Truthcoin

Trustless, Decentralized, Censorship-Proof, Incentive-Compatible, Scalable Cryptocurrency Prediction Marketplace

Paul Sztorc[1]
truthcoin@gmail.com
https://github.com/psztorc/Truthcoin
1M5tVTtynuqiS7Goq8hbh5UBcxLaa5XQb8
Version 1.3 – 8/24/2014

Abstract. Where Bitcoin allows for the decentralized exchange of value, this paper adds[2] the decentralized creation and administration of Prediction Markets (PMs). A proof-of-work blockchain collects information on the creation and state of PMs. An incentive mechanism attempts to guarantee that selfish users resolve outcomes accurately, and bear the economic costs and benefits of the trades they execute and PMs they create. Users can create PMs on any subject, or trade anonymously within any PM, and all PMs enjoy low fees and permanent market liquidity through a LMSR market maker. Scalability and customizability can be achieved via 'branching' (controlled-fork of the VoteCoin set).

[1] Dedicated to Robin Hanson, for taking the high road.

[2] Previous versions of this paper emphasized "moving Bitcoin around" through the use of sidechains, or ideas of even greater technical complexity. To purposefully avoid this issue, this version assumes instead a new value-storage Altcoin (called "CashCoin"), which exists alongside the reputation-Altcoin used for voting (now called "VoteCoin"). This version may appear to be quite different even though the content is largely unchanged.

Article I. Overview

(a) General Strategy

(i) Central Facts

1) Blockchains allow for the programmable, censorship-resistant exchange of value-tokens.

2) While most marketplaces require physical infrastructure to facilitate the trade of physical goods[3], a Prediction Marketplace requires only the trade of digitizable information, and can therefore exist entirely in a software environment.

(ii) Assumptions (Justified in II.f)

1) Truthcoin inherits all of the assumptions of Bitcoin. For example: No malicious entity (an individual or perfectly-coordinated group) controls a large percentage of hashing power.

2) Users are greedy (prefer having more money to having less money), and lazy (prefer putting in low effort to high effort).

3) Upon the Voting Period of each Branch, there exist at least $\Lambda=150$ Decisions to be resolved in future Voting Periods. ("There are always future Decisions to resolve").

4) No malicious entity (individual or perfectly-coordinated group) owns more than $\Phi=75\%$ of the VoteCoins of a given Branch, nor does a single entity own more than 50% of the total CashCoins.

5) Search Costs (for a single Voter to learn the realistic answer to a Decision) are lower than Coordination Costs (for multiple Voters to collectively fabricate a false answer).

(b) Brief Overview of Components

(i) Truthcoin Blockchain

1) A proof of work blockchain with different block-creation/validation rules, containing two types of coin: "CashCoins" (which are functionally identical to Bitcoin) and "VoteCoins".

   a) A CashCoin user can ignore VoteCoins and PMs entirely if he or she wishes.

   b) An incentive mechanism imposes a cost-of-ownership for VoteCoins (because voting consumes time and effort), making a VoteCoin address more "employee ID" and less "checking account number". Therefore, VoteCoins do not interfere with the digital-scarcity or value-storage properties of CashCoins (which act as the permanent store of value).

[3] https://www.lme.com/trading/warehousing-and-brands/warehousing/approved-warehouses/

2) VoteCoins have the following properties:

a) VoteCoins are used in a weighted-voting system.

i) Coins allow Owners to vote on the Yes/No/Scalar/Unknown status of statements called 'Decisions' (questions whose veracity is ultimately measureable at low cost).

ii) Coins allow one to proportionally collect half of the marketplace transaction fees (paid in CashCoin), as well as authorship fees.

b) Ownership of VoteCoins changes with voting activity.

i) VoteCoins are lost if Owners fail to vote, or cast votes differing from the consensus.

ii) VoteCoins are gained if Owners vote on neglected Decisions (those with few votes), or owners vote with the consensus on disputed Decisions (those where the outcome is not unanimous).

(ii) Automated Market-Maker

1) Figuratively, a "trader" who accepts the other side of any and all PM-trades, and understands the creation (pre-trading, pre-event), maturation (post-event) and expiration (post-event, post-trading) of Markets. Literally, a protocol for updating market prices based on trading activity.[4]

2) Has blockchain-properties (constant mining, P2P network) which allow for an always-on, (hopefully) high-speed, censorship-resistant trading environment.

3) Utilizes LMSR technology[5] to ensure permanent market liquidity (such that markets have a tradable market price at all times [even when volume and open interest fall completely to zero]). Low liquidity has been a problem on many implementations, including InTrade and Predictious, and may have prevented the formation of crucial network-effects.

4) Collects, stores, and pays out balances, without human-error or mismanagement.

(iii) Incentive Mechanism

1) Authors

a) Any user can create a prediction market ("Author a Market") about anything.

b) Authors only have an incentive to write Decisions whose outcome (they believe) can be easily assessed by Voters.

c) Authors only have an incentive to create Markets if they anticipate sufficiently-high trading volume (i.e. the issues which would most-benefit from a prediction market).

[4] https://github.com/psztorc/Truthcoin/raw/master/docs/LogMSR_Demo.xlsx
[5] http://www.eecs.harvard.edu/cs286r/courses/fall12/papers/mktscore.pdf

d) Authors completely avoid the (prohibitive) cost of convincing Traders of their trustworthiness.

2) VoteCoin Owners ("Voters")

a) Voters have an incentive to maximize the long-run trading volume of future PMs on their Branch, thus encouraging them to establish and maintain a reputable network.

b) Voters have an incentive to participate in the resolution of all Decisions.

c) Voters have an incentive to vote "the way they believe other Voters will vote", which itself is contrived to be "an accurate description of reality" (see 'Voting Strategy').

3) Traders

a) Any CashCoin user can trade on any PM without directly interfacing with VoteCoins at all. VoteCoins are the "employee layer", not the "customer layer".

b) Traders have an incentive to set the market price to "their personal expectation of the probability of the event taking place", revealing that information to the public.

c) Traders enjoy an absence of counterparty risk (but instead must endure technical risk).

4) Bitcoin Miners

a) Miners have an incentive to mine blocks, as the marginal cost for doing so is zero (merged mining allows reuse of Bitcoin hashes). Were Bitcoin to disappear, the marginal cost/benefit of Truthcoin-mining would equal that of Bitcoin-mining (and mining would therefore continue).

b) Miners have an incentive to include every trade and transaction into a block, as this maximizes dividend revenue and therefore market capitalization of the coins. Miners cannot even read Markets or Votes until they have already been included in blocks, making this process censorship-resistant.

(c) Extensible (Scalable, Customizable) Design

1) Accompanying software is open source.

2) Truthcoin allows for the creation of controlled forks of the VoteCoin set ('Branches') enabling growth of the scope and quantity of Markets, specialized judging, choice of different fee and timing parameters, etc.

Article II. How it Works

(a) Truthcoin Blockchain and Coin Types

1) The Truthcoin Blockchain is a Bitcoin-inspired proof of work Blockchain with different block validation rules. Generally, the Bitcoin blockchain is designed only to hold information about the ownership and transfer of a single coin-type, but the Truthcoin blockchain is designed to contain information not only about the transfer of two coin-types, but also about the existence and state of Prediction Markets.

2) The Truthcoin blockchain contains two types of coin:

	CashCoins ("Bitcoin")	**VoteCoins**
1	Accounts always retain a constant amount of unspent coins.	Accounts may either gain or lose unspent coins (based on voting activity).
2	Private keys only sign messages that transfer coins to a different account.	Private keys can either sign messages which transfer coins to a different account, or Votes (which influence the Outcomes of Decisions).
3	To mimic the experience of gold and provide an objective initial distribution of coins, new coins are periodically introduced in each block by miners, asymptotically approaching 21 million total coins.	To mimic the experience of reputations and fulfill the requirements of voting, the total quantity of coins exists immediately, and is constantly redistributed based on voting behavior.
4	Expectation of huge number of addresses, one per transaction.	Expectation of a maximum of 10,000 addresses, most of which will vote, not transact.
5	Coin values are analogous to a saved quantity of gold.	Coin values are analogous to reputation, influence, or shares of a corporation.

(b) (Decentralized, Incentive-Compatible) Calculation of Decision Outcomes

*(i) Terminology (**figure 1**)*

1) **CashCoins** – A cryptocurrency which is functionally equivalent to Bitcoin, yet with the added benefit that it can interface with Truthcoin prediction markets.

2) **Decisions** – Questions that must be resolved by Voters. These partition the State-space of a prediction market, and are defined by items such as 'event text', 'event date', 'tags', 'author', etc.

a) Truthcoin supports two 'types' of Decision:

i) Binary (Boolean) Decisions: $x \in \{\{0, .5, 1\}, NA\}$

a. Example 1: "Will Hillary Clinton be elected US President in 2016?"

b. Example 2: "Will the NYSE:DJIA closing price ever rise above 20,000 USD/Share in 2017?"

c. State ".5" denotes that a Decision is irresolvable/unobservable (its veracity cannot easily be measured). This has adverse economic consequences for the Decision's Author.

ii) Scaled (Scalar) Decisions: $x \in \{ [x_{min},\ x_{max}],\ NA\}$

a. Example 1: "How many electoral college votes will Hillary Clinton receive in the 2016 US Presidential election (if Hillary does not run, select 'zero')?" [x_{min} = 0, x_{max} = 538]

b. Example 2: "What will the NYSE:DJIA closing price be on January 1st, 2018 (USD/Share)?" [x_{min} = 8000, x_{max} = 24000]

c. x_{min} and x_{max} must be set in advance. Having a Decision expire at or near a bound has adverse economic consequences for the Author of any Market using this Decision.

d. To notate an irresolvable Scaled Decision, one casts a vote for x_{NULL}, which is selected at the time of the Decision's placement into a Vote Matrix, and alternates between x_{min} and x_{max} .

b) At any given time, each Decision will have a 'status' of the following:

i) Active: The Decision has just been created. Decisions of the 'active' status would be likely to be used to create Markets, and those Markets would be actively traded.

ii) Matured: When a Decision is created, its Author sets a 'date by which the information will become available'. After this date has passed, the Decision will enter a Ballot and be Voted on for resolution. During this vote the Decision has a status of 'matured'.

iii) Disputed: If Voters cannot sufficiently agree on the Decision's outcome, the Decision remains un-resolved and gains this status.

iv) Resolved: If Voters do sufficiently agree on the Decision's outcome, their agreed-upon value becomes the final value of the Decision, and the Decision's life-cycle is now over.

3) **Markets** (figure 2) – The lifeblood of the Truthcoin project, Prediction Markets allow anyone with CashCoin to buy and sell shares representing states of the world, and thereby speculate on and profit from selected events. This voluntary, "win-win" speculation aggregates and summarizes information for use by the public.

   a) States: Markets partition the world into 'states' or "mutually-exclusive possible descriptions of reality". When traders buy and sell shares, these shares are of a single Market State.

   b) Status: Markets, like Decisions, exist in one of several statuses:

      i) Trading: In this status, a Market allows traders to buy and sell shares through an automated market-maker. A Market would be in this status from the moment it is created until its Decisions are voted on.

      ii) Disputed: If any of a Market's Decisions attain 'Disputed' status, the Market attains the Disputed status. No one can buy or sell until the Dispute is resolved.

      iii) Audited: If a Market remained in a Disputed state and became audited, the Market would enter this state. Shares can be sold (redeemed) but the payoff formula is slightly more complicated (see Appendix III). Buying is also disabled (for simplicity and consistency).

      iv) Resolved: If all of a Market's Decisions were successfully resolved, the Market enters the resolved state, which disables buying and replaces selling with redeeming.

