# Truthcoin

## *Trustless, Decentralized, Censorship-Proof, Incentive-Compatible, Scalable Bitcoin Prediction Marketplace*

Paul Sztorc[1]
truthcoin@gmail.com
https://github.com/psztorc/Truthcoin
1M5tVTtynuqiS7Goq8hbh5UBcxLaa5XQb8
Version 1 – 1/31/2014

**Abstract.** Where Bitcoin allows for the decentralized exchange of value, this paper addresses the decentralized creation and administration of Prediction Markets (PMs). An alternative proof-of-work blockchain collects information on the creation and state of PMs, with the winning state of a market determined by a modified weighted-vote. An incentive mechanism attempts to guarantee a) that all voters vote honestly, and b) that PM-creators act as entrepreneurs, bearing the economic costs and benefits of the PMs they create. Bitcoin users can create PMs on any subject, or trade anonymously within any PM, and all PMs enjoy low fees and infinite market liquidity through a LMSR market maker. Scalability and customizability can be achieved via 'branching' (controlled-fork). The paper closes with a discussion of implementation details.

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

# Article I. Overview

## (a) General Strategy

### *(i) Central Facts*

1) Bitcoin allows for the programmable, censorship-resistant exchange of value.

2) While a traditional marketplace (Bitcoin or otherwise) requires physical infrastructure to facilitate the trade of physical goods, a prediction marketplace requires only the trade of digitizable information, and can therefore exist entirely in a software environment.

### *(ii) Assumptions*

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

2) The given incentive mechanism will be successful in its attempt to convince a majority of Truthcoin (TRU) voting power to select the realistic status of each Decision. This could be the case for either of two reasons:

   a) A majority of Truthcoin Owners are sufficiently honest, committed to the project, or motivated to maximize long-run revenues to vote realistically.

   b) The search costs for required to learn the realistic answer to a Decision are lower than the coordination cost required to communicate in any way actively with other Owners. There is an attempt to guarantee that this assumption is true (obviating the need to safeguard the first assumption) by:

      i) Allowing Voters to highlight a case where the search costs significantly exceed a coordination cost (or, for example, when the outcome is ambiguous or unmeasurable).

      ii) 'Branching' via safe fork to limit 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.).

## (b) Components

### *(i) Truthcoin Blockchain*

1) An alternate blockchain for 'Truthcoins' with different block-creation/validation rules such that the coins have the following properties:

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

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

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

b) Ownership of coins changes with voting activity.

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

ii) Coins 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).

c) Coins do not compete with Bitcoin as a store of value.

i) Incentive mechanism penalizes idleness (voting requirement) and suggests 1% annual demurrage to foster regenerating decentralization.

ii) Implementation of merged mining to utilize the security of the Bitcoin network, separate Miners from Voters, and respect the efforts of the Bitcoin community.

### *(ii) Automated Market-Maker*

1) Functionality inherent to marketplace which understands the behavior of Truthcoin as it relates to the creation (pre-trading, pre-event), maturation (post-event) and expiration (post-event, post-trading) of Markets.

2) Blockchain functionalities (transactions, rapidly-adjusting micropayments) allow for an always-on, (hopefully) high-speed, censorship-resistant trading environment.

3) Market Maker utilizes LMSR technology[2] to ensure infinite prediction market liquidity (such that markets will always 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 Bitcoin-user can create a prediction market ("Author a Market") about anything.

b) Authors only have an incentive to create the Markets which will see the highest trading volume (i.e. the issues which would most-benefit from a prediction market).

[2] http://www.eecs.harvard.edu/cs286r/courses/fall12/papers/mktscore.pdf

c) Authors only have an incentive to write Decisions whose outcome can be easily assessed by Voters.

d) Authors completely avoid the (prohibitive) cost of convincing Traders of their trustworthiness (as is currently the case).

2) Owners/Voters

i) Voters have an incentive to maximize the long-run trading volume, and therefore usefulness of the coin.

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

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

3) Traders

a) Any Bitcoin-user can trade on any prediction market without directly interfacing with Truthcoin at all.

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 (making the questionable assumption that there are no software bugs or failed assumptions).

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).

b) Miners have an incentive to include every Market and Vote into blocks, 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) Whereas with Bitcoin a fork would indicate confusion and instability, Truthcoin allows for controlled forks ('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

1) The Truthcoin Blockchain is a Bitcoin-inspired proof of work Blockchain with different block validation rules. Key functional differences are as follows:

| | **Bitcoin** | **Truthcoin** |
|---|---|---|
| 1 | Accounts always retain a constant amount of unspent coins. Private keys only sign messages that transfer coins to a different account. | Accounts will likely either gain or lose unspent coins (based on voting activity). Private keys can either sign messages (which transfer coins to a different account), or Votes (which influence the outcome of Decisions). |
| 2 | 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, is redistributed to Miners via an annual 1% demurrage rate, and is constantly redistributed based on voting behavior. |
| 3 | Blockchain designed only to hold information about the transfer of coins. | Blockchain contains information about the transfer of coins, but (far more crucially), also contains information about Markets and Votes. |
| 4 | Expectation of huge number of addresses, one per transaction. | Expectation of a maximum of 10,000 Owners, most of whom will vote, not transact. |
| 5 | Coin values are analogous to a saved quantity of gold. | Coin values are analogous to reputations, or shares of a corporation. |

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

### *(i) Terminology*

1) Markets (figure 1).

   a) States – Mutually exclusive possible descriptions of reality. Traders buy and sell shares of a single Market State.

   b) Decisions – Binary True/False questions that must be resolved by Voters. These partition the state space of the Market .

2) Voters/Owners – Unlike Bitcoin, owning Truthcoin is a liability as well as an asset. Owners are expected to use their coins to vote on the status of each Decision.

