https://delphi.markets

Table of Contents

Introduction

Prediction Markets

> A prediction market is a powerful idea.
> A decentralized prediction market is an even more powerful idea.[1]

Prediction markets are platforms where participants are capable of creating, managing, and exchanging financial shares in *outcomes* or *events*. Put more simply, they are systems which allow people to make bets, and receive compensation if they are correct. The bets could be about anything (the winner of a presidential election, the price of gold at some date, or the final score of a particular sports match, to name a few examples); the important point is that *being right earns rewards.* Skin in the game not only motivates performance,[2] it attaches an incentive directly to honesty and truthful information sharing, which is ultimately the most reliable way to ensure that information becomes publicly available.

> People are fundamentally incentivized by money, and a system that allows people to monetize by betting correctly on outcomes drives better information in the world. This information could be used to create better policies, to build better businesses, and to broadly increase aggregate progress by humanity.[3]

It is extraordinary how effective prediction markets can be. They consistently outperform most sophisticated benchmarks,[4] exhibit unlimited scalability and can assist in the aggregation and distribution of unlimited quantities of information,[5] and are highly resistant to manipulation.[6]

In political forecasting, prediction markets have consistently yielded “extremely accurate” predictions and outperformed large-scale polling organizations. They have similarly been used to accurately forecast box office figures, award nominations, and product sales quantities.[4] They beat professional forecasters’ measures of macroeconomic performance by an average of 5%.[7]

Prediction markets have also seen resounding success in the private sector, forecasting Google’s IPO price better than Google did with its auction mechanisms, outperforming Hewlett-Packard’s official forecasts by as much as 70% in some cases, and continuing to be used internally in a myriad of ways by several multi-billion dollar corporations and interests.[7]

Finally, at least in some cases, prediction markets can help save lives. There have been multiple documented cases of prediction markets providing better and sooner forecasts of influenza and fever outbreaks than alternatives were capable of,[7] which is the sort of time-sensitive data that can be critical to the public health sector when it comes to the proper handling of and response to the spread of contagious diseases.

Clearly, prediction markets possess an impressive track record, and have already demonstrated great utility in recent history. Even so, we have only begun to scratch the surface of the true promise of this technology. The informational advantage that would be made possible by global, liquid, and low-friction prediction markets would unlock countless possibilities and benefits, perhaps even one day allowing us to upgrade democracy itself.[8][9][10]

Smart Contracts and Oracles

> Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way, while avoiding the services of a middleman.[11]
>
> Oracles provide an indispensable service by connecting smart contracts and distributed autonomous organizations with real world data and events.[12]

The original definition of a "smart contract" (coined by Nick Szabo in 1995) was given as "a set of promises, including protocols within which the parties perform on these promises",[13] but a more accessible definition and introduction for both smart contracts and oracles is given by Massimo Bartoletti and Livio Pompianu in *An empirical analysis of smart contracts: platforms, applications, and design patterns*:

> **Smart contracts** are computer programs that can be consistently executed by a network of mutually distrusting nodes, without the arbitration of a trusted authority
>
> **Oracle.** Some contracts may need to acquire data from outside the blockchain, e.g. from a website, to determine the winner of a bet. The Ethereum language does not allow contracts to query external sites: otherwise, the determinism of computations would be broken, as different nodes could receive different results for the same query. **Oracles are the interface between contracts and the outside.** Technically, they are just contracts, and as such their state can be updated by sending them transactions. In practice, instead of querying an external service, a contract queries an oracle; and when the external service needs to update its data, it sends a suitable transaction to the oracle. Since the oracle is a contract, it can be queried from other contracts without consistency issues.[14]

In simpler terms, smart contracts allow code to govern over economic interactions, and oracles are the services which allow that code to "see" the real world.

Beyond the actual contract specification (what it is coded to do), the oracle is the most critical component of any smart contract. Because the oracle determines the contract *input*, it also determines the contract *result* or *output*. Without a trustworthy or reliable oracle (whether it consists of a single party or a complex distributed service), a smart contract can be considered totally compromised.

In computer science, there is a principle and phrase: "garbage in, garbage out,"[15] which refers to program inputs; a useful or accurate output result cannot be reasonably expected from a program which did not receive quality input in the first place. Smart contracts, being digital executables themselves, are no exception to this rule. It has been argued that "the contract is the basic building block of a free market economy",[16] and any technological progress towards improving smart contract capabilities would be fully undermined by neglecting to ensure the quality of the input data and the source of it.

Because oracles serve as the essential link between what happens in the real world and the behavior or execution of a particular smart contract, they possess an enormous amount of power in prediction

market contexts. If the oracle is compromised, so is the entire contract; this is one reason why centralized oracle services are considered a significantly suboptimal solution.[17]

Information has value.

This is a corollary to *knowledge is power.* In much the same way that mass and energy are *equivalent,* or two sides of the same coin, so too are information and value. Despite this equivalence, there can be a friction associated with state changes between the two. Therefore, although blockchains already serve as very useful tools when it comes to the distributed transfer of value, there remains significant untapped potential in the realm of information acquisition, management, and transmission.

True information can be valuable, but the only way we can enjoy the full benefits of that value is to ensure that the information is available to those who can make the most use of it. With working, useful prediction markets in place, we can ensure that those with a knowledge surplus have the correct incentives to reveal that knowledge to others. In this way, the prediction market platform itself can provide value to the world, resulting in a positive-sum global ecosystem yielding a continual stream of societal benefit.

There is societal benefit to the smooth and efficient distribution of information; the more friction that exists in the media through which the information emerges and travels, the less of this benefit is realized. Too much friction, in fact, can prevent prediction markets from functioning at all.

Legality

> Unfortunately, however, current laws limiting gambling create significant barriers to the establishment of vibrant, liquid prediction markets… The legal questions here are complex...[18]

While the predictive accuracy and utility of prediction markets is beyond dispute, many significant jurisdictions around the world legally condemn them, generally classifying them as illegal under some form of gambling-related legislative umbrella. By far one of the worst historical sources of friction in terms of establishing a globally-inclusive, universally available prediction market platform has been legal resistance in one form or another.[19][20][21]

Despite numerous calls for reforms concerning the rampant over-regulation of prediction markets,[7][18][22][23][24] policymakers and entrenched powers have remained staunchly reluctant to relax or revisit the laws in place. These restrictions and their overzealous enforcements continue to stymie progress on the information frontier, lamentably preventing the world from reaching a deeper understanding of so many disparate subjects and events (both present and future).

Augur's whitepaper explains the crux of the problem:[25]

> Prediction markets are often disliked by powerful interests. As the experience of centralized prediction markets – such as InTrade and TradeSports – over the past decade has shown, if governments or special interest groups want to shut down a website, they will find a way:

> InTrade, after all, was an Irish company, shut down as a result of the U.S. Commodity Futures Trading Commissions actions[5, 6]. Even the Defense Advanced Research Project Agency and Central Intelligence Agency were forced to end their foray into prediction markets as a result of Congressional interference[7].

However, regulatory and legal friction are not inescapable. The advent of blockchain technology and the unique properties of distributed, economically-powered consensus networks have promised revolutionary potential. By providing a new, cryptographically-enforced and leaderless operational framework, blockchains have provided an opportunity to deprecate the traditional frameworks of legal or violence-backed interference. As the Cypherpunk Manifesto said so well: "We know that software can't be destroyed and that a widely dispersed system can't be shut down."[26] Later, the authors of *The Sovereign Individual* would echo the same sentiment with even more colorful rhetoric:

> Cyberspace is the ultimate off-shore jurisdiction. An economy with no taxes. Bermuda in the sky with diamonds.[27]

It might be argued that circumventing the restrictions and constraints of old-world legal institutions is a morally *wrong* thing to do, and that building a fully-functioning, open-access, uncensored prediction market platform is not necessarily a goal worth pursuing. However, we contend that the myriad benefits of prediction markets, both those demonstrated already and those yet-to-be-realized, do indeed justify the means by which the ends are achieved (even if it requires the authorship and maintenance of software tools constructed with direct capabilities of law circumvention).

Vision of Delphi

Catalyze information flow.

