Prediction Market Uses (Other Than Prediction)

Paul Sztorc
truthcoin@gmail.com
Version 1.4 – Dec 14, 2015

Summary

Prediction Markets (PMs) can do more than predict the future. First, the mere presence of a PM-based forecast can conclusively end debates, prevent lies, encourage and protect whistleblowers, and provide decision makers with honest advice. Secondly, PMs have applications altogether beyond forecasting: through creative use of the tradable shares, one can provide financial services such as risk-management, insurance, retirement portfolios, recreational gambling, etc. Finally, I discuss five 'Big Ideas' for cryptocurrency PMs: [1] a decentralized governance model for hard forks, [2] blockchain crypto-assets with a stable fiat-value ("BitUSD"), [3] SPV-compatible (headers-only) colored coins, [4] the provision of 'public goods' (such as lighthouses) without coercive taxation or third-parties, and, [5] smart contracts and decentralized applications.

Applied Prediction

Ending a Debate

Prediction markets can put an end to public confusion on any issue where the evidence will eventually settle one way or another (by providing an immediate 'best guess' of that eventual settlement).

"The United States Surgeon General to issue an official statement, linking tobacco cigarette use to lung cancer and chronic bronchitis, on or before Jan 1st, 1966?"

This statement turned out to be true.[1] Although common knowledge today, this information was very surprising at the time, which implies that a prediction of such an announcement would have been controversial and suspicious. Note the arbitrarily chosen maturity date (1965) and source (US Surgeon General). Those who disagree with the suggested date or source could Author a different Market to their liking (to the benefit of us all).

"2015-2020 to contain at least two of the warmest years on record, as measured by GISTEMP at http://data.giss.nasa.gov, dtS Global table, column J-D?"

Global warming is a hotly debated issue. Those who feel that the earth is warming can profit from that information, at the expense of skeptics. Likewise, those who are skeptical can 'set the record straight' while taking money directly from their ideological opponents.

This contract has the additional benefit of forcing a clear definition of global warming. Such a definition shifts the focus from politics to information. Those disagreeing with the timing (2015-2020) or source (NASA) have every opportunity to Author a different Contract to their liking.

Detecting a Lie

"During his (1989-1993) term as President, George H. W. Bush will not introduce new taxes nor increase tax rates?"

"During his (2009-2013) term as President, Barack Obama will close the detention facility at Guantanamo?"

Both of these claims turned out to be false. Did either candidate know that he would be unable to deliver on his promise? No one can say for sure, but if this contract were trading at a low price, voters would understand the low quality of the pledge. Can voters make a truly informed decision *unless* there is a PM for every campaign promise?

[1] http://www.cdc.gov/tobacco/Data_statistics/sgr/history/index.htm

Whistleblowing

Whistleblowers risk lawsuits, job loss, prison time, and their lives, and yet they are guaranteed nothing in return, even if successful. Can we do better? Recall that PM incentives can prevent lies about a target claim. They can also induce awareness of private but interesting claims.

"The United States Anti-Doping Agency (USADA) to conclude that Lance Edward Armstrong engaged in the use of illicit performance-enhancing drugs ('doping') before January 1st, 2013?"

This claim turned out to be true, although it was vehemently denied for years (the reporter who broke the story even facing a libel suit before his evidence was eventually accepted by the public and professionals[2]). Many insiders were later revealed as having known.

"It to be publically revealed that the United States Federal Government collects (and retains indefinitely) all emails sent both by foreign and US citizens?"

Edward Snowden could have instead anonymously created this contract, and bet on 'Yes', alerting the public to this issue. Snowden could then continue to buy 'Yes' shares as they were bid down by an incredulous public or a manipulative government. Ultimately, when his documents were released he would make a fortune.

Whistleblowers can also 'bluff', or whistle-blow without actually coming forward, leaking documents, or even obtaining documents at all. One could, on suspicion alone, anonymously create the relevant market, and leave it to the insiders (who *do* have access to the privileged information) to betray each other for profit in the face of an apparent failure of their conspiracy. As the market nears maturity, insiders with a financial position might realized they've been tricked, yet decide to leak their own secret documents to avoid a loss (more "innocently", insiders could force their organization make to a public admission).

Policy Advice

Multidimensional contracts not only give the likelihood of two events, but also the relationship between events.[3] This would enable us to ask and answer such questions as:

1. If we adopt NGDP targeting, what levels of inflation can we expect?
2. If we go to war, what range of casualties can we expect? What is the worst case scenario?
3. Would our market capitalization increase if we fired our CEO?

Dr. Robin Hanson describes an official governance structure called 'Futarchy'[4] where individuals formally define an after-the-fact measurement of their goals, and then construct multidimensional contracts for decisions related to those goals, and use the decision provided by the market.

[2] http://www.theguardian.com/media/greenslade/2014/jan/28/lance-armstrong-sundaytimes

[3] For the details on how and why this works, see my document covering combinatorial markets.

Summary of Applied Prediction

Having the power to accurately predict the future, prediction markets will expose lies. Additionally, they discourage lies by actively draining the bank accounts of liars. Those who can and would like to make a credible-guarantee, such as politicians, can defend their beliefs and profit from skeptics. Those who uncover amazing secrets can force the general public to trade against the secret, and are thereby compensated for their discovery.