4) **Branches** – Although all Markets are available to all users, Decisions are partitioned into clusters called 'Branches' based primarily on topic. Each Branch has its own set of VoteCoins, its own Decisions, and its own Voting Period.

5) **VoteCoins** – The second cryptocurrency type in Truthcoin. Unlike with CashCoins, ownership of VoteCoins is a liability as well as an asset. Owners are expected to use their coins to vote on the status of each Decision.

6) **Voting Period** – The length of time between two consecutive votes on the same Branch.

7) **Vote** (figure 3) – A Voter's selection (for Binary: a selection from { {True, False, Unknown}, Missing}, and for Scaled: a selection from {[min, max], Missing}), of what the Voter believes would match the Decision to its real-world Outcome. The default value is Missing, which indicates "No response from the Voter".

8) **Ballot** – A set of the current Voting Period's matured Decisions. For this set of Decisions, each Voter must cast a Vote with his report/opinion on the resolved value. Notice that Ballots are defined by the maturation time of their Decisions, not by their organization or use within Markets (and, crucial to the core design, Ballots contain the Decisions of many different Markets).

9) **Vote Matrix** – The matrix created by stacking the Ballots (of a particular Voting Period) by row. The columns of the matrix correspond to Decisions.

10) **Outcome** – The final, calculated result for each Decision, as determined by the consensus algorithm.

(ii) Timeline

1) Decision Added – Markets require Decisions, making this the very first step. A "Decision Author" would select the topic-appropriate Branch, submit the hash of the Decision (and a payment), and wait for the hash to be included in a block.

2) Market Added – With one or more Decisions added, a "Market Author" can create a new prediction market, by submitting its hash, number of states, and payment, and waiting for the hash to be included in a block. The hashed data must include State dimensionality, but the component Decisions can remain hidden until after the Market has been included in a block.

3) Trading – With the Market built, it can now be advertised to traders, who buy and sell shares of the states of the Market (for example, "Buy 3.8 of State 2 of Market m16j9…").

4) Event(s) Occur – At this point in the timeline, the event(s) relevant to the Decision(s) of the Market occur and become observable.

5) Decision(s) Mature(s) – At this point, Voting is done on the Outcome of all the Branch's Decisions which matured in this Voting Period. Voters encrypt, sign, and broadcast a Ballot which contains their Votes and a new public key (for which they have the corresponding private key). Critically, Voters have the option to change their Ballot at any time and for any reason during this period (for example, to update the new public key). Only the latest included Ballot stands.

6) Votes Decrypted – As this phase begins, the Votes have been included in the blockchain. No more voting can take place, and the VoteCoins are now temporarily frozen. Voters reveal the private key used to encrypt their votes in (5), allowing these votes to be decrypted and read into the consensus algorithm.

7) Decisions Resolve – Votes are run through the consensus algorithm to establish the Outcome of each Decision in the Ballot (each Decision that expired during this Voting Period). Simultaneously, the consensus algorithm allocates VTC to the new set of public keys according to RBCR (see below).

8) Redemptions – As a Market's Decisions resolve, the market-maker stops determining/broadcasting market prices, and instead uses the resolved-outcome of Decisions to actively fix shares to their final prices. Instead of sell, Traders "redeem" these shares for CashCoin.

9) Audits – A Market may have a Decision where Voters could not sufficiently agree on an Outcome. Depending on the Branch parameters, Voters may get a "do-over" next Voting Period. Failing to reach a consensus ultimately leads to an Audit. Every Ω = 6 months, disputed Decisions accumulate in an audit-Vote-Matrix. The very same consensus algorithm of (6) is used, but with the original very-specific set of voters (owners of Branch VoteCoins) replaced with a more-general set (all CashCoin owners). See Appendix III for more details.

(iii) Consensus Puzzle Piece 1: Singular Value Decomposition

1) The mathematical process underlying the calculation of Outcomes is the matrix factorization known as singular value decomposition (SVD). Our application performs SVD on the Vote Matrix, which has dimension n Voters (VoteCoin Owners) by m Decisions.

2) The role played by SVD in RBCR is similar to the role SVD plays in the statistical technique of principal components analysis (PCA). It may be conceptually helpful to think of the RBCR function as a weighted PCA.

3) One purpose of SVD is to examine a matrix and reveal and sort its effects by influence. From SVD on the Vote Matrix we will extract the first (most informative) component. In parallel, (for those things we cannot observe ourselves), what we decide to be 'true' is the figurative 'common denominator' among many opinions, each of which could be (and likely is) biased, incorrect, deceptive, or otherwise non-representative. We extract "the story we believe to be most generally consistent" from the multiple eyewitness accounts we experience throughout our lives; supportive friends, deceitful enemies, propagandist politicians, sensationalist news anchors, impractical professors, overcautious parents, reckless children, leftist Left-Party-Members, and right-leaning Right-Party-Members, together co-author our version of "the story most consistent with their combined points of view".

(iv) Consensus Puzzle Piece 2: Coordination Games

1) Imagine a game in which you and a randomly selected individual are each teleported to random locations in the same random city to play a game. The object is simple: you must find each other within 24 hours.

2) What factors would influence your behavior?

   a) Search Costs: You would like to minimize the search costs of Player Two, who is looking for you. Many places would have costly accessibility, such as night clubs (only open at night), or hotel rooms (which cost money). More importantly, a basement, or a forest, would increase the search burden of Player Two prohibitively. Ideally you'd find a news crew, or call emergency services (who are open 24/7, and already serve the function of 'coordinators'), early in the game. Making a gigantic sign that says 'Are you

also looking for someone?' is costly but potentially very beneficial. Densely populated centers are better than empty, windowless rooms.

b) Salience: The concept of salience refers to a kind of psychological perception cost. A single dent in a smooth wall, the largest words of a brand label, a bright orange vest against a grey background, are examples of 'salient' perceptions for which the mental costs are low. Especially salient perceptions can even have a negative cost (one must exert effort to ignore the message), as in advertising. In our game, locations would acquire salience by being uniquely functional or definitive. Economist Thomas Schelling found that the most common verbal response for the NYC version of this game would be "noon at the information booth at Grand Central Station"[6] for the simple reason that (out of all locations in NYC) it most functions as a meeting place. Reportedly, the distant second was the (then) tallest building in NYC (in terrain there are usually many lowest points but only a unique highest point, and height has always been useful for vision [reduced search costs]), and the third most frequent response was the Statue of Liberty (a unique, large, visible, iconic place).

3) In general, humans usually play (and win) these games every day of their lives, by using awareness of shared human psychology to minimize shared mental costs.

*(v) Operationalized Coordination Using SVD (**Figure 4**)*

1) SVD does not handle missing values, so if any are present (despite a Voter incentive to attend to each Decision), they are temporarily filled by reweighting the votes of everyone who did vote and forcing the missing values to adopt this as their vote (see Appendix I). This produces $V_{n\times m}^{filled}$, the completed Vote Matrix.

2) To measure coordination, we use the first column of the U matrix extracted from $SVD(V_{n\times m}^{filled})$. This column represents the degree to which *each voter* varied his or her votes with those of *a theoretical voter maximally representative of the covariance across all votes and Voters* (SVD automatically ranks the columns by influence, hence the choice of column 1).

3) $c_{n\times 1} = U_{,1}$

4) Column *c* is then adjusted via scalar addition, such that the most deviant observation becomes zero. This is done either by *addition of minimum* or *subtraction of maximum*, as determined by a simple rule: whichever adjustment produces the outcomes which minimize total squared difference from those using the weights of the previous period.

5) $c^{adj} = (c_{n\times 1} + a^{*})$

6) This vector is then normalized such that all values are positive and sum to 1. The result is called the 'reputation vector'. However, before normalization a correction is applied:

[6] http://en.wikipedia.org/wiki/Focal_point_%28game_theory%29

multiplication by previous period reputation vector over its mean. This simple correction ensures that reputation-use is additive (making it impossible to increase or decrease one's influence by separating or pooling the same amount of TRU among several accounts).

7) $N(x) = \frac{|x|}{\sum|x|}$

8) $r_{t+1,n\times1} = N(\, c^{adj} \times \frac{r_{t,n\times1}}{mean(r_{t,n\times1})})$

9) Outcomes for each Decision are calculated. Binary Outcomes simply multiply over the vote matrix (a weighted average), Scaled Outcomes use a weighted median.

10) $o_{t+1,1\times m} = \left(r_{t+1,n\times1}\right)^T \times V_{t+1,n\times m}^{filled}$

(vi) Reputation Based Coin Redistribution (RBCR)

1) After a round of voting, Branch VoteCoins are redistributed among all of the VoteCoin accounts. We know where to send the redistributed VoteCoins, as each Ballot contains a destination address.

2) For each account, smooth (weighted average) the value of the previous reputation vector with the value represented by the new reputation vector. For example, I suggest α=.20 (weighing the new value 20% and old value 80%). This parameter represents the dynamism of the voting environment: too low and bad agents can coast on inertia without punishment, too high and the network becomes volatile and neurotic.

(vii) Temporal Economics of RBCR

1) RBCR ensures that, even in one single voting round, each Voter has one incentive to vote realistically: minimal effort. Information search costs and psychological effort will be lowest for the Realistic Ballot.

2) However, the economics of multiple voting rounds adds a second (and more important) incentive to vote realistically: revenue maximization.

3) Fees and dividends:

   a) Authors pay, in CashCoin, Listing Fees when creating a new Market.

   b) Traders pay Trading Fees (in CashCoin) while making trades on Markets.

4) These fees accumulate and are gradually paid out to VTC Owners.

5) The gradual payout:

   a) Rewards past conformity and provides an incentive to get and keep a high reputation.

b) Offsets the constantly-present incentive to be dishonest today (and defraud traders by manipulating the Outcomes).

c) Encourages other behaviors which maximize the future expected trading volume (good judgment, entrepreneurship).

*(viii) Voting Strategy (**Figure 5**)*

1) A coordination game is not a perfect model for the incentive scheme behind Truthcoin, primarily because only laziness prevents a malicious coalition from attempting to communicate and actively coordinate. However, votes are encrypted to prevent any voting commitments from being credible, and Truthcoin actually provides a strong incentive for Voters to lie (to each other) about what they plan to do. Here we rely on the assumption that the search costs to accurately resolve a Decision are very low (lower than the cost of active coordination). The Cheapest Ballot will then be the Realistic Ballot, as all fully-coordinated Ballots would provide the same benefit (the Realistic Ballot has the optimal (lowest cost)/(same benefit) ratio). As some agents will be most likely to select the Cheapest (Realistic) Ballot, all agents will converge to that Ballot simply to achieve coordination. The Realistic Ballot thus becomes the coordination point.

2) Secondly, availability of the VoteCoins on the open marketplace ensures that they are allocated efficiently (in other words, those who most-believe-in and are-most-dedicated-to the project will be VoteCoin owners and therefore Voters). Nonbelievers are likely to also be non-owners. Those who lose the faith would neither neglect nor interfere with the project, as they can instead just sell their coins.