The deeper disruption potential of widespread, critical-mass prediction markets cannot be exaggerated. If we are able to build, maintain, and refine truth-reinforcing technology, we can strive towards an ideal of ubiquitous transparency and inimitable prescience. The low-cost ability to cooperatively exchange outcome-representative value tokens across the Internet will inevitably bring about huge increases in societal productivity and efficacy.

In the immortal words of the Nobel Prize winning economist Friedrich Hayek, from "The Use of Knowledge in Society" (written in 1945):

> The economic problem of society is thus… how to secure the best use of resources known to any of the members of society, for ends whose relative importance only these individuals know.
>
> ...practically every individual has some advantage over all others because he possesses unique information of which beneficial use might be made...

> ...the ultimate decisions must be left to the people who are familiar with these circumstances, who know directly of the relevant changes and of the resources immediately available to meet them. We cannot expect that this problem will be solved by first communicating all this knowledge to a central board which, after integrating *all* knowledge, issues its orders. **We must solve it by some form of decentralization.** But this answers only part of our problem. We need decentralization because only thus can we insure that the knowledge of the particular circumstances of time and place will be promptly used. But the "man on the spot" cannot decide solely on the basis of his limited but intimate knowledge of the facts of his immediate surroundings. There still remains the problem of communicating to him such further information as he needs to fit his decisions into the whole pattern of changes of the larger economic system.
>
> The price system is just one of those formations which man has learned to use (though he is still very far from having learned to make the best use of it) after he had stumbled upon it without understanding it.[27]

Hayek had a deep understanding of the relationship between information and value, and saw that Humanity was just beginning our exploration into the full potential of the efficient and open distribution of knowledge. We think that he would approve of what Delphi is trying to achieve today.

We aim to minimize informational friction. We believe that the most profound and empowering gift that we can provide society is the free and open flow of information. Furthermore, we believe that the widespread availability of prediction markets, functional distributed oracles, and high-quality interface toolsets has the potential to herald an information renaissance, and we intend to spearhead that movement.

Context

History

The basic principles which make prediction markets output such effective and accurate results so consistently are intuitively understandable, and have been discussed for centuries. It is easy to understand why having “skin in the game”[28] would elicit better results out of predictors, and the “wisdom of the crowd”[29] is a well-known phenomenon, and models of collective intelligence have been constructed.[30] Economists from Adam Smith to Friedrich Hayek have discussed the wonders of the emergent “invisible hand” of markets. However, due in large part to regulatory constraints and a lack of globally-available tools to allow parties to transact remotely, the growth of prediction markets in society has been aggressively stymied. As alluded to in Augur’s whitepaper (and in §1.4 of this paper), there is a history of steady regulatory interference when centralized prediction market platforms began to grow past a certain mass threshold.

Bitcoin, the Blockchain, and Ethereum

In 2008, Satoshi Nakamoto published the Bitcoin whitepaper[31], describing a new data construct and distributed ledger design that would come to be known as *the blockchain*. The blockchain is an antifragile[32] distributed economic engine that functions successfully because it relies on a deliberately structured incentive alignment; network participants acting in greedy and self-interested ways actually serve to support, protect, and bolster the network. This is a particularly powerful construct because networks (and in particular monetary networks) become more valuable and useful as they grow in size and usage.[33][34] This means that blockchain networks, once sufficiently bootstrapped, have the potential to establish positive feedback loops of growth. As the creator said during the debut of the technology:

> It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self fulfilling prophecy. Once it gets bootstrapped, there are so many applications if you could effortlessly pay a few cents to a website as easily as dropping coins in a vending machine.[35]

The blockchain provides a mechanism by which value and information can be nearly-frictionlessly shared, without risk of censorship, in globally-inclusive networks with cohesive, fairly-distributed liquidity pools. The potential for such a tool is virtually limitless, and it wasn't long after Bitcoin was released that experiments and explorations into the possibilities of blockchain technology began to flourish.

The most successful blockchain project after Bitcoin is undoubtedly Ethereum,[36] which allows gas-bounded Turing-complete computations to occur in a distributed manner. This allows Ethereum to function as a host platform and gateway to decentralized applications. Bitcoin allowed the world to *move value* across the Internet without middlemen or centralized gatekeepers for the very first time; Ethereum allowed the world to *run code* in the same way.

From the application end of things, the advantages of Ethereum-based design are obvious:

> Since it's run on Ethereum, it cuts out the middlemen and brings costs down to the economic minimum to operate things securely… [with fees of] 1% or less. For the first time people will be able to trade on a censorship resistant, global trading platform without having to trust counter-parties. Liquidity will be truly global because Ethereum **doesn't care** if you are from China *or* the US *or* Russia, you're just a pseudonymous address.[37]

For certain types of applications (in particular those that would benefit from operating on a cryptographically secure, decentralized, tamper-proof and hyper-resilient, hyper-available network), Ethereum is the best network available to build and live upon. Blockchains like Ethereum's serve as freedom-providing tools, allowing individuals to share their knowledge and wealth online without fears of being silenced or stopped by third parties, no matter who those third parties are. They might allow society to finally move past quagmires of legal impasse and achieve its full potential.

Augur

Augur[38] is an early prediction markets implementation, originally designed as an extension to the Bitcoin Core source code and using Bitcoin Script-based logic,[25] which later switched to an Ethereum smart-contract based architecture. The project's goal is "to democratize and decentralize finance"[37] and they held an ICO beginning in August 2015 which was preeminently successful (raising thousands of bitcoins worth millions of dollars at the time, which have furthermore considerably appreciated in value in the time since the auction took place) and the crowdsale was subsequently greatly acclaimed and celebrated.[39][40][41]

Gnosis

Overview

Gnosis[42] was originally announced in June 2016 as "decentralized prediction market platform and oracle standard"[43] and offers a number of conceptual improvements over the Augur design and implementation[44]. The project held a Dutch-auction based public ICO[45] in April 2017[46], which met with unanticipatedly high demand and criticism.[47][48][49][50][51]

Despite suffering from a number of shortcomings and fundamental design flaws, Gnosis has helped to push the state-of-the-art in prediction market technology and lay the foundation for superseding platforms such as Delphi.

The Gnosis Approach: What Was Done Right

Prediction Markets' Potential

The team at Gnosis clearly understand and appreciate the awesome potential of prediction market technology, and how beneficially disruptive ubiquitous usage of these tools would be. Their passion and dedication in this space is clear, and their commitment to further research in this wide new frontier is truly inspiring.

Ethereum-Based Architecture

Modeling prediction markets and oracles as smart contracts atop the Ethereum blockchain is the optimally rational decision. Ethereum allows execution "without any possibility of downtime, censorship, fraud or third party interference"[36] and is designed to host smart contracts natively. The high reliability of the Ethereum network and the the ERC20 token compatibility architecture (and the prospective liquidity such standards might provide) make an extremely compelling case for Ethereum to represent the base level of the stack.

General Implementational Approach

Using ERC20 standard tokens to represent *outcomes* or *state claims*[52] is another intelligent design decision. This allows for frictionless access to the liquidity base that the Ethereum ecosystem possesses, and a standards-compliant approach that will encourage cooperative development with other actors in the community. There are many benefits to this approach, and no clear downsides.

Clean and Modular Code Design

The Gnosis core contract codebase is quite well structured and abstracted, providing clean and flexible interfaces as well as considerable and accessible documentation. There is a general minimalism to the specifications, and the overarching decision to use a standards-based approach so that the market at large can furnish and experiment with the implementation specifics seems to be the correct approach on this front. By providing a de facto "Oracle API" for system participants to make use of, a meaningful market can emerge, with competing service providers vying for usage in the pursuit of transaction or service fees. Once again, Hayek's immortal insight that "the ultimate decisions must be left to the people who are familiar with these circumstances"[27] merits observation; let the oracle markets decide for (and compete amongst) themselves.

No Fees on Layer One

Gnosis provide an excellent breakdown of the rationale behind this decision in their whitepaper:

> The Core layer provides the foundational smart contracts for Gnosis use: event token creation and settlement, a market mechanism, oracle, and a management interface. **This layer is and always will be free and open to use. Creating new markets is near zero marginal cost, and to remain competitive fees will have to approach zero. Instead of grasping at the maximum possible fees while remaining competitive, we feel that it is prudent to eliminate fees at the most basic contract level.** It should be in every party's best interest to use the existing open source and feeless contracts instead of deploying their own version.[53]

This is a compelling argument, and makes complete operational sense.