Event Futures

Buyers in a market for, say, oil, can be separated into 'users' (who need oil to heat their homes), and 'speculators' (who perceive the future opportunity to sell oil at a higher price). Likewise, oil sellers may own an oil refinery ('user'), or they may have downward beliefs about the future price ('speculator'). So far we have focused on the speculators, now we shift the focus to users.

Insurance

One could buy 'Yes' in a Market, not because they believe that this event is likely, but instead to hedge their exposure to the event.

"An MMS 6.0 or greater earthquake to strike the greater New York City area during 2014?"

Should this event happen, an owner of 'Yes' would receive an influx of cash to offset any damages done by the hypothetical earthquake.

Individuals might "bet" on natural disaster, death of an essential leader, election of a ridiculous leader, industry-killing technological innovations, crippling regulatory activities, pandemic, disruptive weather or other harmful events. Many corporate boards have already signed legal commitments to reduce/hedge the above risks to the greatest extent of their ability. Any hedging would thicken the market and draw in profit-seeking speculators, who would produce actuarially fair prices as they competed against each other.

Truthcoin insurance has the advantage of decentralization, and so can (at least attempt to) insure events such as warfare, nuclear obliteration, supervolcano eruption, etc. where the ability of the insurance-provider to pay anything (or even be found alive) is in question. Conversely, the primary disadvantage to decentralization is moral hazard: anyone could commit arson on a fire-insured-property and collect nearly the entire value of that property, perhaps even anonymously. For this reason, insurance is unlikely to be offered on outcomes that are easily influenced by the actions of small group of people.

[4] http://hanson.gmu.edu/futarchy.html

Individuals may also like to insure against the solvency of fiat-cryptocurrency exchanges. Not only would this allow individuals to hedge counterparty risk, the process of price discovery would allow an apples-to-apples cross-exchange price comparison, reducing basis risk for arbitrageurs and thickening the overall exchange rate market.

Portfolio Replication

"What will the market capitalization of NASDAQ:GOOG be on Jan 5th, 2015? [200B to 700B]"[5]

Although PMs do not allow a trader to buy or sell actual securities (stocks, bonds, ETFs, etc.), one can build a portfolio (using only cash and PM shares) which replicates its investment performance. [6] To force this portfolio to track the investment yield of underlying security *at all times*, the only requirement is that at least one agent be a member of both systems for the purpose of conducting arbitrage (to collect any manifestations of risk-free profits).

Although this type of activity may be difficult to sustain for small markets, it is probably very reliable for large tradable indices such as Gold, DJIA, Treasury Yields, and FOREX Rates. PMs can always be used to speculate on any published figures (GDP futures, nonfarm payrolls, etc.), and portfolio returns will converge upon maturation, but without a tradable market there will be no guarantee that returns will be equivalent at all times.

Derivatives

Binary

Tradable Derivatives are the insurance of the finance world. Prediction Markets can very easily be used as binary options:

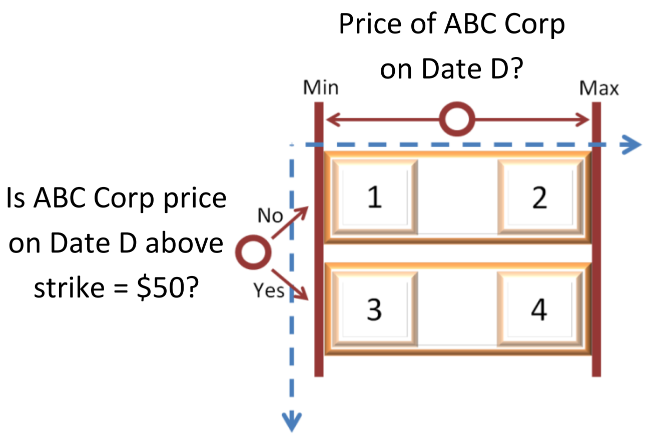
"Greece to make all 2015 coupon payments on bonds (GGGB10YR:IND) in full and on time?"

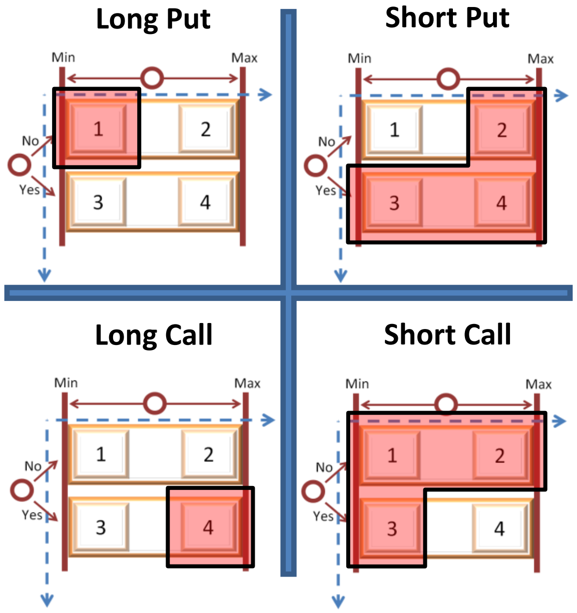
This example is functionally similar to a credit default swap. By revealing the probability of default directly, debt markets would operate with drastically reduced risk. For example, were Greece determined and able to make all debt payments on time, they should theoretically be able to borrow at the risk free rate and escape a debt crisis.