3) Vote – A Voter's selection, of [True/ False/ Unknown/ Missing], of what they believe accurately resolves the Decision. The default value is Missing.

4) Ballot – A set of all the Votes each Voter must cast in a period of time. Notice that Ballots are defined by the maturation time of their Markets, not by the Markets themselves, and (crucial to the core design) contain the Decisions of several different Markets.

5) Vote Matrix – The total matrix composed of each Ballot from all Voters for a period of time (figure 2).

6) 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 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, an 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.

3) Trading – With the market built, it can now be advertised to traders, who buy and sell shares of the States of the Market.

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) Market Matures – On this date (post-event), Voting on the Outcome of the Market Decisions begins. Voters submit encrypted votes.

6) Votes Decrypted – After the Votes have included into the blockchain, Voters reveal the symmetric key used to encrypt the votes, allowing them to be read into the consensus algorithm.

7) Market Expires – Votes are run through the consensus algorithm to establish the Winning State of the Market.

8) Final Sales – Market-maker stops determining the market price, and instead takes the price of Winning State Shares as the unit price (1), and the price of all other shares as zero. All traders sell for the unit price to recover BTC.

### *(iii) 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 (Truthcoin 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) 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"[3] 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 as always been useful for vision [reduced search costs]) and in third the Statue of Liberty (a large, visible, iconic, unique 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 3)*

1) 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).

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

3) 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.

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 minimizes total squared difference from a case using the weights of the previous period.

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

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 simple correction is applied: multiplication by previous period reputation vector over its mean. This 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) $r_{t,n\times 1} = N(\, c^{adj} \times \frac{r_{t-1,n\times 1}}{mean(r_{t-1,n\times 1})})$

9) Finally, decision outcomes for each Decision are calculated as a weighted average over the vote matrix, with the reputations as weights.

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

### *(vi) Reputation Based Coin Redistribution (RBCR)*

1) After a round of voting, coins are redistributed among all of the accounts.

2) For each account, I average the value of the previous block with the value represented by the new reputation block.

3) I chose, arbitrarily, a smoothing parameter alpha=.1 (weighing the new value 10% and old value 90%). 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. Over time, the economics of multiple voting rounds adds a second (and more important) incentive of revenue maximization.

2) Fees and dividends:

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

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

3) These fees accumulate and are gradually paid out to the BTC addresses registered to TRC Owners.

4) The gradual payout:

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

b) Offsets the constantly present incentive to be myopically dishonest for immediate trading advantage.

c) Encourages behaviors that will maximize the total future trading volume (honesty and entrepreneurship).

### *(viii) Measuring Oracle Risk*

1) The efficacy of these protections is actually measureable, adding a few minor layers of protection and enabling skeptics to understand the risks.

2) Recall summary of Market timeline:

| **Phase** | 1 (Trading) | 2 (Ex-Post Trading) | 3 (Judgment) | 4 (Settlement) |
|---|---|---|---|---|
| **Begins When** | Market Written (Trading Begins) | Event Occurs | Market "Matures" (Judging Begins) | Market "Expires" (Judging Ends) |
| **Plausible Duration** | 6 Months* | 2 weeks | 2 weeks | Indefinite |

3) For example, a Market written 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, during which the actual event has occurred but no judging 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 prices to converge quickly to their post-judgment value (0 for all failed states and 1 for the single successful state).

6) If assumption b is violated, and there is 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 'oracle risk/failure'. We can use this metric to calibrate possible improvements.

### *(ix) Voting Strategy (figure 4)*

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 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 cost to accurately resolve a Decision is very low (lower than the cost of active coordination). The Cheapest Ballot will be the Realistic Ballot, as all fully-coordinated Ballots would provide the same benefit (the Realistic Ballot has the (lowest cost)/(same benefit) ratio). As some agents may be 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 coins 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 coin Owners and therefore Voters). Nonbelievers are likely to also be non-Owners. Those who lose the faith have no reason to neglect or interfere with the project as they can just sell.

3) Although an attacker with an extremely high proportion of Truthcoins could attempt to alter the judgment process of a Decision for personal gain, any attack with <50% of the voting power will fail outright, exposing the liars to huge TRU losses.

4) Attacks which attempt to take advantage of Voter laziness are extremely dangerous, as the timeline established in the previous section ensures that such 'gaming' would be visible in advance to Voters who can profit by blocking the attack. By making a special effort to vote for the vulnerable Decision, or submit other votes sooner rather than later to increase their coordination influence, rescuer Voters can profit immensely from RBCR.

5) An attack with >51% of the voting power would be able to successfully alter the state of all Markets 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 >51% Ownership attack is unlikely for several reasons: stake, trust, and coordination.

   a) Stake - As Truthcoins cannot be simultaneously spent (transferred) and used to vote, an 'Ownership attack' would collapse the market price of Truthcoin/Bitcoin before anyone could liquidate. As the network grows, adding more Markets and transaction fees, the market capitalization of Truthcoin (a function of transaction fees) would also grow, making a 51% attack incur a higher and higher opportunity cost (as an attacker forgoes the BTC he could acquire by instead selling).

   b) Trust - Even an attacker-coalition with, say, 70% 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, a hypothetical double-agent 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 70% 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 massively iterated prisoner's dilemma.

   c) Coordination - Lastly, a >51% 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 dividend income. To achieve a great profit quickly, the attack must distort many Markets (as each Market has a bounded loss). Operationally, this entails the purchase of cheap shares (of realistically unlikely states) which will later be worth 1 unit after the attacker-coalition re-writes history.

      ii) To succeed, they coalition must agree on the Markets to distort, and the false state they would like to replace with the realistic state. 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 states become known, participants have an incentive to buy shares of those states until they are priced at 1. 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 cannot exist), 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 cannot 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, if we assume that there is a Ballot of at least 10 Decisions, and two 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 TRU in order to ensure that every single Decision is judged accurately (and that they profit handsomely from RBCR).

