A Brighter Future

Paul Sztorc
truthcoin@gmail.com
Version 0.10 – Feedback Welcome

Our Common Enemy

"All suffering is caused by ignorance."
- Buddha

What if you had access to the combined intellectual powers of all mankind? It would be easier for you to make decisions. You'd know what school to attend (if any), where to live, where to work, what to buy, and how to save/invest. You'd more quickly become aware of new medical treatments, unethical behavior within business/government, terrorist threats, societal problems, and of the consequences of a given law, scientific endeavor, or industrial achievement.

The economic-technology that makes this possible is called a Prediction Market.

What is a Prediction Market?

Whereas a stock market is a place to buy and sell shares of a corporation's earnings, a Prediction Market (PM) is **a place to buy and sell predictions**. Valid predictions entitle their owner to $1[1], whereas false predictions are worth nothing. The current market price of these tradable predictions can then be interpreted as the likelihood of the prediction coming true.

For example, a prediction might reward a dollar if Hillary Clinton is elected US President in 2016, such that any individual who thinks that she has at least a 70% chance of winning the election should be willing to buy that prediction for up to 70 cents. Predictions can be about anything: sports, politics, nominations and awards, scientific theories, the effect of a certain economic policy on the unemployment rate, the relationship between a war-declaration and casualties, etc.

When anyone can trade, no source of information is overlooked, and market forces balance info-sources in a way that is consistently and unanimously acceptable. A PM quickly integrates all available human subject-knowledge into a simple and useful representation of reality: a single number.

[1] Or any amount…call this "the unit price".

I still don't get it.

Television has a gift for simplifying and communicating ideas:

1. John Stossel gives an introduction, The Stossel Show, (4:13).
2. Neil deGrasse Tyson sketches out the general idea[2], Real Time with Bill Maher, (1:22).
3. InTrade and the 2008 Presidential Election, CNBC, (2:22).
4. CEO of InTrade on Elections and Recessions, Kudlow Report, (4:06).
5. News segment on PMs, The Stossel Show, (8:31).

For more examples see PM_Applications.pdf and LogMSR_Demo.xlsx.

The Failure of Conventional Information Sources

Compared to PMs, current info-sources do not inform and are therefore unacceptable.

Formal scientific publications are:

1. Unavailable (one would think that taxpayer-funded work would be freely available to the public, but in fact access to published research has become prohibitively expensive even to Harvard).
2. Incomprehensible (even among insiders).
3. Written/Published slowly (typically one publication is a multi-year process).
4. Ultimately, not even accurate! For university-grade research, from 60% to as high as 90% of published claims later turn out to be false.

Informal sources (TV/Internet):

1. Place no serious emphasis on objectivity, accuracy, or accountability.
2. Reward content that is flattering, amusing, frightening.
3. Manufacture/manipulate content to hold the audience's attention through the next advertisement, even when nothing attention-worthy is happening.

Fortunately, individuals are generally unaware of science and media reporting[3], and instead draw conclusions using their own experience and the comments offered by their friends/family/peers. Perhaps this is partially because the average citizen is unable to persuade info-sources (mainstream media or research universities) to investigate anything that actually affects their lives.

---

[2] Note that a] Maher himself seems more interested in allying the more-popular guest than in learning the science (a psychological/social barrier to truth which PMs aim to overcome), b] the formation of the bet ('the experiment') represents a clear/measureable outcome on which individuals have literally agreed to disagree (they are not open to persuasion), and c] the micro-debate terminates with mutual respect.

[3] Although the average American watches several hours of television per day, even the most popular cable news show never achieved a weekly viewership of even 1% of the US population. Although a large percentage of people claim (in surveys) to watch C-SPAN, these claims are not supported by (for example) Alexis rankings (foxnews.com, cnn.com, and c-span.org, rank 39th, 15th, and 8120th respectively). Of hundreds of acquaintances, I know of only one regular C-SPAN viewer (who is, regrettably, too old to change his mind about anything).

Can PMs help to make knowledge-sharing activities useful, instead of useless? The key problem of our Information Age is not info-availability, but information-aggregation: combining millions of information-sources into one representative assessment. PMs aggregate information by providing those with special knowledge (ie, knowledge differing from the current forecast (the market price)) with an incentive to reveal that information (by making a trade). A PM doesn't need to find the most-informed people in a crowd; these people will come to the PM (and enjoy doing it).