[5] Unfortunately, corporations which undergo restructuring (mergers, acquisitions, demergers, etc.) are likely to have prohibitively inconsistent valuation-metrics. If you have a solution to this problem, please contact me.
[6] http://en.wikipedia.org/wiki/Replicating_portfolio

Put / Call

Multidimensional Prediction Markets can also recreate put and call options (from here, the Put/Call/Binary options can be combined to form any modern financial derivative).





Short Anything - The Other Half of Investing

While it is possible for someone with money (the store of value / unit of account) to willfully invest *in* a good idea, it isn't usually possible to use money to invest *against* a bad idea. Traditional shorting involves [1] borrowing the underlying asset, [2] selling it, and later [3] rebuying it and [4] repaying (covering) the asset. Because this process involves a potentially unlimited[7] magnitude of implied lending, it is facilitated today with trust-heavy financial infrastructure. If an exchange hasn't created a shorting vehicle, or your brokerage firm's margin accounts don't plug into that vehicle, you're out of luck; you *can* call a CEO directly and invest with him, but if you call the CEO directly to bet against him, he will probably refuse the offer.

"Closing price Market Capitalization of Bitshares on March 1st, 2016 ?"

First, it should be obvious that bets against the future exchange rate will pay off if the project is ultimately unsuccessful. Secondly, the creation of a such a Market allows one to recreate the financial infrastructure required to short: by betting that the future market capitalization will be lower than the present market capitalization, traders can put existing owners in a position where they must sell their asset (owners can conduct risk-free arbitrage by selling the more expensive real-asset for 'high' and buying the less expensive PM-asset for 'low', profiting 'high'-'low' today without changing their net investment position). In this way, the PM allows individuals to use money to "sell" assets they don't own.

[7] When you buy, the most you can lose is 100%; when you short, your potential losses are theoretically infinite.

Recreation

In the United States, it is popular to gamble on the NCAA Men's Division I Basketball Championship. The creation of a fully liquid 1x68 market concerning only the champion team (in other words, not a full bracket) only costs about 6 times as much seed capital as authoring a simple 1x2 binary market[8] (although decision fees are 67 times greater).

This allows everyone to compete at once, interactively in a dynamic environment where money can be made and lost before, after, and during a game. Likely, no entertainment experience can compare! Moreover, a prediction market has (by definition) actuarially fair odds (the price is always set to the estimate of the most skilled forecasters). There is no ‘house edge’, and with only a 1% trading fee this is possibly the fairest proposition in the history of gambling.

[8] log(68)/log(2) = 6.087

Five Big Ideas

I now focus on technical opportunities for “blockchain PMs” as they relate to the current needs of the Bitcoin community.

Idea 1: Peer to Peer Governance

Preventing Developer Tyranny

The Hard Fork Problem

Bitcoin enforces rules. With a “soft fork”, these rules can be refined (such that any user can switch back and forth between soft-forked clients), and with a “hard fork” the rules can be actively changed (ie “broken”, such that *all* users must agree to a permanent, one-time switch). On one hand, rules are only useful if they are enforced, (“no excuses”); on the other, it is desirable to be able to replace bad rules with better ones. These aspects are mutually exclusive: either rules *can* be broken, or they *can’t*.

This mutual-exclusivity results in a governance problem: if one group argues **for** a rule-change, and another group argues **against** it, then who resolves this dispute? Bitcoin, designed to be “peer to peer”, cannot permit any “expert” to claim a privileged (non-peer) position of dispute-resolution. Each group can lay an equal claim to Bitcoin’s future; yet, to grant the claim of one, is to deny it to the other.

If a rule-change is introduced before the dispute is resolved, all users, regardless of intelligence or expertise or other virtue, will be forced to adopt, not whichever network they think is best, *but whichever network they think everyone else is adopting*.[9] The very network-effects which ordinarily make Bitcoin robust and tamper-resistant, in this case degenerate the ‘Bitcoin contract’ into a kind of mob rule. Adding to the instability is the dire prospect of a permanent schism (two separate blockchains which never re-merge). While current owners would end up with coins on both networks, by standard network principles (Metcalfe's law, etc) these two networks would, even combined, be worth less than the current network (in no small part due to the resulting public confusion); the setback could last years.

The Solution

A simple 2x2 prediction market (below) solves all of our problems. First, it is inherently viable in at least three ways: [1] it produces a “BitUSD” with the purchase of states {1, 2}, [2] it creates arbitrage opportunities between the real-world exchange rate the PM’s horizontal dimension (State {1} vs. {3}, and {2} vs. {4}), and [3] it allows individuals to insure against the transition (or failure to transition) to a new hard fork (purchases of {1, 3} grant the owner cash if Bitcoin does *not* hard fork, and purchases of

[9] There are many cases where the minority view (or, “less promoted view”) may be most justified. For example, the 2015 Blocksize Debate seemed (pre-Montreal Conference) merely to reflect the ratio of BigBlock-Users (those tending to pay transaction fees, but not to run a full node), to SmallBlock-Users (those tending to run a full nodes, but not to pay transaction fees). Although the BigBlock-ers outnumbered SmallBlock-ers, the SmallBlock-ers ended up having overwhelmingly superior technical justification.

