Arbitration in Decentralized Prediction Markets

David Vorick
Nebulous Inc.
david@nebulouslabs.com

December 17, 2015

Abstract

Decentralized prediction markets attempt to predict the outcomes of real world events. After the event transpires, the outcome must be reported through a process called arbitration. We show that arbiter subjectivity poses a significant challenge to reaching consensus around prediction market resolution. By applying the Byzantine-Altruistic-Rational model of participation, we also show that financially incentivized behavior can disrupt the arbitration process. We provide updated models for decentralized prediction markets that address many of the challenges and problems revealed by our analysis.

1 Introduction

1.1 Prediction Markets

Prediction markets (PMs) are a financial tool designed to predict future events. In a PM, a future event is described and potential outcomes are given (for example, an election where each candidate is a potential outcome). Financial instruments are created that allow market participants to bet on each of the potential outcomes. When the real outcome of the event is certain, bets placed on the correct outcome are rewarded. In several common forecasting scenarios, PMs have demonstrated predictive capability superior to polls, expert opinions, and statistical inference [13].

In general, PMs financially inventivize people to leverage information that they have which may be unavailable to the rest of the world. This knowledge is then made useful to everyone else in the form of a more accurate prediction, even if the exact nature of the knowledge is not exposed.

1.2 Proof-of-Work Blockchains

Bitcoin [6] introduced the proof-of-work blockchain. This blockchain is a database which can support of series of updates, called transactions. Transactions are batched into blocks, and blocks are added to the blockchain which serves as an auditable history of the database. Strict rules enforce limitations on what can be contained in an update (for example, coins can only be spent or created under certain conditions). Before a block is considered valid, it must solve a computationally difficult puzzle which serves to ratelimit updates to the network. Multiple alternate histories can be created, but only the history containing the most computational work is considered the true chain, allowing the network to converge on a global consensus.

Anybody is able to validate the blockchain, the only requirement being that they have all of the blocks. Anybody is able to extend the blockchain, the only requirement is that they solve the proof-of-work (a progress-free function). Because of this, Bitcoin's proof-of-work blockchain features trustlessness and permissionless participation.

Trustlessness means that no single entity or group has the power to violate fundamental assumptions of the network such as the number of coins in circulation, and that everyone can verify for themselves that the fundamental assumptions have not been violated. Systems with trust carry overhead in the form of uncertainty and the occasional turmoil when a trusted party goes rogue. Trust based systems typically also

have punative overhead for the sake of punishing participants who violate trust. A trustless system is able to eliminate the uncertainty associated with trust and eliminates the need for any punative system.

Permissioned systems add barrier to entry for participation and leave room for discrimination. Bitcoin in particular is special because both the mining and the transacting is permissionless. Anybody who can acquire hashrate can create blocks that will be accepted by the nodes of the network. The incentive structure for transactions and general decentralization of the mining environment create censorship resistance even for nonmining participants. This trusless openess levels the playing field for nonpriviledged participants.

1.3 The Value of Decentralizing Prediction Markets

Traditional PMs require trusting a central authority to play the role of both the exchange and the arbiter. The existence of money and potential for corruption means that traditional PMs are either highly regulated, or are unable to use real money. The central authority has great control over who is allowed to participate and what markets are allowed to be created. Inhibiting participation reduces the accuracy of the market, and limiting which markets are allowed stifles innovation. Creating trustless and permissionless prediction markets can eliminate much of the overhead and danger associated with traditional PMs while unlocking their innovative potential.

Multiple groups are currently exploring decentralized prediction markets (DPMs), at least one of which has been successful at raising money [2]. There is clear interest by the public in decentralized prediction markets.

2 The Contributions of this Paper

When a prediction event resolves, there must be some process that informs the DPM of the outcome of the event. This process is referred to as arbitration, and the entities performing the process are called arbiters. Previous literature [3] [17] has used the term oracle in place of the term arbiter. The term oracle has been rejected because the traditional use of the word oracle implies an idealized and infallible entity.