Problems With Traditional PMs

One might rightly ask, "If PMs are so great, why don't we already use them everywhere?". I will explain 3 of the issues with PMs that make the project I designed, I believe, essential to a realistic establishment of the idea.

Truth: Use and Abuse

When persuading others of something complex (for example, "we should spend taxpayer/shareholder dollars on X and not Y"), it's smart to highlight true statements when they support your argument, and hide them away when they support an alternative argument.

You may be less-able to do this in the world of PMs. Leading PM-scholar Robin Hanson argues: "Those currently in power within firms may resist prediction markets because the markets would spread previously privileged information across the company and change perceptions of what is knowable and who knows what."

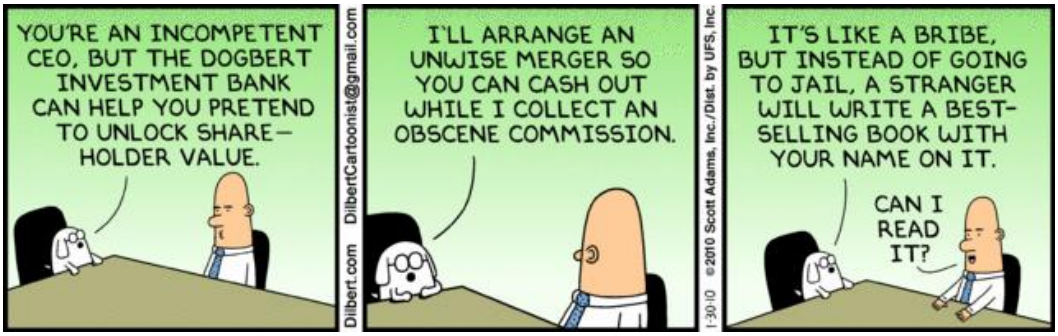

Figure 1. These experts are forecasting a successful merger.

As every member of a large organization knows, **'flattery' and 'loyalty' trump petty details like 'accuracy' every time**. If you're smart, you tell people want they want to hear (and certainly not what you really know). Most organizations don't want accurate forecasts, and anyone who pushes them may appear to be accusing the current forecasters/managers of incompetence or inauthenticity (a career risk). The people who have the information (employees, managers) are different from the people who need the information (shareholders/owners/analysts).

Lack of Public Familiarity/Support

Secondly, **PMs may (at first) look bad**. PMs are essentially betting[4], which can feel taboo. For an excellent summary of the discomfort many have with betting, see this blog post.

Defenseless PMs are targets of anticompetitive lobbying behavior on the part of casinos. According to CFTC bureaucrats trying to advance their political careers, however, PMs are not gambling, but instead an unregulated futures market[5]. No relevant laws exist, and existing irrelevant laws are abused for economic or political gain (at the expense of the public interest). Most famously, the 'Policy Analysis Market', which could have saved countless lives by providing the US government with reliable information about terrorist attacks and Middle East instability, triggered (apparently) the psychological bias known as "taboo tradeoffs" (as, for some contracts, someone might benefit from an event which harms the group), creating an onslaught of uninformed, irrational outrage. Nothing in the public response made any sense, but a few Senators could use it to make their political opponents look bad, and that's enough to close down a life-saving project in this nightmare we call reality.

The situation will never improve. Overwhelming academic and industry support is not enough. Even overwhelming public support would not be enough (were it ever obtained for an idea which is taboo, new, and difficult to explain). Economist Bryan Caplan has remarked that a bet is "a tax on hypocrisy"; would our current leaders really bring a tax upon themselves? Would you place the albatross of honesty on your own head, if you had to do it first and didn't know if others would do the same?

Counterparty Risk

Third, and most practically, **if you make a bet with someone, you have to trust them to pay up.** Tradable-Predictions, defined as "assets with a definite future value based *solely* on their future accuracy" have never existed. Instead, the value of PM-Predictions depended substantially on the behavior of the counterparty (ie, the guy holding the money). You can't "own" a prediction, only a paper claim to money held by the PM administrator.

The PM administrator has proven to be unambitious at best (accepting only a few bet-topics) and unreliable at worst (losing funds and/or going out of business, see Appendix). PM-admins rely on trust (as they hold their customer's money) yet are prevented from accessing trust-forming institutions (law-enforcement, brands/advertising) because of their regulatory/legal/awareness challenges.