3) Although an attacker with an extremely high proportion of a Branch's VoteCoins could attempt to alter the judgment process of a Decision for personal gain, any attack with less than $(1-\Phi)=35\%$ of the voting power will fail outright, exposing the liars to huge VoteCoin losses.

4) An attack with greater than $\Phi=65\%$ of a Branch's VoteCoins would be able to successfully alter the state of all Decisions on that Branch as he or she chooses (and 'profit' from RBCR as well). Indeed, it is because this is the case that the project is capable of determining anything about reality at all. However, a "$>\Phi$ Ownership Attack" is unlikely for several reasons: stake, trust, and coordination.

a) Stake - As VoteCoins cannot be simultaneously spent (transferred) and used to vote, an 'Ownership attack' would collapse the market price of VoteCoin/USD before anyone could liquidate. As a Branch grows, adding more Decisions and trading fees, the market capitalization of the VoteCoins of that Branch (a function of trading fees) would also grow, making a $>\Phi$ attack incur a higher and higher opportunity cost (as an attacker forgoes the money he could acquire by instead selling his VoteCoins).

b) Trust - Even an attacker-coalition which believes it has, say, 75% of the votes faces almost certain failure from a cascading fear of double-agents. A lying coalition involves

coordinated deception to make a quick buck, and yet, by (costlessly) deceiving the coalition and returning to the truth, hypothetical "double-agents" can not only employ deception for a quick profit (against the attackers) but also retain the long run value of their coins. Even the leader of the 75% coalition has an incentive to betray his own strategy to scam his own coalition. It is paradoxical to require a coalition of liars to communicate truthfully, in what amounts to a massive prisoner's dilemma.

c) Coordination - Lastly, a >Φ% coalition may fail to coordinate perfectly: members may have different priorities on which Decision they would most like to distort, and this difference of priorities provides incentives that unwind the entire distortion strategy.

i) For a strategy to be profitable, it must profit tremendously during the attack, to offset the loss of future revenues and coin value. To achieve a great profit quickly, the attack must distort many Markets (as each Market has a finite loss). Operationally, this entails the purchase of cheap shares (of the realistically unlikely states) which will later be expensive after the attacker-coalition re-writes history.

ii) To succeed, the coalition must agree on the Market(s) to distort, and the False Outcome(s) they would like to use to replace the Realistic Outcome(s). Ideally, they would also agree on the total amount of money they expected to take in, and the allocation of those revenues to each participant. However, it will not be possible to manage the allocation of the revenues from the attack, because as the target Markets and Outcomes become known, participants have an incentive to buy shares of those Outcome-States until they are priced at the attack's target value. Each trade changes the price, making it practically impossible for the coalition to end up with a coordinated payout. Absent a credible commitment to reimburse (which is unlikely to exist among a coalition of liars), the coalition will have different priorities for which Decisions to distort.

iii) The incentive mechanism pays Voters to coordinate with each other as much as possible. Therefore, those set on converting a certain Decision would want to play realistically for all the other Decisions (that they are less-interested in), absent any convincing evidence that these uninteresting Decisions would be successfully distorted (which, again, is unlikely to exist). In other words, because RBCR considers the entire Ballot, not just the votes on one Decision, a lying coalition must be extremely complete in its coordination, even though they have every incentive to only partially-coordinate.

iv) As a clarifying example, when $\Phi=\{0\}$ (no audits) and $\lambda > 10$, if there are two Voter-groups, one realistic and one whose members vote completely at random (zero coordination), the honest group needs only to control a tiny plurality, around 5%, of the votes in order to ensure that every single Decision is resolved accurately (and that they profit handsomely from RBCR).

(ix) Measuring Oracle Risk

1) The efficacy of these protections is actually tradable and measureable, which adds a few minor layers of protection and enables skeptics and researchers to understand the risks.

2) Observe this elaboration of a section of the Truthcoin timeline:

Phase	1 (Trading)	2 (Ex-Post Trading)	3 (Judgment)	4 (Settlement)
Begins When	Decision/Market Authored (Trading Begins)	Event Occurs	Decisions "Mature" (Judging Begins)	Market "Resolves" (Judging Ends)
Plausible Duration	6 Months	2 weeks	2 weeks	N/A (Forever)

3) For example, a Market authored in January 2014 predicting Hillary Clinton to win the 2016 US presidential election (on November 8th) may begin its judging activities on December 1st, and not conclude them until Dec 15th. Each phase would respectfully last 34 months, 23 days, and 2 weeks.

4) Note the duration of Phase 2 (23 days), during which the real-world event has occurred but no outcome-resolution activity has yet taken place.

5) Temporarily assuming a) no time value of money and b) absolute certainty that the Voters will rule correctly, one would assume post-event prices to converge quickly to their post-judgment price (for example, a "1$ if Hillary wins in 2016" contract would converge to about 1 dollar at more or less the exact moment Hillary's opponent conceded defeat).

6) If assumption (b) were violated, and there were some risk of unrealistic judging, the holdouts refusing to sell failed shares would produce a residual nonzero price, the interpretation of which would be the probability of misjudgment (or 'oracle risk'). During Phase 2, Traders can literally trade-off this specific risk amongst themselves (VoteCoin owners may be especially likely to make these trades), and we can use this metric to calibrate improvements.

(c) Mining Activity

1) Miners are paid, in CashCoin, to advance the Truthcoin blockchain. This provides an incentive for Miners to keep the value of CashCoins high. The marginal utility of CashCoin over Bitcoin is its ability to use PMs, so CashCoins will be valuable (and Miners rewarded) when the network is functioning properly.

2) Merged mining allows use of the existing Bitcoin infrastructure.

3) Miners cannot censor the creation of prediction markets. Adding a new Decision or Market requires only obscure details (for example hash, date / block number, and payment); the literal content of either may be withheld for several blocks.

4) Miners cannot censor votes, as they will be unsealed over a thousand block period ($\tau_{unsealing}$ = 1 week = 1008 blocks).

5) Optionally, we could introduce anti-vote-censorship measure and force blocks with relatively low cumulative participation to be rejected by nodes.

   a) Each block contains a scalar called 'participation', which is essentially the proportion of the total network of Voters that submitted (on time) their votes during the previous Voting Period.

   b) Each block also calculates the cumulative participation, the sum of participation over the previous, say, 20 blocks.

   c) Blocks are ignored if there exists another orphan chain with:

      i) All valid blocks.

      ii) Similar total proof of work.

      iii) Significantly higher cumulative participation.

   d) This provides censorship-resistance, because someone wishing to exclude certain votes would have to do so consistently across several blocks, which would substantially lower the cumulative participation on that chain.

   e) Miners which innocently overlook a vote can simply include it in the very next block, which would only slightly lower the cumulative participation of that chain. Thus, this rule only discourages exclusion of votes across several consecutive blocks.

   f) Orphaned blocks present a perfect opportunity to 'break' a "voter-exclusion attack", as the miner of an orphaned block, by including all censored votes in the block following his orphan, he has a good change of un-orphaning that block.

   g) Large holders of VoteCoin cannot reliably execute selfish mining[7] (by withholding their own votes in an attempt to boost their block's participation) unless they also control a substantial quantity of hashpower, because cumulative participation is not only a function of the votes included in each block but also of total number of blocks found.

6) Miners are unlikely to block trades, as they collect transaction fees for every tx. Moreover, Owners/Voters collect trading fees off of each trade (and Miners have every incentive to make each coin as valuable as possible).

[7] http://bitcoinmagazine.com/7953/selfish-mining-a-25-attack-against-the-bitcoin-network/

(d) Authoring Activity

(i) This process is fully censorship-resistant. Any user can create a prediction market about anything, provided he or she is willing to pay for it.

1) Three separate fees, in two phases, are paid to successfully create a new prediction market (figure 6).

2) Phase 1 – Authoring the Decision(s)

   a) Fee 1: $K * Fee_{\mathrm{d}}$

      i) K is the number of Decisions required of the Voters.

      ii) As Voter 'participation' falls below a target (95%), Fee_{d} rises.

         a. Voters already have a strong incentive to vote on all Decisions (as falling behind the average participation results in VoteCoins lost to RBCR).

         b. However, if there are simply too many Decisions for Voters (as a group) to work on, participation will fall below target, and this fee will rise, making the creation of new Decisions more expensive for the same influx of trading fees.

         c. Conversely, if participation is above target, this fee will fall to encourage the creation of new Decisions, as they will now be cheaper for the same influx of trading fees.

      iii) Alternatively, assuming at least two competing Branches, VoteCoin owners could democratically change the fee as market conditions warranted.

3) Phase 2 – Adding the Market

   a) Fee 2: $b \log(N)$

      i) Seed capital required to 'make the market'.[8] Anyone can make a Market for trading, but without a cost there will be spam, waste, and needless redundancy. We therefore require all Authors to provide the small amount of seed capital required to ensure permanent market liquidity.

      ii) N is the number of states of the Market.

      iii) b is a user-chosen market liquidity parameter

         a. Low b, and this upfront cost is low, but the Market price is cheaply knocked around by Traders.

         b. High b, and this upfront cost is high, but the price is more expensive to adjust. This can reduce market sensitivity to large trades and encourage trading. As trading fees are a

[8] http://icmlmarketstutorial.pbworks.com/f/tutorial_combined_shortened.pdf

percentage of trading volume (not price activity), a higher b would translate to more trading fees (if price movements were similar).

c. Authors will likely profit by selecting b based on the expected number of traders in the market (popular markets can get away with a low b [as they are already robust to large trades], unpopular markets may benefit from a higher b, as a small trader pool would imply that these traders are less likely to find each other [in a grand coincidence of market-topic and timing] and would each therefore be more reliant on the market maker).

d. This value determines the initial account value of the Market. Although most of the funds required to ultimately pay the winning Traders post-resolution come from other Traders, this seed capital is required to make a liquid market.

b) Fee 3: $Fee_s * N^2$

i) N can potentially be very large, maximally 2^k, and each state requires the software to set aside a digital slot to count the outstanding shares, and use this data to calculate the market price. I anticipate this to be very cheap, but not free.

ii) Fee2 is arbitrarily small, collected only to discourage Markets with more than N=256 states (such Markets would tend to be completely incomprehensible to most humans).

iii) $f_3(N) = Fee_s * N^2 = f_2(N, b) = b\,log(N)$ @ $N = 8,\ b = 1$.

iv) Therefore, $a = log(8)/(8^2)$.

v) Alternatively, we could simply ban Markets with N>200 or so states.

(ii) Authors are entrepreneurial: they bear the costs of Market-creation, but also profit as a result of the Market's use.

1) Authors may cash out upon the maturation of the Market's Decisions.

a) The Market Author is the individual who sets the "Trading Fee Rate" (at, for example, 1% of trading volume). Authors get half of all trading fees (recall that Voters receive the other half).

b) For Scaled Decisions, Authors receive a refund on their unused seed capital. When the market resolves to an outcome at a bound (minimum or maximum, as all Binary Decisions would), all the seed capital is used, and the refund is zero, but otherwise this refund may be sizable.

c) Authors therefore act as entrepreneurs.

i) Authors bear the total lifetime economic costs of a Market, by paying upfront fees for the human judging activity required, the working capital required to make a permanently liquid market and entice Traders, and the technical resources required to administer the market system.

ii) Authors bear also the cost of enforcing the Market. By splitting trading fees with Voters, Authors transfer that judgment to an impartial third party, and eliminate the requirement that Traders trust Authors.

iii) Conversely, Authors receive a payout proportional to the popularity and usefulness of the Market. Highly traded Markets serviced more trades, aggregated more information, and were more economically useful, and therefore generated a higher pool of trading fees with which to reward the Author.

iv) The total lifetime volume of the InTrade Barack 2012 Market was 4.1 million shares, expiring at nearly 2.5 million shares at $10 per share.[9] Although the sum of all marginal updates to the market price is unknown, the trading fees for this Market would likely have been substantial.