{2, 4} grant the owner cash if Bitcoin *does* hard fork). However, the main benefit is that this PM allows users to make purchases *either of one type of Bitcoin or the other*; if Bitcoin evolves in a direction in which traders do not approve, these traders get all of their original investment back. In this way, the market allows users to sell ("eliminate") their hard fork discomfort.

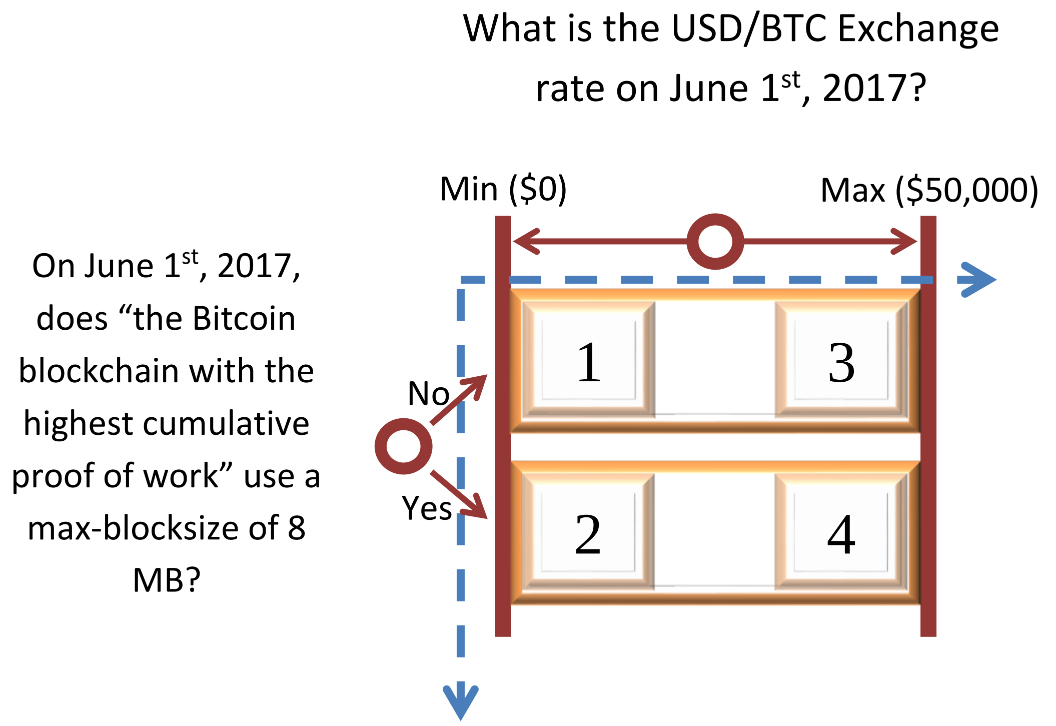

What is the USD/BTC Exchange rate on June 1st, 2017?
Min ($0)
Max ($50,000)
On June 1st, 2017, does "the Bitcoin blockchain with the highest cumulative proof of work" use a max-blocksize of 8 MB?
No
Yes
1
3
2
4

Figure: A market for forecasting (objectively) the exchange-rate effect of an 8 MB blocksize.

A "pro-fork portfolio", has states {1, 3, 4*} purchased in specific quantities: 1 of {1}, 1 of {3}, and enough[10] of {4} to achieve a total investment outlay of 1 unit[11]. If the fork fails to go through, share {4} will be worthless, but {1} and {3} must together be worth 1 unit, producing the full refund. If the fork does go through, {1} and {3} are worth zero, but the remaining shares of {4} will grant traders a long position in the Bitcoin exchange rate. The quantity of {4} shares, determined earlier, will sell for an amount of revenue that, combined with the given original cost of 1 unit, always replicates the return on the Bitcoin exchange rate itself. **Buying the pro-fork portfolio is like buying a "Bitcoin" that you can return if the hard fork doesn't occur.** This logic is the same for an "anti-fork portfolio" (consisting of

[10] While {1} and {3} are purchased in equal quantities, they must be accompanied by a quantity of {4} which varies to induce the appropriate degree of leverage. This amount x^* is defined completely by the current market prices: $x^* = \frac{(p_1+p_3)}{E(H_t) - p_4}$, where $(H_t) = \left(\frac{p_3}{p_1+p_3} * \ (1-(p_2+p_4))\right) + \left(\frac{p_4}{p_2+p_4} * (p_2+p_4)\right)$. Quantity x^* initially equals perfect-refund quantity $x^\ddagger = \frac{1-(p_1+p_3)}{p_4}$, but the quantities diverge as $\frac{p_3}{p_1+p_3}$ and $\frac{p_4}{p_2+p_4}$ separate (as the market prices in differences between each scenario's expected future exchange rate.

[11] This unit (1 USD, 1 EUR, 1 BTC, etc) doesn't matter, only *the percentage return* on it matters.

states {2, 4, 3*}), as well as for a “hard-fork fear portfolio” ({1, 2, 3*}, which goes long one type of coin, short the other, but gets a full refund if the BTC exchange rate collapses[12] in either case).