This paper analyzes decentralized arbitration strategies, providing reviews and criticisms of existing methods of arbitration. A major focus of the paper is the differing subjective views of the world of each arbiter in a decentralized system. Subjective arbitration can result in turmoil, even when all participants are acting altruistically. There is little prior work regarding subjective arbitration, though the topic is briefly touched in the Truthcoin [17] paper.

A stronger threat model is provided for the construction of DPMs which takes into account byzantine, altruistic, and rational participants [4] that tries to model the real world behavior of participants in decentralized systems. The enhanced threat model is applied to create a more restricted set of design goals that can result in stronger DPMs. Existing methodologies for arbitration in DPMs are analyzed under the enhanced threat model, and new methodologies are suggested that improve upon DPMs under the updated design goals.

The paper presents a model for a fully trustless DPM which requires significant validation overhead, but may be useful in limited scenarios. Finally, an outline for a stronger, more scalable DPM is provided which does not have full trustlessness, but does have high trust agility and addresses many of the incentive-incompatible problems found in existing DPMs.

3 Threat Model and Design Goals

This paper assumes a Byzantine-Altruistic-Rational (BAR) model [4] for participant behavior. Participants are divided into three categories: byzantine participants that will act destructively regardless of incentive, altruistic participants that will always follow the protocol, and rational participants that will break protocol if there is incentive to do so. A small number of participants are assumed to operate under byzantine principles, and a small number of participants are assumed to operate under altruistic principles. The vast majority of participants are assumed to be rational actors willing to break protocol if and only if there is incentive to do so.

The BAR model is believed to more correctly map to the real world behavior of participants in decentralized systems. Behavior seen in the wild such as double spending [1] [10] reinforces the idea that participants will break protocol if there is an incentive to do so. Miners on the Bitcoin network have demonstrated meta-rational behavior [5]. Two large miners agreed to give up a substantial amount of revenue in order to preserve compatibility with older nodes, despite having both more recent software and enough hashrate to try and force the network to upgrade and a clear incentive to do so. This is evidence that rational participants can be aware of their dependence on the survival of the system as a whole, and would therefore be willing to accept personal loss for the sake of protecting the system. It is unclear that this meta-rational behavior would persist if profit margins were lower or if competition were more fierce.

The presence of byzantine participants means that all interactions involving individual participants must be prepared for byzantine situations. The presence of altruistic participants means that setups requiring at least one instance of honesty can be expected to be successful, though this paper does not explore any methods of arbitration which require altruism. The assumption that the vast majority of participants rationally maximize their own utility means that designs must be incentive-compatible, and that the most rational behavior is always acceptable to the network.

While every participant operates under a different set of incentives, financial incentives appear to play a heavy, near universal role. Participants that place less value on financial incentives seem to tend towards more altruistic behavior overall, as opposed to byzantine behavior. Analyzing rational participants primarily in terms of financial incentive appears to be a good conservative approach to BAR systems.

Arbitration by rational participants requires incentivization. Even with incentivization, there is a limit to how much arbitration each participant is able to perform. At the extreme upper bounds of arbitration effort, only a few participants worldwide will be able to effectively perform all tasks. Reducing the size of capable and willing arbiters is a centralization pressure. Arbitration must be incentivzed, and participation requirements must be kept to a reasonable level.

Arbiters are incentivized to cheat PMs. If a potential event outcome is unlikely, and therefore priced low, arbiters can make significant financial income by going long on the unlikely outcome and then voting dishonestly to resolve that outcome as true within the DPM. This behavior is called a false arbitration attack. There must be some method of either incentivizing honesty or decentivizing dishonesty that outweighs the incentives motiving false arbitration attacks.

The presence of byzantine participants makes trusting a single arbiter dangerous, as that single arbiter may express byzantine behavior. Bringing in a large number of non-Sybil [14] [15] arbiters minimizes the potential disruption that can be caused by a byzantine arbiter. Having large numbers of arbiters voting on each PM means that arbiters need to vote in consensus. Each arbiter is assumed to have a separate perspective and therefore a different subjective view of the world. This subjectivity can cause multiple altruistic arbiters to provide conflicting results to a real world event, especially where the outcome of the event is not easily accessible to all participating arbiters. A further exploration of this phenomenon and the corresponding pitfalls appear in Appendix A. There needs to be methods for managing arbiter subjectivity within a DPM.