Token Duality

There are two types of tokens used in Gnosis: GNO (10 million total tokens created prior to the ICO, have zero inflation, and are capable of generating WIZ via locking commitments) and WIZ (which are value-pegged, can only be generated via locking GNO tokens, and are used to pay fees on the Services layer, manage subsidies, and market trading).[53] This model adds predictability to the platform costs and can provide use-reinforcing stability,[54] which is an immensely valuable platform property.

WIZ (Only) Fees on Layer Two

The provision of a standard, quantized and pegged-value/predictable-cost Service-fee token is an insightful approach to supporting a dynamic and growing prediction market ecosystem. The Gnosis whitepaper explains that they have strong expectations that "WIZ will be the overwhelmingly predominant method for paying fees in the Gnosis ecosystem"[53] (and in fact their platform is vulnerable if this does not hold true) and have heavily oriented their model around WIZ-usage. We believe that as long as the pegged-value Service-fee token is the *only* supported out-of-the-box fee vehicle, that this represents a commendable approach towards maximal protocol utility.

Long-Term Focus on State-Channels

Distributed network consensus systems suffer from endemically poor scaling properties,[55][56][57] so it is prudent and appropriate to dedicate resources towards the continued research into and refinement of state-channel solutions. Many use cases require superlinear-yield solutions like collapsible state-channels to reach their full potential. Long-term performance should absolutely be a priority for any project of this magnitude and scope.

The Gnosis Approach: Shortcomings and Criticisms

Although the Gnosis design was prudent in many ways, improving significantly upon the approach and model that Augur represents, there remains a great deal of room yet for continued improvement. Gnosis unfortunately suffers from a considerable quantity of flaws itself, some of which may prove fatal for the project's long-term viability. The mistakes, flawed assumptions, and missteps of Gnosis can be broadly divided into three separate categories: *Technological* issues, regarding the actual technical models and specifications of the underlying contract system, *Economic* oversights and blunders, and a general, abiding misalignment of project *Focus*.

Technological

Structure

On a technical level, Gnosis suffers from three fundamental structural risks and shortcomings: the protocol is susceptible to *Oracle Bullying*, there are drawbacks and risks associated with *Non-WIZ Fees*, and an over-concentrated token distribution exposes *Poisonous Token Incentive* vulnerabilities.

Oracle Bullying

As explained in the introduction of this paper, oracles and oracle service providers enjoy an enormous amount of power in prediction market contexts, as the final arbitrators of the inputs to the relevant smart contracts. Because of this, any weakness in a platform's oracle model has wide-reaching consequences and deep implications for the initiative as a whole. The oracle solution is the one component that cannot afford to be ignored or neglected.

While Gnosis did have the right idea in terms of outsourcing the oracle functions to the larger market, providing abstract and general interface specifications for others to extend and build from, the platform is to some degree predicated around and reliant upon a naive and gameable dispute-resolution model that they have termed the *Ultimate Oracle* approach, which represents a serious systemic vulnerability:

> "The Ultimate Oracle." From an overall architectural standpoint, in my opinion this is Gnosis' greatest weakness … many scenarios in which this oracle could fail. … In reality, the "ultimate oracle" would become the "ultimate bullying platform." Essentially, the truth wouldn't matter at all in resolving these markets. All that would matter is who has the biggest pile of ETH with which to challenge and vote with.[17]

The same analysis concludes:

> In summary, Gnosis' planned oracle systems are one of its greatest weaknesses. If they use a centralized oracle, a decentralized platform is pointless. And if they use their proposed decentralized oracle, their system will be rife with scams and bullying.[17]

The Risks of Non-WIZ Fees

The Gnosis whitepaper makes note of a worrisome possibility:

> It is expected that WIZ will be the overwhelmingly predominant method for paying fees in the Gnosis ecosystem. In the unexpected event that this is not true, and users are paying in BTC or ETH, the platform may become vulnerable… [which] may logically cause erosion of the Gnosis userbase, subsequently triggering justified loss of developer confidence...[53]

The team has attempted to protect against such risks with complex and unproven new market-parallel fee-bidding mechanisms, but this unrigorous and indiscriminate approach involving chains of dubious assumptions simply exposes the platform to other classes of vulnerabilities (perhaps even more serious than those originally in question). The Gnosis whitepaper explains that the project maintainers are ultimately assuming (and hoping) that the mechanisms do not end up being widely used:

> NOTE: It is unlikely that this mechanism will be used as game theory and expectations point to users predominantly paying fees in WIZ. In the event this mechanism is triggered, we expect the occurrence to be extremely rare.[53]

As long as these game-theoretical assumptions of Gnosis (which are subject to considerable doubt) manage to hold true, and assuming furthermore that the complex and currently-underspecified technical scheme for their new fee-bidding mechanism manages to be implemented devoid of bugs or errors, this vulnerability should not result in any catastrophic problems for the platform. However, we feel that this trade-off incurs too much risk, for scant benefit.

Asymmetricalities and Poisonous Token Incentives

Although the dual-token model of Gnosis does introduce predictable-costs into the system structure, it also invokes a subtle but profound risk vector if too much of the *generator* token is concentrated into too few hands. As we will show later, this is the exact situation Gnosis is currently in.

From the Gnosis whitepaper:

> Gnosis Wisdom (WIZ) can be used to pay platform fees on the Services layer, subsidize the fees of other participants, provide initial subsidies for markets, or for market trading. **WIZ will be pegged to $1 USD worth of fees.** In this way, WIZ acts as a coupon for $1 of use within Gnosis. **Gnosis tokens (GNO) are the generator for Wisdom token (WIZ) creation.**[53]

This presents a poisonous incentive imbalance if the *generator* token (GNO) is significantly under-distributed. It is illustrative to summarize and rephrase the model above: holding GNO allows the bearer to literally print money (at least within the contexts of the system). Therefore, if one or very few entities were in direct control of a significant majority of the outstanding GNO supply, they would possess unique powers to create vast quantities of money at will, into perpetuity, without any regard to contextual network usage or demand levels; a fundamentally absurd proposition, clearly demonstrating the severity of the oversight in this matter.

Focus

In terms of technical resources, Gnosis appear to be concentrating their future efforts into questionable technological frameworks and potentially heavily-misguided engineering efforts. Specifically, the architectural decision to distribute resources via *IPFS* has no legitimate justification, and the investment of significant capital into the development of a blockchain-based document-search tool (*GnosisDB*) are egregious cases of resource misallocation. Furthermore, Gnosis have already exhibited a distinct lack of attention paid to the *User Experience* in general, which shows a serious misjudgment of priorities.

IPFS

The Gnosis whitepaper explains that “Gnosis is using IPFS to store all static files gnosis.js or any UI element. In addition meta information of events is stored in IPFS”[53] but provides no justification for the utilization of a distinct external blockchain. There do not appear to be any sound reasons for involving IPFS at all, and we estimate that doing so would introduce at least an order of magnitude more complexity into any relevant technological processes’ design and implementation. This decision seems particularly poor from an architectural standpoint, as the introduction of a superfluous secondary blockchain such as IPFS will also inevitably incur additional marginal overhead, resulting in poorer experiences for end users and lower-quality final products due to inefficient resource usage.

GnosisDB

Similar to the lack of supportive reasoning regarding the intent to integrate with IPFS, Gnosis' decision to focus their effort into the construction of a pseudo-decentralized database appears to be a design decision without any real benefits. The expressed intent is allegedly to "compensate the shortcomings of Ethereum and IPFS, which come without search capabilities... and will be used to query event descriptions of prediction markets"[53] but this makes the unfounded assumption that such functionality should be a priority in the first place.

While GnosisDB may indeed expand certain types of blockchain search capabilities, this is orthogonal to the goal of building and maintaining robust and efficient prediction markets, as persistent and indexed decentralized storage is not a prerequisite for prediction market functionality.

The event descriptions needed for the prediction markets can be accessed or served by a wide variety of existing solutions (in fact, a standard block explorer would work, plenty of which already exist), without incurring the additional costs of distributed system overhead. In fact, Gnosis themselves directly acknowledge the underlying issue with their own design:

> **Storage of data on a blockchain is very expensive.** The blockchain should only be used to verify the accuracy of information.[53]

Once again, the decision to invest significant resources into the research and development of broad-scope systems like GnosisDB which do not provide real value to the platform and network represents a source of project uncertainty. Such focus implies a more general problem with regards to Gnosis management's priorities and the overall decision-making process when it comes to the project's resource allocations over longer time horizons.

