Extra-Predictive Applications of Prediction Markets

Paul Sztorc
truthcoin@gmail.com
Version 1.2

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 four 'Big Ideas' for cryptocurrency PMs: First, blockchain crypto-assets with a stable fiat-value ("BitUSD"), second, the provision of 'public goods' (such as lighthouses) without coercive taxation or trusted third-parties, third, SPV-compatible (headers-only) colored coins, and, fourth, 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 stock price 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 Derivatives

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, a disruptive/industry-killing technological innovation, crippling regulatory activities, pandemic, or other harmful events. This purchasing activity thickens the market and draws in profit-seeking speculators, who would produce actuarially fair prices as they compete 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.

The most reasonable expectations for blockchain PM-insurance seem to be airlines forecasting rain and snow delays, and individuals planning their weddings. Individuals may also like to insure against the solvency of fiat-cryptocurrency exchanges. Not only would this allow individuals to hedge

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

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

"How many shares of NASDAQ:GOOG will 1$ buy on Jan 5th, 2015? [0.0005 to .0020]"

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. [5] 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

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.

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[6] (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

[5] http://en.wikipedia.org/wiki/Replicating_portfolio
[6] log(68)/log(2) = 6.087

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.

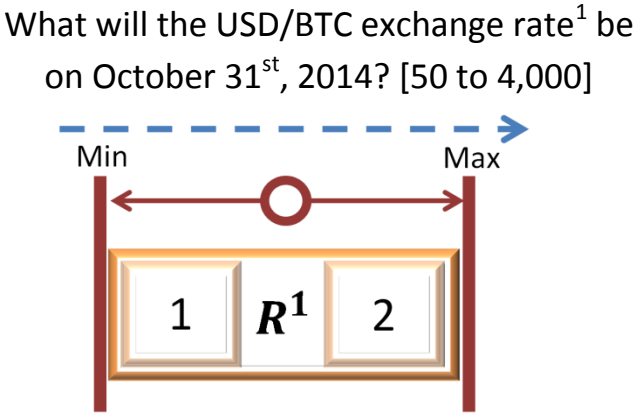
Four Big Ideas

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

Idea 1: 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[7]. 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.



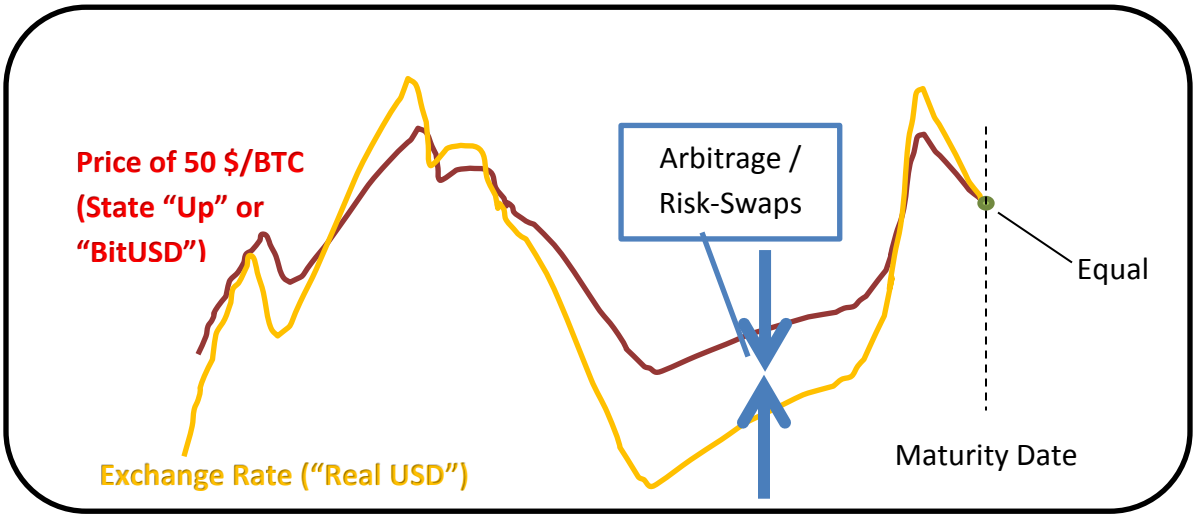
This Market can be traded in two ways:

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

[7] 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?"

(including merchants accepting BitUSD) can profitably[8] become early-adopters, bearing *only* the technical and social risks of the software design (but none of the exchange rate risk).



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.

[8] 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).

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 2: 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 colored-coin protocols).