If there is a single monolithic group for managing arbitration, traders have no options in the event of arbiter corruption. A corrupted monolith may be able to launch false arbitration attacks without losing a substantial amount of trade volume because there is nowhere else to trade. If traders are able to selected alternate arbiters or arbitration groups in the event of corruption, it is much less likely that a corrupted arbitration group will retain relevance. If traders can easily switch between a diverse set of arbitration groups, traders can be said to have a high trust agility. Trust agility measures the ability of participants to switch which groups are trusted with little notice and with little cost. Maximizing trust agility is important for retaining incentive compatibility in systems that rely on trust.

Arbitration groups that have high volumes of non-participation or even small volumes of inaccurate voting are likely to experience significant loss of trust. Arbitration groups therefore need some way to enforce consensus-following participation.

One of the key advantages of decentralization is permissionless participation. Permissionless arbitration in particular is important for maintaining a high level of trust agility in the system. Permissionless participation of all types of participants is a design goal for DPMs.

Summary of Design Goals

- Incentives for participating in arbitration
- Limits to the volume of arbitration required
- Incentives against false arbitration attacks
- Large numbers of arbiters resolving each PM
- Methods for handling arbiter subjectivity among groups of arbiters
- Methods for maximizing trust agility for traders
- Methods for minimizing non-participation and for minimizing voting against consensus
- Permissionless participation for all participants, especially arbiters

4 Related Work

4.1 Trusted Arbitration

The simplest model of arbitration involves assigning trust to a single arbiter or a set of arbiters and trusting them to make the right decision. If arbiters are appointed per PM, a high level of trust agility can be achieved. When one set of arbiters begins to lose trustworthiness or acts dishonestly, a different set of arbiters can be chosen for future PMs. Trusted arbitration features only a minimal amount of decentralization, yet because of the trust agility is a significant improvement to the fully centralized model. The limited number of arbiters involved in a trusted or federated setup means that byzantine participants are able to do interfere with PM arbitration. Trust agility helps to minimize the amount of damage that can be performed, but trust can only be reassigned after a PM has completed, allowing a byzantine participant to disrupt a full PM.

4.2 Keynesian Beauty Contests

The Keynesian beauty contest (KBC) described in [12] proposes PMs that get resolved by the shareholders of the outcomes within a prediction market. Shareholders get to vote on the outcome of the event weighted by the total number of shares owned. To incentivize correct voting, voters must put up a bond that will be sacrificed if they vote against the consensus that is reached.

One key factor to this approach is the method by which shares are distributed. An entity that is able to sweep up a sufficient number of shares in the market can corrupt the voting. In the PMs presented by [12], shares can be acquired in batches that are guaranteed to pay out at a 1:1 ratio. It is costless to acquire large volumes of shares because the payout of a batch is going to be equal to the cost so long as none of the elements of the batch are sold. This costlessness reduces the challenge of winning the KBC to most effectively executing large volumes of costless purchases.

In alternative models, rational participants attempting to resolve a prediction market via a KBC will end up in an arms race where the most heavily invested party wins. Perhaps more significantly, a party that knows it has significantly more financial resources than everyone else will be able to guarantee the outcome of arbitration regardless of the actual truth. Because of the required bonds, the cost of losing the arms race is significant, any arms race that takes off is likely to end with one party experiencing significant damage. There is no clear incentive for parties to join this arms race with the intention of voting honestly because failing to even the scale is very expensive and there's no reward inherent to voting honestly in the first place. Large enough PMs may be protected from arms races, as no single participant may have enough money to dominate the PM. DPMs that feature multiple simultaneous PMs of varying sizes will inevitably have smaller PMs that are more vulnerable to this type of voting strategy.

Alternative implementations of KBC arbitration may overcome these issues, however it seems unlikely due to the fact that arbitration is managed entirely by participants with stake in the outcome according to the amount of stake they have in the outcome. Even if the fundamental issues are overcome, trading against

a PM and arbitrating the outcome of a PM are different skill sets, and are incentivized by different processes. It does not really make sense to have the same people play both roles.