User Experience (UX)

There is always opportunity cost when it comes to resource expenditure, and in the case of Gnosis, it seems that their singular concentration on the development of complex technologies like GnosisDB with IPFS integration has come at the cost of attention to end-user experience. The current official front-end and interface for Gnosis interaction is available at https://admin.gnosis.pm/ and even a brief visit will inevitably leave any user immensely dissatisfied and underwhelmed.

Gnosis have demonstrated beyond any doubt that the experience of the user is a secondary or tertiary concern to them; resources and funding are dedicated towards unconventional pursuits like GnosisDB and legal expenses rather than on user-centric improvements and developments.

Economic

Although Gnosis has multiple outstanding technical issues, the economic problems of the platform are in many ways even more controversial and concerning. In particular, the massive *Wealth Distribution* issues have particularly dangerous implications for Gnosis as a whole, the team has made a number of

dubious *Economic Assumptions* in their approach, and some of these assumptions have already been empirically proven invalid by the *Results* of the project's initial coin offering.

Wealth Distribution

> ...the resulting sale was arguably anything but usual – concluding in less than 15 minutes and with the creators owning the vast majority of the funds (95% worth more than $280m at press time)...[47]

Although it was very successful in terms of raising funds to finance further development, the Gnosis crowdsale was, in economic terms, a catastrophic event for the long-term prospects of the Gnosis platform. This is because the GNO/WIZ token contract details strictly require an open and competitive market in order for the arrangement of incentives to work in the first place, and an excessively concentrated distribution of token ownership would prevent such a market from being possible.

There are a few reasons why wealth concentration is such a serious problem for Gnosis. Firstly, the system is designed so that non-WIZ fees (fees paid in ETH or BTC) are able to be accessed and claimed via a GNO-exclusive bidding system:

> If fees exist in the auction contract, any GNO token holder can submit a bid, bidding their held GNO against some amount of fees contained in the auction contract. If the bid is accepted, the GNO will then enter the auction contract and the user will receive the fees specified.[47]

This means that a single entity having possession of a disproportionate quantity of total GNO tokens would wield intolerable power. No Service-layer fees could ever be truly safe from central-power poaching; all auction contract would suffer from a remote-override vulnerability. To put it bluntly, every single fee ever paid on the Gnosis platform would be at risk of direct and irreversible theft. This has dire repercussions for the efficacy of the prediction markets on Gnosis, because it represents the introduction of a massive source of friction, and furthermore serves to defeat the purpose of operating on a distributed platform at all. If users are not able to meaningfully bid or participate in the fee-auction system, and if the paid fees are perpetually in danger of being claimed by a "super-whale" (whether that is the result of corporate negligence within Gnosis, a rogue or disgruntled employee with sufficient private-key access to effect hazard, or any of a long list of other similar possibilities that result in the same general outcome), then the platform cannot be trusted, and there are sound reasons for would-be users to withhold knowledge that might otherwise be shared out of self-interest.

Haphazard Assumptions

Because the Gnosis core contracts are designed so that GNO tokens are capable of generating WIZ tokens, and because WIZ tokens are pegged to a dollar in value, in order for the overall system to be sustainable, it is required that GNO tokens are reasonably well distributed among economic participants in the market. In other words, a significantly lopsided token distribution would put the entire balance of Gnosis incentives in jeopardy, preventing the open market from fulfilling its duty.

Because a fair token distribution plays such a critical role in allowing Gnosis to do what it was designed to do, the team decided to take an unorthodox approach with their ICO and crowdsale:

> The idea behind the "dutch-style auctioning system" was for the tokens to grow less expensive over time, thereby encouraging investors to buy in later, prolonging the time it would take for users to buy up all the tokens.[47]

After Gnosis announced the details of the Dutch auction crowdsale, but before the ICO actually took place, there was considerable discussion in the community regarding the potential possibilities of how the sale might play out. It was generally agreed that as long as the game-theory assumptions of the Gnosis team held up, and the auction mechanism did its job of preventing too many buyers from claiming the entirety of available tokens too early on, that the final distribution would be acceptable and the project would not be at risk of being economically compromised.[48]

> But, that's not what happened. Further, Gnosis did not add any cap on the amount of tokens that the team would receive, as is typical for other projects… **the incentives of the new system didn't work quite as intended** … the Gnosis token sale architects should have expected the crowdsale to play out the way it did, with investors rushing to buy the tokens before others…[47]

The fact that Gnosis was so blindsided by the auction results (which some have described as "completely expected"[47]) is itself a cause for alarm. We have been able to identify numerous invalid and flawed assumptions that the team have made in our analysis of their project, and the token auction represents incontrovertible proof of the team's deficiency in terms of game theory analysis. Worst of all, because cryptoeconomics is such a complex field, it is also very likely that there are other oversights and controversial conclusions that have gone into the project's design and execution. Some of these miscalibrated hypotheses could very well represent critical, system-threatening vulnerabilities, and the empirical evidence we have available at this time casts serious aspersions on the abilities of the team at Gnosis; when an organization demonstrates a low standard of rigor when it comes to underlying theory, it is generally a strong indication of deeper and more pervasive problems in the organization's approach and implementation.

Results

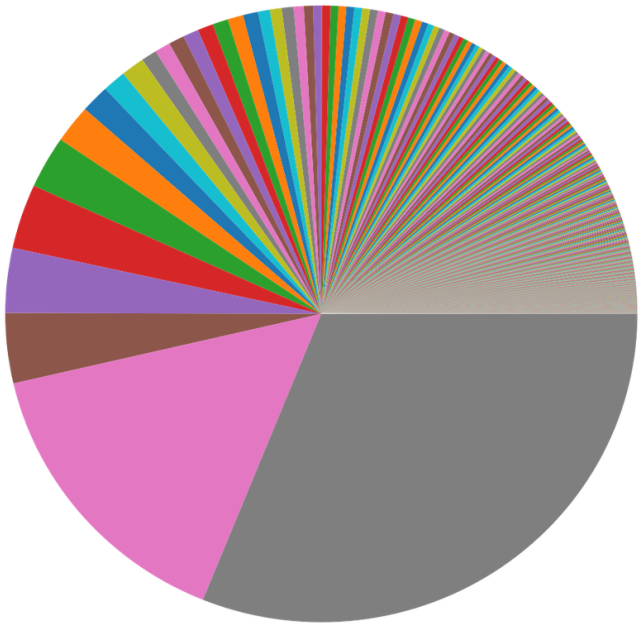
Contrary to what the team was expecting, the Gnosis ICO sold out in a matter of minutes. What would normally be a cause for celebration in this case actually represented a fundamental economic threat to the network,[48] and prospective users and investors expressed extreme dissatisfaction with the auction results:

> ...investors didn't know the details of what they were investing in, and [many later demanded] that a "redo" might be order to more equitably distribute the funds.[47]

It is not surprising that so many called for a "redo" of the auction, because the actual results of how the tokens were ultimately distributed were incredibly disconcerting, especially when seen from a "wealth distribution" standpoint (bearing in mind the risks discussed above):