### (c) Mining Activity

1) Miners are paid, in Truthcoin, to advance the Truthcoin blockchain. This provides an incentive for Miners to keep the value of Truthcoin high.

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 a hash, date (block number), and payment; the literal content of either may be revealed several blocks after inclusion.

4) Miners cannot censor votes, because blocks with relatively low cumulative participation are marked as invalid.

   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 for the previous voting round.

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

   c) Blocks are invalid 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.

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

5) If the implementation requires trades to occur within Truthcoin blocks (which it may not), Miners would need a compelling reason to block trades, as Owners/Voters collect 1% of each trade and Miners every incentive to make the coin as valuable as possible.

### (d) Authoring Activity

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

2) Three separate fees, in two phases are paid to successfully create a new prediction market (figure 5).

3) Phase 1 – Adding Decision(s)

a) $K * Fee_1$

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

ii) Decisions are always: yes/no/unknown (or 1/0/.5).

iii) As Voter 'participation' falls below a target (95%), this fee rises.

a. Voters already have a strong incentive to judge all Decisions (as falling behind the average participation results in Truthcoin 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.

4) Phase 2 – Adding Market

a) $b \log(x)$

i) Seed capital required to 'make market'.[4] 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 infinite market liquidity.

ii) 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 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 trading volume of 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).

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

5) Phase 2 – Adding Market

a) $N^2 * Fee_2$

i) $N$ is the number of states of the Market.

ii) $N$ 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 using this to calculate the market price. I anticipate this to be very cheap, but not free.

iii) 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). Network could suffer abuse on Markets with a huge number of states.

iv) $f1(x) = aX^2 = f2(x) = b\,log(x)\,@\,x = 8.$

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

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

6) Trading Fees are paid out upon expiration of the Market.

Authors get half of all trading fees (recall that Voters receive the other half).

Authors therefore act as entrepreneurs.

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

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 an infinitely 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 eliminate the requirement that Traders trust Authors and transfer the judgment to an impartial third party.

iii) Conversely, Authors enjoy the total lifetime economic benefits of a Market, receiving 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 generate 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.[5] Although the sum of all marginal updates to the market price is unknown, the trading fees for this Market would likely have been substantial.

7) Ensuring Measurable Market States

a) Recall that the Truthcoin votes are scored on Consensus – i.e. how well one Voter's votes agree with those of another Voter. Consensus relied on the assumption that reality was measurable at low search cost.

b) Recall that it is possible to coordinate a Vote 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) ∞ 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. In short this provides a fail-safe which guarantees the 'easy search' assumption (low search cost): lazy Voters will seize any opportunity to turn on you if they can (and they can if your Decision is too confusing).

c) Coordinating on .5 results in:

i) Authors loss of their claim to the trading fees (as a result, Authors have zero incentive to write Markets with any Decisions that might even slightly be too difficult for Voters to determine the ultimate state).

ii) The shares of permanently unresolved Markets are never repurchased by the market maker at the unit price (as would happen otherwise), but they can be sold at their current market price (which would quickly and inevitably converge to a uniform distribution) allowing Traders to recover some money for their shares.

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

iii) A decrease in the 'catch' parameter (which defines the length of the central range within [0,1] that resolves to .5), decreasing the likelihood that future Decisions resolve to (.5). Conversely, low % of .5 "unresolvable Decisions" will increase the 'catch' parameter, within bounds. This acts as a negative feedback loop, where the network responsiveness to incoherent Decisions will always have a helpful degree of context. For example, this discourages an irrational but possible Voter bias toward ruling .5.

### (e) Trading Activity

1) The central goal of a prediction market is to have Traders pay $\boldsymbol{x} \in (\mathbf{0}, \mathbf{1})$ units for shares which they either a) sell either at a future market price, or b) upon maturation of the Market, sell for 1 unit if their event occurs and 0 if it does not. Theoretically, efficient markets will converge "the probability 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-judgment) and paying out at the unit price per share (post-judgment).

2) However, Traders also pay a small fee, arbitrarily chosen to be 1% of their pre-judgment buying or selling activities (vastly smaller than the implied and actual fees for modern financial/betting institutions). As the Traders are the primary beneficiaries of the availability of this service, it is they who must pay for the Voter/Miner overhead.

3) Censorship resistant and confidential; anyone can make pseudonymous trades via Bitcoin. Each trade increases the trading fees collected and the subsequent dividend payments to Truthcoin Owners (Voters and Miners).

## Article III. Scalability, Extensibility, and Customizability via Intentional Forking ('Branching')

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 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, in Truthcoin, the values held by each account represent reputation and relative influence. Forking the reputation by disagreeing on reality would indeed be as frustrating as a Bitcoin fork, but as Withdrawal transactions are delayed for several blocks (precisely for this reason), and Bitcoin transactions cannot be double-spent, one cannot double-extract Bitcoin from the system via fork.

4) What is possible, however, is to fork the project to half the future judging activity required on each of the two new blockchains. 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 change the quality of the Decisions accepted within that blockchain, for example to create "Truthcoin Sports" or "Truthcoin Finance". By forking off a new blockchain, all previous Owners would maintain their old Truthcoins (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 chain. Eventually, some Owners would sell, or simply not use, their coins of a disliked chain, and "Truthcoin Sports" would eventually be owned by individuals especially interested in sports. When "Truthcoin Sports" later splits itself into "Truthcoin Sports:Basketball" and "Truthcoin Sports:NonBasketball" (because, for example, there are just so many basketball Markets), the reputable sports fanatics owning Truthcoin Sports (and no other Truthcoin Owners) will have their voting power transferred to the two new chains. 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 an open source software project, the entire mechanism can be forked 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., and allow anonymous Bitcoin-based participation without revealing any information about Markets, prices, or outcomes to the public.