Byzantine participation may play a role in small PMs, but is unlikely to impact larger PMs due to the assumption that only a small percentage of total participation expresses byzantine behavior.

4.3 Miners Voting on Arbitration

Miner arbitration [12] is a method of arbitration where miners are allowed to vote on the outcomes of markets in every block they find. Miners are required to ignore blocks that contain votes that they disagree with, unless that block already has 'k' confirmations. Voting is finished after an outcome receives 't' confirmations on the longest valid chain.

Determining the outcome of PMs is extra overhead for miners. Not only must the miner pay attention to the open PMs, a miner must also risk getting orphaned due to breaking consensus with the other miners. A miner that chooses to vote on any prediction market has some risk of other miners rejecting the vote and refusing to mine on their block. A miner that chooses never to vote on a prediction market has no risk of rejection, and therefore minimizes the chance of being orphaned. As a miner, the safest and lowest overhead option is to always create blocks that do not vote for PMs.

No reward structure is given for voting on closing a PMs. Choosing to vote on a PM counts towards block size and limits the number of transactions that can be included in a block, therefore limiting the number of transaction fees that can be collected. Even if voting does not count towards to maximum allowed block size, voting on a PM increases block size and therefore the risk of being orphaned due to slower block propagation.

There is a Schelling point [8] [9] around voting according to the votes of other miners. When there is only one block voting for a given PM outcome, the most likely outcome to have a majority of the miner vote is the outcome stated in that block. Especially if incentive is added encouraging miners to vote on PM outcomes, there is strong incentive for miners to detect the majority vote and then go along with it. Miner arbitration is therefore not incentive compatible, and fails under the BAR model for participation.

4.4 Corporation Arbitration

Arbitration can be assigned to corporations [12]. Shares of the corporation, called stock, are divided between a multitude of participants. When closing a PM, the stockholders vote weighted according to stock ownership. Any income to the corporation is divided among the stockholders.

The value of the stock is equal to the total expected future return of the stock. In systems with high trust agility, any sign of malice or untrustworthiness from the corporation will act as a strong disincentive for traders to use PMs arbitrated by the corporation. Less trading means less income, which means there should be an immediate impact on the value of the corporate stock. If the stock is fungible and can be sold on a market, there is further incentive to maintain trustworthiness. Attempting a false arbitration attack will immediately drop the value of the stock to zero, which means that the attack is only profitable if the windfall from cheating is greater than the value of the stock.

Under the BAR model, the majority of arbiters in the corporation will have no incentive to attempt a false arbitration attack so long as the value of their stock is more than could be made by voting dishonestly. Byzantine attacks will require a significant amount of stock to be successful, which is unlikely to happen if the corporation is large and the stock is well distributed. A healthy ecosystem will favor large corporations that have valuations proportional to the abuse potential of the PMs they arbitrate.

High fungible corporate stock also increases decentralization. If stock is owned by many participants and is traded frequently, the amount of trust in any one location is minimized. The opportunities for collusion are also minimized, as the pool of ownership is highly dynamic.

Overall, corporate arbitration seems like the best approach to scalable DPMs due to the ability to price their trustworthyness, the ability to offer arbitration by a diverse set of participants, and due to their ability to decentivize exit scams that would otherwise seem attractive to rational participants.

4.5 Truthcoin

Truthcoin [17] features a single arbitration corporation that can be split under certain conditions. Upon split, another corporation is created that has identical stockholder makeup, though after the split the stock of each corporation can be traded independently. Anybody is allowed to create any PM that will be arbitrated by the corporation, though only a limited number of PMs can be created in total. PMs are closed in batches, where all of the stockholders of the corporation vote on each PM. Statistical analysis is performed on the voting distribution that analyzes inconsistencies in the voting. Inconsistent voters are penalized by having their stock redistributed to the more consistent voters.

Having only one large corporation inhibits trust agility. New corporations can be created, but the process must be approved by an existing corporation, and the new corporation is initialized with stock ownership that is identical to a parent corporation. Stock can then be traded independently, but nonetheless corporations in Truthcoin are likely to have very similar ownership, reducing overall trust agility.