2) Ensuring Measurable Market States

a) Recall that the Branch votes (reports signed by VoteCoins) are scored on Consensus – i.e. how well one Voter's votes agreed with those of other Voters. Consensus relied on the assumption that reality was measurable at low search cost.

b) For Binary Decisions, recall that it is possible to coordinate on any of three values: 0, 1, or .5 ("No", "Yes", and "Unknown"). Coordination on the value of .5 indicates that Voters (believe that other Voters believe)$^{\infty}$ that the True/False status of the given Decision is ultimately non-resolvable. This could indicate that the Decision text is blank, illogical, confusing, relies on inaccessible information or is otherwise unreasonable in its info/search demands. Resolving to this value forfeits the Decision Author's trading fees, which can instead be claimed by Traders. In short, this option provides a fail-safe which guarantees that search costs are low: lazy Voters will seize any opportunity to turn on you if they can (and they can if your Decision is too confusing).

c) For Scaled Decisions, recall that the Author receives some of his market subsidy (Fee 2) back, provided his Decision has not expired near a bound. However, recall also that Voters have an incentive to set unmeasurable Scaled Decisions to a specific and predetermined bound (either the min or max). Thus, Authors of Scaled Decisions also have an incentive only to write Decisions which are measureable.

[9] https://www.intrade.com/v4/markets/contract/?contractId=743474

(e) Trading Activity

1) The central goal of a prediction market is to have Traders pay for shares which they either a) sell either at a future market price, or b) upon maturation of the Market, redeem at a non-market price which is instead a function solely of the prediction's outcome (for example, "worth $1 if Hillary Clinton is elected"). Theoretically, efficient markets will converge "trader's expectations of likelihood of our reality matching the described state" to "the market price of that state". The market maker algorithm facilitates this goal by accepting 'buy' and 'sell' orders at the market price (pre-voting) and paying out at the resolved price per share (post-voting).

2) However, Traders also pay fees in the form of a small percentage (for example 1%) of their trade cost. Competition among Market Authors will ensure that these fees are as low as possible (likely much smaller than the implied and actual fees for modern financial/betting institutions).

3) Trading is censorship-resistant and confidential; anyone can make pseudonymous trades via CashCoin. Each trade increases the trading fees collected and the subsequent dividend payments to VoteCoin owners.

4) Shares themselves can be 'traded' for efficiency or (optionally) even to offload trading-infrastructure to third parties. Instead of selling for CashCoin, transferring CashCoin, and then re-buying (a cost of 2 trading fees and 3 transaction fees, and substantial delay and price risk), a 'transfer' function can simply move shares among keypairs in one transaction. However, to remain incentive-compatible, this function would need to require an explicit payment to the Market of 2 trading fees.

(f) Attempts to Guarantee that the Assumptions Hold

1) "Truthcoin inherits all of the assumptions of Bitcoin. For example: No malicious entity (an individual or perfectly-coordinated group) controls a large percentage of hashing power."

a) As of this writing, Bitcoin has been running for nearly 6 years despite an 8 billion dollar market capitalization and widespread attention from computer science professionals and security experts.

2) "Users are greedy (prefer having more money to having less money), and lazy (prefer putting in low effort to high effort)."

a) Darwinism more or less guarantees that this is true. No extra guarantee is made here.

3) "Upon the Voting Period of each Branch, there exist at least Λ=150 Decisions to be resolved in future Voting Periods. ("There are always future Decisions to resolve")."

a) This can be programmed as a literal requirement, without which Decisions (and their Markets) can just "stall" (ie remain open for trading, but not permanently resolve).

b) With these three conditions: [1] Stalled Branch, [2] Decision-Author's signature, [3] Market-Author's signature, one can move a Market's Decisions to a new Branch. Thus $\Lambda=150$ only truly needs to hold for one Branch, in the entire Truthcoin system.

c) To guarantee that $\Lambda=150$ holds for at least one Branch, we can rely on historically popular betting (sports, recreational gambling, and finance). Users with tied-up shares, Authors on stalled Branches, or entrepreneurial owners of the largest Branch may simply create Decisions specifically for the purpose of de-stalling the Brach they are on.

4) "No malicious entity (individual or perfectly-coordinated group) owns more than $\Phi=65\%$ of the VoteCoins of a given Branch, nor does a single entity own more than 50% of the total CashCoins."

a) A "reliable group" can own $(1-\Phi)$ of the VoteCoins and sign messages proving this. An individual may singlehandedly own $>(1-\Phi)$ of the VoteCoins, and for privacy reasons, split that amount into two accounts (one of which he or she would use to sign such a message).

b) As CashCoins are intended to be used as money, it is extraordinarily unlikely that one individual (or coordinated group) could (or would) reliably control half of the money supply. Today, no individual is within two orders of magnitude of half the global money supply. Although small groups do accumulate vast and disproportionate wealth, this tends not to be in the form of "Cash" and instead is in the form of return-producing, illiquid, investments.

5) "Search Costs (for a single Voter to learn the realistic answer to a Decision) are lower than Coordination Costs (for multiple Voters to collectively fabricate a false answer)."

a) The Ballot cast by Voters is encrypted, and Voters have incentives to keep the Ballot encrypted (for fear of losing coins) and to lie to each other about their voting intentions. Thus, credible communication is impossible and coordination impractical.

b) Voters have the "fail safe" option to highlight a case where the search costs are significantly high (for example, when the outcome is ambiguous or unmeasurable).

c) 'Branching' (see Article III), limits voting influence to individuals with an extremely specific set of interests or knowledge, such as Sports, Finance, or Science, for whom presumably certain information is readily available at low search cost (Super Bowl outcome for a sports fanatic, DJIA close for a finance fanatic, etc.).

Article III. Scalability, Extensibility, and Customizability via 'Branching'

(a) Money Supply vs Franchising

1) In Bitcoin, a fork occurs when the network cannot agree on a single reality. The fork results in two separate chains, each with nearly the same transaction history. All users who held 10 BTC before the fork would have two separate 'versions' of 10 'BTC' on two different forks.

2) This is spectacularly undesirable in a system designed to store value (i.e. a system of money, for example, Bitcoin or CashCoin), for several critical reasons, the chief of which are the instantaneous and unexpected doubling of the money supply (if the chains remain separated) or a full reversal of transaction history for an arbitrary subset of the currency system (if the chains successfully re-merge).

3) However, for VoteCoins, the values held by each account represent reputation and relative influence. Forking the blockchain by disagreeing on reality, or of the location of CashCoins, would indeed be as frustrating as a Bitcoin fork. However, as all VoteCoin-sets ("Branches") use the same CashCoins, and Markets exist independently of Branches, there is no way of doubling the money supply or double-spending by forking only the VoteCoins (ie copying one Branch into two, or "Branching").

4) What is possible, however, is double the supply of VoteCoins in order to half the future judging activity required on each of the two new "Branches" (figure 7). This could be done for simple reasons: because Voters are fatigued at the number of Decisions they are asked to vote on, for the sake of increased competition, or to charge different fees. More interestingly, forking could eventually change the quality of the Decisions accepted for those VoteCoins ("by that Branch"), for example to create a Sports Branch or a Finance Branch. By forking off a new Branch, all previous Owners would maintain their old VoteCoins (and with them the voting influence of their established reputation), which means that the established trust of the system would be upheld in both the new and old Branch. Eventually, some Owners would sell, or simply not use, their VoteCoins of a disliked Branch, and the Sports Branch would eventually be owned by individuals especially interested in sports. When "Sports" later splits itself into "Sports:Basketball" and "Sports:NonBasketball" (because, for example, there are just so many basketball Decisions on the Sports Branch), the reputable sports-fanatics owning VoteCoins of the Sports Branch (and no other VoteCoin Owners) will have their voting power transferred to the two new Branches. Therefore the network grows organically, branching in the same way that a healthy tree splits new branches when the environment can support them.

5) Moreover, as a new "tree" can be "planted", one might create a new VoteCoin set (from nowhere) to create private internal markets for a private business or club. These markets can set up the initial allocation of reputation (and reputation smoothing parameters), to establish an 'eternal dictator' or 'rotating board of directors', etc..

(b) Quality Control

1) Branches impose a number of costs on the network: each needs its own n x m Vote Matrix per Voting Period and its own SVD operation, and less-popular Branches may be likely to freeze (fail to achieve the required $\Lambda=150$ upcoming Decisions) or simply be bought- up and attacked (as they would likely have a low market cap). Moreover, all Branches may gain by committing to rules which make them slightly more exclusive: the option to move to a different Branch may create a spirit of competitiveness and entrepreneurship, but it can also prevent unity/cooperation/network-effects.

2) It may be desirable to impose serious prerequisites for both Branching and Planting. The option to Branch may require an automatic trigger, for example, that there be >500 upcoming Decisions. Planting may require the permanent destruction of, say 1 CashCoin, or Branches could be required to bid for the option to "rent" one "SVD slot" among a fixed (but growing) number of slots. Requiring high λ and Λ parameters would also discourage the creation of frivolous Branches (as these would need to reliably support many Decisions in order to operate effectively).

Article IV. Implementation Details

(a) Basic Aspects (Block Structure / Chain Validation Rules)

1) Parameters for fees, cumulative participation, etc. should be very easy to add, as are the reputation vector, transaction list, and data matrices themselves.

2) Writing a blockchain with different fields and block validation rules has already been done so many times that there are currently about 450 tradable, useable (if not useful) "Altcoins"[10].

3) Transactions should be fine, as well as smoothing of parameters. Blocks can validate any operation, be that message signing or signature verification, or the consensus algorithm. I do not anticipate a problem here.

4) By using a market scoring rule, there is no need for Bids or Asks, or other order book artifacts. Markets are updated with a single signed message.

(b) New Issues

(i) Computational work for SVD

1) Recall that Voters select the True/False/Scalar/Unknown status of each Decision. The vote matrix is [Voters, Decisions], meaning that at 10,000 users and 100 Decisions (my realistic expectation), the matrix becomes quite large. My testing of such a matrix on an average computer indicated that, in Python, the algorithm completed instantaneously, but, in R, the consensus algorithm ran for over 60 seconds.

2) We may have to limit the total number of Voters (but not Owners) on a single blockchain to 100,000 or similar, involving a sort and filter to remove the smallest values. Those with a small amount would probably neither collect dividends nor participate in RBCD at all. If this limit is a problem (which I highly doubt), individuals can privately form corporations and jointly-control a unit of > $1/100000^{th}$ VoteCoin (the minimal un-removable amount). This limit could also be increased as computers become faster.

(ii) Market Maker – Transaction Speed

1) Bitcoin transactions occur at 1 per 10 minute, and a 1 hour confirmation time. This would be acceptable, but unfortunate for a competitive trading environment. It is possible that GHOST[11] or something similar[12] will greatly improve Bitcoin transaction speeds.