# Article IV. Implementation Details

1) I outline here a few basic thoughts on implementation. My expectation is that more experienced computer scientists will quickly come up with superior strategies.

## (a) Basic Aspects

### *(i) Block Structure*

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

### *(ii) Validation Rules*

1) Writing a blockchain with different fields and block validation rules has already been done so many times that there are currently over 70 tradable, useable (if not useful) Altcoins[6].

2) Transactions should obviously 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.

## (b) New Issues

### *(i) Market Maker – Message Signing*

1) Most critically of all, this system will have to sign Withdrawal Transactions so that users can bring Bitcoin out of this system and back into their personal wallets. I have deliberately avoided consideration of this issue, as I have low cryptography experience and others will have better ideas.

2) However, for the sake of completeness, consider the following options:

   a) Master Key: Simple oracle controls all Bitcoin accounting, watches the Truthcoin network and signs BTC transactions several days later unless it detects abnormalities in the blockchain, in which case it calls the development team for emergency Decision making until we figure out what went wrong. Signing parameters would be derived from multiple agents to prevent any individual from using the private key by anyone.

   b) A constantly updated zero-knowledge-proof accounting-system similar to Zerocoin[7]. Zerocoin is promising because it allows one to 'store' coins in a large pool and then 'withdraw' them later under relatively flexible conditions. The downsides are that it is complex and untested.

[6] http://coinmarketcap.com/
[7] http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

c) The method that most mirrors the logical functionality of the system would be to build an M-of-N multisignature withdrawal transaction with very large N (per miner) and M= (p=.51*N), and force each block to have a valid signature to the transaction that was written x=10 (more than the recommended six) blocks ago. Thus the Miners are agreeing on who is to be paid, which they logically already endorsed by participating in the system. This idea is complex and full of incentive questions. Moreover, currently Bitcoin has an N=21 limit[8]. Signatures could be sampled randomly according to Ownership to circumvent this imperfectly, or blocks could be required to accumulate signatures over time. One improvement could be to start with a requirement of p=100% miner signatures, and gradually reduce this as time goes on in a kind of Dutch auction. Eventually, then, no transaction will go unsigned forever (a disaster) but transactions will be signed with the maximum possible percentage of agreement. Miners will always sign, as this transaction contains their dividend payments, and Sybil attacks would be difficult because only those who mine blocks have a change to enter the signing lottery.

d) Master Key: Users send transactions to Oracle, who on request provides a refund transaction which is incrementally updated via LockTime and sequence number.

e) Use of external techniques such as Open Transactions[9] system of federated servers bound by triple entry bookkeeping.

f) Small modification of the Bitcoin protocol to accommodate this system, as was recently done with OP RETURN[10]. Possibly there can are or could be special addresses for which complex events can move the coins without trusting an oracle. Bitcoin script seems flexible.

g) Simply add on Bitcoin functionality and release BothCoin as an Altcoin for testing, after which attempt to reintegrate into Bitcoin or, worst case, fork Bitcoin and compete with it.

3) Again I fully expect these ideas to be abandoned in favor of those from experienced computer scientists. I will even redesign the system around what is possible if there is sufficient reason.

4) If there is no input, my most likely strategy would be sequential intra-block (SIB) trading, with a planned ZeroCoin implementation

### *(ii) Computational work for SVD*

[8] https://bitcointalk.org/index.php?topic=215213.0
[9] Open Transactions
[10] OP return

1) Recall that Voters select the True/False status of each Decision. The vote matrix is [Voters, Decisions], meaning that at (for example) 10,000 users and 100 Decisions (my expectation) the matrix is quite large. My testing on an average computer indicated that the consensus algorithm ran for over 60 seconds on such a matrix, although I used R (not famous for speed) and made no effort to optimize with respect to speed.

2) We will likely have to limit the total number of Voters (but not Owners) on a single blockchain to 10,000 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 > 1/10000th Truthcoin (the minimal un-removable amount). This limit could also be increased as computers become faster.

### *(iii) 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. Possible speedups:

   a) Complete use of Master Key oracle for all Bitcoin accounting, using RAMP[11].

   b) Simply wait for GHOST[12] or something similar[13] to improve Bitcoin transaction speeds.

2) Fast Sequential Intra-Block (SIB) Trading

   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 trade, with ultimately only one timestamp 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 funds.

   b) Payouts to Authors and Miners can be updated via sequence number, and published in blocks to wait until they are sufficient deep in the chain (figure 6).

   c) The Double-Spend 'Problem' in Within Blocks

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

[11] https://en.bitcoin.it/wiki/Contracts#Example_7:_Rapidly-adjusted_.28micro.29payments_to_a_pre-determined_party
[12] https://eprint.iacr.org/2013/881.pdf
[13] http://roamingaroundatrandom.wordpress.com/2013/11/30/bitcoin-idea-temporary-notarized-wallets-secure-zero-confirmation-payments-using-temporary-notarized-p2sh-multisignature-wallets/

ii) The most important advantage here is that, as the double-spent transaction unwinds, the trade also unwinds. Traditional double-spend involves the sale of a good or service for money, and the attacker makes off with the good while paying himself, but here the exchange of Bitcoin for shares and back ('double-trade') takes place within the same transaction, so the double-spender ends up unwinding his second transaction and the second 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, the double spend is just a pointless risk of money. To prevent spamming several mutually-exclusive transactions we could require a tiny micropayment for each submission.