The only way to become an arbiter in Truthcoin is to buy stock from an existing corporation. This inhibits the goals of permissionless participation, as the stockowners may make the decision that they do not want to sell, especially if they have already successfully corrupted the corporation.

Any participant can submit a PM of any subject to a corporation. The corporation is then responsible for arbitrating the PM. The subjective nature of decentralized arbitration means that for some PMs arbiters will have difficulty reaching consensus. The presence of byzantine participants means that at least some PMs can be expected to be significantly disruptive. Disruption is even incentivized, due to the fact that voters are penalized for voting against consensus. A rational participant may seek to create PMs where a minority of competing stockholders vote incorrectly, resulting in their stock being redistributed, benefiting the other stockholders.

The Truthcoin paper argues that traders will have no incentive to participate in vague PMs. This argument does not have strength if the PM only appears vague to some participants. Because trading is a form of gambling, it also seems unlikely that all traders would be deterred by potential disruption in the arbitration process.

5 A Trustless System of Arbitration

It is possible to build a trustless DPM through a form of trustless arbitration. Bitcoin achieves trustlessness by having every node verify every single transaction. DPMs can achieve trustlessness in a similar manner by having node operators independently verify the outcomes of every PM. This type of DPM does not need any form of on-chain arbitration - the node operators individually act as arbiters.

There are two clear disadvantages to trustless arbitration. The first is that every PM outcome must be verified by every single node operator. This is exhausting, and puts strong limitations on the number of PMs and the nature of the PMs. The second issue relates to subjective arbitration, and is perhaps an insurmountable problem. Similar to what is explained in Appendix A, every arbiter has a different worldview, and it may be possible to cause a consensus fork by creating a PM that honest arbiters will interpret in different ways. The set of topics must be restricted to topics that have little chance to be misinterpreted, such as global elections or global sports events. Even then, events that end in dispute (a sports team is declared the winner, but later is found to have cheated) may cause consensus forks on the network. A trustless DPM is likely to require a high amount of social coordination even if the PMs are heavily restricted in both volume and scope.

Due to the validation overhead caused by arbiter subjectivity, a general trustless DPM is unlikely to be worth pursuing. There is no clear way for participants to determine which PMs are worth global arbitration. Highly specific trustless DPMs centered around concrete and infrequent events may be feasible, but the validation overhead is very high.

A trustless DPM does have the advantage of eliminating many of the problems that could arise from byzantine arbiters. Arbiters expressing byzantine behavior in a trustless DPM will simply be ignored, as they will fork onto a separate network. Incetive compatible arbitration also becomes irrelevant in a trustless DPM, because there are no rewards to manipulate, and no false arbitration attacks that can be launched. For very popular or important PMs, the tradeoffs may be worthwhile.

6 Improved Corporate Arbitration

6.1 Protected Arbitration

A whole host of problems related to subjective arbitration can be resolved by allowing corporations to vote on which PMs they choose to arbitrate. This allows corporations to ratelimit the number of PMs to something that all/most stockholders find acceptable. It also gives corporations the ability to reject all PMs that might cause trouble due to arbitration subjectivity.

6.2 Permissionless Corporation Creation

Anybody should be able to create an arbitration corporation. The freedom to do so is important for maximizing the trust agility of traders.

A new corporation may have difficulties bootstrapping trust, as the corporation has no history of good behavior. Leveraging political reputation can be an effective means for bootstrapping trustworthiness. A political figure that has reputation and utility to lose by cheating a DPM is likely to be honest initially. Because of the unstable and difficult to analyze nature of external factors, political reputation should only be used for boostrapping. Heavy reliance on external factors will also impact the fungibility of stock within the corporation, which reduces overall decentralization.

A more pure method of bootstrapping may be bonding or burning coins as a signal of good faith. Burning a large volume of coins may be sufficient for traders to trust the corporations for a low volume PM. As the corporation demonstrates trustworthiness for small PMs, the value will grow and the corporation can be trusted for increasingly high volume PMs. At this point, reputation has been successfully bootstrapped without the use of any external factors such as political or social reputation.