Idea 3: Efficiently Funding Public Goods (Without Trust or Taxes)

The Libertarian Holy Grail

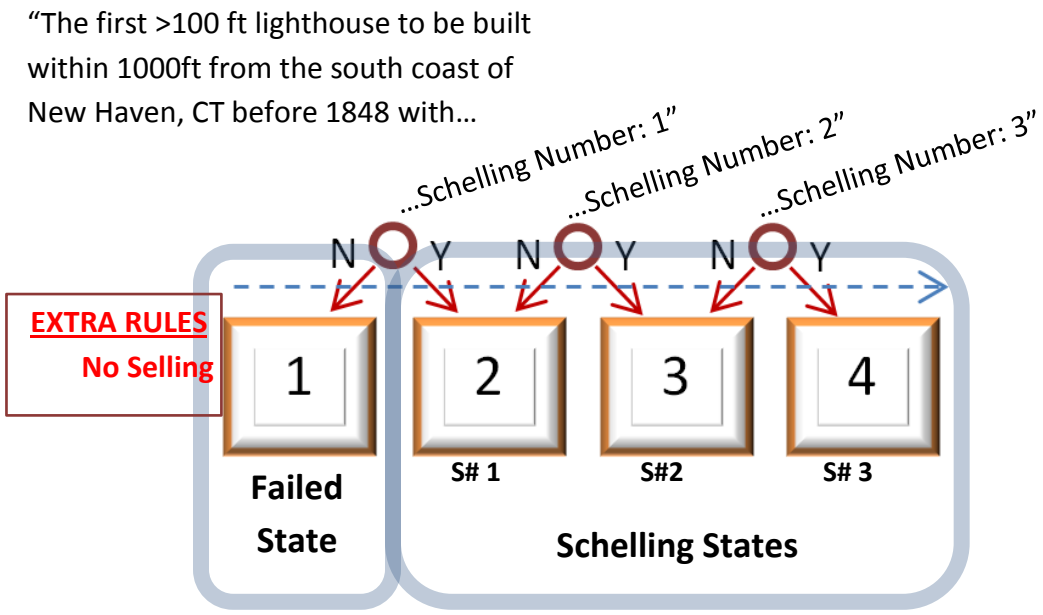


Figure. A special market used to finance a lighthouse. Notice 3 nearly identical decisions, partitioning the market into 4 States. A non-construction of the lighthouse would result in State 1 being the Outcome; hence it is the 'Failed' State. Otherwise, the builder/owner of the lighthouse is expected 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.[9] However, users can cancel their pledge (making it unreliable and introducing strategic frictions), and, upon success, the pooled funds are merely transferred to an individual (with no guarantee that he will provide the good).

To eliminate these problems, one can build a protocol on top of the PM protocol, allowing "trustless dominant assurance contracts" (T-DACs) 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.

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

The funds are collected by creating a special market of dimension 1 x (1+N), in which only buying is allowed. Funds can only be sold upon expiration (i.e., can only be redeemed after the outcome is determined, and not on-demand as would otherwise be the case). 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.

A provider verifies that the market contains enough funds to finance the good, builds the good, and is retroactively reimbursed as follows: the provider makes a single gigantic trade on the Schelling State with the lowest price, and endows his good with this State (with a public statement, a huge flag, poster on the interior, etc.). The provider then wins all of the money in this market.

The incentives provided by this scheme are ideal. Entrepreneurs (in the terminology of the Dominant Assurance Contract), can first create the market, and then purchase the Shelling States uniformly. This ensures that these entrepreneurs will profit if the public good is provided by someone (entrepreneurs have purchased, for <1, a portfolio which will redeem for 1). The public does not have to put forth discussion or effort in deciding which public goods they should consider financing, as profit-seeking entrepreneurs have an incentive to provide them with a menu of projects to choose from.

Contributors have every reason not just to donate, but actually to donate their marginal benefit. If they donate and the project is not built, they profit by winning the prediction market. Moreover, those who donated the most, and the earliest, would have more shares of the Failed State and win more 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. As contributors would never voluntarily overpay, public goods will only be built if they are actually wanted (unlike the projects financed under a taxation scheme).

Note that speculators cannot sell, but they can purchase the set of mutually exclusive states, which has the same effect on prices. If speculators create efficient markets in this way, the sum of the prices of the Schelling States will represent the probability of the public good's eventual construction (by someone), and the price of State 1 will represent the probability of non-construction.