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[14] psychological advantage to a trader in later trading. Although this may work in traditional markets for a variety of reasons, it has been shown that in binary prediction markets so called manipulators actually increase market efficiency and on average improve the bottom line of non-manipulators[15]. Either way, we collect transaction fees for these transactions.

d) Fields of a SIB transaction:

| Field | Example | Description |
|---|---|---|
| Account | TLoxo4R… | A Truthcoin address that has already been funded with Bitcoin. |
| 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. |

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

e) Will algorithmic trading extract rents?

i) This environment has extremely competitive features (unlike those of a traditional fiat exchange), and in general barriers to entry are spectacularly 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.

ii) Moreover, this exchange does not employ high/naked leverage/margin (which creates fragility and momentum), feature naïve individual investors/proxy-investors (hedge funds, mutual funds, pension funds, and other 'agency costs' led by disinterested and incompetent third-parties, which serve as a source of rent-extraction), operate with the approval of a regulatory environment (which allows scam artists to operate comfortably under the illusion of consumer protection), entail an inscrutable tax/fee/legal structure (allowing 'outsiders' to be fleeced), etc.

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

3) Privatize Exchange info centrally.

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

b) As many trades offset each other, this might save on transaction fees, yet because of the delay in making trades into the official blockchain there is increased basis risk.

### *(iv) Preventing Active Coordination*

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

2) To make the voting seals credible, consider the following schedule: encrypt vote with symmetric key encryption, voting deadline passes, reveal encryption key, vote decrypted. Sharing key before voting deadline could allow someone to change your vote (potentially in a malicious way that causes you to lose TRU), so no one could reasonably ask to know your key or vote. This scheme also prevents you from sending 'spending' your coins and voting with them at the same time, which I think is simpler in terms of standardized, fungible buying/selling.

### *(v) Floating Point Math / Decimal Precision*

[16] http://www.extremetech.com/extreme/154977-high-frequency-stock-traders-turn-to-laser-networks-to-make-more-money

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.

### *(vi) Initial Allocation of Coins*

1) One of Bitcoin's most successful implementation details was the Decision to gradually introduce the –initially worthless- coins to existing users at a geometrically decreasing rate. This was such a stroke of genius I would like to replicate it, but there are a number of problems.

   a) Work Problem

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

      ii) The Work problem prevents a Bootstrap Mining Scheme as done with several Altcoin (fast release for Miners before reaching a steady state of 1% demurrage or inflation).

   b) Trust Problem

      i) Initial coin Owners must be trustworthy to vote, yet they will not have established a reputation. This favors some kind of cost, such as the Mastercoin strategy of a donation address.

      ii) The trust problem prevents us from, say, forking the unspent Bitcoin set, unfortunately.

   c) If I had to pick something: I would make a significant portion of the coins, say 95%, provably unusable, and give the rest to myself to ensure honest voting during the initial states of the project, and let demurrage and RBCR siphon off the unusable coins over time. This is consequentially similar to what Satoshi did with Bitcoin.

# Article V. Future Plans

## (a) 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 has no adverse effect upon exsiting Traders and does not allow the market maker to run out of money. 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% for a binary market). It would be convenient if interested parties could donate to a Market to increase its liquidity, trading activity, and accuracy.

## (b) Partial Incoherence

1) Currently if any part of any dimension of a Market is ruled 'Unknown', the entire Market is essentially disabled as the price of all states would equalize (and no one would any longer have a reason to trade based on the underlying information). Instead it would be desirable to only have that Decision disabled, such that a Market with 4 states, instead of converging to (.25, .25, .25, .25), could converge to (0, .5, 0, .5) reflecting what had been marginally decided.

2) I'm very confident that this is easy, but I haven't yet done the algebra required.

## (c) Intelligent Decision Fees

1) To allow reuse of Decisions, they are created in a first phase, paying K for each Decision.

2) Then 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 $b \log(N) + f_2 N$.

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 $Cost(O, B_t) = f_1 K + f_{1b} K'$, 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 only one Market). The incentive structure works best when there are many Decisions. Possibly the first 20 Decisions can be free, or extremely inexpensive.