Bitcoin operates independently of a nation's legal framework, and might avoid closure or regulatory interference. If so, competing "Bitcoin InTrades" would appear to fulfill market demand.

Unfortunately, PMs require a way to store up money and pay it out based on a real world outcome, which implies trusting a third-party with your money. Use of supra-national Bitcoin would prevent the use of any legal guarantee (to justify this trust).

---

[4] PMs are bets where the "odds" change continuously, and are set by market forces instead of bookkeepers.
[5] InTrade was an Irish, not US, company.

Bitcoin is P2P software. It was not ever designed for *other people* to store your money; it was designed for *you* to store your own money. The Bitcoin businesses that oppose this intent by holding customer funds (for example the currency exchanges) lose those funds regularly. Although businesses can prove their solvency, proof of future-solvency is impossible, and even solvent Bitcoin PM-businesses would be able to steal funds by trading on and then reporting incorrect prediction outcomes. This problem worsens with scale, as there is a bigger pot of money for hackers or insiders to steal.

Can A Blockchain Solve These Problems?

To solve these problems, **I designed a blockchain which creates and manages prediction markets**. Although Bitcoin does not solve our PM problems, it demonstrates that a blockchain can provide **scalable, censorship-resistant, and trustless** solutions. Blockchain solutions also generate **efficiency** by cutting out middlemen and avoiding overhead costs (no brick-and-mortar, compliance, administration, etc.). They are **egalitarian and immortal.**

My design was able to solve a few other PM-problems as well. **Any user can create a market about anything**, removing the dual-requirement that a PM-administrator must not only be trustworthy, but also share your prediction-interests. Market scoring rule technology ensures that **trading volume is irrelevant**, and traders will always be able make a trade updating the price to their estimation (even if they are the only trader). Markets are not limited to two 'Yes'/'No' states, nor are they limited to one dimension. Finally, a custom algorithm, based on a game-theoretic application of weighted singular value decomposition, determines and sustains accurate reports about the market outcomes.

I hope you're interested in helping me make world-class knowledge freely available to everyone, and allowing individuals to profit by contributing their personal experiences. To learn more about what I have to say, you could consult the following:

1. If you'd like to dive into the technical details of the PM blockchain, read Truthcoin_Whitepaper.pdf.
2. PMs are easiest to understand in their simplest "Yes" / "No" form, where the price of "Yes" represents the probability of the event happening. However, PMs can easily be combined into more interesting types. File 2_PM_Types.pdf discusses multi-state and multi-dimensional contracts in greater detail.
3. PMs can be used to build the optimal efficient forecast of the future. They aggregate all available information, prefer cheaper info sources to expensive ones, and discourage waste and redundancy. However, PMs can do much more than just predict the future. For a taste of some of these other possible applications, read 3_PM_Applications.pdf .
4. PMs can be difficult to understand. I have personally observed even professional forecasters making the same misinterpretations over and over again. Refer to 4_PM_Myths.pdf to avoid embarrassing yourself!
5. Market manipulation is a frequent subject of discussion in the PM world. If we are to trust PM-accuracy enough to use PM-estimates to inform our decisions, we have to consider how

adversaries might strategically respond to such trust. In 5_PM_Manipulation.pdf I discuss the immunity all PMs have to naïve manipulations, and describe how the Blockchain PMs I designed have unique features which enable them to resist all manipulation attempts, and even profit from these attempts at the expense of the manipulator.

6. For trading, the PM Blockchain employs something called the Logarithmic Market Scoring Rule, which can be difficult to understand. I built an Excel spreadsheet demo of hypothetical trades in LogMSR_Demo.xlsx to help anyone interested.

Conclusion: Market Empiricism and The Second Revolution

For millennia, there was suffering and misery. Can you imagine a world without music, or eyeglasses, or DayQuil? Our ancestors wished they knew how to make those things. They wished they knew how to stay warm, prevent their teeth from falling out, and use the stars to navigate. They probably wondered what stars were. Despite having brains that were essentially the same as ours, no one in any occupation in any region of the world would see an answer to that question or countless others…they wouldn't even see progress, any hope that these questions even *had* answers, until a very special time.

If the utopian Scientific Revolution (1543-1687) had a motto, it was arguably that of the Royal Society of London: *"Nullius in Verba"*, which implored individuals to *"Take no one's word for it".* **Knowledge could not be received passively from an authority figure; it all had to be verified by personal experience**. It was an idea that would literally change the world.