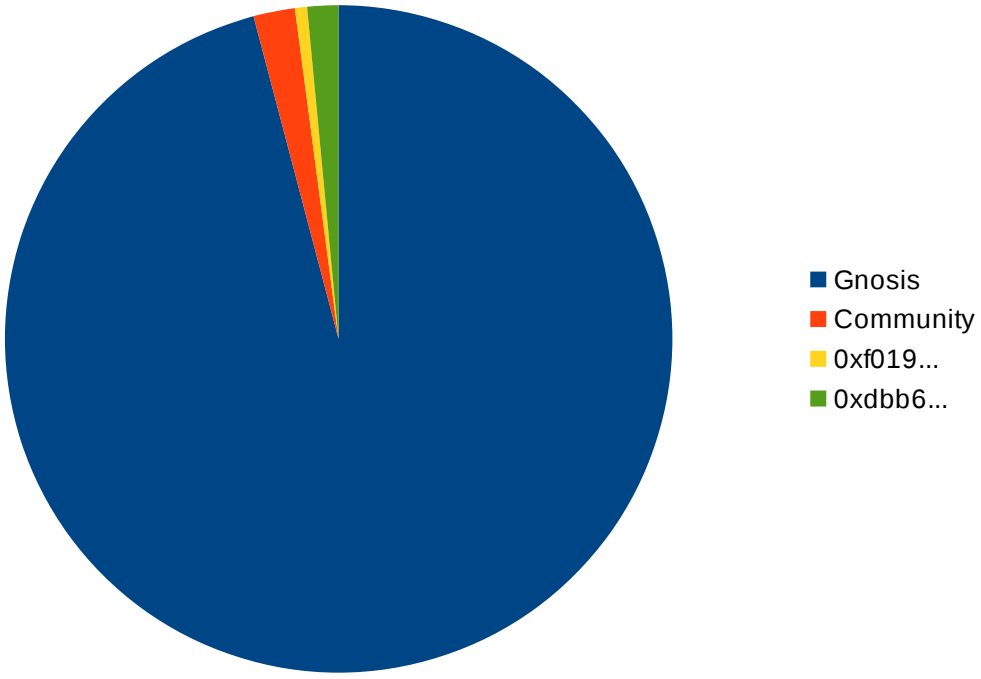
> The biggest transaction was this one with 77777.7 ETH ($3888107). The second one was this one with 38157.0553621044 ETH ($1907471.1975516).
>
> Between these two transactions, they accumulate more than the 46% of the tokens sold during the ICO.[49]

To reiterate the above: *almost half of the auctioned GNO wound up in the hands of **two** bidders.* Here is a graph depicting the results of the auction (showing only the coins that were sold – less than 5% of of the total supply – and omitting the Gnosis holdings that make up the other 95+%):



In light of the platform's economic requirements, the concentration of the auctioned tokens into so few hands is cause enough for alarm itself, but the problem is actually far worse than that. The graph above shows only the *auctioned* GNO tokens, but because the Dutch auction offering didn't transpire as the team expected or intended, this wound up representing only **4.17%** of the total token supply (the other **95.83%** of the tokens being issued to the Gnosis team). This had been projected as a potential "doomsday" scenario prior to the ICO on Reddit, and the final results of the auction prompted widespread criticism and discontentment in the community.[48][50][59][60][61][62][63]

In the end, the actual "economy" of Gnosis, the users themselves, own only **2.25%** of the total token supply. The final token distribution is depicted in the following graph:



Such an imbalanced and lopsided distribution of network tokens serves as a massive deterrent to adoption and usage of the host platform, serving to stymie any potential of legitimate market competition in a fundamental way. From the average prospective user's point of view, it would be economically irrational to use or build on the Gnosis platform: "The game is rigged," so to speak.

In summary, Gnosis relies upon a fair and balanced GNO token distribution, so the team expended significant resources and effort towards attempting to ensure their token auction resulted in a balanced and well-spread-out issuance profile. However, the results of the auction ultimately served to demonstrate how egregiously mistaken the team's assumptions and game theoretical foundations truly were, and the ICO culminated into a radical economic imbalance that jeopardizes the underlying platform's market integrity in a number of ways. When all is said and done, the GNO token supply lacks any meaningful economic distribution, which unfortunately has profound implications in terms of limiting the ultimate efficacy of the platform.

Focus

Building a full-fledged global prediction market platform is an ambitious goal which would demand a great deal out of any organization or team. The allocation of resources (both tangible and intangible) and general framework that the team operates within are important factors in the determination of whether or not such a project ultimately succeeds. If too much capital is invested into ineffectual enterprises, the final product will not achieve its true potential. The vision, direction, and strategy of an organization are vital elements to consider in any sophisticated project evaluation; approaching a

problem in the wrong way, and prioritizing the wrong things, will render any type of success considerably less likely.

Centralization

For all intents and purposes, the Gnosis team do not appear to consider decentralization or a fair distribution of protocol power and influence to be priorities. Critics have written incisive assessments of the platform's expected tendency to regress to centralized oracle dispute resolution:

> It appears that Gnosis plans on resolving most markets with a centralized oracle, which to some extent makes it pointless to run on a decentralized platform. While I don't disagree that centralized oracles would be simpler and likely faster, the point is that a centralized oracle is a point of failure for the system. Whether by regulatory pressure, outright prosecution, or corruption/fraud, relying on a centralized oracle goes against the spirit and idea of what a "Dapp" should be. You take out that "D," and you may as well just use Betfair, Fairlay, or any other number of options. There's no reason to use a blockchain or the Ethereum network if the most critical part of the system is going to be centralized.[17]

In point of fact, Gnosis has blogged that they estimate that due to the trade-offs inherent to their platform's design, *in less than 0.01% of cases* will the oracle function be decentralized.[44]

It has been made clear that the team does not consider inherent centralization chokepoints to represent vulnerabilities, which in turn makes clear that the team do not truly prioritize decentralization to begin with. The team has exhibited a habit of dismissing centralization-related concerns in general and ignoring community feedback and criticisms. Even the radical concentration of token holdings, despite the considerable controversy this has caused and the implications it has for the network as a whole (prompting some in the community to argue that "we are not so decentralized"[63]), serves to reinforce this point.

Legal

As explained in §1.4, the primary source of friction when it comes to building a critical-mass prediction market has historically been governmental regulation and interference. There is no evidence to suggest that this historical pattern will stop holding true now, or that governments will suddenly reverse their decisions on the subject and become more permissive and supportive of prediction markets initiatives. It is therefore irrational to expect or depend upon such an unlikely change of heart and policy.

Although the Blockchain has given us the means to bypass such anachronistic restrictions, Gnosis leadership have opted to channel their efforts into far-fetched attempts at effecting *legal reform* rather than focusing wholeheartedly on *technical refinement* of the tools that could make such reform irrelevant and unnecessary.

Gnosis do acknowledge the unfortunate fact of the matter:

> ...prediction markets have yet to attract mass attention in the realm of forecasting and decision-making despite their documented efficacy for information aggregation. **This is largely due to over-regulation** in many of the world's leading financial sectors… Traditional prediction market applications that operate on centralized platforms will tend towards proprietary designs, siloing data and reducing overall liquidity - a recipe for impotent markets that leave much to be desired in terms of accuracy and precision. Furthermore, these **databases lack the resilience necessary to resist censorship** and reach untapped liquidity pools across the globe, the effect of which suffocates any prediction market's viability as a platform and stunts its growth as a means of information exchange. [53]

However, in spite of this, a considerable fraction of the Gnosis whitepaper is dedicated towards a seeming obsession with regulatory compliance:

> **Legal Costs**
>
> Legal requirements include corporate setups in at least 3 locations for crowdsale, operations, and gaming licenses. Work has been done prior to token launch with a US law firm to develop a legal opinion of the interpretation with US law. Ongoing resources will be required for gaming and possible financial use case legal work. A legal contingency fund will be reserved in case of future issues
>
> ...the Gnosis team exercised extreme legal diligence in the lead-up to our launch … We will be responsive and collaborative with any regulators as necessary going forward … The Gnosis team and our advisors are aggressively pursuing strategies to bring the benefits of Gnosis and the information sharing economy to the globe as quickly as possible. First steps may include obtaining financial or gaming licenses as required by law[53]

The whitepaper even goes so far as to imply that the team may attempt to prosecute "illegal" forks and spin-offs of their core codebase, despite the fact that the code is open source and licensed under the GPL:[64]

> ...[Gnosis] may become vulnerable to low-fee copycats or potentially even illegal forks of the Gnosis codebase.[53]

This not only betrays a profound confusion regarding open source development and licensing, but also serves as another indicator of the fact that Gnosis do not value or prioritize decentralization and the benefits it can provide. The excessive emphasis on working within an existing and outdated legal framework, rather than pushing to expand beyond its limitations, represents a confusion of priorities and a surprising lack of appreciation for the value and strengths of a leaderless, decentralized, and censorship-resistant architecture. Furthermore, there is no reason to expect Gnosis to possess a special competitive advantage when it comes to legislative reform, so in all likelihood, resource expenditure towards this end is counterproductive and represents a real, tangible opportunity cost.