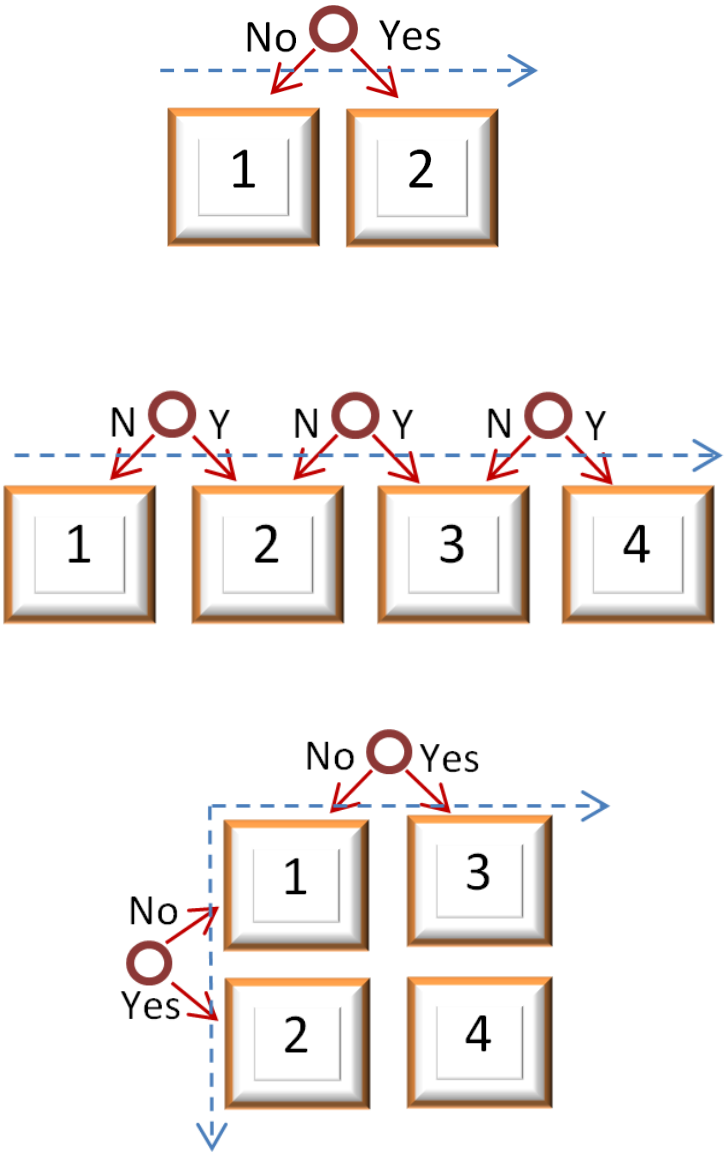



Figure 1. Graphical representation of three prediction markets. Top, the binary form popularized by InTrade, with one dimension (blue dashed arrow), one decision (red circle), and two states (yellow squares). Center, a market with not two but four mutually exclusive states (for example, the winner of a 4-team tournament) and three decisions. Bottom, 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[17] [18], such as the relationship between an election result and the achievement of an economic goal a year later.

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

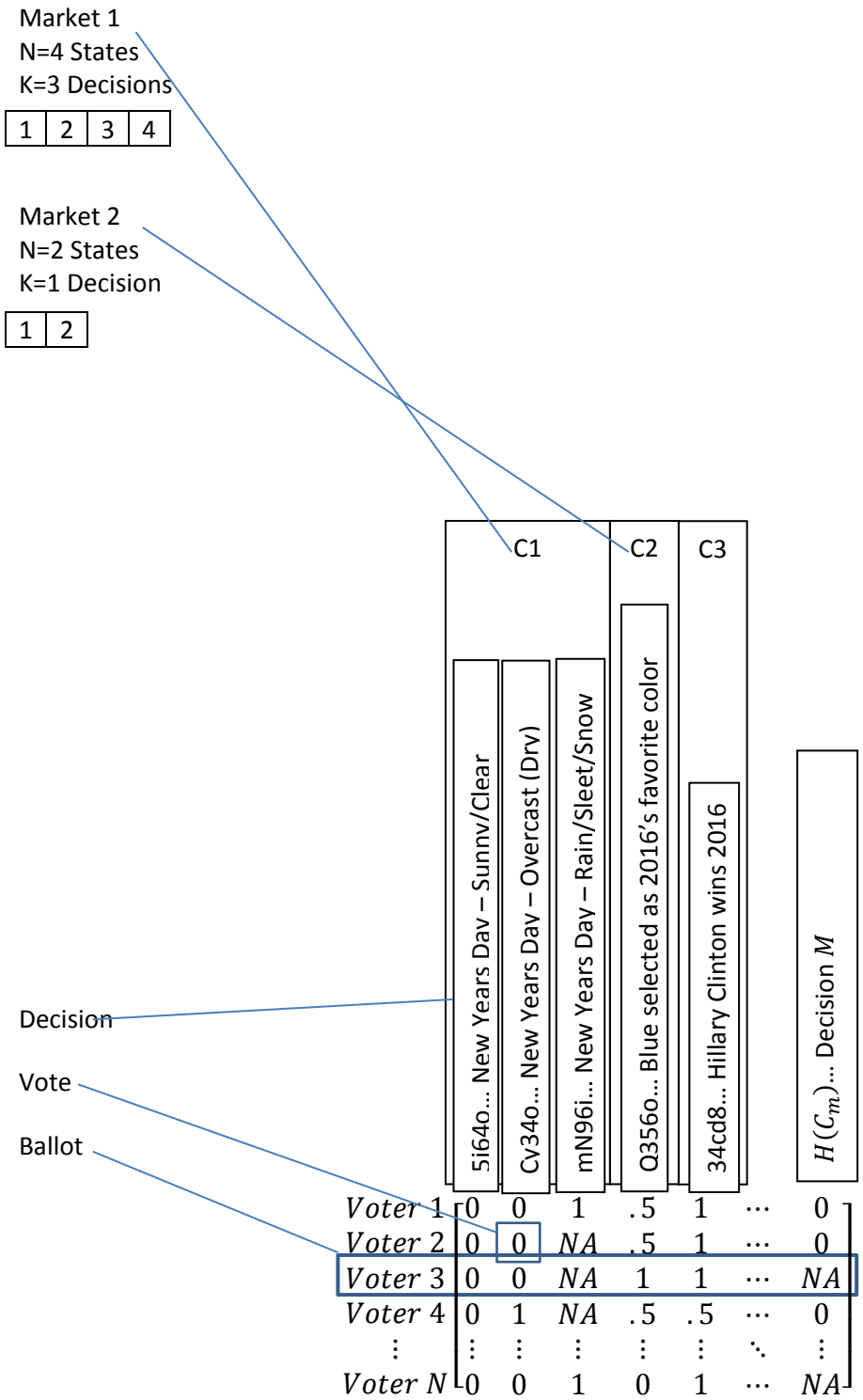



Figure 2. A hypothetical January 2017 Vote Matrix, with annotations.