As trading progresses, onlookers would, today, be able to see and compare two future exchange rates[13]: one with the proposed hard fork and one without. From there, the community as a whole is forced to agree on both the likelihood[14] and the consequences of the fork (ie “if we increase the blocksize, Bitcoin will fall to $150”)[15]. Those who “disagree” are either lying, choosing not to maximize their expected value, or experiencing some kind of psychological episode of bias or self-ignorance. All three types can (and should) be ignored; the dispute is now over (and, crucially, this dispute-ending is known to everyone).

The “Fork Decision Market(s)” can simultaneously evaluate an arbitrary number of mutually-exclusive fork options (and thus avoiding Condorcet’s paradox). Moreover, the market can invoke the fiat exchange rate a second time to price the “full refund” itself in US Dollars[16].

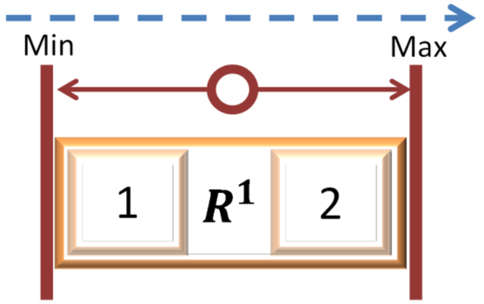
[12] This relies on division, and fails if the exchange rate falls to the value of zero (or if it travels out of range).
[13] In fact, one could (objectively) compare any metric. However, the USD exchange rate is overwhelmingly likely to be the most helpful metric to use, as one is ultimately limited to optimizing one goal at a time, and the exchange rate is itself a metric which optimally combines many sub-metrics.
[14] One of the most threatening/time-consuming aspects of a hard fork is uncertainty surrounding the question “How seriously is this fork being considered?”.
[15] My strong expectation is that the difference in price would be huge—in fact I expect all non-preferred forks to have futures which trade at a near-zero exchange rate.
[16] More details are available at my blog post on the topic.

Idea 2: Stable Cryptoasset Prices ("BitUSD")

Monetary Policy under Perfect Competition

Many desire the advantageous technical properties of the blockchain (cheap, instant transfers, reliability, open access), and yet want to keep their old monetary policy[17]. These individuals desire a "BitUSD" (a unit of cryptocurrency which is constantly worth 1 USD regardless of the USD/BTC exchange rate), or "BitGold", which a PM can actually provide.

What will the USD/BTC exchange rate be on October 31st, 2014? [50 to 4,000]



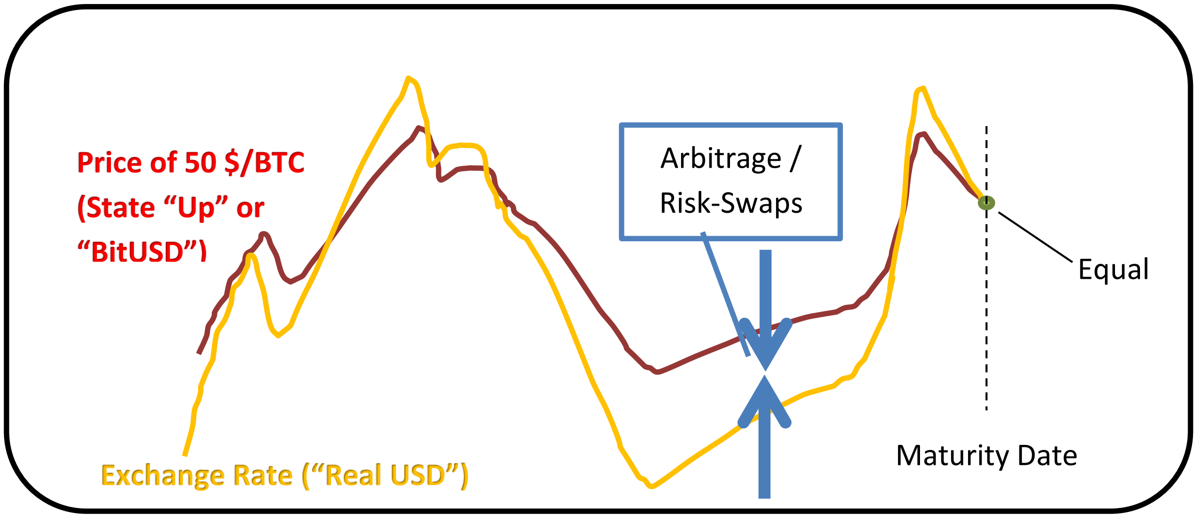
This Market can be traded in two ways:

Market States	Exchange Rate (in $'s)	Owner's **Position**	Value of The Created Share Which the Market Maker Sells You	The owner of this share makes money if...
50 ($/BTC)	0.02,000 BTC/$	"Long USD"	$4000 - Exchange Rate	BTC/USD price falls
4000 ($/BTC)	0.00,025 BTC/$	"Short USD"	Exchange Rate - $50	BTC/USD price rises

The typically expected "No"/"Yes" States are replaced with something more akin to "Lower"/"Higher". Because the Decision was Scaled (not Binary), its Outcome will take on a value anywhere between $50 and $4000. Arbitrageurs can profit by erasing any price-differences, speculators (including merchants accepting BitUSD) can profitably[18] become early-adopters, bearing *only* the technical and social risks of the software design (but none of the exchange rate risk).

