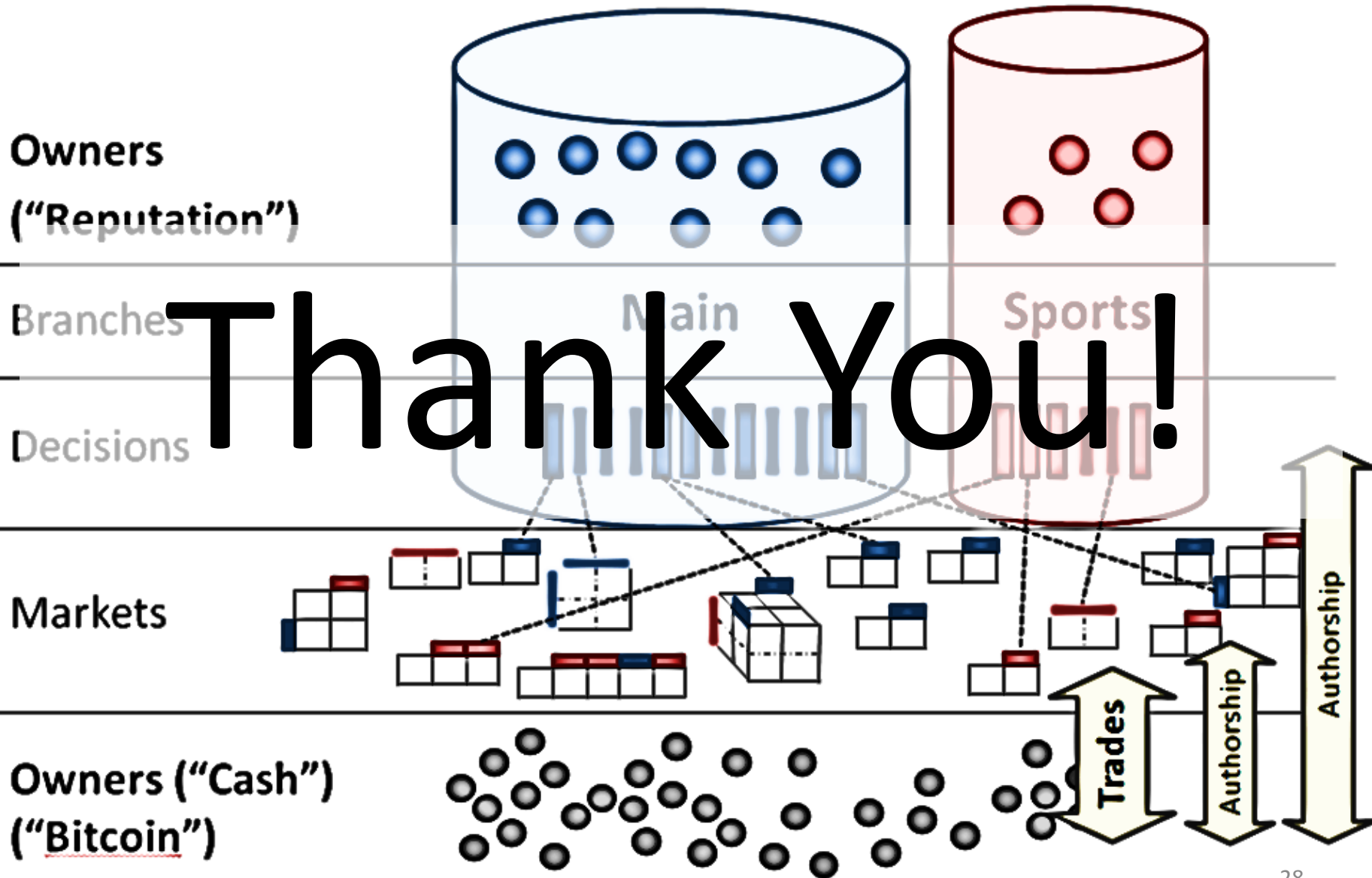## Guarantees Enforced by Legal System

Reintroducing Trust

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or **abridging the freedom of speech** or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Specialized Decisions

By Topic

By Owner

"DJIA close on Date X?"