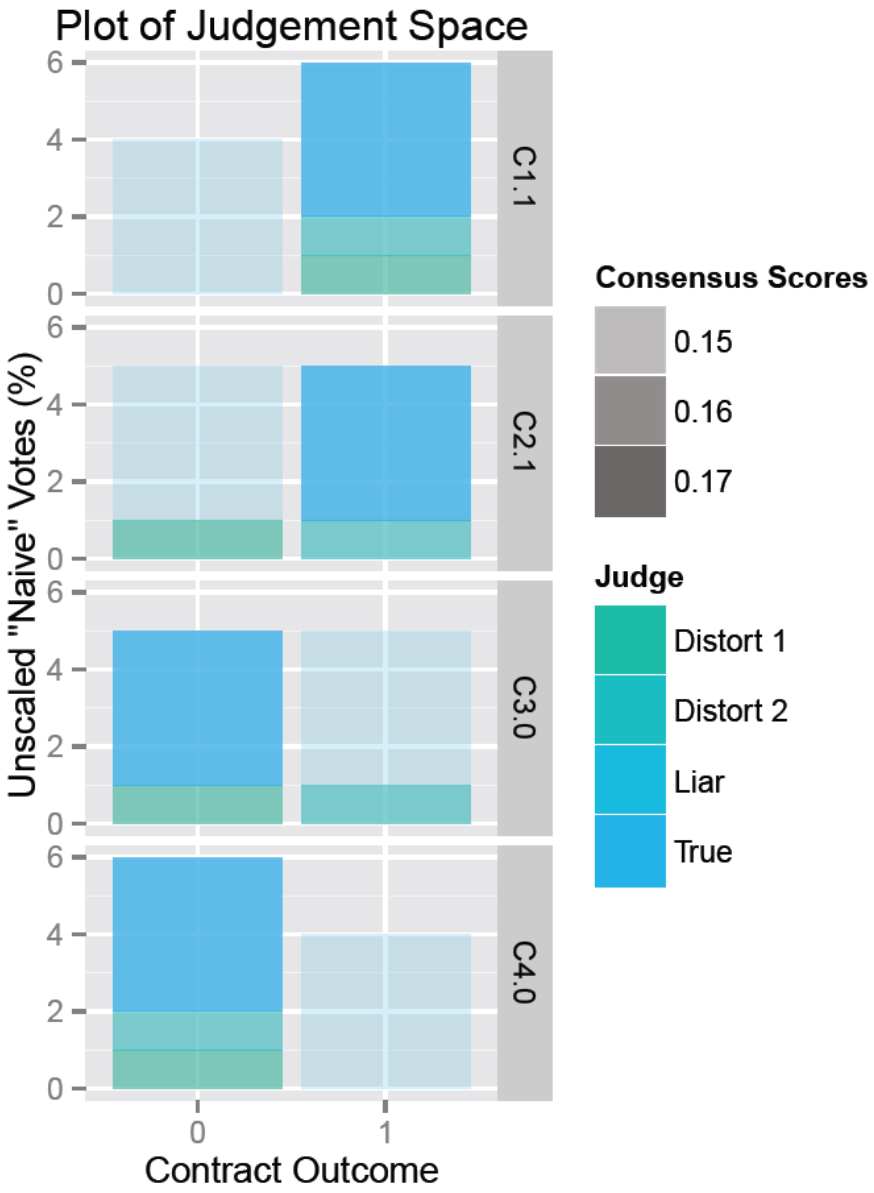
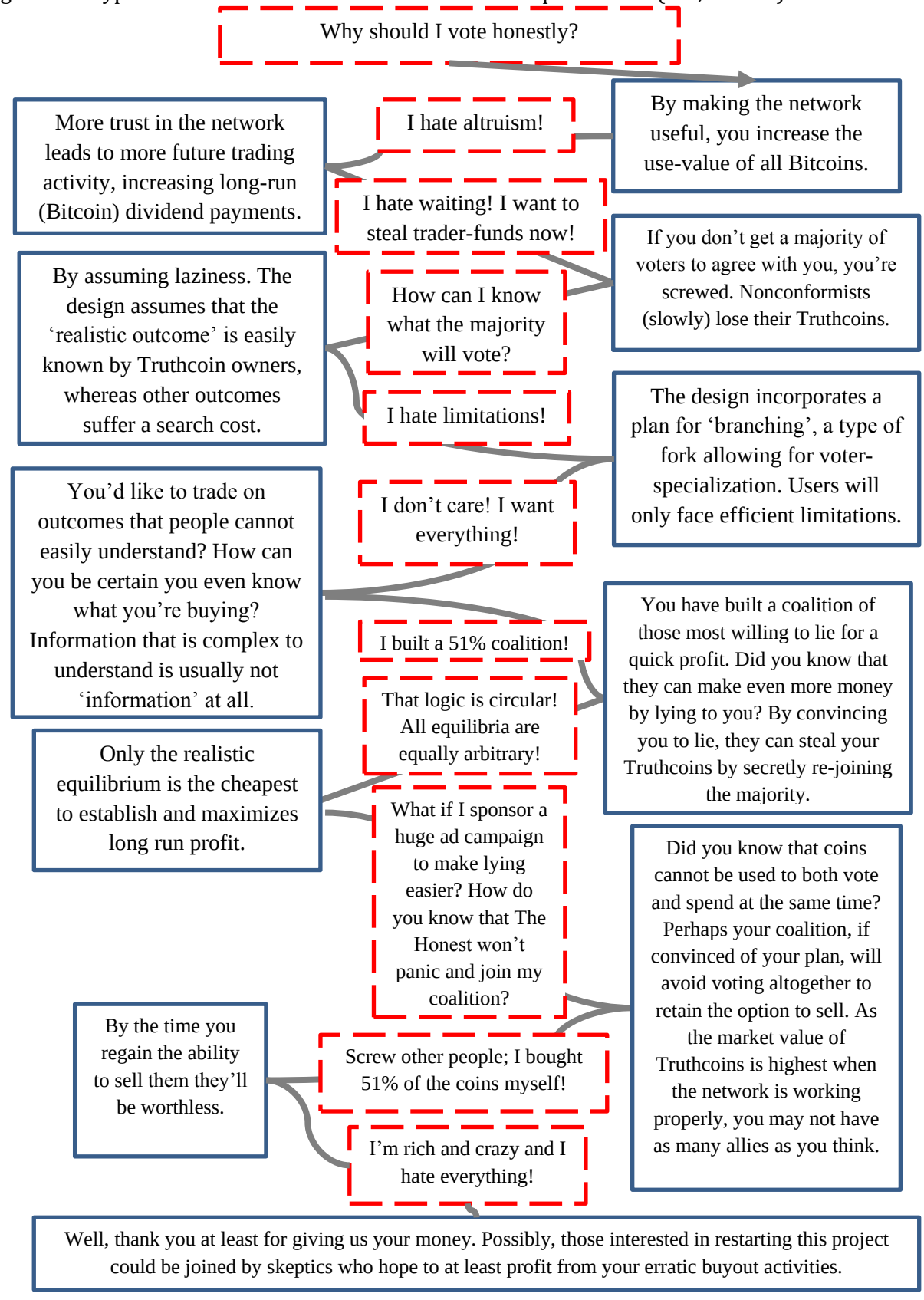