2) Fast Sequential Intra-Block (SIB) Trading

[10] http://coinmarketcap.com/
[11] https://eprint.iacr.org/2013/881.pdf
[12] http://roamingaroundatrandom.wordpress.com/2013/11/30/bitcoin-idea-temporary-notarized-wallets-secure-zero-confirmation-payments-using-temporary-notarized-p2sh-multisignature-wallets/

a) The Market Maker algorithm implies an ordered transaction history (because the market price changes after every trade). Signed messages 'trade X for Y', with nodes accepting the first received trade as valid, and allowing more trades to be built on top of this ("unconfirmed") trade, with ultimately only one timestamp ("confirmation") landing on all of these trades once every 10 minutes would probably still work, because double-trades will not make it far enough to steal (let alone withdraw) funds.

b) The Double-Spend 'Problem' Within-Blockchain

i) Double Spending is substantially less of a problem in these within-blockchain transactions, and especially less of a problem in within-blockchain portfolio trades. In the prediction markets described here, double-spend attempts are likely to actually increase overall market efficiency.

ii) The most important advantage here is that, as the double-spent transaction unwinds, the trade also unwinds. A traditional double-spend involves the sale of a good or service for money, with the attacker making off with the good while paying himself. Here, however, the exchange of CashCoin for shares and back ('double-trade') takes place within the same transaction, so the double-spender ends up unwinding both the payment transaction and the trade.

iii) Moreover, in building a portfolio, it is likely the case that users have a preferred asset allocation. As users have almost no control over which double spend goes through, any double spend is just a pointless financial risk.

iv) Although it is impossible to steal, it may be possible to confuse by making random trades and temporarily distorting prices. This is sometimes phrased 'market manipulation' with a supposed[13] psychological advantage to a trader in a subsequent trade. Although this may work in traditional markets for a variety of reasons, it has been shown that, in prediction markets, so-called manipulators actually increase market efficiency and on average improve the bottom line of non-manipulators[14]. Either way, we collect transaction and trading fees for these transactions.

c) Fields of a SIB transaction:

Field	Example	Description
Account	TLoxo4R…	A funded CashCoin address.
Market	Mjq11qc…	The hash of the Market
State	2	Purchasing shares of State 2.
Amount	.03465	Total cost of this trade.
Price Limit	.70	This trade is only valid if the market price of state 2 is <.70.
Sequence Limit	73	This trade is only valid if there have been 72 or fewer trades on this Market-state since the last block.

[13] http://ideas.repec.org/p/chu/wpaper/08-01.html
[14] http://dmac.rutgers.edu/Workshops/Markets/hanson.pdf

d) Miners would build on the intra-block Market-tx-chains which maximized their transaction and trading fees, which would almost certainly be the longest chain.

(iii) Front-Running

1) In a decentralized blockchain system, "front-running" (where one trader makes a trade, a second trader observes this trade, and 'runs in front' of the trade by copying it and attempting to have his copy included in a block first) may be a problem.

2) Front-runners must be confident that they are copying an informed and valuable trade. They must also be confident that they can reliably manipulate the block-inclusion rules.

3) We might discourage this by introducing an alternate hash-function proof-of-work for transactions.

a) With block-mining, all individuals have an incentive to mine, and all miners have an incentive to improve. However, with an alternate hash function, there is no existential requirement for "tx-mining" to ever exist or be profitable. This might produce a stable "no-front-running equilibrium" where this activity is permanently unprofitable and there is no need to specialize, create ASICs, etc.

b) This exploits the discriminating fact that original trader can build the tx before the attacker can.

c) Professional tx-miners would put a great deal of money at risk, in an environment where they can't control the trade quality (will this trade win?) or quantity (will anyone make a trade for me to front run?)

(iv) Will algorithmic trading extract rents?

a) This environment has extremely competitive features (unlike those of a traditional fiat exchange), and in general barriers to entry are much lower. Traders who invent creative rent-extraction methods will see these rents destroyed by perfect competition. Algo-traders may attempt to fake-out each other with fake trades, pre-trades, and other techniques, in what would ultimately be a large waste of effort impacting actually-informed traders minimally.

b) Moreover, this exchange does not employ leverage (which creates fragility and momentum), does not necessarily operate with the approval of a regulatory environment (which can allow the dishonest to operate comfortably under the illusion of consumer protection[15]), is not bound to a specific tax/fee/legal structure (which can allow 'outsiders' to be fleeced), etc.

[15] http://en.wikipedia.org/wiki/Madoff_investment_scandal#Red_flags

c) Use of Bitcoin Miners discourages targeted hardware-software conspiracy.[16]

(v) Allow exchange information to privatize centrally, in a sort of 'brokerage firm'.

a) Imagine a 'MtGox for trading', or some website, which aggregates trades and then submits large updates to the Truthcoin network.

b) Such an aggregation would certainly save on transaction fees. As many trades offset each other, such a pooling of trades may also save on trading fees, yet because of the delay between trade and block-inclusions there is potentially serious basis risk on the part of the website.

c) These privatized entities would compete on cost and quality, and would be accountable to their customers (with regard to front-running, for example).

(vi) Preventing Active Coordination Among Voters

1) Encrypted votes assist us in discouraging malicious voting by requiring all credible coordination to be tacit.

2) To implement sealed voting, consider the following schedule: encrypt vote[17], sign vote, broadcast vote, voting deadline passes, reveal private key, decrypt vote. Sharing one's key before voting deadline could allow someone to change your vote (potentially in a malicious way) or outright steal your coins, so no one could reasonably ask to know your key or vote. However, votes can contain a transaction (a new private key controlling next period's vote) which becomes valid after the voting deadline passes. This scheme also prevents you from 'spending' your coins and voting with them at the same time, which simplifies coin trading.

(vii) Floating Point Math / Decimal Precision

1) Consensus under continuous math can be a problem because computers occasionally disagree on the number of decimal places to keep, or how to truncate/round. I assume that it will be easy to implement some rule, such as truncation, significant digits, or 'within 99.99% precision' requirement, so that all nodes reach the same answer and hash.

(viii) Initial Allocation of Coins

1) One of Bitcoin's most successful implementation details was its distribution strategy (gradually introducing the initially worthless coins to existing users [miners] at a geometrically decreasing rate). This distribution can be easily replicated with the CashCoins (by giving them completely to Bitcoin owners, and matching the blockreward schedule), but there are at least two problems with doing this for the VoteCoins.

[16] http://www.extremetech.com/extreme/154977-high-frequency-stock-traders-turn-to-laser-networks-to-make-more-money
[17] https://bitcointalk.org/index.php?topic=196378.0

a) Work Problem

i) In Truthcoin, Miners only do some of the work, unlike in Bitcoin where they do almost all of the work. With Truthcoin much of the work is really done through voting.

ii) The Work problem prevents a Bootstrap Mining Scheme as done with several Altcoins (a 'fast release' for Miners before reaching a steady state of some kind).

b) Trust Problem

i) Initial coin Owners must be trustworthy to vote, yet they will not have established a reputation. They may have "bought in" to the coin, but not bought in to the costs and benefits of Voting activity. This favors some kind of cost or sale, for example a Dutch Auction, donation address (Mastercoin), or burn address (Counterparty).

2) It may be useful to distribute the VoteCoins to developers or investors who contribute to an initial release of the software. This makes some economic sense: these individuals bore the marginal cost of adding this functionality to cryptocurrencies, so they should also own the marginal reward (use of PM infrastructure as measured by Trading Fees). This also solves the Trust Problem above: the first developers and investors sacrificed the most to construct the network, and would therefore have the most trustworthy reputation.

(ix) Beta Amplification

1) To increase $\boldsymbol{b_1}$ to $\boldsymbol{b_2}$, additional cost would have originally been an additional $(\boldsymbol{b_2} - \boldsymbol{b_1})\boldsymbol{log}(\boldsymbol{N})$. Testing confirms that this can be done mid-trading with no adverse impact upon existing Traders (and does not allow the market maker to run out of money, etc). Instead it adds liquidity to the markets by making the price harder to move, and, during the Amplification transaction, moves each state's price closer to the uniform distribution (50%-50% for a binary market). It would be convenient if interested parties could donate to a Market to increase its liquidity, trading activity, and accuracy.

2) Some research[18] suggests varying $\boldsymbol{b}$ to achieve more desirable combinations of cost, profit, and liquidity. This may be helpful if, for example, Traders are sufficiently more likely to trade today in markets which will become more liquid tomorrow.

(x) Intelligent Decision Fees

1) Recall that, to allow reuse of Decisions, they are created in a first phase, paying Fee_{d} for each Decision.

2) Recall also that Markets are then, secondly, submitted in the form (L(O), T), where L(O) is an ordered list of Decisions defining the dimensions and space of the Market, and T is the payment transaction amounting to $b\log(N) + Fee_s * N$.

[18] http://www.cs.cmu.edu/~aothman/flex.pdf

3) It is possible to track the number of Decisions required in each Ballot (i.e., each month or so), and incrementally adjust the fee upwards if, say, March is an especially crowded month. A simple solution would be $Cost(O, B_t) = (Fee_{\mathrm{d}} * K) + (Fee_{\mathrm{d}} * K')$, where K' is the number of Decisions exceeding a threshold, say 100.

4) The fee may also be cheaper when there are so few Decisions that the benefits to considering an entire Ballot are reduced (because, for example, a Ballot is of Decisions of only one Market). The incentive structure works best when there are many Decisions. Possibly the first 20 Decisions can be free, or extremely inexpensive.