Permissionless arbitration also ensures that any PM can be created. If the prominent corporations are unwilling to take on a certain PM, a new corporation can be created which does accept the PM.

6.3 An Example Decentralized Prediction Market

To create an example DPM we will start with a Bitcoin style Proof-of-Work blockchain and add some features. This blockchain contains a cryptocurrency which can be traded and saved in the same manner as Bitcoin. A new type of transaction is added which allows for the creation of arbiter corporations. The creation transaction contains a list of stockholders and weights indicating how much stock is owned by each. To preserve arbiter agility, anybody can create an arbiter corporation and there is no limit to the number that can exist. The stock can be traded in the same way that bitcoin can, but carries the extra feature that it participates in the activities of the arbiter corporation. Specifically, the stock can vote on which PMs to open, can vote on the outcome of closing PMs, and receives income from the fees paid towards the corporation. Allowing the stock to be tradable gives retiring arbiters a way to cash out their reputation without committing abuse.

The corporation can open a PM with a PM creation transaction. The PM creation transaction must have signatures representing at least 51% of the stock in the corporation. The signature requirement gives the corporation large control over which PMs must be arbitrated, minimizing the risk of arbiter exhaustion and minimizing problems that arise from arbiter subjectivity. Each corporation is only allowed to have a single PM open at a time.

Each PM features some text indicating an event that is being predicted, a closing window for the event, and then also indicates a series of potential outcomes. A full batch of outcomes can be purchased at any time. When the prediction market resolves, exactly one outcome from the batch will be convertable to the original value of the whole batch, the rest of the outcomes will be worthless. A full batch of outcomes may also be sold at any time, the value of the batch being redeemable for the original purchase price of the batch. Each outcome is an asset that can be traded in the same fashion as bitcoins or corporate stock.

When the closing window of the event arrives, all stockholders in the corporation vote on the outcome of the event. Votes must be submitted after the window opens and before the window closes. The outcome that receives the most votes is declared the correct outcome, and all stockholders that voted for non-winning outcomes have their stock stripped and redistributed to the voters that voted for the winning outcome. All stockholders that did not vote receive the same punishment as the stockholders that voted for a non-winning

outcome. While strict, this rule encourages arbiters to participate and discourages dishonest voting. This rule also limits the ability of byzantine arbiters to damage the amount of trust in an arbitration corporation, as dishonest voting can only happen a single time before the dishonest voters are stripped of all stock.

The result is a system that provides high trust agility for traders, enables permissionless participation for both arbiters and traders, and has a robust strategy for managing arbiter subjectivity.

7 Discussion and Potential Future Research

7.1 Incentives within Corporate Arbitration

Within corporate arbitration, arbiters are incentivized by the income provided by arbitration, and incentivized by increasing the total value of their corporate stock. There is a competing incentive to cheat on PM arbitration, because a large financial payout can be achieved by buying the losing shares of the PM and then voting dishonestly. For incentive compatibility, the value of the corporate stock must be able to drop farther than the most amount of money that can be earned by cheating. The value of corporate stock is determined by the corporate revenue, meaning that the corporate revenue must be high enough to drive the stock value above the potential cheat income.

Arbitration difficulty is largely uncorrelated to the amount of money being thrown at an event. In a free market, the corporations with the lowest fees are likely to attract the most trade volume. Because arbitration is not difficult, corporations may be able to drive the arbitration fee substantially down, below the point that gives the corporate stock enough value to decentivize cheating. Large events may be inherently unstable. Traders are required to have an awareness that trading on PMs which have low fees is potentially dangerous, because the incentive model no longer favors correct PM resolution.

7.2 Freeloading Arbitration

An consensus system can be established which observes a DPM. When a PM is announced, the consensus system can offer zero-fee trading on the results of the PM. When the event is resolved, the consensus system can enforce that the results of the free trading resolve identically to the resolution of the DPM being observed. Traders have incentive to participate in the observational consensus system because there are zero fees and because they receive the full security of the results in the DPM being observed.