"Will Finance-Branch ever Misjudge?"

"Super Bowl winner in X?"

"Will Sports-Branch ever Misjudge?"

Main

Main (Non-Sport)

Walmart Assurance

Insurance Group C

Insurance Group B

Law Firm X

Competing Insurers

Insurance Group A

Consulting Firm Y

Finance

Truthcoin Graphic: Two Coin Types

Thank You!

Owners ("Reputation")

Branches

Main

Sports

Decisions

Markets

Owners ("Cash") ("Bitcoin")

Trades

Authorship

Authorship

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)
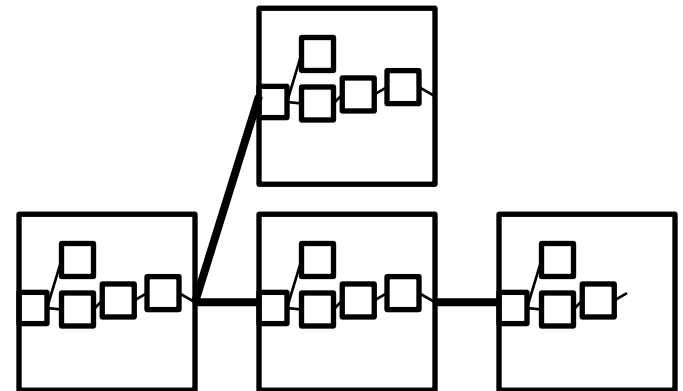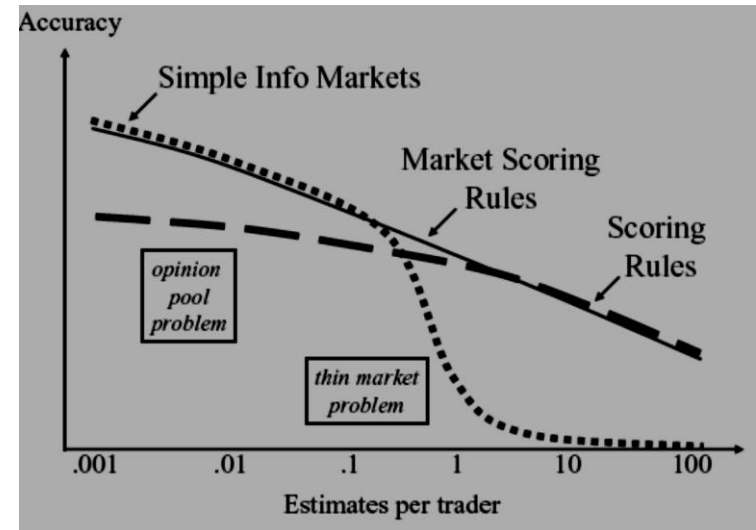
The Applications Slide

- Multidimensional Markets
  - Optimal Advice ("futarchy")
  - Boost econ growth (CEOs)
  - Financing Public Goods
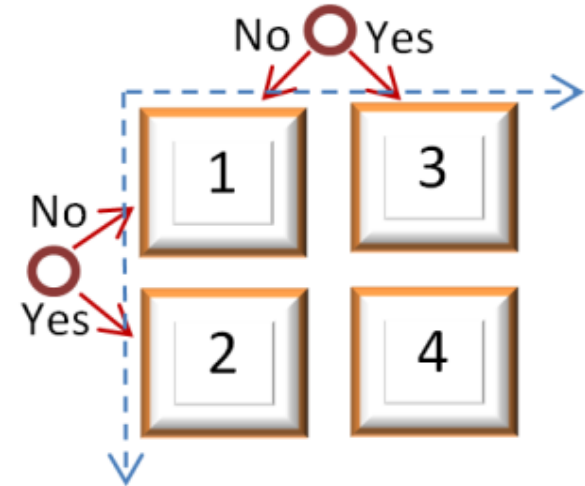
- Smart Contracts
  - (With Selling Disabled) = "Lockbox"
  - Public Goods without Coercion (T-DAC)
  - Focus On: the result, not the computation.