Article V. Figures

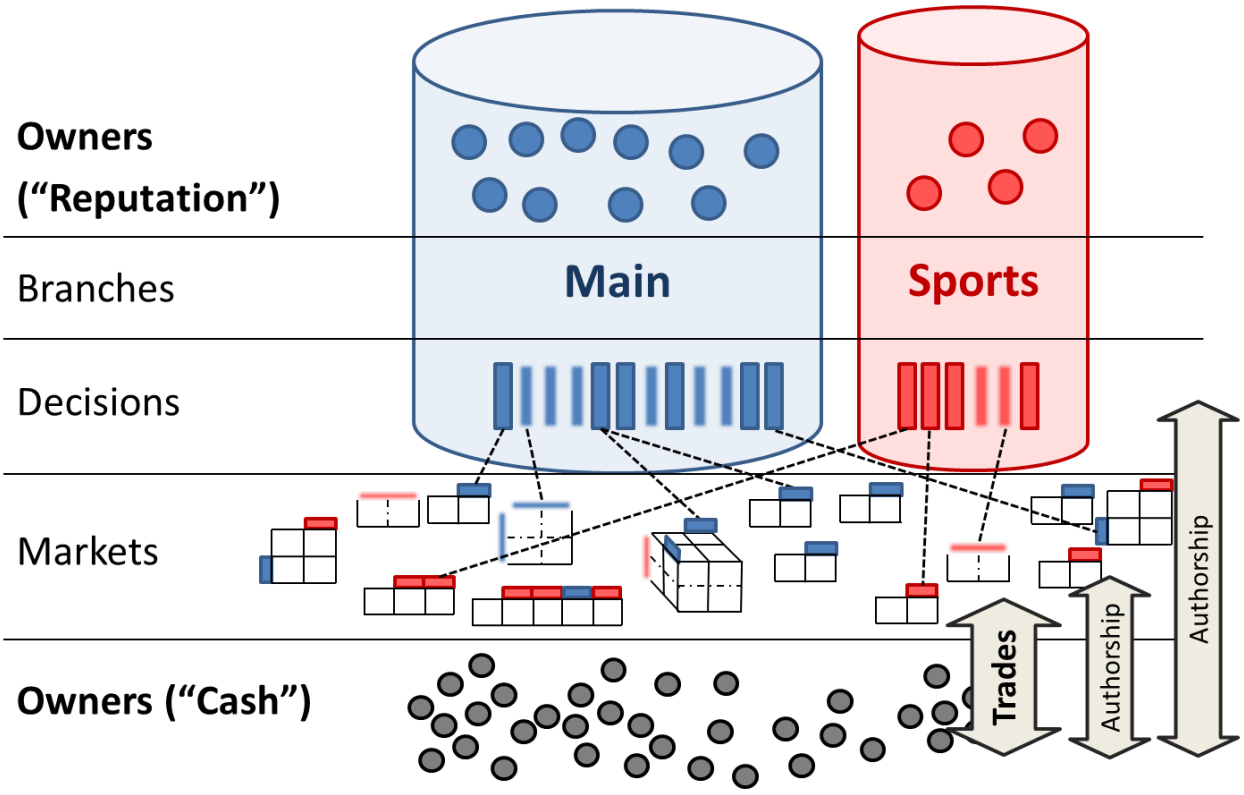


Figure 1. Graphical representation of Truthcoin's structure. Notice the two types of coin (circles), the VoteCoins representing reputation (top, colored) and the CashCoins representing money (bottom, grey). Decisions can either be Binary (bordered) or Scaled (blurred). When used in Markets, Scaled Decisions span an entire dimension, whereas Binaries only partition-from-null.

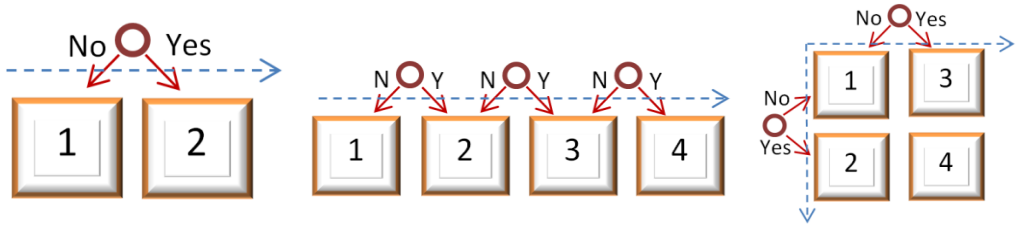


Figure 2. Graphical representation of three Prediction Markets, each with Binary Decisions. Left, the binary form popularized by InTrade, with one dimension (blue dashed arrow), one decision (red circle), and two states (yellow squares). Center, a market with not two but four mutually exclusive states (for example, the winner of a 4-team tournament) and three decisions. Right, a prediction market with two dimensions. Multidimensional prediction markets allow users to trade not only on the probability of each state, but also the relationship between dimensions[19] [20], such as the relationship between an election result and the achievement of an economic goal a year later.

[19] http://www.overcomingbias.com/2008/07/intrades-condit.html
[20] http://www.overcomingbias.com/2008/01/presidential-de.html

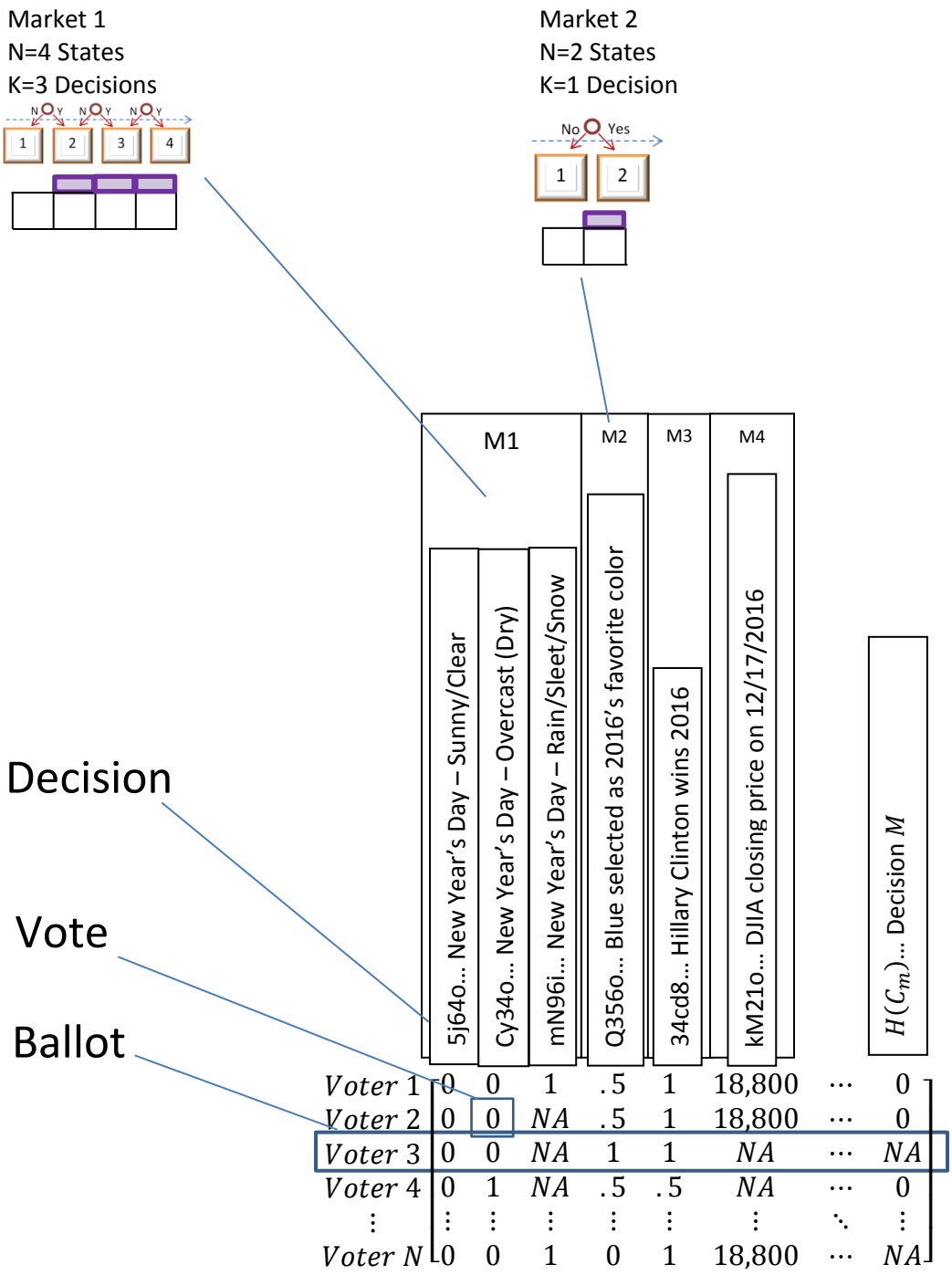
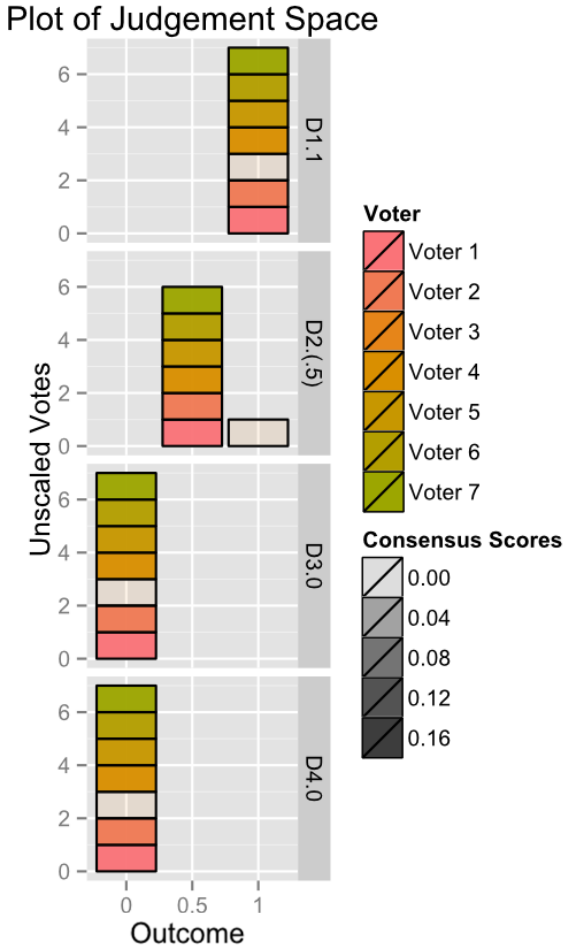


Figure 3. A hypothetical January 2017 Vote Matrix, with annotations. This Vote Matrix would be for a Branch at least general enough to contain Decisions on US weather, politics, and financial indices.

$$\begin{matrix} Voter\ 1 \\ Voter\ 2 \\ Voter\ 3 \\ Voter\ 4 \\ Voter\ 5 \\ Voter\ 6 \\ Voter\ 7 \end{matrix}\begin{bmatrix} 1 & 0.5 & 0 & 0 \\ 1 & 0.5 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0.5 & 0 & 0 \\ 1 & 0.5 & 0 & 0 \\ 1 & 0.5 & 0 & 0 \\ 1 & 0.5 & 0 & 0 \end{bmatrix}$$

$$\begin{matrix} Voter\ 1 \\ Voter\ 2 \\ Voter\ 3 \\ Voter\ 4 \\ Voter\ 5 \\ Voter\ 6 \end{matrix}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$