[17] Very frequently, one encounters comments (informed or otherwise) such as "the blockchain technology is nice, but Bitcoin the currency is a con", or "Why not tie it to gold?"

[18] It is both logical and desirable (at least at first) for BitUSD to be consistently cheaper than actual US Dollars. This would be due to the multitude of risks associated with newer, unsecured, non-legal BitUSD, low-merchant-acceptance and grants an excess return to those bearing these risks (all BitUSD holders).



These Markets would likely be extremely useful, and therefore extremely popular. It would be more than possible to display these (or any) Markets in an organized way, to boost the liquidity of the entire marketplace and currency system.

“The Arbitrage Tool”

Decision Class: “Long USD”		Today’s Date: 10/6/14			
Date	Oct 31st, 2014	Nov 5th, 2014	Nov 7th, 2014	Jan 15th, 2015	Jan 20th, 2015
Markets Using this Decision	M12ab345:V2 M67ab890:V2^ M34ab341:V4`` M85ab857:V2	M32eb345:V2`` M57db890:V4 M74cb341:V2^	M82gb345:V2`` M77hf890:V3 M64hf341:V2 M55ef857:V2^	M1hip332:V4^ M6jmk832:V5``	M12xz311:V4^ M67zy720:V2``
Price	0.9984	0.9856	0.9702	0.9614	0.9702
Days	25	30	32	101	106
Implied r~*	2.367% ^	19.315%	41.243% ``	15.299%	10.987%
Cumulative Depth	Long: $14,087.41 Short: $29,223.90				

*Would be weighted by market depth.
~Would be a function of the current date.
^Denotes cheapest BitUSD.
``Denotes most-expensive BitUSD.

Note that this scheme exploits Truthcoin’s concepts of reusing Decisions in Markets, and then introduces the concept of a ‘Class’ of Decisions (Decisions which are functionally the same but maturing at different times, which allows arbitrageurs to harmonize prices across time).

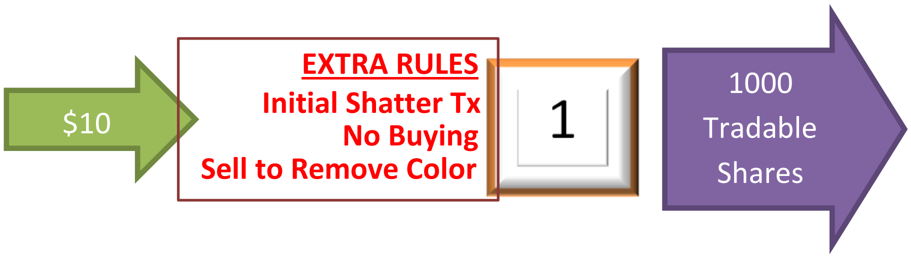
Ignoring technical and counterparty risk, and term structure / yield-curve considerations, those users playing the role of “investment-banker types” can profit over time by converging the “Implied r” values toward the so-called “risk-free rate”. These individuals should also be willing to accept trades near these prices, and may preemptively purchase tradable shares to take advantage of these changing arbitrage conditions. The result is a more efficient marketplace across all BitUSD use-cases.

Idea 3: Protocol-Compatible Colored Coins (SPV, Incentive-Aligned)

Wall St. on the Blockchain

Although our real-life "Stocks and Bonds" are either promissory notes or database entries (both ledger entries or "tokens"), the cumbersome methods by which these assets are created and traded involves multiple trusted third-parties and middlemen. "Colored Coins" aim to replace digital asset ownership institutions with simple Bitcoin transactions (on special Bitcoin value-tokens which have been assigned an arbitrary category or "color").

A PM infrastructure already exchanges cash for shares. To turn PMs into "Colored Coin Issuers", all that needs to be done is *remove* existing functionality. A PM with only one State (ie, not partitioned at all, and containing no Decisions) and only one buy transaction would provide the needed functionality. This single transaction "Shatters" a piece of cryptocoin into tradable shares.



It is difficult to imagine a wasteful creation of Markets, as each requires some actual cryptocoin, and each share-trade entails transaction and trading fees (which profoundly discourages use of excessively-low-value outputs). This Market contains no Decisions and so would never resolve (whatever that would mean), and would exist until all its shares were all discolored.

The key benefit is that such activities take place "within-protocol", meaning that this functionality is compatible with the SPV and headers-only sync concepts of Bitcoin. Moreover, with the protocol aware of this application, it is less necessary to use protocol rules in unintended, unstandardized, and potentially disadvantageous ways (as is currently the case with Bitcoin's colored-coins).