Delphi

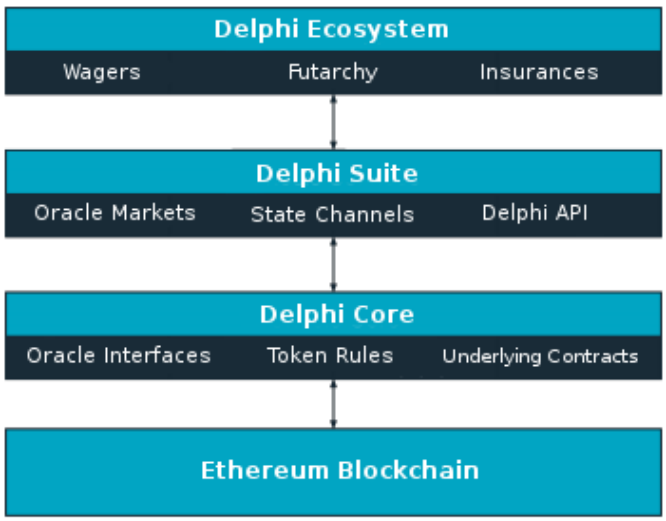
Delphi is economically sophisticated post-Gnosis prediction market technology. With Delphi, the shortcomings and design flaws of the Gnosis platform and model have been addressed. Solutions to all of the problems that currently plague Gnosis have been enacted, and extensions and improvements to the basic Gnosis framework have been carefully implemented.

We have made a deliberate effort to be maximally compatible with the Gnosis model wherever possible, including mirrored data-structures. The synergistic possibilities are even more profound because both tokens are ERC20 compliant and share the Ethereum blockchain. The free flow of information, and ensuring that informational and financial arbitrage is possible between the contract networks, has been and will continue to be a top-tier priority in the evolution of the Delphi project.

Beyond the technical refinements, the fatal economic oversights which fundamentally threaten the long-term viability of the Gnosis platform have been solved with Delphi's economic architecture and distributional model.

Delphi Stack

Like Gnosis, Delphi has been designed as a stack-based platform, with multiple layers defined so that the platform can be as robust and easily-extensible as possible. The general platform layout is inspired by the Gnosis approach, and does continue to use the Ethereum blockchain as the foundation upon which the stack is built, but the Delphi approach is more focused on ease-of-use when it comes to inter-layer integration, effectively allowing each layer to consider the layer below it a black-box API service, if desired.



Layers of the Delphi stack

Layer One: Delphi Core

Although low-level engineering improvements have been incorporated, Delphi have introduced no significant deviation from the Gnosis model when it comes to the purpose and functionality of the Core layer:

> The Core layer provides the foundational smart contracts for... event token creation and settlement, a market mechanism, oracle, and a management interface. This layer is and always will be free and open to use. Creating new markets is near zero marginal cost, and to remain competitive fees will have to approach zero.[53]

The dual-token solution that Gnosis have chosen for this layer has been used in Delphi, as well. Specifically, the Delphi platform involves two types of tokens: DEL (**∇**) and PHI (**Φ**).

Token Name	Symbol	Details
DEL	**∇**	*Generator* token (locked to generate PHI); price floats on open market (allows platform value speculation and demand-driven profit); supply fixed at 10M (zero inflation)
PHI	**Φ**	Used to pay fees, subsidies, and facilitate market-trading (on upper layers of the Delphi stack); price pegged to $1 (to allow predictable-cost usage); can be generated via locking DEL tokens (supply is not fixed)

Layer Two: Delphi Suite

If the Core contract code were all that were available for users to interface with, very few people could be expected to use the platform, and adoption would undoubtedly suffer. Rather than allow this to occur, Delphi offers a second layer, called Delphi Suite, intended to make the interaction with Delphi Core as smooth and frictionless as possible. The Delphi Suite provides the tools and APIs that will make widespread adoption (and upper-layer innovation) truly possible, and represents the efforts of our team to achieve user-friendly platform flexibility to the greatest extent possible. The final two components of the Delphi Roadmap, Pythia and Tholos, can be considered part of the Delphi Suite, and continued research into state-channel implementations will likewise be considered part of this layer.

Though Delphi's second layer is considerably more inclusive than that of the Gnosis model, the Delphi Suite layer is still most analogous to what Gnosis refer to as the "Gnosis Services" layer:

> The Gnosis Services layer will offer additional services on top of Gnosis Core and will use a trading fee model. These services will include a state channel implementation, new market mechanisms, stablecoin and payment processor integrations, open source template applications, application customization tools, and the oracle marketplace.[53]

Layer Three: Delphi Ecosystem

The Delphi Ecosystem layer will most likely cover the largest surface in the end, being comprised of many disparate applications and tools which interact with the lower layers of the Delphi stack. This layer would contain: modernized insurance and recreational gambling services; fund management providers (e.g. hedge funds) which take full advantage of the new dimensions of portfolio risk-management that global prediction markets enable; advertising and market-analytical consultancy services based around predictive insights; new decentralized governance models (for both society at large[9] and for cryptoeconomic systems like blockchains and DAOs[8]); and fully-functioning market pegs for the first time in history. This list is by no means exhaustive, and almost every listed example would, in turn, open the door to even more possibilities. This layer is built and maintained by the community itself, and will undoubtedly exhibit high levels of internal competition.

This layer is most analogous to what Gnosis refer to as the "Gnosis Applications" layer:

> On top of the Services layer (or in some cases, just Gnosis Core) is the Gnosis application layer. These applications are primarily front-ends that target a particular prediction market use case and or customer segment. Some of these applications may be built by Gnosis, while others will be built by third parties. Our vision for Gnosis is to have a wide variety of prediction market applications built atop the same platform and liquidity pool. These applications will likely charge additional fees or use alternative business models such as market making, information selling, or advertising… many Gnosis applications may include token holding as a core component of their business model.[53]

Although Delphi may possibly maintain and support some applications in this layer, as appropriate, the vast bulk of the team's effort will be dedicated towards ensuring that the lower layers of the stack are as robust and easy-to-use as possible. It is expected that the majority of the team's development effort will be concentrated specifically into supporting the middle layer: Delphi Suite.

Summary

Delphi represents the next evolutionary step forward in the development of a decentralized prediction market platform, incorporating numerous significant improvements over both the Augur and Gnosis models. In the same way that Bitcoin established a precedent which allowed subsequent initiatives like Ethereum to learn from and expand upon its shortcomings, Delphi has been able to leverage the research and work of prior attempts in the space. This is an excellent example of iterative development in action, where the successes and mistakes of initial explorations serve to inform subsequent initiatives. What Delphi is doing wouldn't be possible without Bitcoin, Ethereum, Augur, and Gnosis carving the way forward.

The following chart does an excellent job of demonstrating the salient point here:

Comparison of Decentralized Prediction Market Platforms

Feature	Augur	Gnosis	Delphi
Decentralized oracle	✔	✔*	✔
All funds held by contracts	✔	✔	✔
Markets resolve quickly	✘	✔	✔
Active token holder requirements	✔	✘	✘
Scalable	✘	✔	✔
Application ecosystem	✘	✔	✔
Market-based governance protocol research	✘	✔	✔
Cross-compatibility as a standard	✘	✔	✔
Resistant to Oracle Bullying	✔	✘	✔
Centralization-resistant	✔	✘	✔
Resistant to Poisonous Token Incentives	✔	✘	✔
Community-owned majority stake	✔	✘	✔
Predictable-cost usage	✘	✔	✔

* Expected to be centralized in more than 99.99% of cases.

Token Distribution (ICO)

The Delphi crowdsale is structured to avoid the complexity and pitfalls that plagued the Gnosis ICO. Most importantly, 95% of the total existing DEL (∇) will be issued to the community as a result of this crowdsale, inverting the Gnosis result and achieving a much more fair and even distribution of tokens, thereby avoiding the economic vulnerabilities that Gnosis is now susceptible to. The crowdsale is structured so that tokens are granted in two phases: 75% of the tokens are issued to the bidders of a standard half-month-long auction process, proportionally to final amounts invested, and 20% are issued as referral rewards to the auction participants proportionally to the final quantities associated with respective referral codes or addresses.

Standard Auction

Dates: July 1, 12:00 PM UTC – July 16, 12:00 PM UTC
Percentage of ∇ Auctioned: 75%
Total ∇ Auctioned: 7500000
Cap (Maximum): $50,000,000.00 (denominated in ETH, price established on July 1, 12:00 PM UTC via the ETH/USD volume-weighted price on GDAX)
Distribution: Total tokens received for any given participant will be in exact proportion with the ratio of the individual investment made relative to the total investment raised.