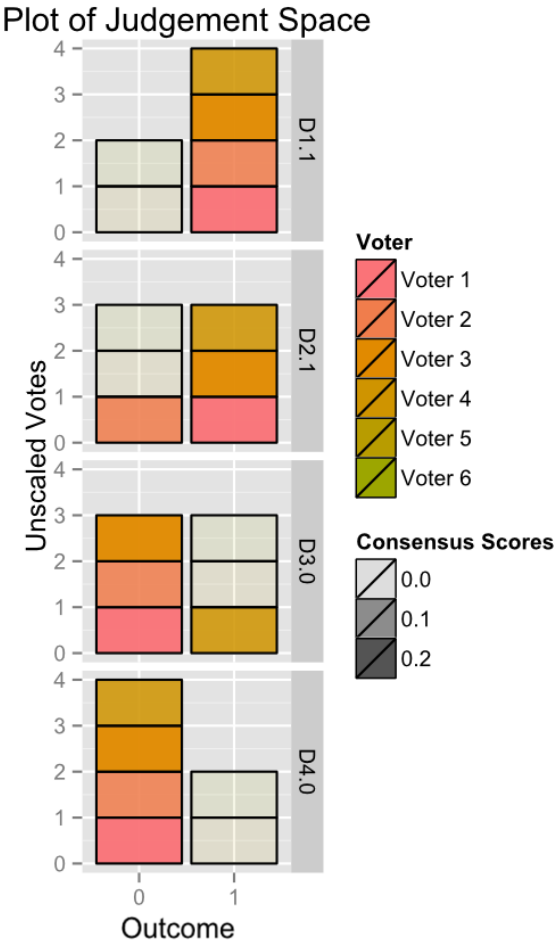
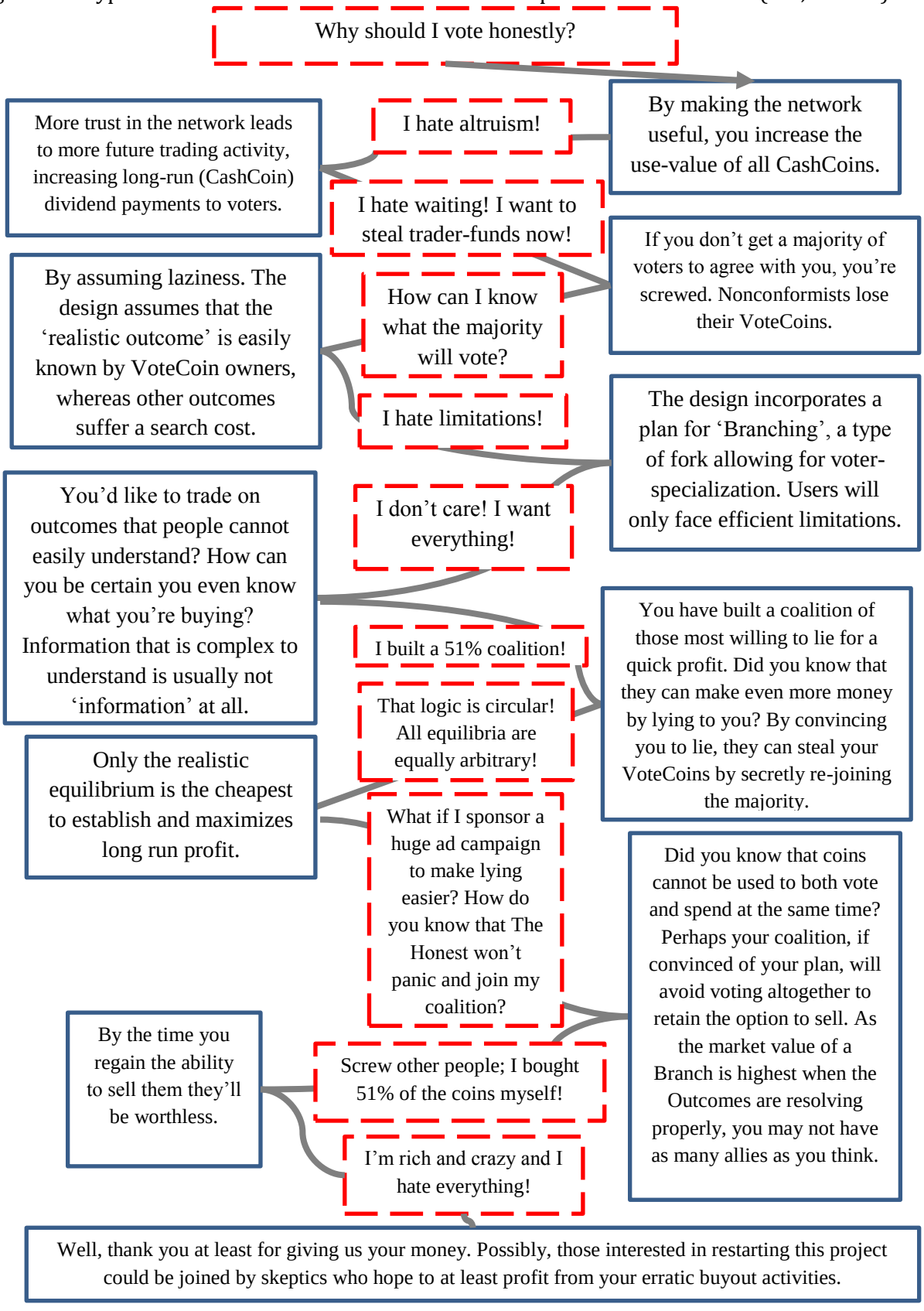


Figure 4. Two Vote Matrices and their corresponding SVD-Outcomes, represented graphically. Left, 7 Voters, and right, 6 voters (matrix row, graph color). 4 Binary Decisions (matrix column, graph row [right axis, above period]), vote count (graph left axis), No/Yes outcomes (matrix cells, graph bottom-horizontal axes), consensus score (how well voters agreed with each other, graph opacity), and intended Outcome (graph row [right axis, below period]).

Left: nearly-perfect agreement. One Voter, (#3), left the group once (Voting "1" for D2), and so his VoteCoin ownership, voting "weight", and CashCoin dividend payout all decrease (opacity). Right: Notice D2 and D3: despite an apparent 50-50 tie in the quantity of votes cast for each outcome, the fact that Voters 5 and 6 were less-conformist than other voters removes enough of their vote-influence to shift the outcomes of D2 and D3 (from 50%-50% ties to 1 and 0, respectively).

Figure 5. A hypothetical flowchart-conversation with a skeptical VoteCoin owner (red, dashed).



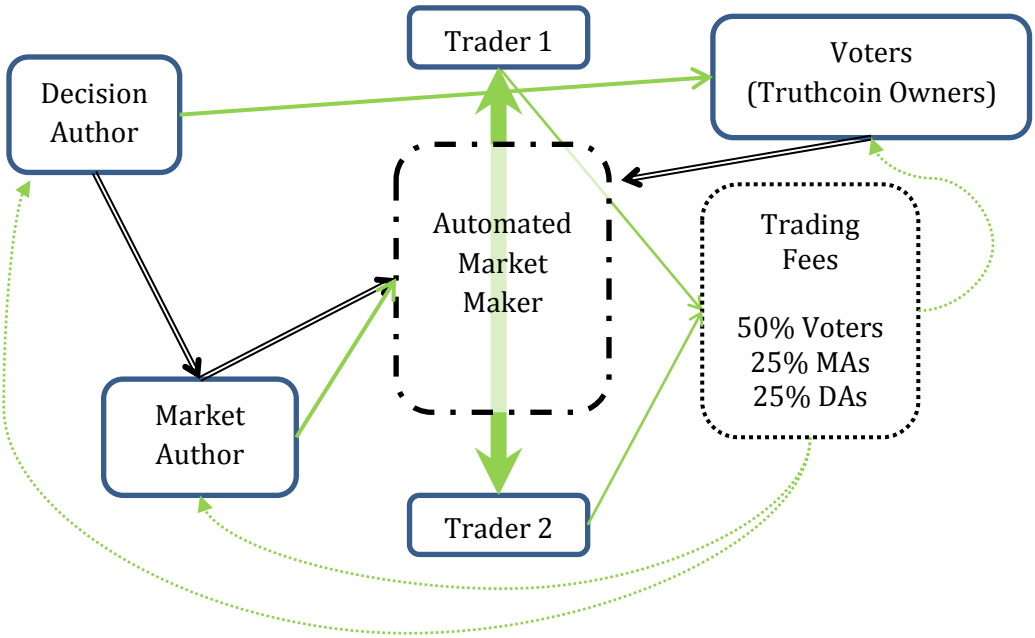


Figure 6. The flow of costs (green solid), revenues (green dashed), and information (black double) among various agents (blue solid) and accounts (black dashed). The horizontal axis corresponds to time, and line widths correspond to expected magnitudes, with the exception of revenues (whose magnitudes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

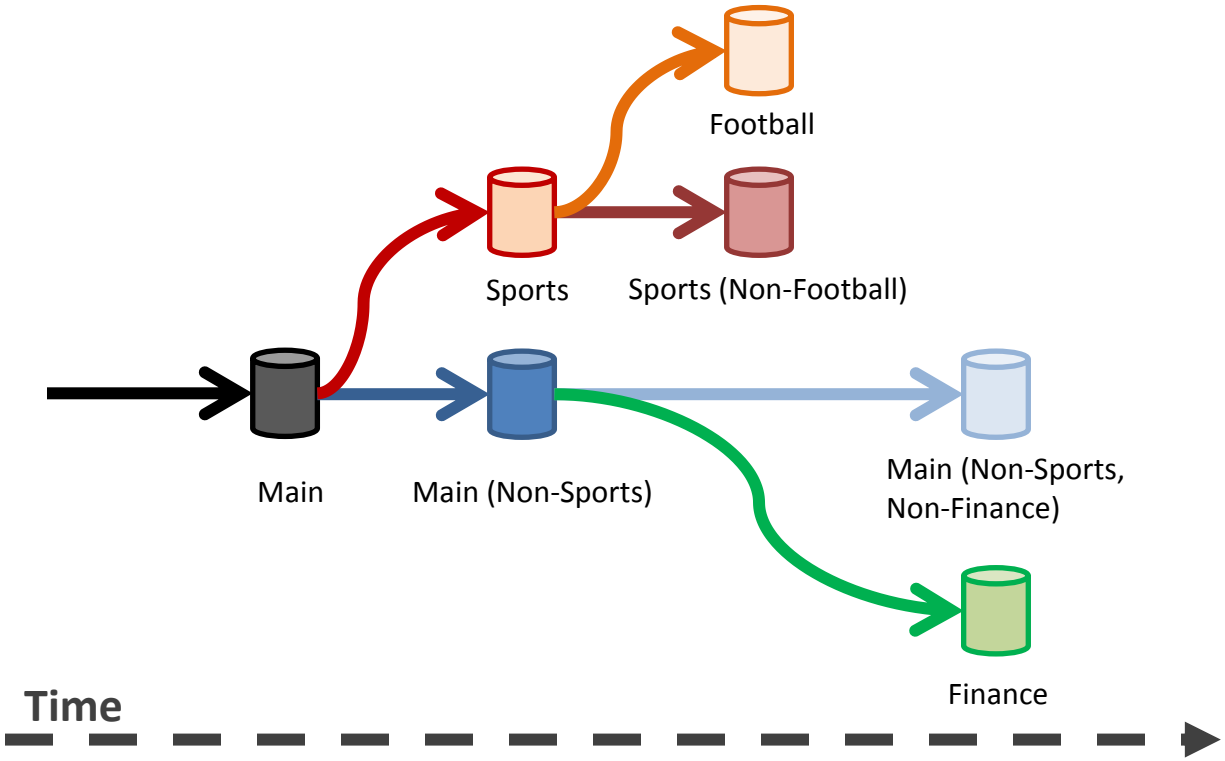


Figure 7. Holders of any Branch have a "free option" to own future branches.

Article VI. Appendices

(a) Appendix I – Calculation of Missing Values

1) SVD cannot be performed on a matrix with missing values.

2) To fill any missing values, a simple procedure is used:

   a) The Decision Outcomes are calculated using all available data (ie, for all votes that were case for a Decision). The previous period reputations are used (as the present period reputations do not yet exist) and they are renormalized by dividing by their sum.

   b) The calculated values are then binned, according to the Catch parameter, into one of three values: 0, .5, and 1, as these represent vote-format.

   c) Each Decision has all of its missing values replaced with the binned calculated outcome.

3) Non-Voters are later penalized according to the following scheme:

   a) Calculate "Participation" for each Voter i as $P_i = \frac{\sum \#VotesCast_i}{\sum \#VotesExpected_i}$, and in total as $P_{total} = \frac{\sum \#VotesCast}{\sum \#VotesExpected}$.