Idea 4: Efficiently Funding Public Goods (Without Trust or Taxes)

The Libertarian Holy Grail

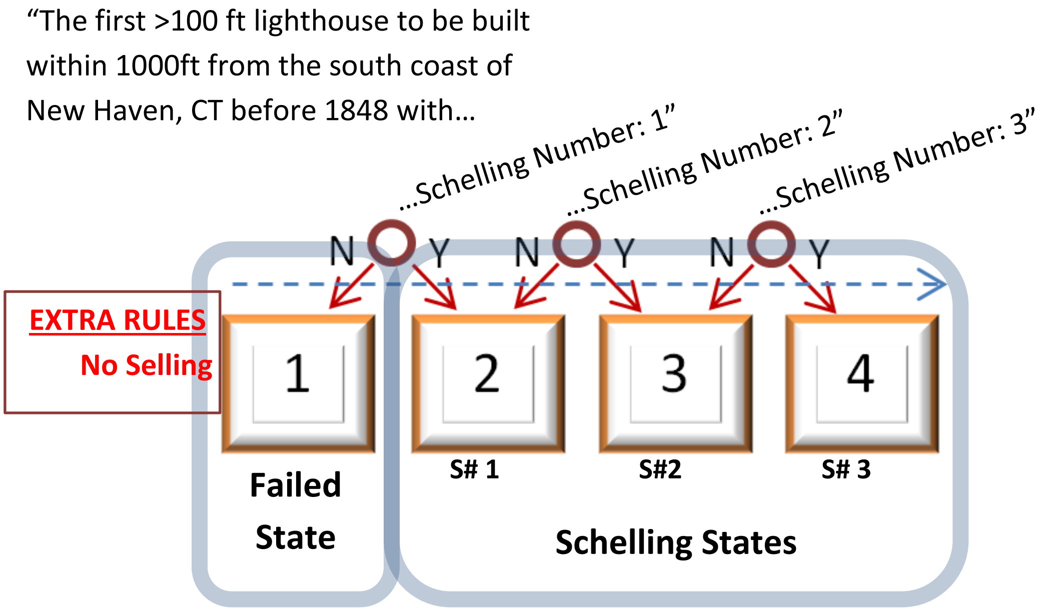


Figure. A special market used to finance a lighthouse. Notice 3 nearly identical decisions, partitioning the market into 4 States. A non-construction of the lighthouse would result in State 1 being the Outcome; hence it is the ‘Failed’ State. Otherwise, the builder/owner of the lighthouse is expected to put a gigantic banner with either a 1, 2, or 3, displayed prominently on the lighthouse in order to control the Outcome and claim the accumulated funds.

Bitcoin users can already pay for public goods, such as roads, lighthouses, national defense, and research projects, through ‘Assurance Contracts’ by using the ‘ANYONECANPAY’ functionality designed by Satoshi.[19] However, users can cancel their pledge (making pledges unreliable and introducing strategic frictions), and, upon success, the pooled funds are merely transferred to an individual (with no guarantee that he has provided, or will provide, the good).

To eliminate these problems, one might build a protocol on top of Truthcoin, allowing “autonomous assurance contracts” (AACs) through the use of ‘Schelling States’.

By definition, public goods are accessible to anyone, and therefore their existence and qualities are publically observable. Operationally, instead of funding a public good with a payment (taxes, pledges, pre-orders, subscriptions, etc.), individuals can lock-in losing PM-trades such that only the provider of the good can make a winning trade and claim the funds.

[19] https://en.bitcoin.it/wiki/Contracts#Example_3:_Assurance_contracts

The funds are collected through a special PM of dimension 1 x (1+N), in which only buying is allowed. Funds cannot be sold[20] (they can only be *redeemed* after the outcome is determined). Contributors then purchase State 1 (the State suggesting the public good was *not* successfully made), and these purchases become the eventual payment to the provider.

Contributors enjoy the beneficial incentives of the traditional assurance contract (getting a full refund if the project is not built). They even enjoy some incentives of the dominant assurance contract: if contributors donate and the project is not built, they actually *profit* by winning any non-contributed money (ie, money spent on Schelling States, or seed capital). Moreover, those who donated the most, and the earliest, would have more shares of the Failed State and “win” the most money. Therefore, the contributors who want the project built –yet believe it won’t be– actually have the strongest incentives to donate as much as they can, as early as they can.

A provider verifies that the market contains enough funds to finance the good, and accepts the contract by making a single gigantic trade on the Schelling State with the lowest price. The provider then creates the good, uses his control over the good to endow it with this State (with a public statement, a huge flag, poster on the interior, etc.), and eventually wins all of the money in this market. The provider holds all the cards in this situation: he need not get involved at all until the market contains an appropriate payment, and he need not worry about his trade been front-run. He is furnished with “an option to sell a good for X amount”, and this option is something he can freely take or leave.