Referral Program

Percentage of ∇ Awarded: 20%
Total ∇ Awarded: 2000000

To encourage wider token distribution and in the effort to incentivize the market to achieve this in a straightforward manner, we have decided to allocate 20% of the total supply of DEL to the community members who help to spread the message and garner more participation in the Delphi crowdsale. The program follows a simple formula and structure: auction bid transactions are allowed to include referral identifiers (any address that has already bid in the auction is eligible, or alternatively an identifying code can be established with Delphi at any time before or during the standard auction), and at the conclusion of the auction, the referral-reward tokens are allocated amongst the referral-identified participants proportionally to how much was invested via their respective identifiers. As an example, if a cumulative total of 10,000 ETH was associated with referral identifiers in the auction, and your individual referral identifier is associated with 10 ETH of contributions, you would be entitled to $1/1000^{th}$ of the total referral program rewards, or 2000∇.

We believe that the overcomplicated Dutch-auction approach taken by Gnosis not only served to confuse the market, but resulted in a wild economic imbalance because of its reliance on shaky game-theoretical assumptions. This has grave implications for the platform as a whole, and has at very minimum resulted in a centralized, single point-of-failure for the system. In an effort to avoid such a similar fate for Delphi, we have opted to simplify the process to a more traditional and open-access crowdfunding approach. We feel that if the community doesn't truly own the project (both figuratively and literally), then it almost certainly will not succeed.

Roadmap

The Delphi Roadmap is divided into four high-level categories:

- Build (Alpha)
- Launch
- Pythia
- Tholos

Those aspects of the first two which are not self-explanatory have already been covered in earlier sections of this paper. The two remaining milestones are *Pythia* and *Tholos*.

Pythia

We have explained in §1.4 of this paper the importance of oracles in the context of prediction markets, but the point bears reiterating: in any smart contract that relies on some form of input from the real world (like the outcome of a particular event), the oracle has total power. As such, any attempt to build a distributed and trustless platform for prediction market operations must also incorporate a thorough and competent treatment of The Oracle Problem. To put it bluntly, no matter how well the rest of the system does its job, if the oracle is centralized, so is the smart contract. This implies the reintroduction of trust into the equation, and entirely defeats the purpose of using a smart contract or blockchain in the first place. A centralized prediction market solution is no solution at all; there is no value added.

To avoid reliance upon centralized oracle services, we have decided to break the problem down from first principles and use these insights to construct a framework within which the open market can optimize its own decentralized solutions through competition. We call this initiative *Pythia*, and consider it to be the most sophisticated and promising oracle market framework envisioned to date.

The Nature of Power

In cryptoeconomics, when it comes to (de)centralization, what we are actually concerned with is *power*. Naturally, a distributed system in which a single entity managed to gain complete control of the network would not be valuable to anyone else at all. A monopoly of power is antithetical to any purpose a blockchain or smart contract might serve, and as such, should be considered an intolerable and fundamentally irrational regression.

Recognizing this, the guiding principle of the Pythic approach is to lay a foundation in which it is very difficult for oracles' power to concentrate or centralize. We believe that ultimately, fair and open competition between selfish participants, with well-understood and rigorously expounded protocol models and rules, is the most reliable way to ensure that such a balance can occur.

Checks and Balances

Gnosis demonstrated wisdom with their insight to define a standardized oracle protocol (one which Delphi is fully backwards-compatible with), which allows the market to implement its own respective services, as long as they adhere to the basic specifications originally laid out by Gnosis. We have taken this one step further, not only providing oracle interfaces and specifications for open and free (that's "free" as in both beer *and* freedom!) use, but also modeling, defining, and implementing a new weighted-signature oracle solution that we believe is the most sophisticated treatment of the problem of sustainable and decentralized oracles.

The concept of a multisignature smart contract has been explored and modeled extensively,[65][66] and even basic multisignature contracts possess incredible and revolutionary potential when it comes to maintaining a useful power balance in decentralized systems. Multisignature schemes can provide a means of distributed checks and balances, preventing any one party from exercising too much control over the others.

We propose an additional innovation beyond a basic multisignature arrangement, when it comes to the determination of the oracle input on a given Delphi smart contract. A weighted signature framework is provided, in what we call a *Pythian Oracle* arrangement, which will provide a host of benefits over naive multisignature majority approaches, including understandable oracle interfaces for developers to work with, faster estimated input arbitration compared to Gnosis, and additional flexibility and extensibility moving forward.

Although the foundation for Pythia has been laid, further research, and in particular a rigorous dissection and exploration of the various possibilities within the framework (e.g. introducing time- or contract-dependent decay functions to the relative signature weights) will be a continued and abiding focus in Delphi. Providing the supportive tools for a sophisticated decentralized oracle marketplace represents a core component of the team's vision, and will not be deprioritized in favor of building superfluous database contrivances or hiring expensive lawyers.

Tholos

> "**User experience is everything.** It always has been, but it's still undervalued and under-invested in. If you don't know user-centered design, study it… **Obsess over it.** Live and breathe it."
> ~ Evan Williams, Twitter Founder and CEO[67]

Vision

The data shows that it is absolutely critical to create an enjoyable experience for the user.[68][69][70] Companies like Apple have shown that attention to detail when it comes to the impression that your products make on users makes all the difference. We believe that the field of UX has been woefully under-emphasized in the burgeoning Blockchain economy, and that most efforts and initiatives in the space have dedicated too few resources towards answering the question: "How can we improve the experiences that our users go through?"

Furthermore, we do not believe that this is a secondary or purely-cosmetic concern, because sufficient and well-distributed liquidity is crucial in a functioning prediction market system. The required adoption can only be achieved by devoting appropriate attention and emphasis into the dimension of user-interactivity and experience.

Tholos represents a vision of rich end-user experience; every interaction that a user has, at any level of the stack, should leave them feeling satisfied. We want our products and tools to be beautiful and to

function smoothly, at every step of the way, and we do not believe that this would be possible to achieve if organizational resources and capital is not wholeheartedly dedicated towards this end.

Top Priority

There is clearly a long road ahead before this industry is is fully matured, in terms of offering quality end-user experiences. As an illustrative example, the current sole interface for the Gnosis platform is available at https://admin.gnosis.pm and leaves much to be desired and considerable room for improvement; it is worth taking a moment to visit the page to experiment with the UI, to understand just how underwhelming the state of the application currently is.

The only realistic way to ensure that this condition is improved is to commit fully towards getting it done. How users feel about the platform and its tool-suite, and how to make them like it even more, should be the organization's guiding principle and top priority. The team at Gnosis appear to have a different focus, oriented around *legislative* and *judicial* efforts and emphasis. In contrast, Delphi boasts an emphasis on *technology* and *users*. We believe that if the platform is good enough at what it does, there would be no need to appeal to lawyers and politicians to improve the world. Rather than asking permission (and spending significant sums of money) to establish a presence in various jurisdictions around the world, we appreciate the fact that public blockchains provide a means of routing around counter-productive regulations, and will instead concentrate everything we have into improving the technology itself to do the job it was built to do in the most intuitive and usable way possible.

Liquidity is Necessary

With insufficient liquidity, a prediction market cannot properly function. An illiquid market would provide a disincentive to share information or wager according to one's knowledge privilege. To put it another way, in a prediction market, liquidity reduces friction.

To achieve appropriate liquidity, the objective must be mass adoption. Granting this, the experience of the end-user *cannot* be ignored. If the user experience is lackluster and the platform is difficult to use, mass adoption will never occur, and the promise of decentralized prediction markets changing the world for the better will never come to fruition.

More than Just Surface-Level

The user experience consists of much more than the pixels that reach users' eyes. Although aesthetics and visual appearances are important in terms of achieving the right impression, other factors can be just as important in determining whether users are satisfied with their experiences and interactions with the technology.

For instance, "timing is everything" when it comes to pleasing users. If a service takes too long to respond or an action takes too long to execute, it can have dramatic effects on users' perception of the situation; even fractions of a second can make a difference in some cases.[71][72]

Tackling the wrong problems, especially when doing so necessarily incurs costs in terms of execution time, can result in compounding user dissatisfaction. The decision to aggressively pursue a pseudo-decentralized GnosisDB architecture and to incur the distributed overhead that this trade-off inevitably implies is an example of deprioritization of the user experience.