Sadly, the world has only partly-changed. Most people still "take someone's word" for their civic and scientific news, and most don't even know how tell if knowledge was or was not "verified by personal experience". Those who do try to verify even a few claims are quickly overwhelmed by the massive amount of work required. Political think-tanks, for example, often reach opposite conclusions with equal vigor. However, there is only one *reality* experienced, and so only one *truth* (in the sense of "a global consensus of honest expectations"). Opposite expectations can't both be true; what to do?

Another problem is that we often take our own "word" for things, when we shouldn't. Modern social psychology reveals that man can be very hypocritical. Evolution produced a creature designed to survive-first, think-later, and to behave and talk accordingly. Optical illusions, for example, help our eyes quickly process information that is nonetheless incorrect.

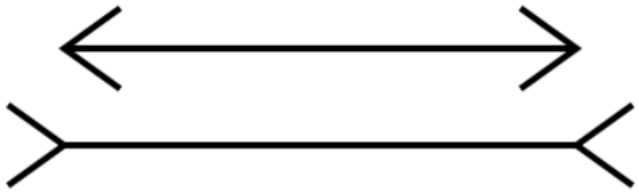

Figure 2. A classic optical illusion. Surprisingly, both horizontals are the same length. More importantly, **even after you verify this equality, you will continue to perceive the figure "wrongly". S**elf-awareness, if achieved, must be constantly maintained…we must always be skeptical of our beliefs.

When everyone pretends to know more than they do (to seem impressive or valuable) it can be hard for a first-mover to admit ignorance honestly. Unfortunately, this means that informed people leave the conversation, and the most oblivious take center stage. Politicians do not need to obscure the truth, if citizens lose the original among a thousand imperfect copies.

PMs allow the layperson to examine the relationship between truth and experience as easily as checking the day's stock prices. Is global warming real, and will it ever affect my life? Check the markets on the likelihood of future temperatures, future sea levels, and future hurricane damages. Will a campaign promise be fulfilled? Will a new medical treatment really live up to its hype? Will a scientific theory still be accepted in 50 years? Which team is mostly likely to win the Super Bowl?

The printing press helped set the stage for first Scientific Revolution, but it took a new (and heretical) way of looking at information – Empiricism – to make *what was printed* have the impact that it did. Similarly, we today have the internet, drowning us in information-sources. *What is broadcast* is less useful than it would otherwise be if we could reliably combine Multiple Sources into One Truth. We need a new (and taboo) way of looking at information today! Viva la revolución!

Appendix 1 – The PM Graveyard (vs BlockChain Immortality)

PM Operators – Unambitious and Short-Lived	
Name / Link	**Status**
economicderivatives.com	Economic variables only (CPI, GDP, payrolls). Expensive/not-anonymous.
intrade.com/v4/home/	Closed following problems with US regulatory compliance in early 2013.
tradesports.com	Sports only, Closed Nov 2008/re-opened Jan 2013/Closed again/ Now back.
inklingmarkets.com	Private only. Scope/pricing unknown.
thewsx.com	Elections only. Long since closed.
bizpredict.com	Closed.
tippie.uiowa.edu/iem	Limits of $500, not anonymous, 3 markets only.
betfair.com	Sports only, Europe Only.
newsfutures.com	Closed. Remnant absorbed into private consulting group.
lumenogic.com	Private only. Scope/pricing unknown.
ideosphere.com	Play-Money only.
policyanalysismarket.com	Closed in a single day by ignorance.

Bitcoin Betting "Solutions" – A Point of Failure (that Worsens with Scale)	
Name / Link	**Status**
BTC Sports Bet	Very old, yet apparently untrustworthy.
BetsOfBitcoin	Also old, yet closed Mysteriously. Funds stolen or missing.
Predictious	Volume: 130 shares (* 10/1 * 1/1000 * 500/1 = $650, or pitifully low). Users do not trust.
bitcointalk Gambling Summary	Bitcointalk Post about Bitcoin gambling insolvency.

Roughly half of Bitcoin exchanges fail. Small exchanges close and large exchanges are hacked, as I argued above. This research was pre-MtGox-failure, a failure that itself resulted in the loss of 6% of the circulating Bitcoin money supply.