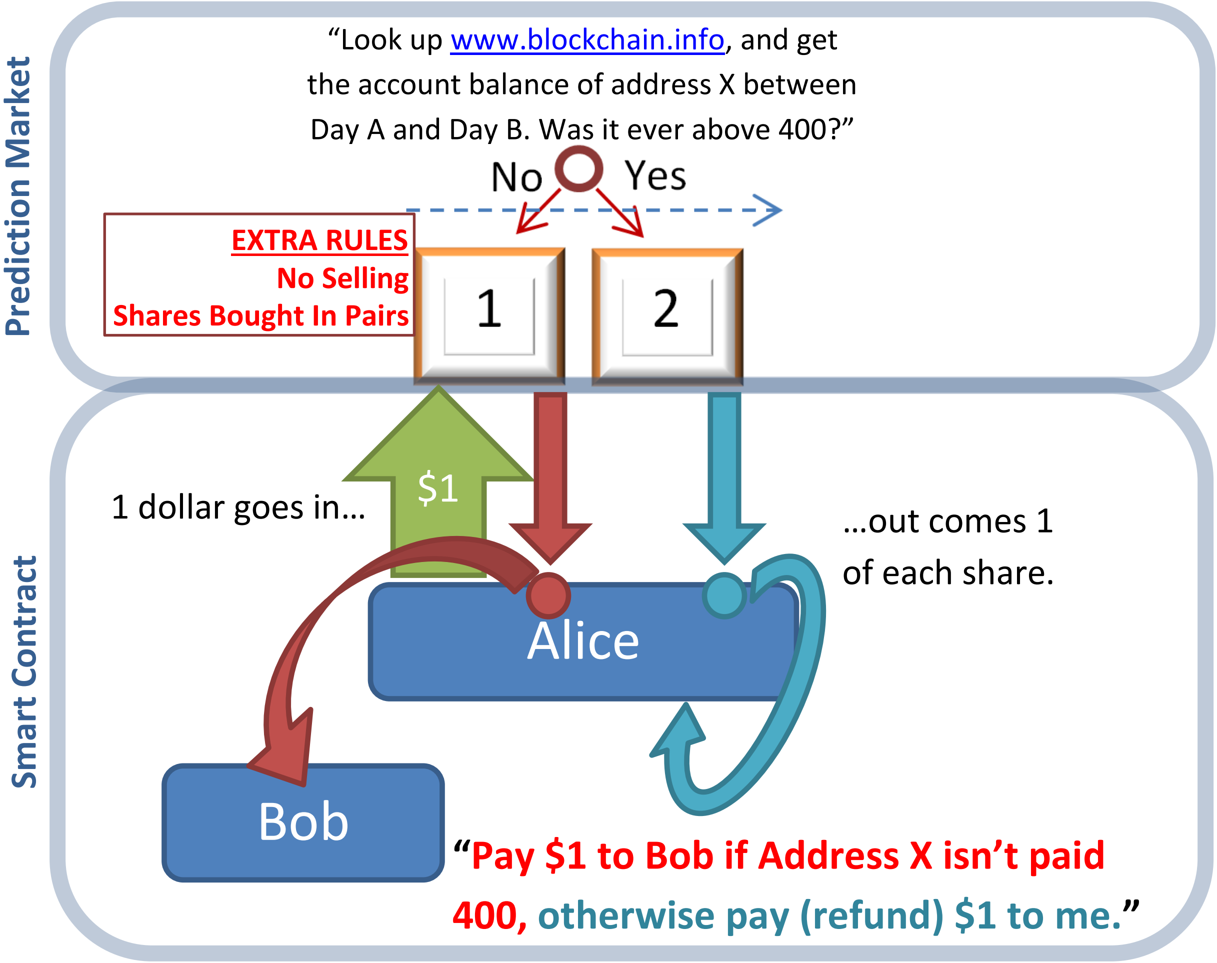
While this scenario is fully incentive-compatible, there is no guarantee that it actually will provide a public good (for example, a scenario “no one creates these markets at all, and everyone agrees to ignore them if they were created” is also fully incentive-compatible). In fact, the process of collecting contributions results in a rather unstable combination: extremely cheap Schelling States, and yet a high (and increasing) likelihood that at least one state will sell for 1. Individuals might purchase these cheap Schelling States to resell one of them post-public good construction, and these purchases actively drain the funds available to the provider. In summary, while the incentives allow for a public good to be provided, they also allow for someone to cheaply ensure that the market never raises enough money.

Public Bads, for example “The ‘New Haven Lighthouse Point Park’ lighthouse to be destroyed before date X” are unlikely to be funded this way, for this and other reasons (namely, that the project requires a publicly known non-anonymous owner, and that the trade claiming the funds must be made well in advance). For more details, see Crime Markets.

[20] Note that speculators cannot sell, but they can purchase the set of mutually exclusive states, which has the same effect on prices.

Idea 5: Blockchain Smart Contracts

Truth-ereum


Prediction Market
"Look up www.blockchain.info, and get the account balance of address X between Day A and Day B. Was it ever above 400?"
No
Yes
EXTRA RULES
No Selling
Shares Bought In Pairs
1
2
Smart Contract
$1
1 dollar goes in…
…out comes 1 of each share.
Alice
Bob
"Pay $1 to Bob if Address X isn't paid 400, otherwise pay (refund) $1 to me."

"Smart Contracts" are abstractions and generalizations of the Autonomous Assurance Contracts just described. There is little to describe specifically: a PM is set up with selling disabled, and individuals buy the 'Smart Shares' evenly (ie, one of each: for a Market with N States, a user would pay $X and receive N shares, whose value totalled $X). Although shares can't be sold back to the market, by holding one share of each State one is guaranteed $X back. Individuals then trade these shares (to other users) as they please. Conceptually **this is a PM asking for the answers to programmable questions, instead of the outcomes of well-known events**.

The Decision text can be literal software code, on (for example) a 'Python Branch', resolved automatically by users' computers (which can connect to the blockchain and read/execute the Decision's python code). Decision code can be as complex or modular as desired (VTC-owners of this Branch could be required to run supercomputers, for example). Each 'Smart Contract' would be publically available to everyone for the duration of its existence, with Market and Decision Authors collecting fees proportional to Market popularity.