This freeloading causes instability across both systems by creating a new source of income for cheating arbiters without contributing to the security that is provided by paying the fee. So long as the amount of freeloading is minimal, things should remain stable and the freeloaders will be rewarded for freeloading. This is a tragedy of the commons [16], where participants can extract value from a common resource (the DPM arbitration) at no cost while having a detrimental effect on security.

To date, there is no known solution to the problem of freeloading in DPMs.

7.3 Applying the BAR Model to the Real World

This paper assumed that most participants on the network were rational, and that only a few participants fell into each of the categories of byzantine and altruistic. While it seems like a reasonable model, there is little scientific evidence that it effectively maps to the real world. Further questions arise when considering the types of incentives that can influence various participants. Some participants may engage in exclusively short term behavior, while others may engage in long term and meta-rational behavior. Further exploration of participant behavior and motivation in real world financial systems and decentralized systems would be useful for tuning the inventive models used in the construction of incentive based systems.

7.4 Scaling Limitations

Bitcoin has significant scaling limitations. Solutions such as the Lightning Network [11] offer significant improvements to scalability but still fall short of being able to accommodate the entire population. DPMs are composed of a much higher number of assets, and have complex voting schemes which make scaling

significantly more difficult. Significant advances in technology and/or theory are necessary to bring DPMs to a global scale.

7.5 Miners are Low-Agility Trusted Entities

An important design consideration for DPMs was ensuring high trust agility with regards to trusted entities such as arbiters. The miners behind the Proof-of-Work blockchain are trusted entities. Participants have little control over miner actions, and have low agility in the event that the miners go rogue. This is largely accommodated by the incentive scheme, and is unlikely to be problematic when hashpower is sufficiently decentralized.

8 Conclusion

The features of decentralization have a lot of potential to add value when applied to prediction markets. One of the difficult problems associated with decentralizing prediction markets is reporting the outcomes of prediction events. Existing decentralized prediction markets have either vulnerable or centralized methods of achieving arbitration. While difficult, there are several strategies that can be used to achieve decentralized, permissionless, and secure prediction market arbitration.

9 Acknowledgements

Special thanks to Andrew Miller, Jeremy Clark, and Luke Champine for reviewing this paper. Additional credit belongs to the members of the Bitcoin development community who have spent many hours patiently teaching the uninformed and the curious.

Appendices

A Subjective Arbitration

In a decentralized system, participants are going to have a diverse set of worldviews. Some prediction market constructions require many arbiters to achieve consensus around the resolution of an event. Due to the differing worldviews of each arbiter, this can prove problematic.

Take for example the task of determining 'The price of a bitcoin on Jan 1st, 2016, at noon EST'. This prompt fails to specify what methods should be used for determining the price. Tickers such as Coinbase may feed different results to different queries. Some participants may be aware that coins are trading at a slightly different price in their jurisdiction. The price of bitcoin is ultimately not a fact that can be acertained through decentralized consensus.

Another example, 'Winner of the 2016 election for the chairman of the parent-teacher association at the Pleasant Hill elementary school in Illinois, USA', inhibits consensus through obscurity. Even if this information is published on the web, the relative irrelevance of the information may make the information difficult to find for arbiters, especially if there is a language barrier. Some arbiters may not realize the level of obscurity if they find the results after only a single attempt. Other arbiters may be unable to find the results even after extensive searching. This problem is amplified by the fact that arbiters can reasonably be expected to have varied skill levels with regards to finding information. For a prediction market that is obscure but not overwhelmingly obscure, consensus between a diverse set of arbiters seems unlikely.

A final example, 'Donald Trump will eat chips at the first cricket game he attends in 2016' is vulnerable to cultural differences between arbiters. The word 'chips' means different things depending on where you are in the world [7]. To make matters worse, Donald Trump is a citizen of the USA, indicating that the word should be interpreted according to American standards, but cricket is more of a British sport, indicating the British definition of the word should be used. A global set of arbiters is unlikely to arrive at perfect consensus should Donald Trump go to a cricket game and order a type of fried potato.