At Delphi, we believe that further research and development into *sharding* and *state-channel* implementations is a very prudent and worthwhile use of time and resources, but we also understand that these innovations will not serve as silver bullets that eliminate all distributed-overhead costs. As such, we are committed to building and supporting these technologies moving forward, as well as any other innovations that may serve to bolster user satisfaction, regardless of whether the improvements and optimizations are visual in nature.

Long-Term, Moving Target

As with most complex design goals (such as the scaling of distributed networks), we will likely never be able to declare the job done, once and for all. Rather, the process is expected to be an iterative one, providing a moving target as the market evolves and matures. This means that in a general sense, Tholos represents the full commitment to improving the experience of users over the long-term, as the platform flourishes and grows and the market circumstances continue to change.

Conclusion

Paul Sztorc, one of the pioneering philosophers and researchers into cryptocurrency-based prediction markets, said it well:

> 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.[5]

It is easy to see that prediction markets have incredible transformative potential and could bring society spectacular prosperity on a number of fronts, but until blockchains and smart contracts came along, it has been impossible for any globally distributed prediction market initiatives to weather the overbearing regulatory friction. Following in the footsteps of Augur and Gnosis, and incorporating improvements over both models, Delphi aims to fulfill the promise of prediction markets. We will open the pathways that allow and encourage information to flow freely, make it in everyone's best interest to express and communicate the truth, and grant society newfound powers of rationality and insight.

To quote Paul Sztorc, one final time:

> 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![5]

References

[1] : https://medium.com/@ConsenSys/why-how-decentralized-prediction-markets-will-change-just-about-everything-15ff02c98f7c

[2] : https://www.quirks.com/articles/the-power-of-prediction-markets

[3] : https://thecontrol.co/improving-the-flow-of-information-in-the-world-87396ca2d776

[4] : http://www.nber.org/papers/w10504.pdf

[5] : http://bitcoinhivemind.com/papers/1_Purpose.pdf

[6] : http://bitcoinhivemind.com/papers/5_PM_Manipulation.pdf

[7] : https://www.mercatus.org/system/files/Ozimek_PredictionMarkets_v1.pdf

[8] : http://bitcoinhivemind.com/papers/3_PM_Applications.pdf

[9] : http://mason.gmu.edu/~rhanson/futarchy2013.pdf

[10] : https://blog.gnosis.pm/how-prediction-markets-can-save-democracy-from-itself-a813a87cf9bd

[11]: https://blockgeeks.com/guides/smart-contracts

[12]: https://media.consensys.net/a-visit-to-the-oracle-de9097d38b2f

[13]: http://www.alamut.com/subj/economics/nick_szabo/smartC_gloss.html

[14]: https://arxiv.org/pdf/1703.06322.pdf

[15]: https://en.wikipedia.org/wiki/Garbage_in,_garbage_out

[16]: http://www.alamut.com/subj/economics/nick_szabo/smartContracts.html

[17]: https://medium.com/@Cryptokeeper/the-gnosis-oracle-system-1cf8b8956950

[18]: http://mason.gmu.edu/~rhanson/PromisePredMkt.pdf

[19]: http://www.cftc.gov/PressRoom/PressReleases/pr6423-12

[20]: https://www.bloomberg.com/news/articles/2013-03-11/what-s-behind-the-mysterious-intrade-shutdown

[21]: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol50no4/using-prediction-markets-to-enhance-us-intelligence-capabilities.html

[22]: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=984584

[23]: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1385778

[24]: https://link.springer.com/article/10.1007%2Fs11149-006-7399-z

[25]: https://bravenewcoin.com/assets/Whitepapers/Augur-A-Decentralized-Open-Source-Platform-for-Prediction-Markets.pdf

[26]: https://www.activism.net/cypherpunk/manifesto.html

[27]: http://www.econlib.org/library/Essays/hykKnw1.html

[28]: https://en.wikipedia.org/wiki/Skin_in_the_game_(phrase)

[29]: https://en.wikipedia.org/wiki/Wisdom_of_the_crowd

[30]: https://en.wikipedia.org/wiki/Collective_intelligence

[31]: https://bitcoin.org/bitcoin.pdf

[32]: https://en.wikipedia.org/wiki/Antifragility

[33]: https://en.wikipedia.org/wiki/Metcalfe's_law

[34]: https://en.wikipedia.org/wiki/Network_effect

[35]: http://satoshi.nakamotoinstitute.org/emails/cryptography/17/

[36]: https://ethereum.org/

[37]: https://medium.com/@AugurProject/augur-master-plan-42dda65a3e3d

[38]: https://augur.net/

[39]: https://medium.com/@TonySwish/augur-the-crowdsale-model-for-open-source-blockchain-decentralized-projects-b2eefc4cb7cc
[40]: https://bitcoinmagazine.com/articles/token-sale-exceeds-1-7m-augurs-reputation-isnt-money-1440027734/
[41]: http://cryptomining-blog.com/6095-augurs-reputation-crowdsale-finishes-with-over-5-million-usd/
[42]: https://gnosis.pm/
[43]: https://bitcointalk.org/index.php?topic=1529098.0
[44]: https://blog.gnosis.pm/the-difference-between-gnosis-and-augur-c08077271a8e
[45]: https://blog.gnosis.pm/introducing-the-gnosis-token-launch-3cc4cffb5098
[46]: https://www.forbes.com/sites/rogeraitken/2017/04/24/gnosis-prediction-market-scores-12-5m-in-record-breaking-crypto-auction/#1b7ef2be87d1
[47]: http://www.coindesk.com/ethereum-ico-irrationality-300-million-gnosis-valuation-sparks-market-concerns/
[48]: https://www.reddit.com/r/ethtrader/comments/64ch1j/gnosis_crowdsale_price/
[49]: https://blog.icofunding.com/some-data-behind-the-gnosis-crowdsale-312656fe7dc8
[50]: https://www.reddit.com/r/ethtrader/comments/66b5qa/why_gnosis_is_a_scam/
[51]: https://www.reddit.com/r/btc/comments/67wfo4/how_the_initial_coin_offering_ico_scam_works_case/
[52]: https://en.wikipedia.org/wiki/Complete_market
[53]: https://gnosis.pm/resources/default/pdf/gnosis_whitepaper.pdf
[54]: https://blog.gnosis.pm/why-so-complicated-ddff533c5620
[55]: http://www.rgoarchitects.com/Files/fallacies.pdf
[56]: https://martinfowler.com/articles/distributed-objects-microservices.html
[57]: https://en.wikipedia.org/wiki/Distributed_operating_system#The_price_of_complexity
[58]: https://blog.icofunding.com/some-data-behind-the-gnosis-crowdsale-312656fe7dc8
[59]: https://www.reddit.com/r/ethtrader/comments/67ax24/to_all_gnosis_token_holders_take_a_seat_before/
[60]: https://www.reddit.com/r/ethtrader/comments/65q6to/the_gnosis_ico_summarized_in_a_3min_hitler_video/
[61]: https://www.reddit.com/r/gnosisPM/comments/63o02s/gnosis_crowdsale_psa/
[62]: https://www.reddit.com/r/ethereum/comments/67aeih/gnosis_ico_sold_out_in_10_min_300m_usd_valuation/
[63]: https://keepingstock.net/a-look-at-the-gnosis-dutch-auction-distribution-25c2ccac2d9d
[64]: https://github.com/gnosis/gnosis-contracts/blob/master/LICENSE
[65]: https://en.wikipedia.org/wiki/Multisignature
[66]: https://en.bitcoin.it/wiki/Multisignature
[67]: http://kevin.lexblog.com/2005/11/29/ten-rules-for-web-startups-evan-williams/
[68]: https://en.wikipedia.org/wiki/User_experience_evaluation
[69]: https://www.smashingmagazine.com/2010/10/what-is-user-experience-design-overview-tools-and-resources/
[70]: http://www.liftigniter.com/the-business-value-of-good-ux-why-user-experience-is-everything-2/
[71]: https://www.nngroup.com/articles/response-times-3-important-limits/
[72]: http://designingforperformance.com/performance-is-ux/