Figure 3. Graphical representation of a sample Vote Matrix, with 4 voters (color), 4 contracts (rows, right axis, above period), vote percentages (left axis), No/Yes outcomes (bottom axis, 0 and 1), consensus score (how well voters agreed with each other, opacity), and result (right axis, below period). Notice contracts C2 and C3 (center): despite an apparent 50-50 tie in the quantity of votes cast for each outcome, the fact that voter 'True' was substantially more conformist than voter 'Liar' gives enough extra weight to his votes to shift the outcomes of C2 and C3 from .5 and .5, respectively, to 1 and 0, respectively. Not a single vote was left Missing, or cast for .5, so these columns are not represented.

Figure 4. A hypothetical flowchart-conversation with a skeptical voter (red, dashed).



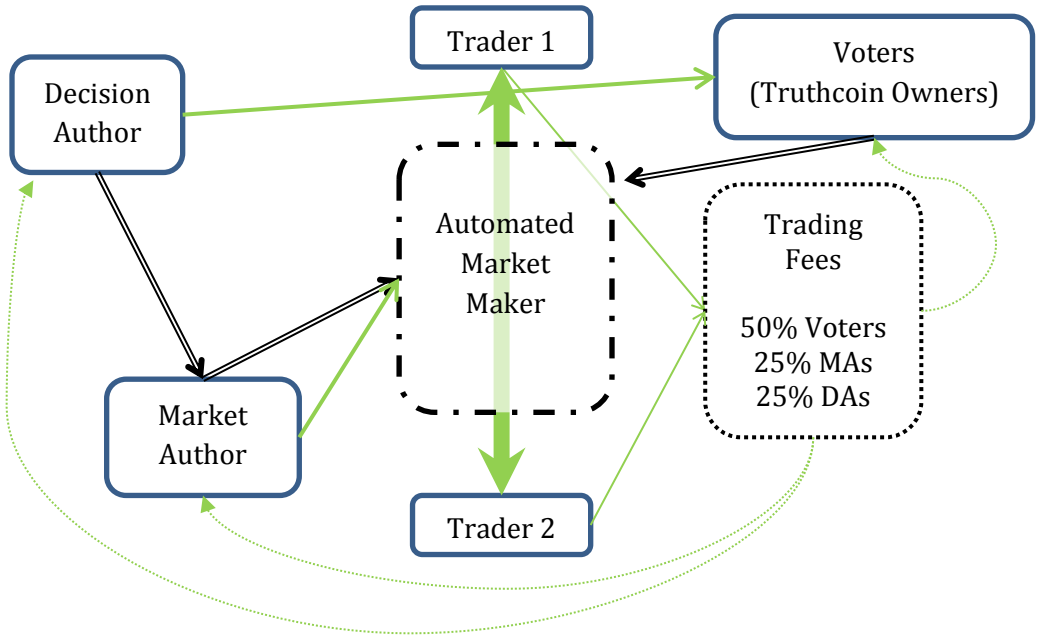



Figure 5. The flow of costs (green solid), revenues (green dashed), and information (black double) among various agents (blue solid) and accounts (black dashed). The horizontal axis corresponds to time, and line widths correspond to expected magnitudes, with the exception of revenues (whose magnitudes are a function of trading volume).

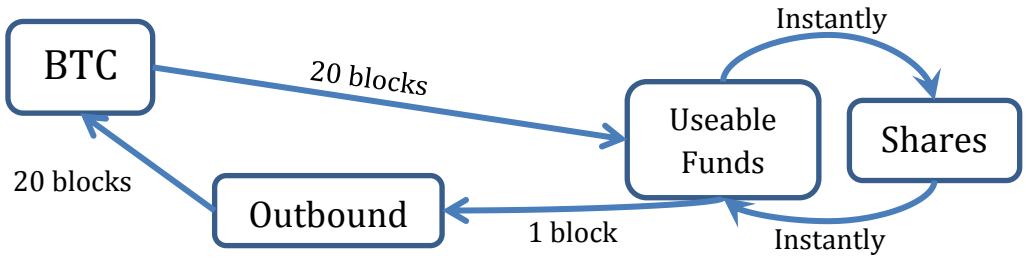



Figure 6. Movement and timing of BTC through the Truthcoin marketplace.