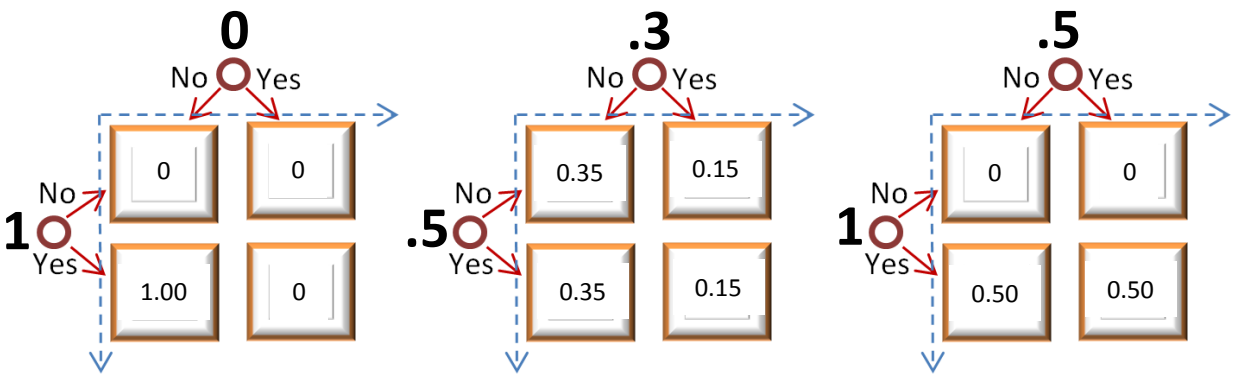
   b) Calculate each voter's "Relative Participation" as $P_i^{rel} = \frac{P_i}{\sum_{i=1}^{n} P_i}$.

   c) Finally, merge the new smoothed RBCR value with this Missing Values value, in direct proportion to the total (1- Participation).

$$r_{final} = (r_{t,n\times 1}) * (Participation) + P_i^{rel} * (1 - Participation)$$

4) This ensures that the penalty for missing a vote is small when few votes are missed, but severe when many votes are missed. If less than 50% of voters are voting, this "penalty" actually becomes a more important determinant of future coin values than agreement with other voters (as it should, because the "other voters" are not actually voting).

(b) Appendix II – How Resolved-Outcomes Translate to Share Prices



Three Markets, each with 2 Decisions and 4 States. The left Market had Outcomes of 1 and 0, the center Market had Outcomes of .5 and .3, and the right Market had Outcomes of 1 and .5. The final sale price is given inside each State-box, constructed by multiplication (precisely as joint probabilities are constructed from marginal probabilities).

The leftmost market is most straightforward: a Binary variable where the row-event happened but the column-event did not. Owners of the appropriate share can earn 1 unit each, owners of other shares get nothing. The center market involved at least one scaled Decision (the column-event), which resolved to ".3".

If a Binary Decision is ruled unresolvable, the winning State of any Market built with this Decision cannot be determined. However, we can preserve the utility of any Market built with an unresolvable Decision by causing that Outcome to take on the equally-spaced value of ".5".

(c) Appendix III - Audit Option

When a Market becomes Disputed, its funds are frozen. If a Market becomes audited, its funds are pooled, a fee ρ=10% is set aside, and the disputed-Decisions are resolved via the same SVD-Consensus, but using a different pool of voters. All of the remaining money is then available for proportional redistribution as usual. When the attacker as invested greatly in a market, honest traders can net profit from attacks.

	SVD-Consensus Weights	Agents must report, or suffer a penalty?	Agents must report with consensus, or else…
Voters	The VoteCoins of a single Branch.	Yes	…they will lose ownership of the VoteCoins that they purchased, and the associated dividend revenue.
Auditors	Any "free" CashCoins a user is willing to lock up with a Vote ("Audit-Ballot").	No	…they won't receive as large a stake-adjusted portion of the Audit Fee as they otherwise would have.

Miner Veto: Miners may set their own Audit-Ballot. If the Auditor-Outcomes do not match the Miner-Ballot, the Audit Transaction can be included in a block, but has no effect. The Disputed Decisions and markets remain that way for another Ω=6 months.[21]

Source of Forecast-Correction	Network Capacity (Cost)	Expected Throughput
Traders	Very High (One trade only)	Very High
Voters	High (n Votes, One SVD proc, One Voting Period)	High
Auditors	Very Low (Out-of-role, costs audit fee, causes considerable delay)	Very Low
Miners	Extremely Low (Out-of-role, volunteer, network-instability)	Extremely Low

Notice that the cost-of-truth has been matched (triangles) with the realistically-expected usage: More expensive truth-sources are rarer.

[21] Some questions remain for this system: Miners may claim that they will not build on a vetoed block, but will their actions back up these claims? Is this scheme robust when mining power can be rented (for the time period surrounding the audit block)?

(d) Appendix IV – Justification of Chosen Parameter Values

Each Branch is defined by the following parameters. Although separate Branches might compete over different parameter-families, it may be advantageous for the blockchain itself to impose "Reasonable Bounds" on possible choices for parameters. Branches themselves may impose "Reasonable Bounds" on Market-specific parameters, (*b*, content-tags, trading/audit fees).

Parameter	Representation	Reasonable Bounds	Reasoning Favoring Low	Reasoning: Favoring High	Reasoning Behind Choice
"Retention" **$\alpha = .80$**	1] Forgiveness of RBCR to Voter-disagreement. 2] Neuroticism in assuming new ownership. 3] Penalty for least-coordinated Voter (loses (1- α) of VoteCoins).	(0,1) Zero and one would remove all long-term reasoning.	1] Want network to adapt quickly. 2] Want attackers (mis-voters) to suffer.	1] VoteCoin should more safely store-value. 2] Individuals may make mistakes, past history should count most.	Past history should count the most, but in general VoteCoin owners are responsible for proper voting. 20% for being the unanimity-failure seems not unreasonable.
"Voting Period" **$\tau = \{\tau_{idle}=6w, \tau_{voting}=1w, \tau_{unsealing}=1w\}$** $\sum \tau$ = 8 weeks	1] Pulse for network to "check in with reality". 2] Scale-economies of Voter-Time (setup costs/total costs). 3] Loss of info-salience over time ("memorability of events").	$\tau_{unsealing}$ involves revealing private keys, implying ~1000 blocks. Others depend on reliance-on-human-input.	1] Want to decrease basis risk for Traders. 2] Believe info decays too rapidly to remain available at low-search cost.	1] It is most important to contain many Decisions in a Vote Matrix to make attacks less practical.	Attacks must be avoided at all costs, but basis risk is also an important factor. With human involvement on the Main branch, a period of 8 weeks seems a helpful balance.
"Audit Accumulation Period" **Ω = 6 months**	1] Time between audits. 2] Minimum time one would have to prepare their Audit-Ballot.	[1 month, 3 years]	1] Believe audit will be easy (info has diffused). 2] Believe audit should span many different Voting Periods.	1] Want to give Miners time to set veto. 2] Want 'punitively slow' audit (should never have reached this point).	The crucial element at play is the Miner-Veto, which should be easy to set and sufficiently infrequent to be nonburdensome.

"Certainty/ Audit Threshold(s)" **Φ = {.65, .65}**	1] Quantity of Disputed votes before audit. 2] Insistence on Certainty, Forgiveness for mis-voters, "Open-mindedness"	{ 0, (.5, .9) } Attacker with a majority can ignore audit. Do not want audit-spam.	1] Want to reduce strategic complexity. 2] Want failed attackers to be punished immediately.	1] Want to rely more on the Threat of Audit. 2] Want attacker-individuals to need to buy more VoteCoins.	2/3rds is a standard democratic threshold. One failure to achieve Certainty could be a simple confusion (and should not go directly to an Audit).
"Minimum Ballot Size" **λ = 30**	1] Paranoia. 2] Emphasis on SVD. 3] Insistence on cross-validation. 4] Branch "barriers to entry".	[10, 200] Covariance operation requires >2 columns.	1] Want votes resolved quickly (decrease basis risk for traders).	1] Want votes resolved accurately.	Accuracy *is* paramount, but 30 should suffice as a bare minimum. Note that this parameter interacts with **τ**.
"Minimum Future Decisions at Stake" **Λ = 200**	1] The value of next year's trading fees. 2] Retirement-Attack Risk. 3] The long term health of the branch. 4] Branch "barriers to entry".	(λ=30, +1000] With time value of money, Λ must be > λ.	1] Believe stalled Branches are a major inconvenience.	1] Believe low quality Branches are a major concern: retirement attacks and low market capitalization are the dominant issues.	If all the Branches freeze, the project is dead anyway (from lack of interest). I support higher-than-usual barriers to entry.
"Audit Fee" **ρ=10%**	1] Cost to the network (technical, systemic, and labor) of the audit.	(0, 20] At zero, there is no incentive to participate. Values exceeding 20% would appear to be excessive.	1] Believe that auditors are charitable and will participate, even if unrewarded. 2] Want to protect Traders from exposure to fees, and reduce associated uncertainty.	1] Want to be robust to auditor-laziness. 2] Feel that Traders are likely to net-profit from attack-investments anyway. 3] Feel that a high-quality audit would outright discourage attacks.	Trader-risk seems to be a serious concern, and trades would ideally be encouraged as much as possible. I am equally persuaded, however, that auditors are likely to be lazy and that a high-quality audit would be unlikely to be triggered.

Article VII. Document History

(a) Version 1.1

1) Substantially edited Article IV “Implementation Details” based on feedback from expert cryptographers, senior bitcointalk.org members, and developers.

2) Added Appendices describing the handling of Missing Values and Partial Incoherence (which were always part of the original design, I had simply forgotten to write about them in version 1).

3) Fixed several typos.

4) Changed wording on LMSR from “infinite” to “permanently nonzero”. The previous wording was incorrect (I don’t know what I was thinking).

5) De-emphasized demurrage as it is unnecessary and confusing.

(b) Version 1.2

1) Added and documented functionality for Scaled Decisions, which take on a Scalar Outcome (not a Boolean).

2) Edited substantially for clarity, removing a few paragraphs which were outdated or otherwise confusing. Caught numerous typos and formatting errors.

(c) Version 1.3

1) Reworked paper to present the idea not as a Bitcoin addon, but instead as a new blockchain and Bitcoin replacement. This included a change in terminology: Bitcoins became "CashCoins" and Truthcoins became "VoteCoins".

2) Improved the assumptions section, by removing implicit and redundant text, and adding a few (previously overlooked) assumptions.

3) Added appendix section "Justification of Chosen Parameter Values".

4) Added the concept of a Transfer (moving shares as one would move Bitcoins).

5) Added the Audit Process, which makes the Outcome-Resolution process more realistic (more time to resolve disagreements), and strengthens incentives to realistically-coordinate by adding a Wealth-layer (audit) and Miner-Layer.

6) Changed the way Binary Outcomes are resolved as "unresolvable", as the previous way has been superseded by the Audit Process.

7) Added protection against Dying Branches (they now "stall" instead, see $\Lambda = 200$).

8) Mentioned tx-PoW requirement to prevent front-running of trades.

9) Edited Implementation Details substantially for clarity and updated-relevance.

10) Edited for clarity generally, and added a few helpful graphics.