A strategy used by Truthcoin [17] attempts to detect when a question is unsuited for global consensus among arbiters. The standard criteria is that a question should be able to be answered within 5 minutes. This too is a subjective measurement. Arbiters that are good at searching the web may be able to find something in 30 seconds that takes other arbiters 10 minutes or more, especially if there is a cultural or language gap.

This problem becomes significantly worse under a model that assumes byzantine participants. An adversary can deliberately craft questions that appear innocent but will be unintentionally misinterpreted by subsets of arbiters due to subtle cultural or linguistic differences. For situations where arbiter consensus is required, individual participants cannot be in control of specifying the prediction market.

While many prediction market topics are ill suited to arbitration consensus, many are just fine. The following criteria defines a good prediction market topic:

- the result of the prediction market will be easily accessible to all arbiters
- the result will be accessible from many independent sources
- the result is well defined and does not use any difficult vocabulary or words with multiple definitions
- the result is difficult to dispute

An example of a good prediction market question is 'Will Donald Trump win the 2016 US Presidential Election'. The results of the US presidential election will be available globally, and from many different sources of information. The question does not contain any tricky wording, the event in question is obvious to everyone. The results of the event will not be questioned once the election is officially over. While there may be a dispute at some point, the dispute will eventually be resolved and a final decision will be made. As a bonus, the US Presidential election is difficult to manipulate, and is unlikely to be affected by the events within the prediction market.

References

[1] macbook-air. *A successful DOUBLE-SPEND US$10000 against OKPAY this morning*. March 12, 2013. https://bitcointalk.org/index.php?topic=152348

[2] https://sale.augur.net

[3] Dr. Jack Peterson, Joseph Krug. *Augur: a Decentralized, Open-Source Platform for Prediction Markets*. Accessed Octorber, 2015.

[4] Amitanand S. Aiyer, Lorenzo Alvisi, Allen Clement, Mike Dahlin, Jean-Philippe Martin, Carl Porth. *BAR Fault Tolerance for Cooperative Services* 2005.

[5] Gavin Andresen. *BIP: 50* April 5th, 2014. https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki

[6] Satoshi Nakamoto *Bitcoin: A peer-to-peer electronic cash system*. 2008.

[7] Wikipedia. *Chip*. 11 December, 2015. https://en.wikipedia.org/wiki/Chip

[8] Thomas C. Schelling. *The strategy of conflict*. 1960. Cambridge: Harvard University Press. ISBN 0-674-84031-3.

[9] Wikipedia. *Focal point (game theory)*. July 27, 2015. https://en.wikipedia.org/wiki/Focal_point_%28game_theory%29

[10] mmitech. *GHash.IO and double-spending against BetCoin Dice*. November 8th, 2013. https://bitcointalk.org/index.php?topic=327767.0

[11] Joseph Poon, Thaddeus Dryja. *The Bitcoin Lightning Network*. DRAFT Version 0.5. https://lightning.network/lightning-network-paper-DRAFT-0.5.pdf

[12] Jeremy Clark, Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Andrew Miller, Arvind Narayanan. *On Decentralizing Prediction Markets and Order Books*. 2014.

[13] K. J. Arrow, R. Forsythe, M. Gorham, R. Hahn, R. Hanson, J. O. Ledyard, S. Levmore, R. Litan, P. Milgrom, F. D. Nelson, G. R. Neumann, M. Ottaviani, T. C. Schelling, R. J. Shiller, V. L. Smith, E. Snowberg, C. R. Sunstein, P. C. Tetlock, P. E. Tetlock, H. R. Varian, J. Wolfers, and E. Zitzewitz. *The promise of prediction markets*. Science, 320(5878), 2008.

[14] John R Douceur. *The Sybil Attack*. 2002.

[15] Wikipedia. *Sybil attack*. December 7th, 2015. https://en.wikipedia.org/wiki/Sybil_attack

[16] Wikipedia. *Tragedy of the commons*. December 4th, 2015. https://en.wikipedia.org/wiki/Tragedy_of_the_commons

[17] Paul Sztorc. *Truthcoin: Peer-toPeer Oracle System and Prediction Marketplace*. Version 1.4.1, July 10th, 2015.