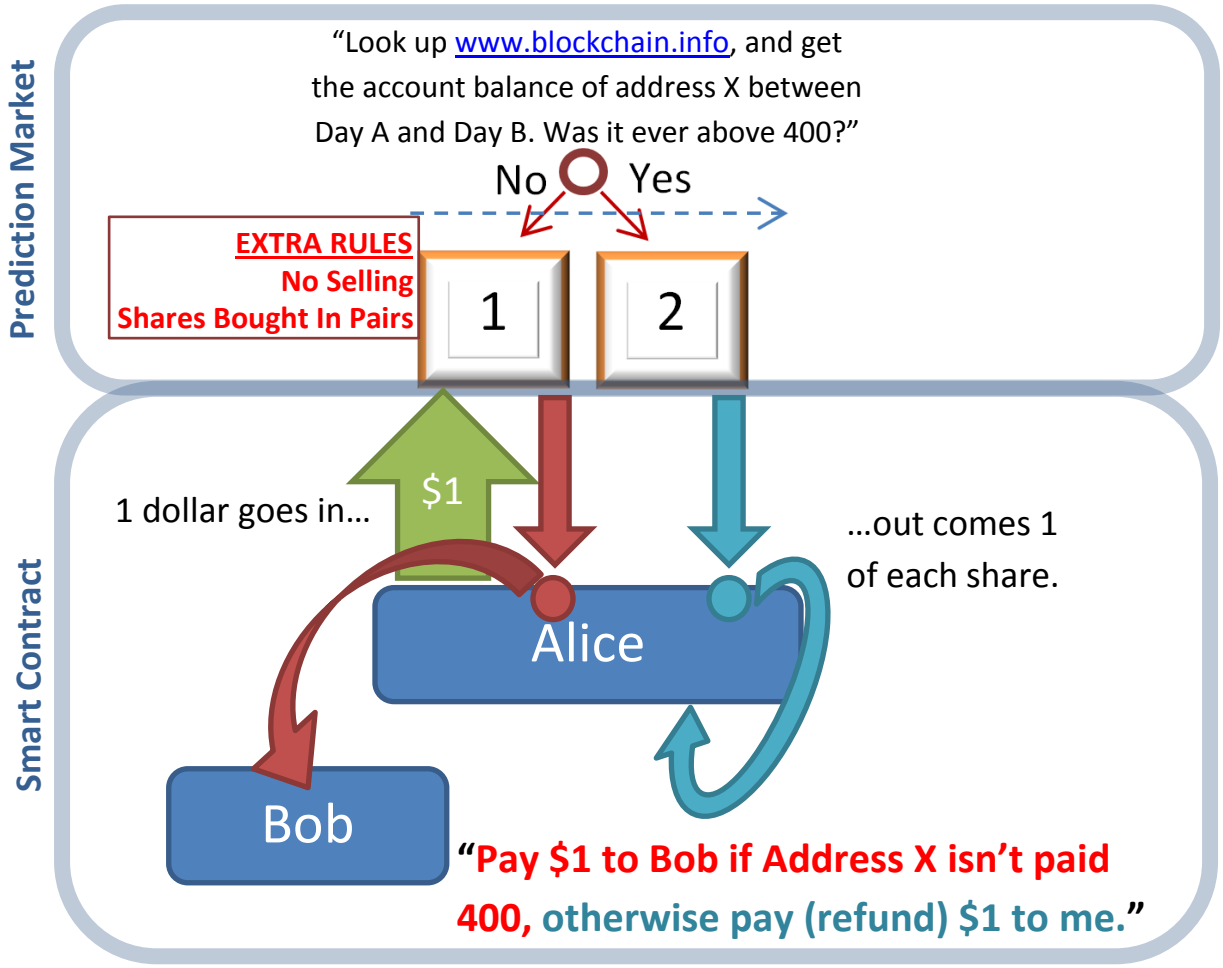
Also note that, although the Schelling State prices can sum to 1 as a project is visibly completed, the State within the Schelling Set which ultimately wins the market is known only the provider of the public good.

Public Bads, for example "The 'New Haven Lighthouse Point Park' lighthouse to be destroyed before date X" are unlikely to be funded this way, because the Winning State must be made public somehow, and criminals must remain private. Attempts to shift the Schelling-indicator from "Number 1/2/3" to something else, such as "on a Monday/Tuesday/Wednesday evening", have the disadvantage of alerting law enforcement in advance of the likelihood and manner of a future crime. Trades made just before the crime would, for free, alert law enforcement to an imminent threat of crime. Such 'tip-off trades' would be made by any profit-seeking members of the crime group themselves. Therefore, (surprisingly and fortunately) this feature cannot fund anonymous goods such as crimes.

Truthcoin markets require seed capital to form, and yet they provide free information to the public in the form of market prices. As such, one could finance the formation of a prediction market with a T-DAC prediction market. This would allow individuals to create markets they are interested in by pooling their funds with like-minded individuals yet without trusting a third party ("Meta-Markets").

Idea 4: Blockchain Smart Contracts

Truth-ereum



"Smart Contracts" are abstractions and generalizations of the Trustless Dominant 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.